ООО «ДИАМАНТ ГРУПП»
Россия, Москва, Б.Черкизовская,
24А, строение 1
тел.: +7 (495) 646-88-71
E-mail: info@parsec.ru

ParsecNET 3.14.202

2024

© 2024 ООО "Диамант Групп"

Право тиражирования программных средств и документации принадлежит ООО «Диамант Групп».

Приобретая программный продукт, описанный в этом руководстве пользователя, Вы тем самым берете на себя обязательство не допускать копирования программ и документации без письменного разрешения ООО «Диамант Групп».
Москва, Сентябрь 2024.

Содержание

Глава I Введение....11
1.1 Общая характеристика....11
1.2 Новое в версии 3.14....15
1.3 Требования к компьютеру....16
1.4 Требования к SQL Server....20
1.5 Количественные ограничения системы....21
1.6 Ограничения версий....22
Глава II Быстрый старт....24
Глава III Типовые роли....26
Глава IV Установка системы....29
4.1 Установка дополнительной рабочей станции....34
4.2 Обновление системы....35
4.3 Удаление системы....36
Глава V Вход в систему....38
Глава VI Пользовательский интерфейс....39
6.1 Инструменты....41
6.2 Рабочий стол программы....43
6.3 Свойства окон программы....45
6.4 Общие свойства редакторов....50
6.5 Блокировка внешнего вида....54
6.6 Средства поиска....56
Глава VII Обзор системы....57
Глава VIII Основные инструменты системы....60
8.1 Редактор оборудования....62
8.1.1 Добавление устройств....64
8.1.1.1 Замена оборудования....68
8.1.2 Настройка контроллеров доступа....69
8.1.2.1 Настройки NC-2000....71
8.1.2.2 Настройки контроллеров семейства NC-8000....76

8.1.2.3 Настройки лифтового контроллера NC-8000-E ... 84
8.1.2.4 Настройки NC-60K / NC-60K.M ... 85
8.1.2.5 Настройки NC-32K.M ... 95
8.1.2.6 Настройки NC-100K-IP ... 99
8.1.2.7 Настройки NC-100K-IP.M ... 104
8.1.2.8 Настройки контроллера распознавания лиц ... 108
8.1.2.9 Настройки дополнительного реле ... 112
8.1.2.10 Настройка релейного расширителя NMO-04 ... 113
8.1.2.11 Настройки картоприемника ... 113
8.1.2.12 Настройка группового прохода ... 115
8.1.3 Настройка IP-шлюзов ... 117
8.1.4 Настройка охранных контроллеров ... 117
8.1.5 Настольные считыватели ... 122
8.1.5.1 Настройка настольных считывателей ... 123
8.1.5.2 Работа с банковскими картами ... 125
8.1.6 Работа с картами Mifare Plus ... 125
8.1.6.1 SL0 в SL3 ... 133
8.1.6.2 SL1 в SL3 ... 136
8.1.6.3 Работа с SL3 ... 140
8.1.7 Алкотестирование ... 141
8.1.8 Временное отключение оборудования ... 149
8.1.9 Удаление и перемещение устройств ... 150
8.1.10 Контроль статуса оборудования ... 152
8.1.11 Построчный принтер ... 154
8.1.12 Системные дополнительные поля ... 155
8.1.13 Настройки считывателей QR-кодов Parsec ... 157
8.1.14 Управление рабочими станциями ... 159
8.1.15 Специальные режимы прохода ... 159
8.1.15.1 Проход под принуждением ... 160
8.1.15.2 Запрет двойного прохода ... 161
8.1.15.3 Жесткий доступ ... 163
8.1.16 Многосерверность ... 164
8.1.16.1 Установка и настройка ftp-сервера FileZilla ... 166
8.1.16.2 Настройка кластера ... 171
8.1.16.2.1 Настройка кластера. Периметр ... 177
8.1.16.2.2 Настройка кластера. Группа доступа ... 178
8.1.16.3 Передача данных вручную ... 179
8.1.16.4 Совместное использование объектов ... 182
8.1.16.5 Выдача идентификатора с совместной группой доступа ... 183
8.1.16.6 Журнал обмена ... 186
8.2 Программный контроллер ... 187
8.3 Редактор операторов ... 191
8.3.1 Безопасность ... 193

8.3.2 Создание групп операторов ... 194
8.3.3 Создание операторов ... 199
8.3.4 Дополнительные возможности ... 201
8.4 Редактор топологии ... 203
8.4.1 Создание территорий ... 205
8.4.2 Создание графпланов ... 208
8.4.3 Связь с камерами ... 211
8.4.4 Инструкции оператору ... 212
8.5 Редактор расписаний ... 213
8.5.1 Недельное расписание доступа ... 216
8.5.2 Сменное расписание доступа ... 219
8.5.3 Расписания рабочего времени ... 221
8.5.3.1 Недельное расписание рабочего времени ... 223
8.5.3.2 Сменное расписание рабочего времени ... 231
8.5.3.3 Присвоение расписания рабочего времени подразделению или сотруднику ... 238
8.5.4 Создание праздников ... 238
8.5.5 Дни-исключения ... 241
8.5.6 Создание расписания из копии ... 243
8.6 Редактор групп доступа ... 245
8.6.1 Создание группы доступа ... 247
8.6.1.1 Особенности лифтового контроллера ... 249
8.6.2 Привилегии ... 250
8.6.3 Сложные группы доступа ... 253
8.6.4 Расширенные QR-коды ... 253
8.7 Редактор персонала ... 255
8.7.1 Создание карточек персонала и подразделения ... 258
8.7.1.1 Дополнительные возможности ... 263
8.7.2 Дополнительные поля ... 264
8.7.3 Идентификаторы ... 268
8.7.4 Персональная группа доступа ... 270
8.7.5 Экспорт и импорт персонала ... 272
8.7.6 Действия с персоналом и подразделениями ... 279
8.7.6.1 Управление черным списком ... 280
8.7.6.2 Запрет и разрешение доступа ... 281
8.7.6.3 Изменение группы доступа ... 283
8.7.6.4 Изменение времени действия идентификаторов ... 284
8.7.6.5 Изменение роли группового прохода ... 285
8.7.6.6 Изменить данные ... 286
8.7.6.7 Переместить в подразделение ... 286
8.8 Монитор событий ... 287

8.8.1 Особые панели монитора событий ... 291
8.8.2 Отчеты монитора событий ... 295
8.8.3 Прямое управление устройствами ... 297
8.8.4 Часто используемые команды ... 299
8.8.5 Настройка звуков ... 300
8.8.6 Тревожные события ... 300
8.9 Отчеты по событиям ... 302
8.10 Отчеты по составу ... 313
8.11 Работа с шаблонами в отчетах ... 314
8.12 Специальные средства ... 317
8.12.1 Редактор организаций ... 317
8.12.2 Редактор заданий ... 321
8.12.2.1 Создание задания ... 322
8.12.2.1.1 Создание, сохранение и отправка на Email отчета УРВ ... 329
8.12.2.1.2 Сообщение в видеосистему IDIS ... 332
8.12.2.1.3 Управление неактивными субъектами доступа и идентификаторами ... 333
8.12.2.1.4 Управление заявками бюро пропусков ... 335
8.12.2.1.5 Создание отчета по событиям системы ... 336
8.12.2.1.6 Создание отчета "Не покидали территорию" ... 339
8.12.3 Редактор системных настроек ... 341
8.12.3.1 Лицензии и ключ защиты ... 344
8.12.3.2 Резервное копирование ... 346
8.12.3.3 Синхронизация с Active Directory ... 348
8.12.3.4 Биометрическая идентификация ... 350
8.12.3.4.1 Система биометрической идентификации Взор ... 350
8.12.3.4.2 Распознавание лиц (Onvif) ... 353
8.12.3.4.3 Алкотестирование, системные настройки ... 355
8.12.3.5 Контроль уникальности сотрудников ... 355
8.12.3.6 Настройки Бюро пропусков ... 356
8.12.3.7 Настройки рабочей станции ... 359
8.12.4 Мобильный терминал доступа ... 360
8.12.4.1 Создание и настройка мобильного терминала в ParsecNET 3 ... 360
8.12.4.2 Установка приложения на смартфон ... 364
8.12.4.3 Инициализация мобильного терминала ... 371
8.12.4.4 Идентификация по лицу ... 372
8.12.4.4.1 Отмена привязки кадра к субъекту доступа ... 377
8.12.5 Приложение Parsec.Сотрудник ... 380
8.12.5.1 Установка сервера приложения ... 380
8.12.5.2 Настройка сервера приложения ... 385
8.12.5.3 Конфигурационный файл ... 391
8.12.6 Telegram бот ... 393

Глава IX Текстовые сообщения....394
9.1 Мини-консоль....395
9.2 Настройка уведомлений....396
9.3 Отправка SMS через GSM-модем....398
9.4 Отправка SMS через интернет-портал....402
9.5 Отправка сообщения в Telegram....408
9.6 Отправка e-mail....409
9.7 Печать уведомлений....411
Глава X Настройка IP-камеры....411
10.1 Подключение и настройка....412
10.2 Использование камеры....414
Глава XI Дополнительные модули....417
11.1 Редактор шаблонов печати....417
11.1.1 Проверка шаблонов и печать пропусков....427
11.1.2 Импорт шаблонов из версии 2.5....430
11.1.3 Форматы штрих-кодов....431
11.2 Модуль бюро пропусков....432
11.2.1 Инструменты бюро пропусков....433
11.2.2 Инициализация бюро пропусков....434
11.2.3 Создание пула идентификаторов....436
11.2.3.1 Создание списка идентификаторов во внешних программах....439
11.2.4 Работа с заявками....441
11.2.5 Черный список....446
11.2.6 Отчеты бюро пропусков....447
11.2.7 WEB-заявки....451
11.2.8 Отправка QR-кода посетителям....454
11.3 Модуль учета рабочего времени....456
11.3.1 Особенности учёта рабочего времени....461
11.3.1.1 Поправки к рабочему времени....462
11.3.2 Отчеты УРВ (версия 4)....469
11.3.2.1 Построение отчётов УРВ....473
11.3.2.1.1 Отчет по автомобилям....474
11.3.2.2 Отчёт по опозданиям....476
11.3.2.3 Отчёт по отклонениям....477
11.3.2.4 Посещения за месяц....478

11.3.2.5 Приход/уход за месяц ... 480
11.3.2.6 Приход/уход за неделю ... 480
11.3.2.7 Табель за месяц ... 482
11.3.3 Отчёты по учёту рабочего времени ... 483
11.3.3.1 Построение отчётов ... 486
11.3.3.2 Отчёт по посещениям ... 489
11.3.3.3 Дифференциальный отчет ... 491
11.3.3.4 Уход раньше времени ... 493
11.3.3.5 Приход/уход за месяц ... 494
11.3.3.6 Кто ушел последним ... 494
11.3.3.7 Отчёт по опозданиям ... 495
11.3.3.8 Табель за месяц ... 496
11.3.3.9 Отчёт по отклонениям ... 501
11.3.3.10 Посещения за месяц ... 503
11.3.3.11 Табель за неделю ... 503
11.4 Модуль видеоверификации ... 506
11.4.1 Дополнительные возможности ... 515
11.5 Интеграция с системами видеонаблюдения ... 515
11.5.1 Система ИСБ "Интеллект" ... 518
11.5.1.1 Подключение и настройка ... 518
11.5.1.2 Использование системы ... 522
11.5.1.3 Автоматизация работы ИСБ "Интеллект" ... 525
11.5.2 Система GOALCity ... 527
11.5.2.1 Подключение и настройка ... 527
11.5.2.2 Использование системы ... 531
11.5.3 Система TRASSIR ... 531
11.5.3.1 Настройка ... 532
11.5.3.2 Подключение и использование системы ... 537
11.5.4 Системы Macroscop и LTV-Gorizont ... 539
11.5.4.1 Подключение и настройка ... 540
11.5.4.2 Использование системы ... 541
11.5.5 Система Milestone ... 543
11.5.5.1 Подключение и настройка ... 544
11.5.5.2 Использование системы ... 545
11.5.5.3 Плагин Access Control ... 549
11.5.6 Система Panasonic Video Insight ... 559
11.5.6.1 Подключение и настройка ... 559
11.5.6.2 Использование системы ... 562
11.5.7 Система SecurOS (ISS) ... 566
11.5.7.1 Подключение и настройка ... 566
11.5.7.2 Использование системы ... 568
11.5.7.3 Модуль распознавания лиц FaceX ... 572
11.5.8 Система IDIS ... 578
11.5.8.1 Подключение и настройка ... 578

11.5.8.2 Использование системы ... 579
11.6 Распознавание автомобильных номеров ... 580
11.6.1 Модуль распознавания автомобильных номеров Parsec ... 582
11.6.2 Система Dallmeier ... 583
11.6.3 Автопроходная на основе программного контроллера ... 584
11.6.4 Контроллер автомобильных номеров ... 588
11.6.4.1 Структура XML-документа ... 591
11.6.5 Распознавание автономеров NumberOK ... 591
11.6.6 Распознавание автономеров ИСБ "Интеллект" ... 593
11.6.7 Распознавание автономеров Hikvision ... 594
11.6.8 Распознавание автономеров Mobotix ... 598
11.6.9 Автопроходная на основе контроллера автономеров ... 601
11.7 Интеграция с системами ОПС ... 603
11.7.1 Система "Стрелец" ... 605
11.7.1.1 Подключение и настройка ... 606
11.7.1.2 Использование системы ... 612
11.7.2 Система "Стрелец-Интеграл" ... 616
11.7.2.1 Подключение и настройка ... 616
11.7.2.2 Использование системы ... 621
11.7.3 Система "Мурена" ... 624
11.7.3.1 Подключение и настройка ... 624
11.7.3.2 Использование системы ... 627
11.7.4 Интегрированная система охраны "Орион" ... 629
11.7.4.1 С2000-ПП. Подключение и настройка ... 630
11.7.4.1.1 Использование С2000-ПП ... 635
11.7.4.2 С3000-Hub. Подключение и настройка ... 638
11.7.4.2.1 Использование С3000-Hub ... 642
11.7.4.3 Взаимодействие систем ... 644
11.7.5 Система Firesec ... 646
11.7.5.1 Подключение и настройка ... 646
11.7.5.2 Использование системы ... 650
11.8 Интеграция с биометрическими устройствами ZKTeco и ЛКД ... 654
11.8.1 Настольный биометрический считыватель отпечатков ... 655
11.8.2 Настенный биометрический терминал ... 660
11.9 Интеграция с терминалами распознавания лиц ... 661
11.9.1 Интеграция с биометрическими устройствами Hikvision ... 663

11.9.2 Интеграция с биометрическими устройствами UniUbi 666
11.10 Интеграция с системами распознавания документов 671
11.10.1 Установка, выбор и настройка 674
11.10.2 Работа с документами 677
11.11 Интеграция с системой хранения ключей KeyGuard 680
11.11.1 Отчет о состоянии ключницы 683
11.12 Интеграция с домофонными системами 684
11.12.1 Система BAS-IP 685
11.12.1.1 Подключение и настройка 685
11.12.1.2 Использование системы 690
Глава XII Демонстрационный режим 691
12.1 Утилита наполнения БД 692
12.2 Эмулятор событий 693
Глава XIII Обращение в техподдержку 694
Глава XIV Контроллеры 696
Глава XV Список транзакций 698
Глава XVI Если вам надо 728
Глава XVII Контакты 733
Указатель 0

1. Введение

Добро пожаловать!

Вы уже установили или собираетесь установить систему ParsecNET 3. Это принципиально новая система, созданная с использованием самых передовых технологий разработки и предоставляющая максимум функциональных возможностей и удобство для пользователей. В зависимости от вашей конфигурации, вы получите либо простую в использовании небольшую систему безопасности, либо сложный многотерриториальный комплекс с возможностями централизованного или распределенного управления.

Программное обеспечение ParsecNET 3 обеспечит новый уровень надежности и безопасности, а также даст вам платформу на многие годы для расширения и развития.

В зависимости от целей и опыта, Вы можете начать работу с системой различными способами:

Если Вы хотите буквально за 10 минут запустить небольшую систему, обратитесь к разделу "Быстрый старт"

В случае, если планируется крупная установка, лучше начать изучение с раздела "Обзор системы[57]"

Детальное рассмотрение функций отдельных редакторов можно найти в разделе "Основные инструменты системы[60]"

Описание основных свойств пользовательского интерфейса находится в разделе "Пользовательский интерфейс[39]"

При наличии дополнительных модулей, таких как "Учет рабочего времени", "Видеоверификация", "Бюро пропусков" с их работой можно познакомиться в разделе "Дополнительные модули[417]".

Информацию о нововведениях данной версии продукта можно посмотреть в разделе "Общая характеристика[11]", а также в разделе "Новое в версии 3.14[15]".

Поскольку система постоянно развивается и улучшается, в документе могут быть расхождения с последней текущей версией. Самую свежую версию справки можно получить на сайте производителя. Мы также будем благодарны Вам за замечания, связанные с содержимым документа.

1.1 Общая характеристика

Программное обеспечение Системы Контроля и Управления Доступом (СКУД) ParsecNET 3 кардинально отличается от предыдущей версии с точки зрения внутреннего устройства и функциональных возможностей, поэтому пользователям, работавшим с предыдущими версиями, рекомендуется ознакомиться с данным разделом для понимания имеющихся отличий.

Сервер, рабочая станция и консоли оператора

В системе ParsecNET 3 существует два типа компьютеров - это:

- Сервер системы, отвечающий за все данные и обмен с другими компьютерами. При этом сервер СУБД может размещаться на отдельном ПК в сети.
- Рабочая станция — ПК, к которому может быть подключено оборудование, а также запущен пользовательский интерфейс.

Пользовательский интерфейс может быть полнофункциональным, либо на ПК может работать только нотификационная консоль, уведомляющая пользователя о выбранных событиях.

При этом все службы системы, обеспечивающие информационный обмен и работу с оборудованием, не зависят от пользовательского интерфейса. Эти службы запускаются автоматически при старте Windows еще до входа пользователя в систему.

Вы можете запустить службы, поддерживающие оборудование, на любом количестве компьютеров в вашей сети. Однако количество рабочих станций, на которых одновременно может быть запущен пользовательский интерфейс, определяется вашей лицензией.

Версии ПО и интерфейса

Предыдущая версия программного обеспечения (ПО) ParsecNET 3 за более чем десятилетнюю историю развития накопила некоторое разнообразие в части вида и интерфейса окон разных приложений.

Пользовательский интерфейс третьей версии полностью унифицирован, то есть все редакторы и инструменты имеют одинаковый внешний вид и эргономику. Это упрощает работу с системой, каким бы инструментом вы не пользовались.

Отдельно следует отметить, что теперь пользовательский интерфейс гибко настраивается под квалификацию и права конкретного пользователя, при этом настройки для любого пользователя сохраняются в базе данных (БД) и восстанавливаются на любом компьютере при входе пользователя в систему.

Программное обеспечение поставляется в одной из двух конфигураций:

- Стандартная версия (Standard) позволяет строить системы среднего масштаба. В ней можно заказывать различные конфигурации для получения оптимального по цене решения. При организации многосерверного[164] кластера лицензия позволяет установить связанный сервер на ПК;
- Профессиональная версия (Professional) позволяет создавать сложные многотерриториальные комплексы с организацией виртуальных подсистем. В ней уже включены практически все дополнительные модули, которые в стандартной версии лицензируются отдельно. При организации многосерверного[164] кластера лицензия позволяет как установить на ПК связанный сервер, так и назначить его мастер-сервером.

При этом в любой версии для неискушенных пользователей можно использовать сокращенный интерфейс пользователя (который включен по-умолчанию после установки системы). Если же требуются максимальные функциональные возможности программы, то используйте расширенный режим. Тип интерфейса в стандартной и профессиональной версиях можно переключить в любой момент работы с системой.

База данных системы

Базу данных (БД) системы поддерживает СУБД MS SQL Server 2012. Сервер СУБД может находиться как на компьютере, на котором работает сервер ParsecNET 3, так и на любом другом компьютере в сети. Главное условие — это доступность сервера СУБД со стороны сервера ParsecNET 3.

Локальные базы данных рабочих станций обслуживает более «легкая» и быстрая СУБД SQLITE, не требующая значительных ресурсов ПК и отдельной процедуры ее установки — она устанавливается автоматически в составе рабочих станций ParsecNET 3.

Локальные базы обеспечивают функционирование отдельных частей системы даже при отсутствии связи с сервером и центральной базой данных, что значительно повышает живучесть и функциональность новой версии. Например, временно отключенный от основной системы удаленный офис продолжит свое функционирование, информация будет накапливаться в локальной БД, а при появлении связи с сервером автоматически будет передана на него. Кроме того, после восстановления связи с сервером, с него будут автоматически скопированы все накопившиеся за время отсутствия связи изменения, включая изменения БД персонала, настроек оборудования и так далее.

Многопользовательская система

ParsecNET 3 является действительно многопользовательской системой. Она позволяет обслуживать территориально объединенные и распределенные объекты, административно

разобщенные объекты таким образом, что каждому пользователю представляется, будто он является единственным пользователем — не принадлежащая ему часть системы полностью изолирована и невидима для данного пользователя (концепция "виртуальных" систем).

Это хорошо поясняется примером крупного бизнес-центра, в котором арендуют площади множество компаний. Каждой компании выделяется часть системы, обслуживающая ее территорию (этаж, группу комнат или даже одна комната). В терминах ParsecNET 3 такая единица именуется организацией. Организация имеет обслуживающее ее оборудование, собственных операторов с различными правами, собственный персонал, которые видимы только в рамках данной организации. Другим организациям все указанные сущности принципиально недоступны.

Общие ресурсы

Если продолжить аналогию с бизнес-центром, то возникает проблема общих ресурсов, например, турникетов при входе в бизнес-центр. Данная проблема решается за счет того, что в системе ресурсы (контроллеры, турникеты, области охраны) могут назначаться более чем одной организации. Таким образом, вход в бизнес-центр, являясь типичным разделяемым ресурсом, может находиться в области видимости всех организаций, находящихся на территории бизнес-центра. При этом персонал каждой организации является ее «собственностью», то есть не виден другим организациям.

Многотерриториальная система

Система ParsecNET 3 является сетевой распределенной системой, позволяющей обслуживать любое количество территорий, между которыми существуют каналы связи (сеть Ethernet). В отличие от предыдущих версий, в которых при потере связи с сервером ParsecNET 3 функционирование рабочих станций полностью прекращалось, в ParsecNET 3 работа рабочей станции при потере связи с сервером продолжается, хотя и в несколько ограниченном объеме. Нельзя выполнять действия, которые связаны с доступом к серверу баз данных системы, то есть редактировать персонал или другие объекты системы. Мониторинг оборудования, сбор текущих событий, прямое управление подключенным на данной территории оборудованием сохраняется в полном объеме.

Более того, система поддерживает работу через сеть Internet - достаточно создать между удаленными территориями канал VPN, и вы можете работать примерно так же, как и в рамках своей локальной сети.

Иерархия объектов и сущностей

Все сущности в ParsecNET 3 организуются в виде иерархий с неограниченным количеством уровней вложенности, при этом видимость объектов для конкретного оператора может быть установлена с любого уровня вложенности. Имеется возможность создания специальных группирующих элементов, служащих исключительно для удобства логического разделения объектов системы.

Вернемся к примеру с бизнес-центром. Предположим, что требуется обеспечить видимость всего персонала всех организаций оператору на проходной, что противоречит принципу разграничения видимости между организациями.

В этом случае можно создать организацию «Бизнес-центр», в которую будет включен весь персонал, причем за его внесение в базу данных системы в этом случае может отвечать бюро пропусков бизнес-центра, а операторы соответствующих организаций — арендаторов будут видеть только свой персонал.

Инсталляторы и операторы

Для обеспечения структуры со многими организациями в системе вводятся различные роли для инсталляторов и операторов с четким разграничением их прав в системе. Для обслуживания физического оборудования системы, его конфигурирования, добавления или удаления в системе существует понятие инсталлятора, то есть оператора со специальными привилегиями по обслуживанию оборудования. Инсталлятор «видит» всю физическую топологию системы и имеет к ней полный доступ. Инсталлятор распределяет физические ресурсы (точки прохода, охранные области и так далее) между организациями. В обычных терминах инсталлятор — это тот, кто осуществляет конфигурирование системы на этапе ее запуска, а в дальнейшем —

обслуживающий персонал (например, техническая служба бизнес-центра). При этом инсталлятор принципиально не имеет доступа к приватным данным других организаций, к которым относятся персонал организаций, операторы организаций и их архивы событий (например, данные о проходах).

В свою очередь, операторы других организаций не имеют доступа к физическому оборудованию системы, за которое отвечает инсталлятор, то есть не могут добавлять или удалять оборудование, а также менять его настройки.

Для маленьких объектов, представляющих одну организацию, все права (как инсталлятора, так и оператора) может выполнять один человек, поскольку в организации «SYSTEM», устанавливаемой по-умолчанию, принципиально объединены все роли.

Автоматизация и задания

В систему изначально встроены некоторые средства автоматизации, в частности, редактор заданий, в котором можно с помощью простых средств определять реакцию системы на различные события, а также программировать события по времени. Одной из функций редактора заданий является создание резервных копий БД системы.

Кроме того, в систему встроена технология plug-and-play, которая позволяет автоматически найти подключенное к компьютеру оборудование и ввести его в состав системы.

Платформа для интеграции

Программный комплекс ParsecNET 3 построен как платформа для интеграции с любым оборудованием и программным обеспечением. С точки зрения внутреннего устройства, представления данных и способов их обработки ParsecNET 3 полностью индифферентен к типу оборудования, с которым необходимо работать. При наличии надлежащих драйверов ParsecNET 3 может управлять не только компонентами системы безопасности, но и кондиционерами, кофеварками и так далее.

На момент выхода коммерческой версии системы комплект драйверов поддерживает полную линейку оборудования торговой марки Parsec (кроме снятых с производства).

В дальнейшем номенклатура подключаемого оборудования будет постепенно расширяться как за счет интеграции с оборудованием сторонних производителей, так и за счет новой линейки оборудования Parsec, которое покроет все необходимые на сегодняшний день потребности пользователей.

Подводя итог,

можно сказать, что система ParsecNET 3 кардинально отличается от предыдущих версий по следующим основным позициям:

- Распределение областей видимости любых сущностей на уровне организаций, а внутри организаций — между группами операторов данной организации.
- Разделение функций обслуживания физического оборудования и текущей работы с компонентами системы.
- Обеспечение полуавтономной работы при временной потере связи с сервером системы.
- Работа в многотерриториальных комплексах с использованием в качестве канала связи сети Интернет.
- Работа основных служб на уровне служб Windows независимо от пользовательского интерфейса.
- Широкий спектр поддерживаемого оборудования, большого количества территорий, операторов и персонала.
- Обширные возможности по интеграции с оборудованием и программным обеспечением сторонних производителей.

Все это позволяет использовать ее на объектах любого масштаба с гибким распределением функций и областей видимости в соответствии с реальными задачами по обеспечению безопасности, управлению персоналом и различным оборудованием.

1.2 Новое в версии 3.14

Ниже перечислен новый и изменный функционал ПО ParsecNET 3 новой версии 3.14. Полностью заметки по релизу изложены в документе.

****=== 3.14.202.41 (от 05.09.2024) ===****

Изменения	Описание	Компоненты
Новый функционал		
	Добавлена поддержка нового сетевого контроллера NC-100K.M с БД емкостью до 200 тысяч пользователей.	Редактор оборудования HAL
	Для настольного считывателя PR-X18 добавлена возможность указывать типы карт, с которыми он будет работать.	Редактор оборудования
	Добавлена опция лицензирования интеграции с IP-видеодомофонами (PNSoft-IC) с максимальным количеством устройств.	
	Для программного контроллера SCL-02 добавлена функция постановки на блокировку.	Монитор событий
Изменения функционала		
	Для контроллеров NC-60K, NC-60K.M, NC-100K.M в режимах прохода «Парный проход» и «Проход с разрешением» добавлена возможность прохода в обычном режиме (Одна карта).	Редактор оборудования
	В групповом действии «Сменить группу доступа» добавлена возможность опциональной установки привилегий	Редактор персонала
	В групповом действии «Изменить время действия идентификаторов» добавлена возможность снятия временности с идентификаторов.	Редактор персонала
	При импорте персонала из CSV файла реализована поддержка длинных (8 байт) кодов идентификаторов.	Редактор персонала
	Теперь для настройки работы настольных считывателей с картами Mifare Classic требуется роль оператора «Настройка Mifare Plus»	Редактор оборудования
	Расширен функционал Мобильного Терминала: • Добавлен функционал локального антипассбэка • Добавлены события для контроля связи с устройством • Добавлены события для контроля действий оператора (вход\выход из приложения, а так же запрос синхронизации данных) Данный функционал доступен в мобильном приложении начиная с версии 2.1.129	Мобильный терминал

	Расширен функционал интеграционного сервиса (см. документ «Описание службы интеграции Системы Контроля Доступа Parsec»).	API, SDK
	В Web-заявках Бюро пропусков реализовано сохранение настроек фильтрации на странице списка заявок. Также, реализован механизм автоматического продления сессии оператора.	Бюро пропусков, Web-заявки
	Добавлена возможность указывать наименование действия «Текстовое сообщение» при формировании задания.	Редактор заданий
	Изменен режим работы с алкотестером «Алкобарьер» - не отправляется команда на остановку теста, что позволяет более комфортно контролировать результат проверки.	

=== 3.14.202.19 (от 26.02.2024) ===

Изменения	Описание	Компоненты
Новый функционал		
	Добавлен модуль Parsec.Сотрудник, предоставляющий возможность использования функционала СКУД на мобильных устройствах.	
	Добавлен режим прохода с использованием автомобильного номера в качестве второго идентификатора при двухфакторной идентификации. Режим доступен для контроллеров: NC-8000 (начиная с версии прошивки 4.3) NC-60K.M.	Редактор оборудования HAL
	Добавлена интеграция с системой распознавания документов Content AI PassportReader SDK.	Распознавание документов
	Добавлена возможность указывать фиксированную высоту поля данных в инструменте «Видеоверификация».	Видеоверификация
Изменения функционала		
	Оптимизирована работа с контроллерами при инициализации и загрузке большого количества пользователей.	HAL
	Добавлена обработка поля «Код подразделения» для системы распознавания документов Regula.	Распознавание документов
	Добавлен функционал блокировки пользователя в Active Directory по факту выхода субъекта за указанный периметр.	Синхронизация с AD

1.3 Требования к компьютеру

Общие требования

В качестве сервера и рабочих станций системы ParsecNET 3 могут использоваться практически все современные компьютеры, имеющие не менее 3 Гб оперативной памяти. Для сервера рекомендуется иметь не менее 4 Гб оперативной памяти. Требуемый объем жесткого диска определяется размерами[20] ваших баз данных и длительностью хранения транзакций системы. Если в систему будет интегрироваться какая-либо подсистема видеонаблюдения[515], то также необходимо учесть способ хранения и объем видеофайлов.



Если для простой системы на несколько дверей можно использовать практически любой ПК, то для серьезной распределенной системы в качестве сервера ParsecNET 3 следует выбирать компьютер, рассчитанный для работы в качестве сервера.

Версии операционных систем

Система ParsecNET 3 работает на современных версиях Windows:

- **Windows 7** (рекомендуется не ниже Professional, Service Pack 1);
- **Windows 8/8.1;**
- **Windows 10;**
- **Windows 11.**

Кроме того, поддерживаются следующие серверные платформы:

- **Windows 2008 Server, Windows 2008 Server R2;**
- **Windows 2012 Server, Windows 2012 Server R2;**
- **Windows 2016 Server,**
- **Windows 2019 Server,**
- **Windows 2022 Server.**

Система устанавливается как на 64, так и на 32 разрядные версии ОС. Для работы некоторых интеграций на 64 разрядных версиях ОС может потребоваться запуск конвертера "ParsecNET 3 - 32 bit converter.exe", который активирует работу приложения в режиме совместимости с 32 разрядной версией.

Все необходимые для работы ParsecNET 3 пакеты (.NET Framework, Visual C++ redistributable и т.п.) входят в состав установочного дистрибутива, кроме необходимого для работы интегрированных систем видеонаблюдения драйверов DirectX 8.0 или выше.



Не рекомендуется даже для рабочих станций (кроме WEB-рабочих станций) использовать "домашние" версии Windows (Home edition), поскольку они имеют ряд физических ограничений, и не обеспечивают гарантированного функционирования ParsecNET 3.

Минимальные аппаратные требования к конфигурациям ПК

Требования к серверу

	1	2	3	4	Комментарий
Количество контроллеров СКУД, обслуживаемых 1 сервером	до 100	до 100	от 100 до 500	от 500 до 1000	Количество контроллеров критично, прежде всего, к дисковой подсистеме. Наличие SSD-дисков серьезно увеличивает производительность. Настоятельно рекомендуется устанавливать SSD-диски на машины, обслуживающие 100 контроллеров и больше. Для конфигураций на 500-1000 контроллеров рекомендуется использовать диски NVME.

Количество субъектов в БД Персонала	до 50 000	до 100 000	до 250 000	до 500 000	При условии разумного распределения субъектов доступа по разным папкам в иерархии подразделений размер БД не оказывает значимого влияния на требования к оборудованию.
Количество отображаемых заявок в списках бюро пропусков	до 10 000	до 20 000	до 30 000	до 100 000	Количество отображаемых заявок в системе нагружает ОЗУ и CPU.
Количество одновременно запущенных рабочих мест (клиентов) Мониторинг/ Видеоверификация	до 2	до 5	до 10	до 30	1 подключенный клиент занимает от 100 до 500 МБ ОЗУ на сервере (в зависимости от того, какие инструменты открыты в нем и сколько в них отображается данных). Поэтому при большом количестве одновременно работающих с системой операторов (50 и выше) рекомендуется устанавливать не менее 32 ГБ ОЗУ на сервер.
Количество одновременно запущенных рабочих мест (клиентов) Персонал	до 2	до 5	до 5	до 20	
Количество одновременно запущенных рабочих мест (клиентов) Бюро пропусков	1	до 5	до 5	до 10	
Количество подключенных IP-камер	до 3	до 3	до 10	до 25	В случае использования функционала IP-камер Parsec (не касается интеграций с системами IP-видеонаблюдения) настоятельно рекомендуется использовать процессоры с поддержкой инструкций AVX, т.к. декодирование видеопотоков на CPU без AVX работает значительно медленнее. Указанные цифры не подразумевают наличия на сервере клиента с запущенным отображением всех камер, имеется в виду только то, что ParsecVideoHAL обслуживает указанное количество камер для реализации функционала сохранения кадров по событиям.
Количество событий, хранимых в БД	Зависит прежде всего от редакции СУБД SQL Server и желаемой глубины хранения архива событий. Значительно уменьшается при активации функционала сохранения в БД кадров с IP-камер и/или кадров событий распознавания автомобильных номеров.				

	Рекомендуемые параметры сервера			
Процессор	Intel Core i3		Intel Core i5	Intel Xeon E
ОЗУ	от 8 ГБ	от 16 ГБ		от 32 ГБ
Сетевая карта	1 Гбит/сек			
SSD для ОС, ParsecNET и SQL Server	от 256 Гб			

HDD для резервных копий и другого ПО	от 1 ТВ		от 2 ТВ	
Дополнительно				IPMI 2.0
	Общее оборудование			
Подключение монитора	разрешение 1280x1024, 16 млн. цветов (True Color)			
Подключение мыши	да			
Подключение клавиатуры	да			
Количество USB портов	от 4			

Требования к дополнительной рабочей станции

	1	2	3	4	Комментарий
Количество контроллеров СКУД, обслуживаемых 1 рабочей станцией	нет	до 100	от 100 до 500	от 500 до 1000	Количество контроллеров критично, прежде всего, к дисковой подсистеме. Наличие SSD-дисков серьезно увеличивает производительность. Настоятельно рекомендуется устанавливать SSD-диски на машины, обслуживающие 100 контроллеров и больше. Для конфигураций на 500-1000 контроллеров рекомендуется использовать диски NVME.
Количество подключенных IP-камер	нет	до 3	до 10	до 25	В случае использования функционала IP-камер Parsec (не касается интеграций с системами IP-видеонаблюдения) настоятельно рекомендуется использовать процессоры с поддержкой инструкций AVX, т.к. декодирование видеопотоков на CPU без AVX работает значительно медленнее. Указанные цифры не подразумевают наличия на сервере клиента с запущенным отображением всех камер, имеется в виду только то, что ParsecVideoHAL обслуживает указанное количество камер для реализации функционала сохранения кадров по событиям.
	Рекомендуемые параметры Рабочей станции				
Процессор	Intel Core i3		Intel Core i5		
ОЗУ	от 4 ГБ	от 8 ГБ		от 16 ГБ	
Сетевая карта	1 Гбит/сек				
Жесткий диск для ОС и ParsecNET	HDD от	SSD от 128 Гб			

	128 Гб	
	Общее оборудование	
Подключение монитора	разрешение 1280x1024, 16 млн. цветов (True Color)	
Подключение мыши	да	
Подключение клавиатуры	да	
Количество USB портов	от 4	

Если планируется использование функционала IP-камер, особенно с включенными функциями распознавания номеров, настоятельно рекомендуется использовать на сервере и рабочих станциях Системы процессоры с поддержкой инструкций AVX.

Требования к сети

Системному администратору необходимо обеспечить следующие условия для работы системы:

- для работы быстрого транспорта на всех машинах должно быть обеспечено прохождение пакетов между любыми компьютерами в системе по порту 10000 UDP;
- для работы ПО на сервере и всех рабочих станциях системы должно быть обеспечено прохождение пакетов между сервером и рабочей станцией по портам с 10000 по 10107 TCP;
- для работы с сетевым оборудованием используются UDP порты 1124, 1125, 6124, 6125;
- экземпляр SQL Server должен быть доступен с сервера системы. Настройка межсетевого экрана для доступа к SQL-серверу описана в статье на сайте Microsoft;
- межсетевой экран (антивирусная программа) должен разрешать работу службам и клиентским приложениям ParsecNET 3;
- интеграционный сервис конфигурируется на порту 10101 http.

1.4 Требования к SQL Server

Поставляемая с системой бесплатная версия Microsoft SQL Server 2017 Express Edition имеет ограничение на размер одной базы данных в 10 Гб. Если вы не укладываетесь в указанный размер, то следует приобрести платную версию, не имеющую таких ограничений.

Обратите внимание, что SQL Server 2017 Express Edition устанавливается только на 64-разрядные операционные системы не ниже Windows 8 или Windows Server 2012.

Минимально поддерживаемая версия СУБД - Microsoft SQL Server 2008 R2.

Для оценки объема БД необходимо учитывать следующие факты:

- Транзакции (сообщения о событиях) системы хранятся в отдельной базе данных (БД). В другой БД хранятся все остальные данные системы (конфигурация, пользователи, настройки, шаблоны и так далее). Поэтому расчеты следует вести отдельно для каждой из баз данных.

- Одна транзакция занимает в БД примерно 0,5 килобайта, при ограничении в 10 Гбайт можно хранить до 20 миллионов событий.
- Размер одной записи в БД персонала зависит от ее состава. При 5-10 дополнительных полях с фотографией одна запись занимает от 50 до 100 килобайт, что на бесплатной версии MS SQL позволяет иметь в БД от 100 до 200 тысяч человек. Если фотографии не используются, то это значение возрастает в десятки раз.

Количество транзакций, генерируемых системой зависит от количества точек прохода, интенсивности движения субъектов доступа через них, транзакций от интегрированной системы видеонаблюдения, охранной системы и ОПС. Также необходимо учесть объем фотографий, если система видеонаблюдения позволяет их делать.

Например, системой пользуется 15000 человек. Видеонаблюдение отсутствует.

Записи субъектов доступа с фотографиями занимают примерно 1 ГБ.

Каждый из них порождает (в идеальном варианте) только два события в течение рабочего дня: вход и выход. Следовательно, создаваемый системой за день объем равен примерно 15 МБ.

Посетителей за день - 100 человек, что дает (запись + события прохода) примерно 100 КБ.

Итого получается, что в день система порождает немногим больше 15 МБ.

Это означает, что бесплатная версия SQL Server 2017 Express Edition сможет обеспечить работоспособность (в идеальном случае) в течение примерно 2 лет.

Система отслеживает оставшийся свободный объем БД. Когда свободного места в БД становится меньше 10%, формируется тревожное аудитное событие "В БД заканчивается свободное место".



Рекомендуется создавать архивные копии БД раз в сутки.

Не реже одного раза в 6 месяцев рекомендуется архивировать БД, установив флажок "Обрезать лог транзакций после создания резервной копии". Это позволит значительно уменьшить размер БД системы (см. раздел справки Резервное копирование[346]).

1.5 Количественные ограничения системы

Система ParsecNET 3 имеет следующие количественные ограничения:

Параметр	Количество
Максимальное количество рабочих станций в системе ParsecNET 3	100
Максимальное количество контроллеров в системе ParsecNET 3 (совокупно, на всех станциях) при использовании версий PNSoft-MAX, PNSoft-Professional	2000
Максимальное количество контроллеров на один управляющий ПК (хост) *Примечание: контроллеры могут быть подключены к ПК через любой из доступных интерфейсных модулей либо через Ethernet*	1000
Максимальное количество контроллеров доступа (серии NC) на одну линию IP-шлюза CNC-12/14-IP	24

Максимальный поток событий от IP-контроллеров на 1 хост для их обработки без задержек	30 событий в секунду
Максимальное количество нагруженных IP-контроллеров (точек прохода с плотностью проходов 30 проходов в минуту) на 1 хост, без задержек в обработке событий на хосте. 1 нагруженный контроллер примерно соответствует 30 слабо нагруженным контроллерам (с плотностью проходов в среднем 1 проход в минуту).	60
Максимальное количество охранных контроллеров (серии AC) на одну линию шлюза CNC-12/14-IP	8
Максимальное количество одновременно подключенных на одну линию IP-шлюза доступных и охранных контроллеров (NC/AC)	18 / 6
Максимальное количество IP-камер, обслуживаемых станцией/сервером системы ParsecNET 3	1 камера на 1 физическое ядро процессора
Максимальное количество биометрических терминалов ZKTeco/ЛКД в системе	50
Максимальное количество ключниц Keyguard, подключенных к одной станции/серверу системы ParsecNET 3	20
Мобильные терминалы Parsec Access Terminal, рекомендуемое количество в системе (на сервер)	10
Болид, С2000-ПП	1 устройство на 1 COM-порт
Стрелец v7.5, РРОП	
Umirs (Мурена)	
Максимальное количество заявок бюро пропусков на одно подразделение	10000 (из них 1000 активных)
Максимальное количество субъектов доступа в одном подразделении	10000
Максимальное количество подразделений в системе	10000
Максимальное количество узлов в кластере при использовании многосерверной топологии	В зависимости от конфигурации

1.6 Ограничения версий

Ниже перечислены элементы, интегрированные с ParsecNET 3, и версии их ПО, на которых интеграция была протестирована и показала успешную работоспособность.

Наименование	Версия ПО, на которой тестировалась интеграция
Видеонаблюдение	**Версия ПО**

Интеллект (ITV)	Интеллект v. 4.10.4.3276, v. 4.11.3.3601
Спецлаб	GOALcity Cassandra v. 4
Macroscop	Macroscop v. 3.1.28, 3.2.66, 3.2.70, 3.3.64
LTV Gorizont	1.12.160 (2015 год)
Trassir (DSSL)	Trassir v. 4.1
Milestone	Xpotect Professional +2019 R3 (13.2a), +2020 R3
Milestone Access Control	Xpotect Professional +2020, +2020 R3
Panasonic	7.3.0.127
ONVIF Device Manager	2.2.250
ISS SecurOS	10.5, 10.6, 11.2, 11.5_R1, 11.6
Видеокамеры Hikvision серии SmartIP	Модель камер: DS-2CD4A26FWD-IZHS/P версия ПО 5.4.5 и iDS-TCM203-A/R/0832 (850 нм) (B). Поддерживаются камеры серии DS-2CD4xxx (Smart IP): https://hikvision.ru/products/project/ipcam-ds2cd4xxx-auto[22]
Распознавание документов	**Версия SDK**
ABBYY PassportReader SDK	1.5R2GM
Scanify Cognitive Passport API	3.0 (Продажа модулей прекращена с декабря 2019 года. Проданные ранее модули поддерживаются.)
Regula	4.10.2
Системы ОПС	
Болид (Орион)	UPROG версия утилиты 4.1.4 PPROG версия утилиты 3.13
Аргус	Стрелец v. 7.5, 9.3 Стрелец-Интеграл v. 7.5, 9.3
FireSec	3.1.2
Динго	**Версия прошивки**
Алкотестер "Динго-B02"	Прошивка ОСТ
ZKTeco	**Версия прошивки/SDK**
TF1700	PullSDK v. 6.64.0012
TF1600	PullSDK v. 6.64.0012
ZK7500	ZKFinger SDK 3.0.1
ZK4500	ZKFinger SDK 3.0.1
ЛКД	**Версия прошивки**
ЛКД СО-04 00	ZKFinger SDK 3.0.1
ЛКД СО-04 01	ZKFinger SDK 3.0.1

ЛКД КО-15 00	PullSDK v. 6.64.0012
SmarTec	**Версия SDK**
ST-FR032EK	PullSDK v. 6.64.0012
BAS-IP	
Список моделей в разделе[685]	API v. 2.3.0, 2.5.0

2. Быстрый старт

Данный раздел содержит описание шагов настройки и запуска небольшой системы **ParsecNET 3**, включая подключение и конфигурирование оборудования.

После выполнения всех описанных ниже шагов можно получить работающую систему ParsecNET 3 в одномашинной конфигурации (то есть, когда функции сервера системы, рабочей станции и сервера баз данных выполняет один компьютер).

Этот раздел не является заменой полному руководству пользователя СКУД ParsecNET 3.

Итак, для создания СКУД ParsecNET 3 выполните следующие действия:

1. Монтаж оборудования

Смонтируйте оборудование в соответствии с указаниями, изложенными в паспортах и руководствах пользователей на это оборудование.

- Смонтируйте и подключите наружный считыватель к контроллеру;
- Смонтируйте и подключите контроллер к сетевой карте компьютера (в случае IP-контроллера, например, NC-8000-IP). Если у Вас контроллер с интерфейсом RS-485, то подключите его к USB-интерфейсу (например, NI-A01), а интерфейс затем к компьютеру;
- Подайте питание на контроллер.

Будем считать, что оборудование подключено, питание на него подано, и все готово к дальнейшей работе.

Далее рассматривается работа с ПО ParsecNET.

2. Установка MS SQL Server

Перед установкой ПО ParsecNET 3 установите экземпляр SQL Server. Сделать это можно либо вручную, задав режим смешанной авторизации (mixed mode, проверка подлинности SQL Server и Windows), либо при помощи скрипта SetupSqlServer.vbs, который находится в папке SERVER на дистрибутивном носителе.

3. Установка программного обеспечения ParsecNET 3

Для установки ПО запустите из дистрибутива файл setup.exe. В окне выбора типа установки и директории для установки выберите установку нового сервера. Во всех остальных окнах мастера установки оставьте значения по-умолчанию, если экземпляр SQL Server установлен с помощью скрипта (Шаг 2), если вручную - необходимо указать имя экземпляра SQL Server.

После завершения установки программы в списке программ появится папка с ярлыками приложений системы **ParsecNET**.



Не забудьте подключить аппаратный ключ защиты ДО запуска программы!

4. Консоль администрирования

Вся настройка оборудования производится в консоли администрирования. Чтобы запустить ее, дважды щелкните по строке приложения "Пуск → Все программы → Parsec 3 → Администрирование" и в окне верификации введите логин и пароль: parsec/parsec. Позднее логин и/или пароль можно изменить (см. раздел справки Редактор операторов).

5. Резервное копирование

Резервное копирование позволит восстановить систему в случае отказа оборудования (например, при отказе ПК, на котором хранились ваши данные), поэтому настоятельно рекомендуется создать правило для периодического резервного копирования. Для этого зайдите в редактор системных настроек и выберите на левой панели раздел "Резервное копирование". На правой панели появятся настройки, которые Вы можете настроить в соответствии со своими предпочтениями.

Теперь можно спокойно приступать к настройке системы.

6. Оборудование

Для настройки оборудования необходимо, чтобы программа обнаружила все подключенные к компьютеру устройства. Для выполнения этой задачи перейдите в редактор оборудования. В левой панели редактора отображаются корневая организация и ваша рабочая станция.

- *Найдите оборудование*

  Выберите в контекстном меню рабочей станции пункт "Поиск оборудования". Программа произведет поиск каналов. После обнаружения каналов, запустите на каждом из них поиск оборудования.

- *Настройте контроллеры*

  Выберите контроллер. В карточке контроллера перейдите на вкладку "Компоненты". Выбирая компоненты, Вы можете задать значения их параметров (в режиме редактирования).

7. Расписания

Чтобы контроллеры предоставляли пользователям доступ на территорию в надлежащее время, нужно создать расписания доступа. В редакторе расписаний по-умолчанию представлено круглосуточное расписание, можно воспользоваться им.

Также можно создать свои расписания доступа (как недельные, так и сменные). Кроме того, для учета рабочего времени персонала можно создать расписания рабочего времени (доступно при наличии лицензии УРВ) (см. раздел справки Редактор расписаний).

8. Группы доступа

Предоставить пользователю право доступа на территорию можно только посредством назначения ему определенной группы доступа, созданной заранее.

В редакторе групп доступа создайте группы, указав для каждой нужную совокупность точек прохода. Сотрудник, которому назначается какая-либо группа, будет иметь право прохода через точки прохода, образующие эту группу.

9. Персонал

Теперь можно приступать к занесению сотрудников в БД. В редакторе персонала создайте подразделения (при наличии лицензии УРВ, назначьте им расписания рабочего времени). Внесите данные сотрудников, включая их в группы доступа и присваивая им идентификаторы (карты).

Для внесения кодов карт в БД удобно использовать настольный считыватель. Но можно вносить код каждой карты вручную.

Для внесения кодов карт также можно настроить считыватель какой-либо двери (см. параграф справки Работа без настольного считывателя).

10. ЖЕЛАТЕЛЬНО

Запишите, если изменяли, новый логин/пароль оператора (подробнее об изменении см. раздел справки Редактор операторов).

Настройка системы завершена, теперь нужно проверить ее работоспособность. Для слежения за событиями в системе предназначен Монитор событий. Запустите его, щелкнув дважды по строке приложения "Пуск → Все программы → ParsecNET 3 → Монитор событий".

11. Проверка работоспособности

- Поднесите карту к считывателю точки прохода;
- Проверьте, что программа сгенерировала сообщение о событии;
- Проверьте, что отобразился корректный субъект доступа;
- Проверьте статус двери, она должна открываться на время, настроенное в карточке контроллера в редакторе оборудования, если этому субъекту доступа разрешен проход через нее;
- Проверьте, что дверь не открывается по карте, у которой нет доступа на данную территорию.

Если появляются какие-то ошибки, проверьте правильность выполнения изложенных выше пунктов. При необходимости обращайтесь к полному руководству пользователя.

Если ошибок нет - система готова к работе.

3. Типовые роли

В данном разделе представлены категории, на которые можно разделить всех сотрудников, использующих ПО ParsecNET 3. Для каждой категории приведены ссылки на разделы справки, в которых описываются функции системы, помогающие сотрудникам исполнять их обязанности.

Конечно, такое разделение весьма условно и в каждой конкретной организации распределение ролей и обязанностей может быть своим.

Менеджер

Менеджер - это должность, обязанностью которого мы видим контроль:

- за работой других сотрудников с системой;

- правильности настроек и заданных параметров.

Следующие разделы будут полезны для выполнения перечисленных выше функций:

Введение 11
Быстрый старт 24
Вход в систему 38
Пользовательский интерфейс 39
Обзор системы 57
Многосерверность 164
Редактор топологии 203
Безопасность 193
Редактор расписаний 213
Редактор групп доступа 245
Редактор персонала 255
Монитор событий 287
Отчеты по составу 313
Отчеты по событиям 302
Редактор системных настроек 341
Текстовые сообщения 394
Использование IP-камеры 414
Дополнительные модули 417
Работа с шаблонами в отчетах 314

Программный контроллер 187

Установщик и настройщик системы

Основные функции установщика-настройщика системы:

- Планирование системы контроля и управления доступом:
  - выбор физической топологии и оборудования;
  - выбор варианта лицензирования ПО.
- Внедрение системы:
  - монтаж;
  - конфигурирование физической топологии;
  - интеграция с системами видеонаблюдения;
  - интеграция с системами ОПС;
  - интеграция с биометрическими и другими системами.
- Начальная настройка и сдача системы в эксплуатацию.

Рекомендованы к обязательному изучению разделы:

Введение 11
Быстрый старт 24
Установка системы 29
Вход в систему 38
Пользовательский интерфейс 39
Обзор системы 57
Редактор оборудования 62
Многосерверность 164
Монитор событий 287
Отчеты по составу 313
Отчеты по событиям 302
Специальные средства 317
Программный контроллер 187
Текстовые сообщения 394
Настройка IP-камеры 411
Дополнительные модули 417

Администратор

Функции администратора:

- Резервное копирование и восстановление;
- Установка/удаление дополнительных рабочих станций;
- Обновление сервера и станций;
- Работа с ключом защиты (обновление);
- Настройка топологии;
- Настройка расписаний доступа;
- Настройка групп доступа;
- Настройка уровней доступа в систему (операторы);

- Настройка рабочих мест оператора системы (настройка профиля оператора – монитор, видеоверификация, видеонаблюдение и т.п.);
- Персонал:
  - Дополнительные поля;
  - Настройка модуля сканирования документов.
- Настройка шаблонов печати пропусков;
- Настройка и формирование отчетов по событиям;
- Настройка автоматизированных заданий.

Поскольку администратор должен быть наиболее подготовленным в работе с системой пользователем, он должен изучить все разделы справки. Поэтому ссылок на какие-то отдельные разделы не приводится.

Сотрудник отдела кадров

Функции сотрудника отдела кадров:

- Ведение базы персонала:
  - Использование модуля сканирования документов (при его наличии).
- Выдача идентификаторов с уровнями доступа;
- Работа с редактором шаблонов печати пропусков;
- Печать пропусков;
- Настройка и формирование отчетов по событиям;
- Настройка и формирование бизнес-отчетов (УРВ):
  - Настройка расписаний РВ;
  - Назначение расписаний сотрудникам;
  - Поправки рабочего времени;
  - Создание шаблонов отчетов (для повторного использования);
  - Построение отчетов.
- Настройка текстовых уведомлений.

Разделы для изучения:

Введение 11
Вход в систему 38
Пользовательский интерфейс 39
Обзор системы 57
Редактор расписаний 213
Редактор групп доступа 245
Редактор персонала 255
Монитор событий 287
Отчеты по событиям 302
Редактор организаций 317
Редактор заданий 321
Отчеты по составу 313
Текстовые сообщения 394
Редактор шаблонов печати 417
Модуль бюро пропусков 432

Модуль учета рабочего времени[456]
Распознавание документов[671]
Работа с шаблонами в отчетах[314]

Сотрудник охраны

Категория подразделяется на две подкатегории:

Сотрудник охраны точки прохода - одна дверь, контроль прохода и т.п.

Функции сотрудника охраны на точке прохода:

- видеоверификация (проверка соответствия проходящего лица и его фотографии в карточке сотрудника);
- видеонаблюдение;
- формирование отчетов по событиям;
- прямое управление точкой прохода;
- постановка на охрану и снятие с охраны помещений и территорий.

Разделы, которые необходимо изучить:
Вход в систему[38]
Монитор событий[287]
Отчеты по событиям[302]
Модуль видеоверификации[506]
Интеграция с системами видеонаблюдения[515]

Сотрудник по контролю тревожных ситуаций в целом по системе

Такой сотрудник отслеживает тревожные события в системе при помощи графплана и имеет следующие обязанности:

- мониторинг состояния элементов системы, территорий и точек прохода;
- прием тревог и организация необходимых действий;
- снятие тревожных состояний элементов системы;
- формирование отчетов по событиям.

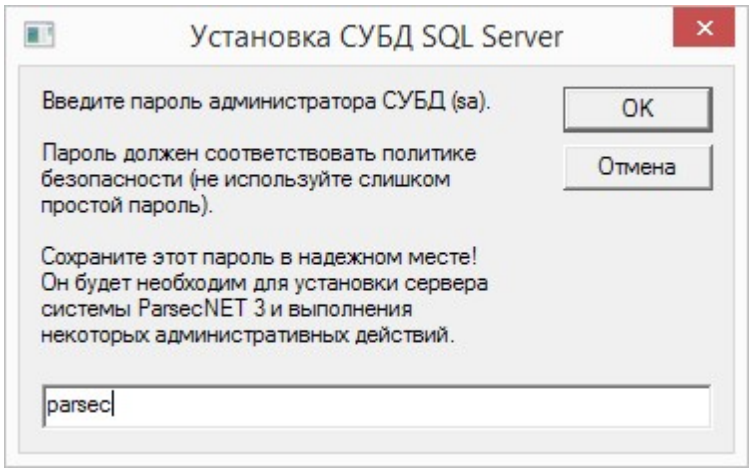
Разделы справки для изучения:
Вход в систему[38]
Монитор событий[287]
Отчеты по событиям[302]
Модуль видеоверификации[506]
Интеграция с системами видеонаблюдения[515]
Интеграция с системами ОПС[603]

4. Установка системы

Для первичной установки сервера системы ParsecNET необходимо иметь установленный и настроенный экземпляр SQL Server. Его можно установить либо самостоятельно, либо при помощи скрипта "SetupSqlServer.vbs", который находится в папке SERVER на дистрибутивном носителе.

При самостоятельной установке необходимо выбрать режим смешанной авторизации (mixed mode, проверка подлинности SQL Server и Windows).

Если при запуске скрипта "SetupSqlServer.vbs" появится предупреждение системы безопасности Windows, подтвердите желание производить установку, нажав на кнопку *Выполнить*. После запуска скрипта откроется окно создания пароля доступа к серверу SQL:



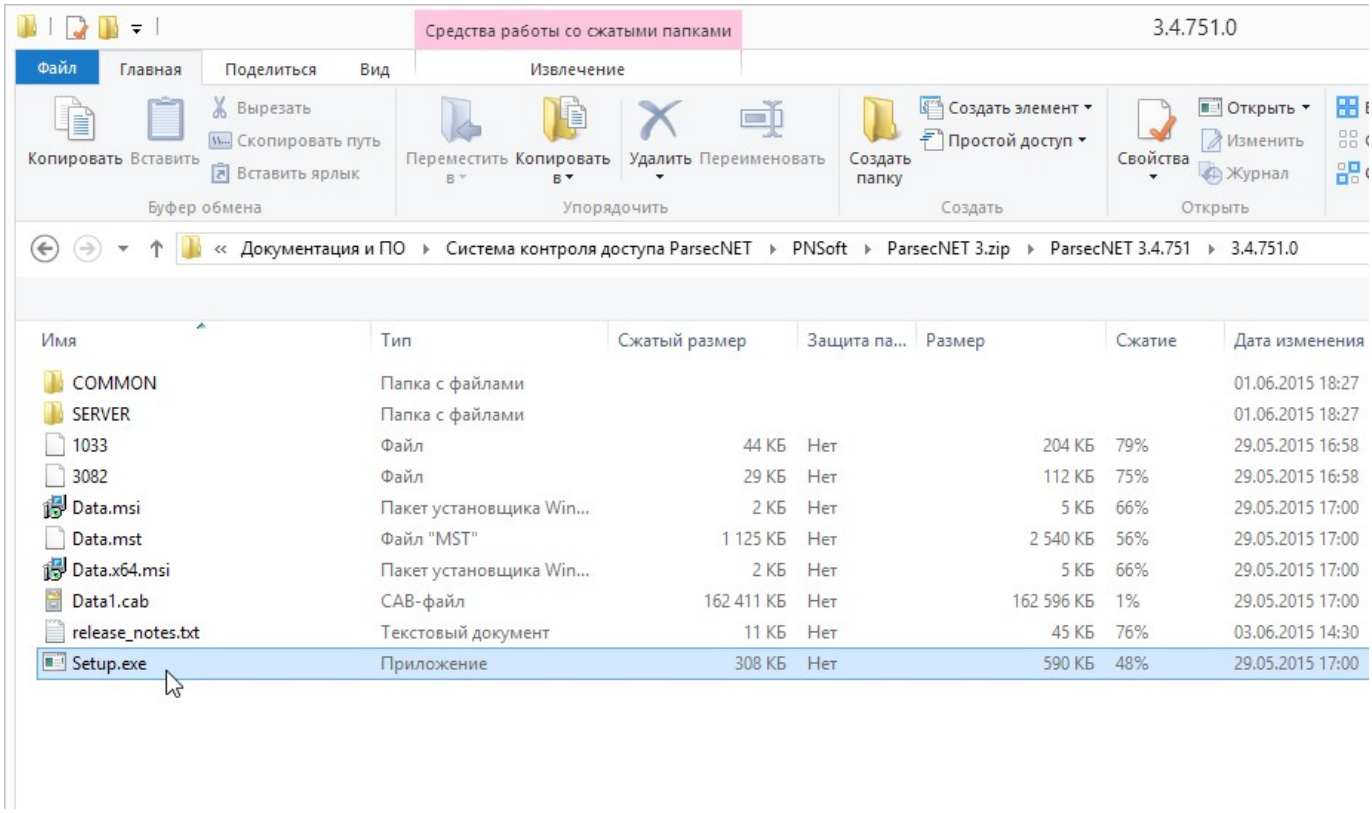
Придумайте и введите пароль для авторизации на SQL-сервере, после чего нажмите на кнопку *OK*.

Обязательно запомните или запишите введенный пароль, он потребуется в дальнейшем для администрирования вашего SQL-сервера.

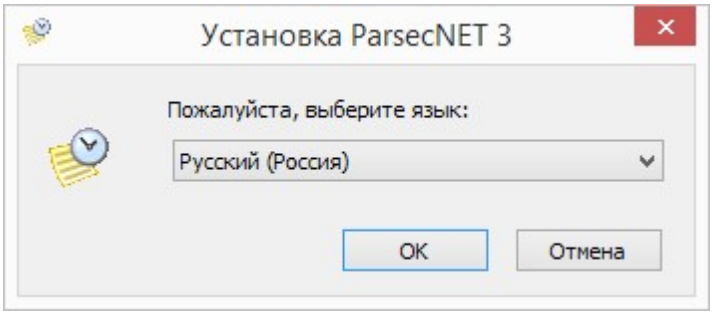
Следуя указаниям мастера, установите экземпляр SQL Server. Скрипт устанавливает экземпляр SQL Server 2012 Express Edition с именем PARSEC3.

Теперь можно приступать к установке СКУД ParsecNET 3:

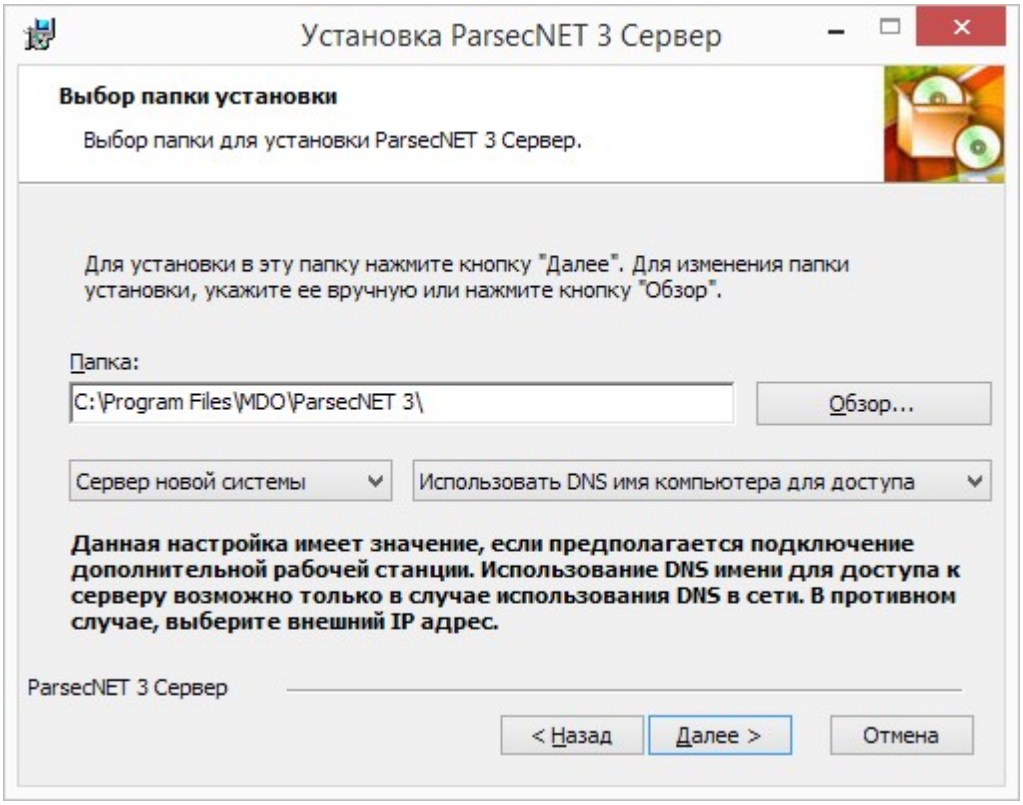
1. Перейдите в место расположения дистрибутива ParsecNET 3 и запустите файл установки "setup.exe":



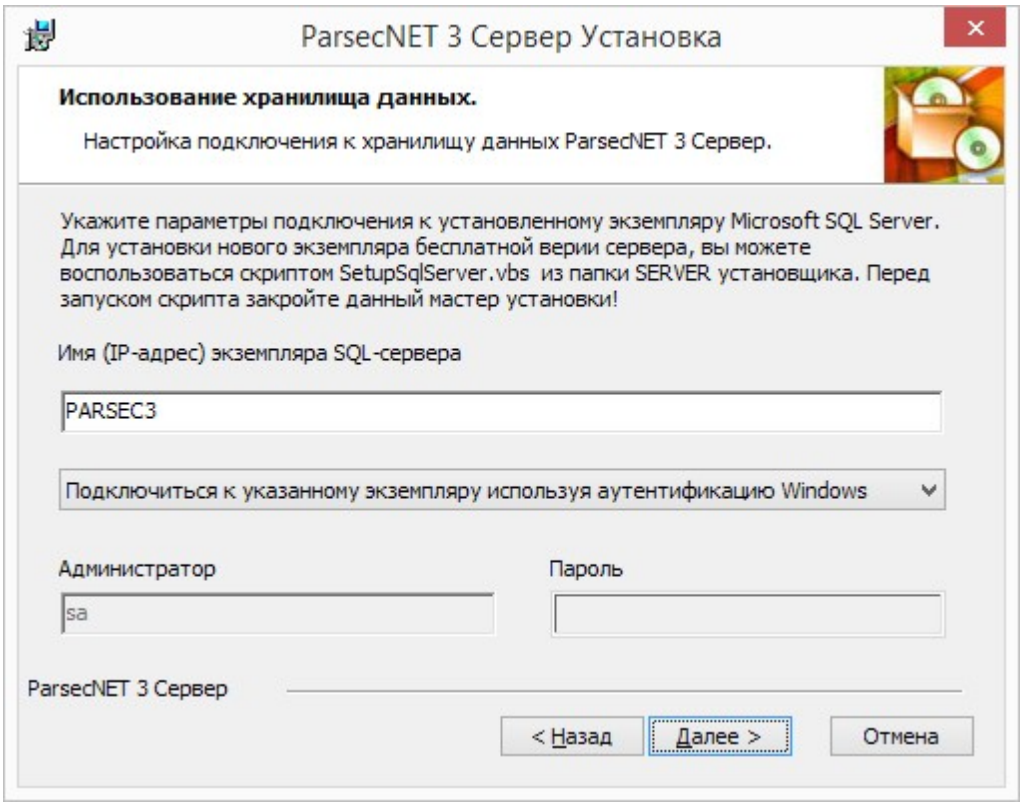
2. После запуска установки будет выведено меню выбора языка. В зависимости от языка операционной системы, языком по-умолчанию может быть английский или русский. Выберите язык, который требуется и нажмите на кнопку *ОК*:



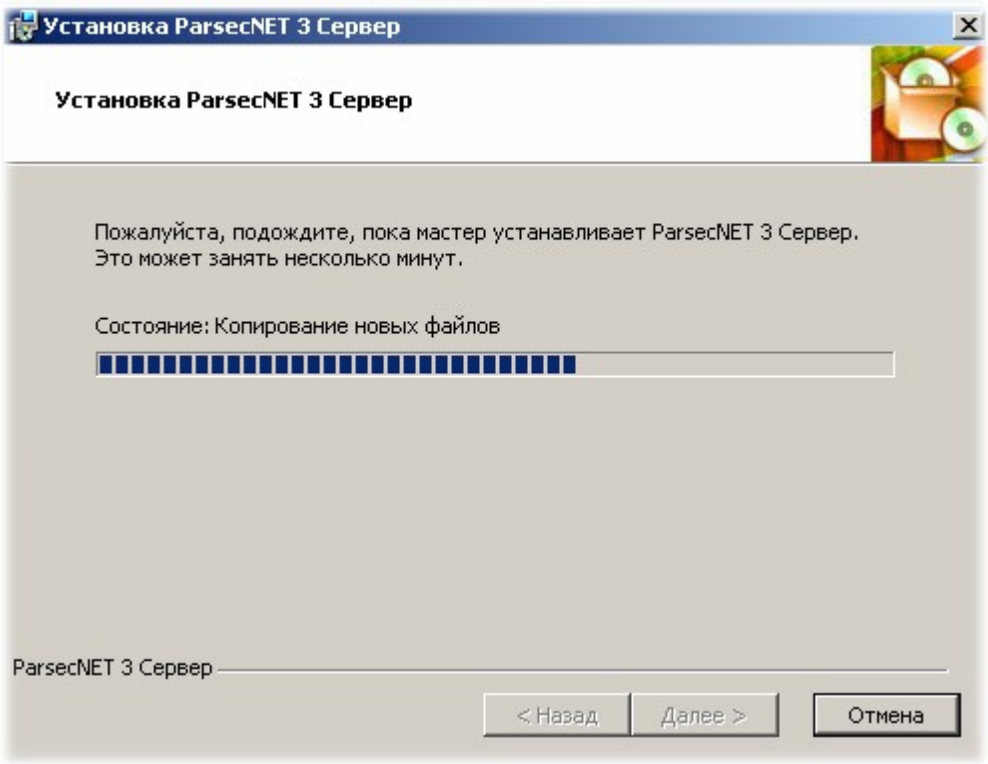
3. После выбора и подтверждения языка установки будет выведен приветственный диалог. Для начала установки нажмите на кнопку *Далее*. Откроется окно лицензионного соглашения;
4. Прочитайте и подтвердите согласие с условиями лицензионного соглашения, после чего нажмите ставшую доступной кнопку *Далее* (кнопка станет активной только после выбора согласия с условиями лицензионного соглашения). Будет выведен диалог с выбором типа установки и пути (директории), в которую будет устанавливаться система;
5. Выберите тип установки *Сервер новой системы*. Без острой необходимости не меняйте предлагаемую по-умолчанию директорию установки:



6. Выберите, как рабочие станции будут подключаться к устанавливаемому серверу: по IP-адресу или по имени компьютера;
7. Нажмите на кнопку *Далее*;
8. Если программа установки автоматически определяет наличие экземпляра PARSEC3 Microsoft SQL Server на ПК, где устанавливается продукт, то следующий диалог предложит подключиться к обнаруженному серверу с автоматически выбранными установками:

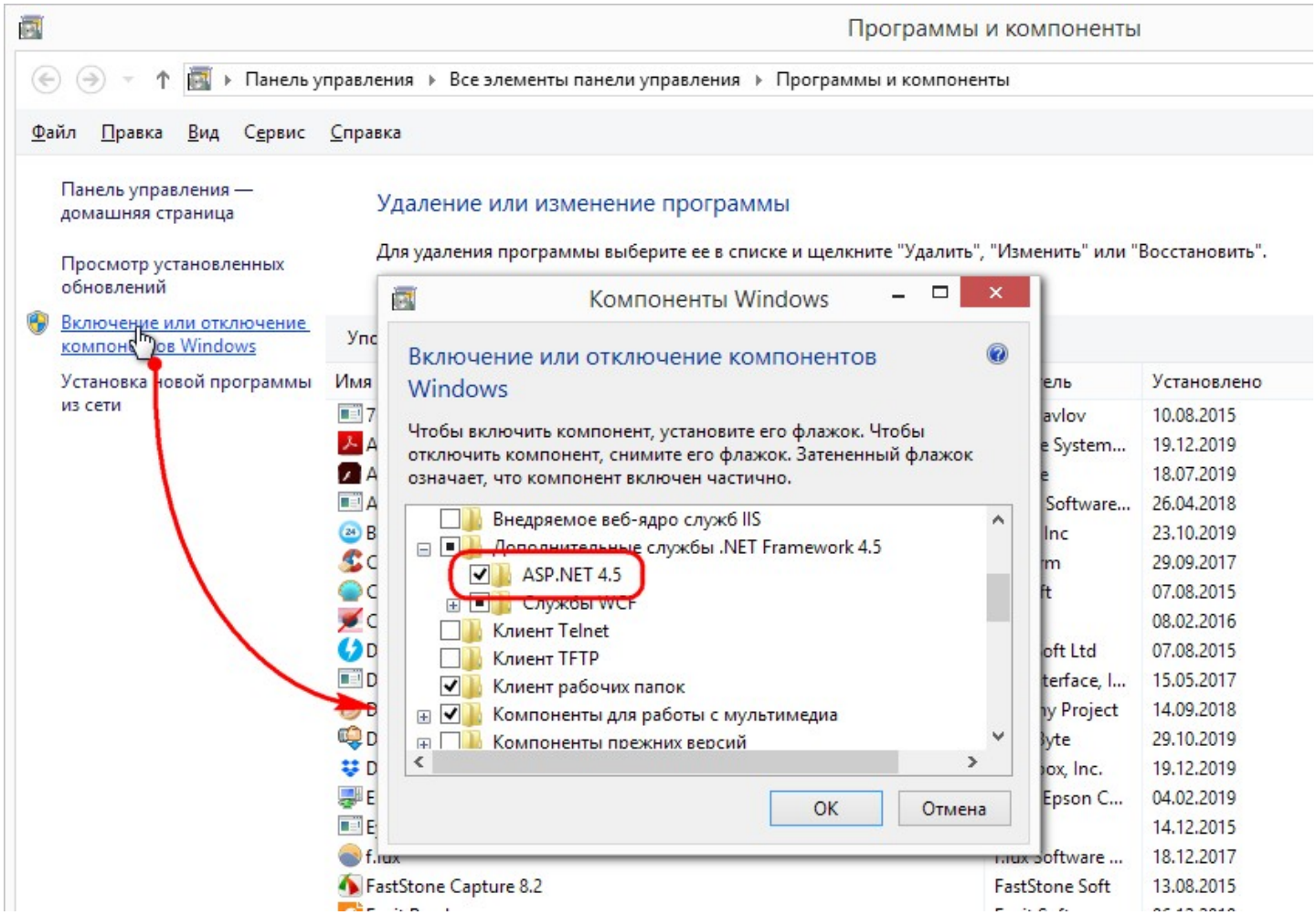


9. При использовании удаленного экземпляра Microsoft SQL Server вручную введите полный адрес вашего экземпляра SQL Server в поле *Имя (IP-адрес) экземпляра SQL-сервера*. Полным адресом экземпляра является строка вида
ИМЯ или *IP сервера\ИМЯ ЭКЗЕМПЛЯРА*
Если экземпляр расположен на локальном компьютере, то в адресе 1-ю часть можно опустить и написать в поле адреса просто <ИМЯ ЭКЗЕМПЛЯРА>, как показано на рисунке выше. Кроме того, в данном диалоге требуется настроить способ аутентификации при обращении к хранилищу данных. Можно использовать аутентификацию средствами ОС или же использовать аутентификацию SQL-сервера. При использовании аутентификации Windows, соединение с сервером БД будет производиться от имени того пользователя Windows, который запустил установку. Во втором случае необходимо ввести имя и пароль SQL-пользователя, от имени которого будет производиться соединение с экземпляром Microsoft SQL Server;
10. После ввода имени используемого экземпляра Microsoft SQL Server, настройки способа аутентификации и подтверждения введенных данных нажатием на кнопку *Далее* будет проверено соединения с сервером, и при его наличии выведен диалог подтверждения начала установки.
При невозможности соединения с сервером БД будет выведен соответствующий диалог. При неправильном вводе логина и/или пароля SQL-сервера пользователю предоставляется возможность ввести данные заново;
11. Нажмите на кнопку *Установить*. Запустится процесс установки ParsecNET 3. Начинается он с установки драйверов ключа защиты Guardant. Если перед установкой система безопасности Windows выдаст предупреждение, то подтвердите желание продолжать установку. Аналогичным образом пройдет установка драйверов FTDI (драйвера USB-устройств). Следом за драйверами начнется непосредственно установка сервера ParsecNET 3. Вид экрана во время установки будет примерно таким:



12. После установки появится диалоговое окно, информирующее о завершении процесса. После нажатия на кнопку *Готово* установка завершится и запустится консоль администратора, можно переходить к работе с системой. Если вам не терпится быстрее настроить систему, то прочитайте раздел "Быстрый старт" - он поможет Вам сделать это за считанные минуты.

После установки системы настойчиво рекомендуется убедиться, что в ОС Windows включен компонент ASP.NET (Панель управления\Все элементы панели управления\Программы и компоненты\Включение и отключение компонентов Windos). Особенно актуально это для ОС Windows 10 и выше.



См. также:

Установка дополнительной рабочей станции 34

Удаление системы 36

4.1 Установка дополнительной рабочей станции

Установка дополнительной рабочей станции системы ParsecNET 3 максимально автоматизирована и требует минимального набора действий, поскольку при установке сервера системы создается специальный пакет данных, содержащий всю необходимую информацию о сервере системы.

Если сервер системы устанавливался в директорию по-умолчанию, установочный пакет дополнительной рабочей станции располагается по следующему пути:

C:\Program Files\MDO\ParsecNET 3\WorkstationSetup\Setup.exe

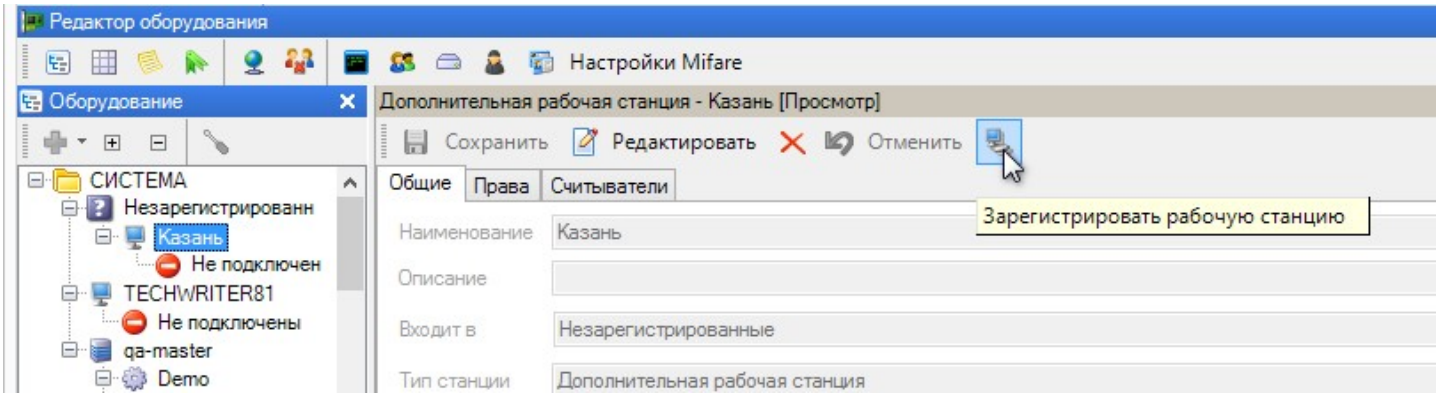
Во время установки сервера системы ParsecNET 3 этот путь автоматически открывается для чтения по сети для всех пользователей (Everyone - Read Only). Имя ресурса общего доступа - ParsecWorkstationSetup.

Установка дополнительной рабочей станции возможна как по сети из указанной выше директории, так и локально. В этом случае пользователь может скопировать установочный пакет на любой сменный носитель и проводить установку с локального компьютера (с жесткого диска, флеш-карты или любого другого доступного носителя).

Если установившее дополнительную рабочую станцию лицо не имеет прав на ее регистрацию в системе, то оно не сможет запустить ПО ParsecNET 3. Для регистрации рабочей станции в системе, первый вход должен осуществить имеющий такое право сотрудник, либо станция должна

быть зарегистрирована на сервере. Для этого на сервере СКУД в ПО ParsecNET 3 проделайте следующее:

- Откройте Редактор оборудования;
- Выберите в дереве раздел *Незарегистрированные*;
- Выберите рабочую станцию;
- В карточке оборудования нажмите на кнопку *Зарегистрировать рабочую станцию*.



В результате в дереве компьютеров данная рабочая станция отобразится в общем списке.

Рабочие станции, как и другие компоненты системы, можно удалять.

При удалении рабочей станции из дерева оборудования удаляются и все ее каналы вместе с подключенным оборудованием, которые в случае повторной установки рабочей станции придется инициировать заново.

Кроме того, как и другое оборудование, рабочие станции можно распределять по организациям, а в организации затем распределять по ее топологии.

Надо иметь в виду, что одновременно в системе могут работать столько рабочих станций, сколько разрешено лицензией, определяемой ключом защиты на сервере. Это правило распространяется на запуск пользовательского интерфейса. Без пользовательского интерфейса в системе для поддержки подключенного к компьютеру оборудования может работать любое число рабочих станций, независимо от лицензии.

4.2 Обновление системы

В этом разделе описан процесс обновления ПО ParsecNET до актуальной версии.

Перед обновлением программы настоятельно рекомендуем создать резервную копию[346] всех данных:

1. Запустите консоль "Администрирование";
2. Выберите пункт главного меню *Инструменты*, далее "Системные настройки";
3. В дереве "Настройки" выберите пункт "Резервное копирование";
4. Нажмите на кнопку *Создать резервную копию.*

По-умолчанию путь сохранения резервной копии: C:\Program Files\MDO\ParsecNET 3\Backup.

После создания резервной копии, появится файл вида "Parsec3_bak_20140916-135142.P3BAK".

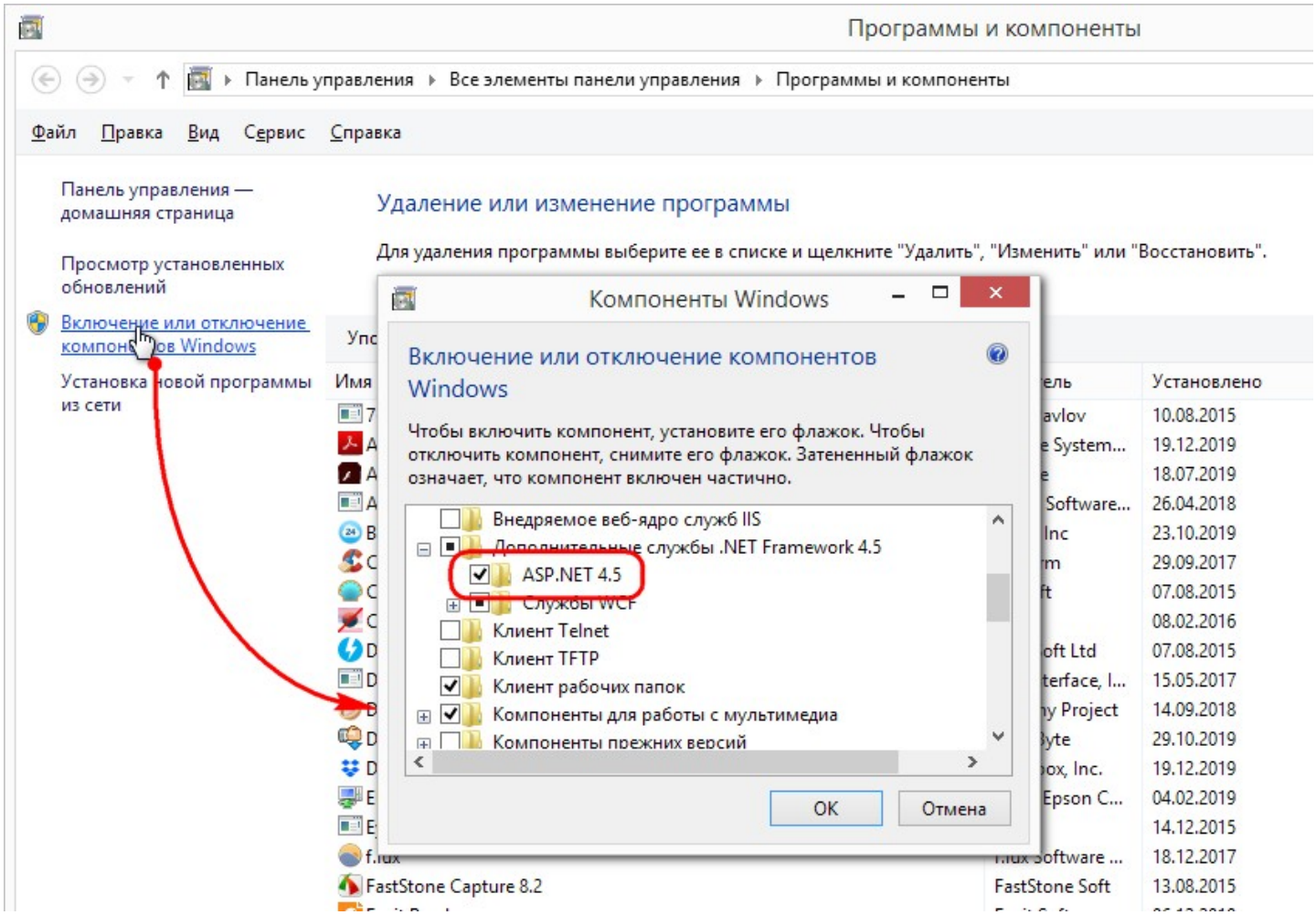
После резервирования информации можно приступать к обновлению. Сначала необходимо обновить сервер системы ParsecNET 3.

Процедура обновления ПО **сервера системы** ParsecNET 3:

1. Перед началом обновления, обязательно закройте все консоли ParsecNET на той машине, где производится обновление;
2. Загрузите с сайта программное обеспечение: https://www.parsec.ru/download/doc_soft/ParsecNET3_update.zip;
3. Разархивируйте файлы для обновления;
4. Запустите setup.exe;
5. Установите новую версию ПО, следуя инструкциям мастера установки программы;
6. Обновление сервера выполнено.

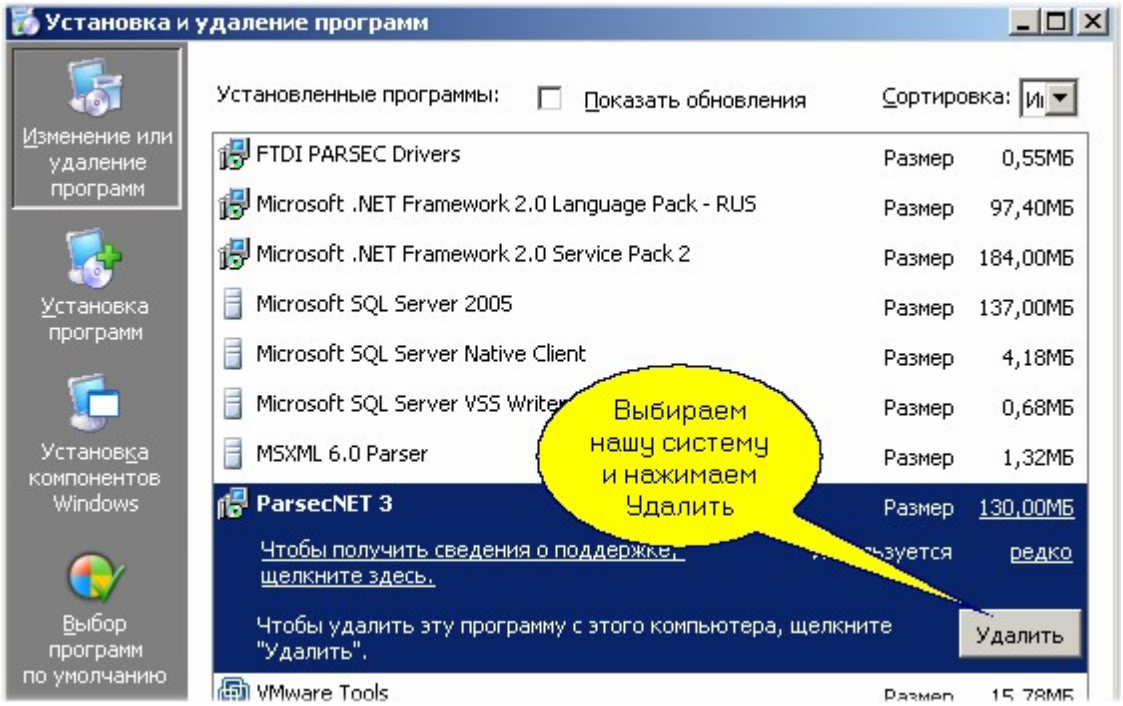
После обновления сервера программы, следует обновить все рабочие станции. Для обновления **рабочих станций** необходимо выполнить их повторную установку[34], используя актуальное ПО из папки \\<ip_сервера>\ParsecWorkstationSetup.

После обновления системы настойчиво рекомендуется убедиться, что в ОС Windows включен компонент ASP.NET (Панель управления\Все элементы панели управления\Программы и компоненты\Включение и отключение компонентов Windos). Особенно актуально это для ОС Windows 10 и выше.

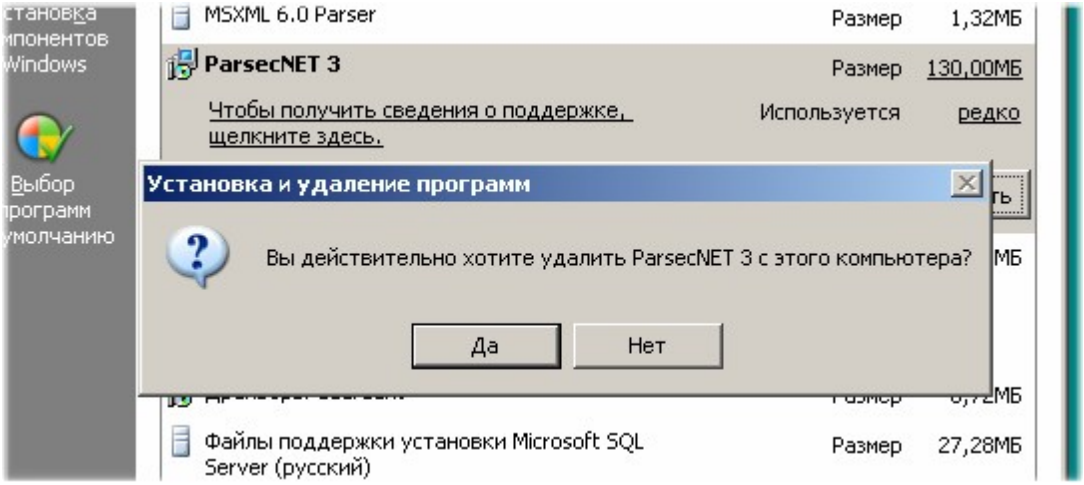


4.3 Удаление системы

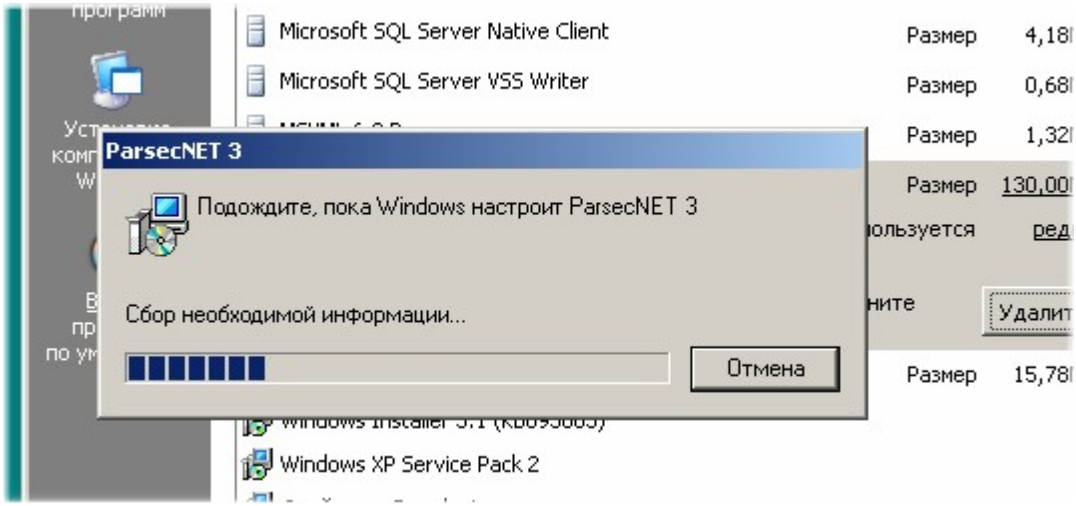
Для удаления ранее установленной системы ParsecNET 3 необходимо через меню Windows "Пуск - Панель управления" выбрать "Установка и удаление программ". В открывшемся окне найдите систему и запустите процесс удаления:



Далее потребуется подтвердить намерение удалить систему ParsecNET 3:



После подтверждения начнется собственно процесс удаления:

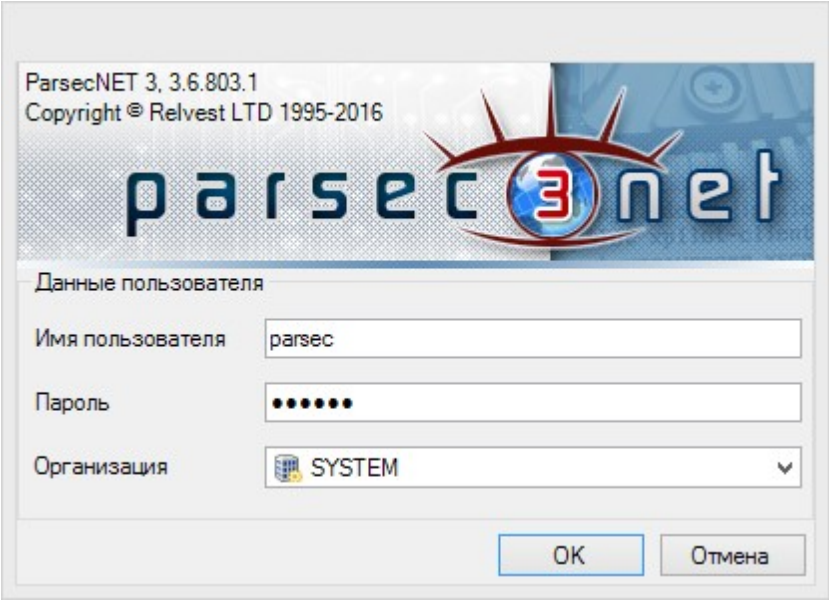


В ходе удаления будет задан вопрос о базах данных системы: вы можете удалить существующие базы данных ParsecNET 3, а можете их оставить (например, если вновь собираетесь ставить систему на этот же компьютер).

Независимо от способа установки системы, SQL-сервер автоматически не удаляется. При необходимости Вам следует самим удалить его аналогичным способом. Также автоматически не удаляются драйвера ключа защиты и драйвера USB-устройств - их тоже надо удалять отдельно.

5. Вход в систему

Запустите приложение Администрирование. Откроется окно авторизации:



Для первого входа используйте имя оператора **parsec** и пароль **parsec**.

Для обеспечения безопасности настоятельно рекомендуется сменить пароль оператора по-умолчанию.

Автоматический вход в систему

Для осуществления автоматического входа в систему ParsecNET 3 необходимо осуществить дополнительные настройки[730].

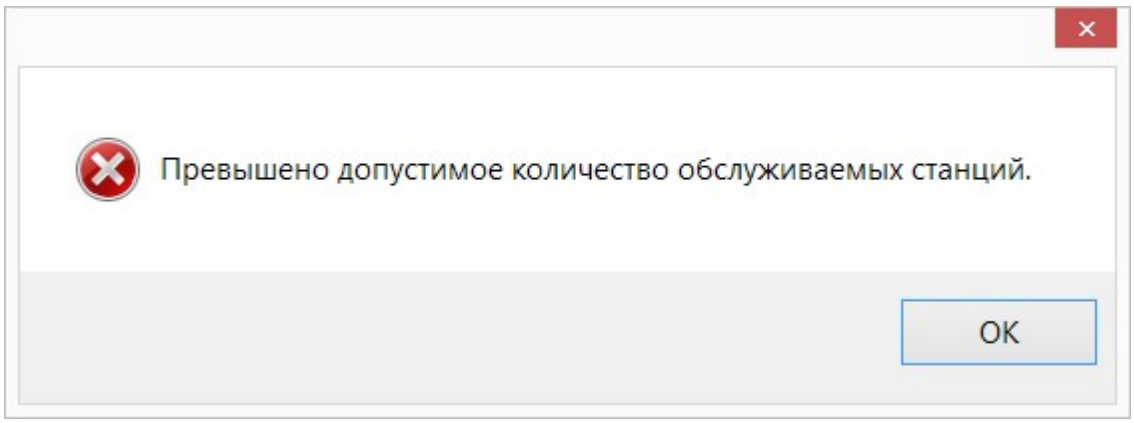
Вход по учетным данным Windows

Система позволяет настроить группы операторов таким образом[201], что операторы смогут входить в систему под теми доменными учетными записями, с которыми они входят в ОС Windows на своем компьютере. Логин при этом должен иметь вид <domain>\<user_name> (можно использовать и обратный слэш "/"), например, apple\jobs.

Функция интеграции с Active Directory работает только в случае, когда пользователь входит в ОС Windows под учетной записью из того же домена, в которой состоит группа разрешенных пользователей (Группа AD).

В случае входа в ОС Windows под локальной учетной записью авторизоваться в систему ParsecNET будет можно только под учетными данными оператора Parsec.

Если вход осуществляется с рабочей станции и количество рабочих станций, разрешенных ключом защиты, исчерпано, появится информационное окно. При этом учитываются только активные рабочие станции, т.е. те, с которых осуществлен вход в систему ParsecNET 3.



Смена пользователя

Чтобы сменить оператора, используйте команду "Сменить пользователя" в главном меню *Файл*. Сервер при этом не перезагружается.

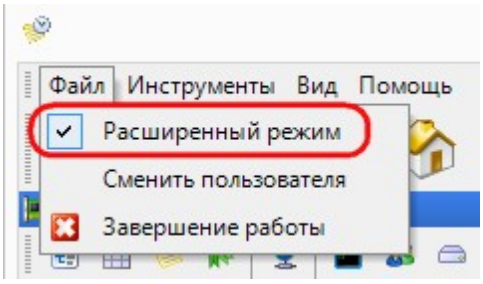
6. Пользовательский интерфейс

По сравнению с предыдущими версиями системы, пользовательский интерфейс ParsecNET 3 заметно изменился. В интерфейсе максимально реализованы все стандарты Windows, при этом все приложения (инструменты системы) имеют однотипный интерфейс пользователя, что облегчает использование системы при всей ее внутренней сложности.

- Все пользовательские инструменты функционируют в рамках "Рабочего стола[43]" системы, даже когда он не виден в явном виде на экране;
- С общими органами управления в приложениях ParsecNET 3 можно познакомиться на странице "Основные инструменты[41]";
- Свойства окон отдельных инструментов[45] и их панелей позволяют очень гибко настроить вид пользовательского интерфейса практически под любые требования, при этом настроенный вид может быть сохранен в профиле оператора и восстановлен в любой момент на любой рабочей станции системы;
- Пользовательский интерфейс поддерживает работу одновременно на нескольких мониторах (при условии, что этот режим поддерживает видеокарта) - можно, например, на одном мониторе открыть редактор персонала, а на другом одновременно запустить систему отчетов.

Режимы отображения интерфейса

После установки системы по-умолчанию включен упрощенный пользовательский интерфейс, функций которого достаточно для работы с простой системой. Если вам нужен полный набор функциональных возможностей, то следует включить расширенный режим в меню *Файл*:



В этом режиме в основных инструментах системы появляются расширенные функциональные возможности. На интерфейс лицензируемых модулей переключение типа интерфейса влияния не оказывает.

См. также:

- Основные инструменты 41
- Рабочий стол программы 43
- Общие свойства редакторов 50
- Свойства окон программы 45

6.1 Инструменты

Все инструменты программы доступны из стандартного меню, с помощью панели инструментов, а также из меню в области задач Windows.

В зависимости от версии системы (определяется вашей лицензией) могут быть доступны все либо часть из перечисленных ниже инструментов.

Меню инструментов рабочего стола использует следующие значки (пиктограммы) для каждого из инструментов:


Редактор оборудования[62] предназначен для конфигурирования аппаратной части системы. Здесь производится подключение оборудования и рабочих станций, настройка параметров контроллеров.


Редактор организаций[317]. Доступен только в профессиональной версии системы. Инструмент позволяет создать несколько независимых подсистем с полным разделением областей видимости.


Редактор системных настроек[341]. Данный инструмент позволяет настроить категоризацию транзакций системы, а также управлять лицензиями.


Редактор операторов[191]. Предназначен для назначения и распределения прав между операторами системы.


Редактор топологии[203]. Позволяет создать иерархическую систему территорий для объекта, например, поэтажную иерархию здания.


Редактор расписаний[213]. Данный инструмент предназначен для создания и редактирования как расписаний доступа, так и расписаний для системы учета рабочего времени.


Редактор групп доступа[245]. Позволяет распределять права субъектов доступа по территориям и по времени на основе групп доступа.


Редактор персонала[255]. Обеспечивает работу с базой данных субъектов доступа системы в рамках текущей организации.


Монитор событий[287]. Мониторинг событий и управление оборудованием организации.


Отчеты по событиям[302] в системе. Средство для ретроспективного анализа событий системы. Обеспечивает отбор событий по набору критериев.


Редактор заданий[321]. Позволяет создать, отредактировать или удалить задания, выполняющие определенную работу без вмешательства оператора.


Редактор шаблонов печати[417]. Обеспечивает подготовку шаблонов карт и пропусков для использования шаблонов при печати карт доступа.


Поправки к рабочему времени[462]. Позволяет вводить в систему такие поправки, как отпуска, больничные, командировки для учета их в системе учета рабочего времени.


Бизнес-отчеты. Версия устарела, рекомендуется использовать инструмент Бизнес-отчеты (версия 4).


Бизнес-отчеты (версия 4)[469]. Построение отчетов учета рабочего времени.


Бюро пропусков[432]. Работа с посетителями.


Отчеты по работе бюро пропусков[447].


Видеоверификация[506]. Специализированное рабочее место сотрудника службы безопасности.


Видеонаблюдение[515]. Работа с внешними системами видеонаблюдения.


Контроль заданного количества людей в помещении[294].

 Завершение работы.

 Вызов данной справки.

См. также

[Основные инструменты системы](60)

[Специальные средства](317)

[Дополнительные модули](417)

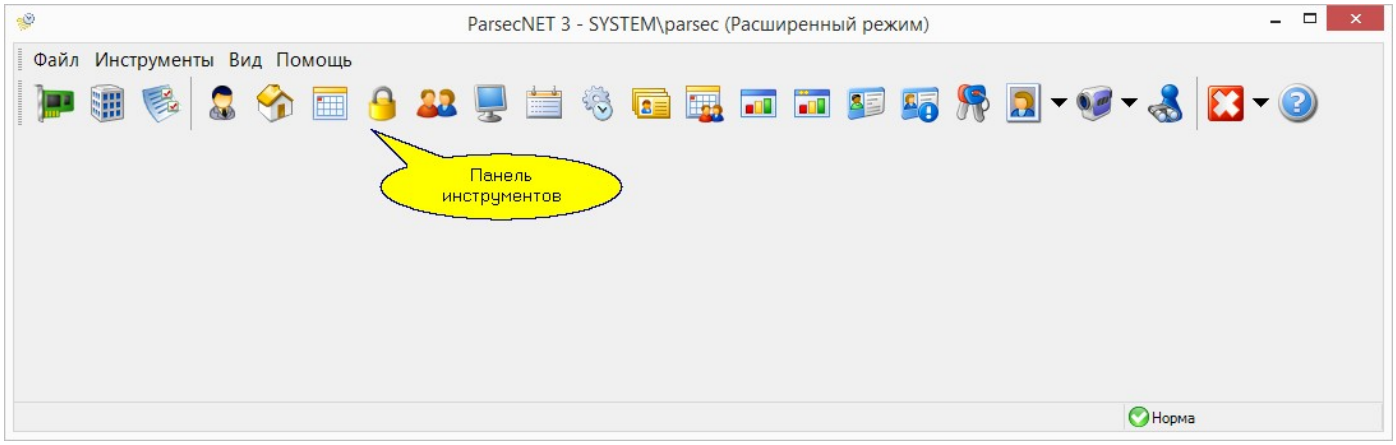
6.2 Рабочий стол программы

Пользователям Windows должно быть известно понятие "рабочего стола". Система ParsecNET 3 также имеет свой рабочий стол, который в отдельных случаях может полностью заменить рабочий стол Windows.

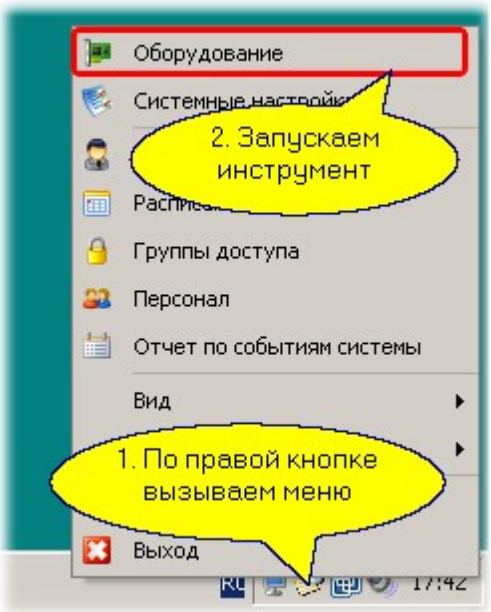
Рабочий стол программы выполняет следующие функции:

- Служит средой исполнения всех пользовательских приложений;
- Сохраняет и восстанавливает внешний вид приложения;
- Реализует различные режимы отображения: полноэкранный, оконный, свернутое в "трей" приложение;
- Обеспечивает доступ ко всем пользовательским компонентам.

Пример пустого рабочего стола (без открытых инструментов):



Можно переключить интерфейс пользователя в [безоконный режим](48), когда доступ к инструментам производится из панели задач Windows:



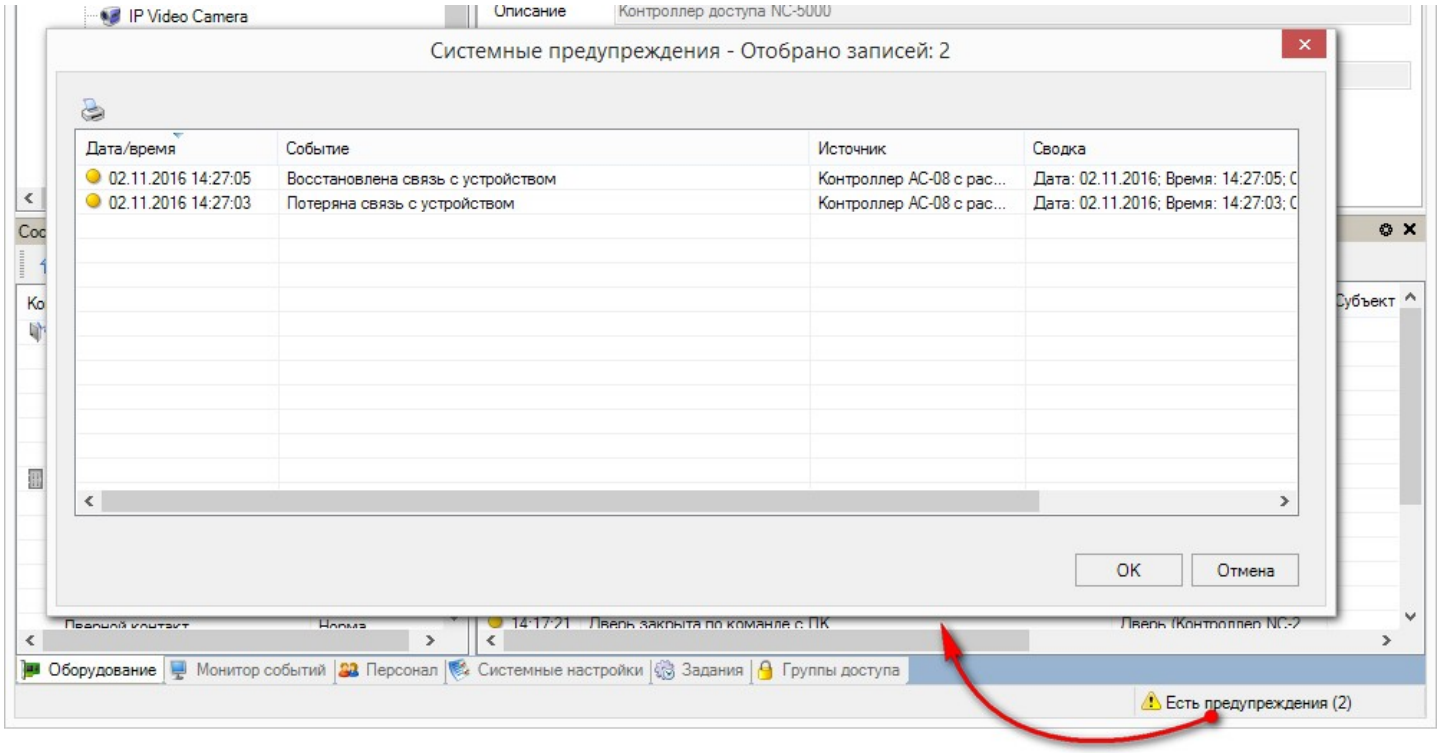
Режим работы рабочего стола, его размеры и положение для конкретного пользователя (оператора) запоминаются в его профиле и автоматически восстанавливаются при очередном

входе в систему. Более того, для каждого пользователя можно создать и сохранить более одного профиля, а при старте системы выбирать необходимый в данном сеансе профиль.

В разделе Свойства окон программы[45] вы можете узнать о различных вариантах настройки рабочего стола.

Справа внизу рабочего стола находится значок, показывающий состояние системы. При щелчке по нему открывается окно *Системные предупреждения*, содержащее диагностические события оборудования и видеособытия. Окно полностью аналогично панели *Диагностика*[153] редактора оборудования, но в нем отображаются только события, имевшие место с момента последнего открытия.

При наличии диагностических или видео событий, значок имеет вид "Есть предупреждения", при отсутствии - "Норма".



См. также:

Свойства окон программы[45]

Общие свойства редакторов[50]

6.3 Свойства окон программы

Начальные установки

После установки продукта вы имеете оконный интерфейс стандартного вида с определенным набором и положением панелей всех инструментов системы ParsecNET 3.

Если в результате экспериментов вы запутались и не можете получить пригодный для работы режим работы пользовательского интерфейса, то воспользуйтесь пунктом меню "Вид - По-умолчанию".

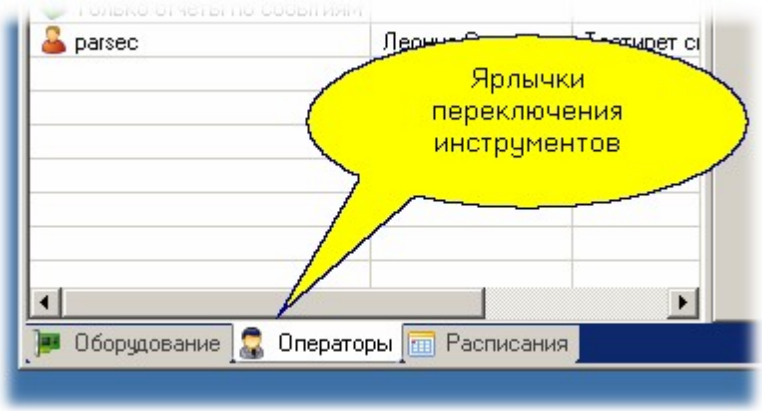


С помощью опции меню "Вид - По-умолчанию" вы всегда можете привести интерфейс системы к виду, который интерфейс программы имеет сразу после первой установки системы на компьютере.

Окна инструментов на рабочем столе

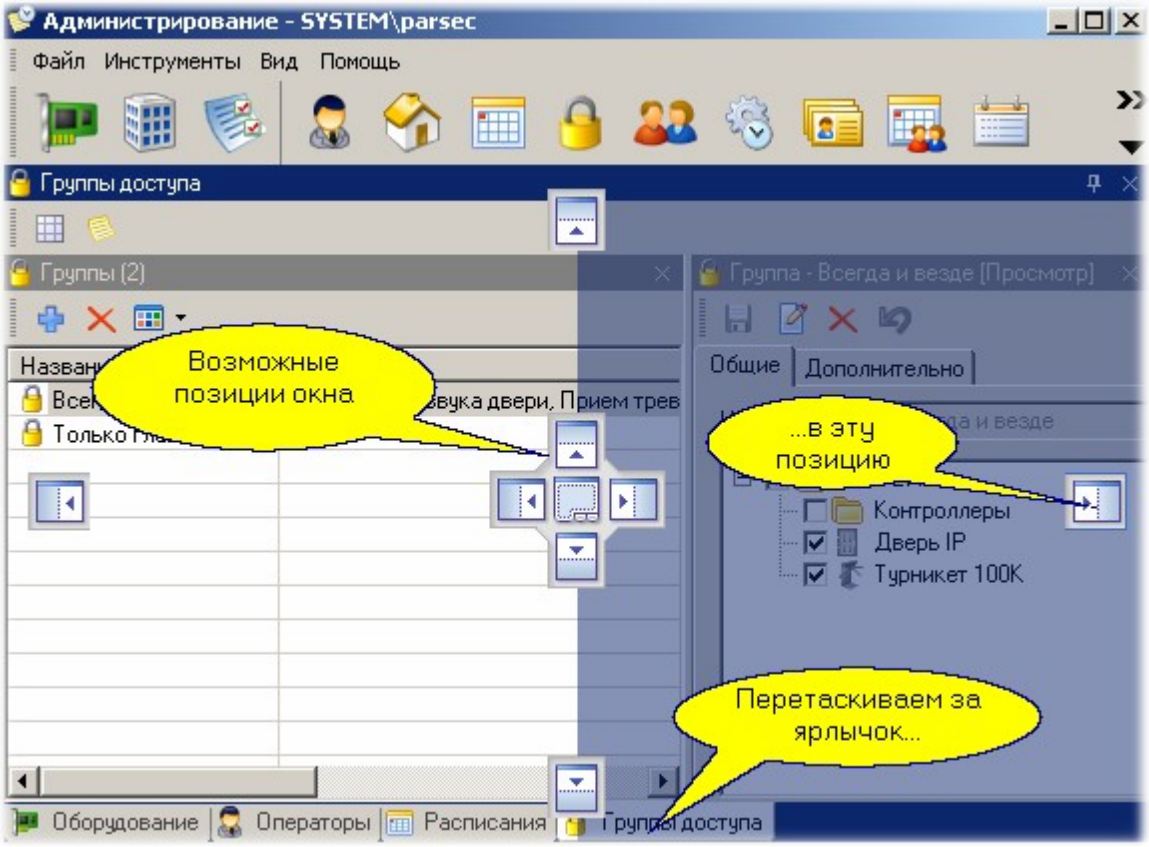
Все панели в каждом инструменте могут располагаться произвольным образом, быть видны или закрыты, при этом всегда есть возможность вывести на экран закрытую панель, а также восстановить вид интерфейса по-умолчанию, как после установки системы. При открытии окна каждого следующего инструмента его окно занимает всю область рабочего стола (кроме области панели инструментов). Переключаться между как-бы находящимися друг за другом окнами инструментов можно разными способами:

- Через панель инструментов или меню *Инструменты*. Повторный вызов ранее открытого инструмента приводит к выводу его на передний план на рабочем столе.
- С помощью ярлыков окон инструментов на нижней границе окна рабочего стола, что иллюстрируется рисунком ниже:

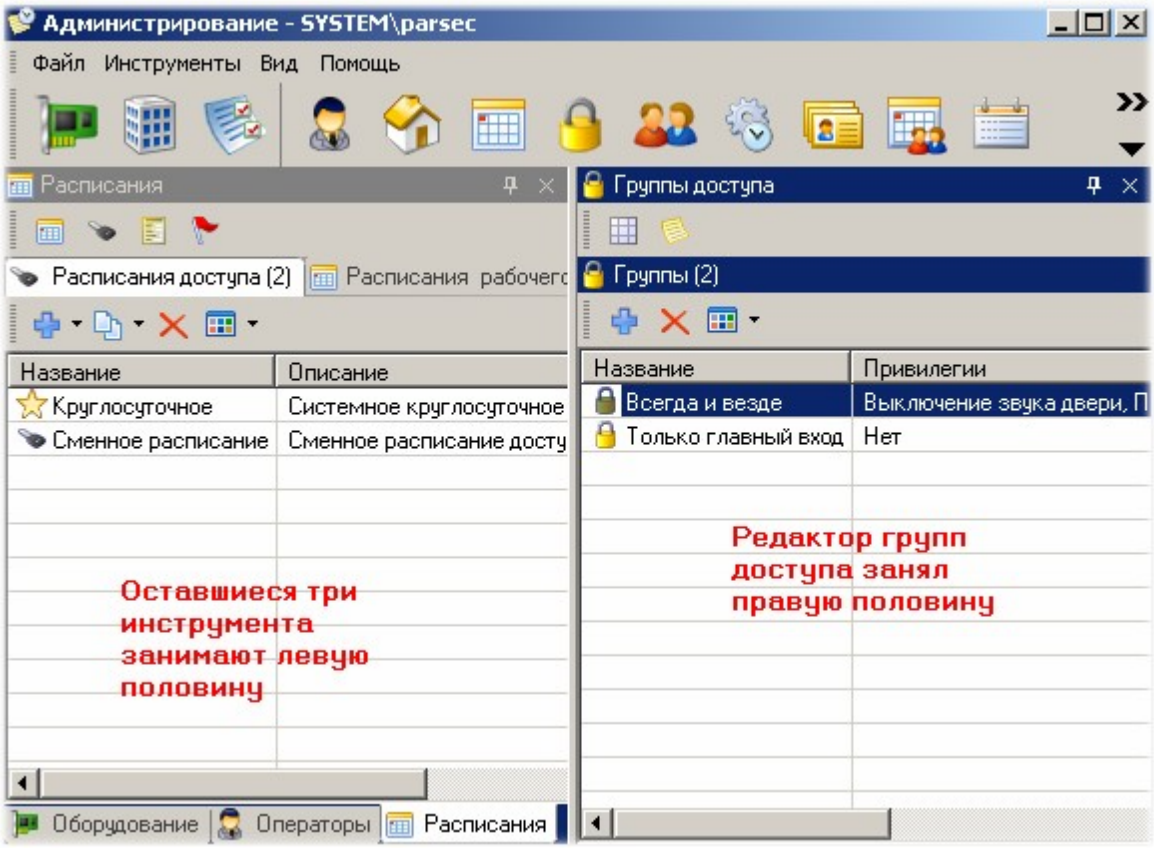


Изменение компоновки окон

Окна инструментов могут располагаться в области рабочего стола системы не только друг за другом, но и в любом другом положении. Чтобы изменить положение окна его необходимо перетащить мышкой, взяв за ярлычок окна инструмента. Во время перетаскивания на рабочем столе появятся маркеры, которые подскажут возможные положения перетаскиваемого окна после его отпускания, а затененный прямоугольник перетаскиваемого окна указывает положение, которое займет окно, если его сейчас отпустить. Это иллюстрируется рисунком ниже:



После отпускания мышки редактор групп доступа займет правую половину рабочего стола программы, как показано ниже:



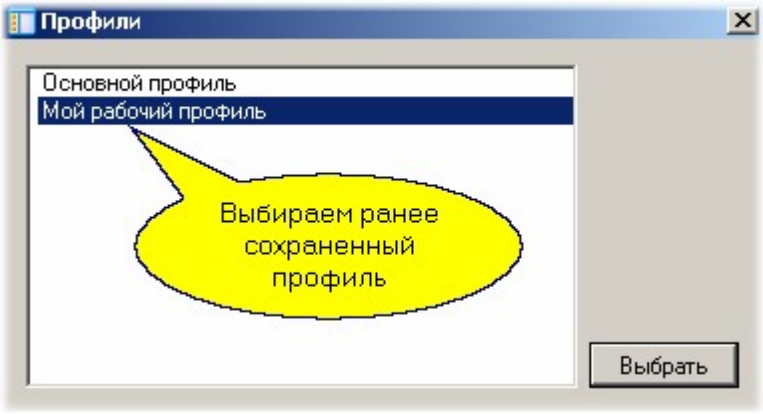
Используя описанную технику вы можете сформировать произвольную компоновку рабочего стола, а затем сохранить ее (по-умолчанию в меню *Вид* включена опция "Автосохранение", и если вы ее не выключали, то ваш набор окон при выходе сохранится автоматически).

Несколько вариантов наборов рабочего стола

Можно создать несколько вариантов наборов окон рабочего стола и сохранить их в профилях с разными именами.

1. Откройте пункт главного меню *Вид*;
2. Выберите "Сохранить как..." чтобы создать новый профиль. Или выберите "Сохранить", чтобы перезаписать текущий профиль (это происходит автоматически каждый раз, когда вы выходите из системы). В последнем случае никаких дополнительных окон не появляется;
3. В открывшемся диалоговом окне *Профили* нажмите на кнопку *Новый* и введите свое названия для профиля;
4. Нажмите клавишу *Enter*.

Теперь при следующем запуске программы вам будет задан вопрос, какой из профилей вы хотите загрузить на текущий сеанс работы с системой. Ниже показан диалог выбора профиля после сохранения дополнительного профиля с именем "Мой рабочий профиль":

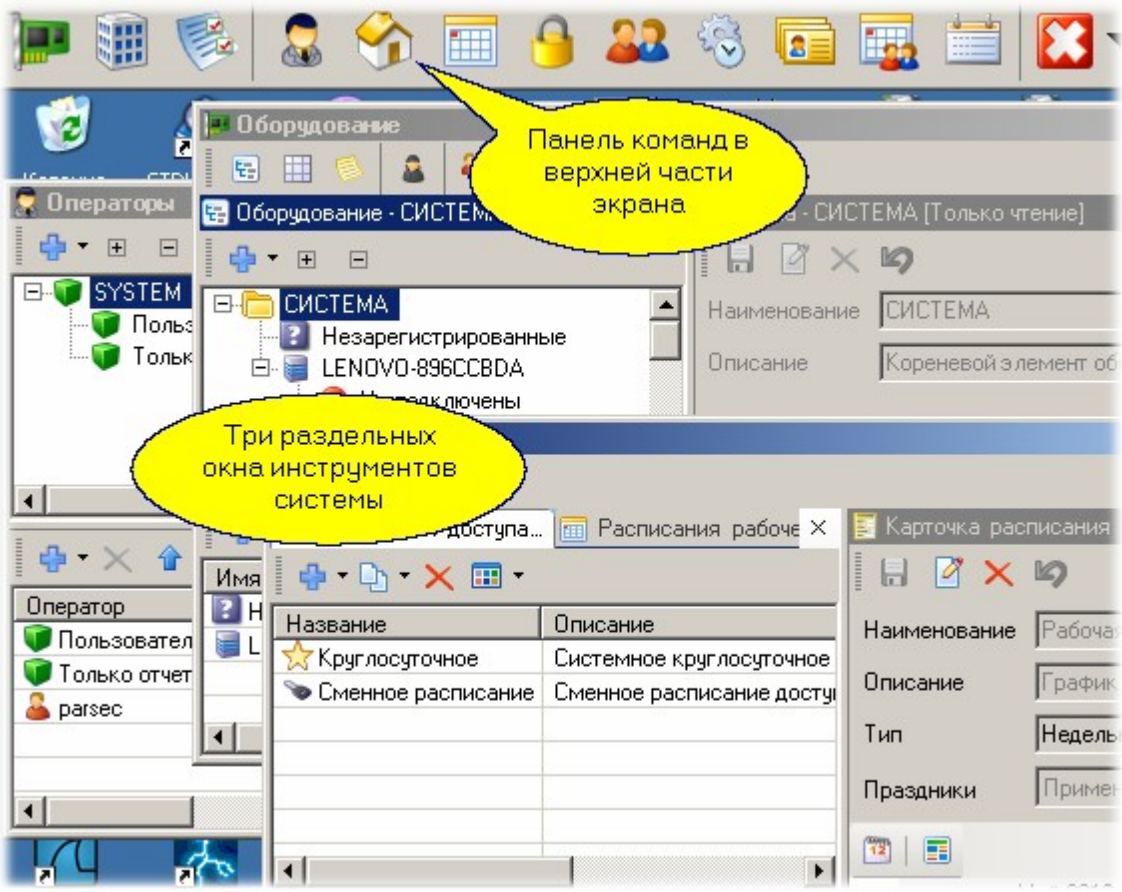


Режимы рабочего стола

Рабочий стол системы может функционировать в различных режимах. Выше мы рассматривали стандартный оконный вариант рабочего стола, однако он может работать и в других режимах:

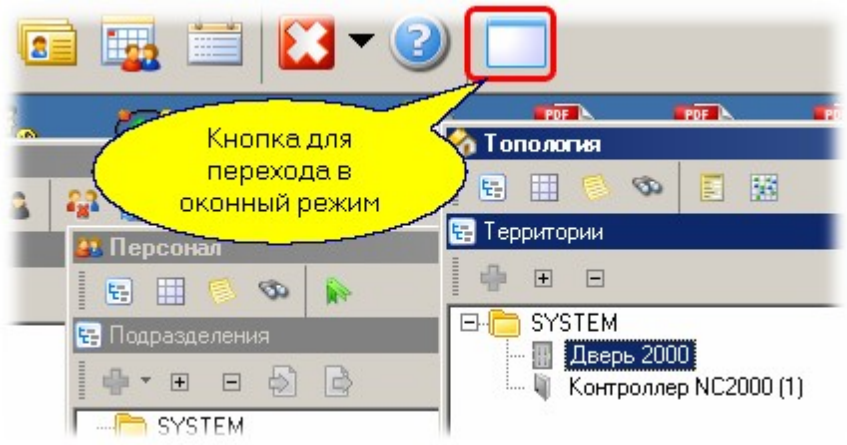
- ***Режим панели команд***

В этом режиме панель инструментов расположена отдельно, а окна инструментов - отдельно в рамках рабочего стола Windows. На рисунке ниже показан такой вариант рабочего стола:



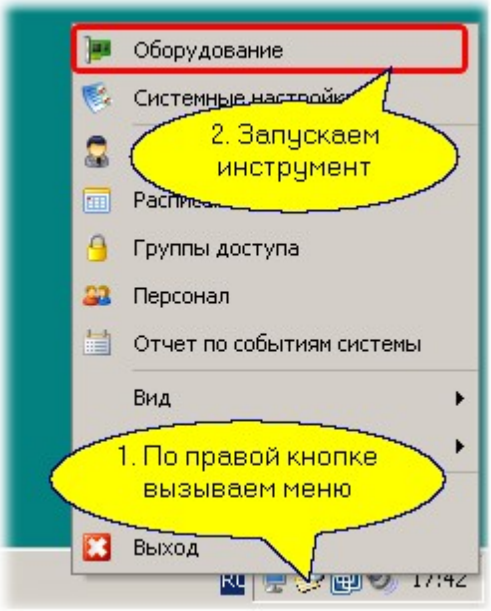
В данном режиме окна отдельных инструментов можно уложить в одно окно с ярлычками. Саму панель инструментов можно расположить вдоль любой стороны экрана (кроме нижней). Для перетаскивания панели инструментов нажмите клавишу *Ctrl*, и удерживая ее, переместите панель в требуемое положение.

При переходе в этот режим на панели инструментов появляется дополнительная "кнопка", которая позволяет оперативно перейти в стандартный оконный режим рабочего стола:



- ***Режим панели задач***

Отличается от предыдущего режима отсутствием панели команд. Доступ к функциям меню в этом режиме осуществляется только через пиктограммку системы в панели задач Windows, как показано ниже:



- ***Полноэкранный режим***

Для конкретного оператора может оказаться полезным организовать полноэкранный режим работы того или иного инструмента: например, монитора событий или видеоверификации. В полноэкранном режиме не будет видна даже панель задач Windows и кнопка *Пуск*, что позволит оператору сосредоточиться на конкретной работе.

Переключение из полноэкранного режима и обратно осуществляется с помощью клавиши **F11**.

См. также:

Рабочий стол программы 43

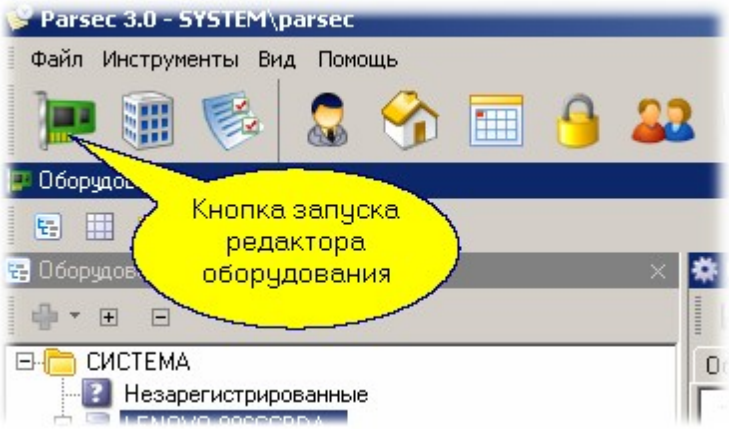
Общие свойства редакторов 50

6.4 Общие свойства редакторов

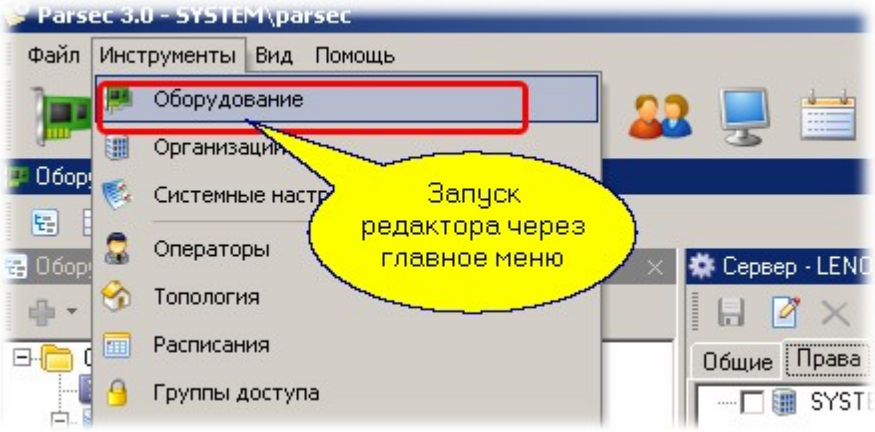
Запуск редакторов

Все редакторы или модули системы запускаются одинаковым образом. Это можно сделать через панель инструментов или через главное меню рабочего стола программного комплекса ParsecNET 3. Покажем это на примере редактора оборудования.

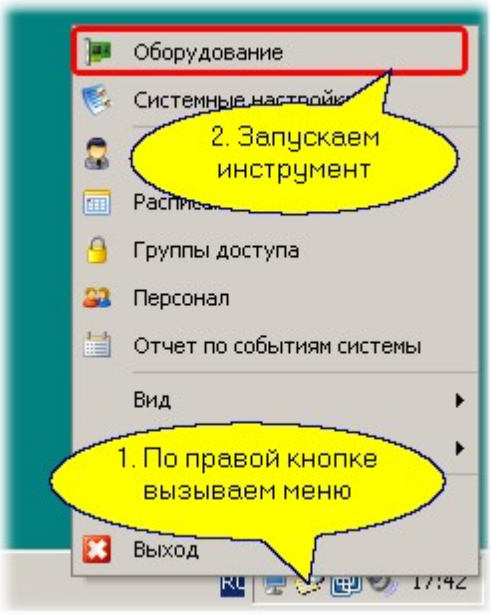
Редактор оборудования запускается из меню рабочего стола системы ParsecNET 3 как показано ниже



Второй способ запуска редактора - из главного меню рабочего стола системы:

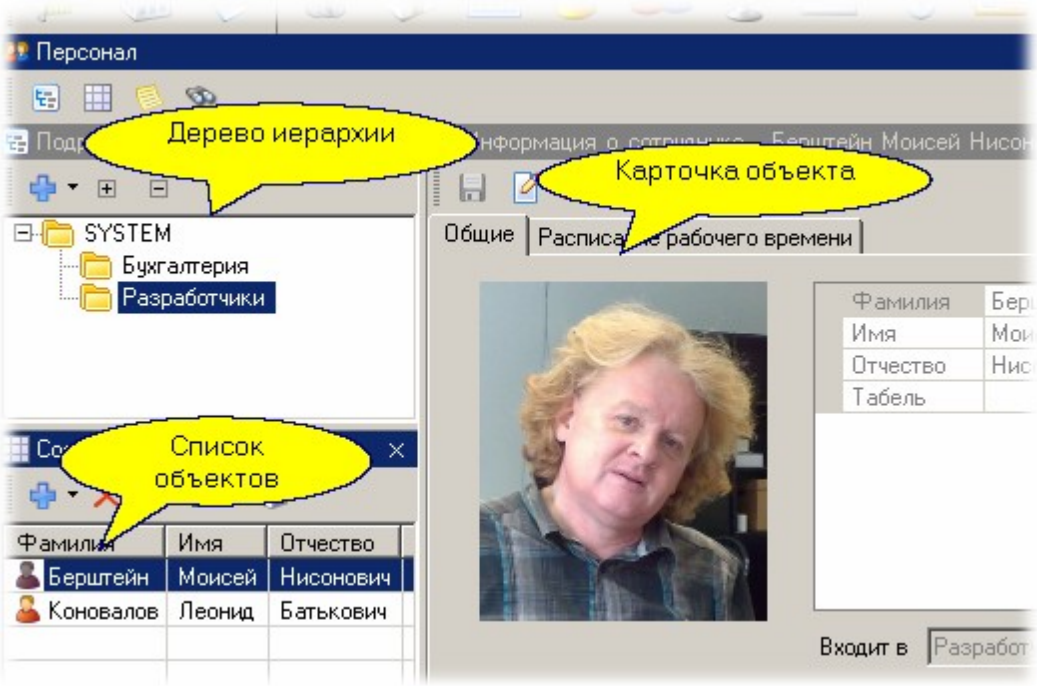


Третий способ запуска инструмента - через панель задач Windows, как показано ниже.

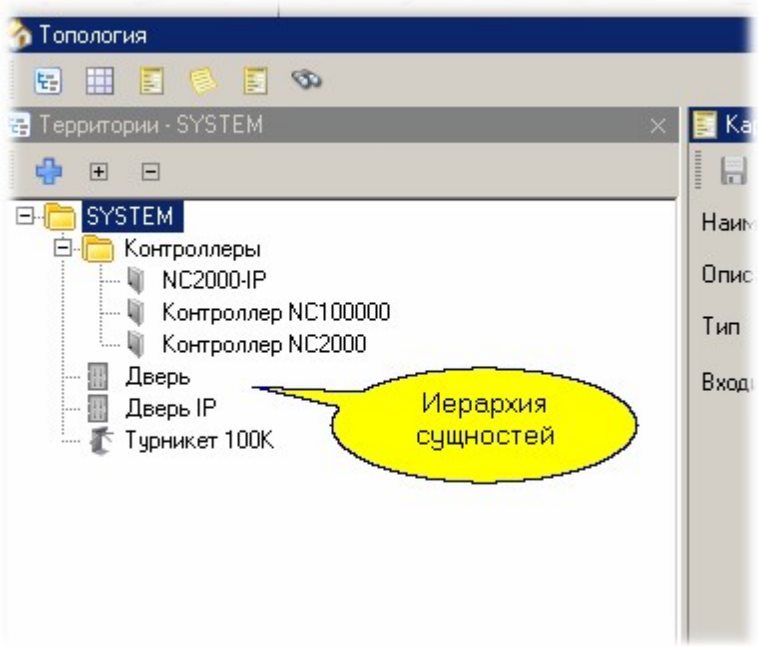


Панели редактора

Рабочие инструменты программы (редакторы) имеют много общего в плане устройства и свойств. Большинство редакторов состоят из трех панелей. Для иллюстрации ниже показаны панели редактора персонала.

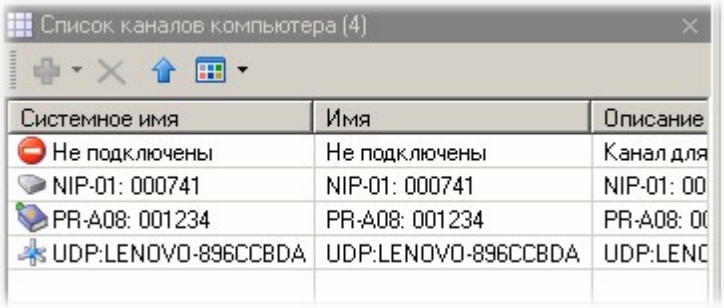


Первая панель показывает иерархию сущностей, с которыми работает редактор. Например, в редакторе топологии системы эта иерархия будет показывать все оборудование текущей организации:

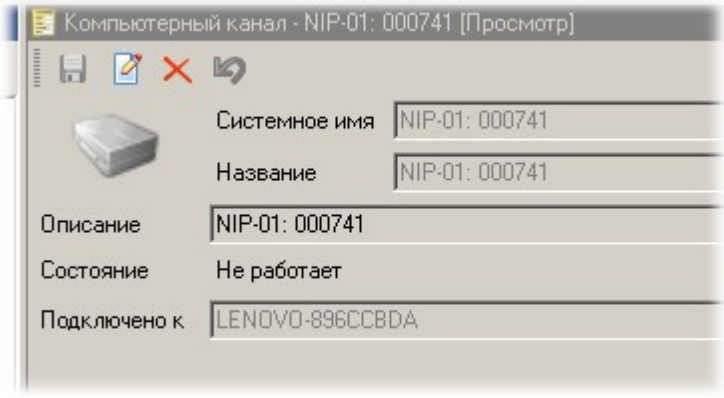


На большинстве панелей, показывающих иерархию, есть две небольшие кнопки: ⊞ и ⊟. Их назначение - полностью раскрыть дерево иерархии или наоборот полностью его свернуть.

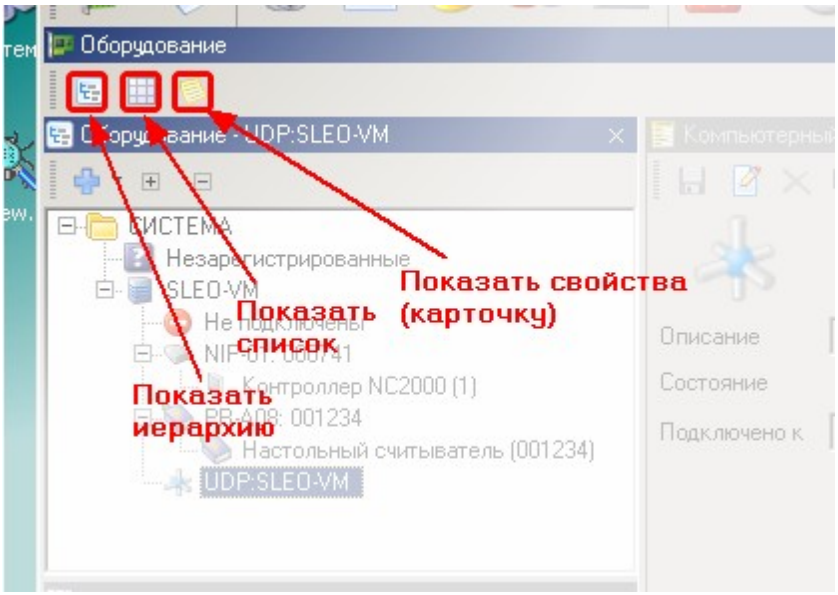
В раскладке по-умолчанию панель иерархии расположена в верхней левой части окна. Под иерархией располагается список компонентов, которые входят в конкретный уровень иерархии. Например, если в редакторе оборудования в иерархии выбрать компьютер, то в список попадут подключенные к нему компоненты:



И, наконец, в правой части окна редактора обычно располагается карточка выбранного компонента со всеми его данными. Именно в карточке можно менять свойства сущности, которую мы редактируем. Ниже показан фрагмент карточки оборудования: интерфейса NIP-01



Вы можете оставить только те панели, которые вам нужны в данный конкретный момент, можете поменять местоположение панелей и их размеры в соответствии с личными предпочтениями. Если потребуется открыть закрытую ранее панель, то это всегда можно сделать с помощью кнопок, расположенных на панели инструментов редактора в его верхней части:



Органы управления редакторов

Во всех инструментах в тех или иных комбинациях используются однотипные органы управления в виде кнопок со значками, соответствующими функциям конкретной кнопки.


Кнопка добавления нового элемента. Если можно добавить больше одного типа элементов, то справа от кнопки имеется стрелка, направленная вниз. При нажатии на стрелку выпадает список типов элементов, которые можно добавлять. Например, в редакторе персонала можно добавить подразделение или сотрудника.


Кнопка удаления выбранного элемента. Находится в активном состоянии при условии, что выбранный элемент может быть удален.


Кнопка перехода в режим редактирования. На время редактирования запись в базе данных об этом элементе блокируется с тем, чтобы параллельно никто не мог редактировать тот же самый элемент.


Кнопка сохранения результатов редактирования. После нажатия на кнопку отредактированные данные сохранятся в базе данных системы, блокировка с записи снимается.


Кнопка отмены результатов редактирования. Изменения не сохраняются, блокировка с записи снимается, делая ее доступной для редактирования с другой рабочей станции.

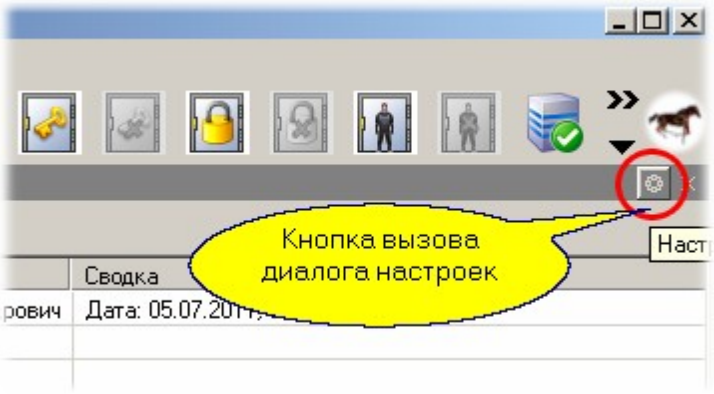

Кнопка переключения вида списка (как и в Проводнике Windows). Список можно представить в виде маленьких или больших иконок, в виде списка или в виде таблицы. по-умолчанию используется табличное представление как наиболее информативное.


Кнопка панели поиска. Если для конкретной сущности есть возможность поиска по заданным критериям, то у редактора есть панель поиска, которая по-умолчанию закрыта, но при нажатии на кнопку появляется в окне редактора. Например, в редакторе персонала можно осуществлять поиск субъектов доступа по фамилии, ее части и ряду других признаков.


Кнопка печати. Присутствует, если в инструменте есть возможность печати каких-либо данных.

Настройки инструментов

Если какая - то панель инструментов имеет отдельный диалог настроек, то в правом верхнем углу панели вы сможете видеть кнопку с символом "шестеренки", как, например, показано на рисунке ниже для панели событий монитора.



См. также:

Свойства окон программы 45

6.5 Блокировка внешнего вида

Для чего это надо

Иногда конкретному оператору надо запретить менять внешний вид его рабочего стола, чтобы он умышленно или не умышленно не мог привести систему в состояние, в котором он не сможет выполнять свои прямые обязанности

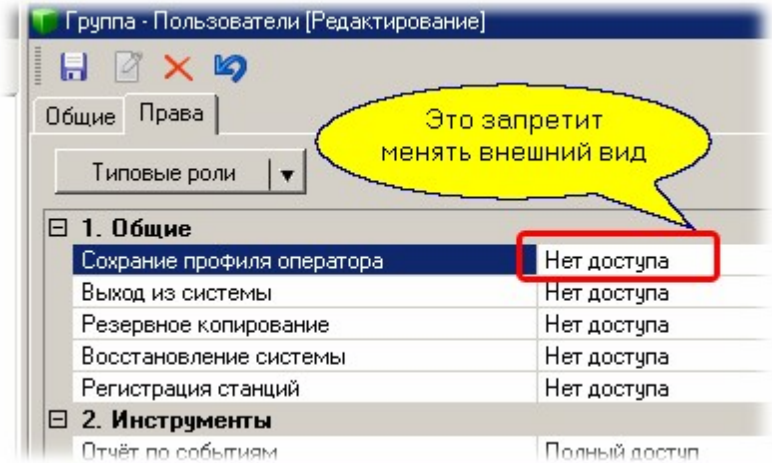
Для этого можно запретить операторам конкретной группы менять внешний вид рабочего стола.

Как это делается

Для блокировки внешнего вида конкретной группе операторов следует проделать следующие шаги:

Шаг 1. Создание группы операторов с ограниченными правами

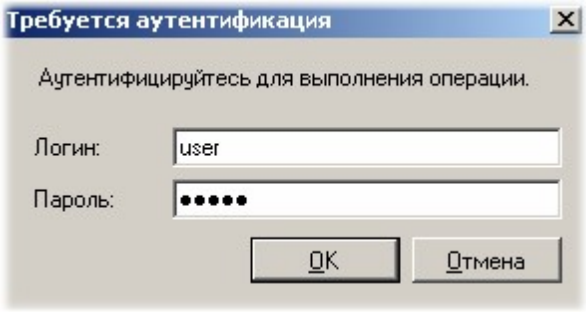
1. Запустите приложение ***Администрирование***.
2. В редакторе операторов создайте новую группу, например, "Наблюдатели".
3. Поменяйте права этой группы как показано на рисунке ниже. Дополнительно можно запретить оператору выход из системы (это тоже показано на рисунке).



4. Создайте в этой группе оператора с конкретным именем и паролем.

Шаг 2. Настройка внешнего вида рабочего стола

1. Зайдите в систему от имени созданного на предыдущем шаге оператора с ограниченными правами.
2. Поменяйте настройки рабочего стола так, как это необходимо. При сохранении созданного вида в профиль оператора будет выведен диалог подтверждения полномочий на выполнение операции следующего вида:



3. Вам следует ввести имя и пароль оператора, который имеет право на изменение внешнего вида рабочего стола.

Если вам необходимо проделать несколько различных манипуляций и не для одного, а для нескольких операторов, то чтобы не вводить многократно имя и пароль оператора с ограниченными правами можно поступить следующим образом:

1. В редакторе операторов временно поднять права для группы, для которой вы будете настраивать пользовательский интерфейс.
2. Сделать и сохранить требуемые профили для оператора (или нескольких операторов). Если вы делаете разные настройки для нескольких операторов, то вам все равно придется несколько раз заходить в систему от имени этих операторов.
3. После этого следует восстановить ограничение прав для данной группы операторов.

6.6 Средства поиска

В каких инструментах работает поиск

Поиск вам не потребуется, если у вас одна точка прохода (дверь) и десяток субъектов доступа, а оператор вообще один. Если же у вас крупная система с десятками операторов и тысячами субъектов доступа, то найти что-то конкретное в больших базах данных вручную будет проблематично.

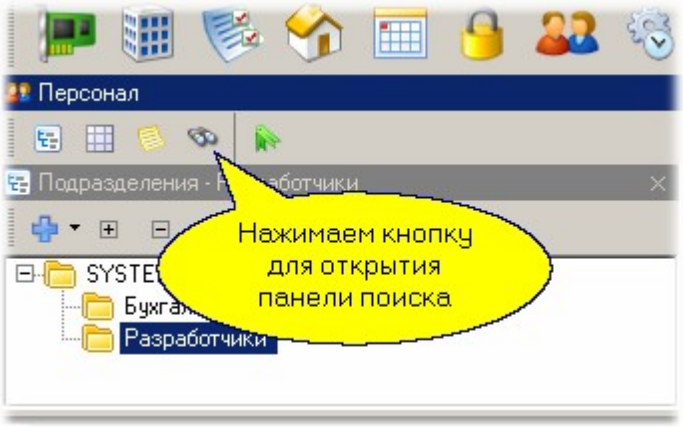
Функция поиска работает в следующих базовых инструментах системы:

- Редактор операторов[191]
- Редактор топологии[203]
- Редактор персонала[255]
- Модуль поправок рабочего времени[462]
- Монитор событий[287]
- Отчеты по событиям[302]

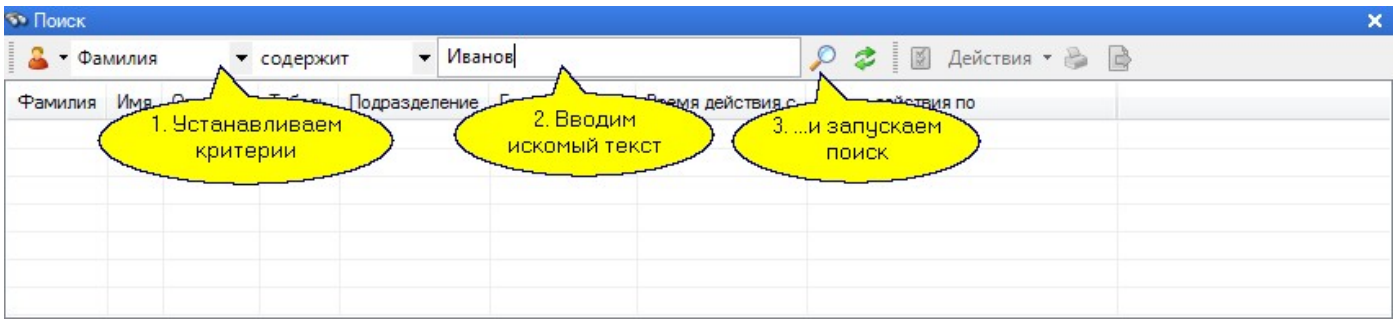
Здесь не упоминаются средства поиска для дополнительных инструментов (отдельно лицензируемых модулей) - они описаны в соответствующих разделах руководства.

Как работает поиск

Для примера рассмотрим работу системы поиска в редакторе персонала. Панель поиска открывается по нажатию кнопки с изображением бинокля, как показано ниже:



В открывшейся панели поиска выбираем критерии, по которым требуется осуществлять поиск, в данном случае сотрудника, и нажимаем на кнопку поиска. Указанные действия и полученный результат иллюстрируются следующим рисунком:



Набор полей, по которым может осуществляться поиск, зависит от того, в каком редакторе и какие сущности вы собираетесь искать. Подробнее об этом можно узнать в описаниях конкретных

редакторов системы. В частности, в редакторе персонала в качестве критерия могут выбираться не только фамилия, имя и отчество, но и данные всех введенных вами дополнительных полей.

7. Обзор системы

Общие положения

В данном разделе мы рассмотрим последовательность основных операций по вводу в эксплуатацию системы ParsecNET 3. Детальное описание работы с конкретными инструментами вы найдете в других разделах руководства.

Система оперирует с ***оборудованием***, которое привязывается к ***территориям***, и с ***персоналом***, который принадлежит какой-то ***организации*** и может быть сгруппирован по ***подразделениям***. Работой системы управляют ***операторы***, которые, в свою очередь, входят в группы для упрощения назначения им разных наборов привилегий. Области видимости для каждой группы операторов могут быть назначены индивидуально. При этом в область видимости входит территория, объекты которой видны оператору, и подразделения, с персоналом которых может работать оператор данной группы.

Мы пока оставим в стороне распределение прав между группами операторов и будем считать, что работаем под логином Администратора системы, которому доступны все объекты. Кроме того, наша система будет состоять только из одной организации.

Общая последовательность действий по вводу системы в работу такова:

Подключение оборудования

Оборудование подключается к системе с помощью Редактора оборудования[62]. Если оборудование подключено к компьютеру до запуска системы, то программа сама находит и подключает известное ей оборудование, как это описано в разделе Быстрый старт.

Любую единицу оборудования можно в любой момент подключить вручную с любой зарегистрированной рабочей станции. Для каждого контроллера необходимо настроить его режимы работы и требуемые для нормальной работы параметры. Например, для контроллера доступа надо установить режим работы: дверь с односторонним проходом, с двухсторонним проходом или турникет, а также выставить еще целый ряд параметров, про которые можно узнать из руководства пользователя на конкретную модель контроллера.

Если система обнаружила оборудование в автоматическом режиме, то для него устанавливаются режимы по-умолчанию, которые, возможно, надо будет позже скорректировать. Кроме того, автоматически найденное оборудование распределяется в корень территории Система. В дальнейшем, если вы создаете сложную структуру территорий, вам понадобится перенести оборудование из корня в соответствии с вашей топологией. Это повышает информативность, упрощает управление системой, а также позволяет ввести разграничение областей видимости территорий и оборудования для разных операторов.

Создание территорий и распределение оборудования

Если у вас система среднего или большого масштаба, вам непременно надо создать топологию. Топология представляет собой "дерево" территорий. Она отображает структуру объекта, на котором установлена система, в удобном для пользователей виде.

Детальное описание процесса создания территорий см. в разделе Редактор топологии[203].

После того, как структура территорий создана, необходимо распределить между ними имеющееся оборудование в соответствии с его принадлежностью. Подробнее об этом в разделе Редактор оборудования[62].

Создание расписаний

Для обеспечения привязки прав субъектов доступа ко времени необходимо создать расписания. В системе могут быть два типа расписаний: расписание доступа, определяющее интервалы времени, в которые у субъекта есть доступ на ту или иную территорию, и расписания рабочего времени, используемые подсистемой УРВ.

Работа с расписаниями описана в разделе Редактор расписаний[213] .

Кроме того, имеется два типа расписаний в каждой группе, отличающиеся привязкой к календарю. Недельные расписания всегда связаны с днями недели календаря и имеют период только 7 дней.

Сменные расписания могут иметь любой период, в том числе и 7-дневный, но к дням недели никак не привязываются. В сменном расписании праздник может быть вставлен так, что следующие за праздником дни расписания просто сдвинутся на день. В недельных расписаниях вставка праздника с раздвижкой расписания невозможна.

Следует отметить, что многие типы контроллеров поддерживают ***только недельные расписания***. Подробную информацию ищите в документации на контроллеры.



Замечание: В системе всегда есть круглосуточное расписание доступа, которое позволяет предоставить доступ без ограничений по времени. Если такой режим вас устраивает, то создавать собственные расписания нет необходимости.

Создание групп доступа

Понятие группы доступа введено для упрощения назначения прав каждому из субъектов доступа. Группа доступа определяет ***объекты системы***, к которым у субъекта есть доступ с учетом назначенного группе ***расписания доступа***. Работа с группами доступа описана в разделе Группы доступа[247] , а описание редактора в разделе Редактор групп доступа[245] .

Без назначения субъекту группы доступа невозможно дать ему права на пользование системой.

Отдельно следует отметить, что в системе каждому субъекту можно назначить более одной группы доступа даже для одной карты (напомним, что у пользователя может быть зарегистрировано в системе и несколько карт).

Кроме того, группы доступа имеют свой ***тип***. Группы доступа для подсистемы доступа ***Parsec***, охранной подсистемы ***Parsec*** и охранно-пожарной подсистемы "***Стрелец***" являются разными.

Создание подразделений и ввод персонала

Для совсем небольшой системы нет необходимости создания подразделений, персонал можно ввести в корень организации Система. Для более крупных систем логично построить структуру подразделений, и персонал распределить по подразделениям в соответствии с реальной принадлежностью.

Данный процесс описан в разделе Персонал[258] , а детальное описание редактора персонала приведено в разделе Редактор персонала[255] .

Добавление групп операторов

Рассмотренных выше шагов достаточно для создания полнофункциональной системы, однако необходимо не забыть ограничить права тех операторов системы, которым по должности или другим причинам нет необходимости пользоваться теми или иными функциями системы. Как это сделать вы можете прочитать в разделе Безопасность[193] , а в разделе Редактор операторов[191] дано подробное описание соответствующего инструмента.

Дополнительные возможности

Для того, чтобы получить максимум от установленной системы, администратору может понадобиться изучить и некоторые дополнительные возможности, к которым, в частности, относятся:

Множественные организации

Если позволяет ваша лицензия, кроме организации Система (SYSTEM), создаваемой по-умолчанию при установке системы, можно создать необходимое число дополнительных организаций. Версия с поддержкой более одной организации может потребоваться для крупного объекта типа бизнес-центра, где есть одна эксплуатирующая компания и множество арендаторов, желающих ограничить доступ к приватным данным своей организации. Как это реализуется, можно посмотреть в разделе Редактор организаций[317] . Все дополнительные организации не будут иметь доступа к редактору оборудования, то есть не смогут добавлять, удалять, редактировать контроллеры, поскольку в крупных системах это привилегия службы эксплуатации.

При использовании нескольких организаций, ***только в системной организации*** будут доступны следующие три редактора:

- Редактор оборудования;
- Редактор организаций;
- Редактор системных настроек.

При создании новой организации создается ее администратор, то есть оператор с максимальными правами. Его задача - при необходимости создать других операторов.



Пароль администратора новой системы необходимо сохранять, так как при его утере не будет никакой возможности войти в организацию. Желательно логин и пароль главного администратора системы продублировать картой, которую затем спрятать в надежное место.

Лицензии и ключ защиты

Устанавливаемый на сервере системы ParsecNET 3 ключ защиты определяет широту вашей лицензии, то есть возможности системы, которыми вам разрешено пользоваться. Целый ряд возможностей системы, таких, например, как учет рабочего времени, создание шаблонов печати карт, Бюро пропусков являются платными, и в минимальной версии ПО будут недоступны. Вы можете получить временную лицензию для ознакомления с работой таких модулей, и если модуль окажется необходим, то можно купить постоянную лицензию на него.

Кроме специальных возможностей, ключ защиты определяет количество точек прохода и дополнительных рабочих станций, которые могут быть использованы в системе.

О том, как обновить имеющийся у вас ключ, можно прочитать в разделе Редактор системных настроек[344] .

Автоматизация

В системе ParsecNET 3 имеется возможность создавать достаточно сложные сценарии автоматического управления с использованием Редактора заданий[321] . Данный инструмент, работающий в фоновом режиме, позволяет создавать задания, которые будут по времени или по заданному событию посылать команды оборудованию для выполнения тех или иных действий. Например, можно по расписанию открывать и закрывать двери, ставить на охрану и снимать с охраны отдельные области, создавать резервную копию БД и так далее.

Задания исполняются ядром системы, которое работает как служба Windows, поэтому единственным условием работоспособности является включенный компьютер. Запуск пользовательского интерфейса для работы менеджера заданий не требуется.

Категории событий

Самым опытным пользователям может потребоваться редактирование Категории транзакций. Это происходит крайне редко, но такая возможность системой предусматривается. Изначально в системе ParsecNET 3 все события (транзакции системы) распределены по различным категориям в соответствии с их смыслом. При необходимости можно перенести события из одной категории в другую, а также создать свои собственные категории.



Настоятельно рекомендуем не менять категоризацию событий без необходимости, потому что это может привести вас к путанице.

Если вы все-таки решили это сделать, обратитесь к Редактору системных настроек[341].

Мини-консоль

Это специальное маленькое приложение, которое позволяет выводить уведомления о наступлении заранее настроенных событий через панель задач Windows. Это единственное приложение с пользовательским интерфейсом, которое требует работающего механизма заданий.

Мини-консоль[394] предназначена в первую очередь для руководителей различного уровня, которым нужна минимальная оперативная информация из системы (например, о приходе определенного сотрудника или о наступлении обеденного перерыва).

8. Основные инструменты системы

Базовые инструменты

В данном разделе вы найдете детальное формальное описание основных инструментов системы ParsecNET 3. Инструменты для специфических применений, связанных с дополнительным лицензированием компонентов системы, будут рассмотрены в отдельном разделе: Дополнительные модули[417].

Инструменты будут рассматриваться в том порядке, в котором ими рекомендуется пользоваться при начальной настройке системы. При ее эксплуатации можно пользоваться инструментами в произвольном порядке, в зависимости от текущих задач.

Общие свойства редакторов (для исключения многократного повторения по тексту документа) изложены в разделе Общие свойства редакторов[50].

Итак, в данном разделе мы рассмотрим инструменты:

- Редактор оборудования[62]. Предназначен для конфигурирования аппаратной части системы. Только с правильно подключенным и сконфигурированным оборудованием система сможет корректно выполнять возложенные на нее функции.
- Многосерверность[164] не является отдельным инструментом сама по себе. Этот функционал позволяет в крупной, территориально распределенной организации установить несколько серверов ParsecNET и организовать между ними синхронизацию данных для выполнения некоторых общих задач.
- Редактор топологии[203]. Предназначен для создания иерархической структуры территорий вашего объекта.
- Редактор операторов[191]. Необходим для создания групп операторов с различным набором прав и самих операторов.

- Редактор расписаний[213] . Необходим в случае, если вы используете правила доступа, отличные от круглосуточного доступа в любое из помещений.
- Редактор групп доступа[245] . На основе структуры территорий и расписаний создает группы доступа, которые затем присваиваются персоналу.
- Редактор персонала[255] . Позволяет вводить в систему субъектов доступа, с назначением им прав доступа. Позволяет также вести небольшую кадровую базу данных за счет произвольно конфигурируемых дополнительных полей.
- Монитор событий[287]. Основное средство для оперативного наблюдения за происходящим в системе.
- Отчеты по событиям[302] . Модуль позволяет проводить ретроспективный анализ происходящего в системе с гибким назначением интервалов времени, типов событий. Может использовать шаблоны типовых отчетов, созданные пользователем (оператором).

Специальные инструменты

К специальным инструментам на текущий момент относятся :

- Редактор организаций[317]. Используется только в профессиональной многоорганизационной версии системы.
- Редактор системных настроек[341] . Необходим для обновления ключа защиты (ваших лицензий), для управления резервным копированием и настройки новых категорий транзакций.
- Редактор заданий[321]. Позволяет автоматизировать многие действия в системе, а также необходим для работы мини-консоли[394] .

Эти инструменты отдельно описаны в разделе Специальные средства[317] .

Лицензируемые модули также описаны в специальном разделе Дополнительные модули[417] . Там вы найдете информацию о следующих модулях:

- Редактор шаблонов[417] для печати карт;
- Модуль бюро пропусков[432];
- Модуль учета рабочего времени[456] ;
- Поправки к рабочему времени[462] ;
- Модуль видеоверификации[506];
- Интеграция с видеооборудованием[515] (в т.ч. с системами распознавания автомобильных номеров);
- Интеграция с системами ОПС[603];
- Интеграция с биометрическими устройствами ZKTeco и ЛКД[654] ;
- Распознавание документов[671] .

8.1 Редактор оборудования

Некоторые термины

Прежде, чем подключать оборудование, определим некоторые термины для системы.

Локальная работа. Соответствует одномашинной конфигурации, все аппаратные средства подключены к данному ПК и управление системой производится тоже с этого ПК. Использование дополнительных рабочих станций невозможно (средства поддержки сети при запуске программы не загружаются). Такой режим характерен для конфигурации Lite.

Компьютер сервер. Данный ПК является сервером системы. Ключ защиты подключен именно к этому компьютеру. Возможно использование дополнительных рабочих станций.

Рабочая станция. Дополнительный ПК в системе с установленным ПО рабочей станции для подключения оборудования и/или организации дополнительного рабочего места оператора.

Канал. Оборудование может подключаться к ПК через COM-порт, через USB-вход, а также через сеть Ethernet. Для определения типа подключения введено логическое понятие "Канал". Через COM-порт поддерживается оборудование, подключаемое к ЦКС (CNC-08, CNC-16). USB каналы образуются подключенными к ПК интерфейсами NI-A01. Контроллеры с интерфейсом Ethernet подключаются через сетевой канал по протоколу UDP. Кроме того, для внешних подсистем (ОПС, видеонаблюдение) также автоматически создаются соответствующие каналы.

С версии 3.2 добавлен ***программный канал***, через который подключаются:

- Программный контроллер[187] SCL-02. Может использоваться, например, для организации автомобильных проходных.
- GSM-модем[398]. Позволяет рассылать уведомления о различных событиях посредством SMS-сообщений.
- e-mail клиент[409]. Позволяет рассылать уведомления о различных событиях по электронной почте.
- Контроллер[580] автомобильных номеров. Служит источником идентификаторов типа "Автомобильный номер".
- Мобильный терминал доступа[360].

После установки системы канал PROGRAM всегда существует, и на нем присутствует интерфейс мини-консоли. Остальные компоненты вы добавляете по мере необходимости.

Оборудование в систему может быть добавлено автоматически либо вручную. Соответствующие процедуры описаны в разделе Добавление устройств[64]. После добавления устройств можно перейти к более тонкой настройке доступных[69] или охранных[117] контроллеров, если это необходимо.

Независимо от способа добавления контроллеров, они автоматически добавляются в корень территории Система. В дальнейшем, если у вас иерархическая топология, вы можете сами перенести аппаратные ресурсы на требуемые территории.

Назначение редактора оборудования

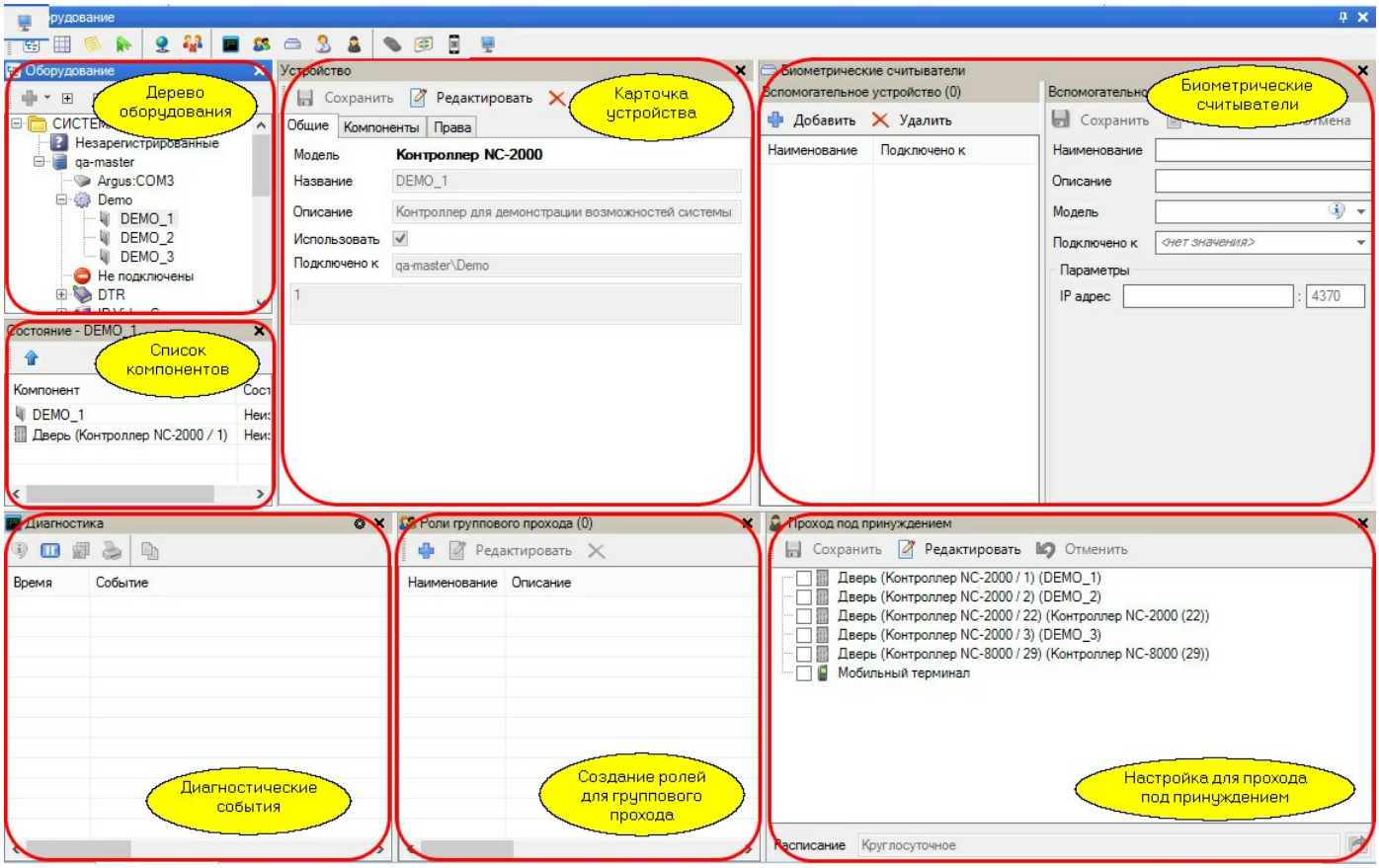
Редактор оборудования предназначен для включения в состав системы любого поддерживаемого оборудования: контроллеров, настольных считывателей, сетевых контроллеров, дополнительных рабочих станций. Напомним, что редактор оборудования доступен только в организации SYSTEM, устанавливаемой по-умолчанию.

Именно в данном редакторе можно настроить все параметры оборудования, задать режимы его работы, а также распределить подключенное оборудование по организациям, если их в системе несколько.

Как правило, доступ к редактору оборудования имеет установщик, служба технической эксплуатации или лицо, их заменяющее. В маленьких системах данную функцию может совмещать единственный оператор.

Панели редактора оборудования

Редактор оборудования имеет в своем составе следующие панели и инструменты:



Дерево оборудования показывает все имеющееся в системе оборудование: компьютеры, компьютерные каналы, контроллеры, настольные считыватели и так далее. Эта структура имеет прямое соответствие с физической структурой системы. Каждый компонент может входить в дерево системы только один раз, в отличие от топологии.

Список компонентов. Данная панель показывает компоненты, входящие в выбранную в дереве ветвь. Имеет вспомогательный характер, может наряду с деревом использоваться для навигации по оборудованию системы. При показе конкретного экземпляра оборудования (выбранного в дереве) отображает физический статус данной единицы оборудования.

Карточка устройства. Показывает свойства выбранной в данный момент единицы оборудования. Именно в карточке осуществляется редактирование всех настроек единицы оборудования, распределение оборудования по организациям. Вид карточки определяется типом выбранного на данный момент оборудования и будет различным для компьютера, контроллера, настольного считывателя.

Системные дополнительные поля. Диалог[155] создания полей для различных задач.

Настройка кластера. Настройки, позволяющие реализовать функцию многосерверности[164].

Группы АПБ и жесткого доступа. Панель настройки функции "Запрет двойного прохода[161] "и настройки групп жесткого доступа[163]

Панель диагностики. Представляет собой аналог панели событий монитора с предопределенным фильтром - сюда попадают только диагностические события оборудования[341] (например, выключение контроллера). Обеспечивает удобство настройки оборудования системы без открывания окна монитора событий.

Роли группового прохода. Панель настройки[115] для функции группового прохода.


Биометрические считыватели. Позволяет добавлять в систему и настраивать интегрированные биометрические устройства ZKTecko[654], Hikvision[663] и UniUbi[666].


Алкотестирование. Позволяет добавлять в систему и настраивать анализаторы[141] паров алкоголя в выдыхаемом воздухе.


Проход под принуждением. Панель настройки функции[160].


Настройки настольных считывателей[122].


Настройки работы с Mifare Plus. Настройки работы с картами Mifare Plus[125].


Настройки считывателей QR кодов Parsec[157].


Просмотр и завершение[159] работы подключенных к серверу рабочих станций.

Основные операции, выполняемые в редакторе оборудования

Добавление устройств[64] и их настройка
Настройка настольных считывателей[122]
Удаление или перемещение оборудования[150]
Временное отключение оборудования[149]

Специальные режимы прохода

В редакторе оборудования имеются дополнительные панели для расширенных настроек системы:

- Системные дополнительные поля[155];
- Роли группового прохода[115];
- Биометрические считыватели[654];
- Проход под принуждением[160];
- Запрет двойного прохода[161];
- Жесткий доступ[163].

8.1.1 Добавление устройств

Устройства системы (контроллеры доступа, охранные контроллеры, интерфейсы и настольные считыватели) могут добавляться в систему как автоматически, так и вручную. При автоматическом добавлении устройства всегда распределяются в корень топологии организации Система, но вы всегда при необходимости можете поменять их положение в Редакторе топологии.


Для добавления в систему оборудования необходимо зайти в систему с правами администратора. Оператор с данными правами автоматически создается при установке системы.

Автопоиск устройств

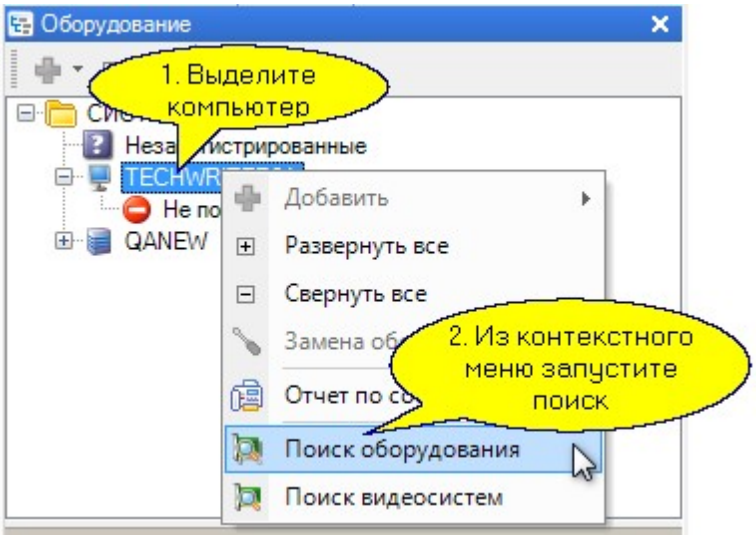
Автоматически система находит только каналы для подключения оборудования (к таковым относятся интерфейсы NI-A01, CNC-12/14, канал настольного считывателя, сетевой канал для контроллеров с Ethernet, программный канал, а также каналы интегрируемых сторонних систем).

Достаточно подключить, например, NI-A01 к вашему ПК, и в течение 10-15 секунд в дереве оборудования появится соответствующий канал.

Для обнаружения оборудования (или при неудачном автоматическом обнаружении) запустите поиск по всей станции (компьютеру) либо по нужному каналу.

Отметим, что если после окончания процедуры поиска вы подключите, например, еще один контроллер, то его потребуется либо вручную ввести в систему, либо принудительно запустить процесс поиска для вашего интерфейса.

Запуск процедуры поиска осуществляется с использованием контекстного меню (вызывается правой кнопкой мышки) при выборе компьютера, для которого необходимо произвести поиск, либо только для конкретного канала, как показано на рисунке ниже:



Также при поиске обнаруживаются контроллеры с Ethernet-интерфейсом при условии, что у них корректно настроены сетевые параметры (в том числе адрес компьютера, который будет выполнять для них роль сервера).

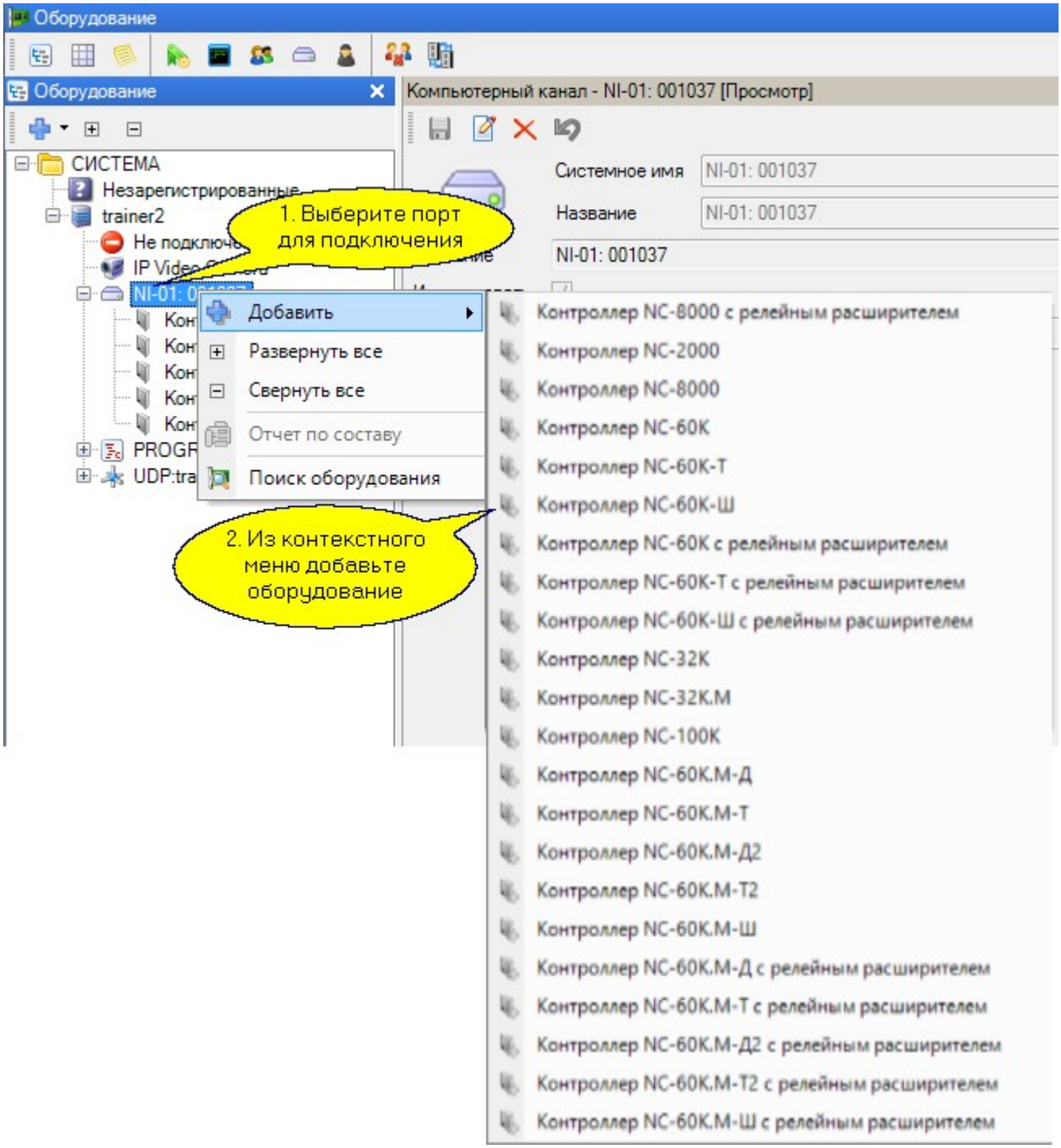
Поиск видеосистем используется для обнаружения внешних систем видеонаблюдения по IP-адресу.

Если в буфере транзакций контроллера есть неотправленные транзакции (например, после работы в режиме офф-лайн), то такой контроллер может не обнаружиться при сканировании. Его нужно будет добавить вручную.

Ручное подключение контроллеров

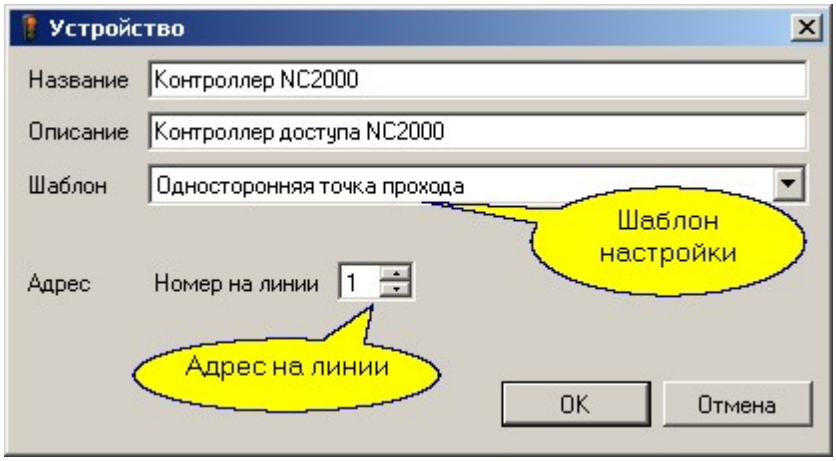
Ниже описано добавление контроллера доступа. Для ***охранного контроллера*** процесс добавления аналогичен с той разницей, что для него не требуется указывать шаблон, и все настройки нужно осуществлять в соответствии с его назначением и аппаратной конфигурацией (задействованные области охраны, распределение подключенных датчиков).

Выберите канал, к которому должен подключаться контроллер, и нажав правую кнопку мышки, либо через панель инструментов редактора (синий крестик) выберите из появившегося меню тип подключаемого контроллера, как показано ниже на рисунке:



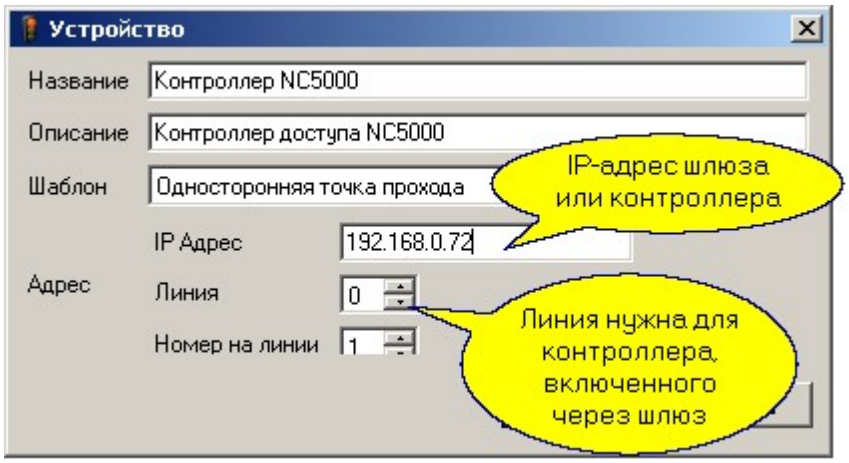
Обратите внимание, при добавлении контроллера NC-60K/NC-60K.M необходимо выбирать версию, соответствующую установленному в веб-интерфейсе контроллера типу точки прохода: для двери - NC-60K/NC-60K.M-Д, для турникета - NC-60K/NC-60K.M-T, для шлюза - NC-60K/NC-60K.M-Ш. Кроме этого, если к контроллеру подключаются две двери или два турникета, то следует выбирать соответственно NC-60K/NC-60K.M-Д2 и NC-60K/NC-60K.M-T2.

После выбора типа контроллера появится диалоговое окно, в котором необходимо установить самые общие параметры. Более тонкая настройка может быть произведена с помощью редактора оборудования позже. Например, если мы выберем из списка контроллер тип NC-32K.M, то диалог будет выглядеть следующим образом:



Назначение отдельных полей диалога следующее (конкретный набор полей зависит от типа порта, к которому подключается контроллер):

- *Название*. Данное поле задает название, под которым данная точка прохода будет фигурировать в системе. Выберите подходящее название длиной не более 32 символов. Это имя всегда будет соответствовать контроллеру в редакторе оборудования, при этом в топологии конкретной системы название контроллера может быть изменено.
- *Описание*. Это поле не является обязательным и служит как справочное для установщика или администратора системы.
- *Шаблон*. В этом поле выбирается типовая конфигурация контроллера, установленного на данной точке прохода. Шаблоны описывают типовые конфигурации точки прохода, которые вы в дальнейшем сможете скорректировать для более тонкой настройки контроллера.
- *IP адрес*. Поле присутствует у контроллеров с интерфейсом Ethernet. В данной строке вводится IP-адрес контроллера.
- *Линия*. В случае использования шлюза, в этом поле выбирается номер линии шлюза (значение от 1 до 4), к которой подключен данный контроллер. Если шлюз не используется, то значение обязательно установить в ноль.



- *Адрес*. В режиме редактирования дверного канала текущий адрес устанавливается в соответствии с адресом, установленным на программируемом контроллере. При добавлении нового контроллера это поле по-умолчанию устанавливается в 1. Вы можете установить любой незанятый адрес от 1 до 63.



Необходимо помнить, что у всех контроллеров, находящихся на одной линии связи, не должно быть одинаковых адресов.

После добавления, если выбрать устройство в дереве оборудования, станет доступна карточка устройства. Для контроллер, помимо перечисленных выше полей будут отображаться также следующие поля:

- *Использовать*. Включает или выключает опрос контроллера системой.
- *Подключено к.* Показывает, к какой рабочей станции подключено данное устройство.

Более тонкая настройка доступных[69] или охранных[117] контроллеров описана в соответствующих разделах. Кроме того, для подсистемы доступа возможна организация специальных режимов доступа: вход под принуждением, защита от двойного прохода (антипассбэк), жесткий доступ. Эти режимы описаны в разделе Дополнительные настройки[159].

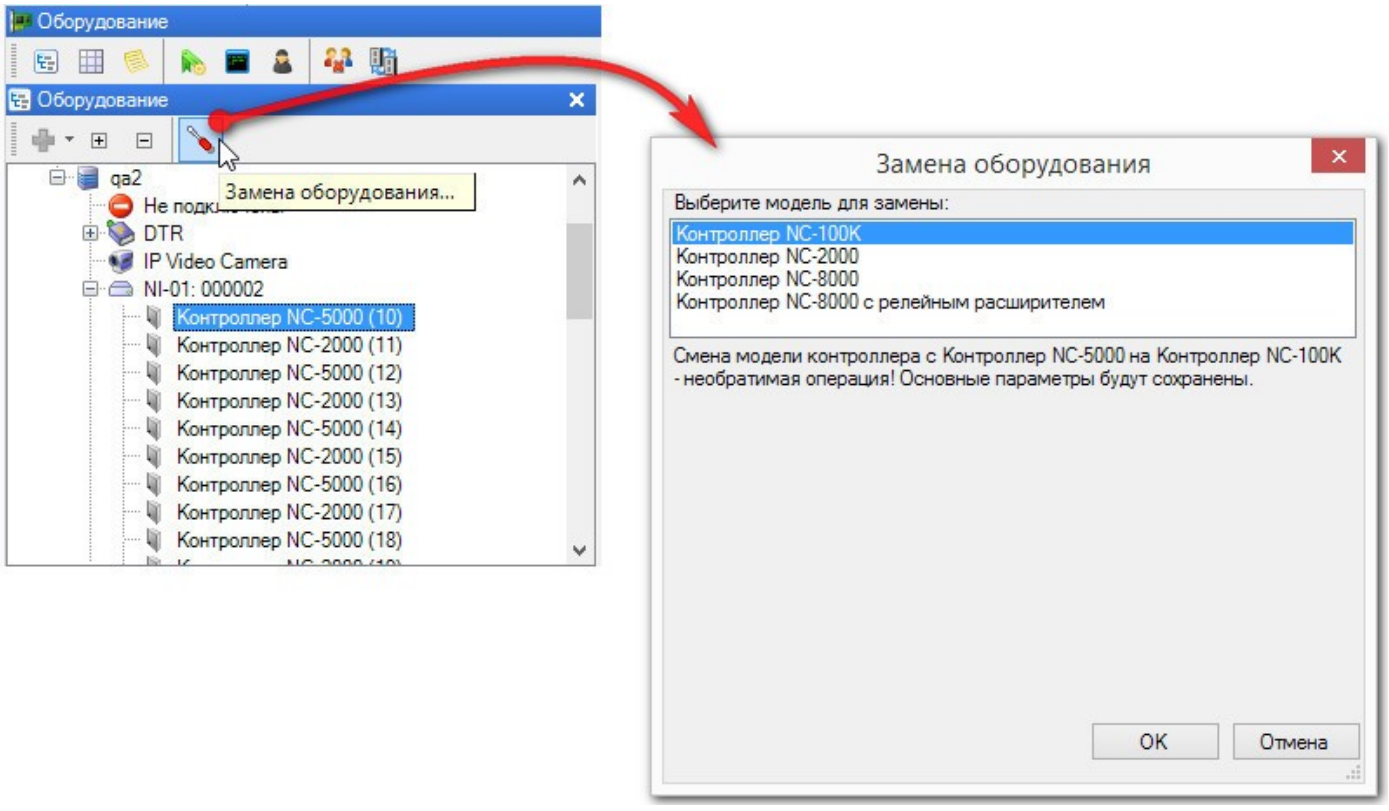
Биометрические терминалы добавляются[655] только вручную.

8.1.1.1 Замена оборудования

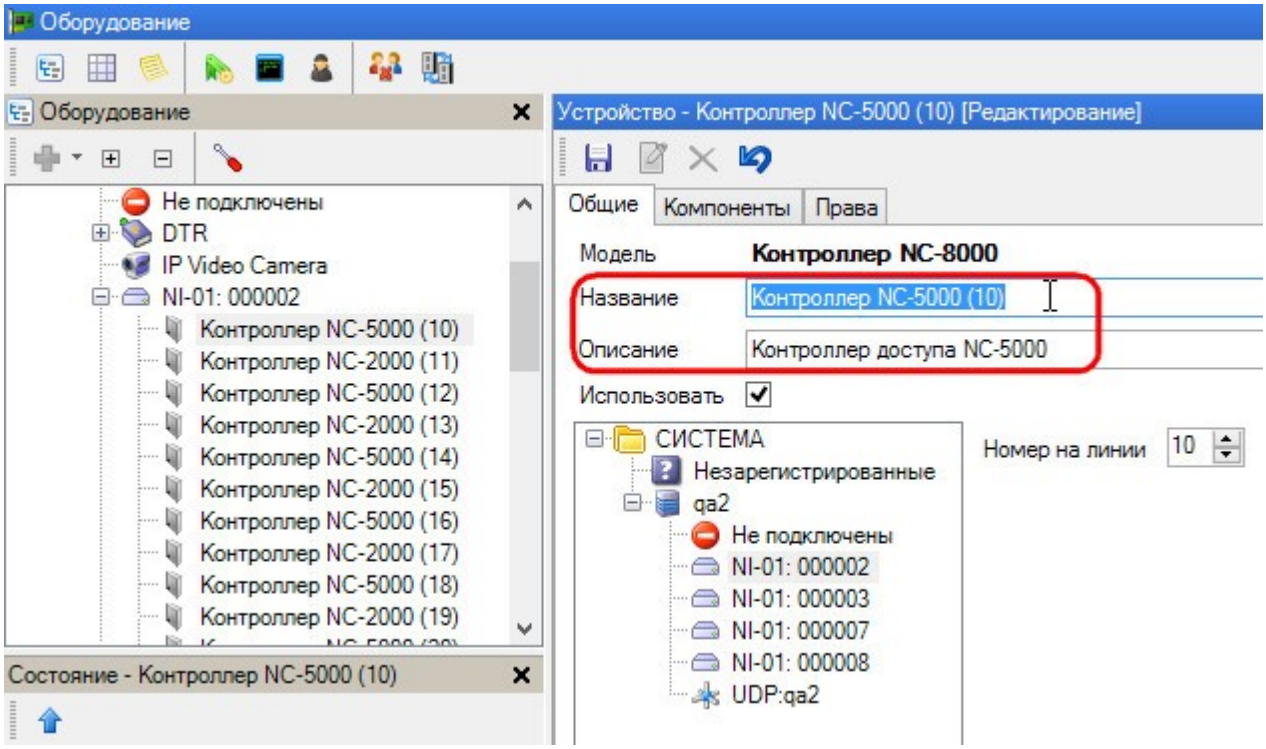
При замене контроллера доступа новой моделью можно удалить[150] из системы запись о старом контроллере, а затем добавить[64] новый. Однако можно воспользоваться функцией замены оборудования, которая позволит перенести настройки из старого в новый контроллер. Эта функция доступна для замены устройства более современной моделью и при смене типа точки прохода у контроллера NC-60K/NC-60K.M[85].

Чтобы заменить контроллер, выполните следующие шаги:

1. В редакторе оборудования выделите устройство, которое физически будет или было заменено, и нажмите на кнопку *Замена оборудования*:



2. В открывшемся окне выберите из списка доступных моделей нужную и нажмите на кнопку *ОК*;
3. При необходимости измените название и/или описание (либо какие-то иные параметры) контроллера в карточке оборудования, перейдя в режим редактирования.



4. По завершении настройки контроллера нажмите на кнопку (*Сохранить*).
5. После замены одного контроллера другим, новый контроллер необходимо инициализировать[298].

8.1.2 Настройка контроллеров доступа

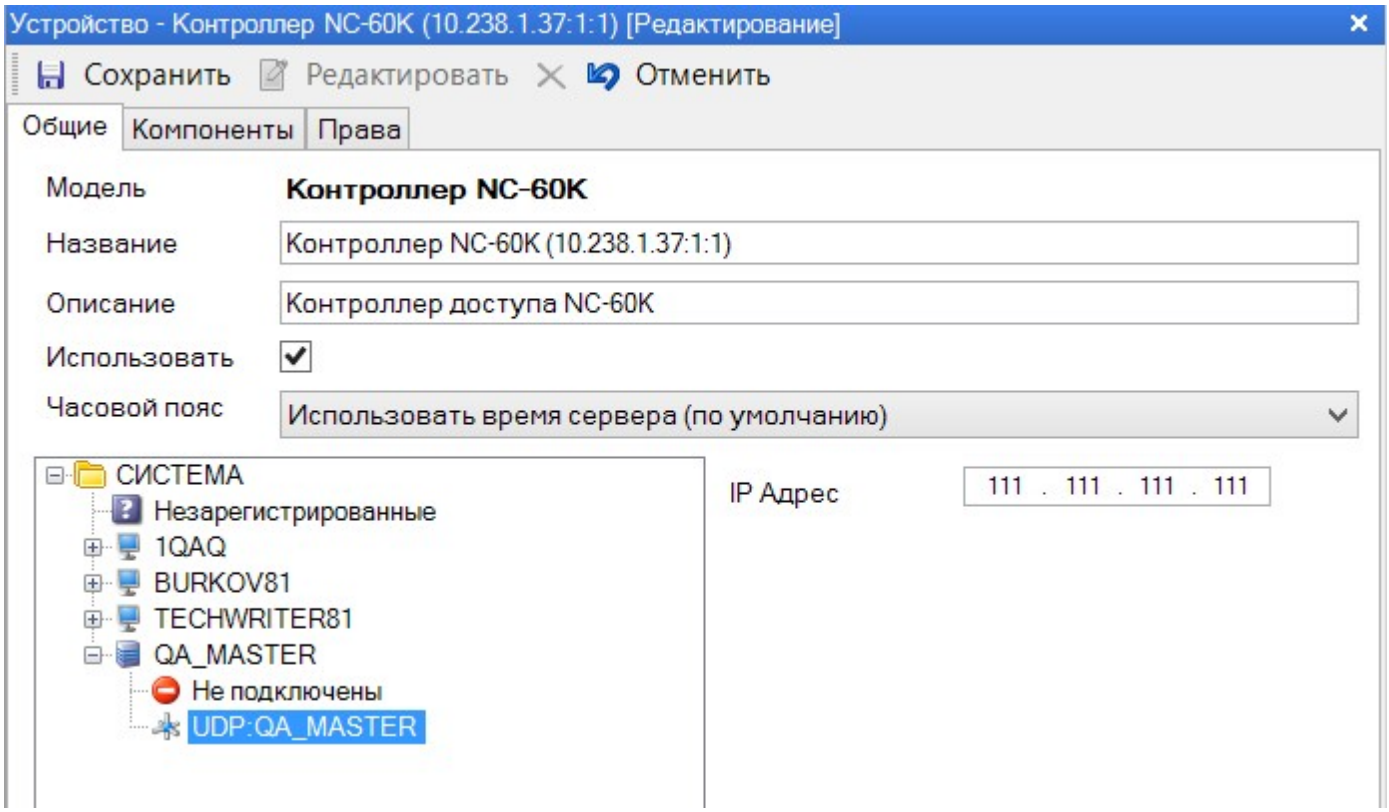
В разделе приведены описания настроек для контроллеров торговой марки Parsec. Одинаковые для всех контроллеров вкладки *Общее* и *Права* описаны в текущем разделе ниже. Отличающиеся настройки контроллеров, сгруппированные во вкладках *Компоненты*, описаны в соответствующих моделям контроллеров разделах:

- NC-2000[71] (сняты с производства. Также в этом разделе находится описание настроек снятых с производства контроллеров NC-1000/1000.M/5000);
- NC-8000[76] (всех моделей);
- лифтового контроллера NC-8000-E[84];
- NC-60K / NC-60K.M[85];
- NC-32K.M/32K-IP[95];
- NC-100K-IP[99];
- программного контроллера распознавания лиц[108].

Кроме этого, приведено описание дополнительных функций контроллеров:

- настройка дополнительного реле[112] всех основных контроллеров;
- настройка картоприемника[113] (для NC-32K, NC-60K/NC-60K.M и NC-100K);
- настройка прохода по 2 картам[115] (для NC-8000 и NC-60K/NC-60K.M).

Вкладка "Общие"



Параметр	Описание
Название	Автоматически генерируемое название устройства. Можно изменить на любое удобное.
Описание	Автоматически генерируемое описание устройства. Можно изменить на любое удобное.
Использовать	Включает или выключает опрос контроллера системой.
Часовой пояс	Из раскрывающегося списка можно выбрать часовой пояс, в котором расположен контроллер. После этого для событий в БД будут сохраняться как время по UTC, так и часовой пояс контроллера.
IP Адрес	IP адрес контроллера. Контроллеры NC-8000, NC-60K/NC-60K.M и NC-100K-IP имеют веб-интерфейс, доступ к которому осуществляется по адресу, отображенному этом поле (подробнее о веб-интерфейсе в Руководстве по эксплуатации соответствующего контроллера).

В дереве оборудования отображается канал сервера/дополнительной рабочей станции, к которому подключен контроллер.

Режим Wiegand 26

Функция данного флажка одинакова для всех контроллеров, поэтому приведена здесь. Он находится на вкладке *Компоненты* в нижней части слева. При его установке в контроллеры вместо стандартных четырехбайтовых кодов карт будут загружаться только три младших байта, поскольку в этом случае со считывателей в контроллер поступают также трехбайтовые коды.

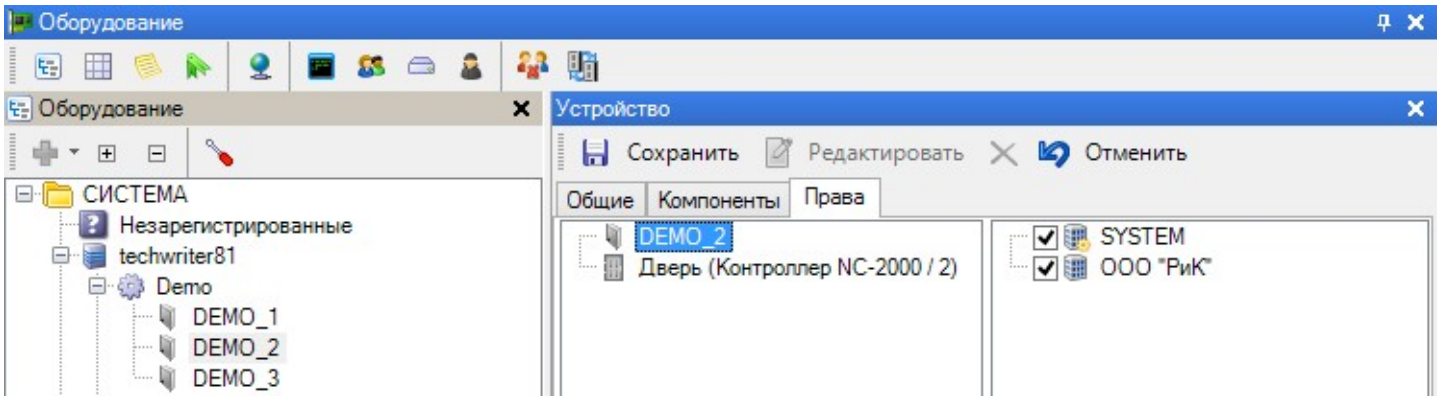
Как правило такой режим требуется в случае, если к контроллерам подключаются считыватели сторонних производителей через интерфейс NI-TW.

Если установить режим Wiegand 26 со считывателями серии PNR-xxx, подключенными по интерфейсу Touch Memory или Parsec, то система корректно работать не будет. Это относится и к контроллеру NC-100K-IP,

если у него основные считыватели серии PNR-xxx, независимо от того, что на картоприемнике будет стоять считыватель с интерфейсом Wiegand 26.

Вкладка "Права"

На этой вкладке необходимо указать, какие организации будут иметь доступ к настраиваемому контроллеру. Для этого выделите контроллер, перейдите в режим редактирования и на вкладке *Права* на правой панели поставьте флажки у нужных организаций. Операторы тех организаций, у которых не поставлены флажки, не смогут "видеть" этот контроллер в программе ParsecNET 3 и, соответственно, использовать его в своей топологии.

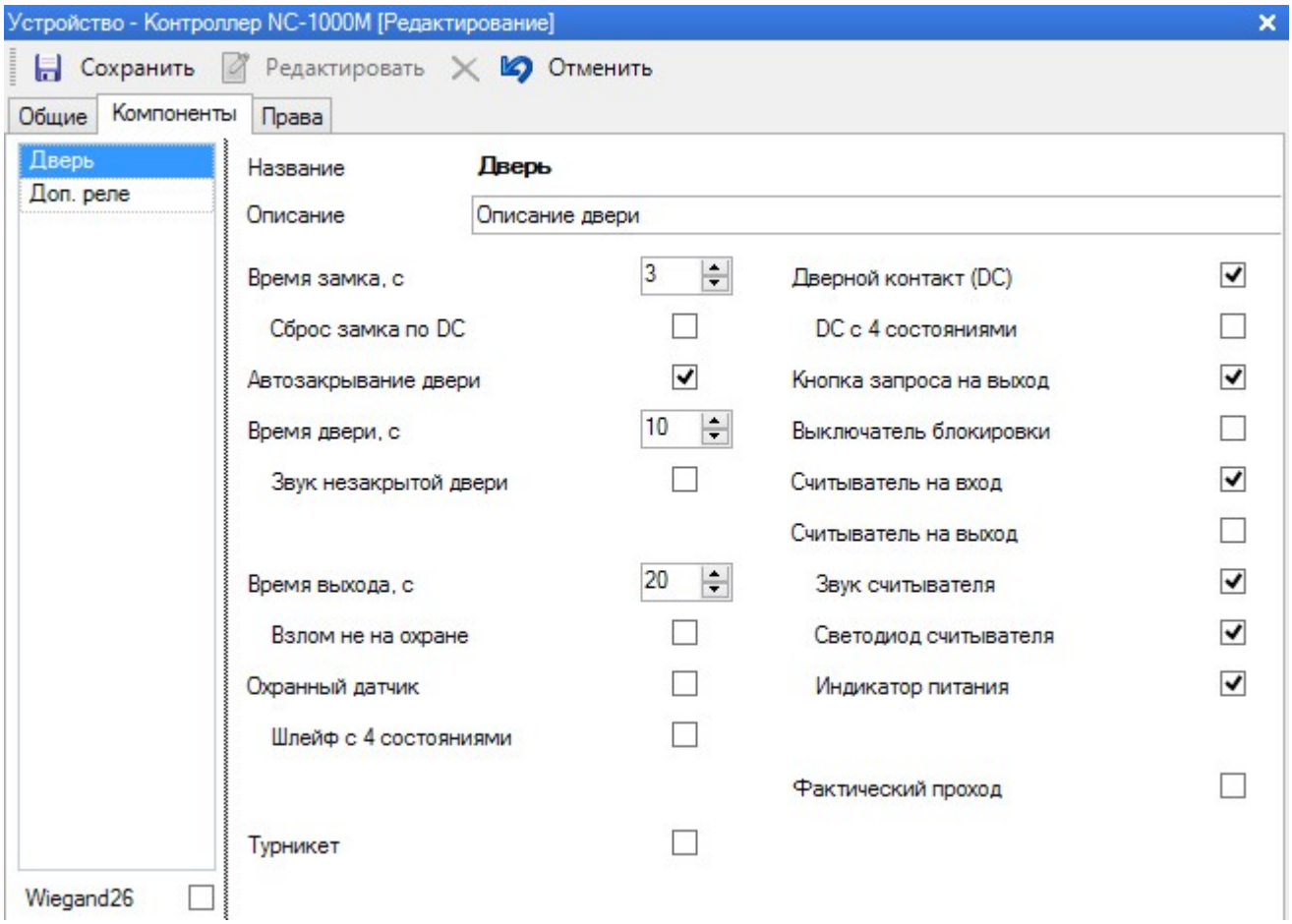


8.1.2.1 Настройки NC-2000

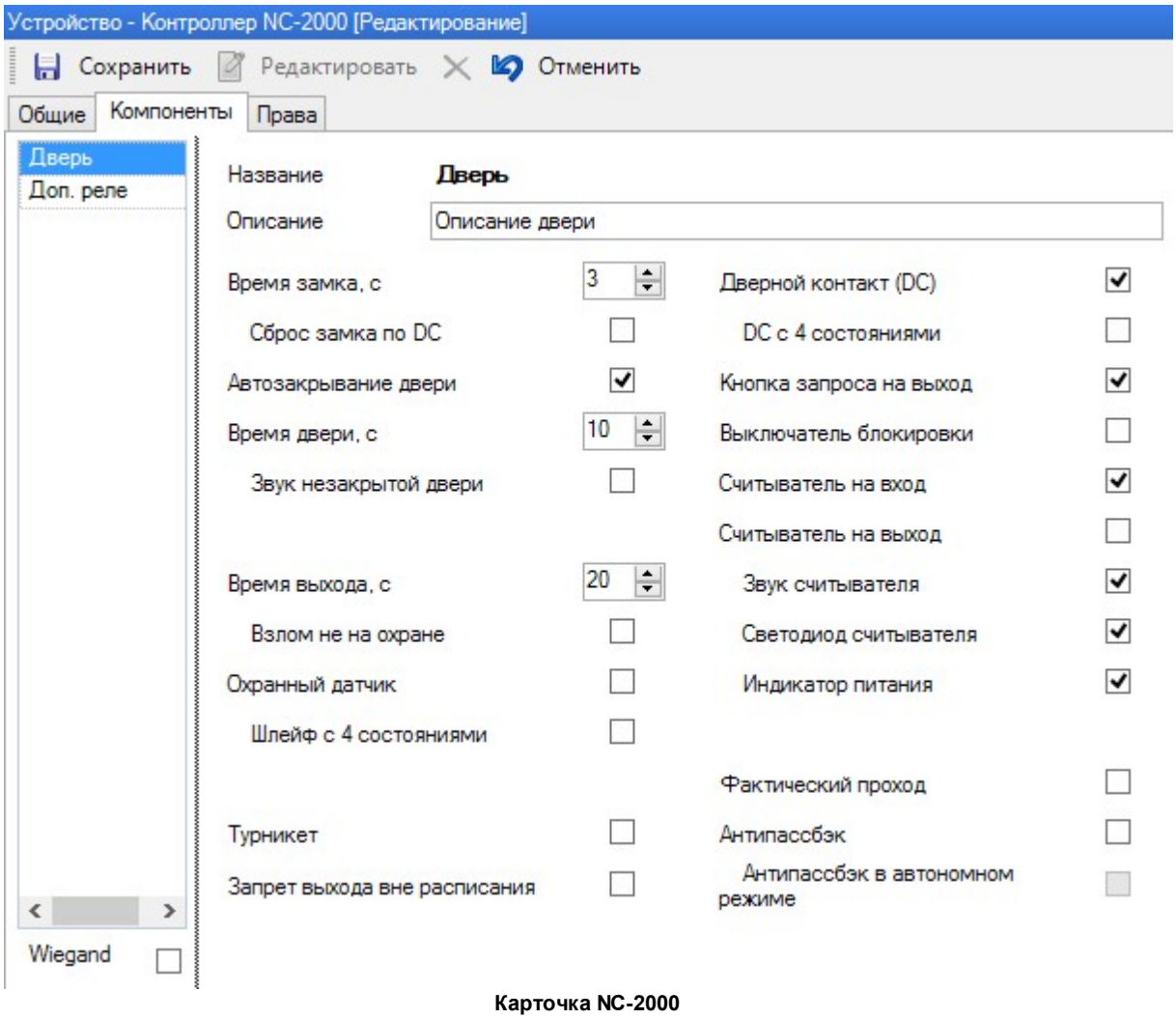
В данном разделе описаны настройки контроллера NC-2000, а также снятых с производства контроллеров NC-1000/1000.M/5000, имеющих минимальные отличия в параметрах настройки. Все настройки этих контроллеров отображаются на вкладке *Компоненты.* Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].

Переключение доступных типов точек прохода производится в карточках контроллеров флажком "Турникет". Контроллеры поддерживают точки прохода типов "Дверь" и "Турникет". Текущий тип точки прохода отображается на левой панели. При переключении на работу с турникетом настройки дополнительного реле становятся недоступными.

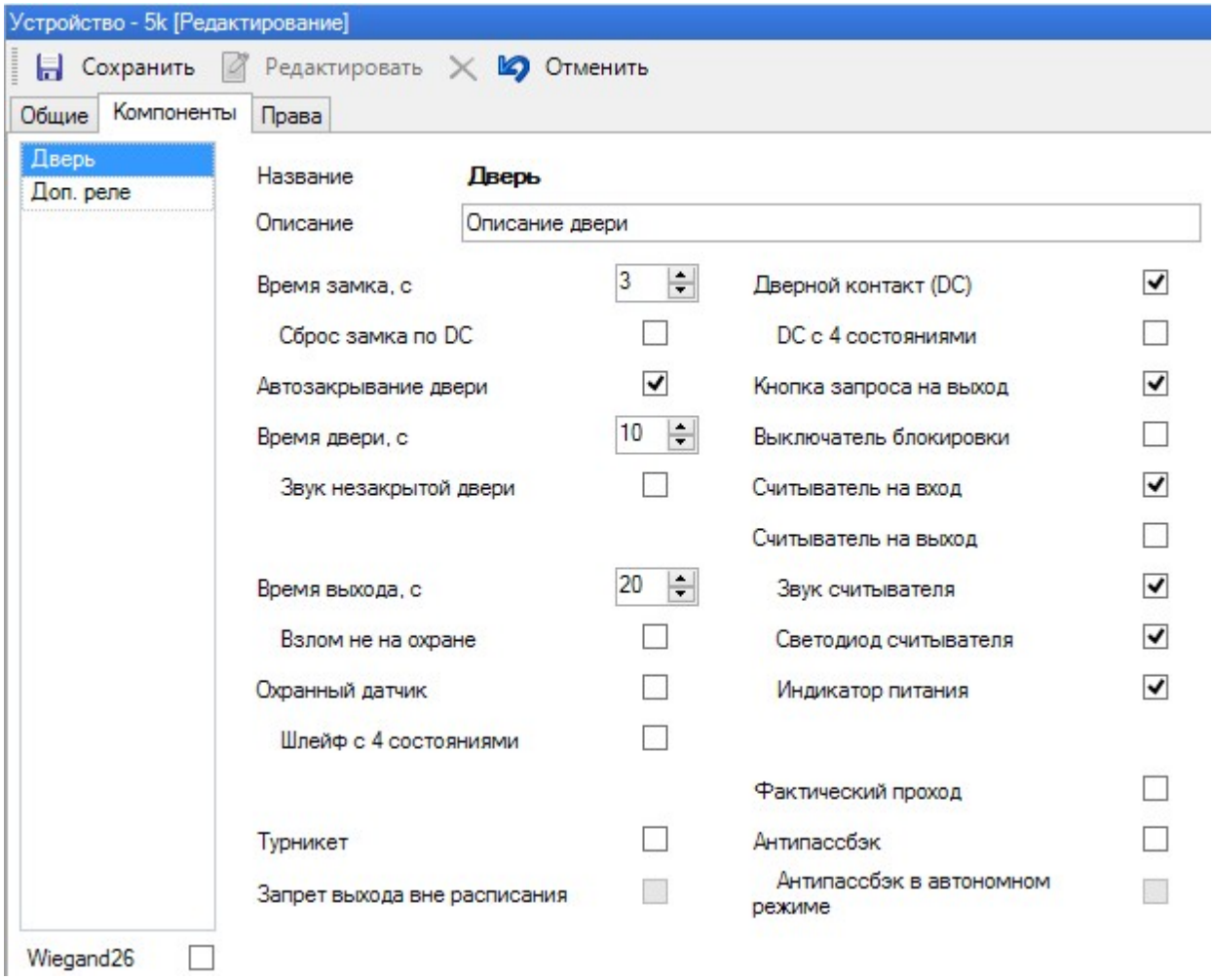
Изображения карточек устройств ниже интерактивны: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх.



Карточка NC-1000.M



Карточка NC-2000



Карточка NC-5000

Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов). Параметр доступен при установленном флажке *Считыватель на вход* или *Считыватель на выход,* либо обоих одновременно. Данный параметр недоступен для контроллеров NC-1000/1000M.
Антипассбэк в автономном режиме	Данный параметр доступен при установленных флажках *Считыватель на вход* и *Считыватель на выход*. Этот параметр определяет, будет ли работать режим локального антипассбэка для данной точки в случае отсутствия связи между контроллером и ПК. Для точки прохода, не включенной ни в одну область, этот параметр имеет смысл включать всегда, так как отслеживается многократный проход только через эту точку прохода. Включать ли данный параметр для точек прохода, входящих в состав областей антипассбэка, – зависит от политики службы безопасности.

Взлом не на охране Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.

Считыватель на вход Данный параметр доступен для всех типов контроллеров, кроме контроллеров старых версий NC-1000, где внешний считыватель считается подключенным всегда. Начиная с версии NC1K08 у контроллера NC-1000 также доступен данный параметр. Наличие только внутреннего считывателя может понадобиться, например, в случае использования контроллера на выезде с парковки, где внешний считыватель на вход (въезд) не нужен.

Считыватель на выход Включается, если точка прохода двухсторонняя (оборудована двумя считывателями). Кнопка RTE при этом дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки.

Время выхода Это время, которое дается на успокоение датчиков внутри помещения при постановке его на охрану. Время начинает отсчитываться после замыкания дверного контакта (закрытия двери).

Время двери Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». При включенной звуковой индикации и включенной опции «Звук открытой двери» считыватель начинает подавать прерывистый звуковой сигнал, напоминая, что дверь необходимо закрыть.

Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.

Время замка Это время в секундах, в течение которого подается управляющий сигнал на контакты замка для его открывания. Рекомендуется для электромеханических замков устанавливать 1 секунду, для электромеханических защелок от 3 до 5 секунд, для электромагнитных замков от 5 до 10 секунд, для турникетов - от 0 до 3 секунд (в зависимости от типа турникета). Например, для турникетов фирмы PERCo, не отрабатывающих снятие сигнала управления, следует устанавливать 0 секунд (что реально соответствует времени в 0,4 секунды), поскольку при установке даже 1 секунды возможен последовательный проход двух человек.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Дверной контакт (DC) Включается, если точка прохода оборудована датчиком закрытого состояния точки прохода (например, геркон на двери или датчик проворота турникета). При установке дверного контакта имеется возможность отслеживать состояние двери в различных ситуациях (взлом двери, дверь оставлена открытой и так далее).

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Звук незакрытой двери Есть смысл включать только при наличии дверного контакта. При включенном состоянии, если дверь открыта больше суммы времени замка и времени открытой двери (см. выше), то считыватель начинает подавать прерывистый звуковой сигнал (при условии, что включена звуковая

сигнализация считывателя), напоминающий о том, что необходимо закрыть дверь.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход, то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

Сброс замка по DC Во включенном состоянии позволяет снять открывающий сигнал с замка по факту закрытия двери, до истечения времени замка. Работает только в том случае, если имеется дверной контакт.

Описание Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.

Охранный датчик Флажок устанавливается, если к контроллеру доступа подключен охранный датчик, например, инфракрасный детектор движения, или любой другой.

Светодиод считывателя Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Турникет Данный параметр определяет тип точки прохода: дверь или турникет. При включении параметра для контроллеров NC-1000/NC-5000/NC-2000-IP изменения будут состоять в том, что в Мониторе событий появляется возможность не просто открыть точку прохода, но и выбрать, открывать ее на вход или на выход, что немаловажно при использовании турникетов. Если флажок *Автозакрывание* не будет установлен, то при открывании турникета с ПК команда на его закрытие не будет отсылаться автоматически по истечении времени замка и оператору придется посылать ее вручную.

Кроме этого, для контроллеров NC-1000/NC-5000/NC-2000-IP становится недоступным и управление параметрами дополнительного реле. У данных контроллеров в турникетном режиме дополнительное реле работает точно с такими же параметрами, как и замковое. То есть, при установке времени замка равным 3 секундам, дополнительное реле для открывания турникета на выход также будет срабатывать на 3 секунды.

Фактический проход При включении опции событие прохода генерируется не по предъявлению карты, а после последовательности событий предъявление карты + срабатывание дверного контакта. Целесообразно устанавливать в случае, если точка прохода не может быть преодолена без срабатывания датчика (например, датчик проворота «вертушки» на турникете). Это позволяет исключить обман системы путем «холостого» предъявления карты - рабочее время в таком случае засчитываться не будет.

Шлейф с 4 состояниями Переключает шлейфы охранного датчика в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание. Такой режим соответствует большей безопасности, однако, требует включения на шлейфах дополнительных резисторов (более подробно о подключении смотрите в руководстве по контроллеру).

DC с 4 состояниями Переключает шлейфы дверного контакта в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание. Такой режим

соответствует большей безопасности, однако, требует включения на шлейфах дополнительных резисторов (более подробно о подключении смотрите в руководстве по контроллеру).

Wiegand 26 Включение режима Wiegand 26[70].

8.1.2.2 Настройки контроллеров семейства NC-8000

В данном подразделе описаны настройки контроллеров семейства NC-8000: NC-8000, NC-8000-D и NC-8000-I. Раздел содержит описание вкладки *Компоненты*:

- Основные настройки;
- Режимы проходов[80];
- Дополнительные функции[83];
- описание настройки контроллера[113] с релейным расширителем NMO-04.

Лифтовый контроллер, созданный на базе NC-8000, имеет значительные отличия и описан в отдельном разделе[84].

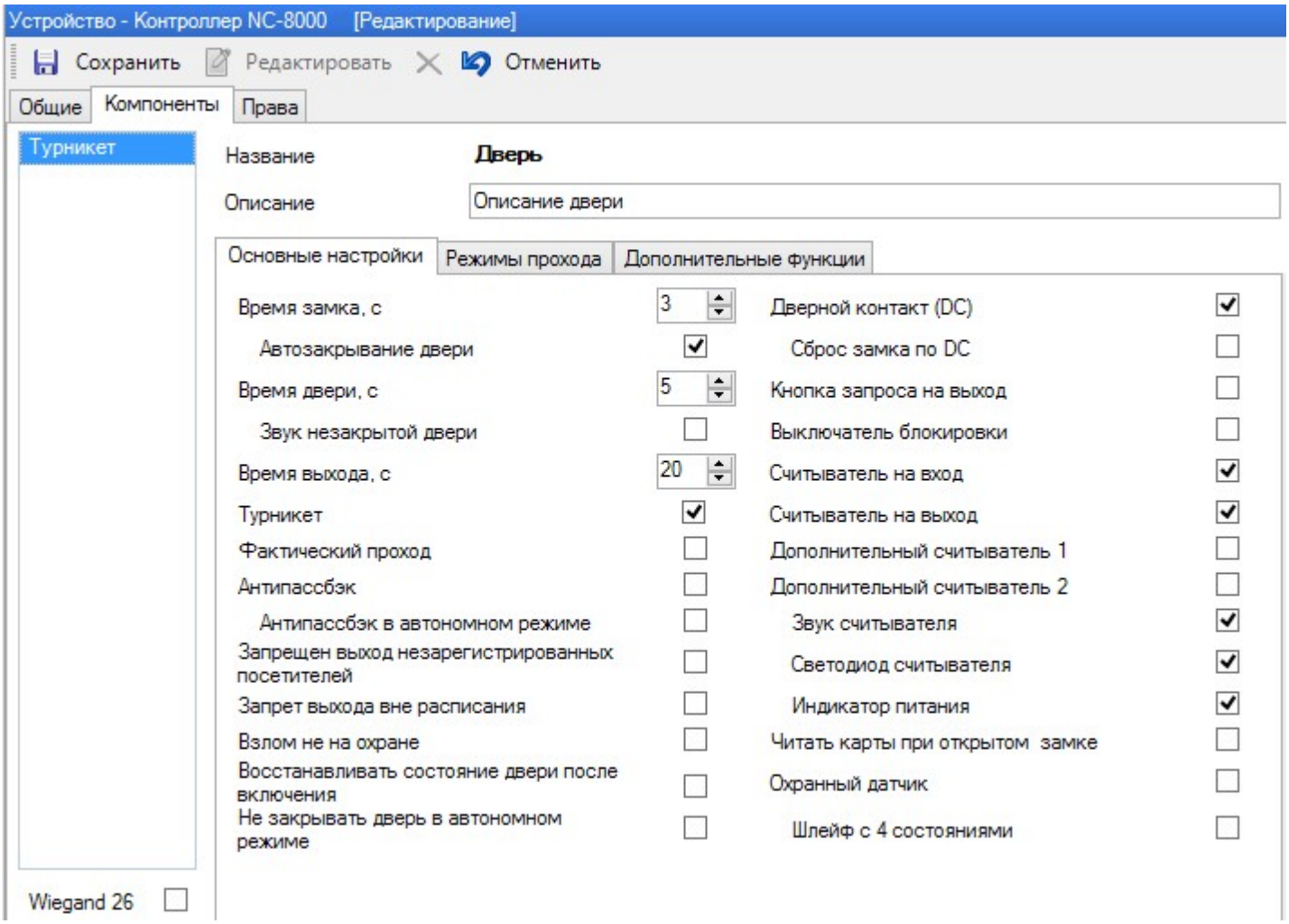
Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].

Переключение доступных типов точек прохода производится в карточке контроллера флажком "Турникет". Контроллер поддерживает точки прохода типов "Дверь" и "Турникет".

Текущий тип точки прохода отображается на левой панели вкладки "Основные настройки".

Изображения карточек устройств ниже интерактивны: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх.

Вкладка "Основные настройки"



Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов). Параметр доступен при установленном флажке *Считыватель на вход* или *Считыватель на выход,* либо обоих одновременно.
Антипассбэк в автономном режиме	Данный параметр доступен при установленных флажках *Считыватель на вход* и *Считыватель на выход*. Этот параметр определяет, будет ли работать режим локального антипассбэк-а для данной точки в случае отсутствия связи между контроллером и ПК. Для точки прохода, не включенной ни в одну область, этот параметр имеет смысл включать всегда, так как отслеживается многократный проход только через эту точку прохода. Включать ли данный параметр для точек прохода, входящих в состав областей антипассбэк-а, – зависит от политики службы безопасности.
Взлом не на охране	Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.
Восстанавливать состояние двери после включения	После восстановления питания контроллера восстанавливаются следующие состояния точки прохода: • открытая дверь, если до потери питания она была открыта: - с ПК; - кнопкой аварийного выхода. • состояние охраны.
Время выхода	Это время, которое дается на успокоение датчиков внутри помещения при постановке его на охрану. Время начинает отсчитываться после замыкания дверного контакта (закрытия двери).
Время двери	Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». При включенной звуковой индикации и включенной опции «Звук открытой двери» считыватель начинает подавать прерывистый звуковой сигнал, напоминая, что дверь необходимо закрыть. ***Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.***
Время замка	Это время в секундах, в течение которого подается управляющий сигнал на контакты замка для его открывания. Рекомендуется для электромеханических замков устанавливать 1 секунду, для электромеханических защелок от 3 до 5 секунд, для электромагнитных замков от 5 до 10 секунд, для турникетов - от 0 до 3 секунд (в зависимости от типа турникета). Например, для турникетов фирмы PERCo, не отрабатывающих снятие сигнала управления, следует устанавливать 0

секунд (что реально соответствует времени в 0,4 секунды), поскольку при установке даже 1 секунды возможен последовательный проход двух человек.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Дверной контакт (DC) Включается, если точка прохода оборудована датчиком закрытого состояния точки прохода (например, геркон на двери или датчик проворота турникета). При установке дверного контакта имеется возможность отслеживать состояние двери в различных ситуациях (взлом двери, дверь оставлена открытой и так далее)..

Дополнительный считыватель 1 Включает внешний дополнительный считыватель (адрес 0), который используется как источник дополнительного идентификатора при двухфакторной идентификации пользователя. При установленном флажке считыватель будет опрашиваться системой. Перемычка XJ2 на плате контроллера должна находиться в правом положении. Считыватель подключается к каналу READER 2 на плате контроллера.

Дополнительный считыватель 2 Включает внутренний дополнительный считыватель (адрес 1), который используется как источник дополнительного идентификатора при двухфакторной идентификации пользователя. При установленном флажке считыватель будет опрашиваться системой. Перемычка XJ2 на плате контроллера должна находиться в правом положении. Считыватель подключается к каналу READER 2 на плате контроллера.

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Запрещен выход незарегистрированных посетителей Только для карты с привилегией[250] "Гостевая карта". Если флажок установлен, то субъект доступа с привилегией "Гостевая карта" сможет выйти только через ту точку прохода, через которую вошел. Контроллеры других точек прохода не позволят ему выйти.

Звук незакрытой двери Есть смысл включать только при наличии дверного контакта. При включенном состоянии, если дверь открыта больше суммы времени замка и времени открытой двери (см. выше), то считыватель начинает подавать прерывистый звуковой сигнал (при условии, что включена звуковая сигнализация считывателя), напоминающий о том, что необходимо закрыть дверь.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

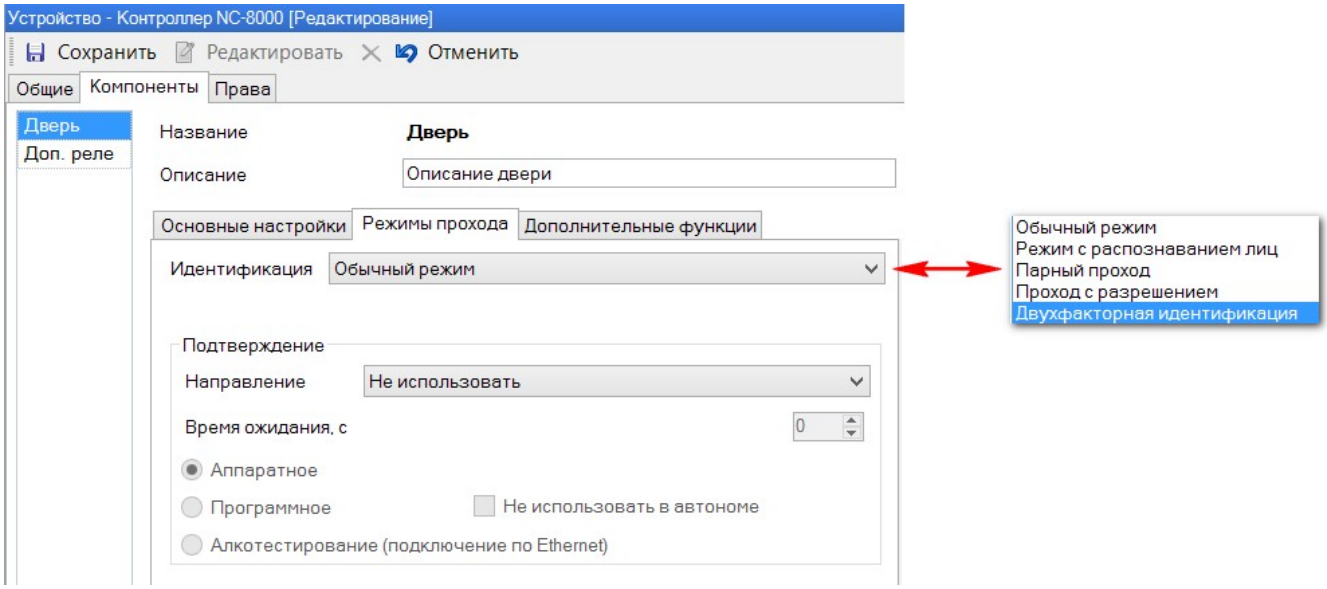
Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход, то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

Сброс замка по DC Во включенном состоянии позволяет снять открывающий сигнал с замка по факту закрытия двери, до истечения времени замка. Работает только в том случае, если имеется дверной контакт.

Не закрывать в автономном режиме	Если дверь открыта с ПК (из Монитор событий) и контроллер в это время теряет связь с сервером, то: • при установленном флажке замок остается открытым; • при снятом флажке замок закрывается.
Описание	Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.
Охранный датчик	Флажок устанавливается, если к контроллеру доступа подключен охранный датчик, например, инфракрасный детектор движения, или любой другой.
Светодиод считывателя	Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).
Считыватель на вход	Наличие только внутреннего считывателя может понадобиться, например, в случае использования контроллера на выезде с парковки, где внешний считыватель на вход (въезд) не нужен. Считыватель подключается к каналу READER 1 на плате контроллера.
Считыватель на выход	Включается, если точка прохода двухсторонняя (оборудована двумя считывателями). Кнопка RTE на двусторонней точке прохода дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки. Считыватель подключается к каналу READER 1 на плате контроллера.
Турникет	Данный параметр определяет тип точки прохода: дверь или турникет. При включении параметра в Мониторе событий появляется возможность не просто открыть точку прохода, но и выбрать, открывать ее на вход или на выход, что немаловажно при использовании турникетов. Если флажок *Автозакрывание* не будет установлен, то при открывании турникета с ПК команда на его закрытие не будет отсылаться автоматически по истечении времени замка и оператору придется посылать ее вручную. При установленном флажке становится недоступным управление параметрами дополнительного реле. У данных контроллеров в турникетном режиме дополнительное реле работает точно с такими же параметрами, как и замковое. То есть, при установке времени замка равным 3 секундам, дополнительное реле для открывания турникета на выход также будет срабатывать на 3 секунды.
Фактический проход	При включении опции событие прохода генерируется не по предъявлению карты, а после последовательности событий предъявление карты + срабатывание дверного контакта. Целесообразно устанавливать в случае, если точка прохода не может быть преодолена без срабатывания датчика (например, датчик проворота «вертушки» на турникете). Это позволяет исключить обман системы путем «холостого» предъявления карты - рабочее время в таком случае засчитываться не будет.
Читать карты при открытом замке	При установке флажка контроллер принимает коды карт от считывателя в течение "времени замка". При снятом флажке контроллер не принимает коды карт, пока на реле замка подается управляющий сигнал. **Будьте внимательны**!
Шлейф с 4 состояниями	Переключает шлейфы охранного датчика в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание. Такой режим соответствует большей безопасности, однако, требует включения на шлейфах дополнительных резисторов (более подробно о подключении смотрите в руководстве по эксплуатации контроллера).
Wiegand 26	Включение режима Wiegand 26 70.

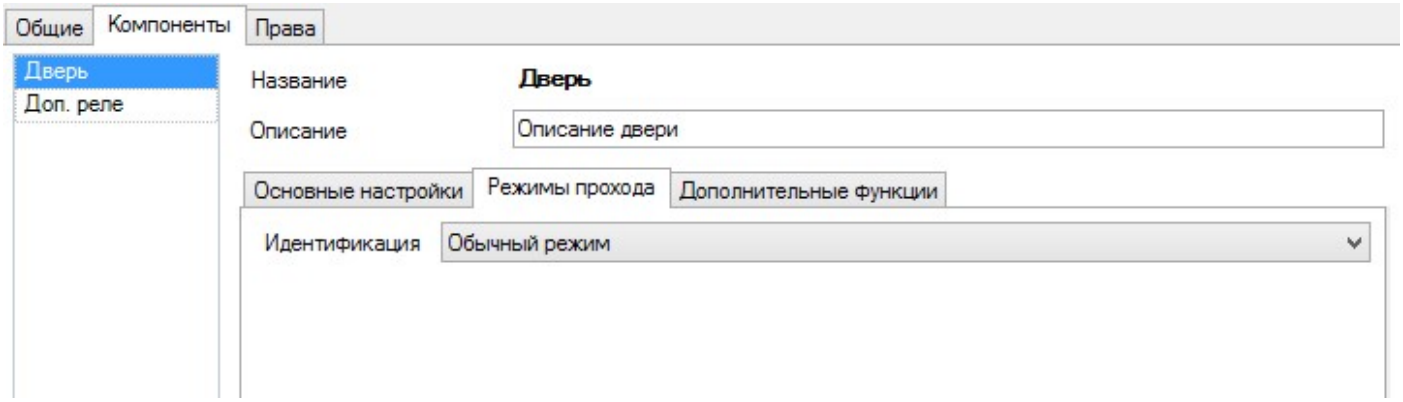
Вкладка "Режимы прохода"

Вкладка позволяет выбрать вариант прохода через точку доступа и настроить его.

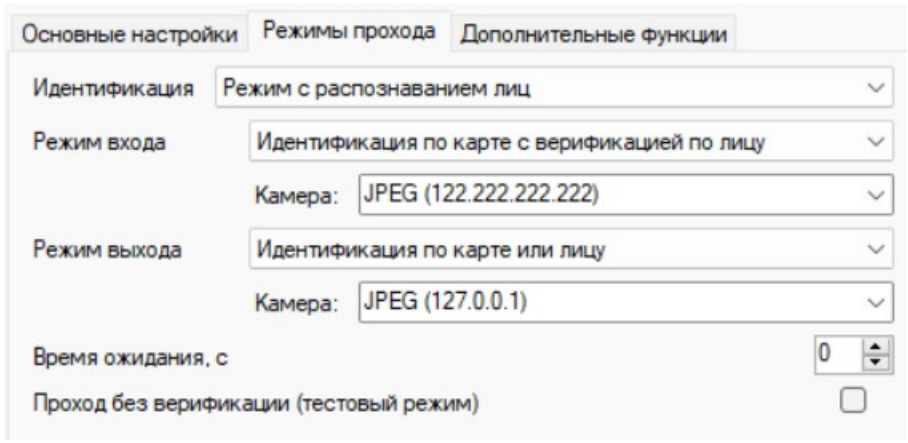


Контроллеры семейства NC-8000 поддерживают следующие режимы прохода:

1. "Обычный режим" - проход только по карте, ПИН-коду или карте с набором ПИН-кода, в зависимости от настроек считывателей:



2. "Режим распознавания лиц" позволяет выбрать разные варианты идентификации пользователя с использованием систем распознавания лиц:



В раскрывающихся списках *Режим входа* и *Режим выхода* выбираются способы, которыми будет осуществляться идентификация пользователя:

- "Идентификация по карте" - субъект доступа идентифицируется по предъявленной карте;

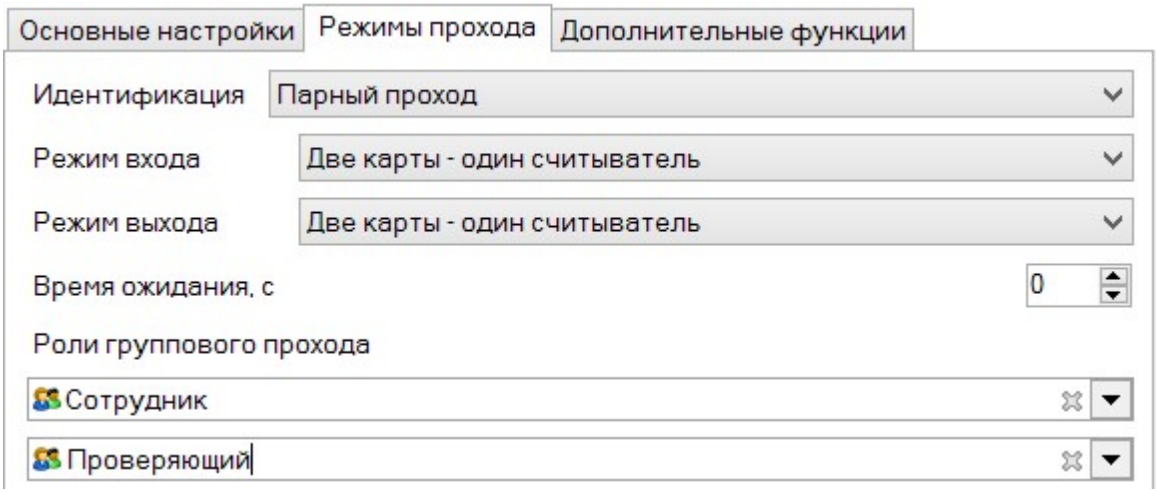
- "Идентификация по лицу" - субъект доступа идентифицируется, если его лицо соответствует фото в БД системы распознавания лиц (СРЛ);
- "Идентификация по карте или лицу" - субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты;
- "Идентификация по карте с верификацией по лицу" - субъект доступа идентифицируется совместно и по коду карты, и по лицу. Полное время сессии распознания субъекта доступа начинается с момента поднесения карты к считывателю и должна завершиться до истечения времени, заданном в поле *Время ожидания.*

Камера - из раскрывающегося списка необходимо выбрать камеру, с которой работает задействованная СРЛ.

Время ожидания, с - время с момента когда контроллер подтвердил право прохода карты, до момента открытия двери. Включает в себя сканирование лица, поиск соответствия ему в БД СРЛ и получение сигнала на открытие двери.

Проход без верификации (тестовый режим) - субъект идентифицируется по коду карты, даже если лицо не будет совпадать с фото в БД СРЛ. Если субъект идентифицирован и СКУД разрешает доступ, то дверь откроется только после истечения полного времени ожидания. Рекомендуется для использования на период отладки взаимодействия с СРЛ.

3. "Парный проход" и "Проход с разрешением" - режимы прохода, для которых требуется два пользователя. Используются в целях повышения безопасности доступа.
Настройки[115] для этих режимов одинаковые, но в случае парного прохода система включит обоих пользователей в списки антипассбэка, их обоих посчитает счетчик проходов и система сформирует сообщения о проходе двух пользователей. В случае прохода с подтверждением в системе будет учтен только первый приложивший карту пользователь. Если при этом на территорию (в помещение) зайдут оба, то возможны ошибки в работе, например, система посчитает, что из помещения вышли все и попытается поставить помещение на охрану. Но неучтенный пользователь в этом помещении вызовет тревогу.



В обоих этих режимах необходимо задать настройки для входа и выхода:

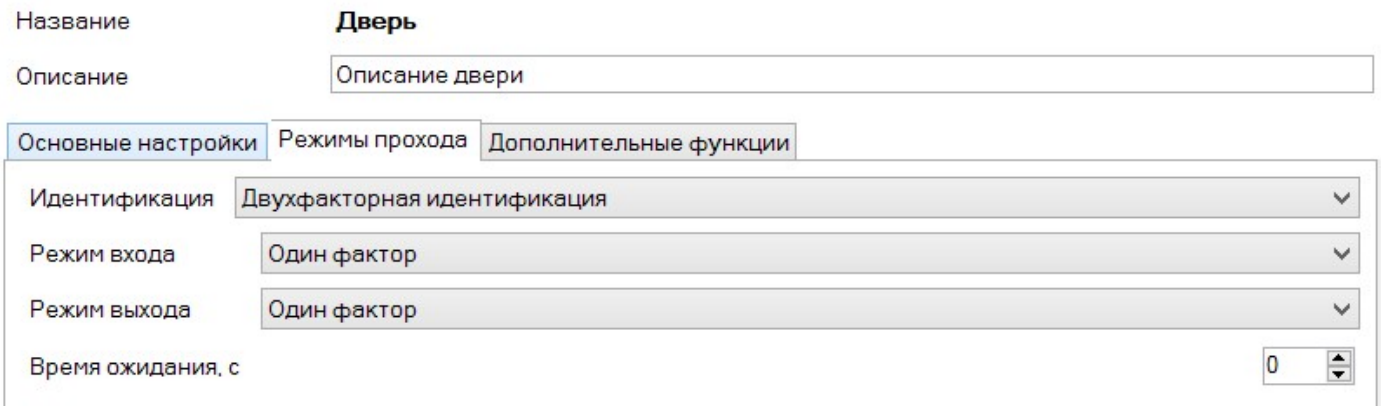
- *Не используется* - проход в этом направлении невозможен;
- *Две карты - один считыватель* - поднесение двух карт (с опциональным вводом ПИН-кода) к одному и тому же считывателю;
- *Две карты - разные считыватели* - поднесение двух карт (с опциональным вводом ПИН-кода) к двум разнесенным считывателям (чтобы не допустить поднесение двух карт одним человеком).

Время ожидания, с - максимальное время между поднесениями карт к считывателю(-ям);

Роли группового прохода - описание настроек приведено в разделе Настройка группового прохода[115].

4. "Двухфакторная идентификация" - режим может применяться, когда пользователи имеют несколько разных идентификаторов. Например, карта, отпечаток пальца, скан радужной

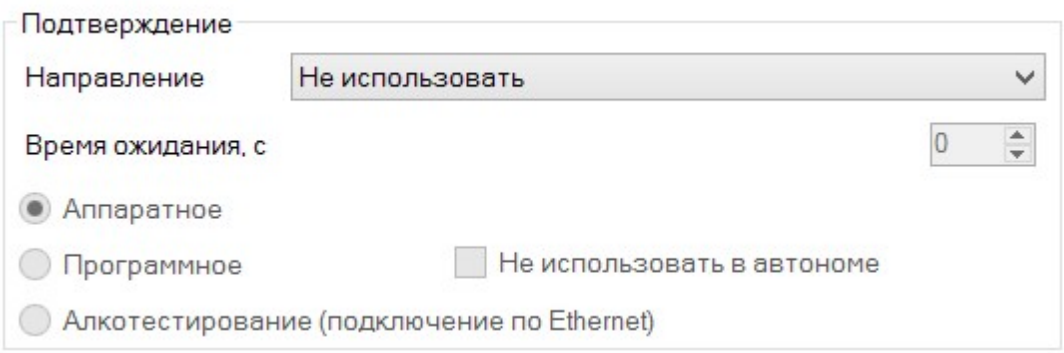
оболочки глаза, скан лица и т.п. При проходе в этом режиме необходимо будет предъявить выбранное количество разных идентификатора из числа тех, которые загружены в БД контроллера. Количество факторов идентификации выбирается отдельно для входа и для выхода: "Не используется", "Один фактор" или "Два фактора".



Время ожидания, с - максимальное время между предъявлением двух идентификаторов. Пример представлен в разделе[732].

Блок данных ***Подтверждение*** работает независимо от выбранных режимов прохода.

Использование подтверждения состоит в том, что после разрешения пользователю доступа в соответствии с выбранным режимом прохода система должна дополнительно получить подтверждающий сигнал, например, от весовой платформы или измерителя температуры.

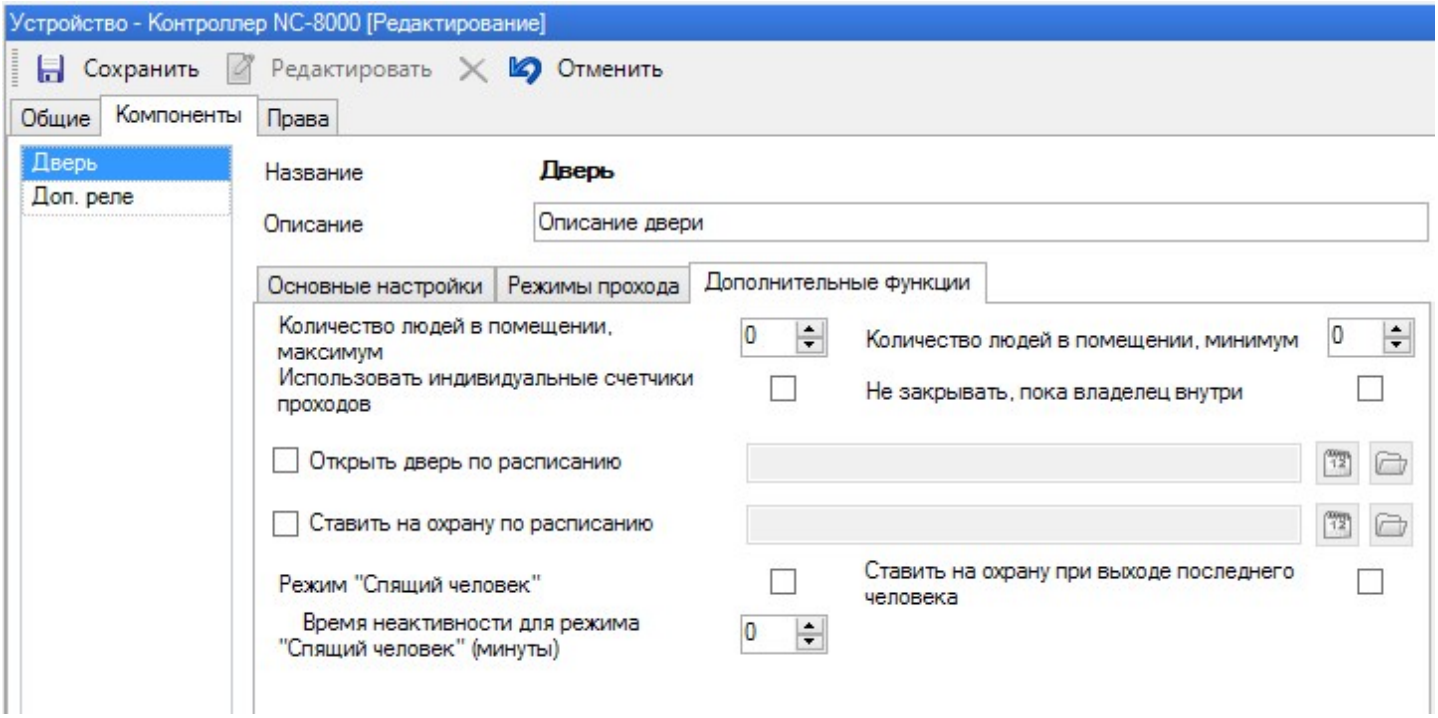


Элементы управления:

- *Направление* - подтверждающий сигнал будет необходим для выбранного из раскрывающегося списка направления прохода: "Не использовать", "Вход и выход", "Только вход", "Только выход";
- *Время ожидания, с* - в поле задается время в течение которого необходимо пройти дополнительную идентификацию для получения подтверждающего сигнала. В противном случае весь цикл идентификации субъекта доступа придется выполнить с самого начала.
- *Аппаратное* - флажок устанавливается в случае, когда сигнал подтверждения получается от какого-либо внешнего устройства, например, алкотестера или просто кнопки;
- *Программное* - флажок устанавливается, когда подтверждающий сигнал получается программным методом;
- *Не использовать в автономе* - установленный флажок отменяет необходимость подтверждающего сигнала, если контроллер точки прохода не имеет связи с сервером и работает в автономном режиме;
- *Алкотестирование (подключение по Ethernet)* - флажок устанавливается, когда алкотестер[141] подключен к Системе через Ethernet. При этом время ожидания показывает время ожидания контроллера от считывания кода идентификатора до получения кода от алкотестера.

Вкладка "Дополнительные функции"

Настройки это вкладки описаны в разделе Настройка контроллеров доступа[69]. Настройки картоприемника (поле Режим картоприемника и параметры ниже)



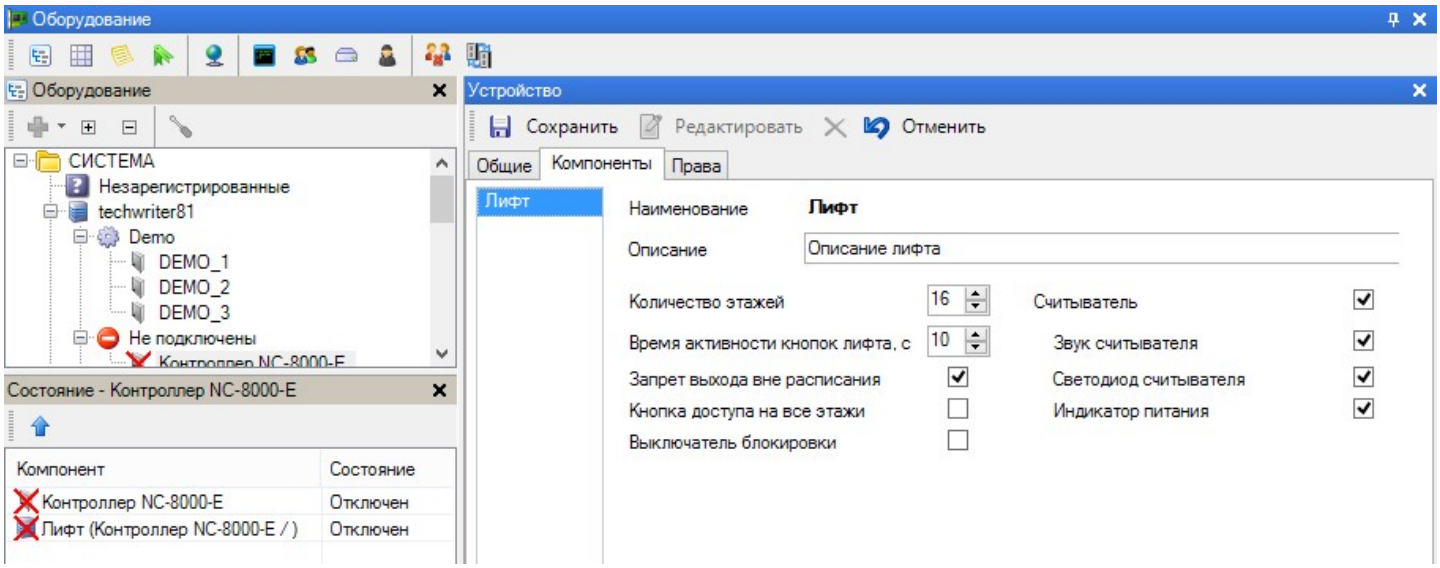
Параметр	Описание
ремя еакт ивност и для ежима "Спящий еловек" (минут ы)	Время, по истечении которого в режиме "Спящий человек" формируется транзакция "Тревога "Спящий человек".
спользоват ь ндивидуальные ет чики проходов	При установленном флажке контроллер постоянно ведет подсчет входов карт, у которых установлен лимит проходов (максимум 127). Недоступен при выборе режимах прохода "Парный проход" и "Проход с разрешением". Может отменяться привилегией "Не использовать счетчик проходов".
оличест во людей в омещении, аксимум	Количество сотрудников в помещении, при достижении которого вход сотрудников будет заблокирован.
оличест во людей в омещении, инимум	Количество сотрудников в помещении, при достижении которого выход сотрудников будет заблокирован.
е закрыват ь, пока аделец внут ри	*ежим дост упен т олько для двуст оронних т очек прохода* . Если в помещение вошел сотрудник с идентификатором, для которого установлен флажок *Владелец кабинет а* , то дверь остается открытой до его выхода. После выхода дверь переходит в обычный режим доступа. Поднесение к считывателю карт остальных пользователей в этот период порождает обычные транзакции входа/выхода (без управления замком). Если в помещение вошли несколько сотрудников с такой привилегией, то дверь перестанет быть постоянно открытой после первого выхода одного из них.
т крыт ь дверь по асписанию	Электрозамок двери открывается и закрывается по специально созданному расписанию, соответственно в начале и конце рабочего времени (периода разрешенного доступа).
ежим "Спящий еловек"	В данном режиме датчики отслеживают движение в помещении, в которое вошел сотрудник. При отсутствии движения в течение заданного времени формируется транзакция "Тревога "Спящий человек". После того, как

	тревожная транзакция сформирована, отсчет времени перезапускается в момент срабатывания датчика движения в этом помещении.
т авит ь на охрану о расписанию	Территория ставится на охрану по отдельно созданному расписанию доступа *вачале* рабочего времени (периода разрешенного доступа), снимается с охраны *вконце* периода рабочего времени. Т.е. начало рабочего времени этого "охранного расписания" должно совпадать с завершением рабочего времени того расписания, по которому ходят сотрудники.
т авит ь на охрану ри выходе оследнего еловека	При отсутствии людей в помещении, оно автоматически ставится на охрану, при условии, что время выхода больше времени замка. В противном случае, помещение на охрану не ставится.

8.1.2.3 Настройки лифтового контроллера NC-8000-E

Контроллер управления лифтом предназначен не для открытия двери, а для разблокировки кнопок лифта тех этажей, на которые у пользователя есть доступ.

Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].



Для настройки у лифтового контроллера кроме обычных доступны следующие особые параметры:

Параметр	Описание
Время активности кнопок лифта, с	После считывания идентификатора контроллер замкнет на указанное время контакты реле, к которым подключены кнопки лифта или иные исполнительные устройства. По истечении времени активности кнопки лифта станут неактивны и необходимо сново поднести идентификатор к считывателю.
Выключатель блокировки	Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.
Запрет выхода вне расписания	При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.
Звук считывателя	Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).
Индикатор питания	Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

Кнопка доступа на все этажи	Флажок устанавливается в случае, когда к контроллеру подключается кнопка, которая разблокирует все кнопки лифта.
Количество этажей	Указывается количество этажей, на которые контроллер обеспечивает доступ.
Описание	Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.
Светодиод считывателя	Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).
Считыватель	Снятие флажка выключает считыватель. Доступ будет возможен только по кнопке доступа на все этажи.

Кроме этих параметров, требуется дополнительная настройка групп доступа[249], включающих лифтовый контроллер.

8.1.2.4 Настройки NC-60K / NC-60K.M

В данном разделе описаны настройки контроллера NC-60K/NC-60K.M. Раздел содержит описание вкладок раздела *Компоненты*:

- Основные настройки;
- Режимы проходов[90];
- Дополнительные функции[94];
- описание настройки контроллера[113] с релейным расширителем NMO-04.

Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].

Контроллер поддерживает точки прохода типов "Дверь", "Турникет" и "Шлюз". При этом маркировка контроллеров в Редакторе оборудования будет, соответственно, NC-60K.M-Д, NC-60K.M-Т и NC-60K.M-Ш.

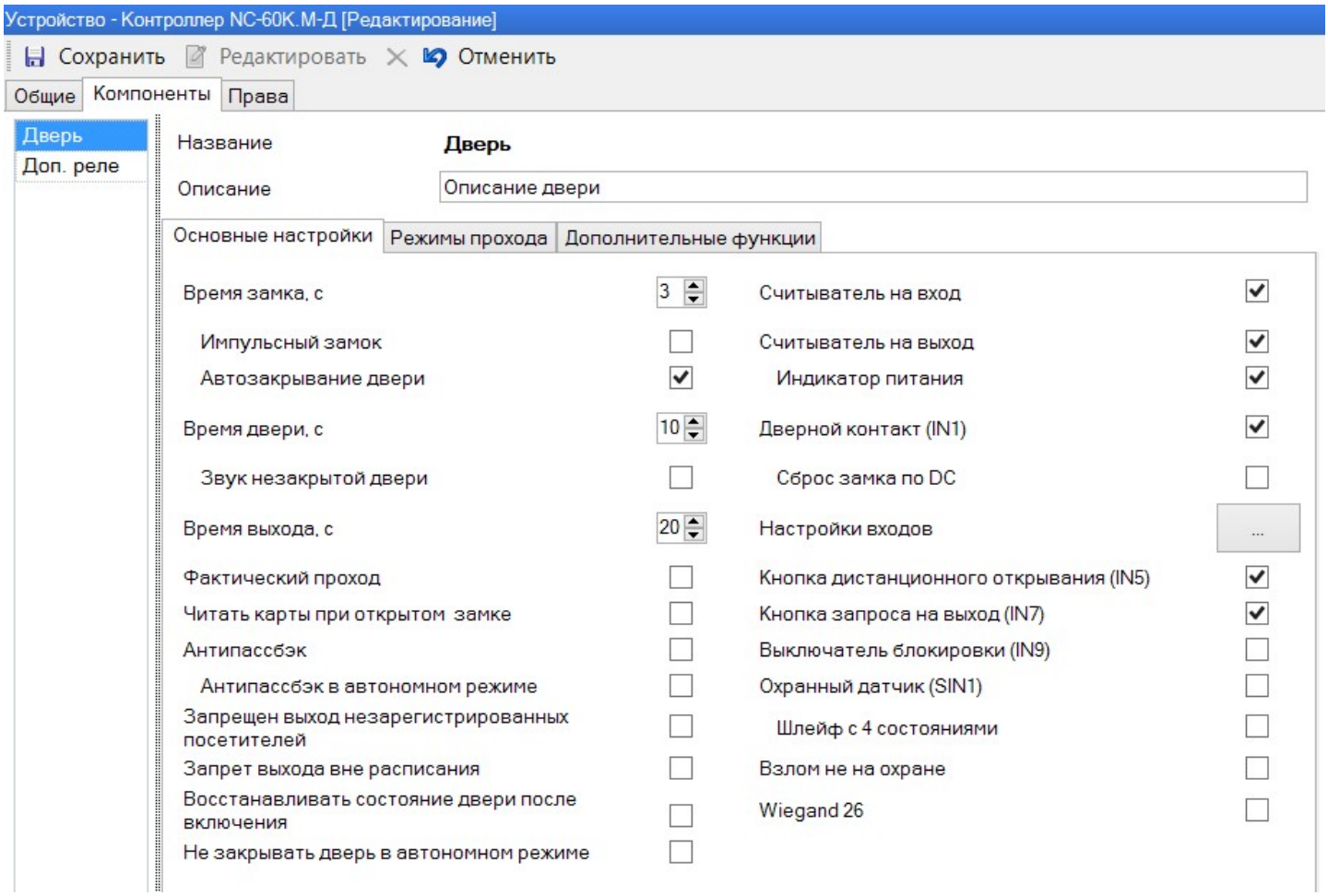
К контроллеру могут быть подключены 2 двери и 2 турникета. Маркировка для них отличается: NC-60K.M-Д2 и NC-60K.M-Т2.

Текущий тип точки прохода отображается на левой панели вкладки "Основные настройки".

Изображения вкладок карточки устройства ниже интерактивны: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх.

Карточки контроллеров различных типов точек прохода имеют незначительные отличия. В таблицах ниже приведены описания элементов карточек всех вариантов точек прохода.

Вкладка "Основные настройки"



Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов). Параметр доступен при установленном флажке *Считыватель на вход* или *Считыватель на выход,* либо обоих одновременно.
Антипассбэк в автономном режиме	Данный параметр доступен при установленных флажках *Считыватель на вход* и *Считыватель на выход*. Этот параметр определяет, будет ли работать режим локального антипассбэка для данной точки в случае отсутствия связи между контроллером и ПК. Для точки прохода, не включенной ни в одну область, этот параметр имеет смысл включать всегда, так как отслеживается многократный проход только через эту точку прохода. Включать ли данный параметр для точек прохода, входящих в состав областей антипассбэка, – зависит от политики службы безопасности.
Блокирующий шлюз	При установленном флажке: если в течение заданного времени проход не осуществлен, то обе двери блокируются и пользователь не может покинуть шлюз. Двери открываются кнопками удаленного открывания (DRETE, наружняя) и запроса на выход (RTE, внутренняя), либо из Монитора управления кнопками прямого управления.

При снятом флажке: если в течение заданного времени проход не осуществлен, первая открытая дверь снова открывается и пользователь может выйти из шлюза.

Взлом не на охране Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.

Восстанавливать состояние двери после включения После восстановления питания контроллера восстанавливаются следующие состояния точки прохода:

- открытая дверь, если до потери питания она была открыта:
  - с ПК;
  - кнопкой аварийного выхода.
- состояние охраны.

Время выхода Это время, которое дается на успокоение датчиков внутри помещения при постановке его на охрану. Время начинает отсчитываться после замыкания дверного контакта (закрытия двери).

Время двери Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». При включенной звуковой индикации и включенной опции «Звук открытой двери» считыватель начинает подавать прерывистый звуковой сигнал, напоминая, что дверь необходимо закрыть.

Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.

Время замка Это время в секундах, в течение которого подается управляющий сигнал на контакты замка для его открывания. Рекомендуется для электромеханических замков устанавливать 1 секунду, для электромеханических защелок от 3 до 5 секунд, для электромагнитных замков от 5 до 10 секунд, для турникетов - от 1 до 3 секунд (в зависимости от типа турникета).

В случае импульсного управления замком/турникетом время замка следует устанавливать равным времени разблокировки исполнительного устройства, которое настраивается непосредственно в нем. В течение этого времени на считывателях будет гореть зеленый светодиод, а при установке флажка "Фактический проход" контроллер в течение этого времени также будет ожидать срабатывания дверного контакта или датчика проворота (DC).

Время успокоения датчика Время, необходимое на успокоение датчика присутствия. Система опрашивает датчик присутствия по истечении заданного времени после закрытия выходной двери шлюза.

Время выхода Время для успокоения охранного датчика перед постановкой на охрану посредством идентификатора с соответствующей привилегией.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Датчик присутствия в шлюзе Флажок устанавливается при использовании датчика присутствия, который используется для определения наличия субъекта внутри шлюза.

Дверной контакт Установка/снятие флажка соответственно активирует/деактивирует входной дверной контакт.

Датчик прохода - вход Установка/снятие флажка соответственно включает/выключает датчик проворота турникета на вход.

Датчик прохода - выход Установка/снятие флажка соответственно включает/выключает датчик проворота турникета на выход.

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Запрещен выход незарегистрированных посетителей Только для карты с привилегией "Гостевая карта". Если флажок установлен, то субъект доступа с привилегией "Гостевая карта" сможет выйти только через ту точку прохода, через которую вошел. Контроллеры других точек прохода не позволят ему выйти.

Звук незакрытой двери Есть смысл включать только при наличии дверного контакта. При включенном состоянии, если дверь открыта больше суммы времени замка и времени открытой двери (см. выше), то считыватель начинает подавать прерывистый звуковой сигнал (при условии, что включена звуковая сигнализация считывателя), напоминающий о том, что необходимо закрыть дверь.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Импульсный замок Если флажок установлен, то для открытия на замок посылается короткий сигнал. Если флажок снят, то сигнал открытия продолжается все время замка.

При установке флажка контроллер будет ожидать сигнала с дверного контакта или датчика проворота (DC) после разрешения доступа в течение заданного времени замка.

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

Кнопка дистанционного открывания Если к соответствующему входу контроллера подключена кнопка дистанционного открывания (DRTE), то флажок должен быть установлен.

Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход (RTE), то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

Кнопки на выход из шлюза При установке флажка из шлюза можно будет выйти, нажав на кнопку выхода.

Кнопка открывания - вход Кнопка, открывающая дверь, турникет или шлюз на вход.

Кнопка открывания - выход Кнопка, открывающая дверь, турникет или шлюз на выход.

Название Отображает название выбранного типа точки прохода (устанавливается DIP-переключателями FUNCTION на плате контроллера):

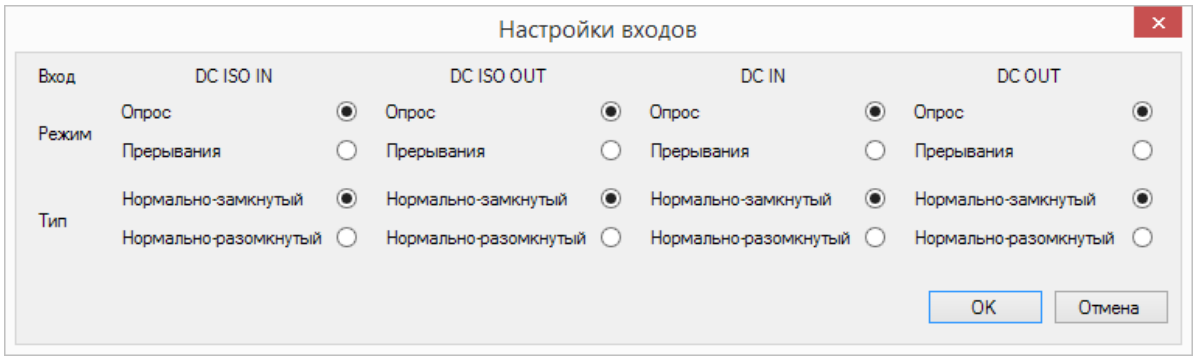
- Дверь - в дереве оборудования и на панелях других инструментов системы отображается как NC-60K/NC-60K.M-Д;

- Турникет - отображается как NC-60K/NC-60K.M-T;
- Шлюз - отображается как NC-60K/NC-60K.M-Ш.

Смена типа точки прохода выполняется только через процедуру замены оборудования[68], после чего необходимо установить DIP-переключатели FUNCTION в правильное положение и перезагрузить контроллер. Отображение контроллера новой точки прохода исправляется в Редакторе топологии.

Направление безопасного выхода Параметр определяет, куда будет выпущен субъект доступа из шлюза при возникновении нештатной ситуации. Например, пропало и потом восстановилось электропитание, когда человек был внутри шлюза. "Наружу" - откроется дверь на выход (вовне охраняемой территории). "Внутрь" откроется дверь на вход (внутрь охраняемой территории).

Настройки входов При нажатии на кнопку открывается окно настроек:



В режиме *Опроса* система периодически опрашивает дверной контакт/датчик проворота. В этом режиме есть вероятность пропустить импульс от них, если контакт/датчик сработает во время паузы опроса.

Режим *Прерывания* характеризуется тем, что импульс от дверного контакта/датчика проворота запускает процесс в системе, но если контакт/датчик замыкается с дребезжанием, то на одно срабатывание может быть запущено несколько процессов.

Нормально-замкнутый или *Нормально разомкнутый* - выбор типа контактов дверного контакта/датчика проворота. В дежурном состоянии точки прохода (бездействующее состояние контакта/датчика) для нормально-замкнутых контактов (NC) используется низкий уровень сигнала, для нормально-разомкнутых (NO) - высокий.

Не закрывать в автономном режиме Если дверь открыта с ПК (из Монитор событий) и контроллер в это время теряет связь с сервером, то:

- при установленном флажке замок остается открытым;
- при снятом флажке замок закрывается.

Описание Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.

Охранный датчик Флажок устанавливается, если к контроллеру доступа подключен охранный датчик, например, инфракрасный детектор движения, или любой другой.

Сброс замка по DC Во включенном состоянии позволяет снять открывающий сигнал с замка по факту закрытия двери, до истечения времени замка. Работает только в том случае, если имеется дверной контакт.

Светодиод считывателя Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Считыватель на вход Установка флажка задействует считыватели с нечетными адресами (1,3,5,7), подключенные напрямую к шине OSDP, или считыватели, подключенные к клеммам OUTDOOR преобразователя Wiegand-OSDP (OMP-W02).

Считыватель на выход Установка флажка задействует считыватели с четными адресами (2,4,6,8) на шине OSDP считыватели, подключенные к клеммам INDOOR преобразователя Wiegand-OSDP (OMP-W02).

Кнопка RTE на двусторонней точке прохода дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки.

Считыватели на выход из шлюза При установке флажка из шлюза можно будет выйти, приложив идентификатор к считывателю.

Удалять временные карты Установленный флажок значит, что контроллер будет самостоятельно удалять идентификатор временной карты из БД контроллера. После этого его можно использовать снова. Функция применяется контроллером при отсутствии связи с сервером. Если в режиме offline идентификатор временной карты не удалить из БД контроллера, то по ней можно будет получить доступ и по истечении срока действия.

Фактический проход При включении опции событие прохода генерируется не по предъявлению карты, а после последовательности событий предъявление карты + срабатывание дверного контакта. Целесообразно устанавливать в случае, если точка прохода не может быть преодолена без срабатывания датчика (например, датчик проворота «вертушки» на турникете). Это позволяет исключить обман системы путем «холостого» предъявления карты - рабочее время в таком случае засчитываться не будет.

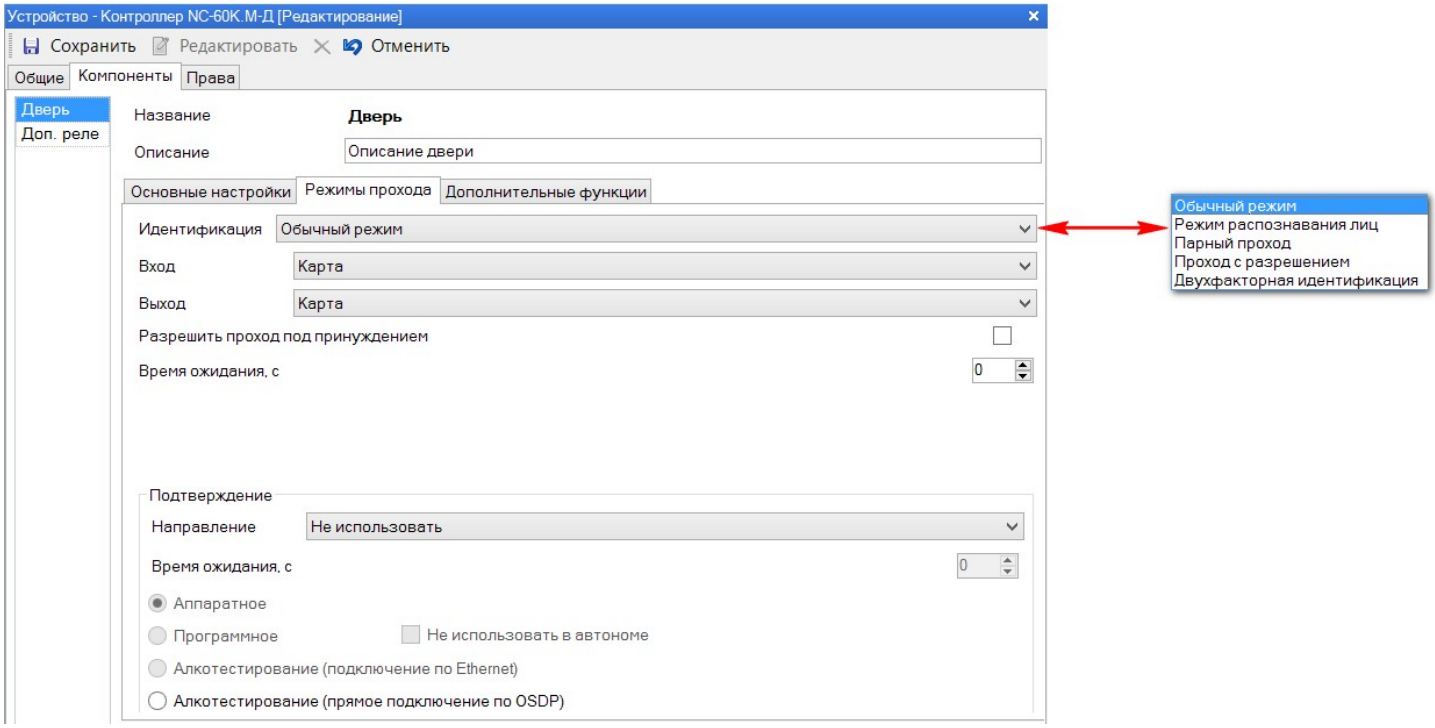
Читать карты при открытом замке При установке флажка контроллер принимает коды карт от считывателя в течение "времени замка". При снятом флажке контроллер не принимает коды карт, пока на реле замка подается управляющий сигнал. **Будьте внимательны**!

Шлейф с 4 состояниями Переключает шлейфы охранного датчика в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание. Такой режим соответствует большей безопасности, однако, требует включения на шлейфах дополнительных резисторов (более подробно о подключении смотрите в руководстве по контроллеру).

Wiegand 26 Включение режима Wiegand 26[70].

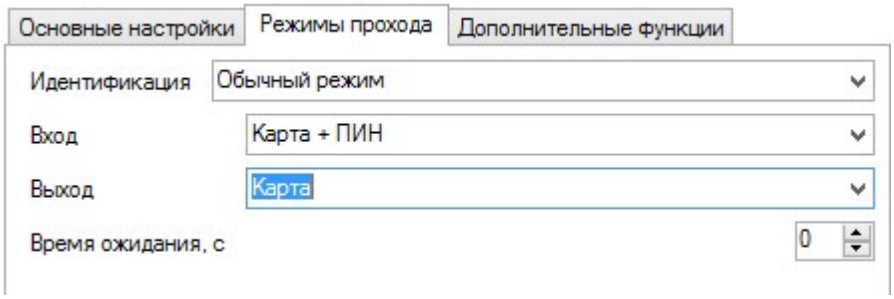
Вкладка "Режимы прохода"

Вкладка позволяет выбрать вариант прохода через точку доступа и настроить его.



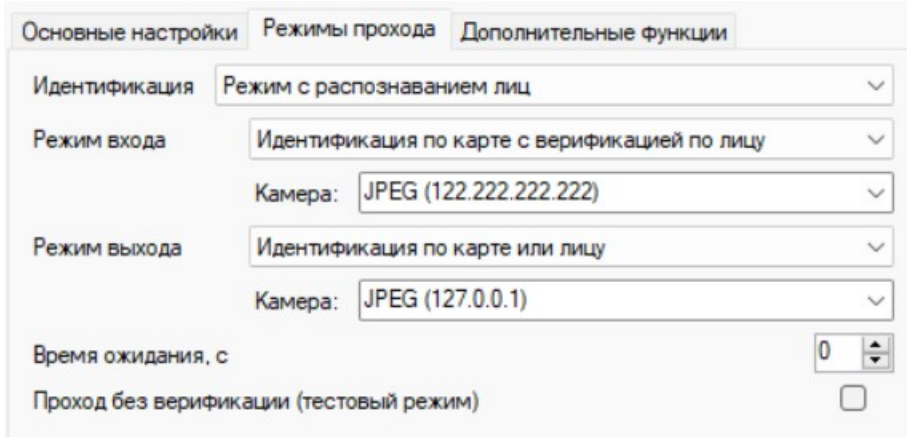
Контроллер NC-60K/NC-60K.M поддерживает следующие режимы прохода:

1. "Обычный режим" - проход только по карте или карте и набору ПИН-кода. Поскольку считыватели к контроллеру подключаются по интерфейсу OSDP, то ПИН-код от клавиатурного считывателя обрабатывается контроллером. Поэтому необходимо настроить отдельно условия для входа и выхода:



- *Время ожидания, с* - в поле устанавливается время, в течение которого система ждет ввода ПИН-кода после прочтения карты;

2. "Режим распознавания лиц" позволяет выбрать разные варианты идентификации пользователя с использованием систем распознавания лиц:



В раскрывающихся списках *Режим входа* и *Режим выхода* выбираются способы, которыми будет осуществляться идентификация пользователя:

- "Идентификация по карте" - субъект доступа идентифицируется по предъявленной карте;

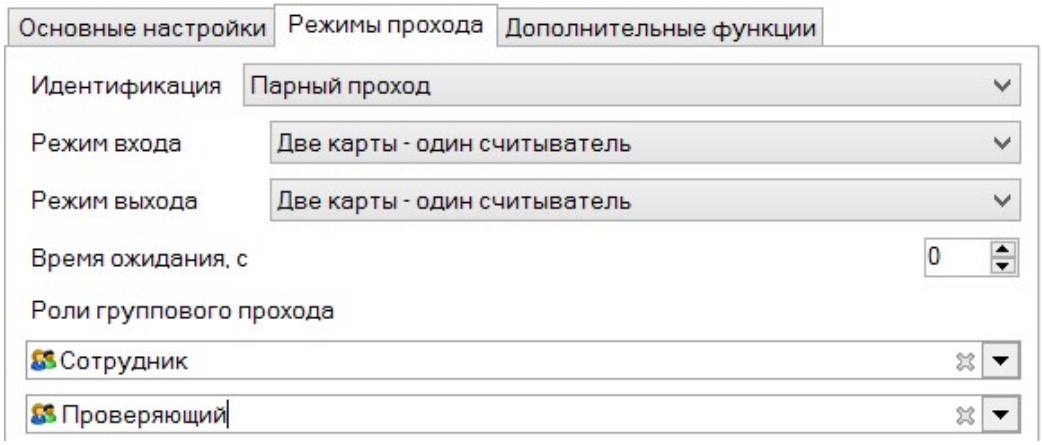
- "Идентификация по лицу" - субъект доступа идентифицируется, если его лицо соответствует фото в БД системы распознавания лиц (СРЛ);
- "Идентификация по карте или лицу" - субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты;
- "Идентификация по карте с верификацией по лицу" - субъект доступа идентифицируется совместно и по коду карты, и по лицу. Полное время сессии распознания субъекта доступа начинается с момента поднесения карты к считывателю и должна завершиться до истечения времени, заданном в поле *Время верификации.*

Камера - из раскрывающегося списка необходимо выбрать камеру, с которой работает задействованная СРЛ.

Время ожидания, с - время с момента когда контроллер подтвердил право прохода карты, до момента открытия двери. Включает в себя сканирование лица, поиск соответствия ему в БД СРЛ и получение сигнала на открытие двери.

Проход без верификации (тестовый режим) - субъект идентифицируется по коду карты, даже если лицо не будет совпадать с фото в БД СРЛ. Если субъект идентифицирован и СКУД разрешает доступ, то дверь откроется только после истечения полного времени ожидания. Рекомендуется для использования на период отладки взаимодействия с СРЛ;

3. "Парный проход" и "Проход с разрешением" - режимы прохода, для которых требуется два пользователя. Используются в целях повышения безопасности доступа.
Настройки[115] для этих режимов одинаковые, но в случае парного прохода система включит обоих пользователей в списки антипассбэка, их обоих посчитает счетчик проходов и система сформирует сообщения о проходе двух пользователей. В случае прохода с разрешением в системе будет учтен только первый приложивший карту пользователь. Если при этом на территорию (в помещение) зайдут оба, то возможны ошибки в работе, например, позднее система посчитает, что из помещения вышли все и попытается поставить помещение на охрану. Но неучтенный пользователь в этом помещении вызовет тревогу.



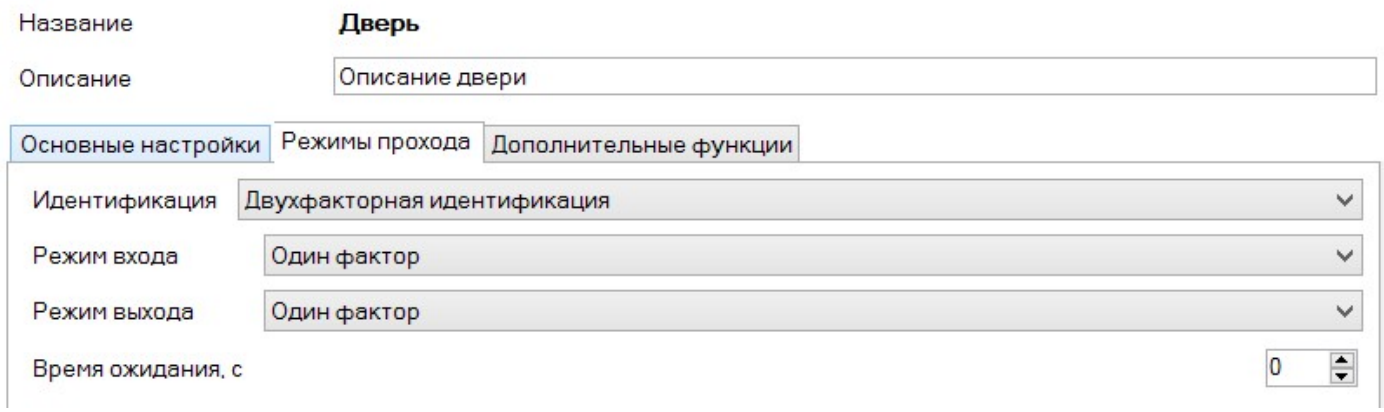
В обоих этих режимах необходимо задать настройки для входа и выхода:

- *Не используется* - при в проходе в этом направлении функционал режимов не задействуется. Происходит обычнй проход по одному идентификатору;
- *Две карты - один считыватель* - поднесение двух карт (с опциональным вводом ПИН-кода) к одному и тому же считывателю;
- *Две карты - разные считыватели* - поднесение двух карт (с опциональным вводом ПИН-кода) к двум разнесенным считывателям (чтобы не допустить поднесение двух карт одним человеком).

Время ожидания, с - максимальное время между поднесениями карт к считывателю(-ям);

Роли группового прохода - описание настроек приведено в разделе Настройка группового прохода[115];

4. "Двухфакторная идентификация" - режим может применяться, когда пользователи имеют несколько разных идентификаторов. Например, карта, отпечаток пальца, скан радужной оболочки глаза, скан лица и т.п. При проходе в этом режиме необходимо будет предъявить выбранное количество разных идентификатора из числа тех, которые загружены в БД контроллера. Количество факторов идентификации выбирается отдельно для входа и для выхода: "Не используется", "Один фактор" или "Два фактора".



- *Время ожидания, с* - максимальное время между предъявлением двух идентификаторов.

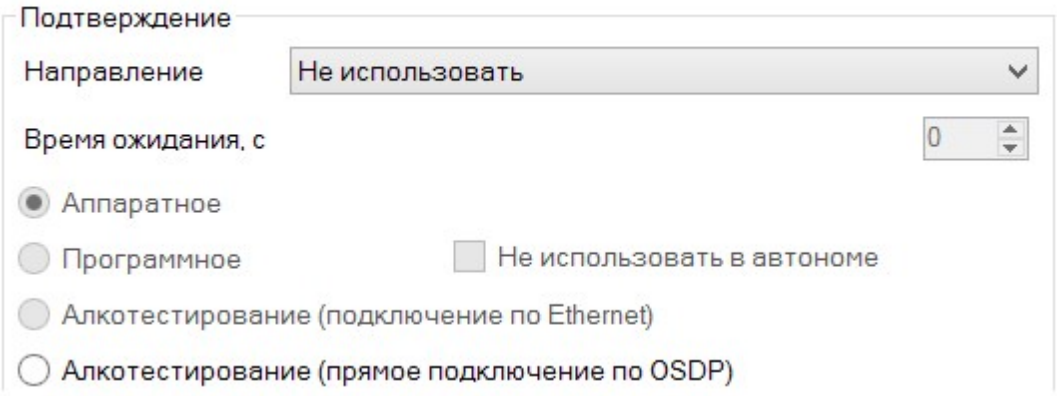
Пример представлен в разделе[732].

При установленном флажке *Разрешить проход под принуждением* доступ субъекта доступа при наборе кода принуждения предоставляется. Для этого, естественно, требуется считыватель с клавиатурой и соответствующие его настройки. Если флажок не установлен, то доступ предоставлен не будет. В обоих случаях в системе генерируется событие доступа под принуждением.

У контроллера NC-60K.M-Ш на этой вкладке отображается флажок *Повторная идентификация внутри шлюза*. Если его установить, то субъекту доступа потребуется повторно приложить идентификатор к считывателю внутри шлюза, чтобы выйти из него.

Блок данных ***Подтверждение*** работает независимо от выбранных режимов прохода.

Использование подтверждения состоит в том, что после разрешения пользователю доступа в соответствии с выбранным режимом прохода система должна дополнительно получить подтверждающий сигнал, например, от весовой платформы или измерителя температуры.

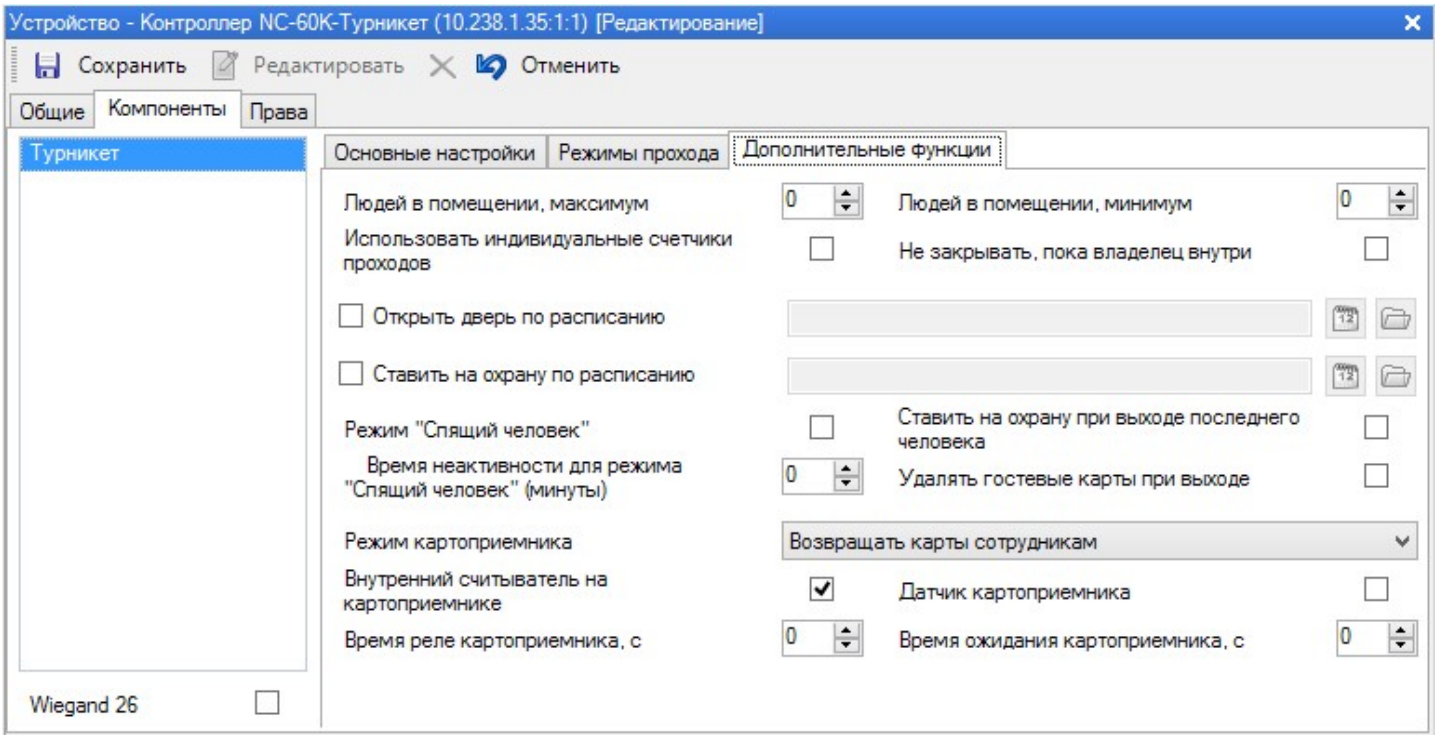


Элементы управления:

- *Направление* - подтверждающий сигнал будет необходим для выбранного из раскрывающегося списка направления прохода: "Не использовать", "Вход и выход", "Только вход", "Только выход";

- *Время ожидания, с* - в поле задается время в течение которого необходимо пройти дополнительную идентификацию для получения подтверждающего сигнала. В противном случае весь цикл идентификации субъекта доступа придется выполнить с самого начала;
- *Аппаратное* - флажок устанавливается в случае, когда сигнал подтверждения получается от какого-либо внешнего устройства, например, алкотестера или просто кнопки;
- *Программное* - флажок устанавливается, когда подтверждающий сигнал получается программным методом;
- *Не использовать в автономе* - установленный флажок отменяет необходимость подтверждающего сигнала, если контроллер точки прохода не имеет связи с сервером и работает в автономном режиме;
- *Алкотестирование (подключение по Ethernet)* - флажок устанавливается, когда алкотестер[141] подключен к Системе через Ethernet. При этом время ожидания показывает время ожидания контроллера от считывания кода идентификатора до получения данных от алкотестера;
- *Алкотестирование (прямое подключение по OSDP)* - флажок устанавливается, когда алкотестер подключается напрямую к шине OSDP контроллера. В этом случае время ожидания так же означает время ожидания контроллера от считывания кода идентификатора до получения данных от алкотестера.

Вкладка "Дополнительные функции"



Описание настроек картоприемника (параметры ниже флажка *Удалять гостевые карты при выходе*) вынесены в отдельный раздел[113].

Параметр	Описание
Время неактивности для режима "Спящий человек" (минуты)	Время, по истечении которого в режиме "Спящий человек" формируется транзакция "Тревога "Спящий человек".
Использовать индивидуальные счетчики проходов	При установленном флажке контроллер постоянно ведет подсчет входов карт, у которых установлен лимит проходов. Максимальное количество проходов - 63. Недоступен при выборе режимах прохода "Парный проход" и "Проход с разрешением". Может отменяться привилегией "Не использовать счетчик проходов".

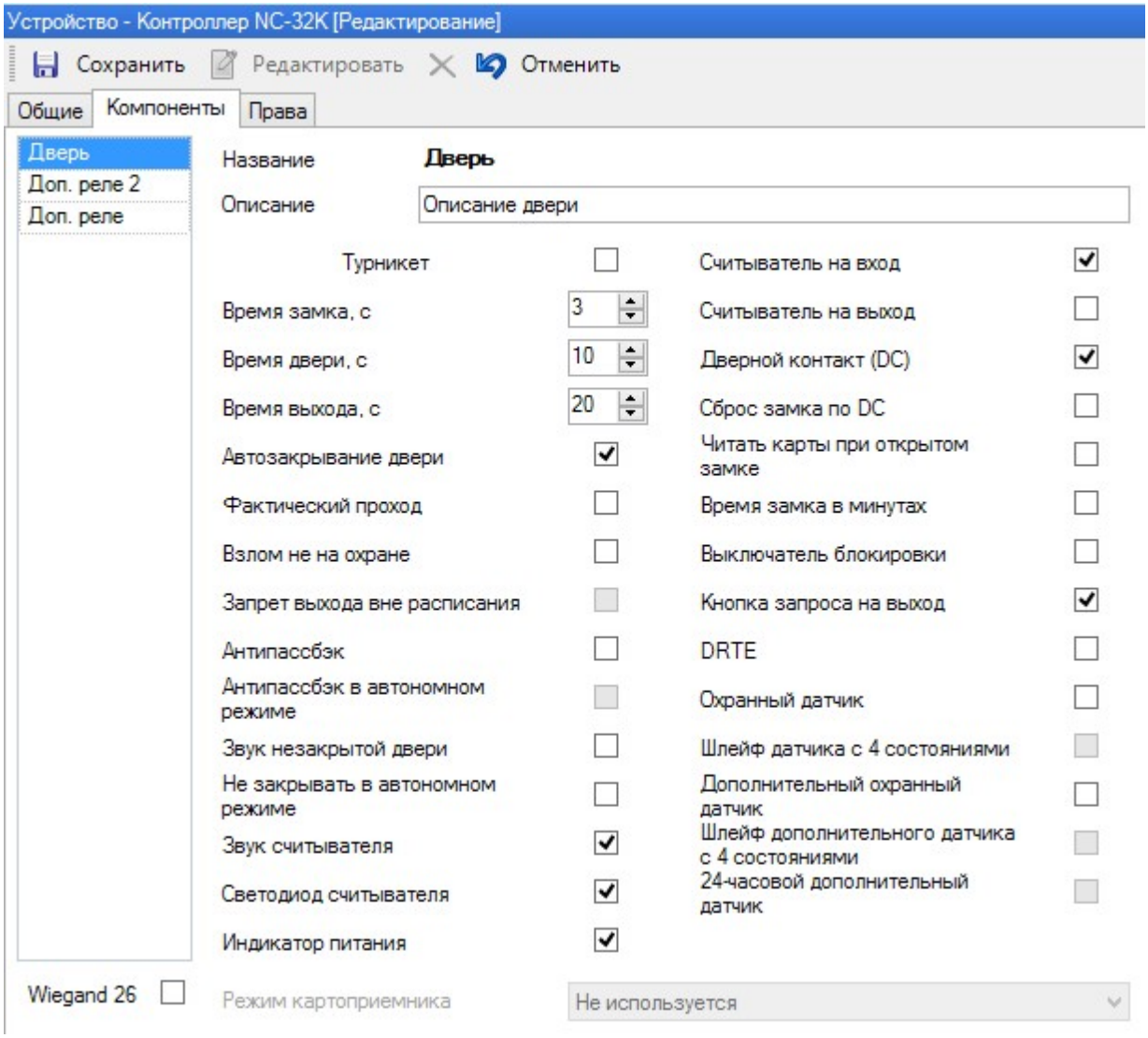
юдей в помещении, аксимум	Количество сотрудников в помещении, при достижении которого вход сотрудников будет заблокирован.
юдей в помещении, инимум	Количество сотрудников в помещении, при достижении которого выход сотрудников будет заблокирован.
е закрыват ь, пока аделец внут ри	*ежим дост упен т олько для двуст оронних т очек прохода* . Если в помещение вошел сотрудник с идентификатором, для которого установлен флажок *Владелец кабинет а* , то дверь остается открытой до его выхода. После выхода дверь переходит в обычный режим доступа. Поднесение к считывателю карт остальных пользователей в этот период порождает обычные транзакции входа/выхода (без управления замком). Если в помещение вошли несколько сотрудников с такой привилегией, то дверь перестанет быть постоянно открытой после первого выхода одного из них.
т крыт ь дверь по асписанию	Электрозамок двери открывается и закрывается по специально созданному расписанию, соответственно в начале и конце рабочего времени (периода разрешенного доступа).
ежим "Спящий еловек"	В данном режиме датчики отслеживают движение в помещении, в которое вошел сотрудник. При отсутствии движения в течение заданного времени формируется транзакция "Тревога "Спящий человек". После того, как тревожная транзакция сформирована, отсчет времени перезапускается в момент срабатывания датчика движения в этом помещении.
т авит ь на охрану о расписанию	Территория ставится на охрану по отдельно созданному расписанию доступа *вначале* рабочего времени (периода разрешенного доступа), снимается с охраны *вконце* периода рабочего времени. Т.е. начало рабочего времени этого "охранного расписания" должно совпадать с завершением рабочего времени того расписания, по которому ходят сотрудники.
т авит ь на охрану ри выходе оследнего еловека	При отсутствии людей в помещении, оно автоматически ставится на охрану, при условии, что время выхода больше времени замка. В противном случае, помещение на охрану не ставится.
Удалять гостевые карты при выходе	Установленный флажок значит, что контроллер будет самостоятельно удалять идентификатор карты с привилегией "Гостевая карта" из БД контроллера. После этого его можно использовать снова. Если идентификатор гостевой карты не удалить из БД контроллера, работающего в режиме offline, то по ней можно будет снова получить доступ.

8.1.2.5 Настройки NC-32K.M

В данном разделе описаны настройки контроллера NC-32K.M/32K-IP, отображаемые в разделе *Компоненты.* Описание вкладок *Общие* и *Права* находится в вышестоящем разделе 69.

Переключение доступных типов точек прохода производится в карточке контроллера флажком "Турникет". Контроллер поддерживает точки прохода типов "Дверь" и "Турникет". Текущий тип точки прохода отображается на левой панели.

Изображения вкладок карточки устройства ниже интерактивны: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх.



Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов). Параметр доступен при установленном флажке *Считыватель на вход* или *Считыватель на выход,* либо обоих одновременно.
Антипассбэк в автономном режиме	Данный параметр доступен при установленных флажках *Считыватель на вход* и *Считыватель на выход*. Этот параметр определяет, будет ли работать режим локального антипассбэк-а для данной точки в случае отсутствия связи между контроллером и ПК. Для точки прохода, не включенной ни в одну область, этот параметр имеет смысл включать всегда, так как отслеживается многократный проход только через эту точку прохода. Включать ли данный параметр для точек прохода, входящих в состав областей антипассбэк-а, – зависит от политики службы безопасности.

Взлом не на охране Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.

Время выхода Это время, которое дается на успокоение датчиков внутри помещения при постановке его на охрану. Время начинает отсчитываться после замыкания дверного контакта (закрытия двери).

Время двери Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». При включенной звуковой индикации и включенной опции «Звук открытой двери» считыватель начинает подавать прерывистый звуковой сигнал, напоминая, что дверь необходимо закрыть.

Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.

Время замка Это время в секундах, в течение которого подается управляющий сигнал на контакты замка для его открывания. Рекомендуется для электромеханических замков устанавливать 1 секунду, для электромеханических защелок от 3 до 5 секунд, для электромагнитных замков от 5 до 10 секунд, для турникетов - от 0 до 3 секунд (в зависимости от типа турникета). Например, для турникетов фирмы PERCo, не отрабатывающих снятие сигнала управления, следует устанавливать 0 секунд (что реально соответствует времени в 0,4 секунды), поскольку при установке даже 1 секунды возможен последовательный проход двух человек.

Время замка в минутах При установке этого флажка время замка будет исчисляться в минутах, вместо используемого по умолчанию исчисления в секундах.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Дверной контакт (DC) Включается, если точка прохода оборудована датчиком закрытого состояния точки прохода (например, геркон на двери или датчик проворота турникета). При установке дверного контакта имеется возможность отслеживать состояние двери в различных ситуациях (взлом двери, дверь оставлена открытой и так далее).

Дополнительный охранный датчик Флажок нужно установить, если к контроллеру подключен дополнительный (второй) охранный датчик.

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Звук незакрытой двери Есть смысл включать только при наличии дверного контакта. При включенном состоянии, если дверь открыта больше суммы времени замка и времени открытой двери (см. выше), то считыватель начинает подавать прерывистый звуковой сигнал (при условии, что включена звуковая сигнализация считывателя), напоминающий о том, что необходимо закрыть дверь.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход, то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

DRTE В дверном режиме установите этот флажок:
- при одностороннем проходе для подключения в качестве дополнительной кнопки открывания двери;
- при двустороннем проходе для подключения в качестве кнопки открывания двери (т.к. кнопка запроса на выход работает только для постановки на охрану).

В турникетном режиме установите этот флажок для подключения кнопки, открывающей турникет на вход.

Сброс замка по DC Во включенном состоянии позволяет снять открывающий сигнал с замка по факту закрытия двери, до истечения времени замка. Работает только в том случае, если имеется дверной контакт.

Не закрывать в автономном режиме Если дверь открыта с ПК (из Монитор событий) и контроллер в это время теряет связь с сервером, то:
- при установленном флажке замок остается открытым;
- при снятом флажке замок закрывается.

Описание Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.

Охранный датчик Флажок устанавливается, если к контроллеру доступа подключен охранный датчик, например, инфракрасный детектор движения, или любой другой.

Светодиод считывателя Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Считыватель на вход Данный параметр доступен для всех типов контроллеров, кроме контроллеров старых версий NC-1000, где внешний считыватель считается подключенным всегда. Наличие только внутреннего считывателя может понадобиться, например, в случае использования контроллера на выезде с парковки, где внешний считыватель на вход (въезд) не нужен.

Считыватель на выход Включается, если точка прохода двухсторонняя (оборудована двумя считывателями). Кнопка запроса на выход на двусторонней точке прохода дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки.

Турникет Данный параметр определяет тип точки прохода: дверь или турникет. При включении параметра в Мониторе событий появляется возможность не просто открыть точку прохода, но и выбрать, открывать ее на вход или на выход, что немаловажно при использовании турникетов. Если флажок *Автозакрывание* не будет установлен, то при открывании турникета с ПК команда на его закрытие не будет отсылаться автоматически по истечении времени замка и оператору придется посылать ее вручную.

При установленном флажке становится недоступным управление параметрами дополнительного реле. У данных контроллеров в турникетном режиме дополнительное реле работает точно с такими же параметрами, как и замковое. То есть, при установке времени замка равным 3 секундам, дополнительное реле для открывания турникета на выход также будет срабатывать на 3 секунды.

Фактический проход	При включении опции событие прохода генерируется не по предъявлению карты, а после последовательности событий предъявление карты + срабатывание дверного контакта. Целесообразно устанавливать в случае, если точка прохода не может быть преодолена без срабатывания датчика (например, датчик проворота «вертушки» на турникете). Это позволяет исключить обман системы путем «холостого» предъявления карты - рабочее время в таком случае засчитываться не будет.
Читать карты при открытом замке	При установке флажка контроллер принимает коды карт от считывателя в течение "времени замка". При снятом флажке контроллер не принимает коды карт, пока на реле замка подается управляющий сигнал. Будьте внимательны!
Шлейф датчика с 4 состояниями	Переключает шлейфы охранного датчика в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание. Такой режим соответствует большей безопасности, однако, требует включения на шлейфах дополнительных резисторов (более подробно о подключении смотрите в руководстве по контроллеру).
Шлейф дополнительного датчика с 4 состояниями	Переключает шлейфы дополнительного охранного датчика в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание.
24 часовой дополнительный датчик	При активации этой опции дополнительный датчик переходит на круглосуточный режим работы. При этом тревожное событие генерируется в любом режиме работы контроллера.
Wiegand 26	Включение режима Wiegand 26[70].

8.1.2.6 Настройки NC-100K-IP

В данном разделе описаны настройки контроллера NC-100K-IP. Раздел содержит описание вкладок *Компоненты*:

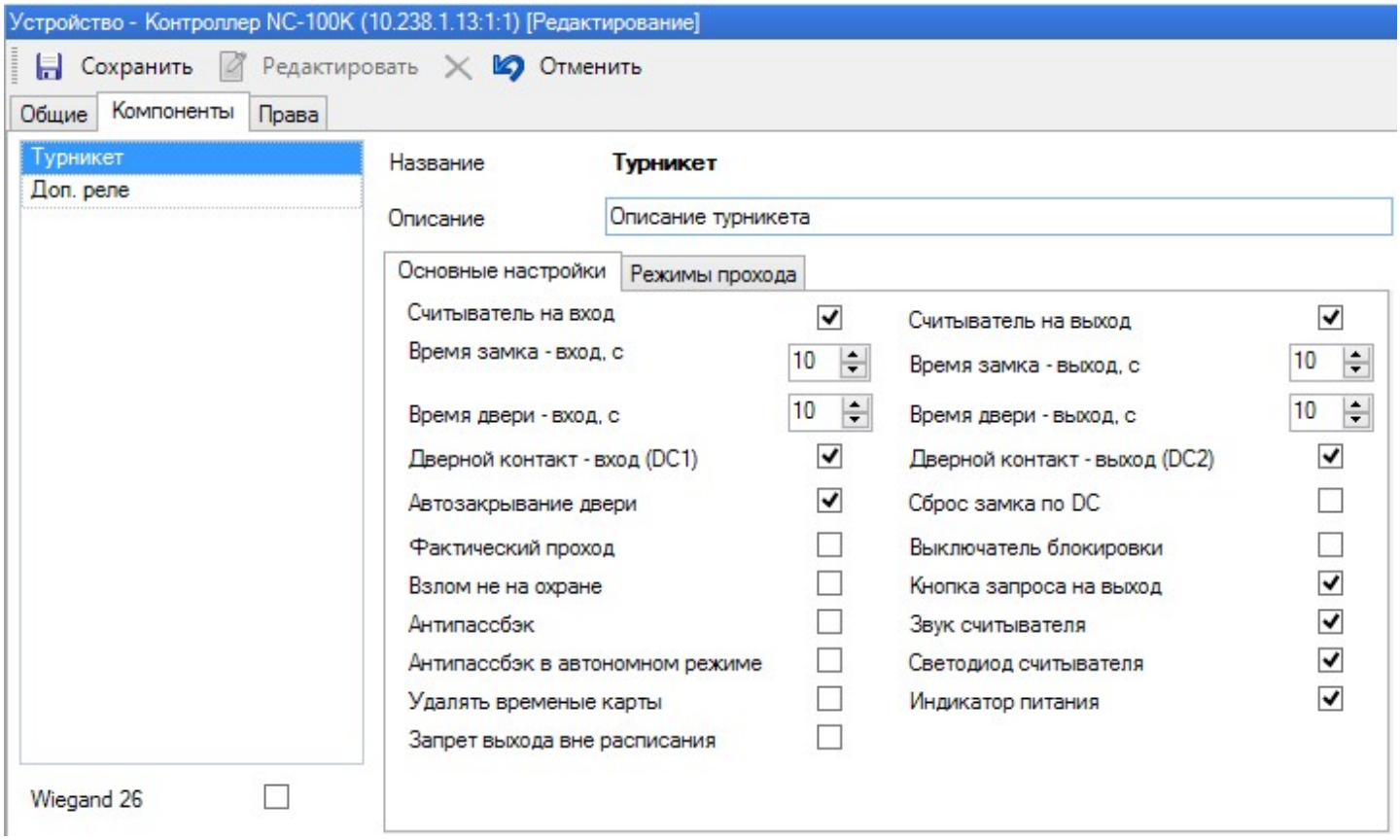
- Основные настройки;
- Режимы проходов[102].

Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].

Контроллер работает только с точками прохода типа "Турникет".

Изображения вкладок карточки устройства ниже интерактивны: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх

Вкладка "Основные настройки"



Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов). Параметр доступен при установленном флажке *Считыватель на вход* или *Считыватель на выход,* либо обоих одновременно.
Антипассбэк в автономном режиме	Данный параметр доступен при установленных флажках *Считыватель на вход* и *Считыватель на выход*. Этот параметр определяет, будет ли работать режим локального антипассбэк-а для данной точки в случае отсутствия связи между контроллером и ПК. Для точки прохода, не включенной ни в одну область, этот параметр имеет смысл включать всегда, так как отслеживается многократный проход только через эту точку прохода. Включать ли данный параметр для точек прохода, входящих в состав областей антипассбэк-а, – зависит от политики службы безопасности.
Взлом не на охране	Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.
Время двери	Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». У контроллера NC-100K-IP время двери настраивается отдельно для входа и для выхода.

Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.

Время замка Это время в секундах, в течение которого подается управляющий сигнал на контакты реле замка для разблокировки турникета. В зависимости от типа турникета рекомендуется устанавливать от 0 до 3 секунд. Например, для турникетов фирмы PERCo, не отрабатывающих снятие сигнала управления, следует устанавливать 0 секунд (что реально соответствует времени в 0,4 секунды), поскольку при установке даже 1 секунды возможен последовательный проход двух человек.

У контроллера NC-100K-IP время замка настраивается отдельно для входа и для выхода.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Дверной контакт К контактам DC1 и DC2 подключаются датчики проворота турникета соответственно на вход и на выход.

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход, то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

Сброс замка по DC Во включенном состоянии позволяет снять открывающий сигнал с замка по факту закрытия двери, до истечения времени замка. Работает только в том случае, если имеется дверной контакт.

Описание Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.

Светодиод считывателя Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Считыватель на вход Данный параметр доступен для всех типов современных контроллеров. Наличие только внутреннего считывателя может понадобиться, например, в случае использования контроллера на выезде с парковки, где внешний считыватель на вход (въезд) не нужен.

Считыватель на выход Включается, если точка прохода двухсторонняя (оборудована двумя считывателями). Кнопка RTE на двусторонней точке прохода дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки.

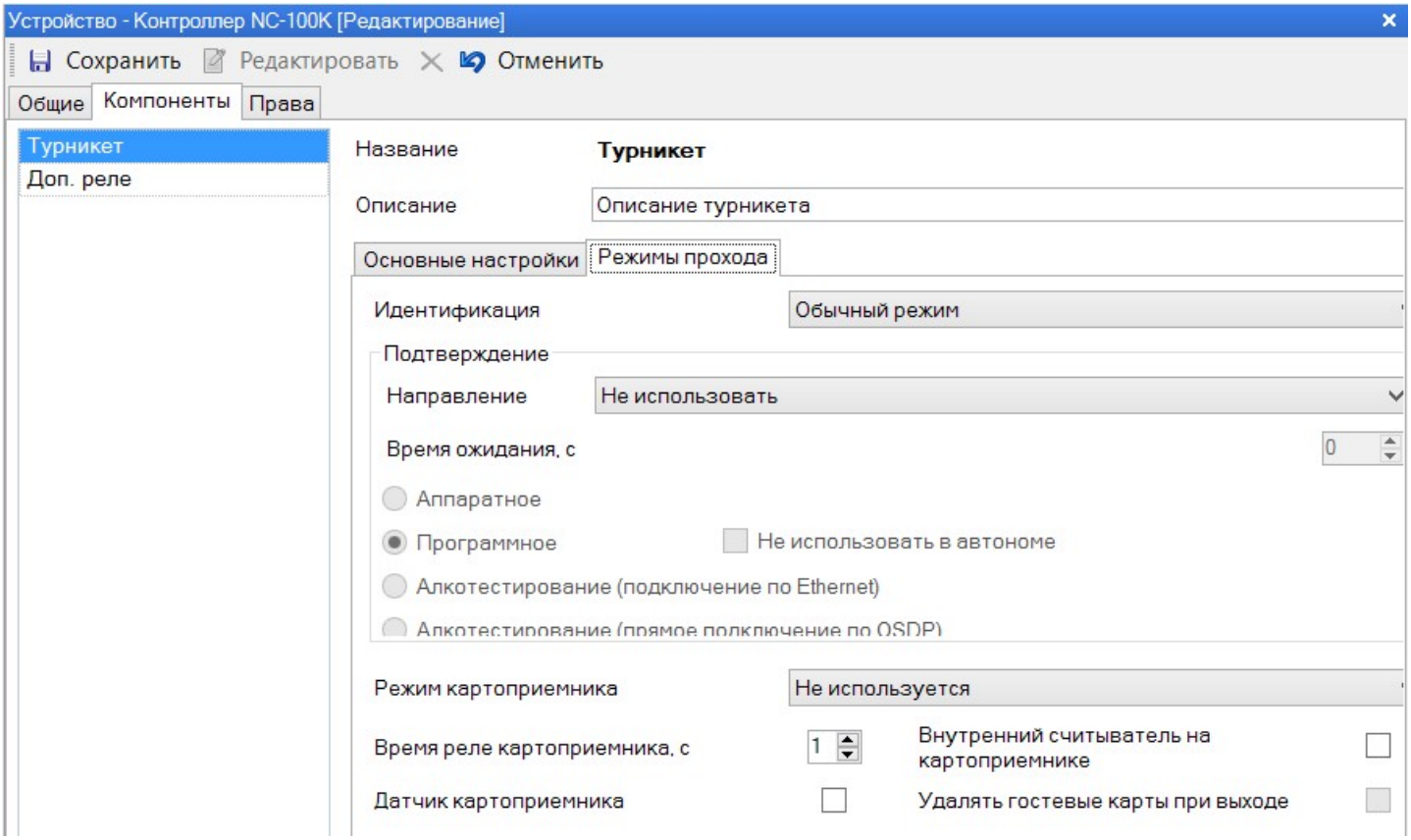
Удалять временные карты Установленный флажок значит, что контроллер будет самостоятельно удалять идентификатор временной карты из БД контроллера. После этого его можно использовать снова. Функция применяется контроллером при отсутствии связи с сервером. Если в режиме offline идентификатор

временной карты не удалить из БД контроллера, то по ней можно будет получить доступ и по истечении срока действия.

Фактический проход При включении опции событие прохода генерируется не по предъявлению карты, а после последовательности событий предъявление карты + срабатывание дверного контакта. Целесообразно устанавливать в случае, если точка прохода не может быть преодолена без срабатывания датчика (например, датчик проворота «вертушки» на турникете). Это позволяет исключить обман системы путем «холостого» предъявления карты - рабочее время в таком случае засчитываться не будет.

Wiegand 26 Включение режима Wiegand 26[70].

Вкладка "Режимы проходов"



Настройки картоприемника описаны в отдельном разделе[113].

Контроллер NC-100K-IP поддерживает следующие режимы прохода:

1. "Обычный режим" (рисунок выше) - проход только по карте, ПИН-коду или карте с набором ПИН-кода, в зависимости от настроек считывателей:

   Блок данных ***Подтверждение*** работает только в обычном режиме прохода.

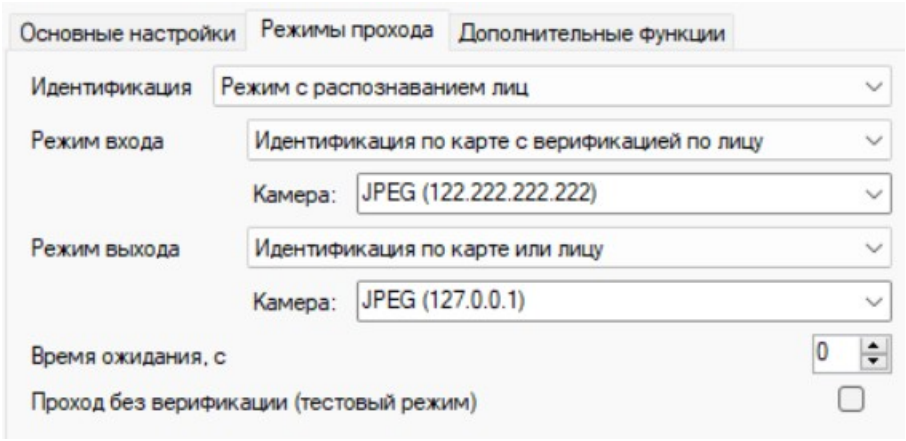
   Использование подтверждения состоит в том, что после разрешения пользователю доступа в соответствии с выбранным режимом прохода система должна дополнительно получить подтверждающий сигнал, например, от весовой платформы или измерителя температуры.

   Элементы управления:

   - *Направление* - подтверждающий сигнал будет необходим для выбранного из раскрывающегося списка направления прохода: "Не использовать", "Вход и выход", "Только вход", "Только выход";
   - *Аппаратное* - флажок устанавливается в случае, когда сигнал подтверждения получается от какого-либо внешнего устройства, например, алкотестера или просто кнопки;

- *Программное* - флажок устанавливается, когда подтверждающий сигнал получается программным методом;
- *Не использовать в автономе* - установленный флажок отменяет необходимость подтверждающего сигнала, если контроллер точки прохода не имеет связи с сервером и работает в автономном режиме;
- *Алкотестирование (подключение по Ethernet)* - флажок устанавливается, когда алкотестер[141] подключен к Системе через Ethernet. При этом время ожидания показывает время ожидания контроллера от считывания кода идентификатора до получения кода от алкотестера;
- *Алкотестирование (прямое подключение по OSDP)* - флажок устанавливается, когда алкотестер подключается напрямую к шине OSDP контроллера. В этом случае время ожидания так же означает время ожидания контроллера от считывания кода идентификатора до получения кода от алкотестера.
- *Время ожидания, с* - в поле задается время в течение которого необходимо пройти дополнительную идентификацию для получения подтверждающего сигнала. В противном случае весь цикл идентификации субъекта доступа придется выполнить с самого начала.

2. "Режим распознавания лиц" позволяет выбрать разные варианты идентификации пользователя с использованием систем распознавания лиц:



В раскрывающихся списках *Режим входа* и *Режим выхода* выбираются способы, которыми будет осуществляться идентификация пользователя:

- "Идентификация по карте" - субъект доступа идентифицируется по предъявленной карте;
- "Идентификация по лицу" - субъект доступа идентифицируется, если его лицо соответствует фото в БД системы распознавания лиц (СРЛ);
- "Идентификация по карте или лицу" - субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты;
- "Идентификация по карте с верификацией по лицу" - субъект доступа идентифицируется совместно и по коду карты, и по лицу. Полное время сессии распознания субъекта доступа начинается с момента поднесения карты к считывателю и должна завершиться до истечения времени, заданном в поле *Время ожидания.*

Камера - из раскрывающегося списка необходимо выбрать камеру, с которой работает задействованная СРЛ.

Время ожидания, с - время с момента когда контроллер подтвердил право прохода карты, до момента открытия двери. Включает в себя сканирование лица, поиск соответствия ему в БД СРЛ и получение сигнала на открытие двери.

Проход без верификации (тестовый режим) - субъект идентифицируется по коду карты, даже если лицо не будет совпадать с фото в БД СРЛ. Если субъект идентифицирован и СКУД разрешает доступ, то дверь откроется только после истечения полного времени ожидания. Рекомендуется для использования на период отладки взаимодействия с СРЛ.

8.1.2.7 Настройки NC-100K-IP.M

В данном разделе описаны настройки контроллера NC-100K-IP. Раздел содержит описание вкладок *Компоненты*:

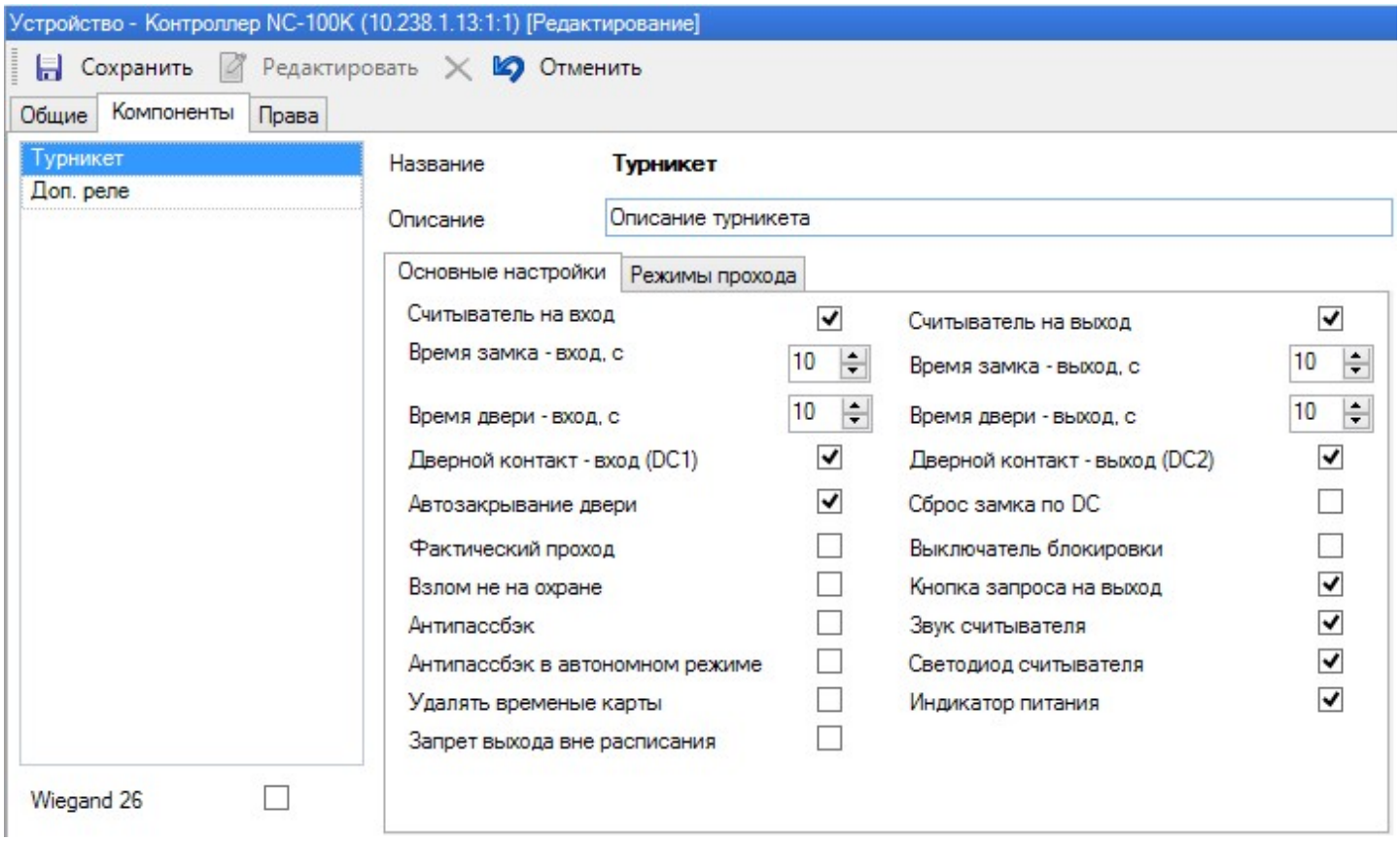
- Основные настройки;
- Режимы проходов[106].

Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].

Контроллер работает только с точками прохода типа "Турникет".

Изображения вкладок карточки устройства ниже интерактивны: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх

Вкладка "Основные настройки"



Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов). Параметр доступен при установленном флажке *Считыватель на вход* или *Считыватель на выход,* либо обоих одновременно.
Антипассбэк в автономном режиме	Данный параметр доступен при установленных флажках *Считыватель на вход* и *Считыватель на выход*. Этот параметр определяет, будет ли работать режим локального антипассбэк-а для данной точки в случае

отсутствия связи между контроллером и ПК. Для точки прохода, не включенной ни в одну область, этот параметр имеет смысл включать всегда, так как отслеживается многократный проход только через эту точку прохода. Включать ли данный параметр для точек прохода, входящих в состав областей антипассбэк-а, – зависит от политики службы безопасности.

Взлом не на охране Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.

Время двери Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». У контроллера NC-100K-IP время двери настраивается отдельно для входа и для выхода.

Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.

Время замка Это время в секундах, в течение которого подается управляющий сигнал на контакты реле замка для разблокировки турникета. В зависимости от типа турникета рекомендуется устанавливать от 0 до 3 секунд. Например, для турникетов фирмы PERCo, не отрабатывающих снятие сигнала управления, следует устанавливать 0 секунд (что реально соответствует времени в 0,4 секунды), поскольку при установке даже 1 секунды возможен последовательный проход двух человек.

У контроллера NC-100K-IP время замка настраивается отдельно для входа и для выхода.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Дверной контакт К контактам DC1 и DC2 подключаются датчики проворота турникета соответственно на вход и на выход.

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

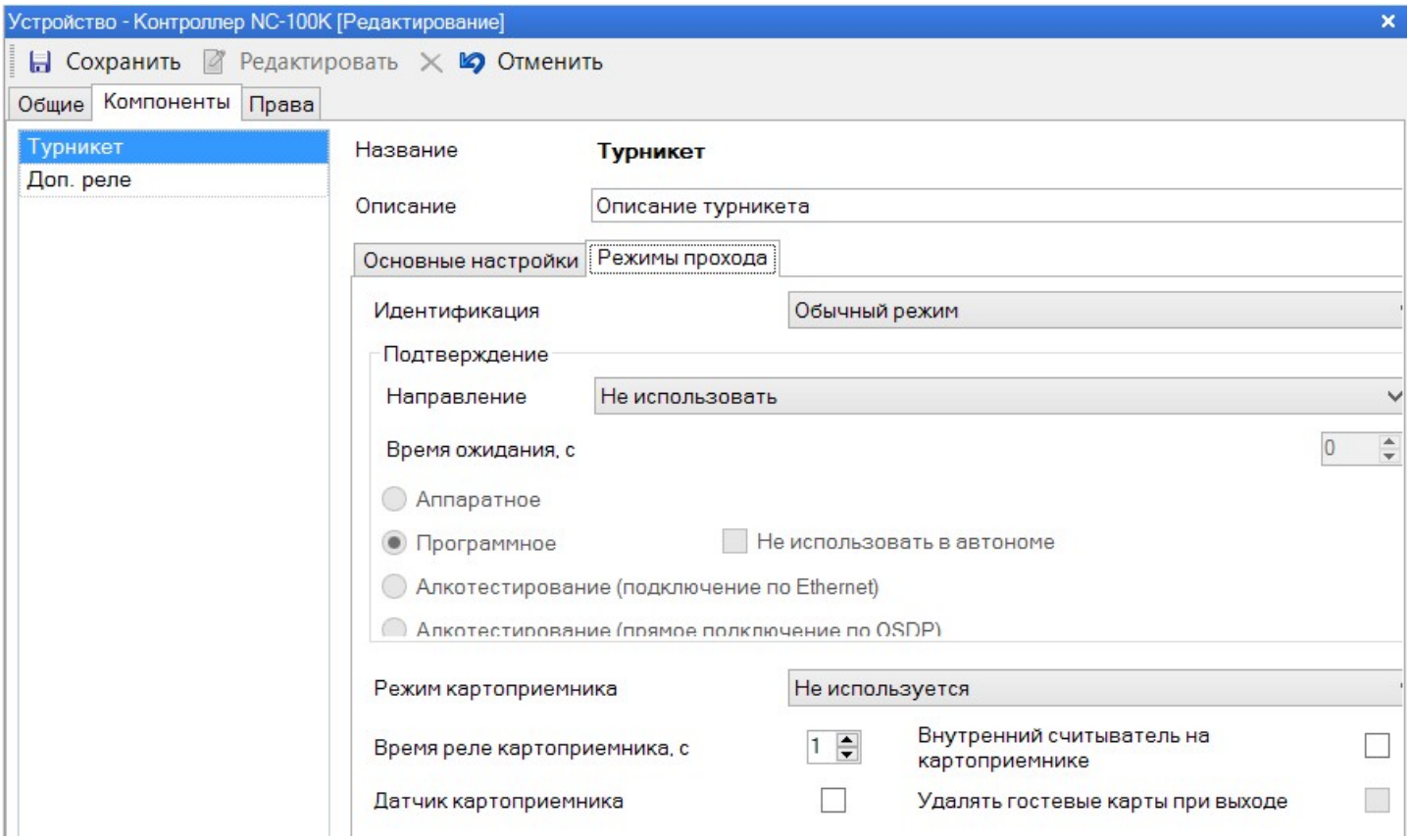
Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход, то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

Сброс замка по DC Во включенном состоянии позволяет снять открывающий сигнал с замка по факту закрытия двери, до истечения времени замка. Работает только в том случае, если имеется дверной контакт.

Описание Произвольное описание. Рекомендуется вводить такое описание, которое впоследствии поможет точно идентифицировать контроллер.

Светодиод считывателя	Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).
Считыватель на вход	Данный параметр доступен для всех типов современных контроллеров. Наличие только внутреннего считывателя может понадобиться, например, в случае использования контроллера на выезде с парковки, где внешний считыватель на вход (въезд) не нужен.
Считыватель на выход	Включается, если точка прохода двухсторонняя (оборудована двумя считывателями). Кнопка RTE на двусторонней точке прохода дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки.
Удалять временные карты	Установленный флажок значит, что контроллер будет самостоятельно удалять идентификатор временной карты из БД контроллера. После этого его можно использовать снова. Функция применяется контроллером при отсутствии связи с сервером. Если в режиме offline идентификатор временной карты не удалить из БД контроллера, то по ней можно будет получить доступ и по истечении срока действия.
Фактический проход	При включении опции событие прохода генерируется не по предъявлению карты, а после последовательности событий предъявление карты + срабатывание дверного контакта. Целесообразно устанавливать в случае, если точка прохода не может быть преодолена без срабатывания датчика (например, датчик проворота «вертушки» на турникете). Это позволяет исключить обман системы путем «холостого» предъявления карты - рабочее время в таком случае засчитываться не будет.
Wiegand 26	Включение режима Wiegand 26[70].

Вкладка "Режимы проходов"



Настройки картоприемника описаны в отдельном разделе[113].

Контроллер NC-100K-IP поддерживает следующие режимы прохода:

1. "Обычный режим" (рисунок выше) - проход только по карте, ПИН-коду или карте с набором ПИН-кода, в зависимости от настроек считывателей:

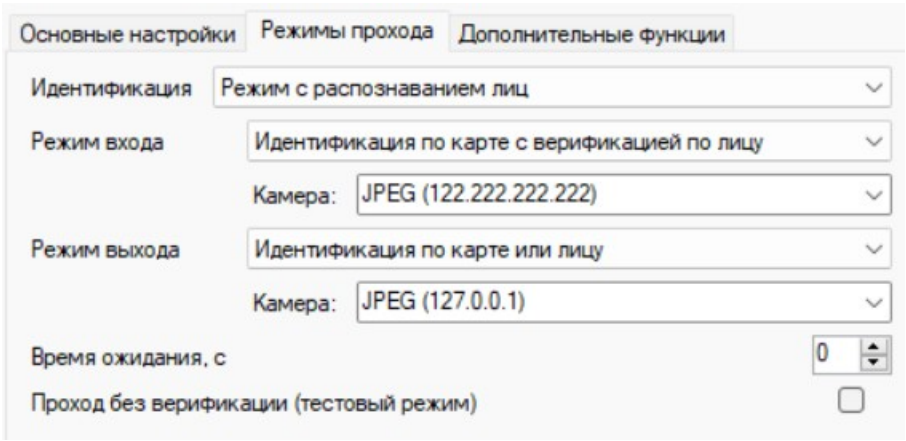
   Блок данных ***Подтверждение*** работает только в обычном режиме прохода.

   Использование подтверждения состоит в том, что после разрешения пользователю доступа в соответствии с выбранным режимом прохода система должна дополнительно получить подтверждающий сигнал, например, от весовой платформы или измерителя температуры.

   Элементы управления:

   - *Направление* - подтверждающий сигнал будет необходим для выбранного из раскрывающегося списка направления прохода: "Не использовать", "Вход и выход", "Только вход", "Только выход";
   - *Аппаратное* - флажок устанавливается в случае, когда сигнал подтверждения получается от какого-либо внешнего устройства, например, алкотестера или просто кнопки;
   - *Программное* - флажок устанавливается, когда подтверждающий сигнал получается программным методом;
   - *Не использовать в автономе* - установленный флажок отменяет необходимость подтверждающего сигнала, если контроллер точки прохода не имеет связи с сервером и работает в автономном режиме;
   - *Алкотестирование (подключение по Ethernet)* - флажок устанавливается, когда алкотестер[141] подключен к Системе через Ethernet. При этом время ожидания показывает время ожидания контроллера от считывания кода идентификатора до получения кода от алкотестера;
   - *Алкотестирование (прямое подключение по OSDP)* - флажок устанавливается, когда алкотестер подключается напрямую к шине OSDP контроллера. В этом случае время ожидания так же означает время ожидания контроллера от считывания кода идентификатора до получения кода от алкотестера.
   - *Время ожидания, с* - в поле задается время в течение которого необходимо пройти дополнительную идентификацию для получения подтверждающего сигнала. В противном случае весь цикл идентификации субъекта доступа придется выполнить с самого начала.

2. "Режим распознавания лиц" позволяет выбрать разные варианты идентификации пользователя с использованием систем распознавания лиц:



В раскрывающихся списках *Режим входа* и *Режим выхода* выбираются способы, которыми будет осуществляться идентификация пользователя:

- "Идентификация по карте" - субъект доступа идентифицируется по предъявленной карте;
- "Идентификация по лицу" - субъект доступа идентифицируется, если его лицо соответствует фото в БД системы распознавания лиц (СРЛ);

- "Идентификация по карте или лицу" - субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты;
- "Идентификация по карте с верификацией по лицу" - субъект доступа идентифицируется совместно и по коду карты, и по лицу. Полное время сессии распознания субъекта доступа начинается с момента поднесения карты к считывателю и должна завершиться до истечения времени, заданном в поле *Время ожидания.*

Камера - из раскрывающегося списка необходимо выбрать камеру, с которой работает задействованная СРЛ.

Время ожидания, с - время с момента когда контроллер подтвердил право прохода карты, до момента открытия двери. Включает в себя сканирование лица, поиск соответствия ему в БД СРЛ и получение сигнала на открытие двери.

Проход без верификации (тестовый режим) - субъект идентифицируется по коду карты, даже если лицо не будет совпадать с фото в БД СРЛ. Если субъект идентифицирован и СКУД разрешает доступ, то дверь откроется только после истечения полного времени ожидания. Рекомендуется для использования на период отладки взаимодействия с СРЛ.

8.1.2.8 Настройки контроллера распознавания лиц



Начиная с версии 3.11.127 использование контроллера распознавания лиц невозможно. Его функционал передан в настройки контроллеров NC-100K-IP[99], NC-60K/NC-60K.M[85], NC-8000[76] (-D, -I). При этом контроллеры должны иметь внутреннее ПО:

- ***NC-100K-IP - версии 8.4 и выше;***
- ***NC-60K/NC-60K.M - любая версия;***
- ***NC-8000 (-D, -I) - версии 3.7 и выше.***

Данный контроллер предназначен для обеспечения работоспособности биометрической системы распознавания лиц. Контроллер является программным модулем и построен на базе контроллера NC-8000. База данных такого контроллера находится на жестком диске ПК. Контроллер работает только в онлайн режиме.

В данном разделе описаны настройки контроллера распознавания лиц, содержащиеся на вкладках:

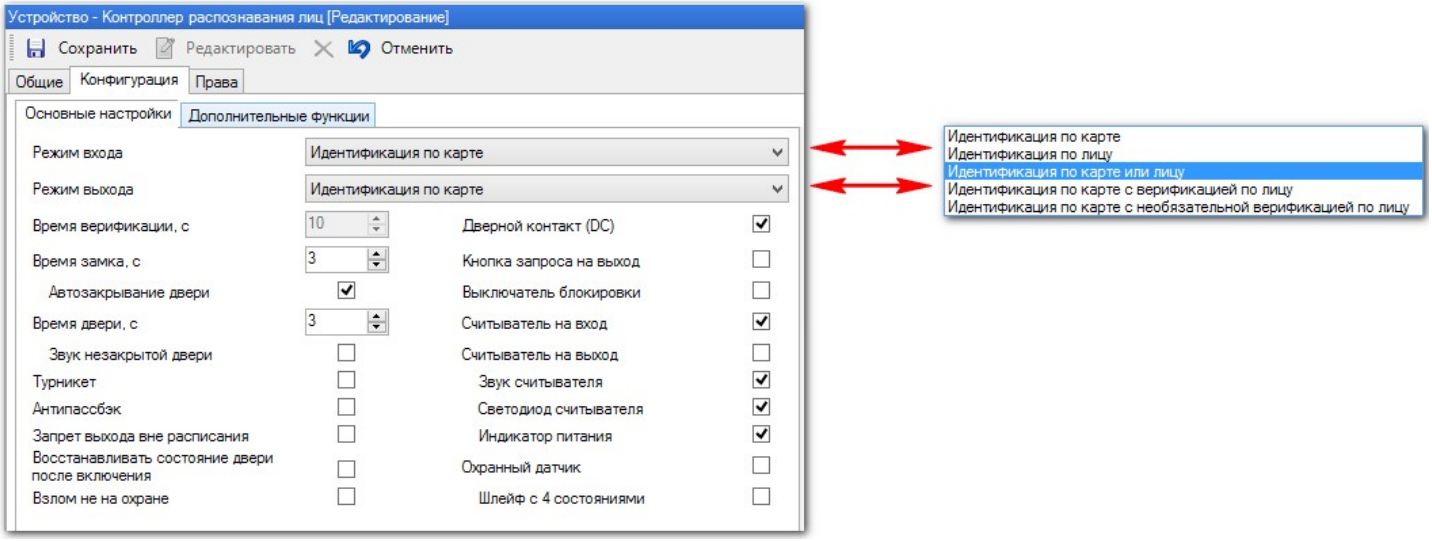
- Основные настройки;
- Дополнительные функции[111].

Описание вкладок *Общие* и *Права* находится в вышестоящем разделе[69].

Переключение доступных типов точек прохода производится в карточке контроллера флажком "Турникет". Контроллер поддерживает точки прохода типов "Дверь" и "Турникет".

Изображения вкладки *Основные настройки* ниже интерактивно: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх.

Вкладка "Основные настройки"



Параметр	Описание
Автозакрывание двери	Если данный параметр включен, то при открывании двери с ПК, дверь будет закрываться автоматически по истечении времени замка. ***Примечание: Некоторые типы электрозамков не допускают длительной подачи напряжения, в связи с чем будьте внимательны при настройке параметров – в подобной ситуации не рекомендуется отключать опцию «Автозакрывание».***
Антипассбэк	Включает для данной точки прохода режим антипассбэка. Данная точка становится также доступной для формирования областей антипассбэка в редакторе групп АПБ[161] (кнопка *Группы АПБ* на панели инструментов).
Взлом не на охране	Если дверь оборудована дверным контактом, то выключение данной опции позволяет не генерировать тревогу взлома при механическом открывании двери. Это бывает необходимо, например, если не установлена кнопка запроса на выход, а дверь изнутри открывается ручкой замка.
Восстанавливать состояние двери после включения	После восстановления питания контроллера восстанавливаются следующие состояния точки прохода: • открытая дверь, если до потери питания она была открыта: - с ПК; - кнопкой аварийного выхода. • состояние охраны.
Время верификации	Время полной сессии распознания субъекта доступа. Начинается с момента поднесения карты к считывателю и включает в себя считывание кода карты, сканирование лица, поиск соответствия им в БД СРЛ, отправку данных на контроллер распознавания лиц и получение сигнала на открытие двери.
Время двери	Это время, которое начинает отсчитываться после окончания времени замка, и по истечении которого контроллер генерирует событие «Дверь оставлена открытой». При включенной звуковой индикации и включенной опции «Звук открытой двери» считыватель начинает подавать прерывистый звуковой сигнал, напоминая, что дверь необходимо закрыть. ***Примечание: При установке времени двери, равном нулю, состояние двери отслеживаться не будет и транзакция «Дверь оставлена открытой» не появится.***

Время замка Это время в секундах, в течение которого подается управляющий сигнал на контакты замка для его открывания. Рекомендуется для электромеханических замков устанавливать 1 секунду, для электромеханических защелок от 3 до 5 секунд, для электромагнитных замков от 5 до 10 секунд, для турникетов - от 0 до 3 секунд (в зависимости от типа турникета). Например, для турникетов фирмы PERCo, не отрабатывающих снятие сигнала управления, следует устанавливать 0 секунд (что реально соответствует времени в 0,4 секунды), поскольку при установке даже 1 секунды возможен последовательный проход двух человек.

Выключатель блокировки Флажок устанавливается, если необходимо отслеживать состояние входа аппаратной блокировки. О подключении кнопки блокировки смотрите в документации на контроллер.

Дверной контакт (DC) Включается, если точка прохода оборудована датчиком закрытого состояния точки прохода (например, геркон на двери или датчик проворота турникета). При установке дверного контакта имеется возможность отслеживать состояние двери в различных ситуациях (взлом двери, дверь оставлена открытой и так далее).

Запрет выхода вне расписания При установленном флажке субъект доступа не сможет покинуть территорию после того, как истек период времени, в который ему разрешен доступ на эту территорию.

Звук незакрытой двери Есть смысл включать только при наличии дверного контакта. При включенном состоянии, если дверь открыта больше суммы времени замка и времени открытой двери (см. выше), то считыватель начинает подавать прерывистый звуковой сигнал (при условии, что включена звуковая сигнализация считывателя), напоминающий о том, что необходимо закрыть дверь.

Звук считывателя Установка флажка приводит к тому, что считыватель выдает звуковые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).

Индикатор питания Снятие флажка приводит к тому, что светодиод на считывателе в дежурном режиме не горит.

Кнопка запроса на выход Если к соответствующему входу контроллера подключена кнопка запроса на выход, то данная опция должна быть включена. (При двухстороннем проходе она выполняет роль кнопки постановки на охрану, но не открывает дверь).

Охранный датчик Флажок устанавливается, если к контроллеру доступа подключен охранный датчик, например, инфракрасный детектор движения, или любой другой.

Режим входа

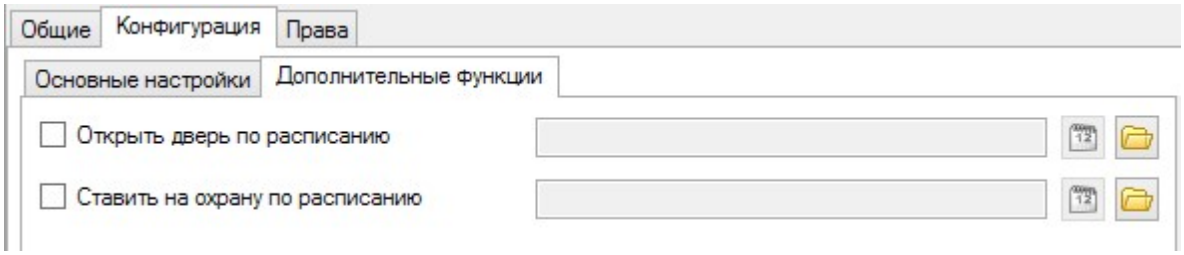
Режим выхода

Способы, которыми будет осуществляться идентификация пользователя при входе и при выходе.

Идентификация по карте	Субъект доступа идентифицируется по предъявленной карте.
Идентификация по лицу	Субъект доступа идентифицируется, если его лицо соответствует фото в БД СРЛ.
Идентификация по карте или лицу	Субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты.
Идентификация по карте с	Субъект доступа идентифицируется совместно и по коду карты, и по лицу. Полное время сессии распознания субъекта доступа начинается с момента

верификацией по лицу	поднесения карты к считывателю и должна завершиться до истечения времени, заданном в поле *Время верификации*
Идентификация по карте с необязательной верификацией по лицу	Субъект идентифицируется по коду карты, даже если лицо не будет совпадать с фото в БД СРЛ. Если субъект идентифицирован и СКУД разрешает доступ, то дверь откроется только после истечения полного времени верификации
Светодиод считывателя	Установка флажка приводит к тому, что считыватель выдает световые сигналы в соответствии со своей схемой индикации (подробнее см. Руководство по эксплуатации на конкретную модель считывателя).
Считыватель на вход	Наличие только внутреннего считывателя может понадобиться, например, в случае использования контроллера на выезде с парковки, где внешний считыватель на вход (въезд) не нужен.
Считыватель на выход	Включается, если точка прохода двухсторонняя (оборудована двумя считывателями). Кнопка RTE на двусторонней точке прохода дверь не открывает, а может использоваться только для постановки помещения на охрану с помощью карточки.
Турникет	Данный параметр определяет тип точки прохода: дверь или турникет. При включении параметра в Мониторе событий появляется возможность не просто открыть точку прохода, но и выбрать, открывать ее на вход или на выход, что немаловажно при использовании турникетов. Если флажок *Автозакрывание* не будет установлен, то при открывании турникета с ПК команда на его закрытие не будет отсылаться автоматически по истечении времени замка и оператору придется посылать ее вручную. При установленном флажке становится недоступным управление параметрами дополнительного реле. У данных контроллеров в турникетном режиме дополнительное реле работает точно с такими же параметрами, как и замковое. То есть, при установке времени замка равным 3 секундам, дополнительное реле для открывания турникета на выход также будет срабатывать на 3 секунды.
Шлейф с 4 состояниями	Переключает шлейфы охранного датчика в режим контроля 4 состояний шлейфа: Нормально, Тревога, Обрыв, Короткое замыкание. Такой режим соответствует большей безопасности, однако, требует включения на шлейфах дополнительных резисторов (более подробно о подключении смотрите в руководстве по контроллеру).

Вкладка "Дополнительные функции"



Параметр	Описание
т крыт ь дверь по асписанию	Электрозамок двери открывается и закрывается по специально созданному расписанию, соответственно в начале и конце рабочего времени (периода разрешенного доступа).
т авит ь на охрану о расписанию	Территория ставится на охрану по отдельно созданному расписанию доступа *вачале* рабочего времени (периода разрешенного доступа),

снимается с охраны *в конце* периода рабочего времени. Т.е. начало рабочего времени этого "охранного расписания" должно совпадать с завершением рабочего времени того расписания, по которому ходят сотрудники.

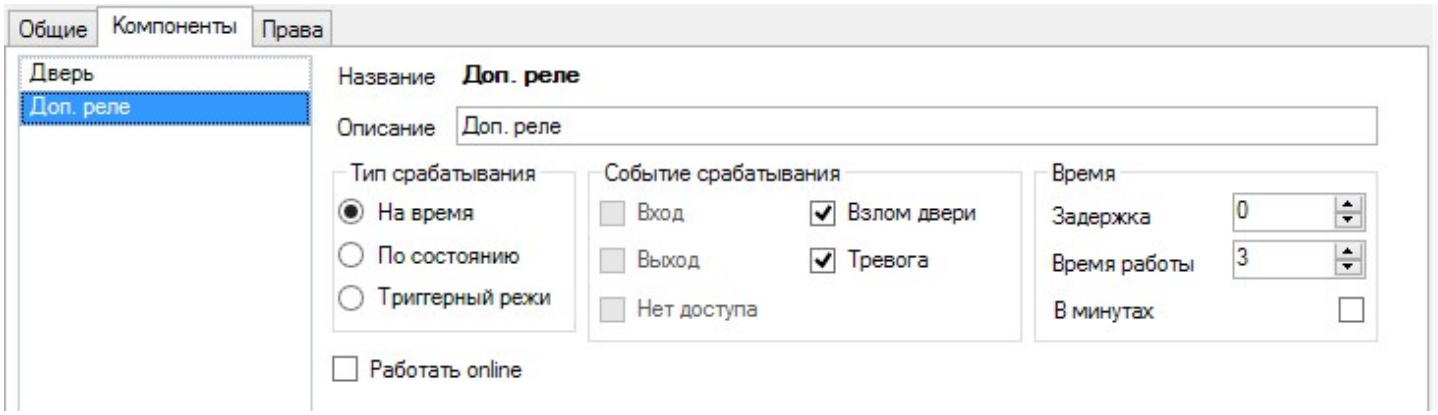
8.1.2.9 Настройки дополнительного реле

В разделе приведено описание настроек дополнительного реле, одинаковые для всех контроллеров. Настраиваемое реле контроллеров NC-32K.M и NC-32K-IP обозначается в карточке устройства как "Доп. реле 2". Обратите внимание, при включении картоприемника в карточке контроллеров NC-32K.M/NC-32K-IP "Доп. реле 2" начинает работать как реле картоприемника[115].

Дополнительное реле можно использовать для активации работы внешний исполнительных устройств. Например, можно к дополнительному реле подключить сигнальную лампу. А в настройках выбрать тип срабатывания «По событию», установить флажки *Нет доступа* и *Работать online*. В этом случае, при отказе субъекту в доступе по каким-либо причинам, кроме сообщения в монитор событий также будет зажигаться сигнальная лампа, привлекая внимание сотрудника охраны.

Настройки дополнительного реле доступны всегда для контроллеров NC-32K.M/NC-32K-IP и NC-100K-IP, а также для остальных типов контроллеров, если не установлен турникетный режим. Чтобы увидеть настраиваемые параметры, нажмите на *Дополнительное реле* на левой панели вкладки *Компоненты*. Описание настроек дополнительного реле приведено в таблице ниже.

Изображение вкладки ниже интерактивно: щелчок по интересующему параметру переведет к строке с его описанием. Для возврата к изображению нажмите на синюю стрелку вверх.



Параметр	Описание
Тип срабатывания	
На время	Функционирование реле определяется выбранными событиями, а также временными параметрами, заданными в блоке «Время».
По состоянию	Реле срабатывает по выбранному тревожному событию и сохраняет свое состояние, пока событие, вызвавшее это срабатывание, не будет снято.
Триггерный режим	При наступлении тревожного события, на срабатывание от которого настроено реле, оно изменяет свое состояние на противоположное.
Событие срабатывания	
Вход	Авторизованный вход субъекта доступа на территорию.
Выход	Авторизованный выход субъекта доступа с территории.
Нет доступа	Запрет прохода субъекта доступа через точку прохода.
Взлом двери	Тревожное событие: несанкционированный доступ через точку прохода.
Тревога	Тревожное событие.

Время

Задержка Время от возникновения события до фактического срабатывания реле. Можно, например, задержать подачу сигнала тревоги через реле контроллера на некоторое время.

Время работы Время, в течение которого реле находится в сработавшем состоянии.

В минутах По-умолчанию время реле устанавливается в секундах. Однако для организации продолжительных задержек срабатывания реле и подачи длительных сигналов можно выбрать в качестве единиц измерения минуты, и тогда установленные числа задержки и работы реле будут соответствовать минутам, а не секундам.

Работать online Если флажок установлен, то реле срабатывает по указанному событию всегда. Если не установлен, то реле срабатывает только при отсутствии связи контроллера с компьютером. Это позволяет, например, при работающем ПК выводить сигнал тревоги только оператору на экран, а при отключенном ПК включать локальное сигнальное устройство.

Алгоритм работы дополнительного реле по тревожному событию

Дополнительное реле контроллера можно настроить на срабатывание по тревожному событию. Выключение реле происходит по разному в разных контроллерах:

- У всех контроллеров (кроме NC-32K.M) реле выключается, как только охранный датчик возвращается в нормальное состояние (тревожное событие прекращается);
- У NC-32K.M для выключения дополнительного реле необходимо либо поднести к считывателю контроллера карту с привилегией "Прием тревоги", либо оператору принять тревогу через консоль "Монитор событий". В данном случае состояние охранного датчика не влияет на выключение дополнительного реле.

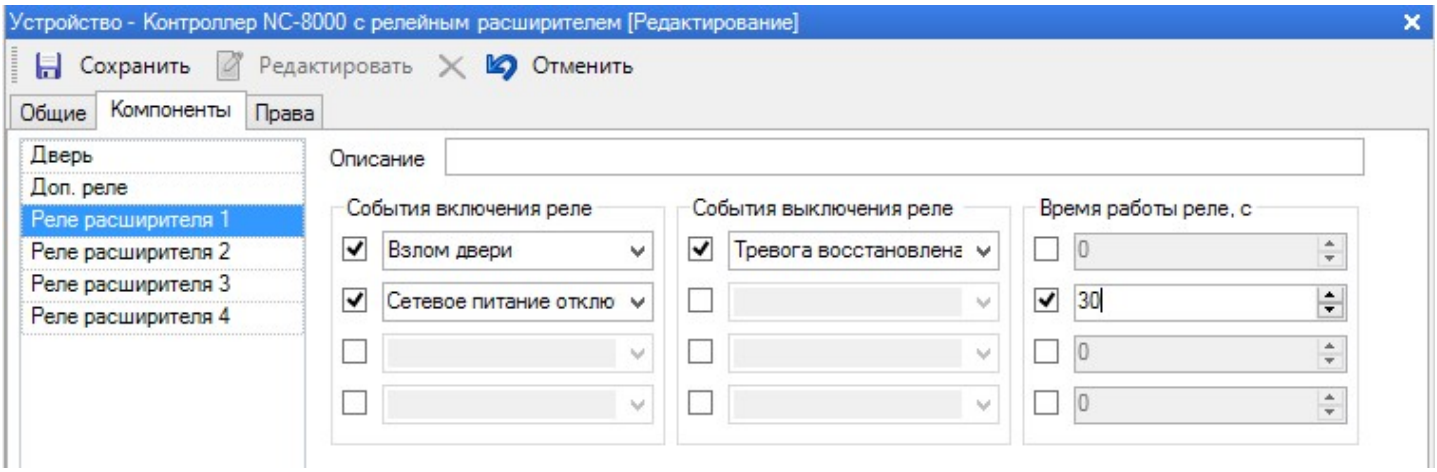
Примечание: у NC-100K-IP нет охранных функций.

8.1.2.10 Настройка релейного расширителя NMO-04

К контроллерам NC-8000 (-D, -I) и NC-60K/NC-60K.M можно подключить релейный расширитель NMO-04.

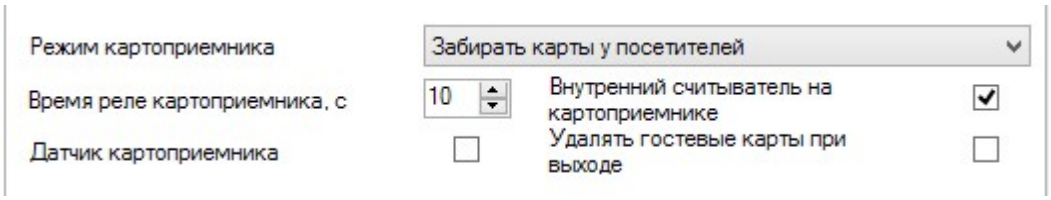
Функционал контроллера с релейным расширителем позволяет настроить включение и/или выключение каждого из реле расширителя. Для этого у нужных реле активируйте поля включения и/или выключения, установив слева от них флажки. Затем из раскрывающихся списков выберите событие, которое будет приводить к включению, а также выключению реле.

Кроме выключения реле по событию, его также можно выключить по истечению заданного времени работы.

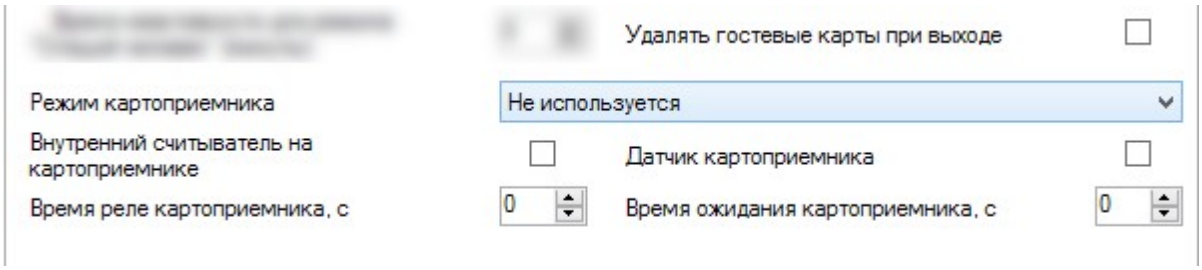


8.1.2.11 Настройки картоприемника

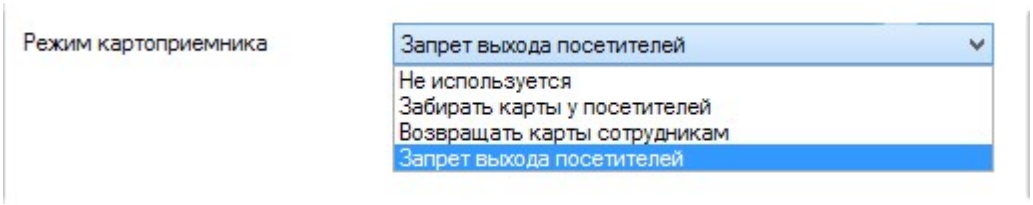
Картоприемник можно использовать только с контроллерами NC-32K, NC-60K/NC-60K.M и NC-100K.



Настройки картоприемника в карточке контроллера NC-100K-IP



Настройки картоприемника у контроллера NC-60K.M



Выбор режима работы картоприемника у контроллера NC-32K

Ниже приведена сводная таблица настроек картоприемников:

Параметр	Описание
Внутренний считыватель на картоприемнике	Флажок устанавливается, если для работы картоприемника используется считыватель на выход, как, например, в турникете Perco TBC-01 (не имеющем встроенного считывателя). При этом обязательно использование датчика картоприемника.
Время ожидания картоприемника	У контроллера NC-60K/NC-60K.M это величина задержки, с которой картоприемник будет забирать либо возвращать карту сотруднику. Работает только при установленном флажке *Датчик картоприемника*. При отсутствии датчика или значении "0" забор/возврат карты осуществляется без задержки. У контроллера NC-100K это время всегда равно 5 сек.
Время реле картоприемника	Время, на которое включается реле картоприемника при заборе карты у посетителя. Задать время вручную можно только у NC-60K.M.
Датчик картоприемника	Флажок может устанавливаться для картоприемников, оборудованных таким датчиком. Распознает наличие карты в приемном бункере.
Режим картоприемника	
Не используется	Стандартный режим. Контроллер использует один или два считывателя (устанавливается в конфигурации контроллера) и может обслуживать стандартную дверь или турникет. Тип карты (гость или постоянный сотрудник) в этом случае значения не имеет.
Забирать карты у посетителей	Для картоприемников, которые забирают только карты определенной категории. В этом режиме при опускании гостевой карты в щель картоприемника она будет забрана, а карта сотрудника - нет.
Возвращать карты сотрудникам	Для картоприемников, которые забирают все карты. В данном режиме карта сотрудника будет вытолкнута обратно, а карта гостя помещена в

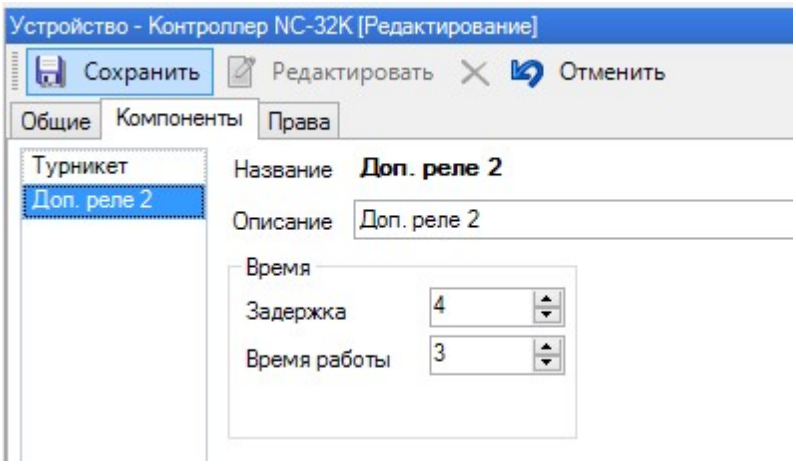
накопитель.

Запрет выхода посетителей Только для NC-32K.M. Выход посетителя с гостевой картой запрещен. Формируется транзакция "Выход запрещен - гостевая карта".

Удалять гостевые карты при выходе Установленный флажок значит, что контроллер будет самостоятельно удалять идентификатор карты с привилегией "Гостевая карта" из БД контроллера. После этого его можно использовать снова.
Если идентификатор гостевой карты не удалить из БД контроллера, работающего в режиме offline, то по ней можно будет снова получить доступ.

После того, как картоприемник забрал карту у посетителя, сервер удаляет идентификатор из системы, независимо от состояния флажка "Удалять гостевые карты при выходе". После этого карта готова для дальнейшего использования.

При работе контроллеров NC-32K.M/NC-32K-IP с картоприемником вкладка *Доп.реле 2* меняет свой вид и отображает настройки реле картоприемника:



8.1.2.12 Настройка группового прохода

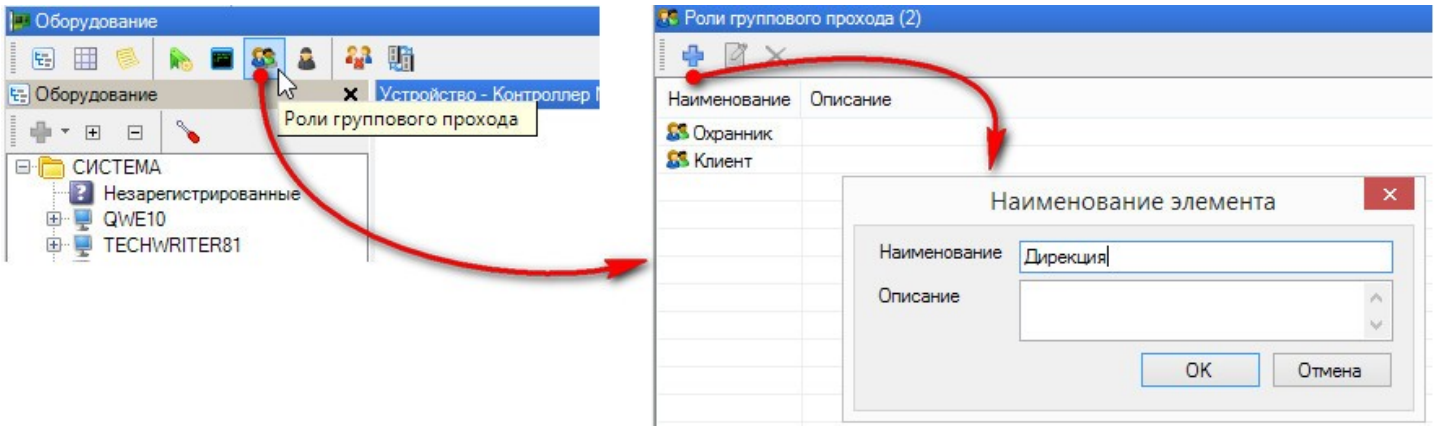
Режим доступен только для контроллеров NC-8000 и NC-60K/NC-60K.M.

Режим недоступен при включенной функции контроллера "Использовать индивидуальные счетчики проходов".

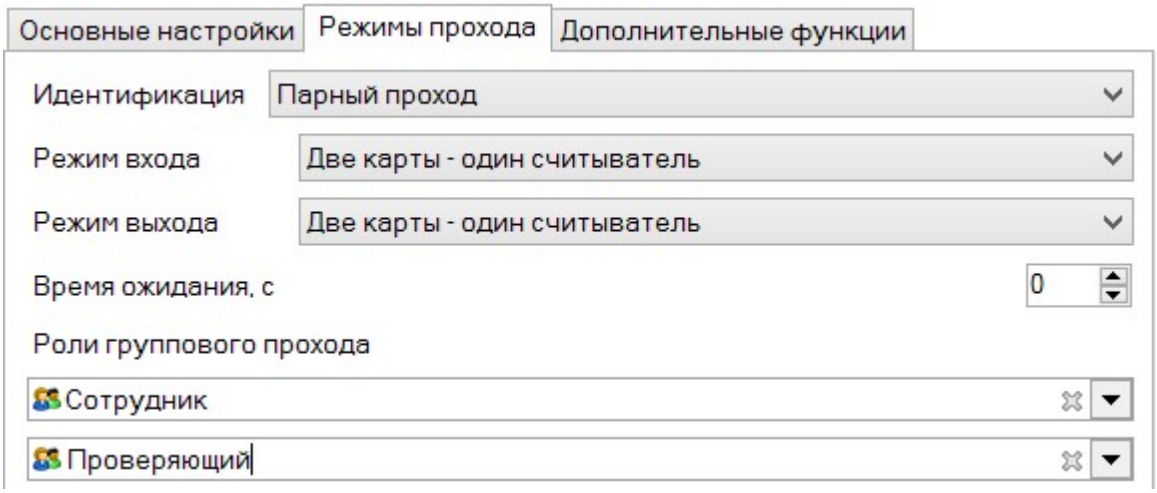
Групповой проход могут осуществлять только те лица, у которых в карточке персоны[261] установлен флажок *Групповой проход* и выбрана групповая роль.

Для настройки группового прохода выполните следующие действия:

1. В редакторе оборудования нажмите на кнопку *Роли группового прохода*. Откроется одноименное окно;
2. В окне ролей группового прохода нажмите на кнопку *(Создать)*. Откроется форма создания новой роли;
3. Введите наименование и, при необходимости, описание новой роли группового прохода, после чего нажмите на кнопку *ОК*:



4. Повторяя шаги 2 и 3, создайте необходимые для группового прохода роли.
5. В Редакторе оборудования выберите контроллер NC-8000 или NC-60K/NC-60K.M и перейдите на вкладку *Компоненты* на карточке устройства;
6. Перейдите в режим редактирования, нажав на кнопку (Редактировать) на панели инструментов карточки устройства;
7. Перейдите на вкладку *Режимы прохода* и выберите один из режимов:
   - "Парный проход" - система включит обоих прошедших субъектов доступа в списки антипассбэка и сформирует сообщения о проходе двух пользователей;
   - "Проход с разрешением" - в системе будет учитываться только первый приложивший карту пользователь. Если при этом на территорию (в помещение) зайдут оба, то возможны ошибки в работе, например, система посчитает, что из помещения вышли все люди и попытается поставить помещение на охрану. Но неучтенный пользователь в этом помещении вызовет тревогу.



8. Задайте направление, в котором будет требоваться проход по 2 картам:
   - *Вход и выход* - в этом режиме как для входа, так и для выхода требуется поднести две карты (с опциональным вводом ПИН-кода) к одному и тому же считывателю соответственно на вход и на выход;
   - *Вход (2 считывателя)* - для входа необходимо поднести две карты (с опциональным вводом ПИН-кода) к двум разнесенным считывателям (чтобы не допустить поднесение двух карт одним человеком). Выход осуществляется по кнопке запроса на выход (у NC-8000), EXIT у NC-60K, IN7 у NC-60K.M;
   - *Выход (2 считывателя)* - для выхода необходимо поднести две карты (с опциональным вводом ПИН-кода) к двум разнесенным считывателям, установленным на выход.

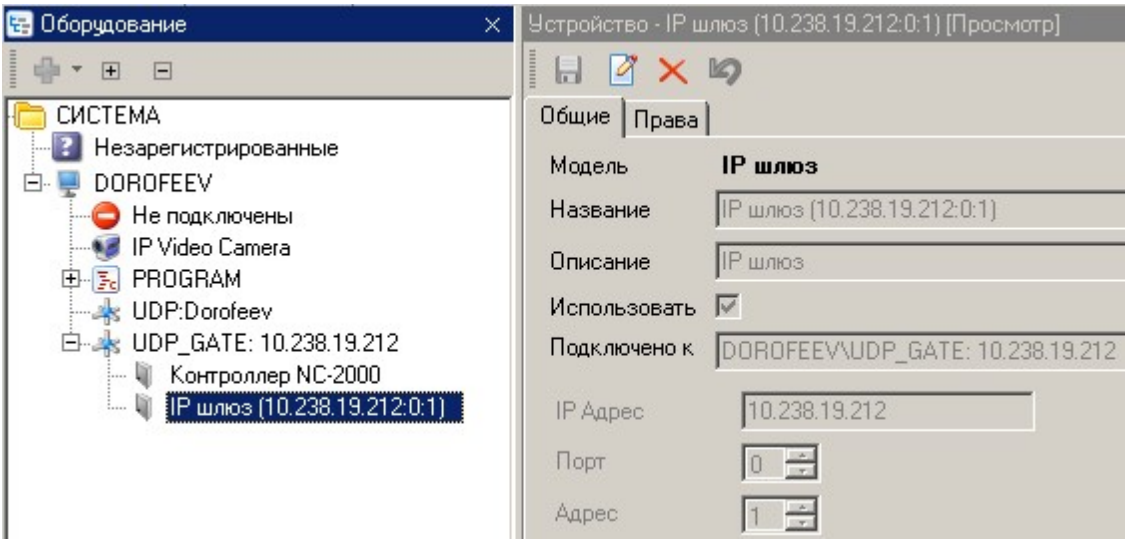
   Во всех случаях контроллер фиксирует групповой проход. При задействовании двух считывателей в карточке контроллера должны быть установлены флажки *Считыватель на вход* и *Считыватель на выход.*

В режимах "Вход (2 считывателя)" и "Выход (2 считывателя)" сигналы от любых двух считывателей (независимо от варианта их подключения к контроллеру или режима, установленного посредством утилиты PNR_Tune) будут интерпретироваться Системой как сигналы соответственно на вход и на выход.

9. В поле *Время ожидания* задайте максимальное время между поднесениями карт к считывателю(-ям);
10. Выберите из раскрывающихся списков роли для доступа. Обязательно выберите обе роли, иначе настройки сохранены не будут и групповой проход функционировать не будет;
11. По завершении сохраните сделанные в настройках контроллера изменения.

8.1.3 Настройка IP-шлюзов

Параметры шлюзов отображаются в Редакторе оборудования[62] в карточке конкретного шлюза.



На вкладке *Общие* отображаются параметры шлюза, которые устанавливаются автоматически при добавлении шлюза в систему.

На вкладке *Права* можно выбрать организации, которые смогут работать с данным шлюзом: просматривать статус в редакторе топологии.

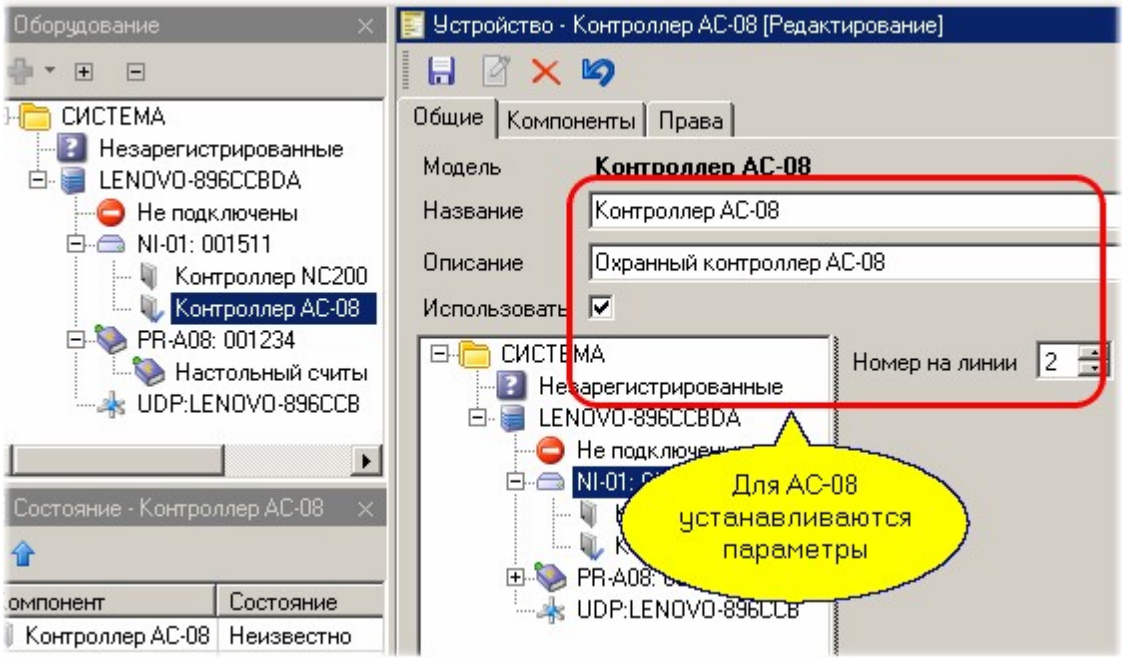
За более подробной информацией обращайтесь к документации на конкретную модели устройства.

8.1.4 Настройка охранных контроллеров

Общие положения

Подсистема охраной сигнализации ***Parsec*** работает с охранными контроллерами AC-08. К охранному контроллеру можно подключить до 16 охранных зон (8 на контроллере и 8 на зонном расширителе). Основные операции (постановка на охрану, снятие с охраны) производятся с охранными областями, к которым может быть приписано от 1 до 16 охранных зон.

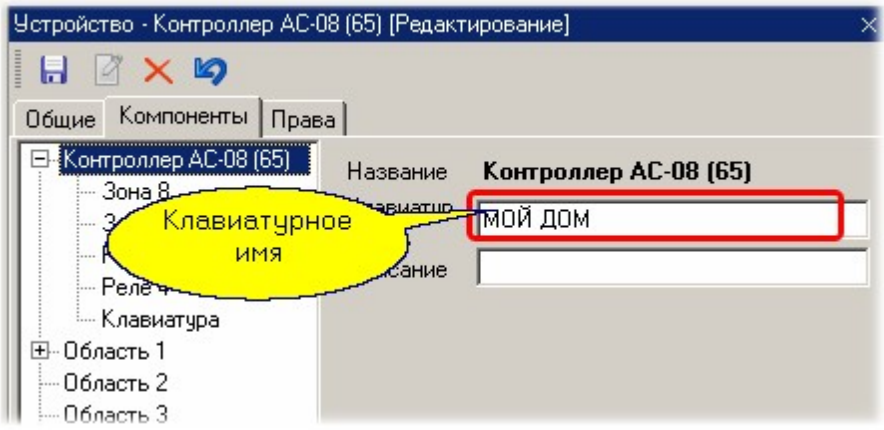
При настройке контроллера устанавливаются следующие параметры:



- *Название*. Данное поле задает название, под которым данный охранный контроллер будет фигурировать в системе. Выберите подходящее название длиной не более 31 символа.
- *Описание*. Это поле не является обязательным и служит как справочное для установщика или администратора системы.
- *Линия*. В случае использования IP-шлюз, в этом поле выбирается номер линии шлюза (значение от 1 до 4), к которой подключен данный контроллер.
- *Использовать*. Включает или выключает опрос контроллера системой.
- *Номер на линии*. Задает адрес контроллера на линии RS-485, к которой подключен данный контроллер.

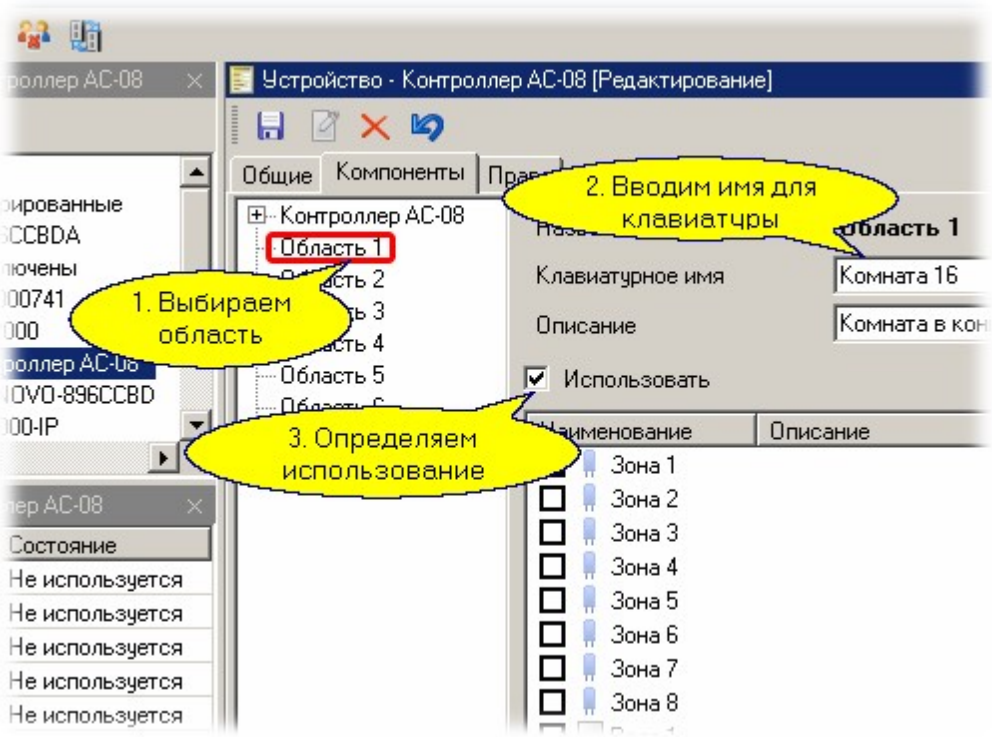
Имя системы на клавиатуре

При использовании клавиатуры в дежурном режиме на ее дисплее отображается название системы (или объекта охраны). Для изменения этого названия следует на вкладке *Компоненты* карточки контроллера выбрать сам контроллер и в режиме редактирования ввести имя, которое будет отображаться на клавиатуре, как показано на рисунке ниже:



Конфигурирование областей

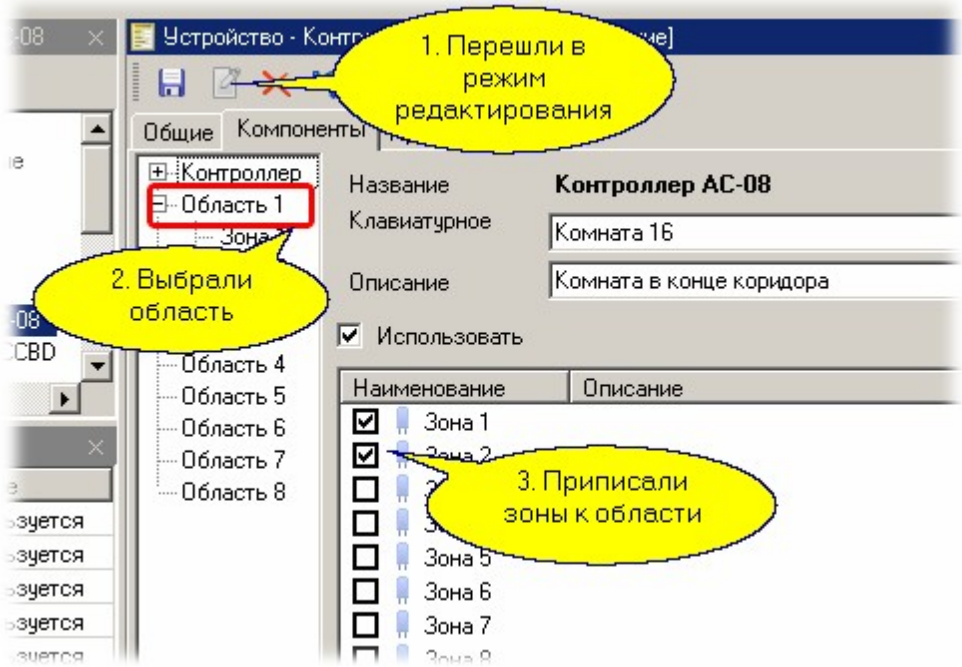
1. Изначально все восемь охранных областей контроллера установлены в состояние "Использовать". Для редактирования настроек охранных областей надо перейти на закладку Компоненты и последовательно сконфигурировать все требуемые области. Неиспользуемые области следует отключить, сняв флажок *Использовать*.



Клавиатурное имя позволяет ввести название области, которое будет отображаться на подключенной к контроллеру клавиатуре.

Не забудьте сохранить выбранные параметры!

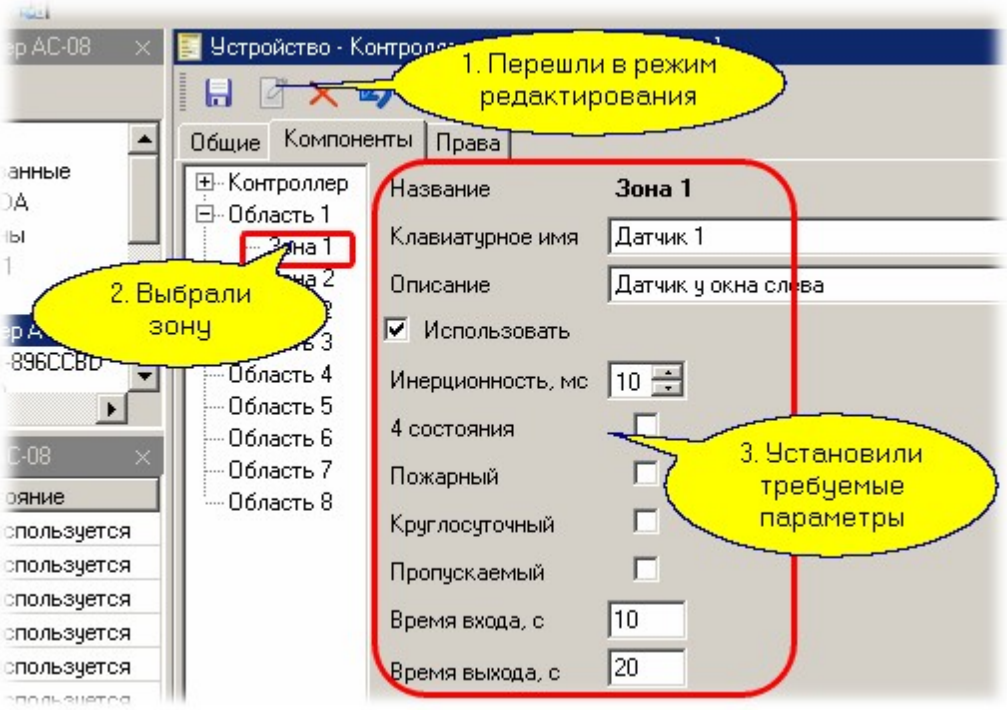
2. К каждой области следует приписать от одной до восьми охранных зон, которые будут работать в составе этой области. Ниже для примера мы приписали первую и вторую зоны к первой области:



Не забудьте сохранить выбранные параметры!

Аналогично следует распределить остальные зоны, если это необходимо.

3. Далее для всех зон следует установить требуемые параметры в соответствии с типом датчиков, типом шлейфа датчиков и требованиями по инерционности срабатывания зоны:



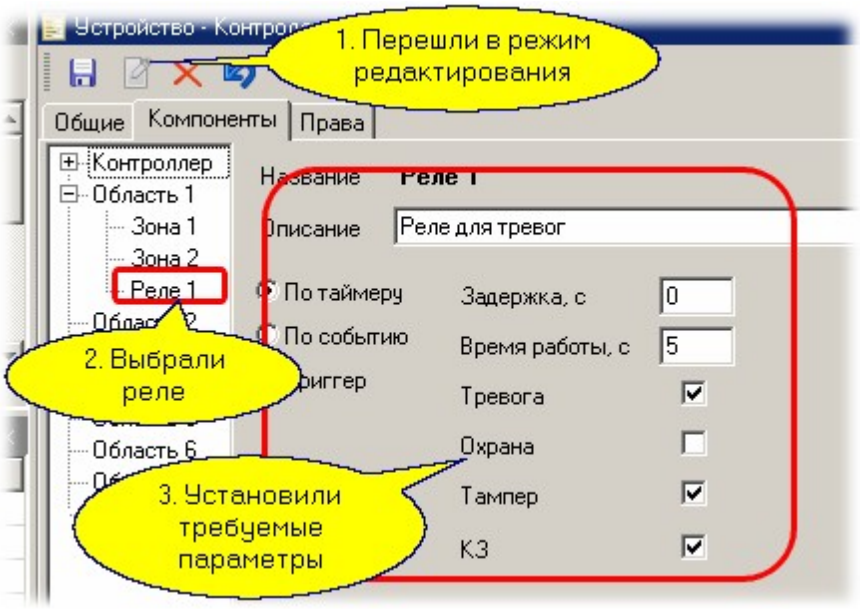
Не забудьте сохранить выбранные параметры!

Имеется возможность настроить следующие параметры охранной зоны:

- *Клавиатурное имя*. Название зоны, которое будет отображаться на дисплее клавиатуры.
- *Использовать*. Если флажок не установлен, то контроллер не будет следить за данной зоной.

- *Инерционность*. Время, в течение которого датчик должен быть в сработавшем состоянии, чтобы контроллер зафиксировал тревогу в зоне.
- *4 состояния*. Для шлейфа с контролем четырех состояний (с нагрузочными резисторами).
- *Пожарный*. Определяет тип тревоги от датчика. В данной версии контроллеров не используется.
- *Круглосуточный*. При установке данного флажка датчик генерирует сигнал тревоги даже если область, в которую он включен, в это время не на охране (например, датчик разбития стекла).
- *Пропускаемый*. При установке данного атрибута неисправный датчик при постановке на охрану может быть автоматически пропущен (исключен из охраны до следующей постановки).
- *Время выхода, Время входа*. Эти параметры определяют задержку постановки на охрану и задержку подачи сигнала тревоги соответственно.

4. К каждой области можно приписать реле контроллера (от одного до 4 или восьми: четыре на плате контроллера и четыре на плате релейного расширителя). Каждое реле, в отличие от зоны, может быть приписано более чем к одной области. Реле назначается области так же, как и зона (см. выше).
5. Если реле используется, то необходимо настроить его параметры как показано ниже:



Не забудьте сохранить выбранные параметры! А настроить можно следующее:

- *По таймеру, По событию, Триггер*. Определяет алгоритм, по которому будет включаться реле. По таймеру - выбранное событие (или несколько событий) запускает сначала отсчет времени задержки, а по истечении задержки реле включается на заданное время. По событию - реле работает в течение времени, пока существует заданное событие (например, охрана). Триггерный режим переводит реле в противоположное состояние при каждом приходе выбранных событий.
- *Задержка*. Определяет время задержки до включения реле при режиме "По таймеру".
- *Время работы*. Определяет время работы реле до выключения при режиме "По таймеру".
- *Тревога*, *Охрана*, *Тампер* (вскрытие корпуса или обрыв шлейфа), *КЗ* (короткое замыкание шлейфа) - события, при наступлении которых должно сработать реле.

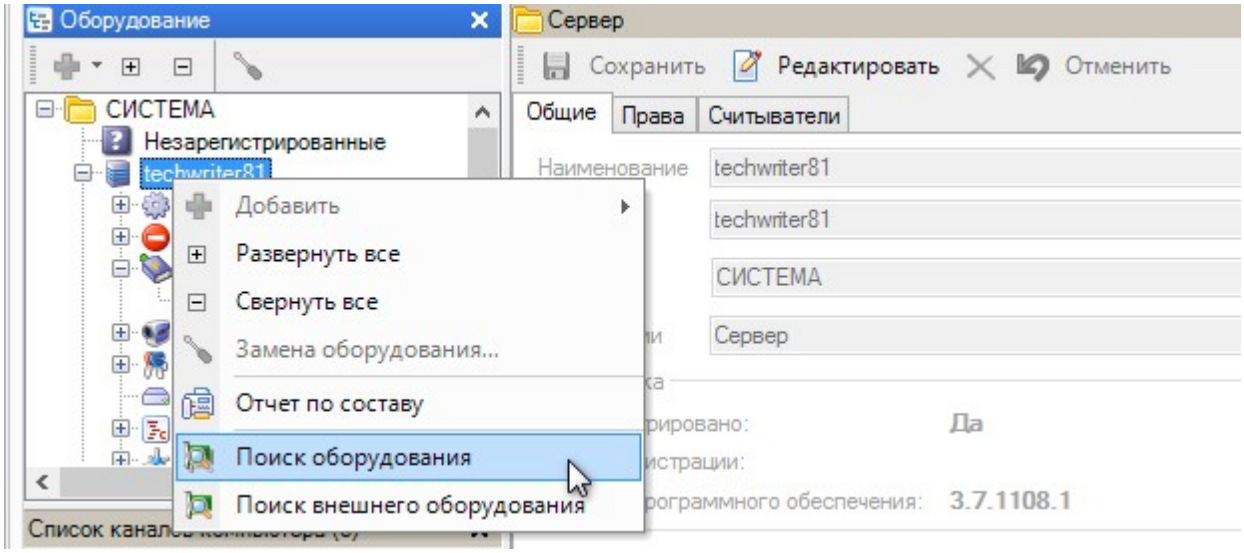
8.1.5 Настольные считыватели

Настольный считыватель используется в двух случаях:

1. Для ввода кодов карт доступа при создании или редактировании персонала системы;
2. Для входа оператора в систему, если при создании оператора ему была присвоена карта.

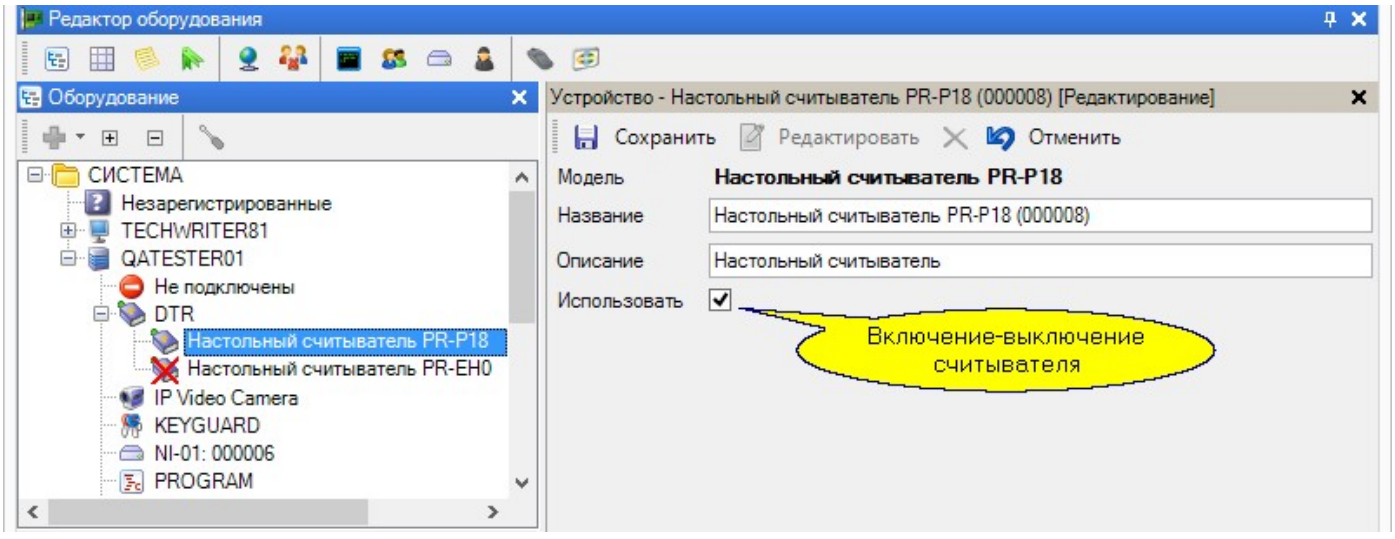
Система предоставляет возможность использования настольных считывателей для имитации входов и выходов (например, для системы учета рабочего времени). Для этого необходимо использовать настольные считыватели как источники кодов карт для программного контроллера SCL-02.

Стандартные настольные считыватели определяются системой и добавляются в систему автоматически либо по команде поиска оборудования, которая доступна при выборе в дереве оборудования компьютера (сервера или рабочей станции):



В дереве оборудования настольный считыватель представлен своим USB каналом и непосредственно считывателем, как показано на рисунке ниже (канал *DTR*).

После того, как считыватели найдены, в карточке оборудования можно подключать или отключать каждый считыватель в зависимости от ваших потребностей. По-умолчанию найденный считыватель ставится в активное состояние (установлен флажок *Использовать*).



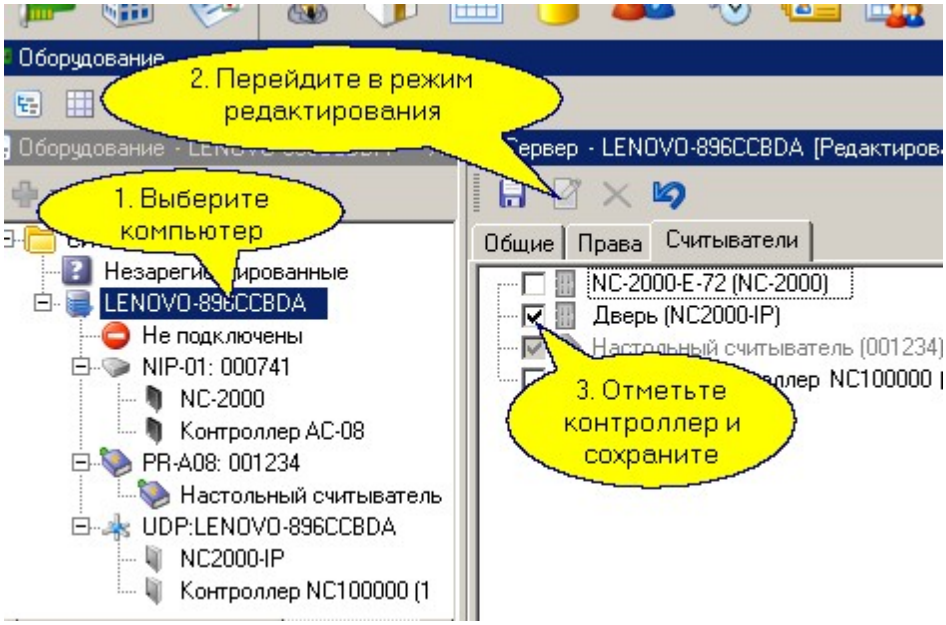
Настройки считывателей описаны в разделах далее.

Работа без настольного считывателя

Система ParsecNET 3 позволяет вводить коды карт и при отсутствии настольного считывателя. В этом случае роль считывателя может выполнять настенный считыватель точки прохода (считыватель одного из контроллеров доступа, подключенных к данному ПК).

Для того, чтобы считыватель контроллера работал и как настольный считыватель системы, в редакторе оборудования необходимо проделать следующие операции:

- Выделить компьютер, с контроллера которого мы хотим получать коды карт при работе с персоналом;
- На панели карточки компьютера открыть закладку *Считыватели* (рисунок ниже);
- Перейти в режим редактирования и отметить тот контроллер (точнее, дверь того контроллера), откуда мы будем вводить коды карт:

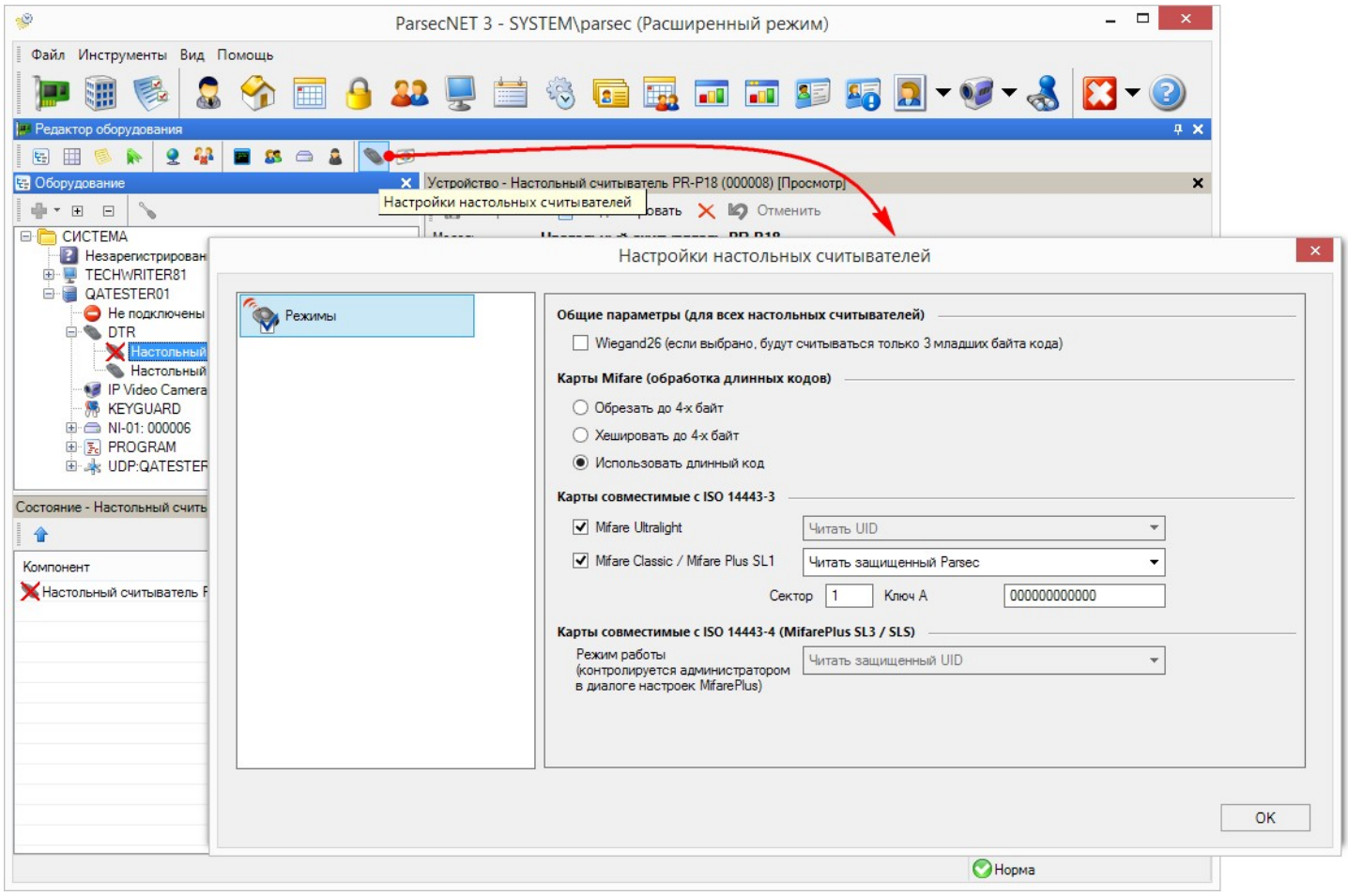


Вы можете одновременно использовать и настольный считыватель, и считыватель на двери, если это необходимо.

Если настенные считыватели подключены к контроллеру NC-100K-IP, то при выборе режимов работы "Идентификация по лицу" и "Идентификация по карте с верификацией по лицу" считыватели контроллера невозможно использовать в качестве настольных.

8.1.5.1 Настройка настольных считывателей

Настольные считыватели могут работать в нескольких режимах, которые отличаются тем, как интерпретируется считанный код идентификатора. Выбранный режим должен быть таким же, как и у настенных считывателей, используемых на точках прохода (задается при помощи утилиты PNR_Tune). Для перехода к настройкам настольного считывателя нажмите на кнопку *Настройки настольных считывателей*:



Доступны следующие варианты:

Общие параметры (для всех настольных считывателей):

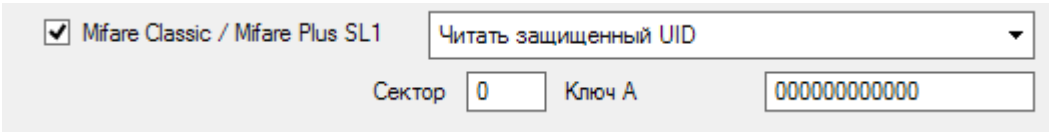
- *Wiegand 26* - при установке этого флажка со считывателя передаются только три младших байта кода карты независимо от длины кода в самой карте. Этот режим необходим, когда к контроллерам подключаются считыватели сторонних производителей через интерфейс NI-TW, и используются только три байта от полного кода карты.

Карты Mifare (обработка длинных кодов):

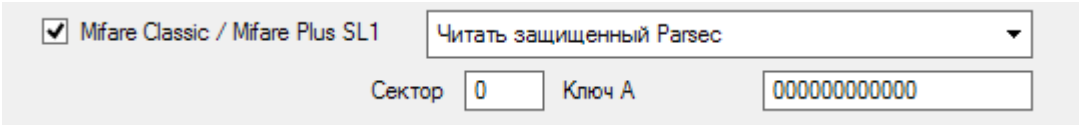
- *Обрезать до 4 байт* - длинный код обрезается до 4 байтов (обрезаются старшие байты);
- *Хэшировать до 4 байт* - длинный код Mifare TypeA при помощи хэш-функции преобразуется в код длиной 4 байта;
- *Использовать длинный код* - оригинальный код карты используется без изменений.

Карты совместимые с ISO 14443-3

- *Mifare Ultralite* - считыватель читает оригинальный незашифрованный UID карты. Поле не имеет возможности выбора;
- *Mifare Classic / Mifare Plus SL1* - считыватель читает код карты в зависимости от выбранного режима:
  - *Читать UID* - в качестве идентификатора используется оригинальный незашифрованный UID карты;
  - *Читать защищенный UID* - в качестве идентификатора используется оригинальный UID карты, который выдается считывателем только после аутентификации по ключу заданного сектора* [125] :



- *Читать защищенный Parsec* - в качестве идентификатора считыватель выдает номер, записанный в один из секторов карты, после аутентификации по ключу этого сектора*[125]:



Карты совместимые с ISO 14443-4 (Mifare Plus (SL3) / SLS). Параметры в этом разделе актуальны для настольных считывателей PR-P18 и PR-X18:

- *Режим работы* - в поле отображается режим работы, выбранный в настройках работы[127] с картами Mifare Plus.

*Если первый сектор карты не инициализирован для работы в защищенном режиме (карта находится в транспортном состоянии или инициализирована для работы другого приложения с сектором 1), то считыватель на такую карту не отреагирует. Секретный ключ доступа – это «пароль» для доступа к считыванию идентификатора карты, хранящегося в защищенном этим ключом секторе карты. Подробнее работа настольных считывателей в защищенном режиме описана в Руководствах по эксплуатации на конкретную модель считывателя.

8.1.5.2 Работа с банковскими картами

СКУД Parsec может использовать для организации контроля доступа банковские карты, совместимые с ISO 14443-4:

- с установленным нефинансовым приложением SLS. Для прохода по таким картам используется режим SLS[127];
- без приложения SLS. Доступ по таким картам может быть организован с чтением UID или чтением защищенного UID[127] (если известны сектор и ключ доступа к нему). Либо с чтением PAN-кода[123], либо кода с телефона с функцией Apple Pay (подробнее о работе с PAN-кодом и Apple Pay смотрите Руководство по эксплуатации утилиты PNR Tune). Код далее преобразуется для использования в качестве идентификатора субъекта доступа. Чтение PAN-кода (кода из Apple Pay) доступно для считывателей PR-P18 и PR-X18.

8.1.6 Работа с картами Mifare Plus

СКУД ParsecNET начиная с версии 3.8 имеет возможность работать с картами Mifare Plus.

Вообще, в системе ParsecNET 3.8 и выше в качестве идентификаторов для доступа могут использоваться следующие типы карт Mifare:

- Карты семейства Mifare Ultralight, которые не поддерживают криптографию;
- Карты семейства Mifare Classic, использующие криптографию Crypto-1 (Mifare ID, Mifare Classic 1K/4K и их разновидности);
- Карты семейства Mifare Plus, поддерживающие криптографию AES. Уровень безопасности SL1 или SL3.

В зависимости от задач, пользователи системы могут использовать на одном объекте несколько типов карт, например, Mifare Plus на SL3 для сотрудников и Mifare Ultralight для посетителей с гостевым уровнем доступа.

Кроме настольных считывателей PR-P18 и PR-X18 поддержка Mifare Plus обеспечивается в настенных считывателях серий PNR-Pxx и PNR-Xxx с версией прошивки 4.0 или выше. Прошивку настенных считывателей до версии 4.0 можно обновить, начиная с версии 3.2.

При эмиссии карт Mifare Plus используется стандарт структуры данных Mifare Application Directory (MAD), что обеспечивает возможность использовать карту для нескольких приложений (например, дополнительно в локальных платежных системах предприятий и для других приложений), а не только в качестве идентификатора доступа.

При использовании карт Mifare Plus в системе ParsecNET возможны следующие варианты:

1. Карты приобретаются не персонализированными (SL0), их полная персонализация осуществляется средствами программного обеспечения СКУД. Наиболее предпочтительный вариант, при котором потребитель может максимально реализовать возможности карты (и не только для применения в СКУД). Карта персонализируется как многофункциональная с применением стандарта MAD (раздел SL0 в SL3[133], перевод SL0 в SL1 средствами Системы не осуществляется);
2. Для СКУД предполагают применить уже используемые карты уровня SL1 - Mifare Classic или Mifare Plus в режиме совместимости с Mifare Classic. В этом случае необходимо запросить и получить у эмитента/производителя карт текущие ключи SL1 (Mifare Classic) и AES от всех секторов карты, а также служебные ключи Mifare AES (SL1 в SL3[136]);
3. У пользователя имеются карты SL3, персонализированные либо с применением стандарта MAD, либо без него. С такими картами ПО ParsecNET может работать только в режиме *Чтение защищенного UID*. Для этого требуется знание ключа доступа на чтение сектора карты, который используется для аутентификации. Номер сектора и ключ необходимо запросить и получить у эмитента/производителя карт. В качестве идентификатора в этом режиме применяется только UID карты (Работа с SL3[140]).

В первом и втором вариантах возможно применение в качестве идентификатора пользователя не только оригинального UID карты, но и идентификатора, заносимого в сектор карты, выделенного для применения в СКУД. В этом случае идентификаторы генерируются СКУД ParsecNET.

Персонализация карт Mifare Plus в системе ParseNET. Общие сведения



Персонализация карт Mifare Plus (запись данных на карту) возможна только при помощи настольных считывателей PR-P18 и PR-X18.

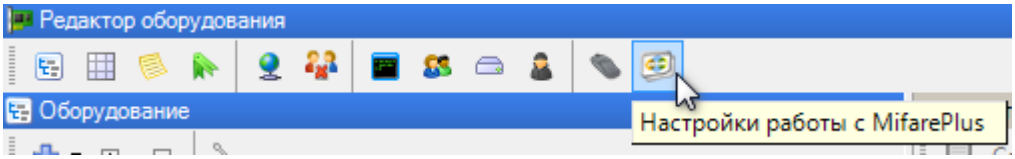
На практике, при использовании карт Mifare Plus мы можем столкнуться как с уже персонализированными кем-то картами (уровня безопасности SL1 или SL3), так и с «чистыми» картами (уровня безопасности SL0), которые необходимо персонализировать:

1. Если выдаваемые пользователям карты уже ранее персонализированы **не** в рамках системы ParsecNET, то Система будет работать с ними, если у них имеются свободные сектора, ключи доступа к которым должны быть предоставлены

администратору системы ParsecNET организацией, осуществившей эмиссию этих карт. Работа с такими картами описана в разделах SL1 в SL3[136] и Работа с SL3[140].

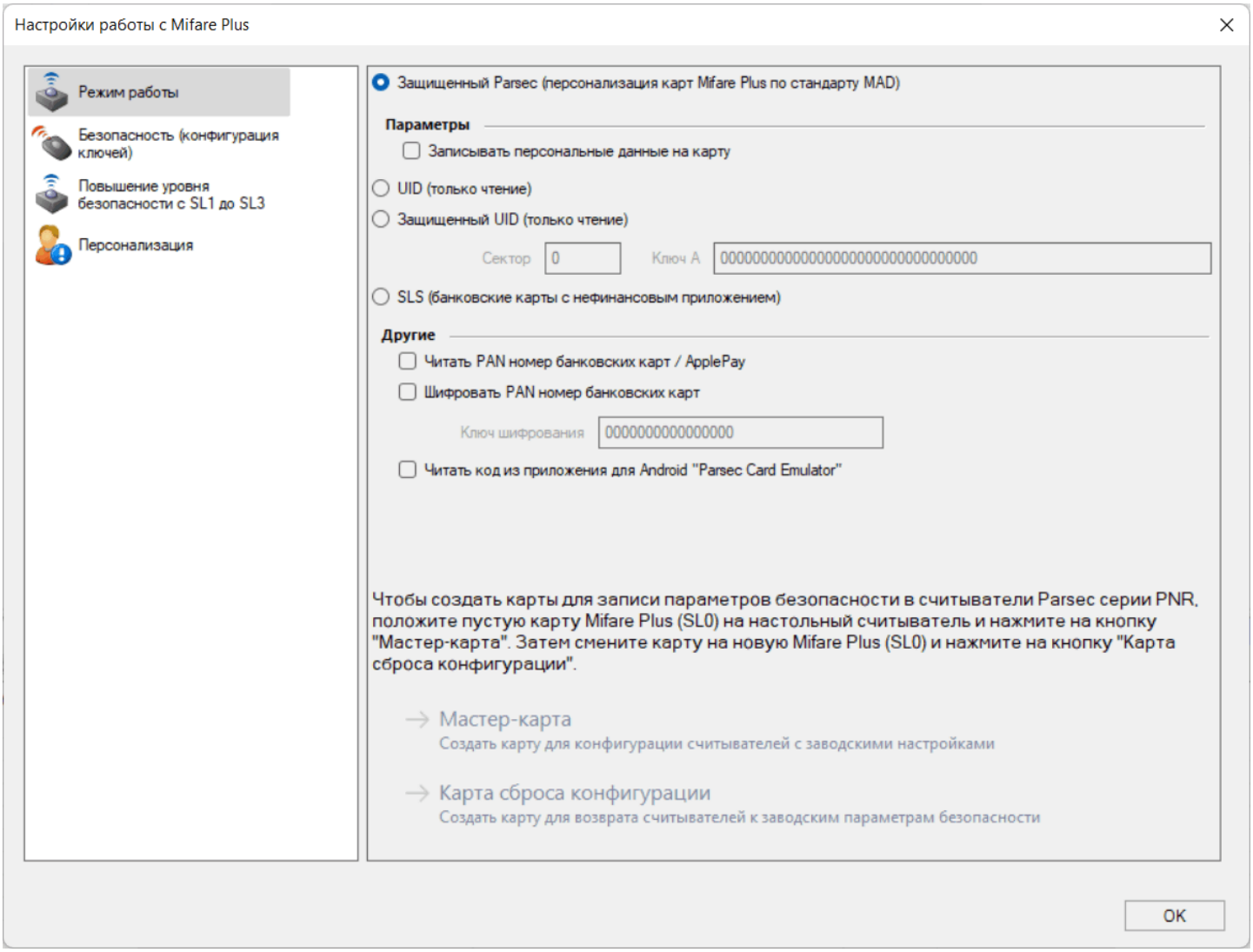
2. Если пользователям будут выдаваться новые (чистые) карты, то для настройки их персонализации используется методика, приведенная в разделе SL0 в SL3[133].

Окно настроек для работы с картами Mifare Plus открывается нажатием на кнопку *Настройки работы с Mifare Plus*:



Ниже приведены описания элементов разделов окна. При первом запуске, когда конфигурация ключей безопасности еще не создана, отображаются только два раздела *Режимы работы* и *Безопасность (конфигурация ключей)*. Разделы *Повышение уровня безопасности с SL1 на SL3* и *Персонализация* появляются только после создания конфигурации и сохранения изменений кнопкой *OK*.

В разделе *Режимы работы* можно выбрать режим, в котором настольный считыватель будет работать с картами.



Выбор режима работы с картами производится при помощи 4-позиционного переключателя:

1. *Защищенный Parsec* - режим для выпуска карт SL3, а также для перевода карт SL1 на уровень SL3. Неактивен до тех пор, пока не будет создана конфигурация ключей;
   - *Записывать персональные данные* - если флажок установлен, то при сохранении карточки субъекта доступа после работы с ней на карту записываются его ФИО. В противном случае эти данные не записываются;
2. *UID (только чтение)* - в качестве идентификатора используется оригинальный незашифрованный UID карты;
3. *Защищенный UID* (только чтение) - в качестве идентификатора используется оригинальный UID карты, который выдается считывателем только после аутентификации по ключу заданного сектора;
4. *SLS (банковские карты с нефинансовым приложением)* - режим для банковских карт, на которые установлено приложение от фирмы SmartLab Solutions, позволяющее использовать их в качестве доступных карт.
5. Другие:
   - *Читать PAN номер банковских карт / Apple Pay* - чтение PAN номера любых банковских карт или с телефона с функцией Apple Pay. Код далее преобразуется для использования в качестве идентификатора субъекта доступа;
   - *Шифровать PAN номер банковских карт* - PAN номер кодируется ключом шифрования и результат используется в качестве идентификатора (длиной 8 байт) субъекта доступа. В настоящее время для использования данной функции необходимы настольный считыватель PR-X18 и контроллер NC-60K/NC-60K.M с подключенными считывателями PNR-P19.S.
   - Ключ шифрования - 10- или 16-ричный код, используемый для шифрования PAN номера банковских карт. Вводится вручную;
   - *Читать код из приложения для Android "Parsec Card Emulator"* - режим чтения карт, эмулированных мобильным приложением Parsec Card Emulator для платформы Android, установленным на устройстве с NFC-модулем.



После смены режима, необходимо сохранить сделанные изменения в Системе нажав на кнопку *ОК*. Окно при этом закроется.

Кроме этого в данном разделе находятся кнопки, которые становятся активными после того, как на считыватель была помещена карта:

- *Мастер-карта* - создается карта, используемая для занесения в настенные считыватели серий PNR-Pxx и PNR-Xxx ключей проходных карт, заданных в разделе *Безопасность*. Настенный считыватель должен предварительно быть переведен в режим работы с Mifare Plus при помощи утилиты PNR_Tune (либо при помощи созданной в PNR_Tune технологической карты).
  Использование мастер-карты с иными настройками безопасности возможно только после возврата считывателя к заводским настройкам безопасности;
- *Карта сброса конфигурации* - создается карта, при помощи которой можно вернуть считыватель из текущей конфигурации SL3 к заводской (в считыватель будут записаны транспортные ключи). Также к заводским (транспортным) ключам настенные считыватели серий PNR-Pxx и PNR-Xxx можно сбросить аппаратно (см. Руководство по эксплуатации на эти устройства).



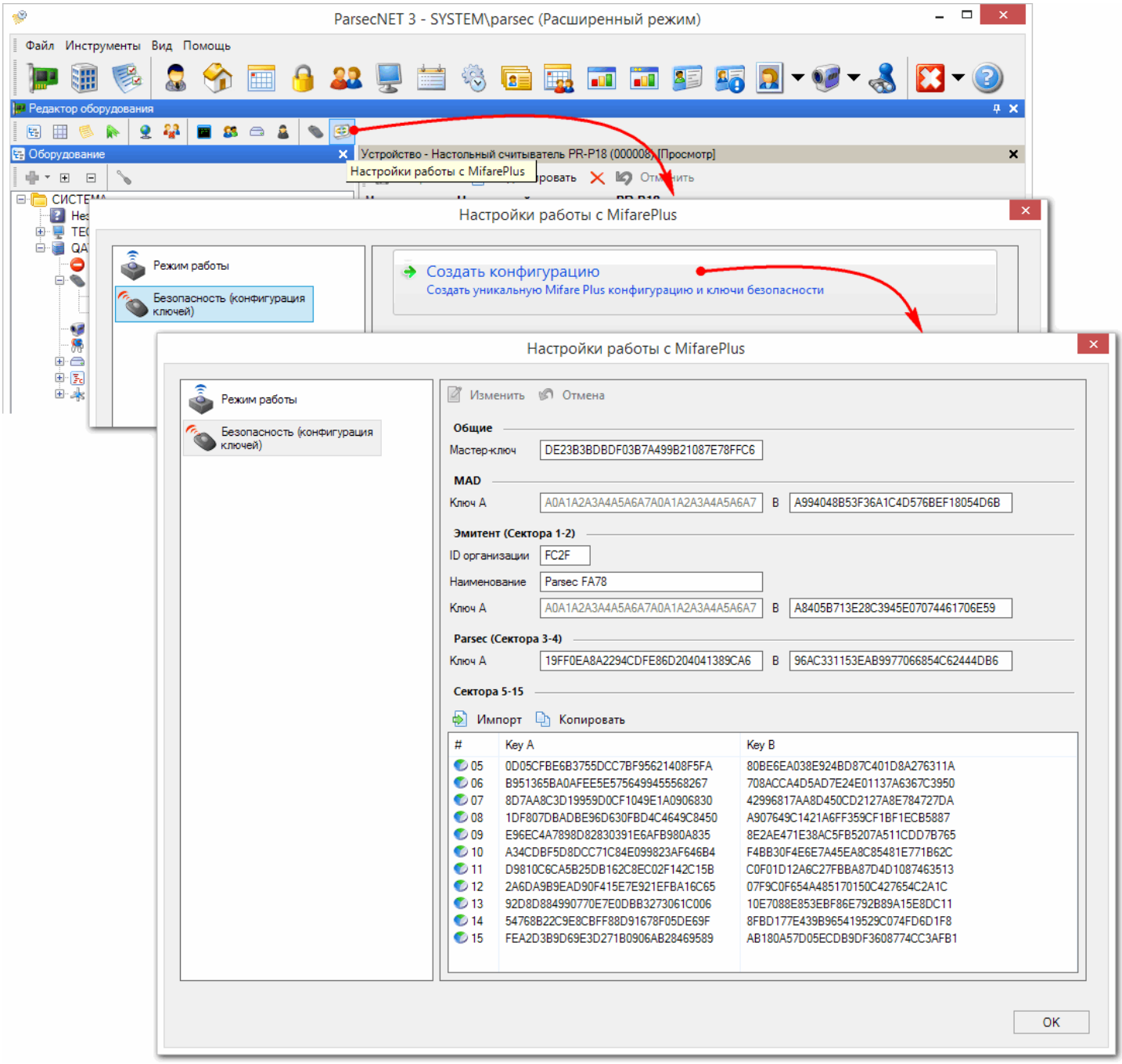
Настоятельно рекомендуется создавать сразу пару карт: Мастер-карту и Карту сброса конфигурации. Это позволит легко вернуть заводские параметры безопасности считывателя без необходимости аппаратного сброса.

Чтобы создать карты для записи параметров безопасности в считыватели Parsec серии PNR положите пустую карту MifarePlus (SL0) на настольный считыватель и нажмите на кнопку *Мастер-карта*. Затем смените карту на новую MifarePlus (SL0) и нажмите на кнопку *Карта сброса конфигурации*.

Содержимое генерируемых карт зависит от установленного режима работы и заданных параметров безопасности (ключей, номера сектора в режиме Защищенный UID).

Раздел *Безопасность (конфигурация ключей)* содержит сгенерированные ключи, применяющиеся для эмиссии карт Mifare Plus уровня безопасности SL3. Для генерации ключей нажмите на кнопку *Создать конфигурацию*. Система создаст ключи для эмиссии карт Mifare Plus уровня безопасности SL3.

Обратите внимание, данное действие необратимо!



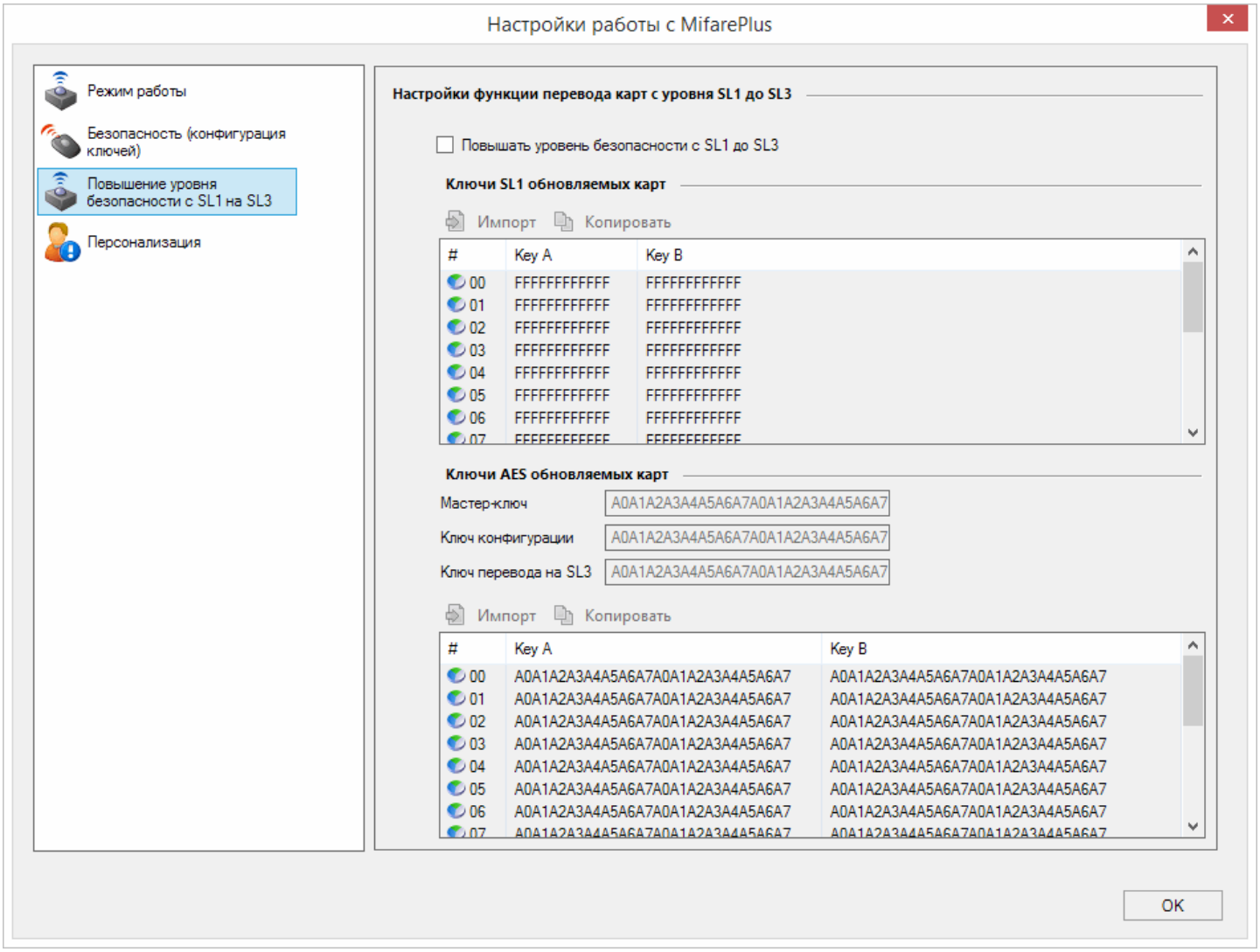
Элементы управления окна:

- Кнопка ***Изменить*** - включает режим редактирования. Поля, доступные для редактирования, становятся активными. **Обратите внимание, редактировать**

данные следует ДО эмиссии карт! Если изменить ключи после эмиссии карт, то выпущенные карты потеряют права доступа и другие возможности;

- Кнопка ***Отмена*** - выход из режима редактирования без сохранения внесенных изменений;
- ***Общие /*** *Мастер-ключ* - ключ, который позволяет перезаписывать информацию в выпущенной ранее карте уровня SL3;
- ***MAD*** - нулевой сектор карты, где находится информация MAD о том, как работать с данными на карте;
  - *Ключ А* позволяет читать данные в нулевом секторе и является фиксированным для всех карт Mifare Plus по всему миру, недоступен для редактирования;
  - *Ключ В* позволяет записывать информацию в нулевой сектор и известен только эмитенту карт, доступен для редактирования.
- ***Эмитент (Сектор 1-2):***
  - *ID организации* - сгенерированный идентификатор организации-владельца (эмитента) карт. Поле доступно для редактирования;
  - *Наименование* - поле содержит наименование эмитента карты, поле доступно для редактирования;
  - *Ключ А* - тот же ключ, что и *MAD ключ А*, открытый фиксированный ключ для чтения информации об эмитенте карты из этих секторов;
  - *Ключ В* - генерируемый эмитентом ключ для записи информации о владельце (из поля *Наименование*) в 1-2 сектора карты, доступен для редактирования.
- ***Parsec (Сектора 3-4)*** - в секторах содержится информация СКУД об идентификаторе доступа, сертифицированном для работы с картами Mifare Plus приложении и другая сопутствующая информация.
  - *Ключ А* и *Ключ В* генерируются эмитентом в момент выпуска карты и предоставляют доступ соответственно к чтению и записи данных в сектора 3 и 4.
- ***Сектора 5-15*** - ключи для чтения и записи сведений в указанные сектора. Может использоваться для записи данных сторонних приложений, например, платежное приложение и тому подобное. Эти ключи можно скопировать и передать, например, из центрального офиса организации в филиал, чтобы идентификаторы, выпускаемые в этом филиале, имели возможность использовать установленное в данных секторах приложение при посещении центрального офиса;
  - Сектора 5 и 6 используются в мастер-картах, которые создаются в разделе *Режим работы* для записи ключей проходных карт в настенные считыватели.

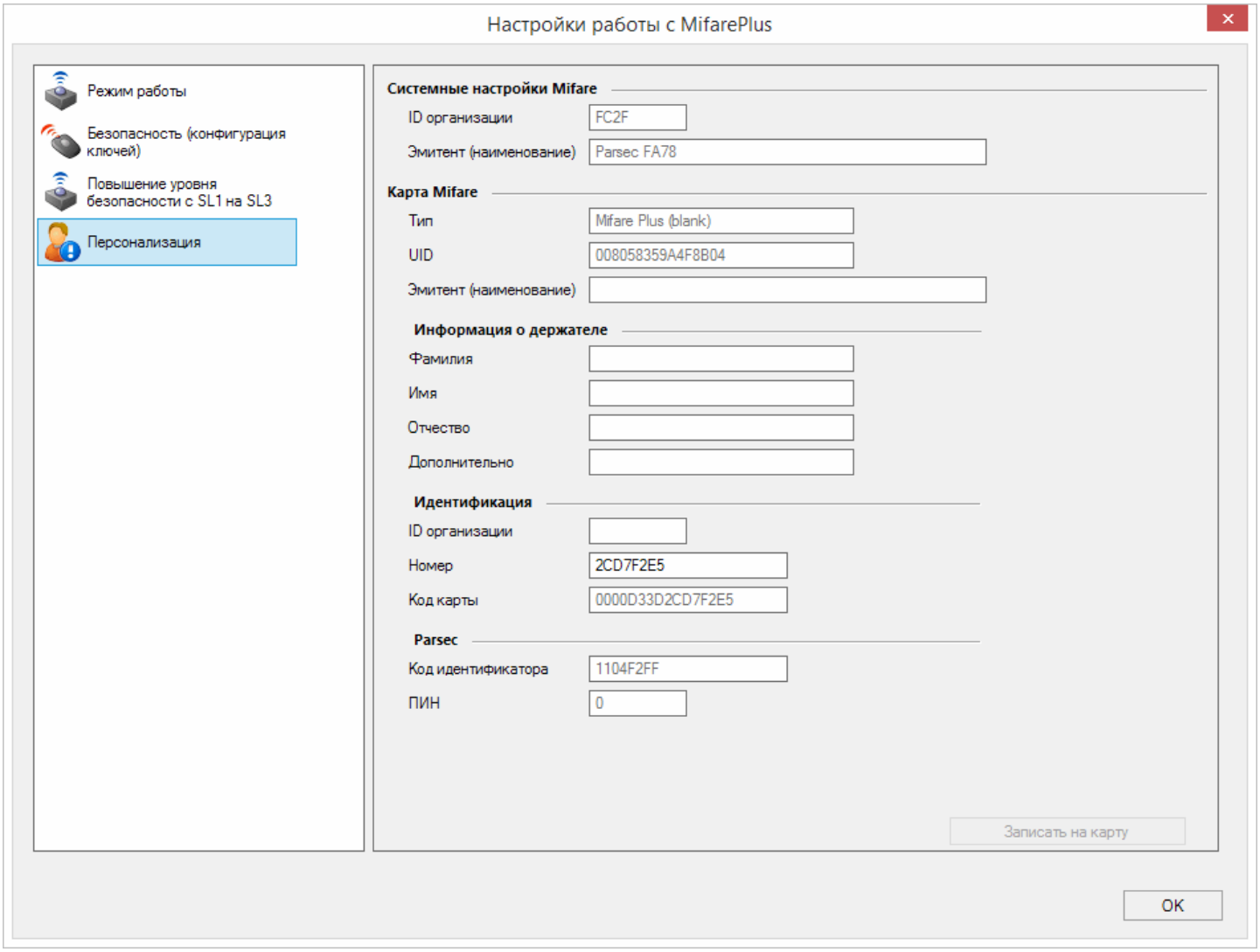
Раздел *Повышение уровня безопасности с SL1 на SL3* содержит ключи, необходимые для перевода карт уровня безопасности SL1 на уровень SL3.



Элементы управления окна:

- *Повышать уровень безопасности с SL1 до SL3* - если флажок установлен, имеются в наличии все ключи SL1 и AES , а также если биты доступа к секторам и ключам установлены подходящим для утилиты SePro 18 образом, то карта уровня безопасности SL1 может быть переведена на уровень SL3 с использованием ключей, сгенерированных в разделе *Безопасность (конфигурация ключей)*;
- Ключи SL1 и AES обновляемых карт необходимо получить у эмитента карт и импортировать в Систему, при помощи кнопок *Импорт* соответствующих панелей окна. *Мастер-ключ*, *Ключ конфигурации* и *Ключ перевода на SL3* вводятся вручную.

В разделе *Персонализация* отображаются данные, считанные с карты. На рисунке ниже показан результат чтения пустой карты Mifare Plus (SL0). Можно изменить сведения в полях, доступных для редактирования и записать новые данные на карту, нажав на кнопку *Записать на карту*. Данный раздел предназначен не для массовой выдачи карт сотрудникам, а для проверки и исправления записанных на ней данных.



Значение некоторых полей:

- ***Системные настройки Mifare*** - текущие настройки, хранящиеся в Parsec:
  - *ID организации* - генерируется случайным образом при создании конфигурации карт Mifare Plus в разделе *Безопасность*. Хранится в 4 секторе карты;
  - *Эмитент (наименование)* - значение из поля *Наименование* в блоке ***Эмитент*** раздела *Безопасность*.
- ***Карта Mifare*** - данные читаются из поднесенной к настольному считывателю карты*:*
  - *Тип* - определенный при чтении тип карты (Ultralight, Classic или Mifare Plus)*;*
  - *UID* - заводской неизменяемый (для оригинальных карт NXP Semiconductors) номер карты;
  - *Эмитент* (наименование) - значение из сектора 1 карты (при персонализации туда записывается значение поля *Наименование* в блоке ***Эмитент*** раздела *Безопасность*).
- ***Информация держателя*** - данные читаются из сектора 2 поднесенной к настольному считывателю карты:
  - *Фамилия*, *Имя*, *Отчество* - в полях на латинице отображается ФИО сотрудника, которому была выдана карта (на рисунке выше данные из не персонализированной карты);
  - *Дополнительно* - в поле можно ввести дополнительную текстовую и цифровую информацию.

- ***Идентификация*** (если карта пустая, то отображаются значения из ПО Parsec):
  - *ID организации* - ID организации-владельца, выпустившей карту (см. выше). Хранится в 4 секторе карты.
  - *Номер* - уникальное для текущего сервера ParsecNET значение (4 байта). Генерируется заново при каждом чтении чистой карты;
  - *Код карты* - генерируемый системой ParsecNET уникальный 8-байтовый идентификатор карты. Старшие 4 байта - значение поля *ID организации*, младшие 4 байта - значение поля *Номер.* Хранится в 4 секторе карты.
- ***Parsec*** (если карта пустая, то отображаются значения из ПО Parsec):
  - *Код идентификатора* - 4-байтовый код, передаваемый считывателем контроллеру после прочтения данной карты. Если флажок *Хэшировать UID 7 байт в 4 байт* в настройках настольных считывателей[123] не установлен, то 7-байтный номер обрезается до 4 байт (обрезаются старшие байты). При установленном флажке 7-байтный код хэшируется до 4-байтов;
  - *ПИН* - ПИН-код, генерируется случайным образом, сохраняется в 4 секторе.

8.1.6.1 SL0 в SL3

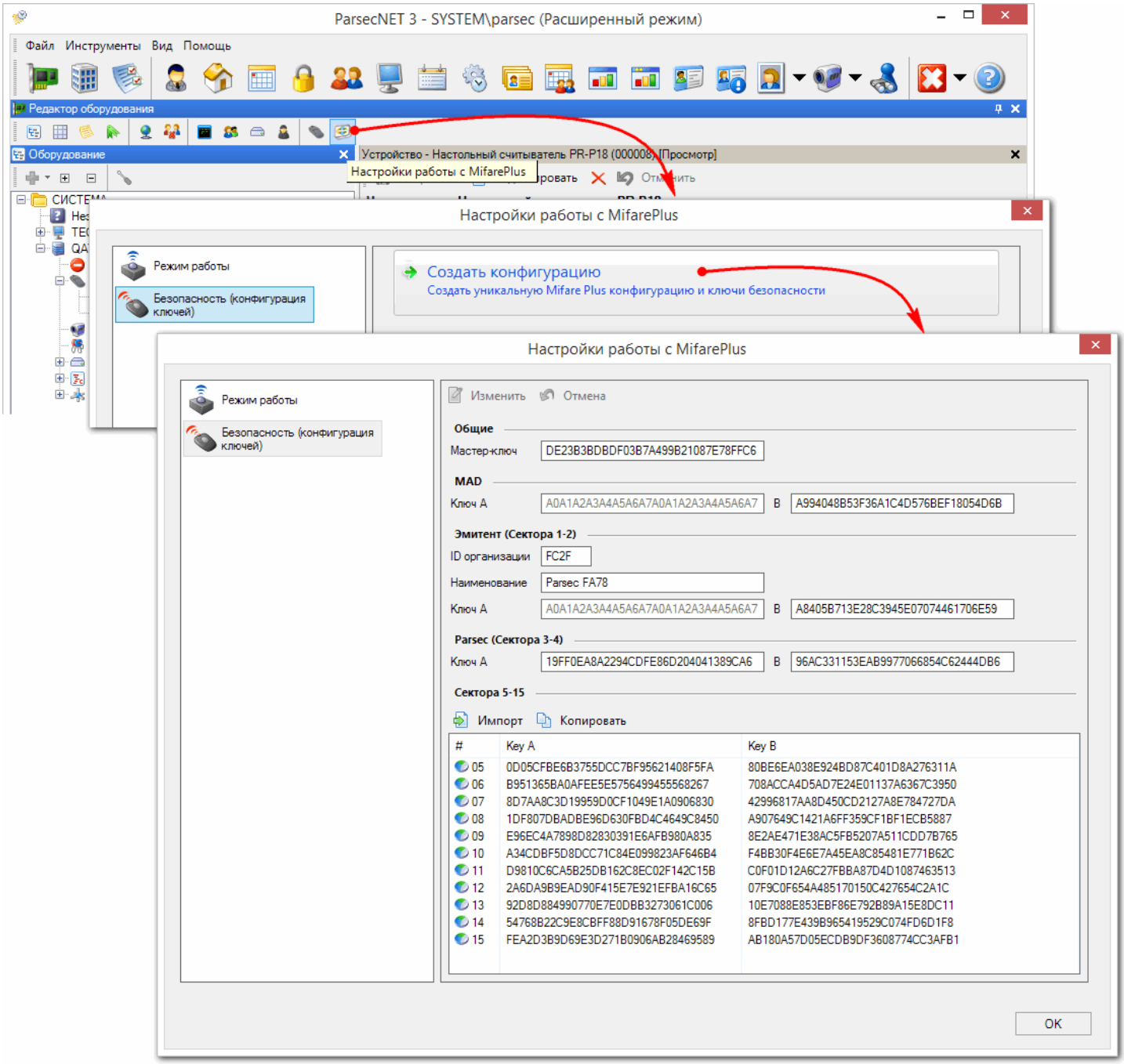
Для выдачи субъектам доступа новых (чистых) карт уровня безопасности SL0, одновременно переводя их на уровень SL3, используется приведенная ниже методика:

1. В *Редакторе оборудования* ParsecNET 3 нажмите на кнопку *Настройки работы с Mifare Plus*.
   Откроется окно настроек, работать можно на любой рабочей станции системы;
2. В разделе *Безопасность (конфигурация ключей)* нажмите на кнопку *Создать конфигурацию.*

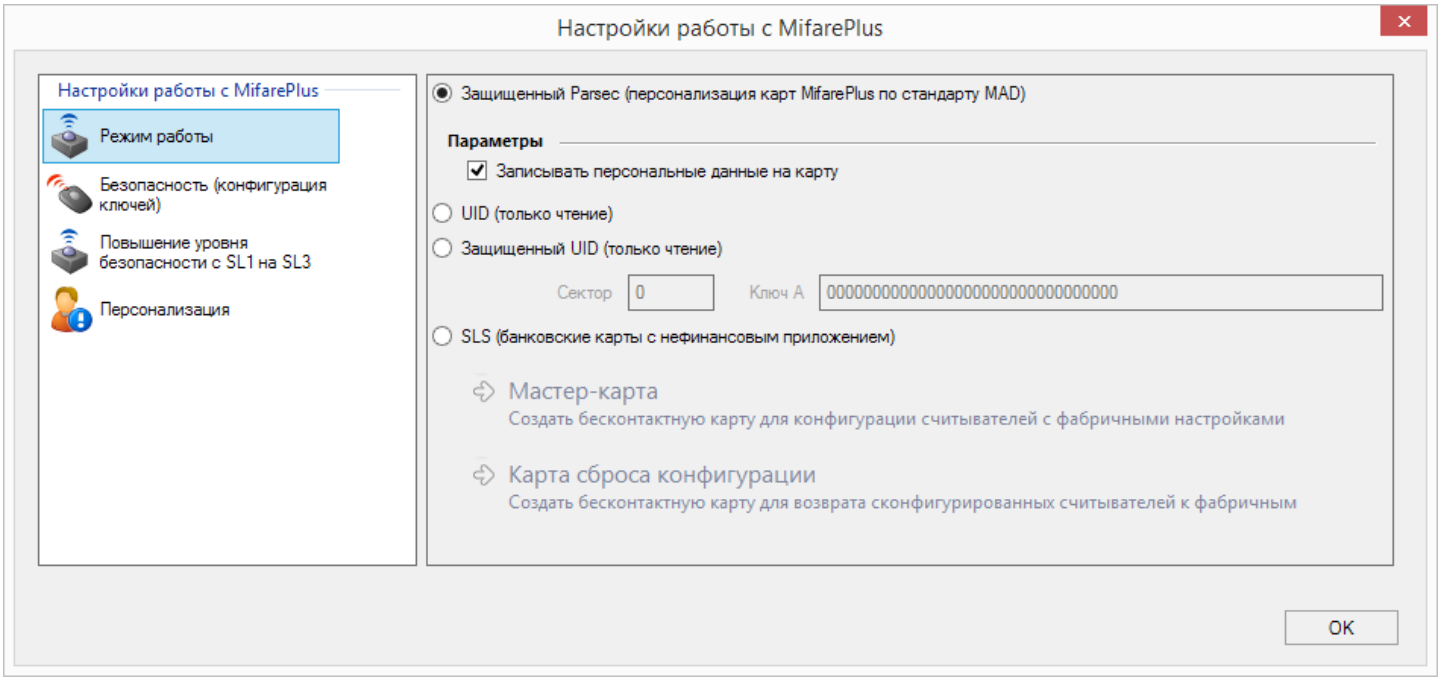


Обратите внимание, данное действие - необратимо! Если после эмиссии карт произвести изменения в этой конфигурации, проход по выпущенным картам будет невозможен.

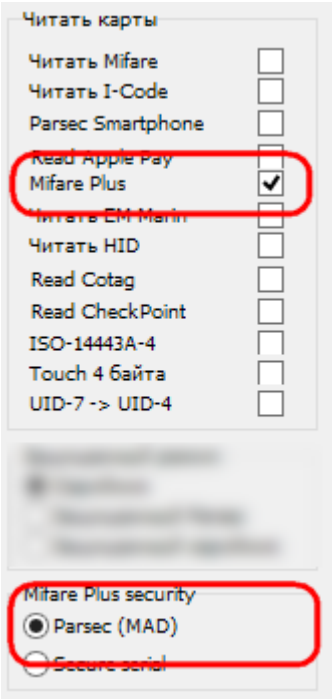
Система сгенерирует ключи для эмиссии карт Mifare Plus уровня безопасности SL3. При первой генерации ключей, окно будет находиться в режиме редактирования, можно будет изменить значения доступных полей. Внесенные изменения сохраняются в Системе при закрытии окна кнопкой *ОК* и при переходе в другой раздел;



3. Если необходимо, отредактируйте поле *ID организации*;
4. Перейдите в раздел *Режим работы* и выберите *Защищенный Parsec*;
5. Установите флажок *Записывать персональные данные на карту*, если необходимо:



6. Положите чистую карту Mifare Plus 0 на считыватель PR-P18/PR-X18 и создайте мастер-карту, нажав на ставшую активной кнопку *Мастер-карта*;
7. Замените мастер-карту чистой картой Mifare Plus 0 и создайте карту сброса конфигурации;
8. Нажмите на кнопку *OK*. Настройки сохранятся в Системе;
9. Нажмите на кнопку *Настройки настольных считывателей*[123] и задайте требуемые параметры;
10. С помощью утилиты PNR_Tune для всех считывателей, которые будут работать с выданными картами Mifare Plus SL3, в конфигурации считывателей установите флажок *Читать карты - Mifare Plus* (остальные должны быть сняты), а переключатель *Mifare Plus security* установите в положение *Parsec (MAD)*:



Данную настройку можно сделать путём подключения каждого считывателя к ПК через преобразователь интерфейса RS-485 -> USB либо с помощью технологической карты, которая может быть подготовлена с помощью утилиты PNR_Tune, а затем поднесена к каждому считывателю. **Для подготовки**

технологической карты должна использоваться чистая карта Mifare Classic (или Mifare Plus уровня SL1) и настольный считыватель (PR-P18/PR-X18);

11. Поднесите мастер-карту, созданную на шаге 6, ко всем настенным считывателям. Сгенерированный профиль безопасности будет записан в их память.

Теперь можно выдавать карты субъектам доступа как обычно[261], используя чистые карты уровня SL0. При выдаче они будут переводиться на уровень SL3 и иметь доступ через настроенные точки прохода.

8.1.6.2 SL1 в SL3

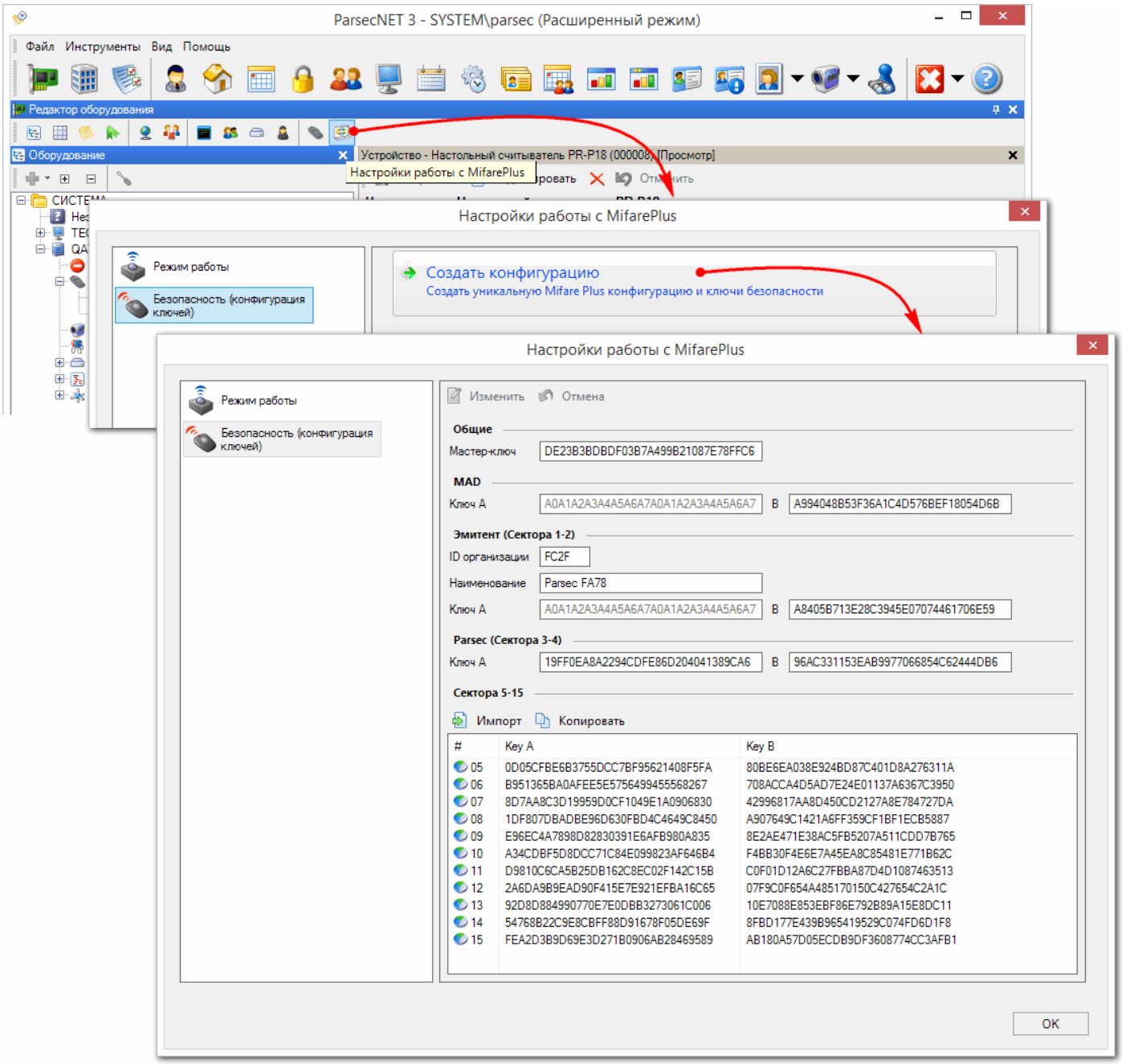
Если в организации использовались карты Mifare Plus на уровне SL1 (режим совместимости с Mifare Classic), то Система предоставляет возможность перевести их на уровень SL3. Для этого выполните следующие шаги:

1. В Редакторе оборудования ParsecNET 3 нажмите на кнопку *Настройки работы с Mifare Plus*.
   Откроется окно настроек, работать можно на любой рабочей станции системы;
2. В разделе *Безопасность (конфигурация ключей)* нажмите на кнопку *Создать конфигурацию.*.

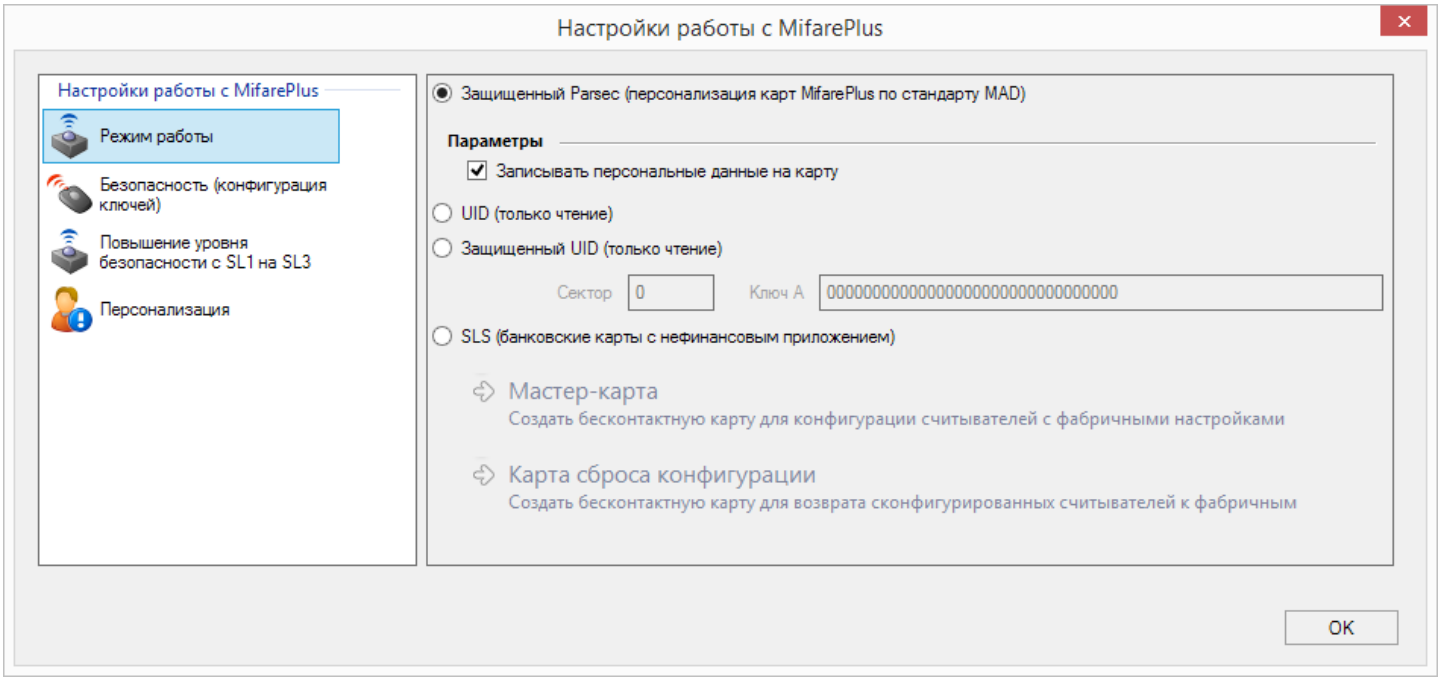


Обратите внимание, данное действие - необратимо! Если после эмиссии карт произвести изменения в этой конфигурации, проход по выпущенным картам будет невозможен.

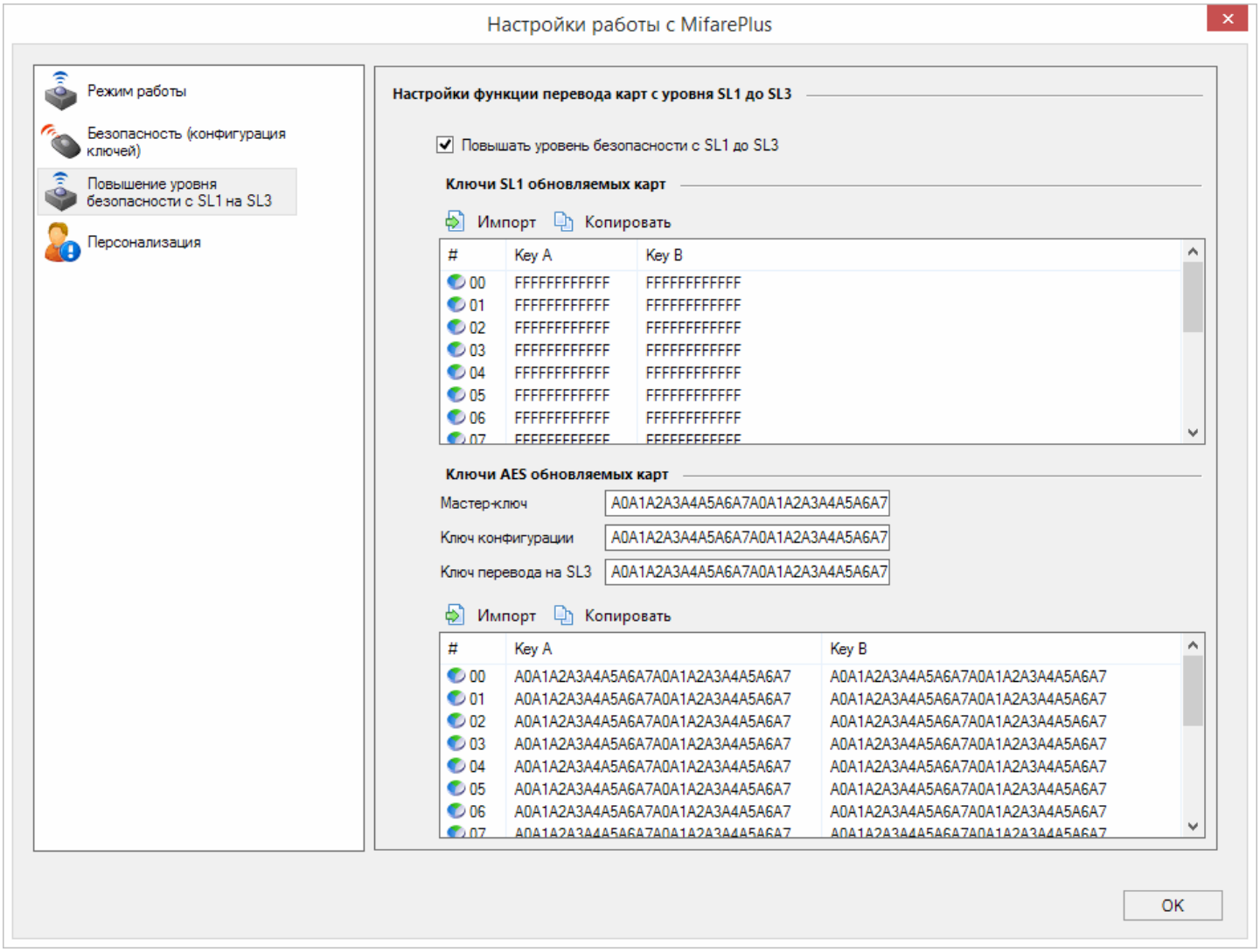
Система сгенерирует ключи для эмиссии карт Mifare Plus уровня безопасности SL3. При первой генерации ключей, окно будет находиться в режиме редактирования, можно будет изменить значения доступных полей. Внесенные изменения сохраняются в Системе при закрытии окна кнопкой *ОК* и при переходе в другой раздел;



3. Если необходимо, отредактируйте поле *ID организации*;
4. Перейдите в раздел Режим работы и выберите Защищенный Parsec. Со всеми остальными режимами функция повышения уровня безопасности не работает;



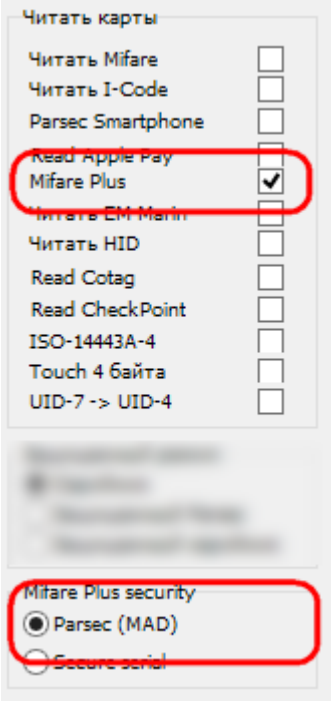
5. Установите флажок *Записывать персональные данные*, если необходимо;
6. Перейдите в раздел *Повышение уровня безопасности с SL1 до SL3* и установите флажок *Повышать уровень безопасности с SL1 до SL3*;



7. Для повышения уровня безопасности карты Mifare Plus с SL1 на SL3 необходимо задать текущие ключи SL1 (Mifare Classic) и AES от всех секторов карты, а также

служебные ключи Mifare AES. Эти ключи задаются при эмиссии карт и их нужно запросить и получить у эмитента/производителя карт. Импортируйте из файла формата CSV ключи Mifare Classic и AES, а также введите ключи в поля *Мастер-ключ*, *Ключ конфигурации* и *Ключ перевода на SL3*;

8. Положите чистую карту Mifare Plus 0 на считыватель PR-P18/PR-X18 и создайте мастер-карту, нажав на кнопку *Мастер-карта* в разделе *Режимы работы*;
9. Замените мастер-карту чистой картой Mifare Plus 0 и создайте карту сброса конфигурации;
10. Нажмите на кнопку *ОК*. Настройки сохранятся в Системе;
11. Нажмите на кнопку *Настройки настольных считывателей*[123] и задайте требуемые параметры;
12. С помощью утилиты PNR_Tune для всех считывателей, которые будут работать с выданными картами Mifare Plus SL3, в конфигурации считывателей установите флажок *Читать карты - Mifare Plus* (остальные должны быть сняты), а переключатель *Mifare Plus security* установите в положение *Parsec (MAD)*:



Данную настройку можно сделать путём подключения каждого считывателя к ПК через преобразователь интерфейса RS-485 -> USB либо с помощью технологической карты, которая может быть подготовлена с помощью утилиты PNR_Tune, а затем поднесена к каждому считывателю. **Для подготовки технологической карты должна использоваться чистая карта Mifare Classic (или Mifare Plus уровня SL1) и настольный считыватель (PR-P18/PR-X18)**;

13. Поднесите мастер-карту, выпущенную на шаге 8, ко всем настенным считывателям. Сгенерированный профиль безопасности будет записан в их память.

Теперь можно переводить карты SL1 на уровень SL3:

- В Редакторе персонала откройте карточку субъекта доступа, карту которого требуется перевести на уровень SL3;
- Переведите карточку в режим редактирования;
- Приложите карту доступа к настроенному настольному считывателю (PR-P18/PR-X18). На нее будут записаны новые данные;
- Сохраните изменения в БД Системы, нажав на кнопку *Сохранить* в карточке субъекта доступа.

Карта доступа теперь готова к использованию с уровнем безопасности SL3.

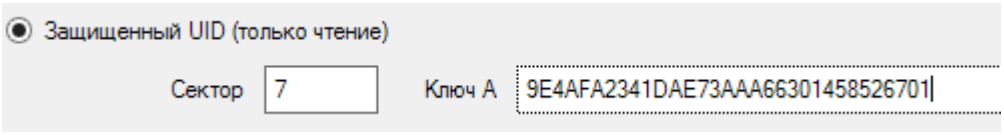
8.1.6.3 Работа с SL3

Работа с картами уровня SL3 возможна только в том случае, когда известны ключи доступа к защищенным секторам.

A. Если карта **персонализирована в вашей организации**, то работа с ней возможна только в случае, когда ключи карты совпадают с ключами, сгенерированными в разделе *Безопасность*[129]. Если после выпуска карт конфигурация ключей была изменена, работать с ними можно только по варианту B;

B. Если карты Mifare Plus персонализированы **в сторонней организации с использованием стандарта MAD**, то для работы с ними используется режим *Защищенный UID*. Для этого необходимы данные о секторе и ключе для аутентификации, записанные при персонализации:

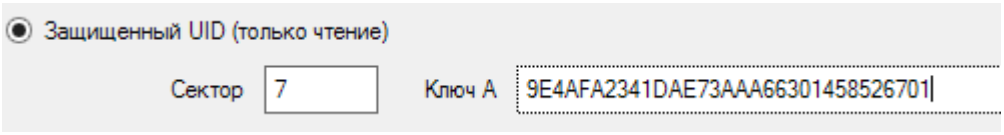
1. Для чтения таких карт настольным считывателем в разделе *Режимы работы* выберите *Защищенный UID* и в поле *Сектор* и *Ключ А* введите известные значения, например:



2. Перейдите в раздел *Безопасность (конфигурация ключей)* и в том же секторе введите тот же ключ А (для нашего примера как на рисунке выше);
3. Далее действуйте, как описано в разделе SL0 в SL3[133], начиная с шага 6.

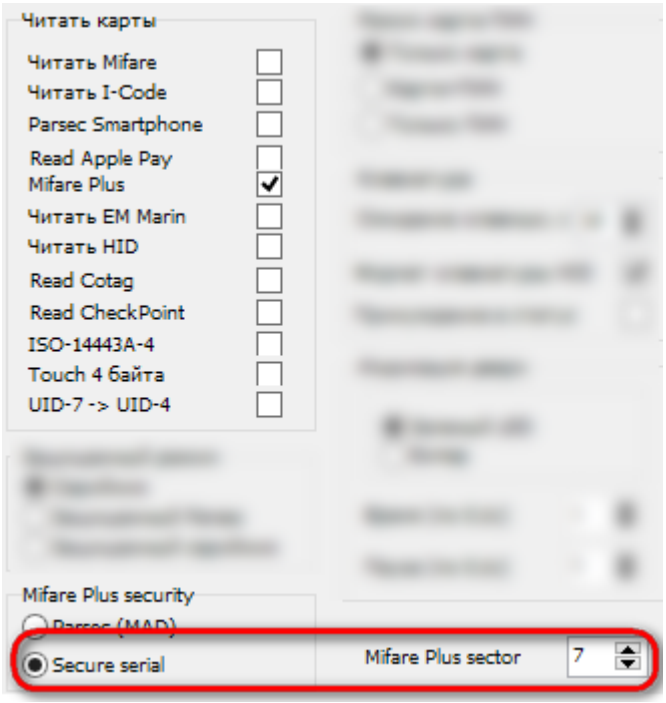
C. Если карты Mifare Plus персонализированы **без использования стандарта MAD**, работать с ними можно тоже только в режиме *Защищенный UID* и при условии, что известны сектор и ключ аутентификации:

1. Для чтения таких карт настольным считывателем в разделе *Режимы работы* выберите *Защищенный UID* и в поле *Сектор* и *Ключ А* введите известные значения, например:



2. Перейдите в раздел *Безопасность (конфигурация ключей)* и в том же секторе введите тот же ключ А (для нашего примера как на рисунке выше);
3. Далее действуйте, как описано в разделе SL0 в SL3[133], начиная с шага 6.

Единственное изменение в этом случае состоит в настройках настенных считывателей через утилиту PNR_Tune - переключатель *Mifare Plus security* необходимо установить в положение *Secure serial*, а также указать номер сектора (в нашем примере номер 7):



Если требуется **перевыпустить** карту Mifare Plus уровня SL3:

1. Перейдите в раздел *Режимы работы* окна *Настройки работы с Mifare Plus*;
2. Выберите корректный режим работы с картами Mifare Plus:
   - *Защищенный Parsec* - если карта выпущена системой Parsec с текущей конфигурацией в разделе *Безопасность*;
   - *Защищенный UID (только чтение)* - при иных вариантах выпуска. Введите номер сектора и ключ (их необходимо получить у эмитента карты).
3. Перейдите в раздел *Персонализация*;
4. Поместите карту на настольный считыватель PR-P18/PR-X18;
5. Внесите исправления в отобразившиеся данные и нажмите на кнопку *Записать на карту*;
6. Снимите карту со считывателя и при необходимости повторите с другой картой;
7. Закройте окно *Настройки*, нажав на кнопку *ОК*.

8.1.7 Алкотестирование

Лицензируется как PNSoft-TA1CH

Функция алкотестирования позволяет СКУД предотвратить доступ на защищенную территорию или выход с нее лиц, находящихся в состоянии алкогольного опьянения, что актуально для транспортных компаний, организаций с жесткими требованиями к соблюдению техники безопасности и производителей алкоголя.

Общий принцип контроля состоит в том, что для прохода нужно получить разрешение на проход как по карте сотрудника, так и от алкотестера. Для этого задаются общие или индивидуальные параметры алкотестирования.

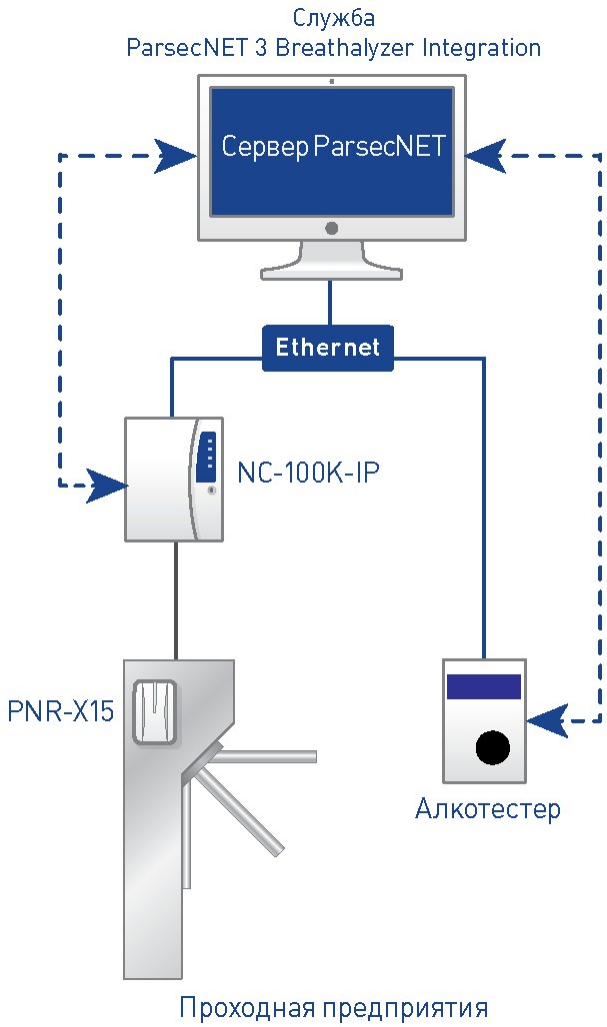
При попытке прохода, после подтверждения права доступа для идентификатора, активируется алкотестер. Владелец идентификатора делает выдох в прибор и, в зависимости от измерений алкотестера и настроенных правил тестирования, система либо разрешает, либо запрещает проход. В настоящее время функционал алкотестирования поддерживают контроллеры NC-8000 всех модификаций с прошивкой 3.8 и выше, NC-60K/NC-60K.M и NC-100K-IP (прошивка 8.4 и выше) только в обычном режиме прохода.

Интеграция и тестирование работы СКУД проведена с алкотестером «Алкобарьер» производства компании ООО «АЛКОТЕКТОР», имеющим точность измерения +/- 0,05 мг/л.

Алкотестер "Алкобарьер" должен иметь в своем составе интерфейсный модуль Ethernet, поскольку связь с контроллером Parsec осуществляется только по сети.

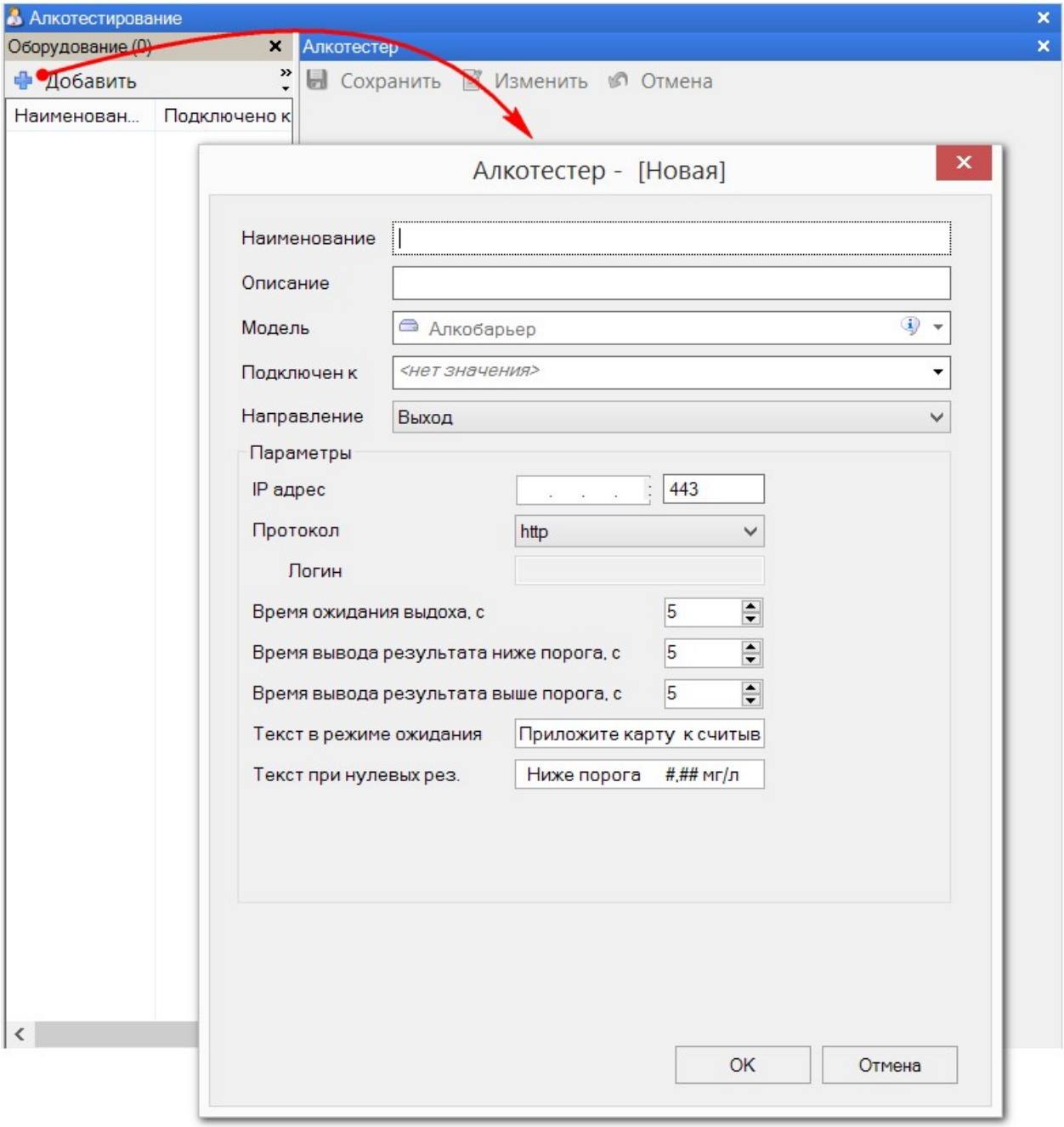
Для организации доступа с использованием алкотестера установите его в соответствии с "Инструкцией по монтажу, пуску и настройке" и "Руководством по эксплуатации" и настройте в Редакторе оборудования (описано ниже).

ПО сервера или рабочей станции ParsecNET 3 и ПО алкотестера должны быть установлены на разных ПК ввиду конфликта драйверов FTDI.



Настройка алкотестера в Редакторе оборудования

Нажмите на кнопку  (*Алкотестироавние*) на панели инструментов Редактора оборудования. В открывшемся окне нажмите на кнопку *Добавить*. Откроется окно параметров алкотестера:



При заполнении полей этого окна следуйте указаниям в Руководстве пользователя на алкотестер.

Заполните поля *Наименование* и *Описание* так, чтобы можно было однозначно идентифицировать данное устройство и его местоположение.

В поле *Подключен к* выберите контроллер Parsec, который будет работать с алкотестером (NC-8000(-D, -I), NC-60K/NC-60K.M или NC-100K-IP).

В раскрывающемся списке *Протокол* выберите протокол обмена данными: http или https.

Для http никаких дополнительных настроек не требуется.

Для https необходимо установить сертификат безопасности. Инструкции по получению файла сертификата безопасности находятся в web-интерфейсе Алкобарьера. В процессе генерации файла сертификата задайте логин и пароль. После того, как файл сертификата сгенерирован импортируйте его на сервер Parsec в хранилище сертификатов "Локальный компьютер". Логин, заданный при генерации сертификата, необходимо указать в настройках алкотестера в ПО Parsec.

Если сертификат безопасности импортирован в пользовательское хранилище, модуль интеграции работать не будет.

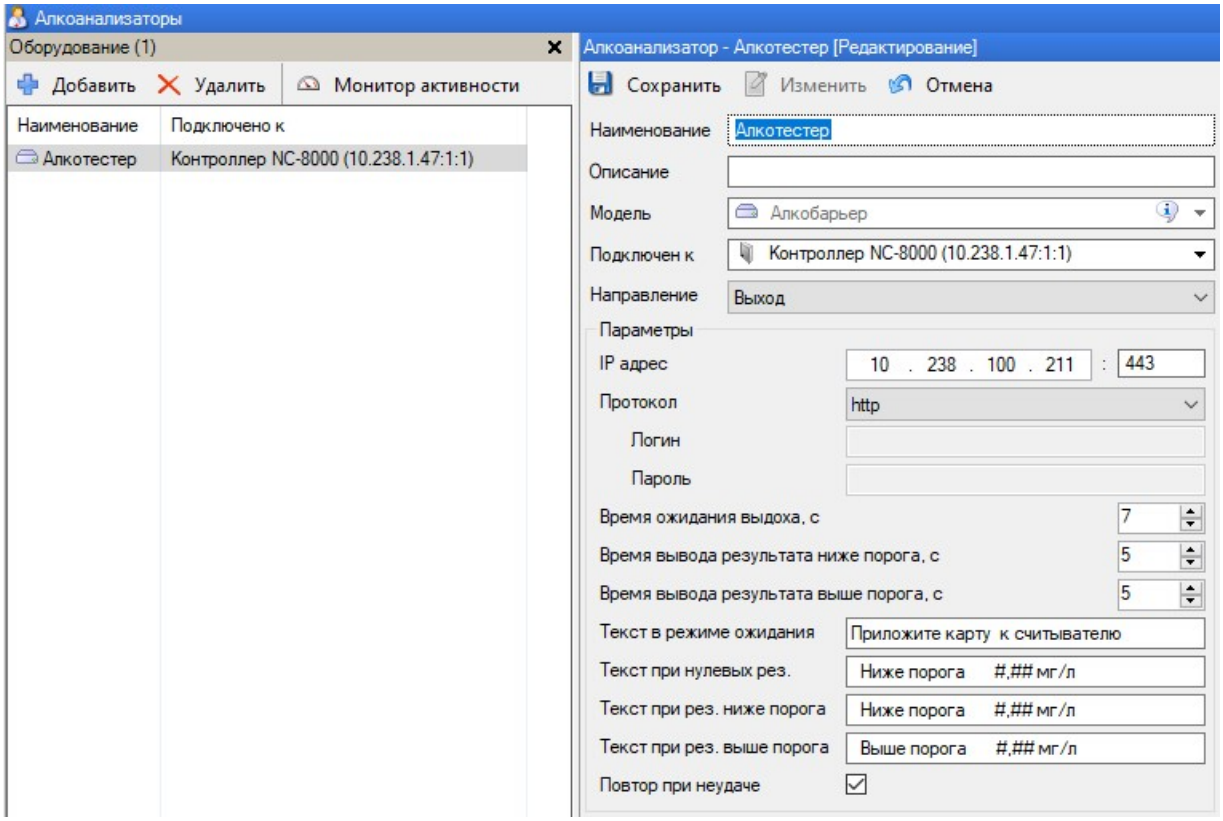
Время ожидания выдоха показывает время после активации алкотестера, в течение которого сотрудник должен сделать выдох в приемную воронку устройства.

Время вывода результата показывает как быстро будет отображаться результат в случаях, когда он выше и ниже заданной границы.

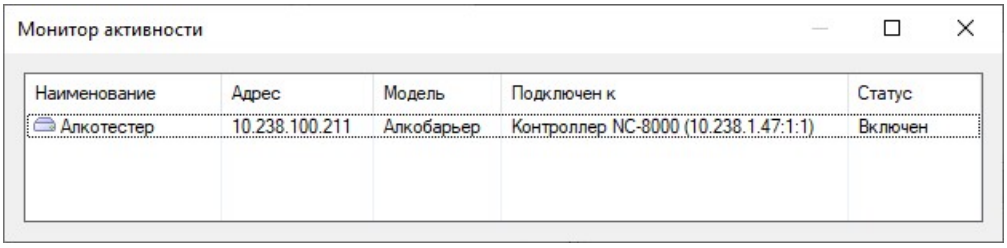
В полях *Текст...* можно ввести информацию, которая будет отображаться на экране алкотестера.

При установленном флажке *Повтор при неудаче* цикл анализа начинается заново, например, при истечении времени ожидания выдоха. Время второго (и более) циклов необходимо учитывать при задании времени ожидания подтверждения в настройках контроллера.

После введения необходимых параметров и нажатия на кнопку *ОК* появится карточка устройства:



Нажав на кнопку *Монитор активности* можно просмотреть статус выбранного устройства:

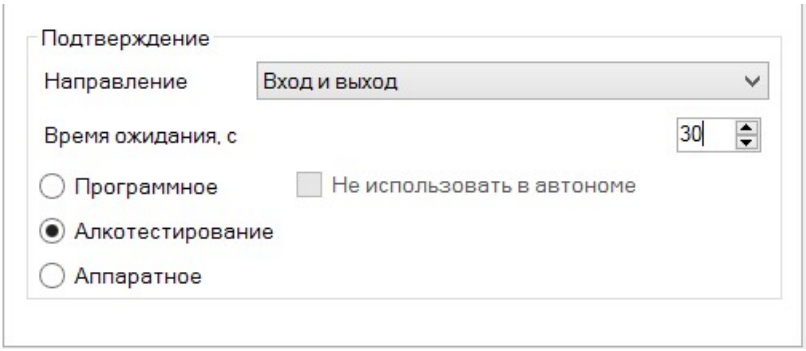


Настройка контроллера

Настройки алкотестирования у всех поддерживающих этот функционал контроллеров (NC-8000(-D, -I), NC-60K/NC-60K.M и NC-100K-IP) производится одинаковым образом:

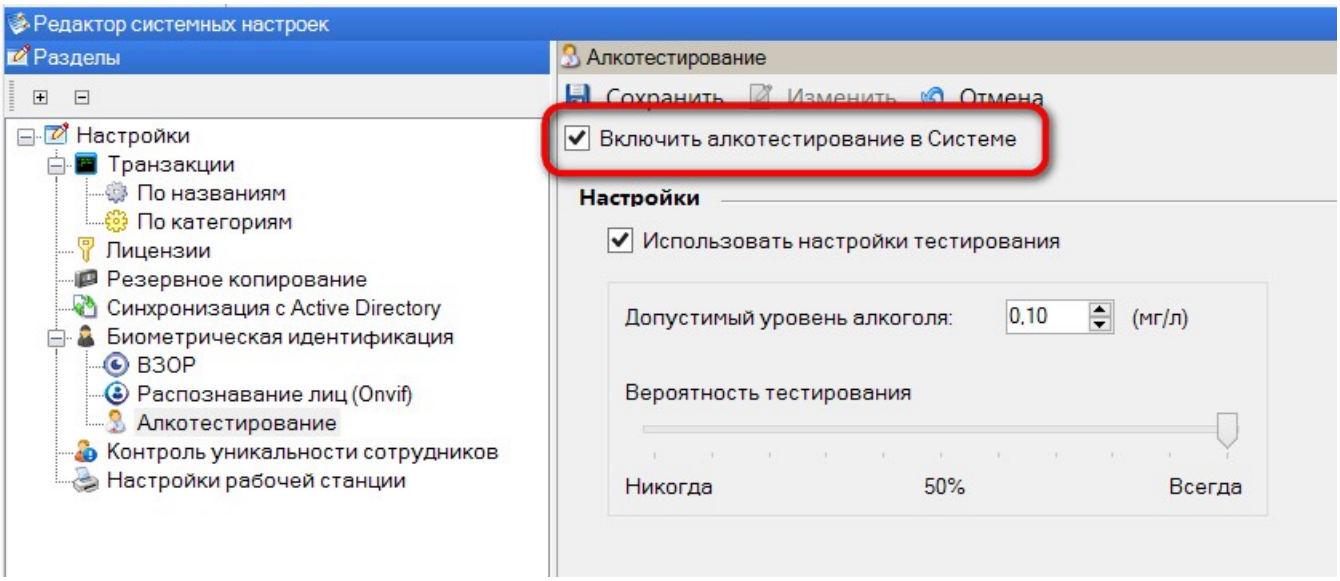
1. В Редакторе оборудования перейдите в карточку контроллера и включите режим редактирования;
2. На вкладке *Режимы* проходов в блоке *Подтверждение* выберите из раскрывающегося списка *Направление* направление прохода, при котором будет производиться алкотестирование;

3. Задайте *Время ожидания* - время от момента считывания кода идентификатора, которое контроллер будет ждать сигнала от алкотестера. По истечении этого времени идентификатор будет необходимо снова поднести к считывателю и весь цикл идентификации будет выполнен снова. При задании времени ожидания учитывайте вероятность неудачных попыток анализа выдыхаемого субъектом доступа воздуха. Контроллер обрабатывает код от алкотестера при первой удачной попытке.
   Например, определим время неудачной попытки равным 10 секундам. Разрешим 3 неудачные попытки, после чего субъект доступа должен будет снова предъявить карту для считывания. Следовательно, время ожидания контроллера необходимо задать равным 30 секундам.
4. Установите переключатель в положение *Алкотестирование*;
5. Сохраните внесенные изменения.



Настройка параметров алкотестирования

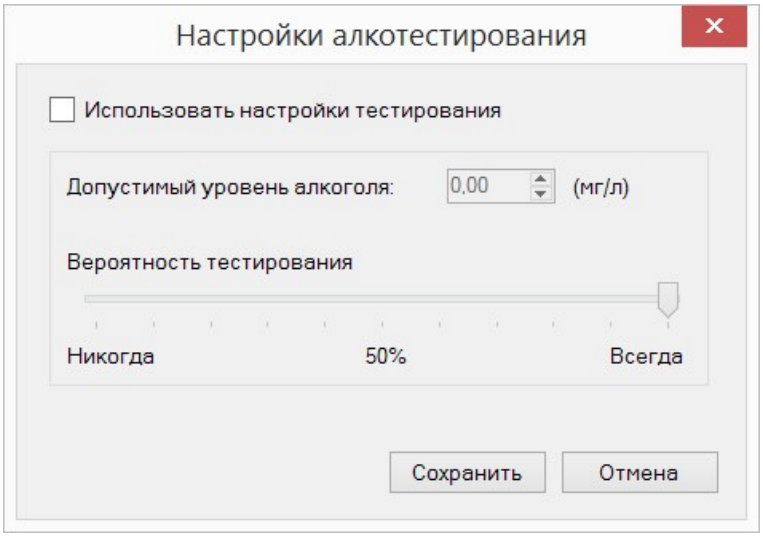
1. В редакторе системных настроек поставьте флажок *Включить алкотестирование в Системе* (шаг 4 ниже). При его отсутствии никакие настройки алкотестирования не будут учитываться при проходе субъектов доступа:



2. Задайте настройки алкотестирования в соответствии с желаемым масштабом проверок:
   - для тестирования всех субъектов доступа - в Редакторе системных настроек (шаг 4);
   - для тестирования субъектов определенной(-ых) групп доступа - в настройках этих групп (шаги 2 и 3);
   - для тестирования конкретных субъектов доступа - в карточке этих субъектов (шаг 1).

Окно настройки параметров алкотестирования одинаково для всех редакторов СКУД ParsecNET 3. Их расположение описано ниже в тексте.

Окно имеет следующие вид:



Элементы окна:

- Флажок *Использовать настройки тестирования* - при установке флажка при алкотестировании будут учитываться заданные параметры;
- *Допустимый уровень алкоголя* - в поле устанавливается граничное значение наличия алкогольных паров в выдыхаемом воздухе;
- *Вероятность тестирования* - положение ползунка показывает шанс, с которым будет проведен тест. Система будет проводить проверку на алкоголь в соответствии с заданной в процентах вероятностью. Такая опция позволяет сохранить приемлемую пропускную способность точки прохода, при этом усилив контроль.

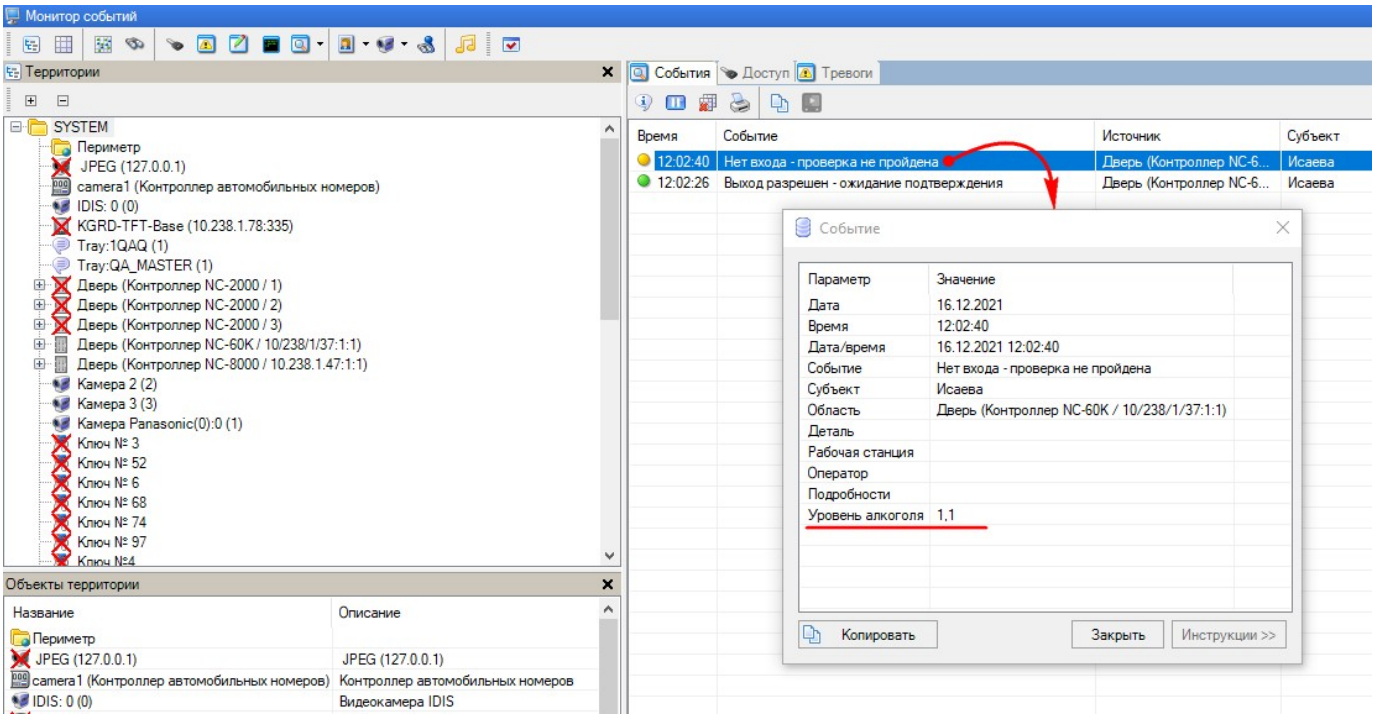
Обратите внимание, что проверка начинается с индивидуальных настроек. Иными словами, можно задать для всей системы одни настройки алкотестирования. Для какой-то группы доступа - другие. А для отдельных субъектов доступа - индивидуальные.
При попытке прохода Система сначала проверяет наличие индивидуальных настроек и соответствует ли им выдыхаемый субъектом доступа воздух.

Если индивидуальные настройки отсутствуют, то проверяются настройки группы доступа, а потом вложенной группы доступа (при ее наличии).

Если и этих настроек нет, то используются общесистемные настройки алкотестирования.

Если в выдыхаемом воздухе наличие паров алкоголя не превышает заданный уровень, то фиксируется обычный проход по ключу.

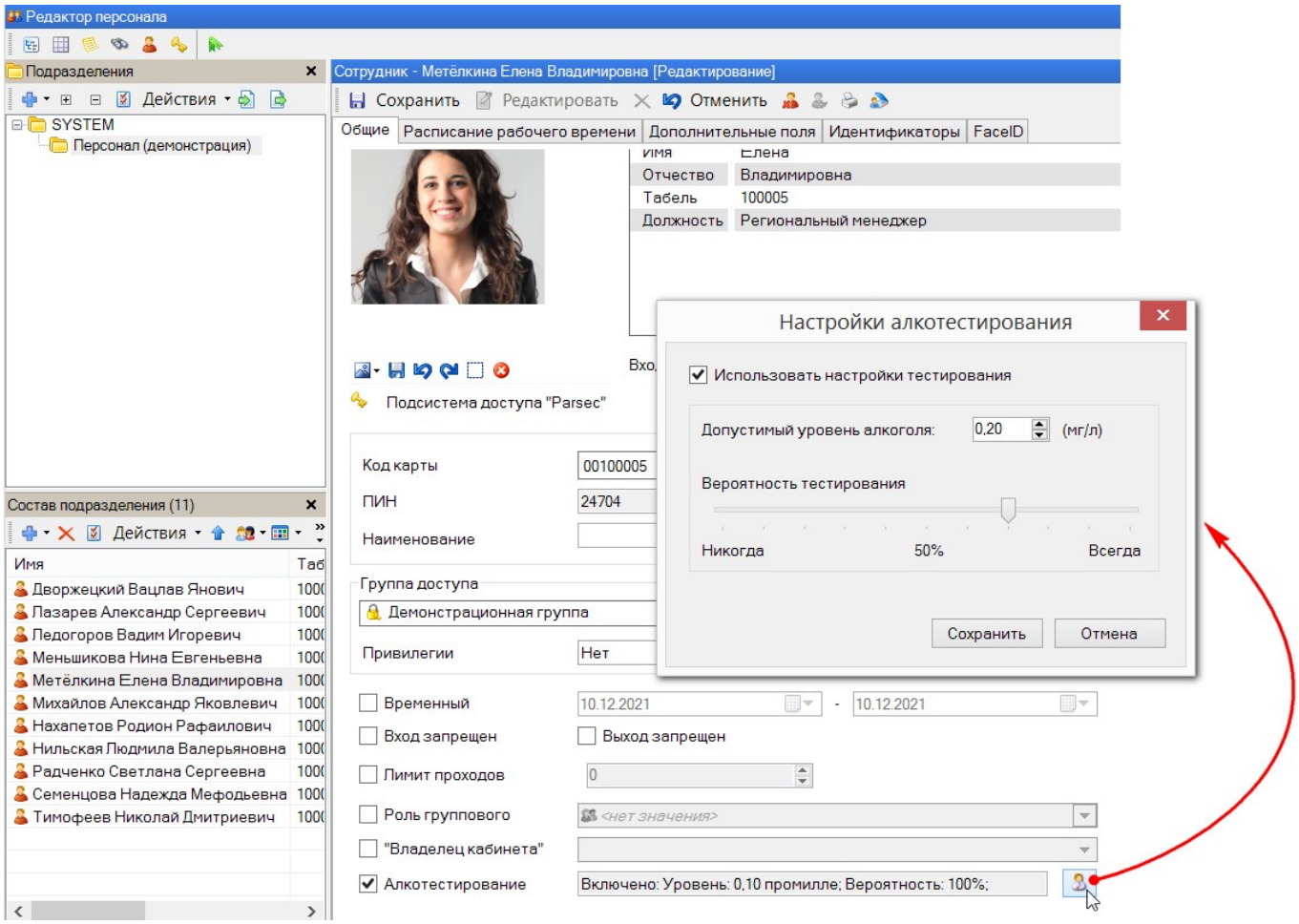
Если же уровень алкогольных паров выше заданного, проход будет запрещен. В Мониторе событий можно просмотреть данные события (выбрав в контекстном меню одноименную команду) и уровень алкогольных паров в мг/л:



Проверка соответствия показаний заданным параметрам алкотестирования производится по алгоритму, описанному ниже (принимаются первые заданные параметры):

Шаг 1. Проверка настроек алкотестирования для текущего идентификатора

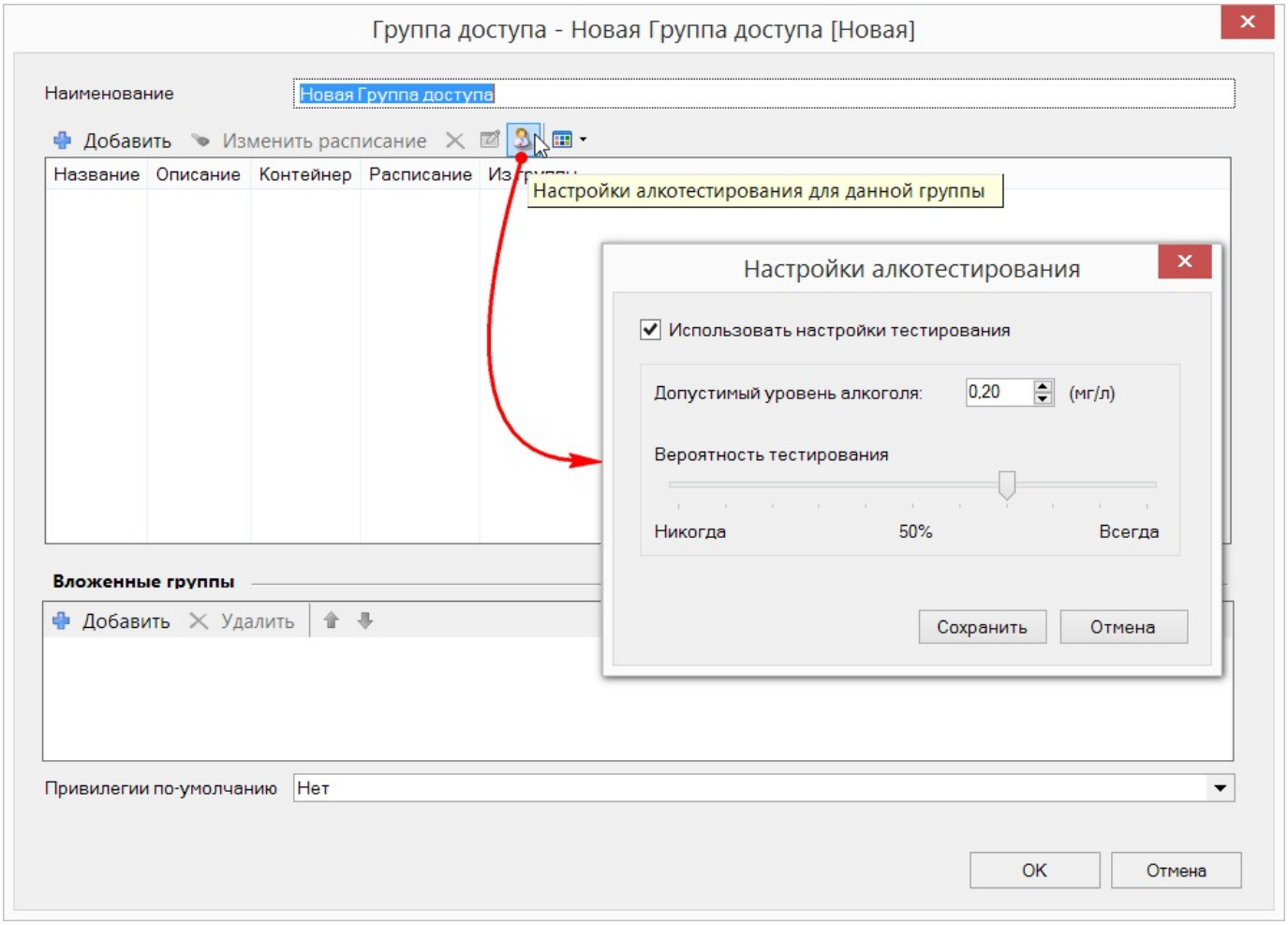
Настройки параметров алкотестирования для отдельного субъекта доступа производится в Редакторе персонала.



Шаг 2. Проверка настроек алкотестирования для группы доступа

Параметры алкотестирования для группы доступа можно задать во время ее создания, либо позже, в карточке группы.

Заданные параметры будут применяться ко всем субъектам доступа, которым назначена данная группа.



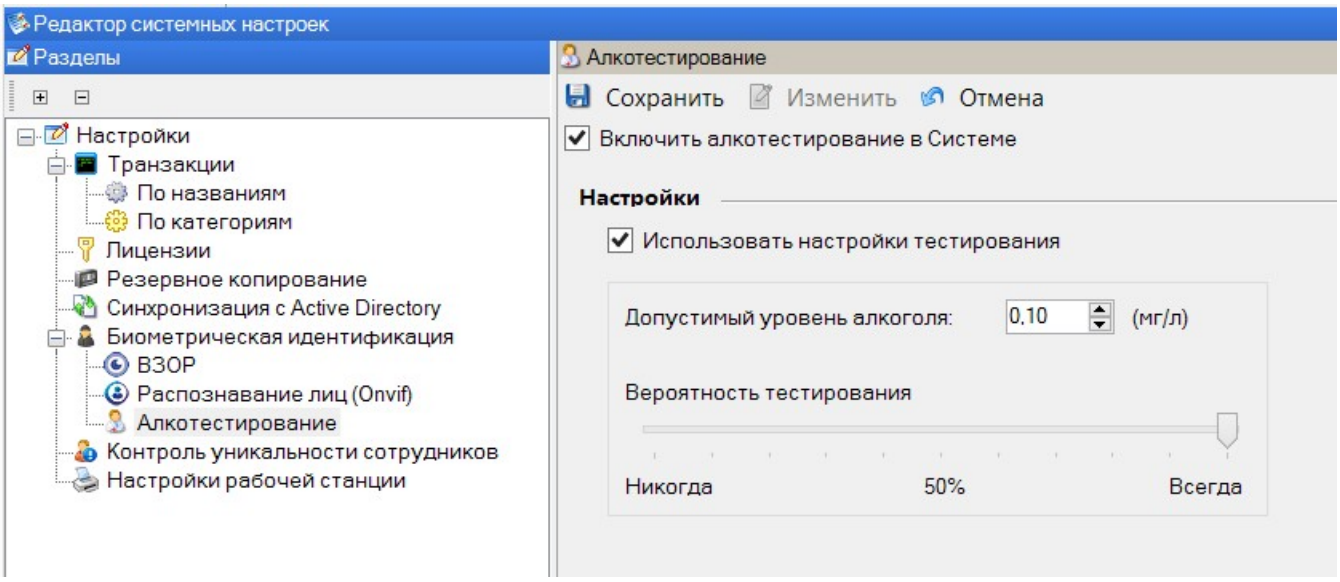
Шаг 3. Проверка настроек алкотестирования для вложенной группы доступа с высшим приоритетом

Поскольку вложенная группа доступа должна быть предварительно создана как любая другая группа доступа, настройка параметров алкотестирования для нее аналогична описанной в шаге 2.

Шаг 4. Проверка системных настроек алкотестирования

Параметры алкотестирования, заданные в системных настройках, применяются ко всем субъектам доступа, всем группам доступа и всем организациям СКУД ParsecNET 3.

Если флажок *Алкотестирование* не установлен, то функционал работать в Системе не будет.

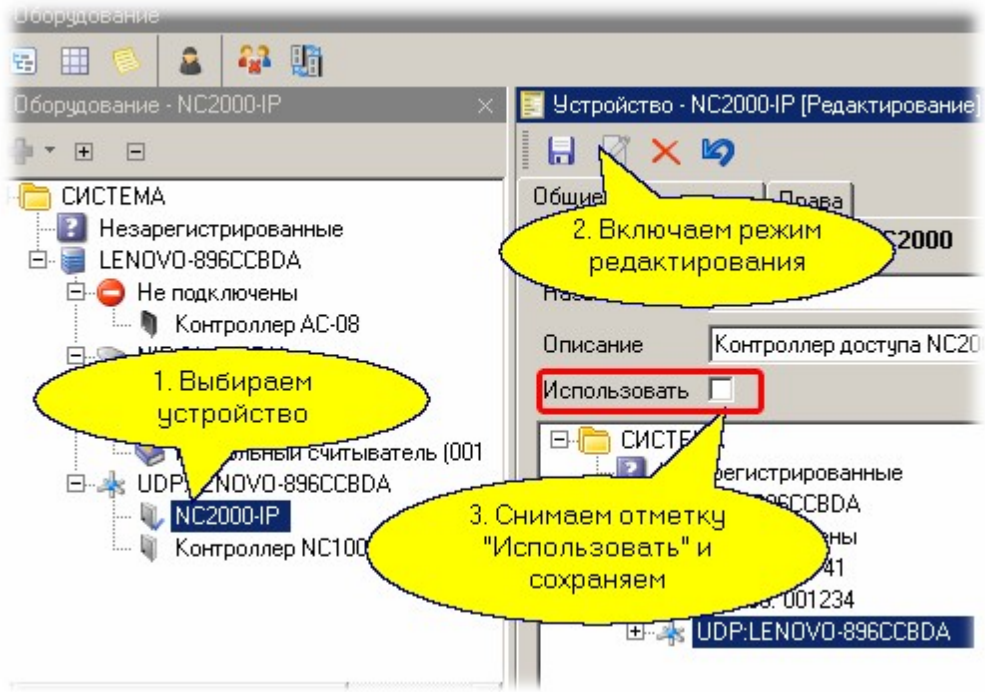


8.1.8 Временное отключение оборудования

Контроллеры или считыватели могут быть временно отключены от системы. В этом случае вся информация о них в системе сохраняется, но система к ним не обращается. Например, вы не можете загрузить данные нового субъекта доступа в такой контроллер, даже если физически он существует и работает.

Отключение чаще всего может понадобиться на этапе запуска и настройки системы, когда не все оборудование физически установлено и работает.

Отключение производится через карточку оборудования, как показано на рисунке ниже на примере контроллера NC-2000:



Аналогичным образом ранее отключенное оборудование можно в любой момент подключить снова.

Система пытается сама отследить те изменения, которые касались отключенного оборудования, и при его включении отсылает накопленные

изменения в его память. Однако, если вы не уверены, что все отработано правильно в автоматическом режиме, воспользуйтесь функцией инициализации контроллера, доступной из Монитора событий[297] .

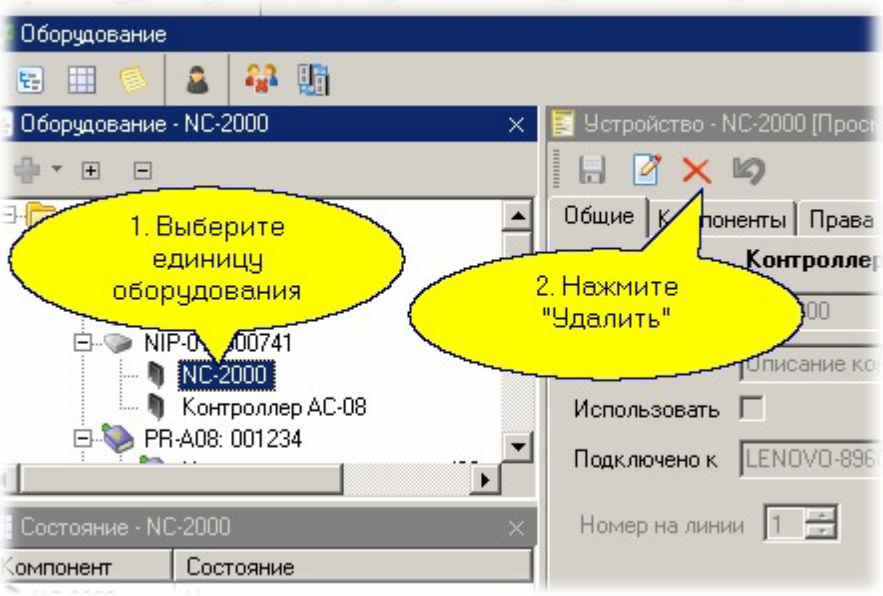
8.1.9 Удаление и перемещение устройств

Любое оборудование, имеющееся в системе, может при необходимости быть удалено или перемещено на другой канал или компьютер. Это может понадобиться при переконфигурировании системы в связи с изменением ее реальной структуры - переносом оборудования на новое место, его физическое удаление.

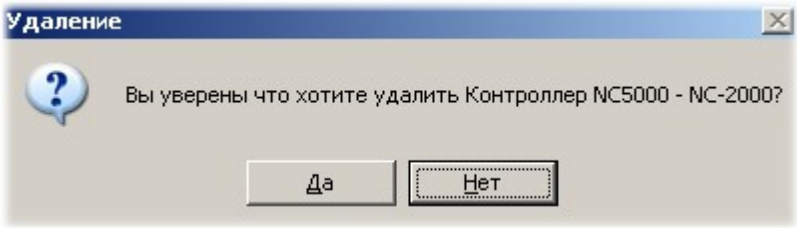
Указанные операции делаются в редакторе оборудования с административными правами.

Удаление оборудования:

Для удаления оборудования (контроллера, настольного считывателя, канала тип NI-A01 и так далее) выберите необходимый компонент для удаления в дереве или в списке оборудования, затем перейдите в карточку компонента и нажмите на кнопку *Удалить*, как это иллюстрируется рисунком ниже.



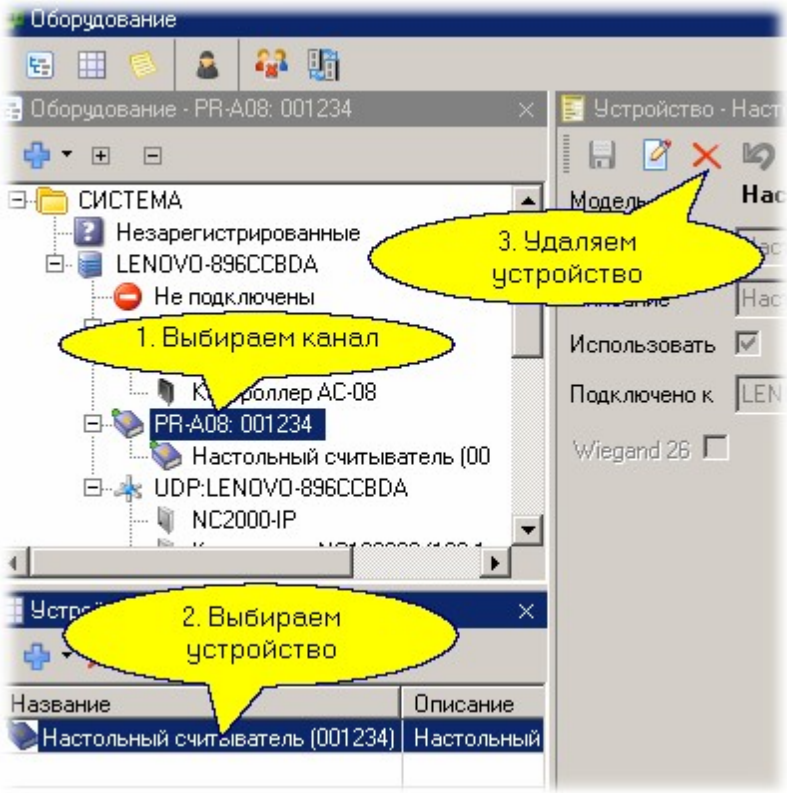
В ответ на запрос о подтверждении удаления ответьте требуемым вам образом.



Удаленное оборудование впоследствии не может быть восстановлено - вам заново придется вводить его и назначать параметры, если вы захотите восстановить удаленное оборудование в системе.

Удаление оборудования через список

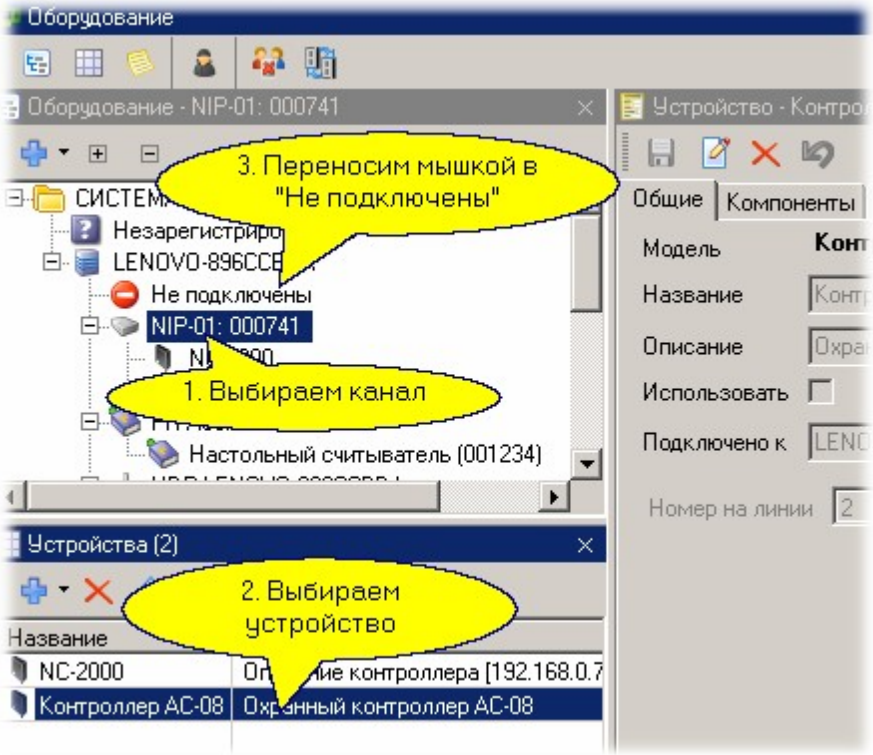
В дереве оборудования выберите необходимый канал (NI, NIP, CNC, UDP), перейдите в область списка *Оборудование*, выберите необходимое устройство для удаления (в нашем примере мы удаляем настольный считыватель) и нажмите на кнопку *Удалить*, как показано на рисунке ниже.



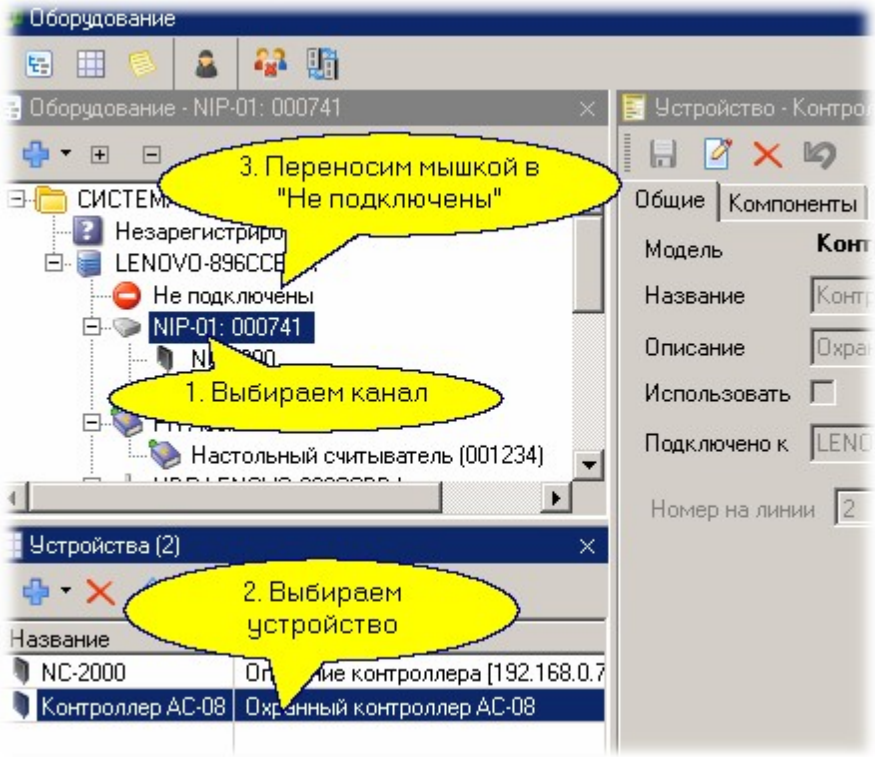
После вашего подтверждения оборудование будет безвозвратно удалено из системы.

Перемещение устройств

Иногда при физическом переносе оборудования бывает рационально подключить его в систему через другое устройство (другой интерфейс NI-A01, другой канал ЦКС и так далее) с сохранением всех настроек конкретной единицы оборудования. Это можно сделать следующим способом:



После отпускания кнопки мышки над новым местоположением переносимой единицы оборудования будет выведен запрос на подтверждение, чтобы при переносе случайно не "уронить" переносимый контроллер в неопределенное местоположение:

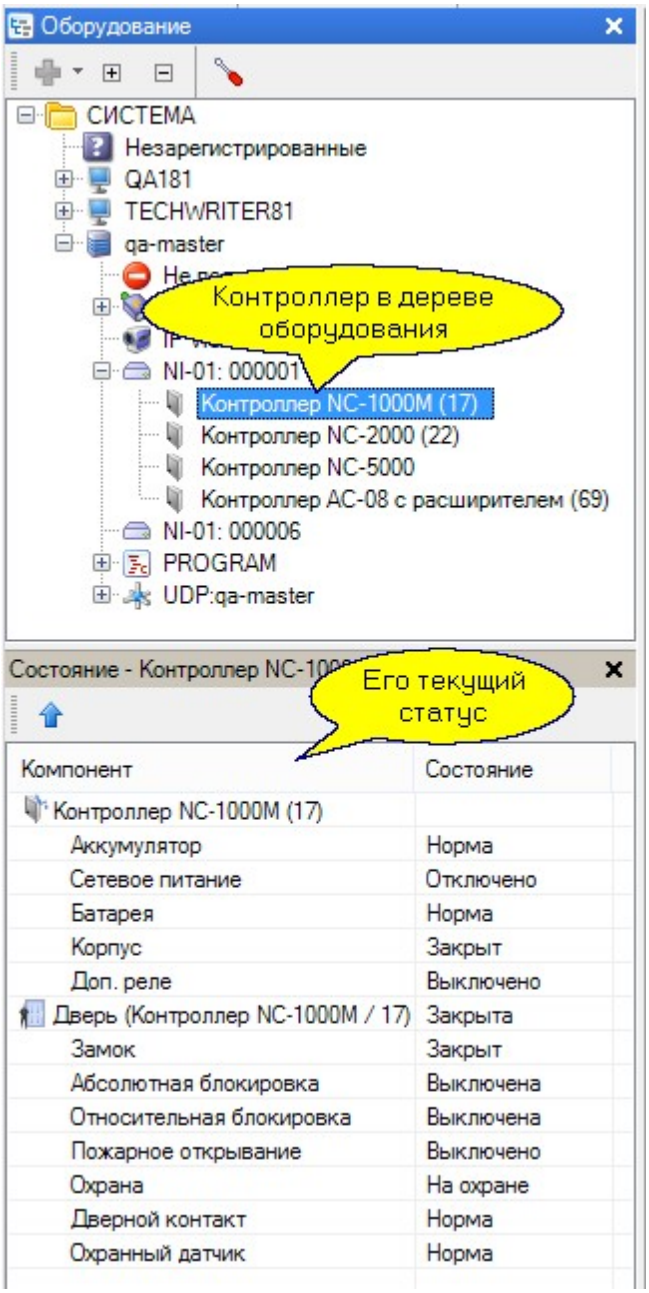


Переносить оборудование можно только между совместимыми портами. Нельзя, например, перенести контроллер с интерфейсом Ethernet на порт NIP-01 или наоборот, так как реально оборудование работать не сможет.

После перемещения оборудования оно будет автоматически проинициализировано.

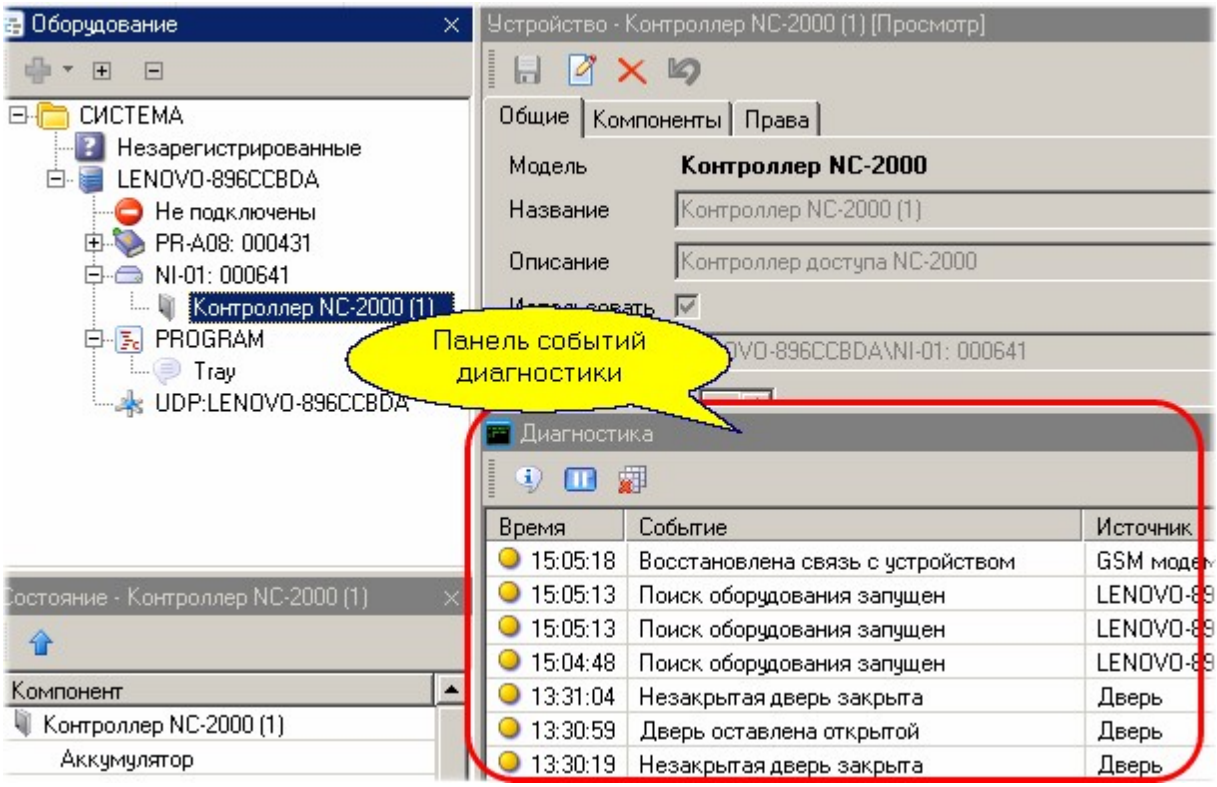
8.1.10 Контроль статуса оборудования

Контроль за состоянием оборудования необходим в большей степени администратору системы, чем оператору, выполняющему свою вполне конкретную задачу. Поэтому, помимо возможности видеть текущий статус оборудования в мониторе системы, его можно контролировать в режиме реального времени и в редакторе оборудования.



На рисунке выше в дереве оборудования виден контроллер NC-100K-IP. Описанные возможности позволяют администратору системы или установщику оперативно проводить диагностику компонентов системы при возникновении нештатных ситуаций.

В Редакторе оборудования присутствует также панель диагностических сообщений, в которую выводятся все события, связанные с оборудованием - его подключение, отключение, вскрытие корпуса и так далее. На следующем рисунке показана данная панель в составе Редактора оборудования.



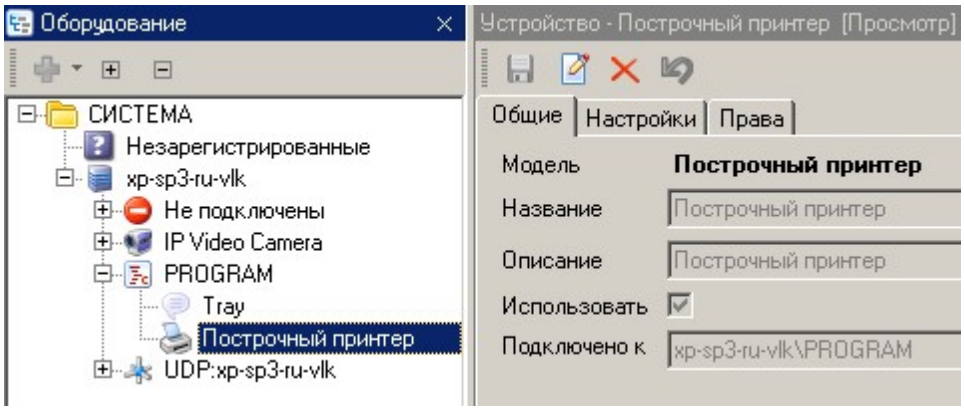
Это повышает удобство использования системы - теперь контроль событий оборудования можно производить без запуска Монитора событий непосредственно из редактора.

8.1.11 Построчный принтер

Система предоставляет организациям возможность выводить на печать сообщения о происходящих в ней событиях. Это имеет смысл делать на принтерах, имеющих рулонную подачу бумаги. В противном случае каждое сообщение будет отпечатано на отдельном листе.

Замечание: Принтер должен быть подключен к компьютеру, на котором установлено ПО ParsecNET 3.

Построчный принтер устанавливается на программный канал организации при первом запуске системы, либо при выполнении команды контекстного меню *Поиск оборудования*.



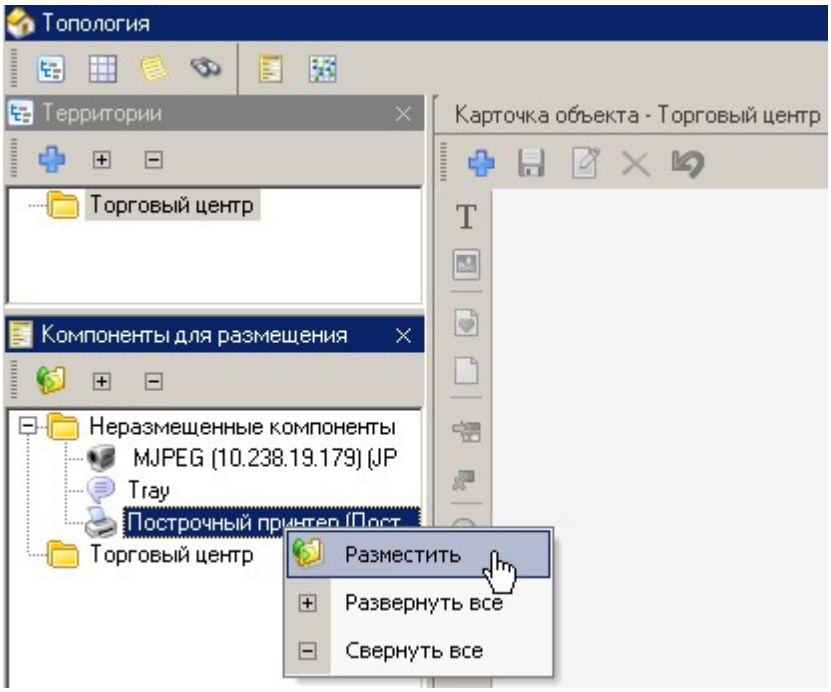
Для настройки принтера перейдите в режим редактирования.

На вкладке *Настройки* главный администратор системы в раскрывающемся списке указывает модель физического принтера.

На вкладке *Права* выбираются те организации, которым будет доступен данный принтер.

После сохранения изменений операторы организации, для которой настроен принтер, смогут создать задачи для вывода сообщений на печать.

Чтобы принтер отображался в списке устройств организации при создании задания[321] , оператор "подчиненной" организации должен разместить его на своей территории в редакторе топологии:



См. также:

Редактор заданий[321]

Печать уведомлений[411]

8.1.12 Системные дополнительные поля

Системные дополнительные поля предназначены, в отличие от обычных дополнительных полей[264] , для поддержки различных операций. Системные дополнительные поля задаются в редакторе оборудования.

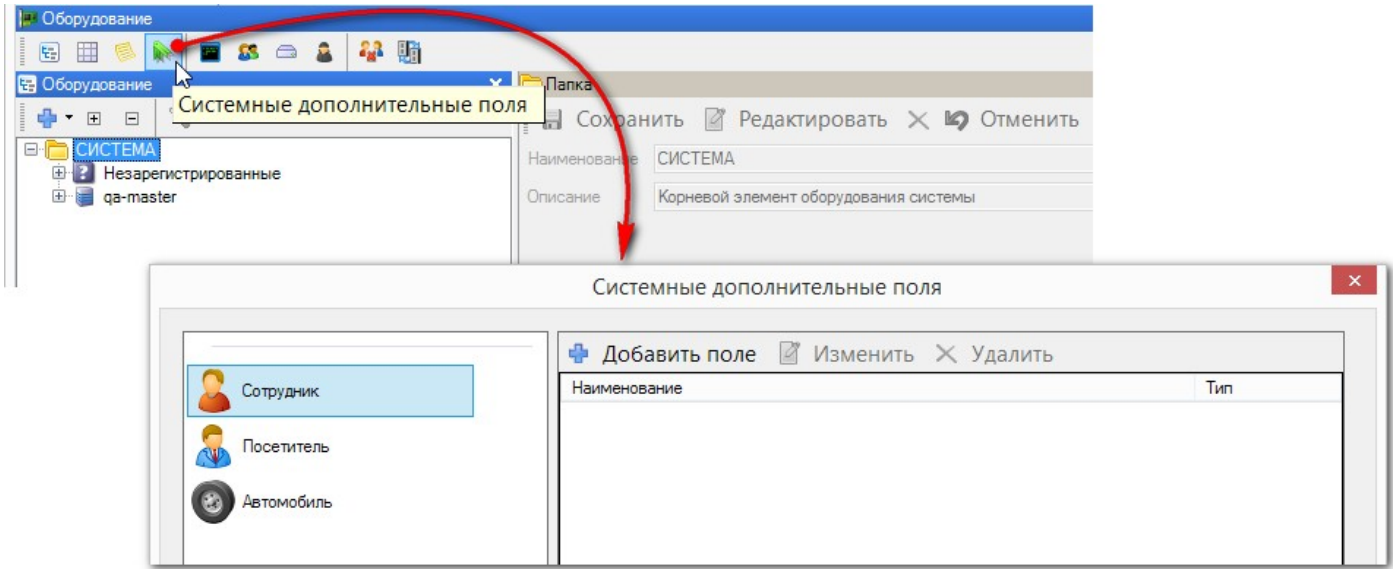
Основное их назначение – использование значений полей в программных контроллерах для получения дополнительных данных о субъекте доступа. В качестве системных дополнительных полей могут фигурировать такие сущности, как номер для отправки SMS сообщений через GSM-модем, адрес электронной почты для рассылки уведомлений о событиях, возможно их использование для обеспечения сложной логики работы шлюзов, например со взвешиванием и так далее.

Системные дополнительные поля назначаются раздельно для каждой категории субъектов доступа: сотрудников, посетителей и автомобилей.

После установки системы список полей пуст, его необходимо наполнять самостоятельно.

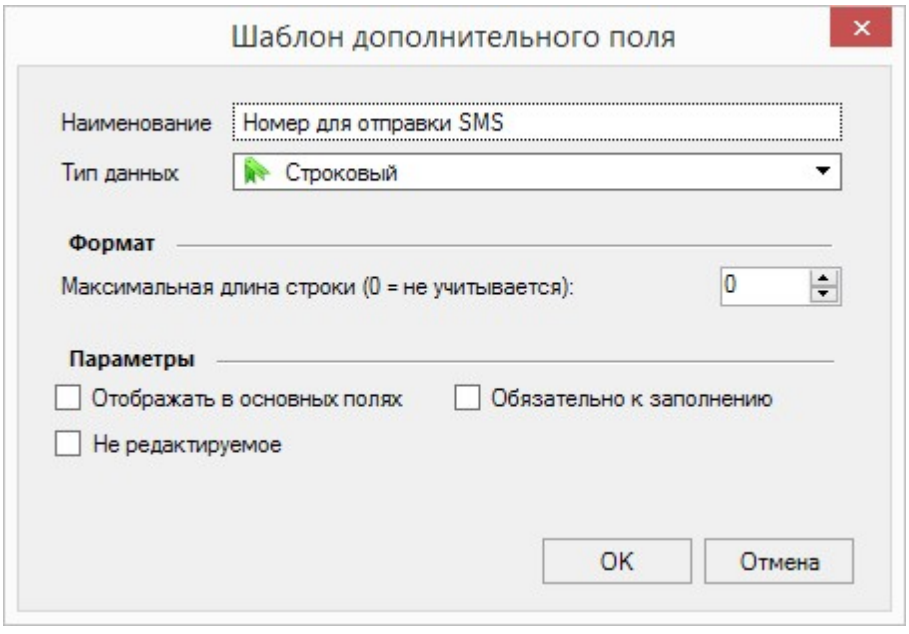
Создание системных дополнительных полей

Для создания нового поля необходимо открыть панель системных допполей, как показано ниже на рисунке, затем выбрать, для какой категории субъектов доступа будет создаваться поле:



Можно начать как с создания групп, а потом внутри групп создавать дополнительные поля, так и сначала создать все поля, а потом, создав группы, распределить между ними созданные дополнительные поля при помощи стрелок *Вверх* и *Вниз*.

Для создания системного дополнительного поля нажмите на кнопку *Добавить поле*. В открывшемся окне введите наименование:



В нашем примере введен номер телефона как строка без ограничений на ввод. Настройте параметры поля, которые соответствуют выбранному типу. Для нашего примера:

- *Формат* - указывается максимальное количество символов для этого поля. При значении "0" количество символов не ограничивается;
- *Отображать в основных полях* - при установке флажка созданное дополнительное поле будет отображаться в карточке сотрудника на первой вкладке *Общие*;
- *Обязательно к заполнению* - при установленном флажке, если при создании карточки нового или изменении существующего сотрудника оставить это поле незаполненным, система выдаст предупреждающее сообщение;
- *Не редактируемое* - при установке флажка содержимое поля в карточках сотрудников нельзя будет изменить.

Аналогично создайте другие системные поля, в том числе для других субъектов доступа.

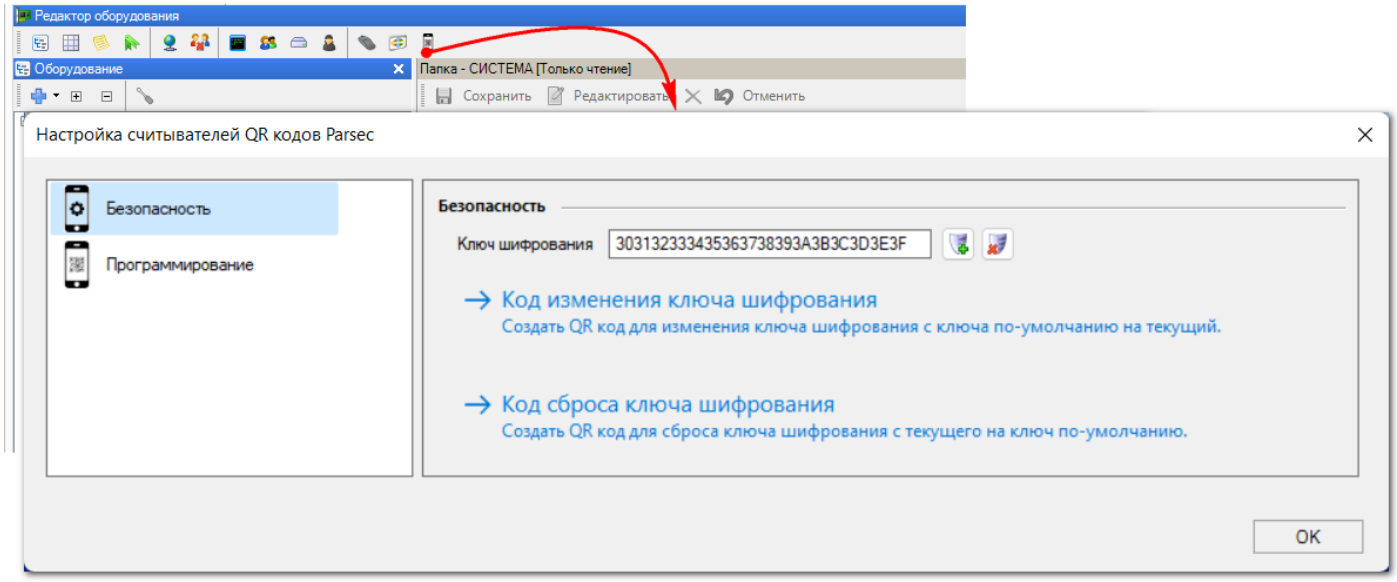
8.1.13 Настройки считывателей QR-кодов Parsec

СКУД ParsecNET 3 наряду с давно устоявшимися типами носителей кода идентификатора (карта, брелок, NFC модуль) может использовать и QR-коды, сгенерированные в собственном формате.

Для корректной работы с QR-кодами необходимо настроить считыватели, имеющие такую функцию. На текущий момент в линейке считывателей Parsec имеется один считыватель с функцией чтения QR-кодов - PNR-QX29.

Для настройки выполните следующие шаги:

1. В редакторе оборудования нажмите на кнопку *Настройка считывателей QR-кодов Parsec*. Откроется окно настроек, по умолчанию в разделе *Безопасность*:



Элементы окна:

- *Ключ шифрования* - в поле отображается текущий ключ, используемый для шифрования данных, которые содержатся в QR-коде.

	Отображаемый ключ используется для работы на вкладке *Программирование* и сохраняется в Системе после нажатия на кнопку *ОК* или перехода на вкладку *Программирование*.

-  - кнопка *Генерировать новый ключ*. При каждом нажатии создается новый случайный ключ шифрования;
-  - кнопка *Установить ключ по-умолчанию*. При нажатии в качестве ключа шифрования устанавливается исходный заводской ключ.
- *Код изменения ключа шифрования* - нажатие на эту кнопку формирует QR-код, содержащий в себе рабочий ключ, но зашифрован он заводским ключом, чтобы считыватель мог его прочитать. При поднесении такого QR-кода к считывателю QR-кодов Parsec он расшифровывается при помощи заводского ключа и в считыватель записывается новый ключ шифрования. О чем генерируется сообщение "Ключ шифрования записан". Новый рабочий ключ можно записать только в считыватель в заводской конфигурации (с заводским ключом);
- *Код сброса ключа шифрования* - сгенерированный по нажатию этой кнопки QR-код содержит заводской ключ шифрования (ключ по умолчанию), а сам QR-код зашифрован текущим ключом. При поднесении кода к считывателю QR-кода Parsec тот читает его, расшифровывая текущим ключом и записывает в себя содержание QR-кода - заводской

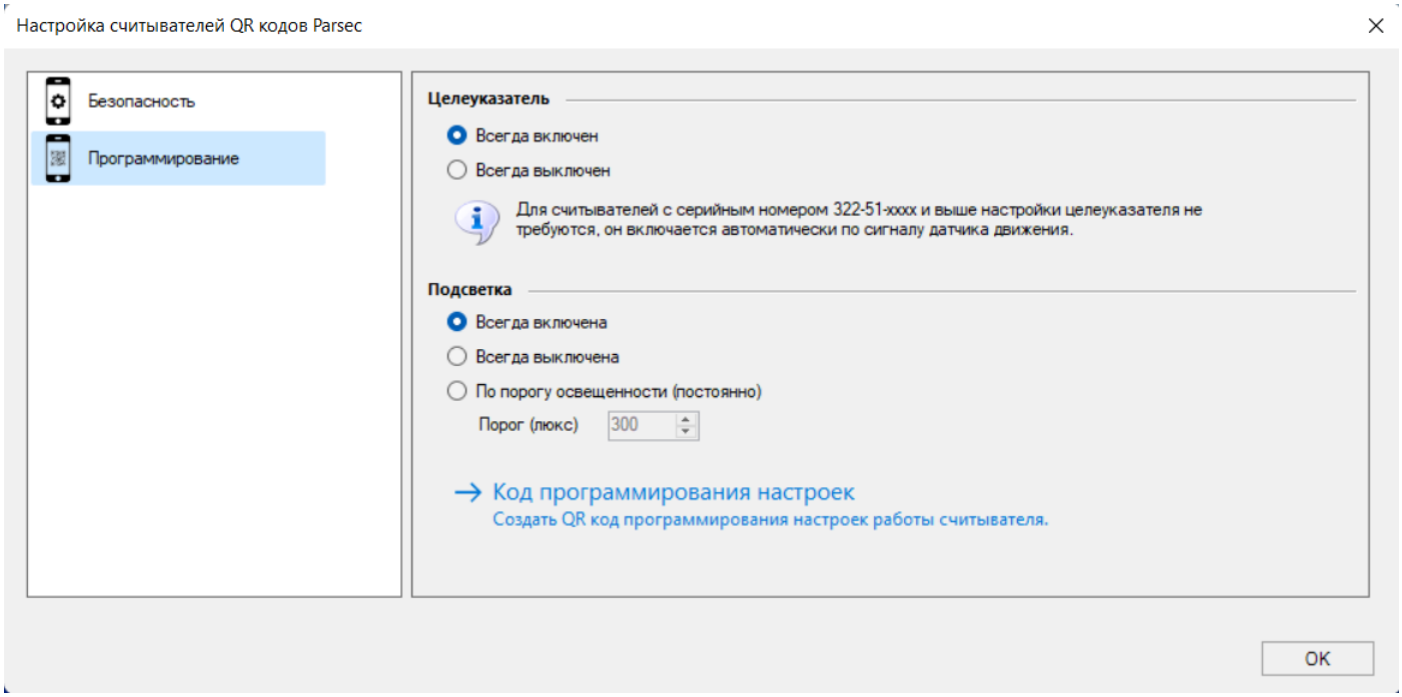
ключ шифрования. Об этом будет также сгенерировано сообщение "Ключ шифрования записан".

2. Задайте новый ключ шифрования, нажав на кнопку  ;
3. Сгенерируйте код изменения ключа шифрования, нажав на одноименную кнопку. В открывшемся окне отобразится сгенерированный QR-код. Сохраните его или распечатайте на удобном носителе;
4. Сгенерируйте код сброса ключа шифрования и распечатайте его.

Коды изменения и сброса ключа шифрования можно сгенерировать и распечатать и позже, в любое время.

	Чтобы сменить в считывателе рабочий ключ шифрования на другой, необходимо сначала сбросить текущий (т.е. записать в считыватель заводской ключ), а потом - записать новый.

5. Перейдите в раздел *Программирование*:



Элементы окна:

- *Целеуказатель* - красный луч светодиода считывателя PNR-QX29, используемый для правильной ориентации QR-кода перед камерой считывателя. Может находиться в одном из состояний: *Всегда включен* или *Всегда выключен*. Для считывателей с серийным номером 322-51-xxxx и выше настройки целеуказателя не требуются, он включается автоматически по сигналу датчика движения;
- *Подсветка* - два светодиода справа от камеры считывателя. Предназначены для освещения поднесенного QR-кода. Может находиться в одном из состояний: *Всегда включена, Всегда выключена* или *По порогу освещенности (постоянно)*. В последнем случае подсветка включается, когда датчик освещения регистрирует снижение освещения до установленного в поле *Порог (люкс)* значения;
- *Код программирования настроек* - при нажатии на кнопку заданные в разделе настройки будут сведены в QR-код. Поднесение этого кода к считывателю приведет к смене настроек его целеуказателя и подсветки на задаваемые QR-кодом, о чем будет сгенерировано событие от контроллера "Настройки считывателя записаны". Можно сделать несколько вариантов настроек и, соответственно, QR-кодов для программирования считывателей, находящихся в разных условиях.

6. Задайте нужные параметры и нажмите на кнопку *Код программирования настроек*. В открывшемся окне отобразится сгенерированный QR-код. Сохраните его или распечатайте на удобном носителе;
7. По завершении работы с настройками считывателей QR-кодов нажмите на кнопку *OK*. Окно настроек закроется.

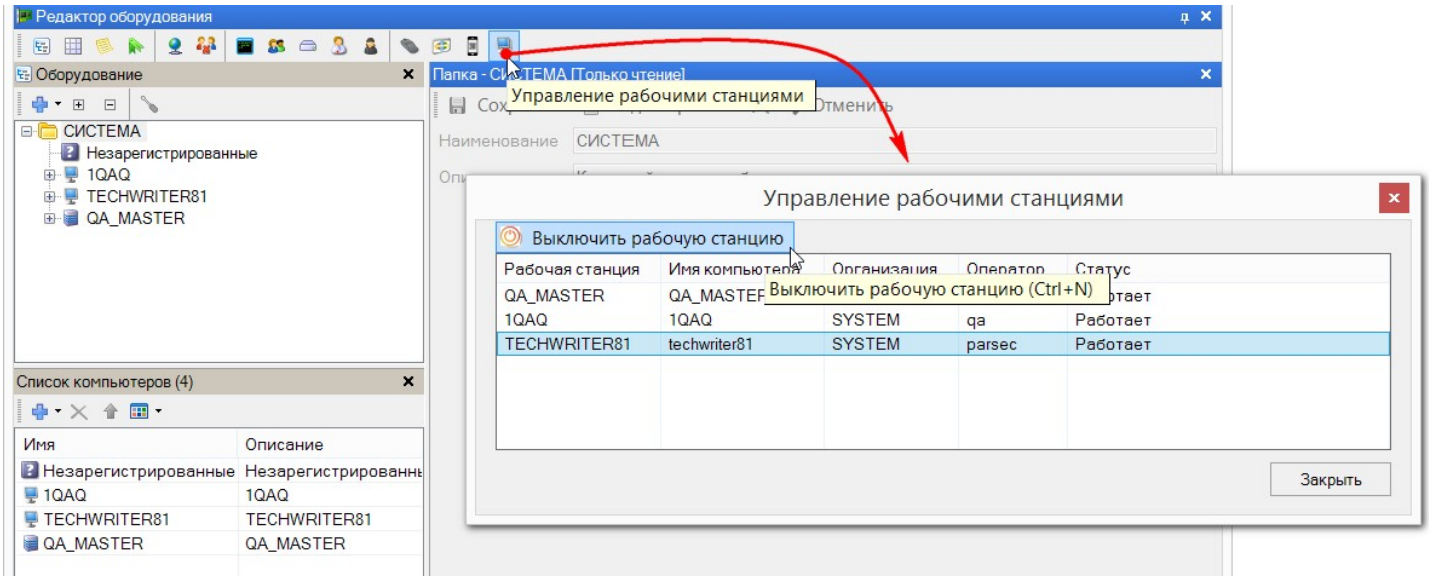
Для использования идентификаторов "QR-код Parsec" для прохода, их необходимо добавить[269] в Редакторе персонала или в Бюро пропусков[356], а затем распечатать (предварительно создав шаблон печати[424]) или передать на мобильное устройство либо на почту пользователя в виде графического файла.

Расширенные QR-коды описаны в одноименном разделе[253].

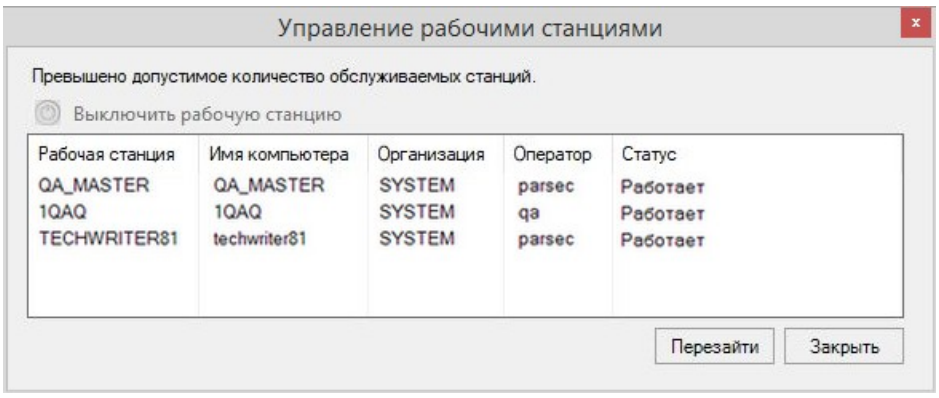
8.1.14 Управление рабочими станциями

Окно управления рабочими станциями позволят просматривать статус установленных рабочих станций, а также прекращать их работу.

Кнопка "Управление рабочими станциями" и собственно сама возможность выключать рабочие станции доступна только операторам с правом "Управление рабочими станциями".



В случае, если обладающий этим правом оператор пытается войти в систему, а количество запущенных рабочих станций уже исчерпало лимит, предоставляемый лицензией, появится аналогичное диалоговое окно. Оно позволит оператору выключить неиспользуемую или наименее загруженную рабочую станцию и повторить вход в систему, нажав на кнопку *Перезайти*:



8.1.15 Специальные режимы прохода

Система позволяет организовать специальные режимы для подсистемы доступа. Это:

- Роли группового прохода[115];

- Биометрические считыватели[654];
- Проход под принуждением[160];
- Защита от двойного прохода[161] (антипассбэк);
- Жесткий доступ[163].

Эти режимы частично реализуются аппаратно, на уровне контроллеров, а частично - с помощью программного обеспечения системы.

Для реализации специальных режимов доступа требуется, чтобы компьютер, к которому подключено оборудование, использующее специальные режимы, был постоянно включен.

Пользовательский интерфейс при этом может не работать, так как рассматриваемые функции обслуживается службами, запускаемыми одновременно со стартом Windows (в отличии от предыдущих версий системы).

8.1.15.1 Проход под принуждением

Назначение функции

Введение поддержки функции "вход под принуждением" позволяет решить проблемы связанные с ситуацией, когда вас заставляют открыть дверь под принуждением.

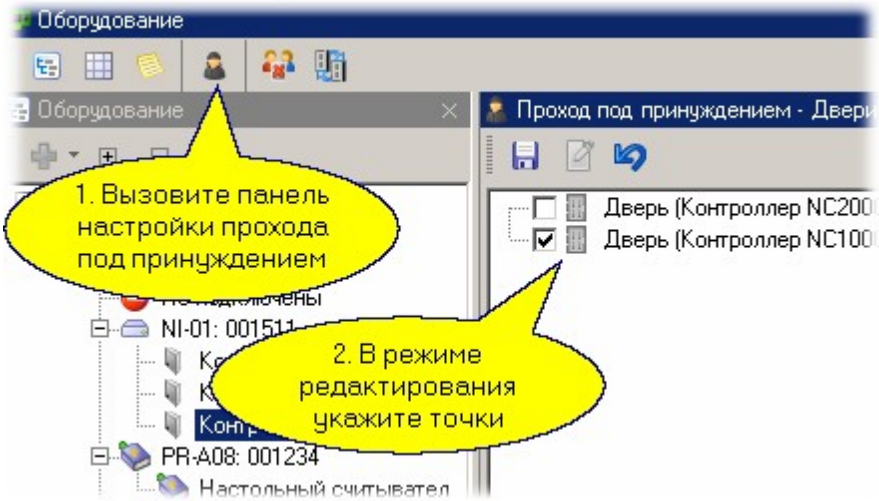
Для того, чтобы определить такую ситуацию, необходимо иметь на точке прохода считыватель с клавиатурой, а также определить права на "вход под принуждением".

Механизм данной функции реализован следующим образом: на считывателе с клавиатурой набирается специальный код и оператору (охране) приходит сообщение о "входе под принуждением". В зависимости от присвоенных привилегий сотрудник сможет пройти в помещение или нет но в любом случае охрана будет проинформирована.

Специальный код для "входа под принуждением" у каждого сотрудника персональный и получается путем прибавления к последней цифре ПИН-кода единицы (например, если Пин-код равен 12345, то для "входа под принуждением" будет - 12346. Если последняя цифра кода равна 9, то для кода 23459 вход под принуждением соответствует вводу кода 23450).

Проход под принуждением

Для настройки режима прохода под принуждением откройте соответствующую панель, выберите требуемые двери, назначьте расписание и привилегии для данного режима:



Расписание для данного режима задается отдельно из соображений безопасности человека (например, в нормальной ситуации у него сейчас нет доступа, но дверь надо открыть, иначе его жизни может угрожать опасность).



Для поддержки данного режима контроллер для входа в помещение должен иметь считыватель с клавиатурой.

8.1.15.2 Запрет двойного прохода

Назначение функции

Функция "антипассбэк" (запрет двойного прохода) позволяет исключить проход на территорию объекта нескольких человек по одной карте. Работу функции проще всего объяснить на примере.

Предположим, что вход в здание осуществляется через три турникета. Каждый из турникетов обслуживается своим контроллером. Если кто-то из сотрудников вошел через один турникет, то информация об этом рассылается в два других контроллера, и пока вошедший сотрудник не покинет здание, его карта не сможет быть использована для повторного входа через эти турникеты.

В области антипассбэка, как правило, объединяются точки прохода, ограничивающие проход на объект, например, проходные на предприятии, входы в здание и т.д.

Количество областей антипассбэка в системе не ограничено, Каждая точка прохода может присутствовать в любом количестве областей. Но при этом необходимо четко представлять перемещение сотрудников, чтобы не возникало "конфликтных" ситуаций, связанных с вхождением точки прохода более чем в одну область.

Запрет двойного прохода (антипассбэк, АПБ)

Локальный (аппаратный) антипассбэк осуществляется самим контроллером и включается установкой флажка в настройках. Т.е. при локальном антипассбэке информация о проходе пользователя хранится в контроллере и он сам принимает решение на отказ в повторном проходе, генерируя соответствующую транзакцию.

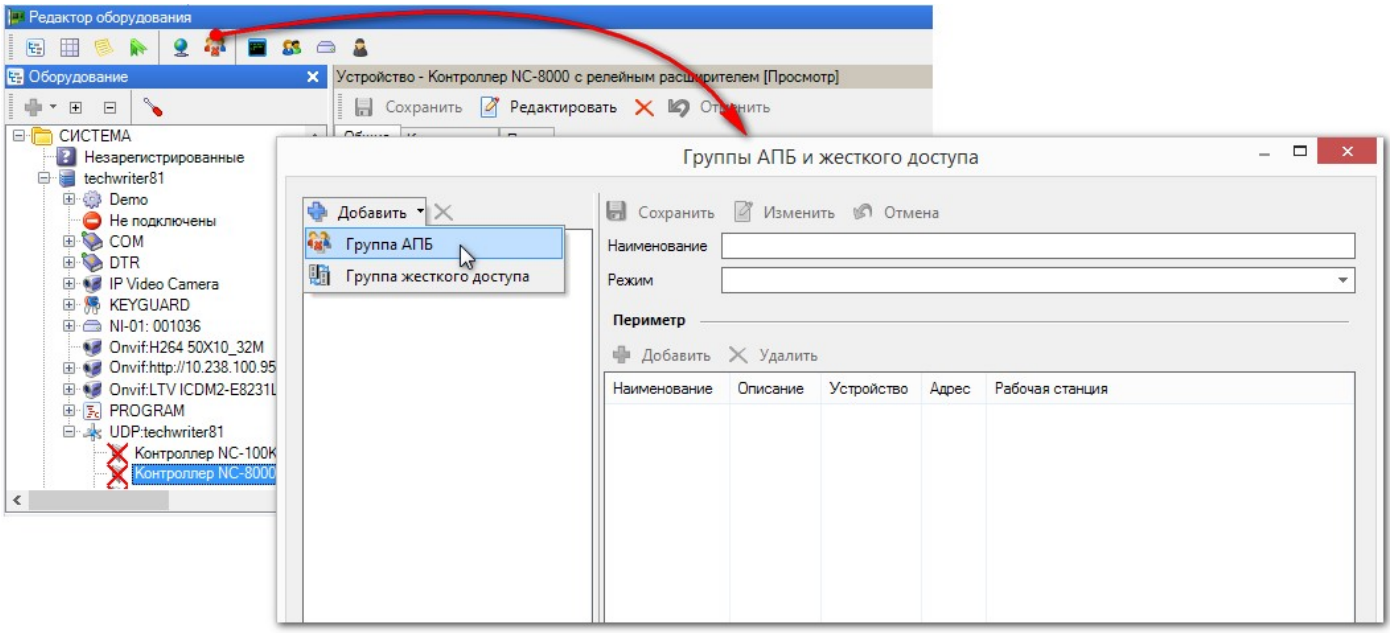
При глобальном (программном) антипассбэке информация о проходе пользователя рассылается на все контроллеры, входящие в область антипассбэка при помощи ПО. Поэтому, например, при проблемах со связью с компьютером функция глобального антипассбэка не сможет функционировать надлежащим образом.



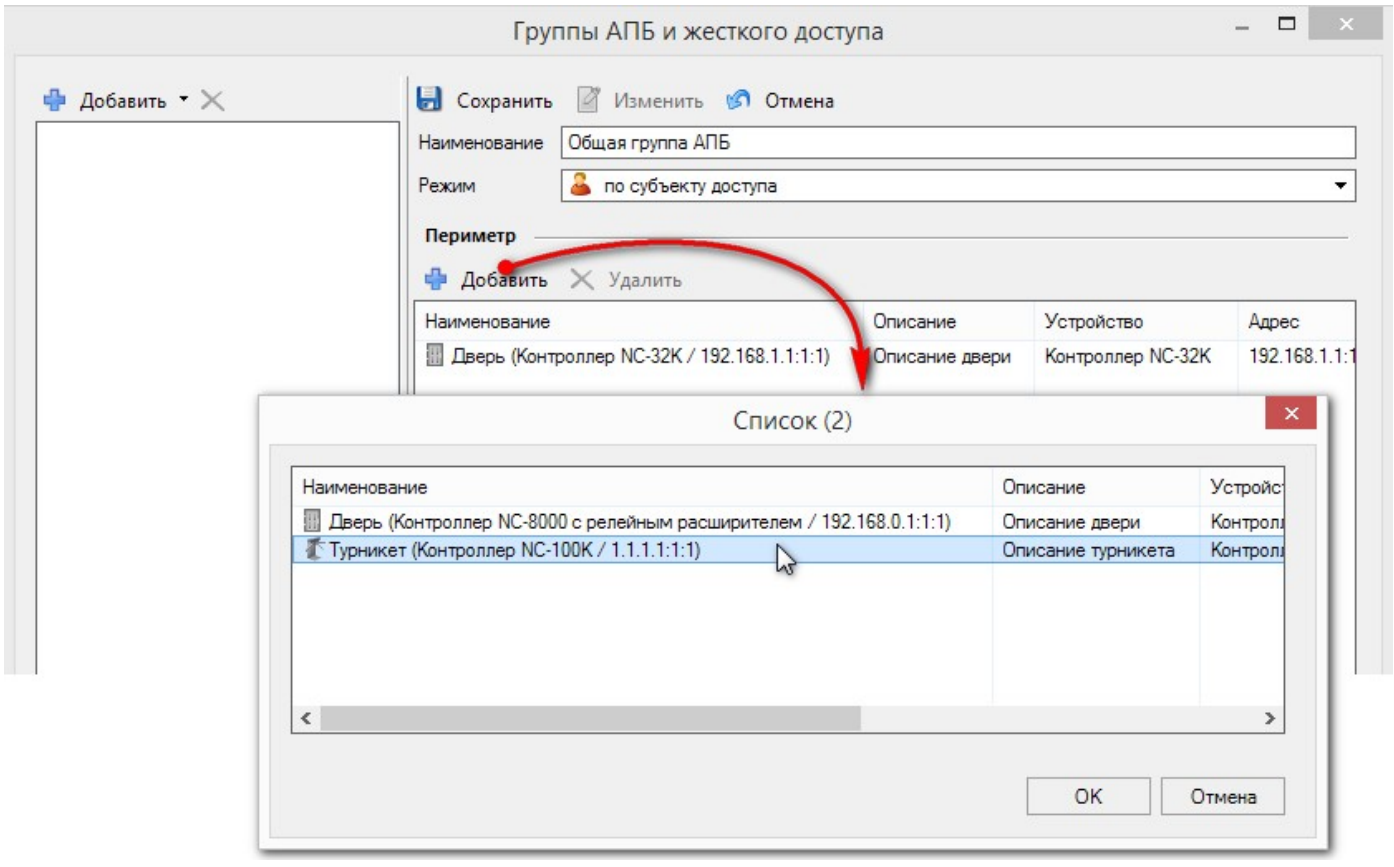
В список контроллеров для создания областей антипассбэка попадут только контроллеры, в которых включен режим антипассбэка.

Область антипассбэка задается следующим образом:

1. Установите флажок *Антипассбэк* в настройках тех контроллеров, которые должны поддерживать АПБ;
2. Откройте окно редактирования групп антипассбэка и жесткого доступа, нажмите на кнопку *Добавить* и выберите команду *Группа АПБ*:



3. Введите название группы и выберите режим:
   - "по идентификатору" - информация на контроллеры группы АПБ рассылается для контроля только одного идентификатора;
   - "по субъекту доступа" - информация на контроллеры группы АПБ рассылается для контроля всех идентификаторов субъекта доступа (т.е. ему не удастся пройти, например, на вход по одному идентификатору, а потом - по другому).
4. В блоке данных *Периметр* нажмите на кнопку *Добавить* и, удерживая клавишу *Ctrl*, отметьте контроллеры (не менее двух), которые образуют контур антипассбэка, затем сохраните результат:



В список контроллеров области АПБ могут входить как контроллеры с двухсторонним проходом (два считывателя), так и с односторонним, поскольку точки прохода могут работать в одном направлении (один турникет только на вход, другой только на выход).

Замечания:

1. Не рекомендуется использовать АПБ на обычных дверях, так как в этом случае не гарантируется определение местонахождения человека (в отличие от турникета).
2. Для четкой работы режима АПБ желательно включать на контроллере, управляющем турникетом, режим фактического прохода.

Сброс АПБ для пользователя описан в разделе[298] Монитора событий.

8.1.15.3 Жесткий доступ

Назначение функции

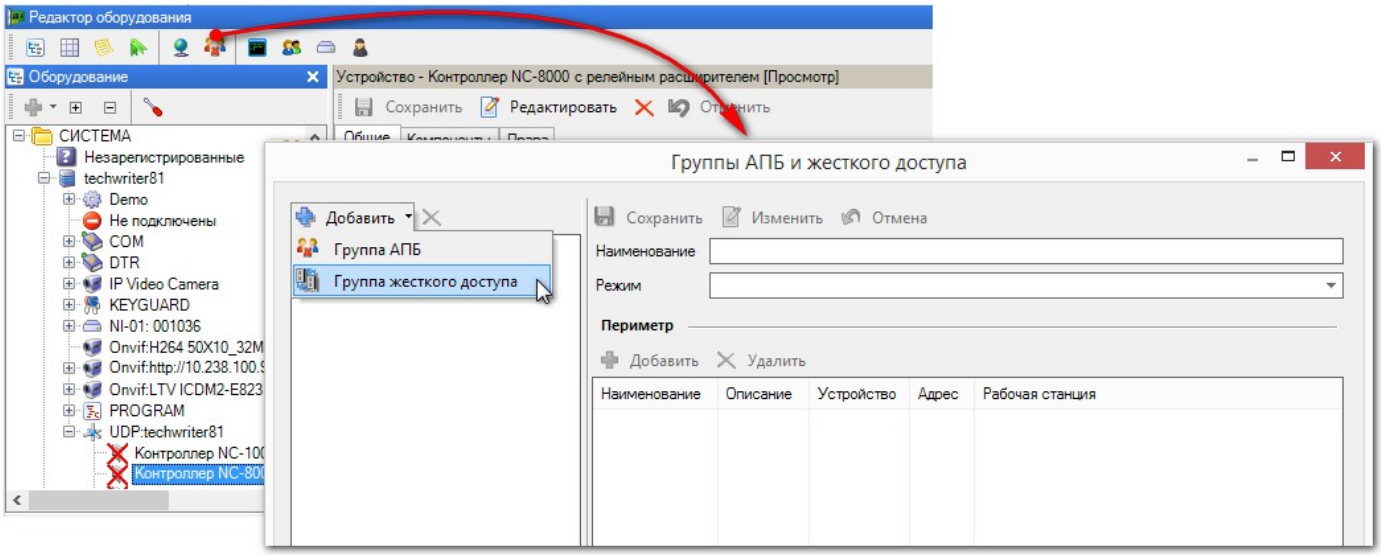
Функция "жесткий доступ" позволяет не пропустить человека на внутреннюю территорию, если он не прошел через внешний периметр, то есть субъект доступа при использовании жесткого доступа должен обязательно "отметиться" на определенных точках прохода в заданной последовательности. Иными словами, система "отслеживает" правильность пути, по которому человек попадает на рабочее место.

Следует иметь в виду, что функция работает только при условии, что компьютер, к которому подключены контроллеры доступа, находится во включенном состоянии, поскольку именно через ПК передается информация о проходах через заданные точки прохода.

Жесткий доступ

В список контроллеров для определения периметра попадут только контроллеры, у которых в конфигурации указаны оба считывателя - и внешний, и внутренний, так как иначе нахождение субъекта доступа внутри территории определить невозможно.

Для организации жесткого доступа следует определить контроллеры двух областей: периметра и внутренних помещений. Для этого откройте панель редактора групп АПБ и жесткого доступа и нажмите на кнопку *Добавить*:

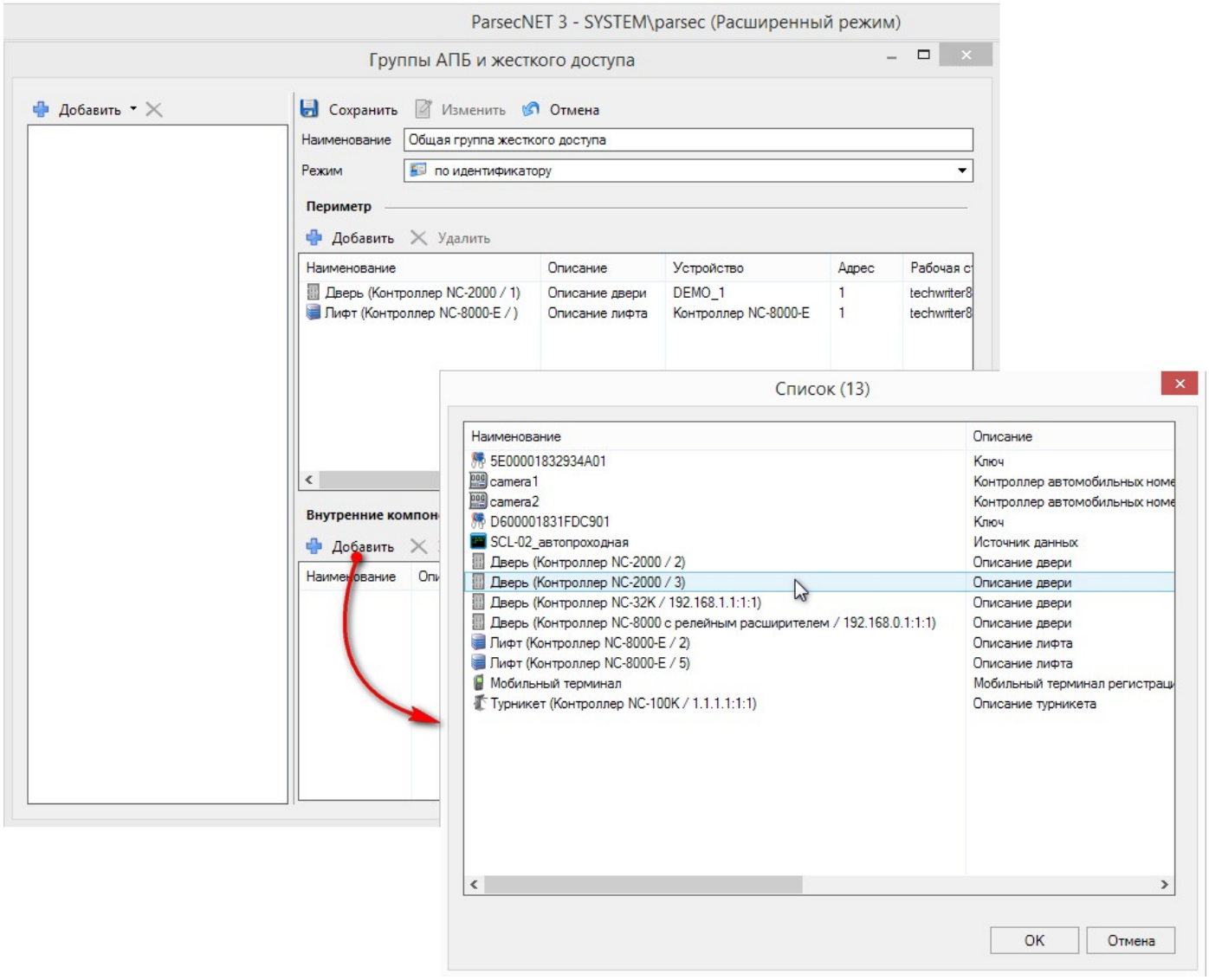


Введите название группы и выберите режим:

- "по идентификатору" - информация на контроллеры группы жесткого доступа рассылается для контроля только одного идентификатора;

- "по субъекту доступа" - информация на контроллеры группы жесткого доступа рассылается для контроля всех идентификаторов субъекта доступа.

Теперь необходимо в верхнем списке *Периметр* отметить контроллеры, которые образуют периметр территории для жесткого доступа, а в нижнем списке *Внутренние компоненты* - элементы системы, обслуживающие внутренние помещения:



Сохраните настроенную группу жесткого доступа, нажав на кнопку *Сохранить*.

После создания, сохранения или удаления группы жесткого доступа настоятельно рекомендуется произвести инициализацию тех контроллеров, которые входили в состав Внутренних компонентов и были из них удалены.

Замечания:

1. На периметральных точках прохода желательно использовать турникеты.
2. Для четкой работы режима жесткого доступа на контроллерах рекомендуется включить режим фактического прохода.

8.1.16 Многосерверность

Начиная с версии 3.7 СКУД ParsecNET становится мультисерверной. Это означает, что в крупной, территориально распределенной организации можно установить несколько серверов

ParsecNET и организовать между ними синхронизацию некоторых данных для выполнения следующих общих задач:

- Обеспечение сквозного доступа сотрудников компании на территории филиалов;
- Получение бесшовных кумулятивных отчетов УРВ по подразделениям компании вне зависимости от фактических перемещений (командировок);
- Обеспечение единообразной структуры данных (правила наименования, структура подразделений, праздники и т.д.) всех филиалов;
- Облегчение разворачивания СКУД в новых точках.

Для успешного решения этих задач в вовлеченных филиалах (серверах) необходимо выполнить следующие общие шаги:

1. Установить и настроить ftp-сервер[166]. Если подключение к ftp-серверу невозможно, используйте обмен данными вручную[179];
2. Настройка кластера:
   - Подключиться к ftp-серверу[171];
   - Настроить топологию[177]: отнести к территории "Периметр" необходимые для учета точки прохода. В отчетах УРВ по прикомандированным сотрудникам будут отображаться события прохода через эти точки прохода;
   - Создать[178] и сделать совместной группу доступа, которая будет назначаться прикомандировывающимся сотрудникам.
3. Перевести объекты в категорию совместных[182];
4. Повторно выдать[183] командируемым сотрудникам их идентификаторы (карты), назначив им совместную группу доступа, созданную тем филиалом, куда командируется сотрудник.

По завершении этих шагов события по проходу командированного сотрудника через точки доступа в филиале, куда он командируется, будут учитываться в системе. Т.е. с точки зрения системы это будет один и тот же сотрудник, как по месту основной работы, так и по месту командировки. Это позволяет легко составлять отчеты УРВ по командированным сотрудникам.

Мастер-сервер - это обычный связанный сервер, имеющий дополнительные права на передачу данных в кластер. В кластере может быть только один мастер-сервер, но кластер может функционировать и без него. Роль мастер-сервера может, при необходимости, передаваться между серверами кластера. Связанные сервера кластера могут обмениваться следующими данными:

1. Персонал;
2. Идентификаторы;
3. Группы доступа;
4. События доступа.

Мастер-сервер, в дополнение к этим данным, может рассылать связанным серверам:

1. Расписания;
2. Праздники;
3. Шаблоны печати;
4. Шаблоны дополнительных полей.

Лицензирование

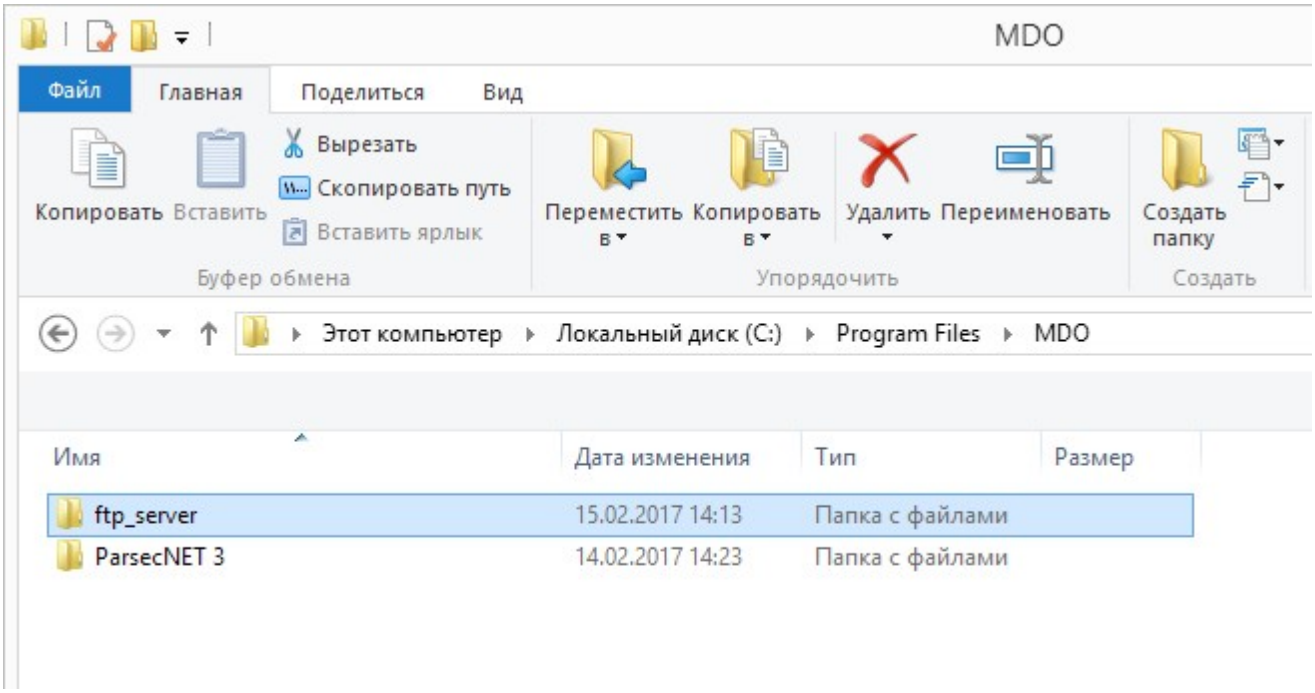
Связанный сервер можно создать только на том ПК, на котором стоит аппаратный ключ защиты лицензии PNSoft-Standart или PNSoft-Proffessional. Однако мастер-сервером можно назначить только тот сервер, который установлен на ПК с аппаратным ключом лицензии PNSoft-Proffessional.

8.1.16.1 Установка и настройка ftp-сервера FileZilla

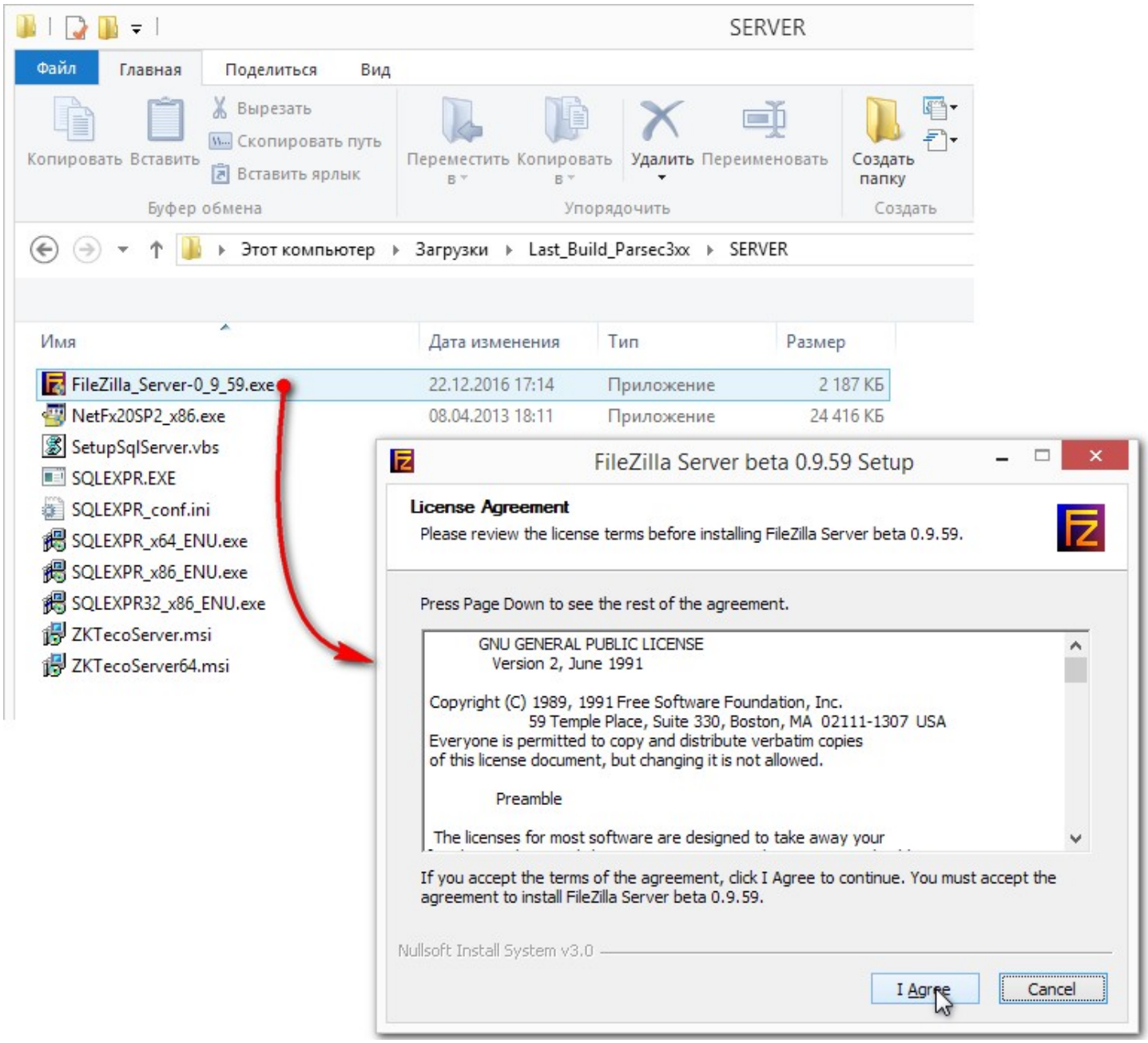
Обмен данными между серверами кластера осуществляется посредством ftp-сервера. Можно создать ftp-сервер на той же машине, на которой установлен ParsecNET, а можно на другой, если этого требует политика безопасности.

Для установки и настройки ftp-сервера выполните следующие шаги:

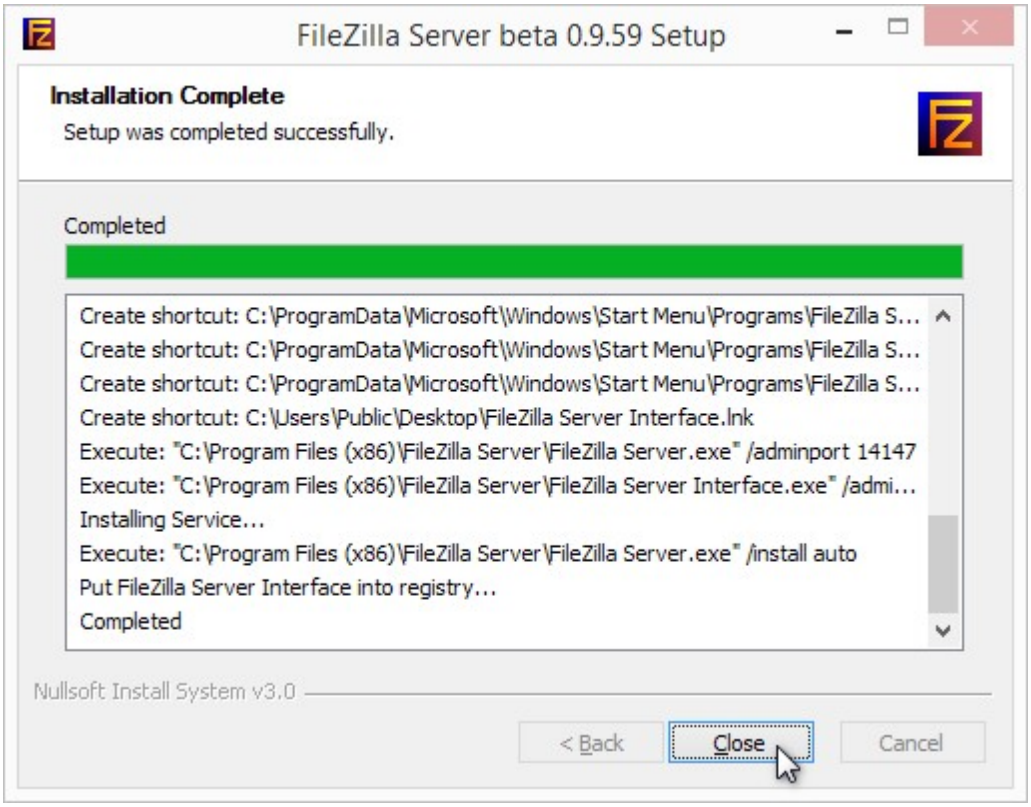
0. Создайте папку с произвольным именем (используйте латиницу) в директории C:\ProgramData\MDO. В ней будут храниться рабочие файлы программы FileZilla. В нашем примере это папка "ftp_server":



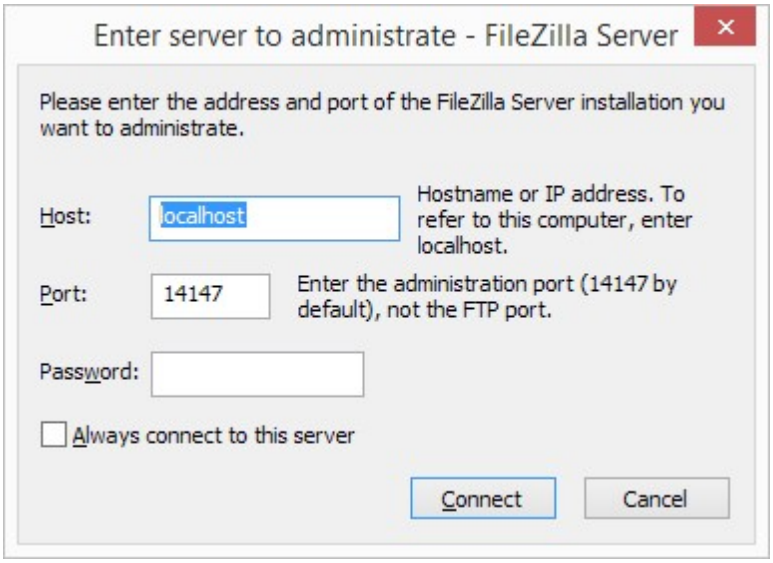
1. Запустите программу установки и настройки ftp-сервера "FileZilla_Server-xxxx.exe". Она находится в папке SERVER вашего установочного дистрибутива СКУД ParsecNET, а также доступна на сайте производителя.
   После двойного щелчка по установочному файлу появится окно лицензионного соглашения.
2. Ознакомьтесь с лицензионным соглашением и нажмите на кнопку *I Agree*.



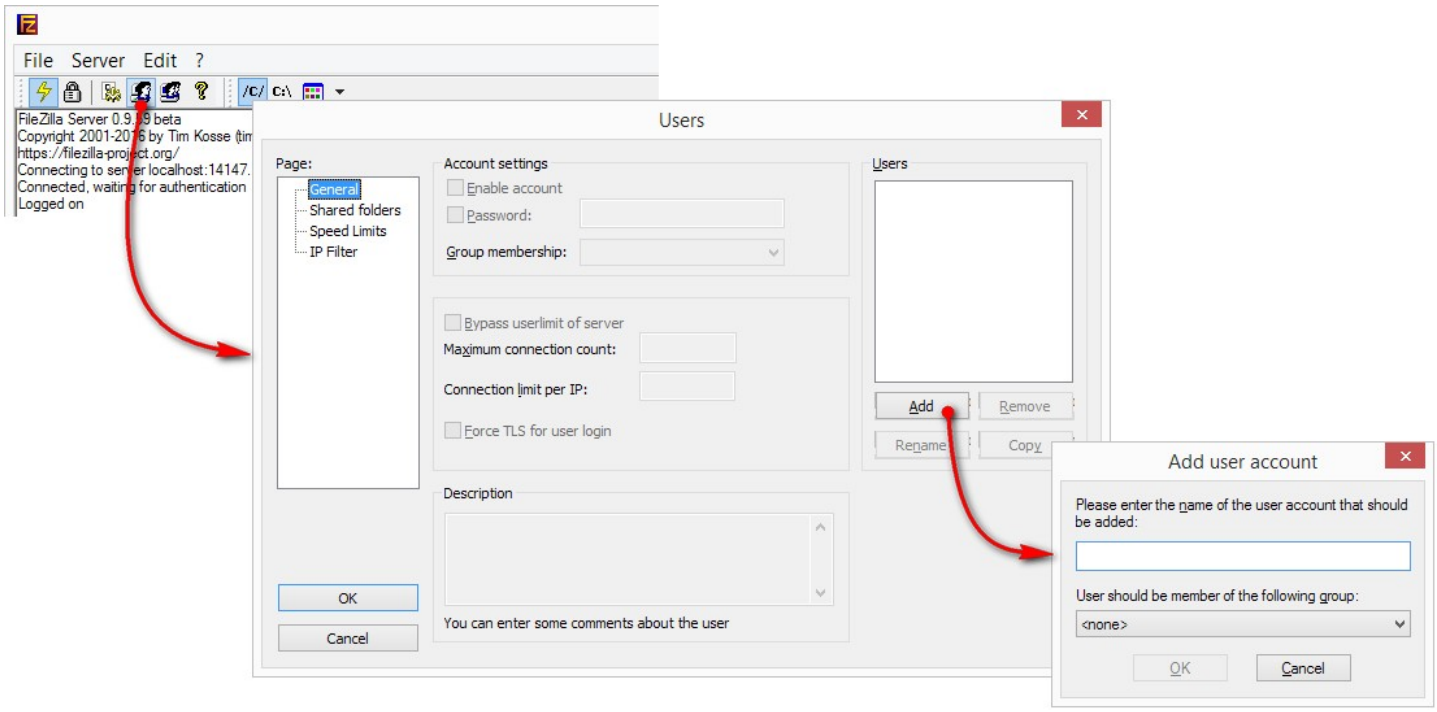
3. Далее следуйте указаниям мастера установки. Рекомендуется оставлять значения по-умолчанию, нажимая на кнопку *Next*. В последнем окне нажмите на кнопку *Install*. Начнется процедура установки ftp-сервера, по завершению которой, нажмите на кнопку *Close*:



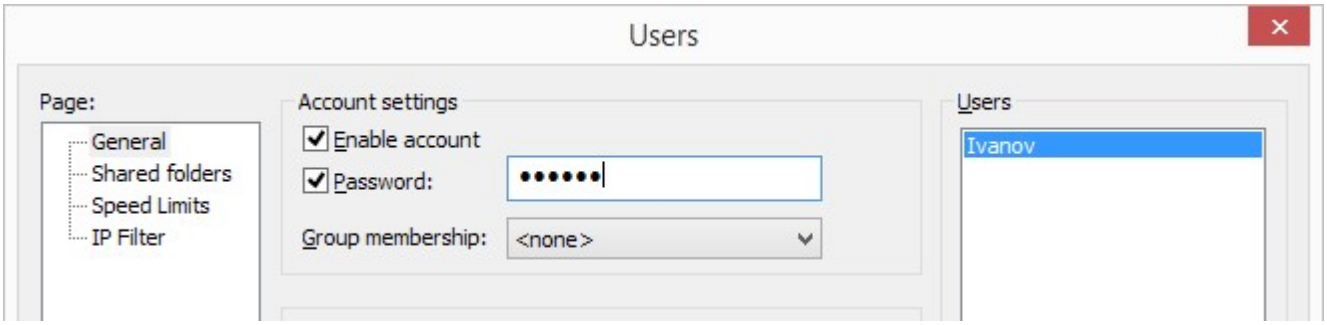
Программа запустится и откроется диалоговое окно подключения к серверу FileZilla:



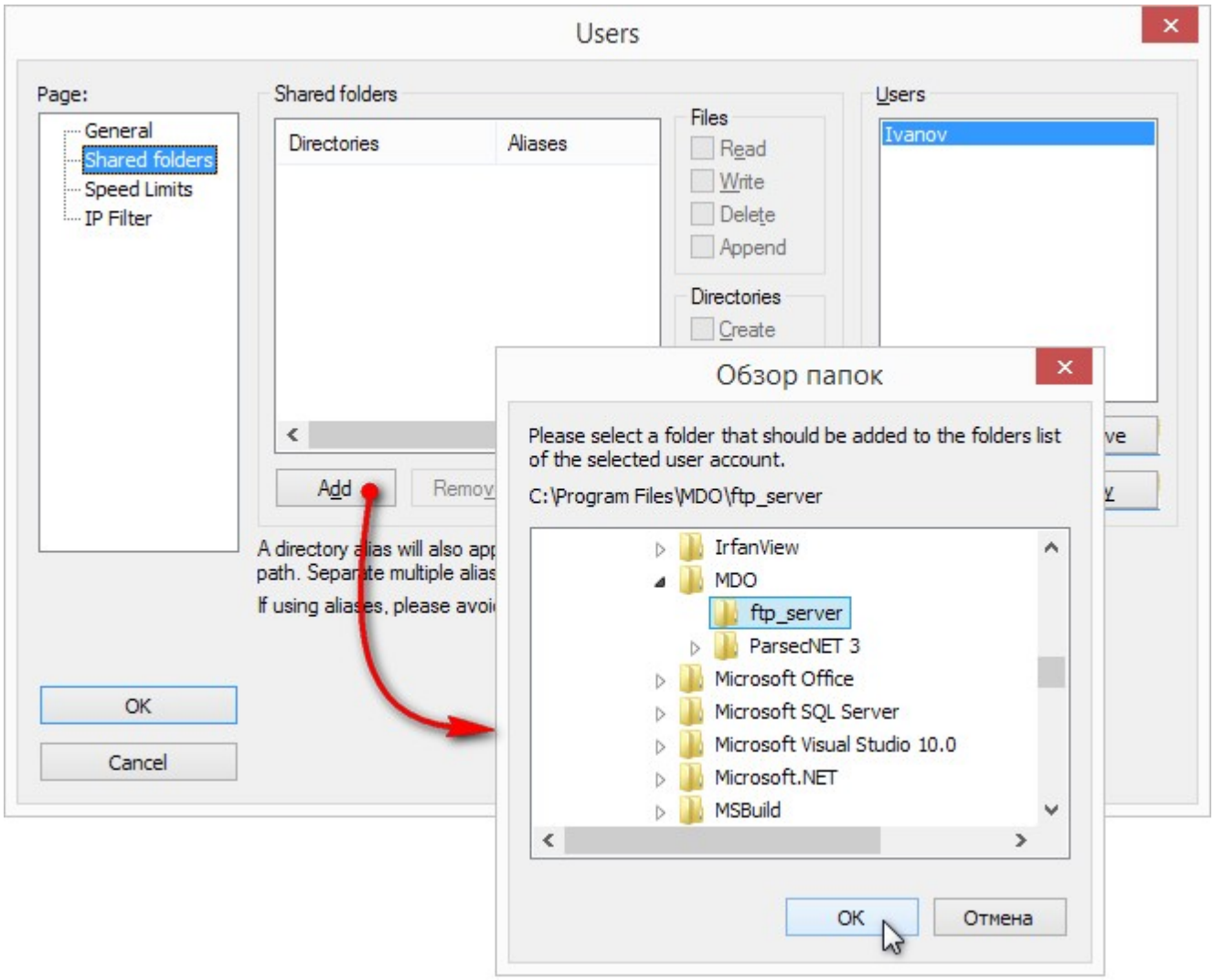
4. Нажмите на кнопку *Connect*, не вводя никаких дополнительных данных. Программа подключится к локальному серверу;
5. Перейдите в окно *Users*, нажав на кнопку с изображением компьютера и одного человека:



6. В блоке *Users* раздела "General" нажмите на кнопку *Add*, откроется окно добавления учетной записи пользователя *Add user account* (см. рис. выше);
7. Введите имя пользователя и нажмите на кнопку *OK*;
8. Поставьте флажок *Password* и задайте пароль. Данные логин и пароль будут использоваться для подключения к ftp-серверу всеми участниками обмена данными в кластере;

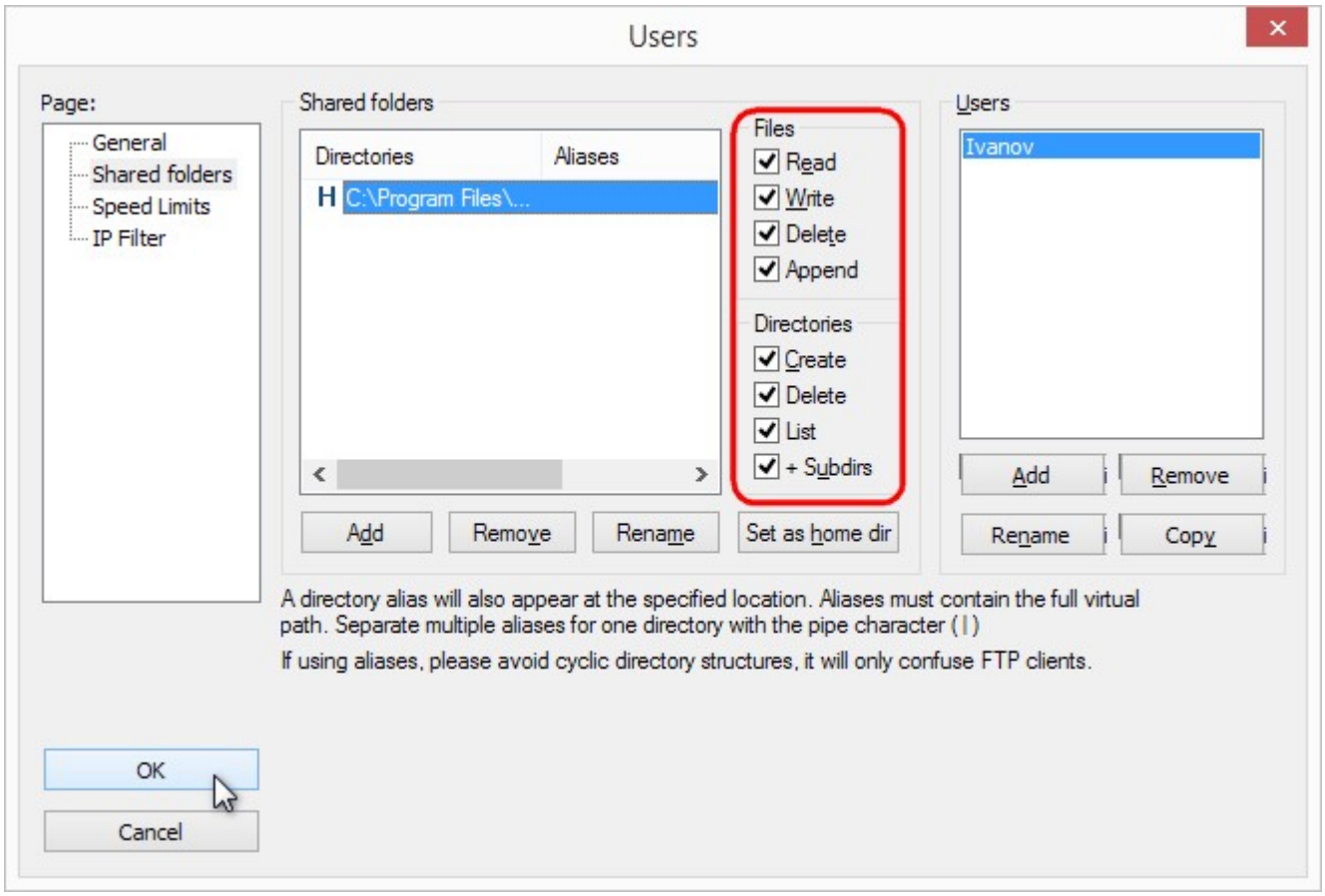


9. Перейдите в раздел "Shared folders" и в блоке данных *Shared folders* нажмите на кнопку *Add*. Откроется окно браузера;
10. Выберите папку, которую создали на шаге 0 (в нашем примере это папка "ftp_server") и нажмите на кнопку *OK*:

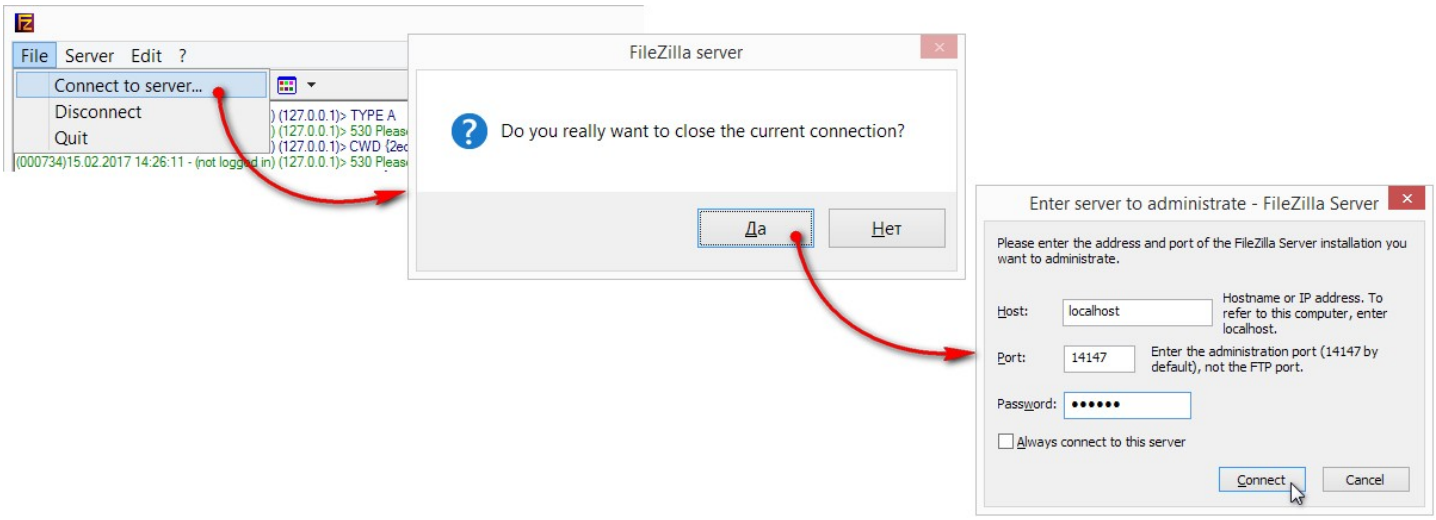


11.Папка будет добавлена в список папок с общим доступом:

12. Выделить добавленную папку и поставьте все флажки в блоках *Files* и *Directories*:



13. Нажмите на кнопку *OK* (см. рис. выше);
14. Откройте пункт главного меню *File* и выберите подпункт *Connect to server*, при появлении системного сообщения нажмите на кнопку *Да*, подтверждая разрыв соединения с сервером производителя программы. Откроется окно нового подключения (см.рис. ниже);
15. Введите пароль, заданный на шаге 8 и нажмите на кнопку *Connect*:



16. Программа подключится к ftp-серверу от имени пользователя, которому принадлежит введенный пароль.

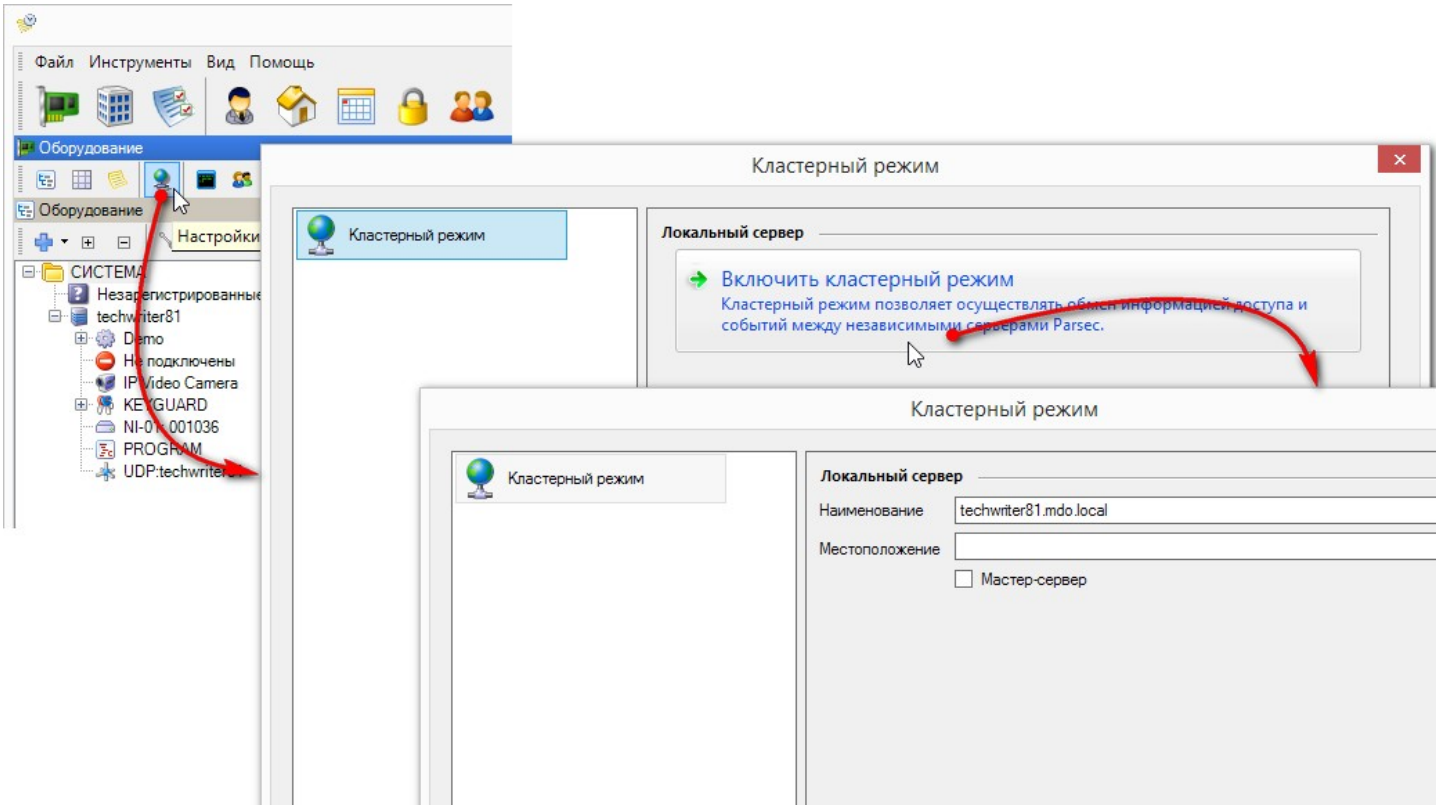
Теперь на серверах кластера ParsecNET необходимо произвести настройки[171] для подключения к этому серверу обмена данными.

Работоспособность с другими ftp-серверами в настоящее время не гарантируется, поскольку каждый из них имеет свои особенности.

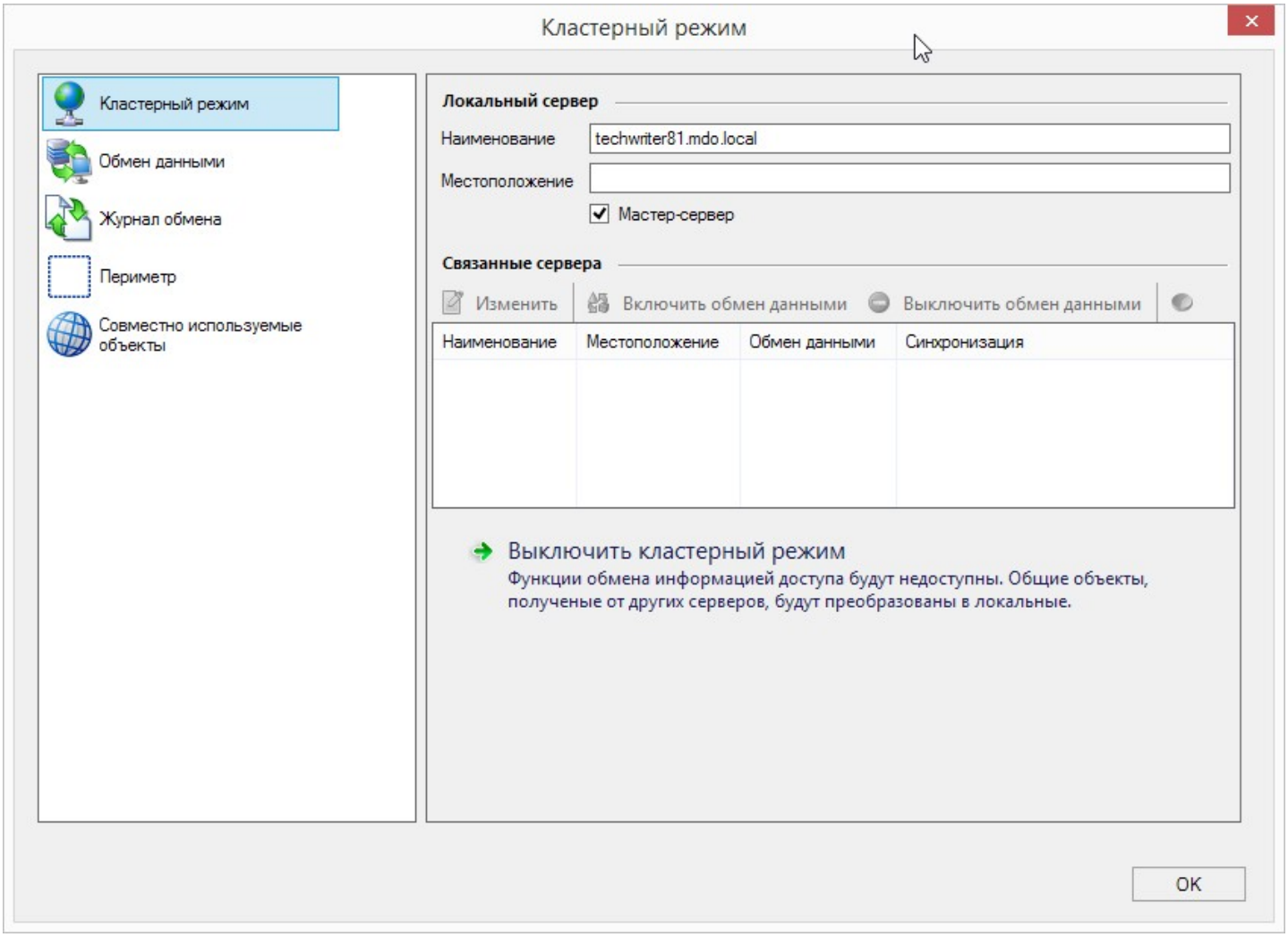
8.1.16.2 Настройка кластера

Для включения сервера в кластер необходимо произвести настройки в Редакторе оборудования. Для этого выполните следующие шаги:

1. В Редакторе оборудования нажмите на кнопку *Настройка кластера*. Откроется окно *Кластерный режим*;
2. Нажмите на кнопку *Включить кластерный режим*, откроется панель *Локальный сервер*:



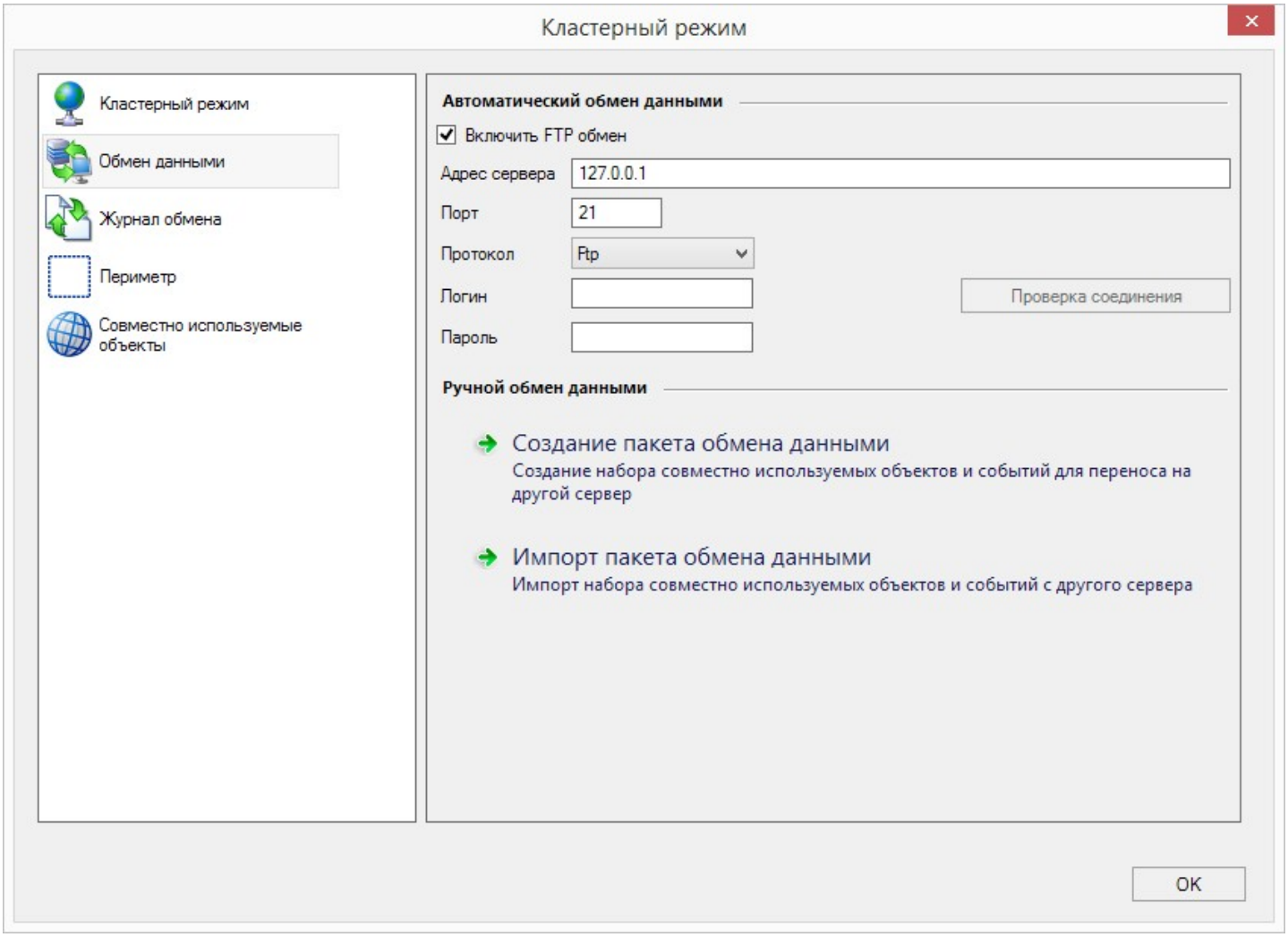
3. Заполните поля:
   - *Наименование* - оставьте созданное автоматически наименование или введите свое. Впоследствии только Вы можете менять это наименование. Оно также будет изменяться на всех серверах кластера;
   - *Местоположение* - необязательное поле. Операторы других серверов кластера в окне *Связанные сервера* (см. рис. ниже) могут изменить это поле для Вашего сервера по своему усмотрению, но измененные значения будут видны только им самим. Если же Вы меняете текст в поле *Местоположение* своего сервера, то он меняется и на всех серверах кластера;
   - *Мастер-сервер* - установите флажок, если Ваш сервер является мастер-сервером кластера. Если мастер-сервер уже существует в кластере, установить флажок не удастся.
   Если мастер-сервер меняется, то кластер будет пользоваться расписаниями, списком праздничных дней, шаблонами печати и доп.полей старого мастер-сервера до тех пор, пока оператор нового мастер-сервера не обновит эти данные.
4. Нажмите на кнопку *ОК*. Окно *Кластерный режим* закроется;
5. Снова нажмите на кнопку *Настройка кластера.* Открывшееся окно *Кластерный режим* будет иметь другой вид:



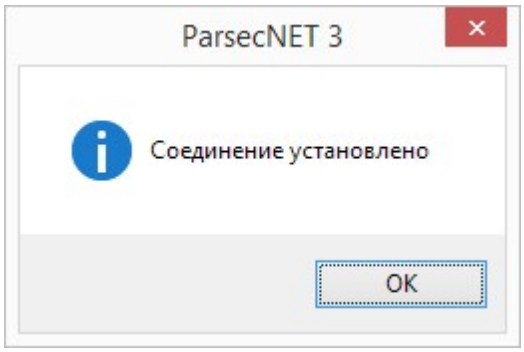
Левая панель содержит следующие разделы:

- *Кластерный режим* - открывается по-умолчанию. Позволяет изменить описание местоположения текущего сервера, просматривать и настраивать взаимодействие со связанными серверами и выключать кластерный режим;
- *Обмен данными* - предназначен для настройки локального сервера для связи с ftp-сервером, а также экспорта и импорта пакетов данных при обмене данными вручную[179];
- *Журнал обмена*[186] - предназначен для отслеживания переданных и полученных файлов связанными серверами кластера;
- *Периметр*[177] - предназначен для выбора точек прохода, предназначенных для совместных групп доступа. У каждого сервера кластера свой состав точек прохода в периметре;
- *Совместно используемые объекты* - в этом разделе оператор сервера переводит объекты системы в категорию совместных для участия в обмене данными.

6. Для настройки автоматического обмена данными или создания файла для ручного обмена перейдите в раздел *Обмен данными*:



7. Установите флажок *Включить FTP обмен* и заполните ставшие активными поля:
   - *Адрес сервера* - IP-адрес сервера обмена данными (ftp-сервера);
   - *Порт* - оставьте 21 порт по-умолчанию, или введите номер порта, указанный в настройках ftp-сервера;
   - *Протокол* - из раскрывающегося списка выберите один из двух поддерживаемых протоколов передачи данных:
     - *FTP* (File Transfer Protocol) - стандартный протокол передачи данных;
     - *SFTP* (SSH File Transfer Protocol) - безопасный протокол передачи данных. В отличие от стандартного FTP он шифрует и команды, и данные, предохраняя пароли и конфиденциальную информацию от открытой передачи через сеть.
   - *Логин* - введите логин пользователя, созданного при настройках ftp-сервера на шаге 7;
   - *Пароль* - введите пароль указанного выше пользователя для доступа к ftp-серверу.
8. Нажмите на кнопку *Проверка соединения*. При неудачной попытке установить соединение, проверьте правильность введенных данных, заданных настроек и т.п. и повторите попытку. После соединения с сервером обмена данными система сообщит об этом:

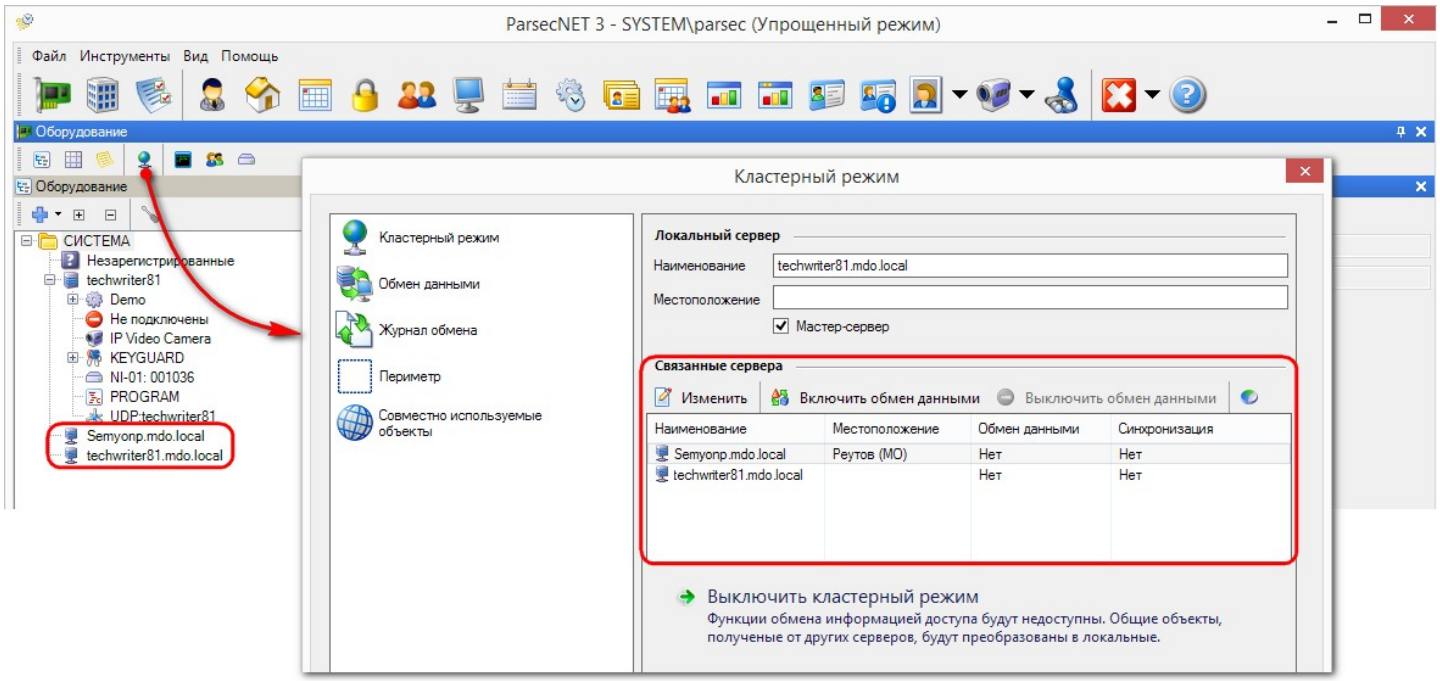


9. Нажмите на кнопку *ОК*.

На этом настройка локального сервера для участия в обмене данными завершена.

Брандмауэр может блокировать прохождение пакетов данных между серверами кластера.

В разделе *Кластерный режим* в блоке *Связанные сервера* теперь будет отображаться список связанных серверов (серверов кластера). Связанные сервера также отображаются в дереве оборудования Редактора оборудования:



Для каждого из связанных серверов можно отредактировать наименование и местоположение. Отредактированные сведения будут видны только Вам.

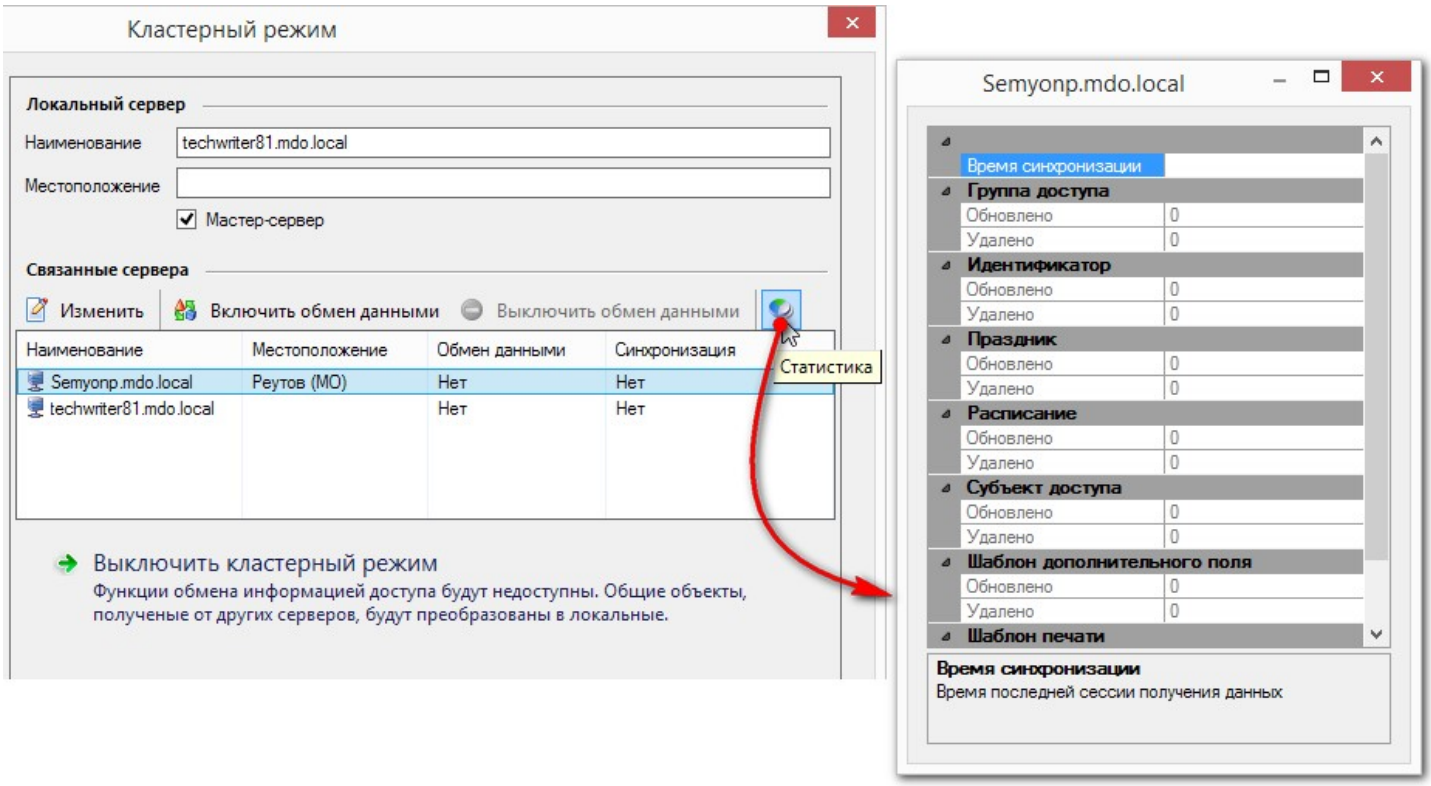
Наименование сервера может редактировать только оператор этого сервера.

После добавления своего сервера в кластер в списке связанных серверов необходимо выделить и включить обмен данными с теми серверами, с которыми это Вам необходимо. Для этого выделите сервер и нажмите на кнопку "Включить обмен данными".

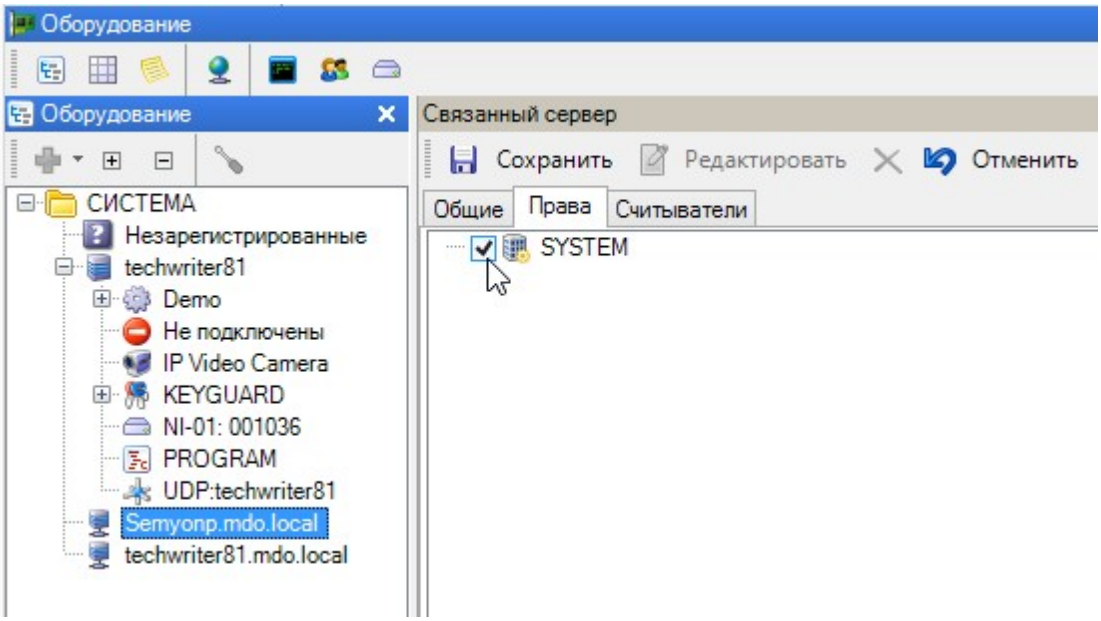
После чего нужно связаться с операторами этих серверов и добиться, чтобы они также включили обмен данными с Вашим сервером. В противном случае обмена данными между вашими серверами не будет.

Остановить обмен даными с выбранным связанным сервером можно кнопкой *Выключить обмен данными*.

Кнопка *Статистика* позволяет просмотреть количество отправленных и полученных данных от выбранного связанного сервера.



Для построения отчетов УРВ по связанному серверу (по его точке прохода на территории "Периметр") необходимо предоставить Вашей организации право доступа. Для этого выделите связанный сервер в дереве Редактора оборудования, перейдите на вкладку *Права* и установите флажок у своей организации (или той организации, которой предоставляется право доступа к событиям прохода ваших командированных сотрудников на связанном сервере):



Выключение кластерного режима

Чтобы исключить сервер из кластера, необходимо нажать на кнопку *Выключить кластерный режим*. При этом связь между вышедшим сервером и остальными серверами кластера полностью прекращается, а с ранее переданными данными производятся следующие действия:

- при выходе обычного сервера на всех связанных серверах **удаляются** совместные группы доступа этого сервера, откомандированные сотрудники становятся **локальными** и у них удаляются идентификаторы, назначенные выходящим из кластера сервером;

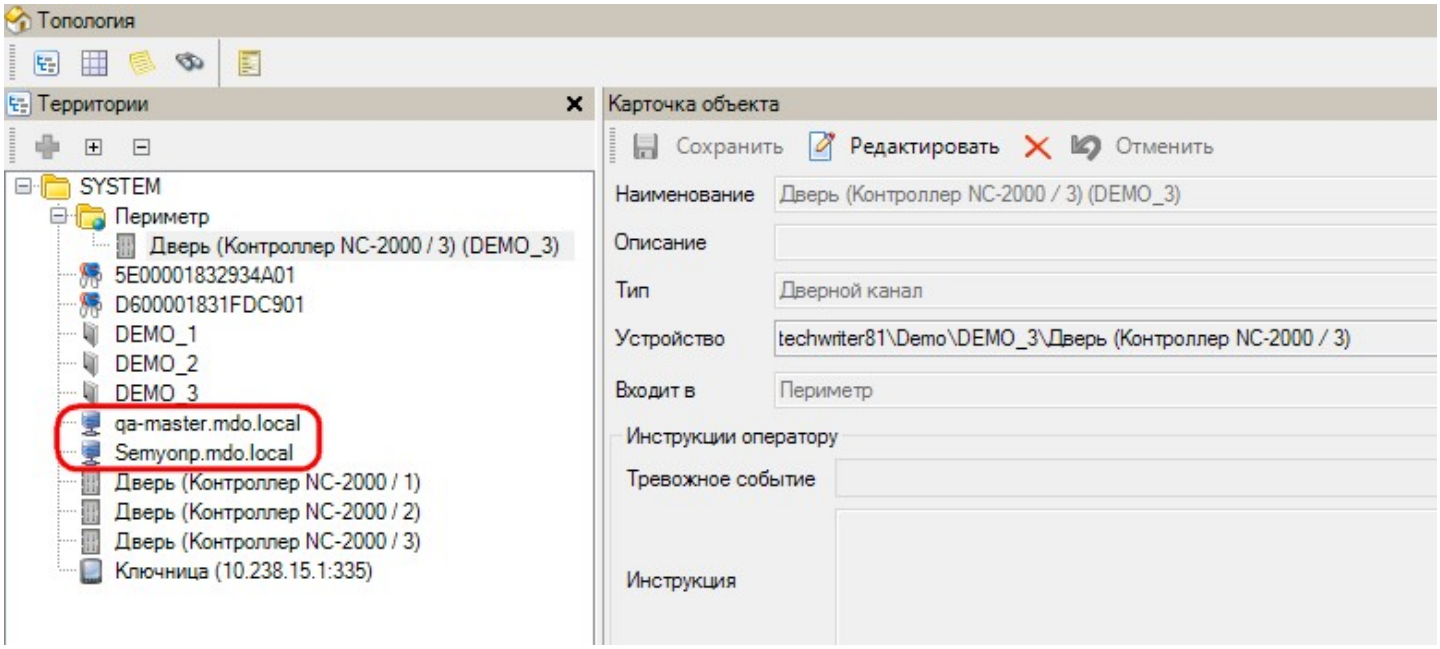
- при выходе мастер-сервера дополнительно к вышеописанному на связанных серверах **локальными** становятся расписания, список праздничных дней, шаблоны печати и доп.полей, переданные этим мастер-сервером.

8.1.16.2.1 Настройка кластера. Периметр

После настройки кластера в Редакторе топологии появляется территория "Периметр", в которой должна размещаться точка прохода, предназначенная для совместной группы доступа. События доступа прикомандированных сотрудников через данную точку прохода будут отправляться на сервер того подразделения, из которого прибыл данный сотрудник.

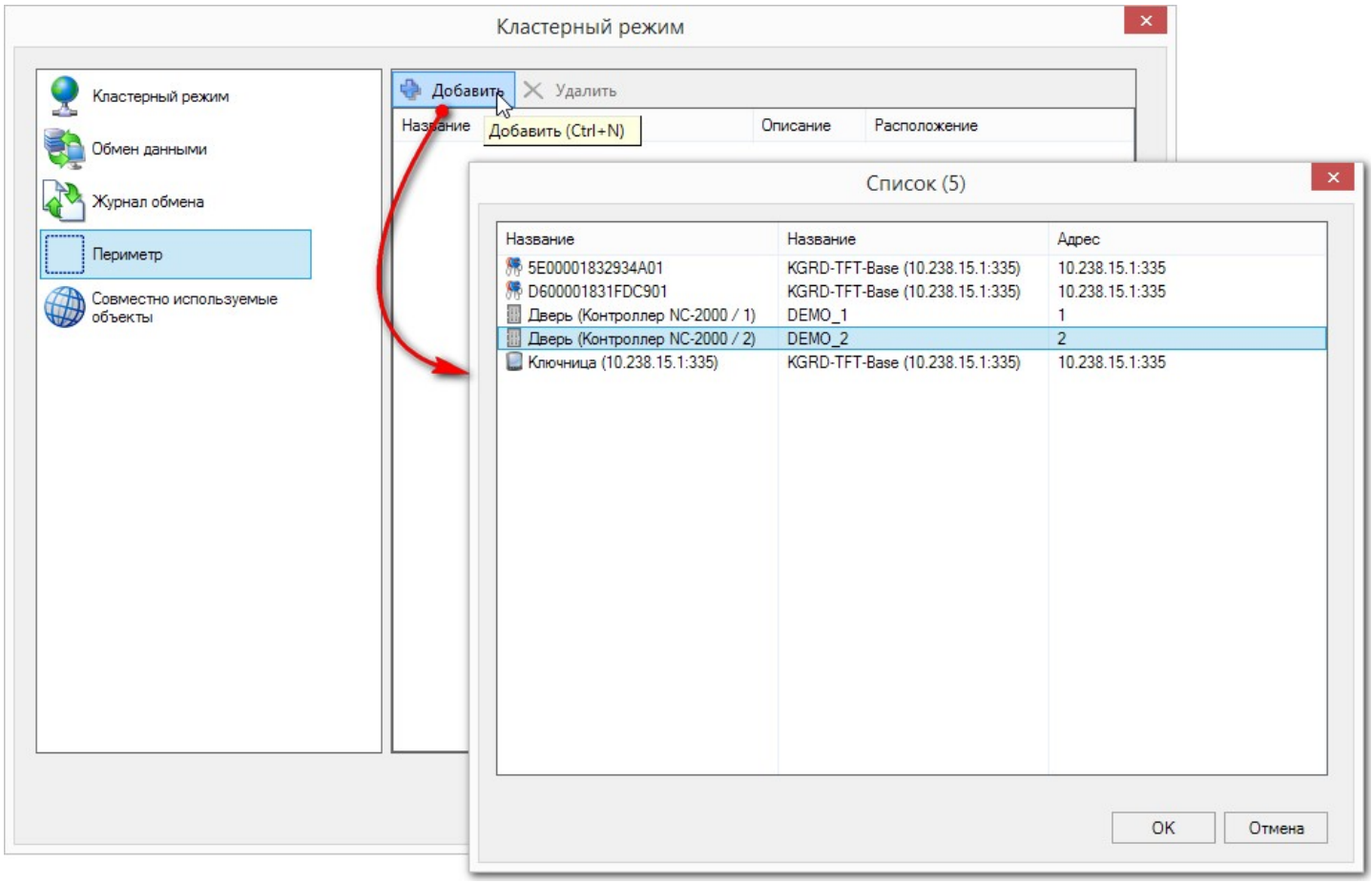
Вы можете получать события доступа по вашим командированным сотрудникам только от тех серверов, которые отображаются в дереве территории Редактора топологии. В нашем примере это территории серверов, выделенных красной рамкой. Хотя в топологии отображается название сервера, система видит за ней точку прохода, входящую в территорию "Периметр" организации, в которой установлен этот сервер.

Территория связанного сервера начинает отображаться в Редакторе топологии после создания совместно используемого объекта.



Сколько бы ни было отнесено к территории "Периметр" точек прохода, для других филиалов события прохода их сотрудников через эти точки будут выглядеть как проход через одну и ту же точку. Поэтому для территории "Периметр" рекомендуется выбрать самую внешнюю точку прохода на территории организации.

Выбор точки прохода может осуществляться как в Редакторе топологии[206], так и в разделе *Периметр* окна *Кластерный режим*:

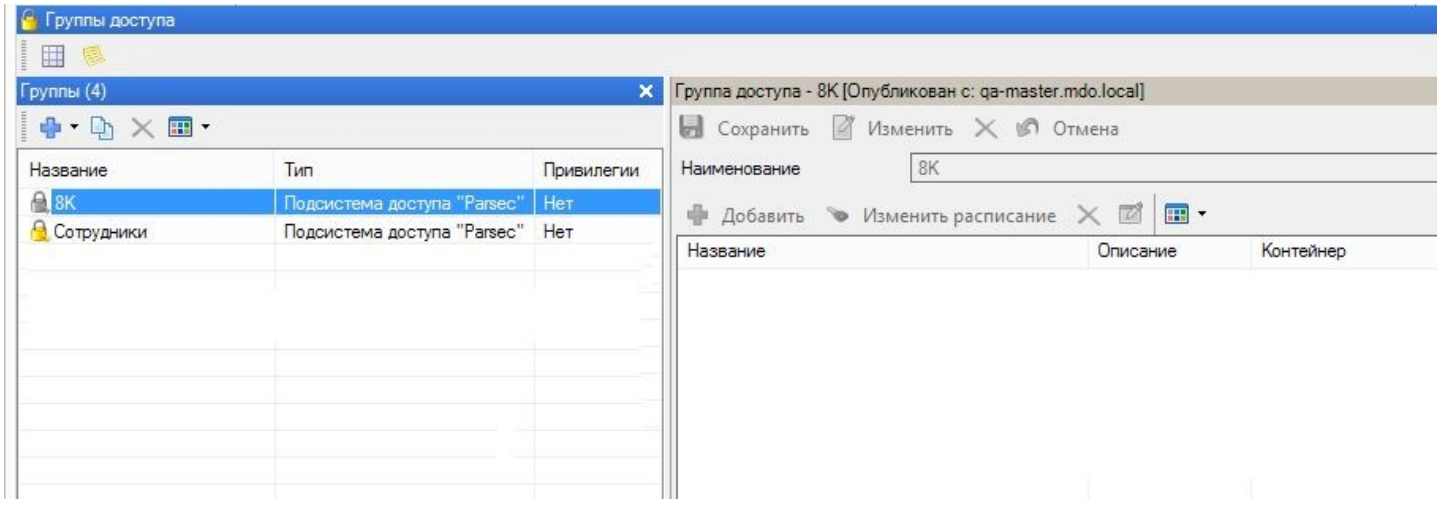


8.1.16.2.2 Настройка кластера. Группа доступа

Чтобы командируемый Вами сотрудник мог проходить на территорию филиала, оператор сервера этого филиала должен создать группу доступа и перевести ее в совместные. Тогда Вы сможете назначить эту группу доступа своему сотруднику и он будет ходить под своим идентификатором как через точки прохода своей организации, так и через периметральную точку прохода принимающего филиала.

И наоборот, если к Вам прикомандировывается сотрудник, Вам также обходимо сделать группу доступа совместной.

Такая группа доступа должна управлять точкой прохода территории "Периметр".



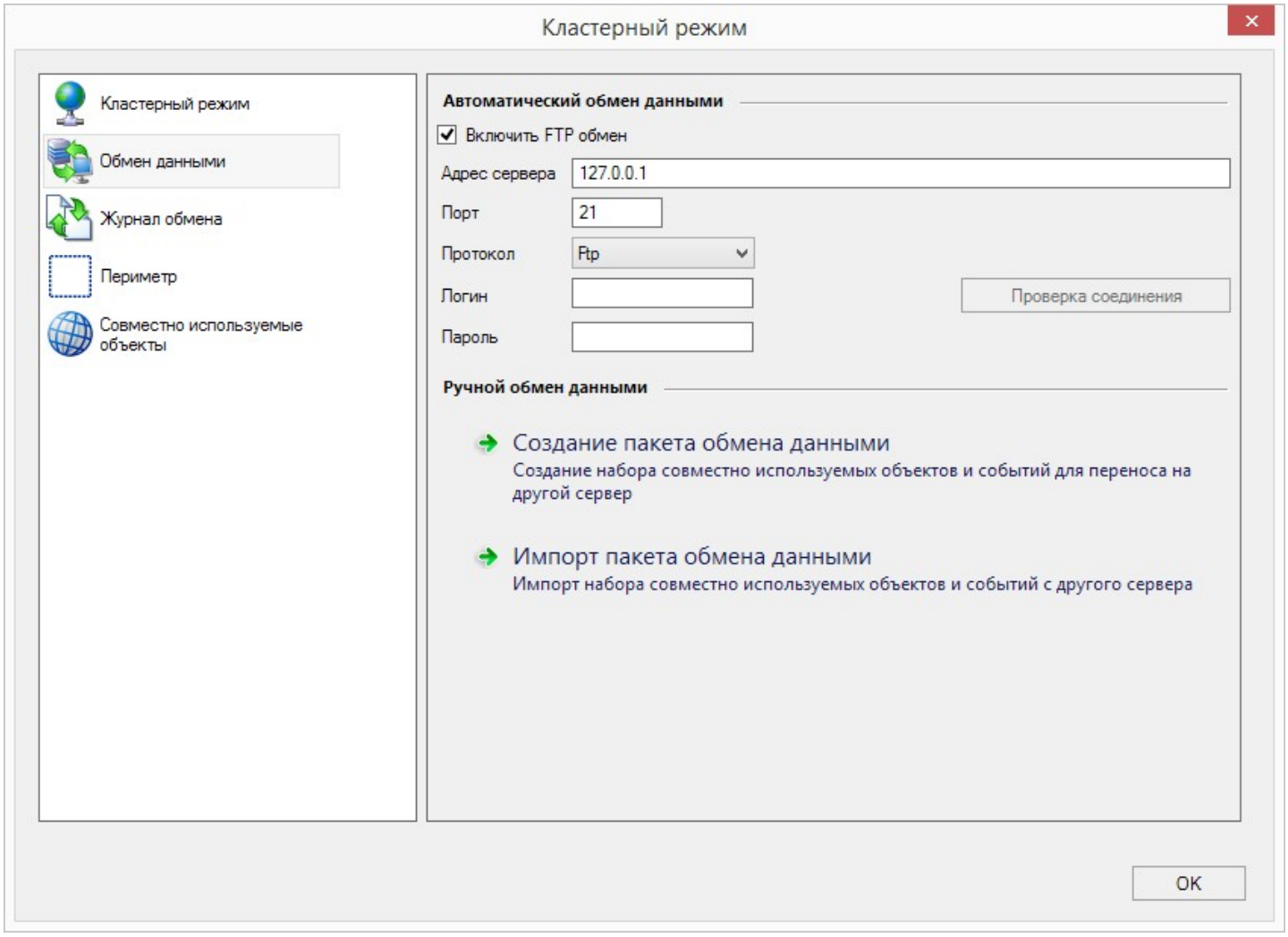
Совместные группы доступа связанных серверов отображаются в Вашем Редакторе групп доступа серым цветом (см. рис. выше, группа "8К"). Вы не можете редактировать такую группу, равно как и у других операторов кластера нет возможности редактировать созданную Вами совместную группу доступа.

8.1.16.3 Передача данных вручную

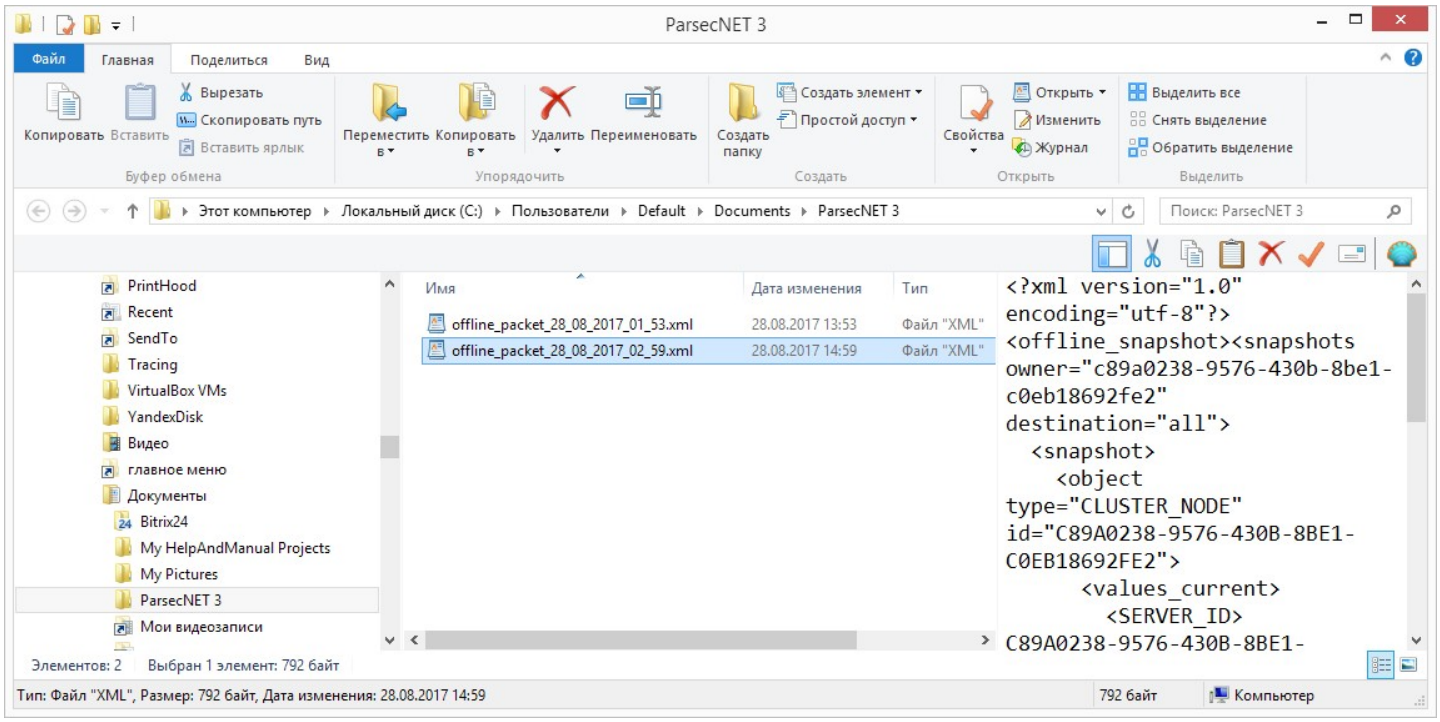
Если по каким-либо причинам между связанными серверами отсутствует и даже если такая связь принципиально не может быть установлена, система позволяет производить обмен данными вручную. Для этого предоставляется функционал экспорта и импорта[180] пакетов данных.

Чтобы сформировать пакет данных для передачи связанному серверу, выполните следующие действия:

1. Нажмите на кнопку *Настройка кластера*. В открывшемся окне перейдите в раздел *Обмен данными*:



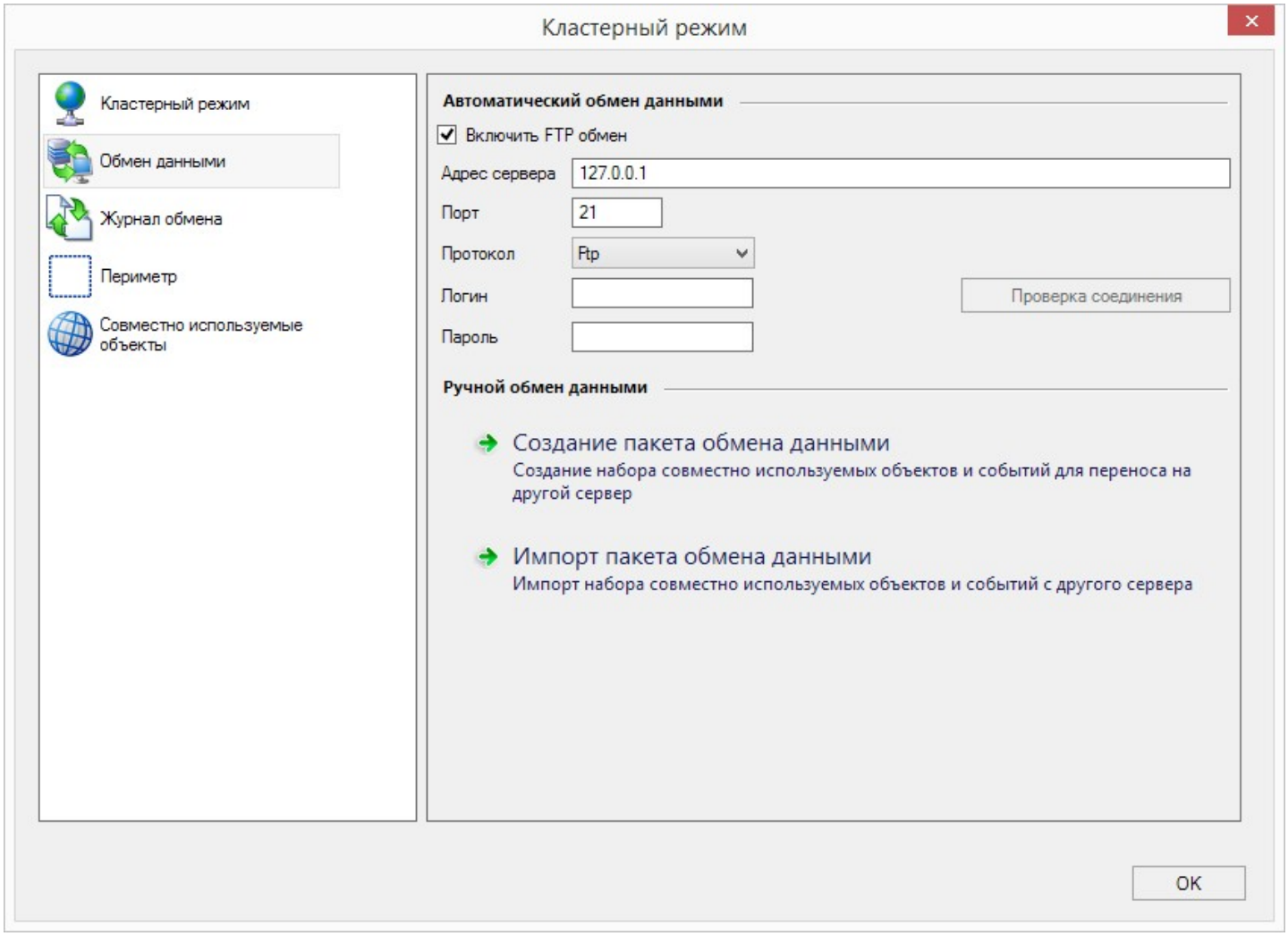
2. Нажмите на кнопку *Создание пакета обмена данными*. Откроется папка, содержащая сгенерированный файл с именем вида offline_packet_<DD_MM_YY_hour_min>. Папка по-умолчанию расположена по адресу C:\Users\<username>\Documents\ParsecNET 3:



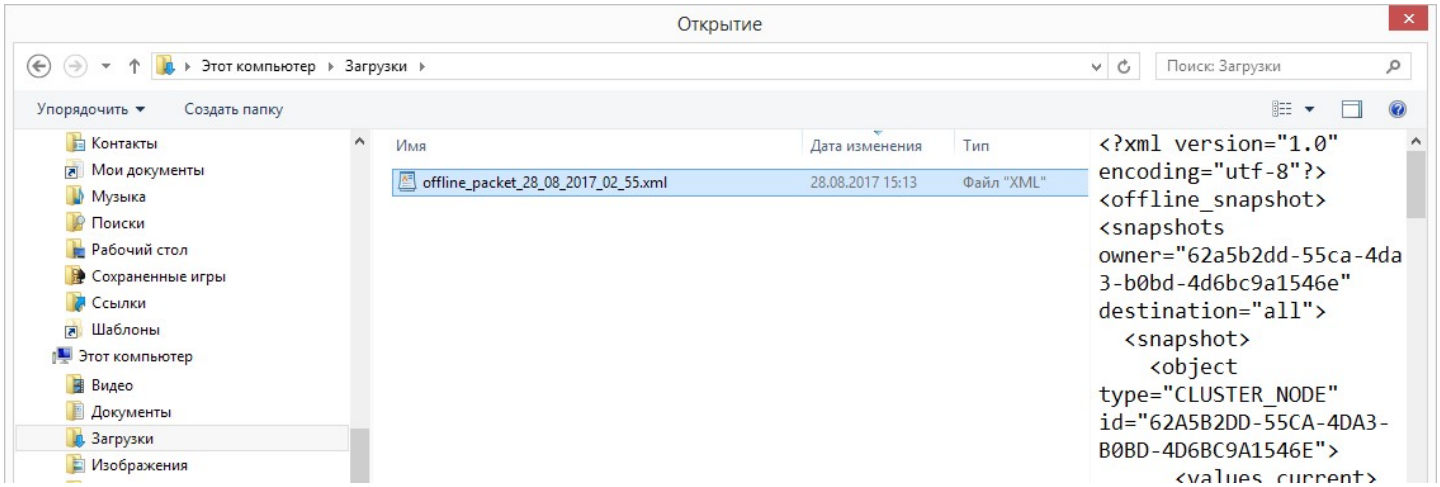
3. Скопируйте файл и отправьте его на нужный сервер или рабочую станцию системы ParsecNET3. (Имя файла, при необходимости, можно изменить).

При получении файла с данными выполните следующие шаги:

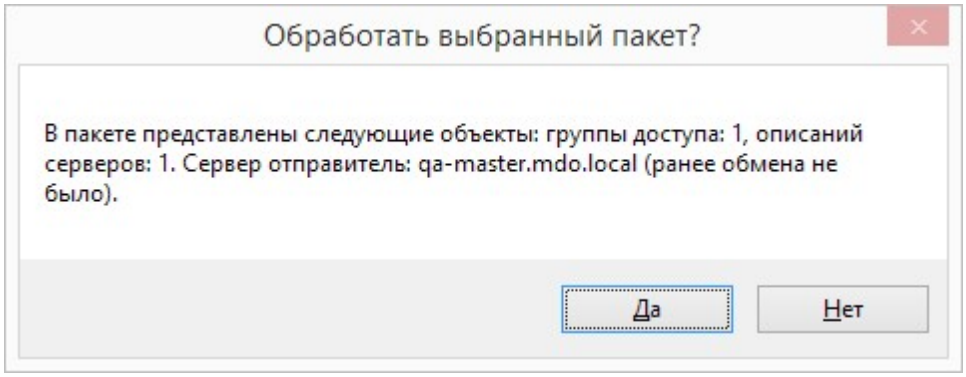
1. Нажмите на кнопку  *Настройка кластера*. В открывшемся окне перейдите в раздел *Обмен данными*:



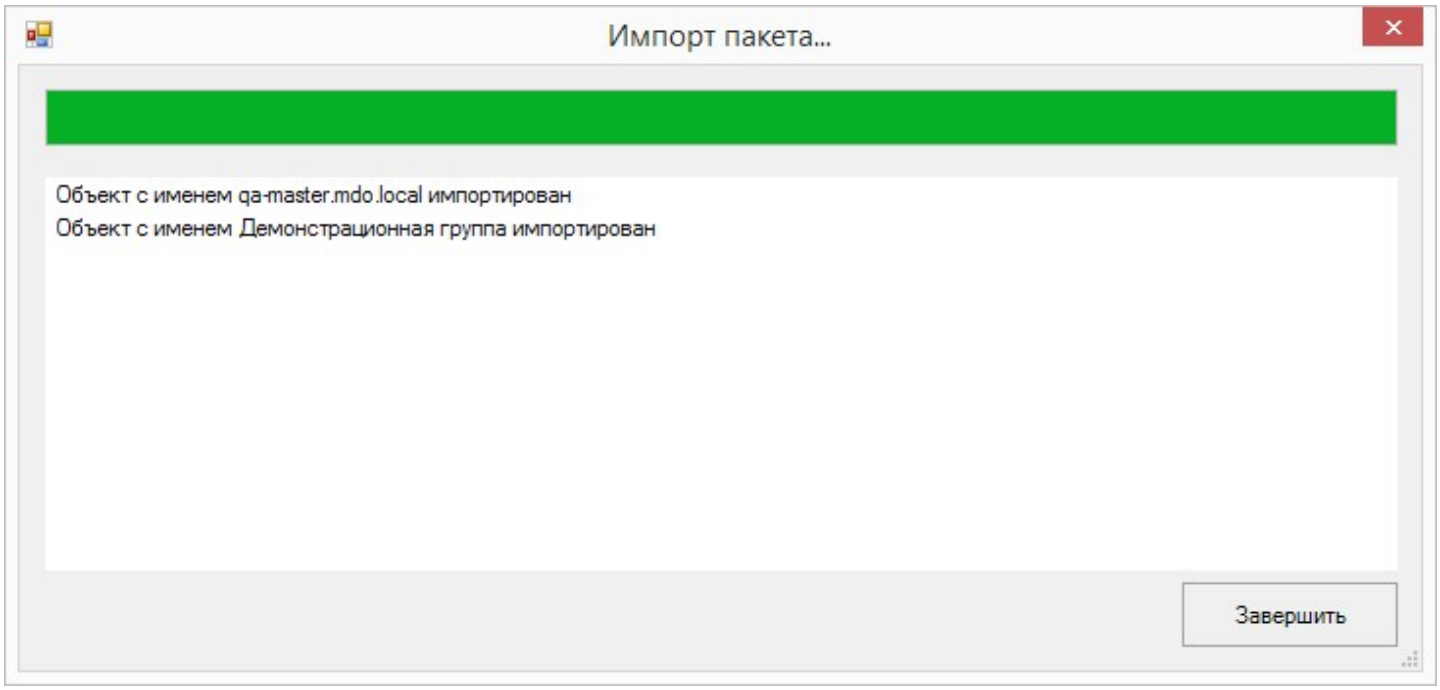
2. Нажмите на кнопку *Импорт пакета обмена данными*. В открывшемся окне выберите и откройте полученный файл с данными:



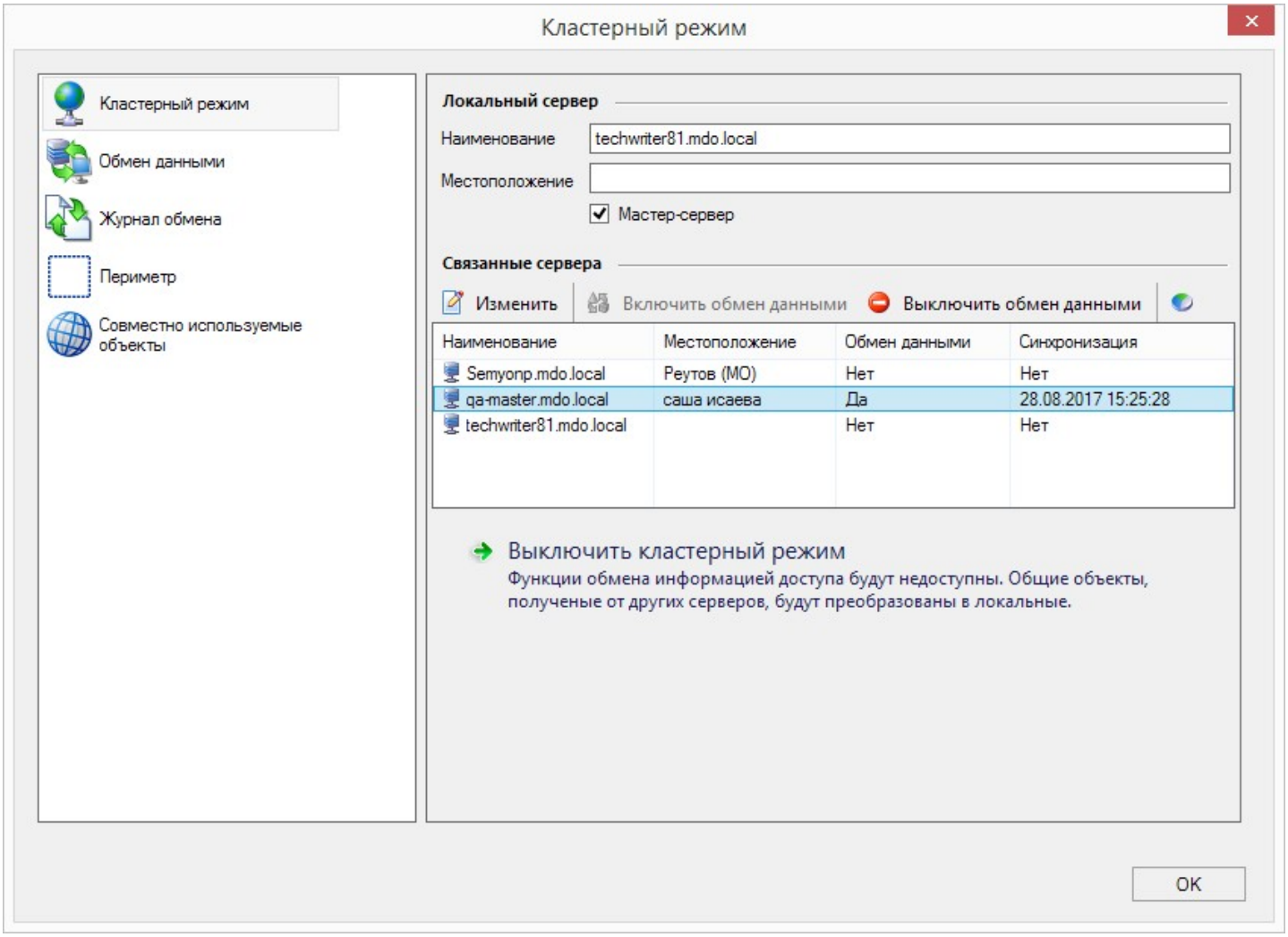
3. Система попросит подтвердить действие. Нажмите на кнопку *Да*, чтобы выполнить импорт:



4. Начнется обработка пакета. По окончании процесса нажмите на кнопку *Завершить*:



5. Теперь в системе ParsecNET 3 на текущем компьютере появились публичные объекты связанного сервера, с которым нет связи по сети:



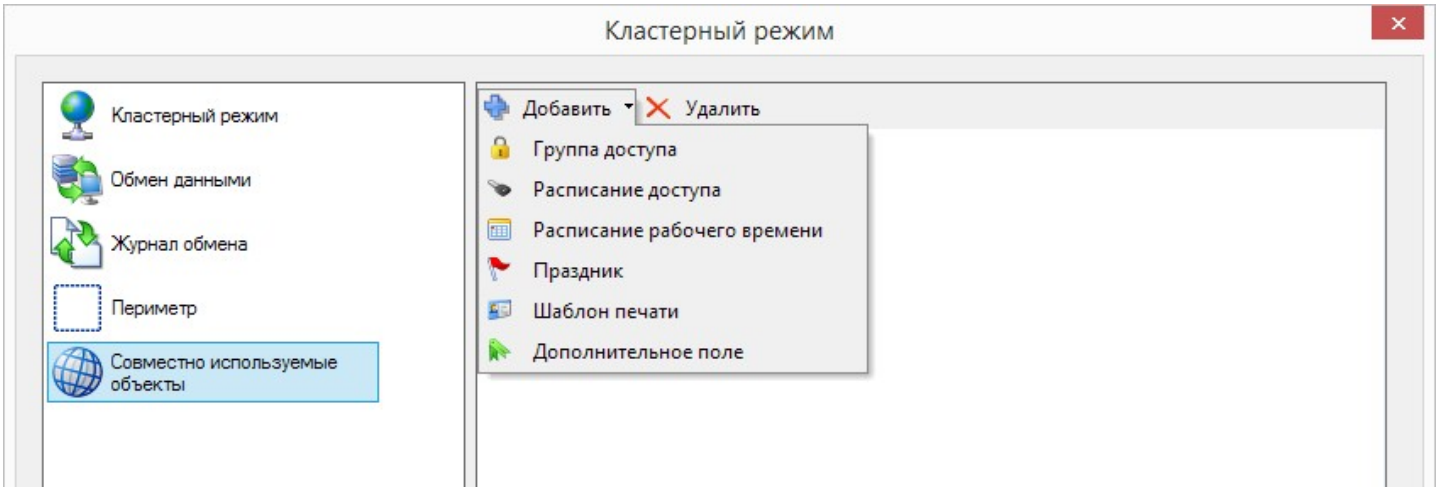
8.1.16.4 Совместное использование объектов

Для участия в обмене данными оператор сервера должен перевести те или иные объекты в категорию совместных (с общим доступом).

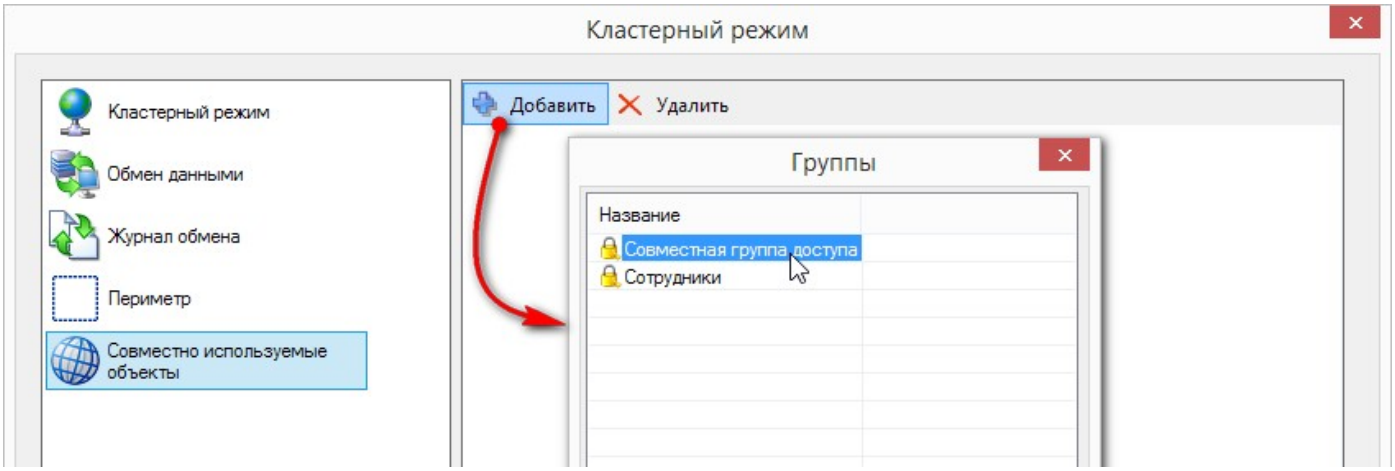
Чтобы сделать объект совместным, выполните следующие шаги:

1. В Редакторе оборудования нажмите на кнопку *Настройка кластера*. В открывшемся окне *Кластерный режим* перейдите в раздел *Совместное использование объектов;*
2. Нажмите на кнопку *Добавить*:

   Оператор **мастер-сервера** может сделать совместными следующие объекты:



   Оператор **связанного сервера** может сделать совместной только группу доступа:



3. Выберите объект для совместного использования и добавьте его в список.

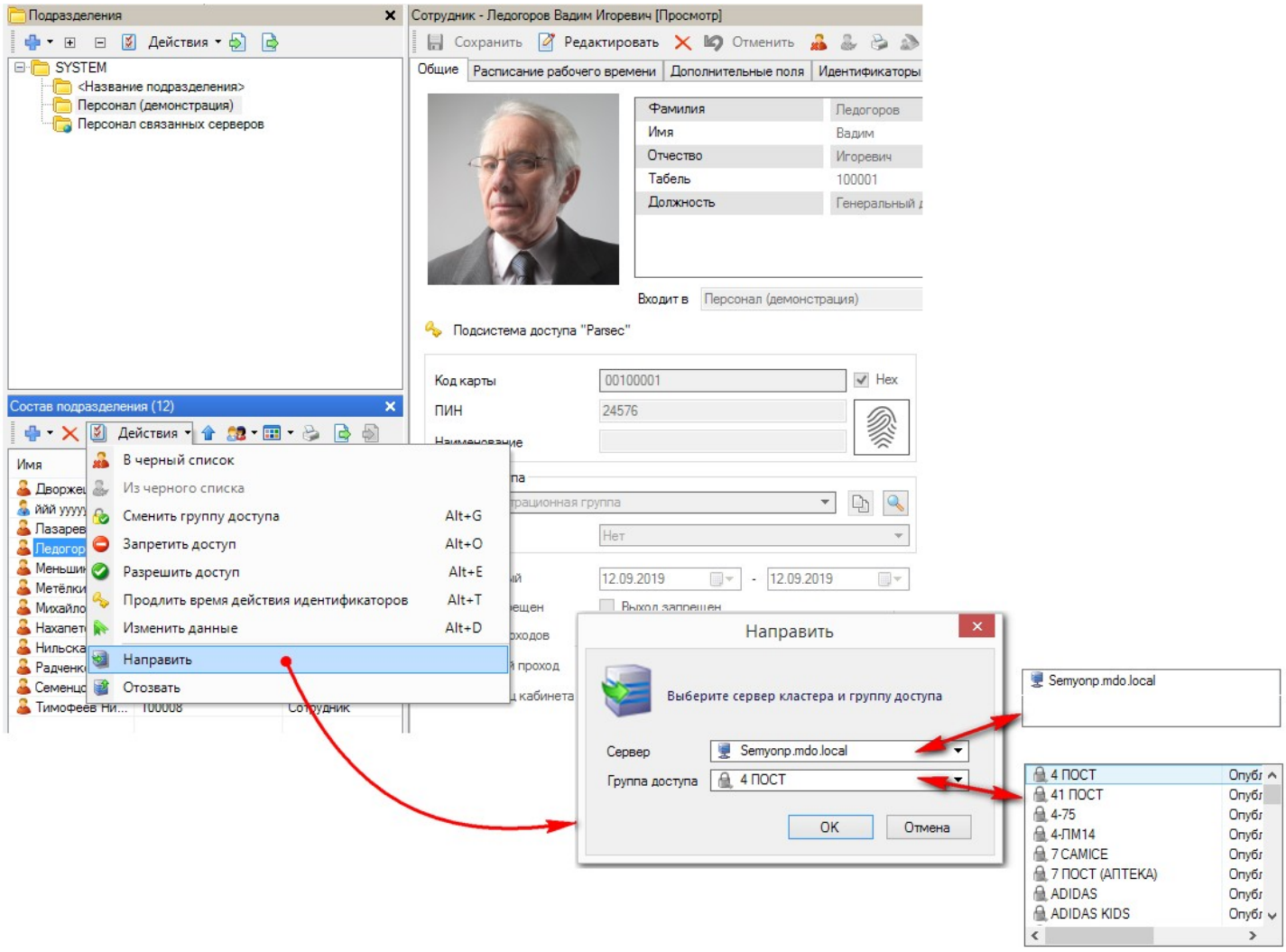
После добавления объекта он появится в соответствующих консолях всех серверов кластера.

8.1.16.5 Выдача идентификатора с совместной группой доступа

Чтобы командированные Вами сотрудники получили доступ на территорию того филиала, куда их командируют, необходимо назначить им (их идентификаторам) совместную группу доступа принимающей стороны.

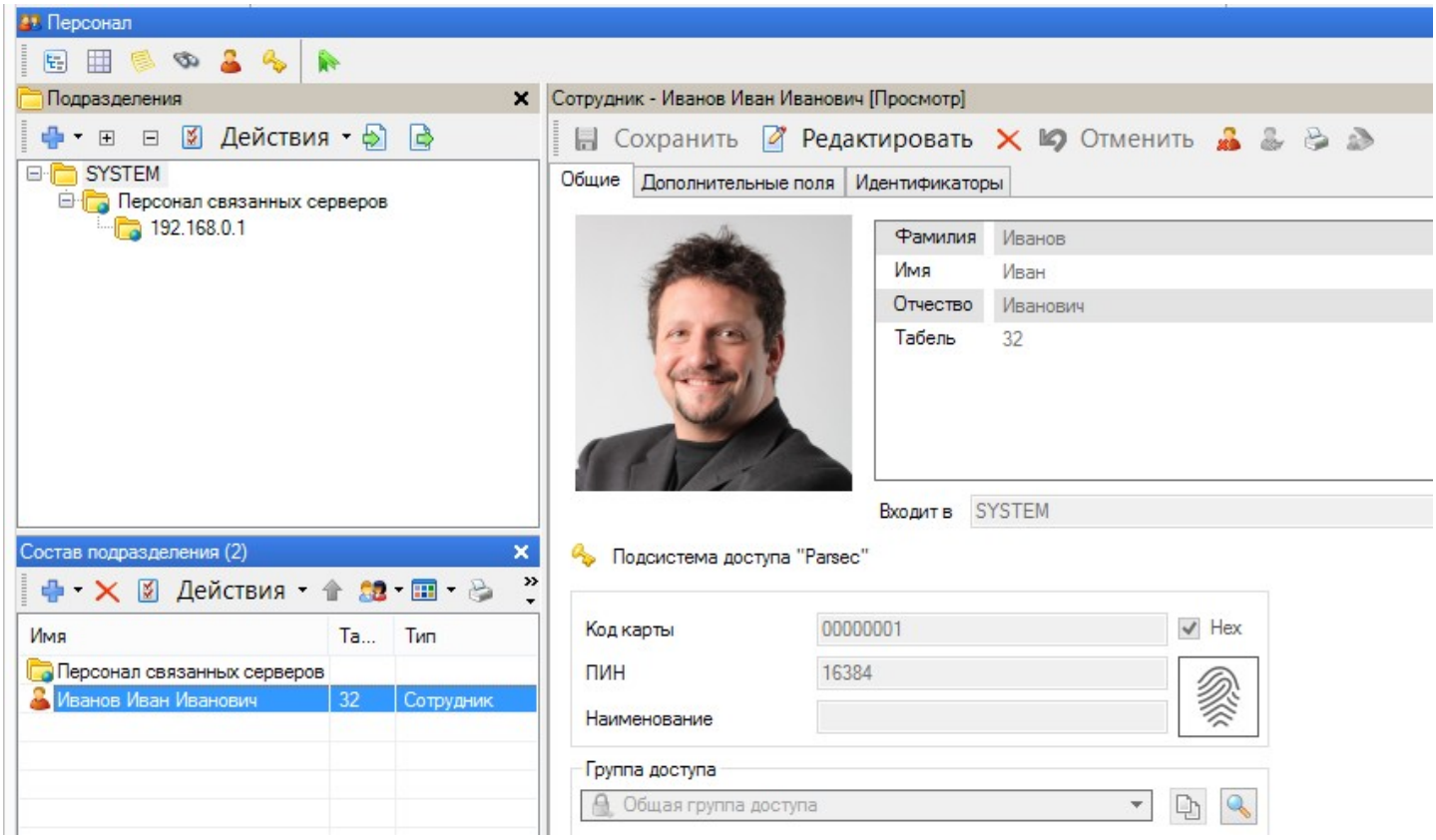
Чтобы назначить совместную группу доступа **первичному идентификатору** сотрудника, выполните следующие шаги:

1. Выделите сотрудника (несколько сотрудников), которого нужно отправить в командировку в один из филиалов, создавших совместную группу(-ы) доступа;
2. Выберите пункт "Направить" меню *Действия* панели *Состав подразделения* (также этот пункт доступен в меню *Действия* в окне поиска). Откроется окно *Направить*;
3. В поле *Сервер* выберите сервер того филиала, куда командируется сотрудник;
4. В поле *Группа доступа* выберите совместную группу доступа, созданную оператором сервера филиала;
5. Нажмите на кнопку *ОК*. Первичному идентификатору вашего сотрудника будет назначена совместная группа доступа. Посмотреть изменения можно на вкладке *Идентификаторы* редактора персонала (доступна при включении расширенного режима отображения).



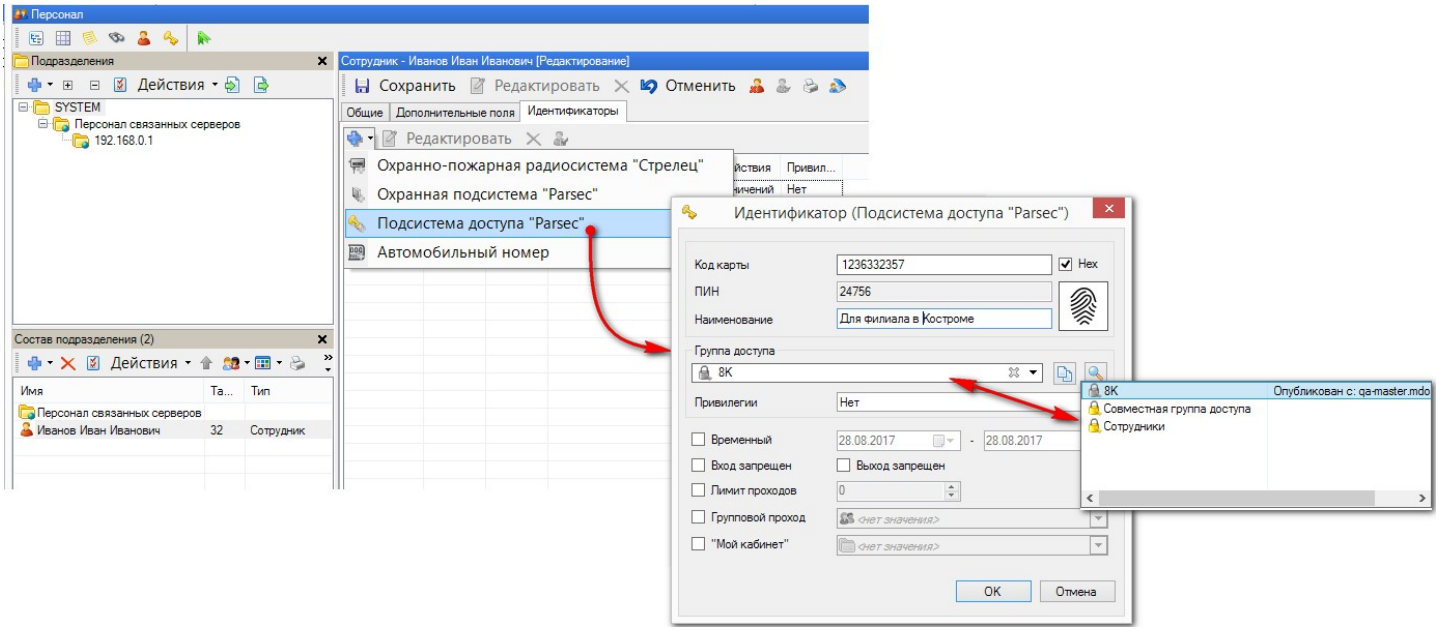
Если требуется назначить совместную группу доступа **не первичному идентификатору** сотрудника, то выполните следующие шаги:

1. Откройте Редактор персонала и выберите командируемого сотрудника:



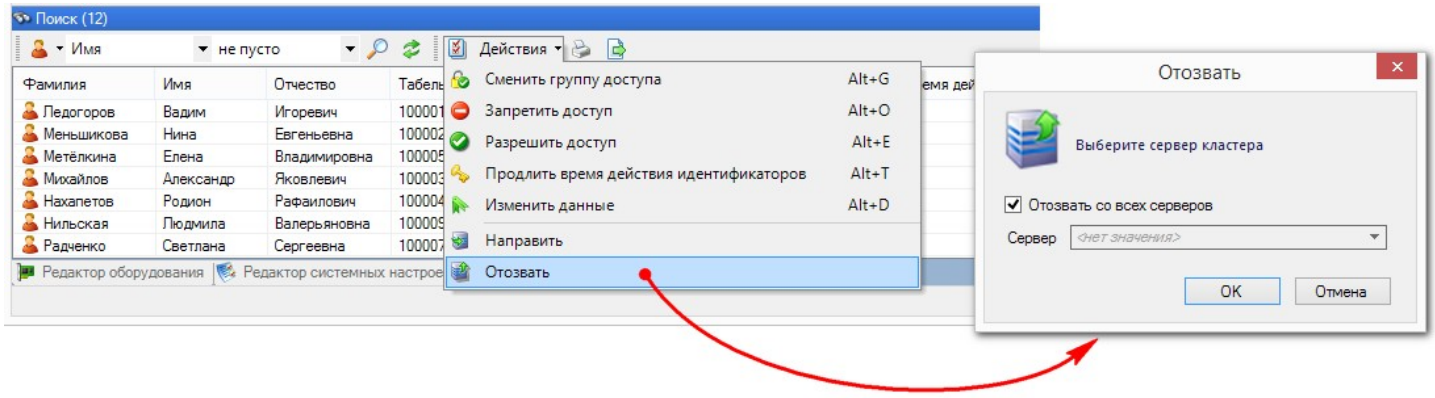
Из рисунка видно, что сотруднику Иванов И.И. назначена группа доступа - "Общая группа доступа";

2. Перейдите на вкладку *Идентификаторы* и нажмите на кнопку *Добавить*;
3. В открывшемся окне введите номер существующего идентификатора (карты) сотрудника. Также можно выдать новый идентификатор только для совместной группы доступа. Обратите внимание ,что на одном сервере идентификатору можно назначить только одну группу доступа. Другими словами, идентификатору сотрудника можно назначить одну группу доступа по месту его основной работы, и по одной группе доступа (совместной) на каждом из остальных серверов кластера;
4. В раскрывающемся списке выберите группу, которую филиал, принимающий вашего сотрудника, сделал совместной;
5. Нажмите на кнопку *ОК*:



Теперь сотрудник имеет доступ на территорию своего подразделения по общей группе доступа, а также на территорию филиала по совместной группе доступа (в нашем примере, это группа "8К").

Отозвать идентификатор сотрудника с одного или всех связанных серверов (тем самым запрещая ему проход через соответствующие точки прохода) можно, выбрав команду "Отозвать" меню *Действия* на панели инструментов. В открывшемся диалоге из раскрывающегося списка выберите конкретный сервер или оставьте установленный по-умолчанию флажок *Отозвать со всех серверов*:



8.1.16.6 Журнал обмена

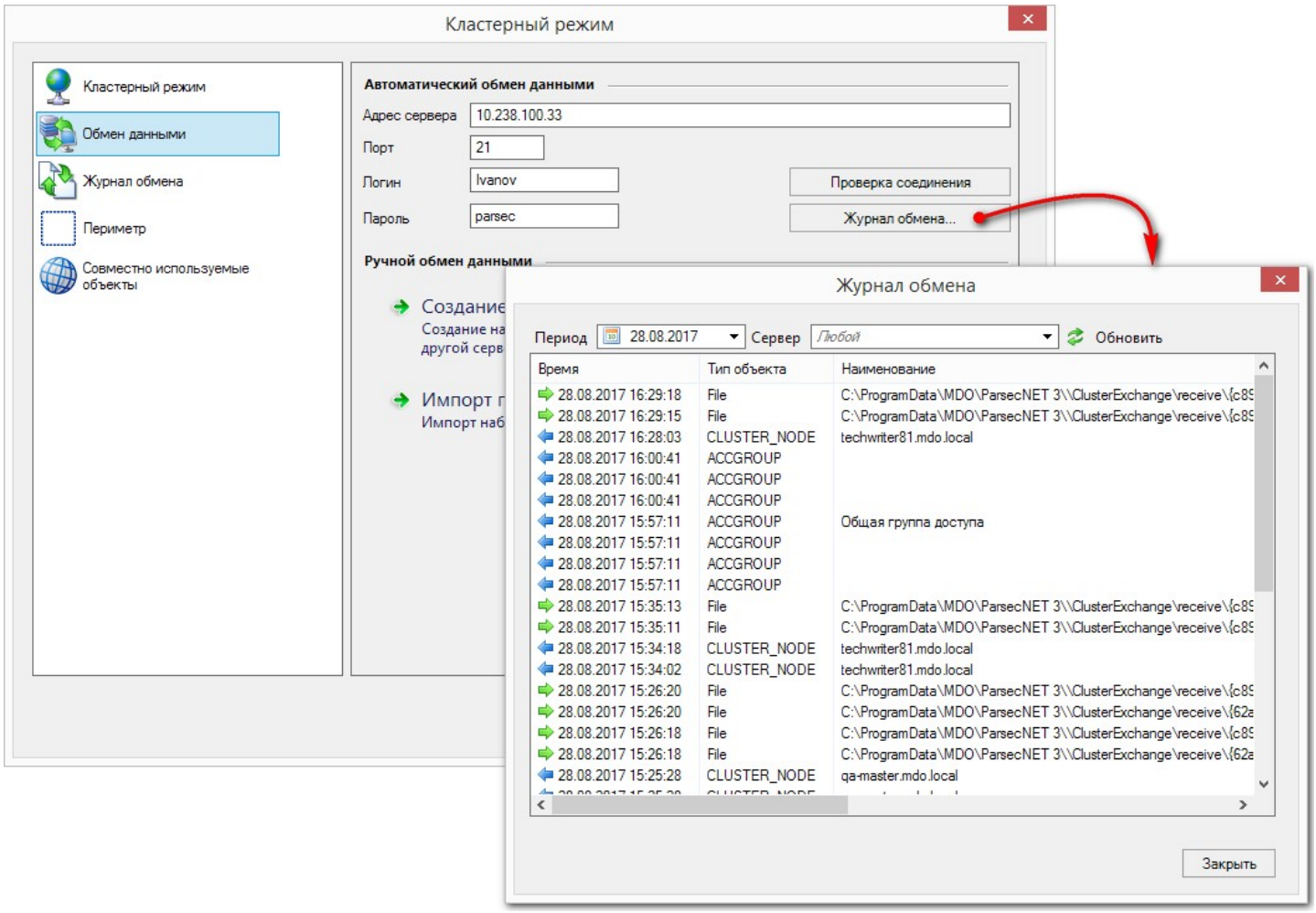
Журнал обмена предназначен для отслеживания переданных и полученных файлов связанными серверами кластера.

В системе хранится список оправленных и полученных файлов за 10 последних дней, которые можно выбрать в раскрывающемся календаре.

В раскрывающемся списке *Сервер* можно выбрать конкретный сервер для просмотра отправленных ему и полученных от него совместных данных.

Кнопка *Обновить* доступна только при выборе текущего дня.

Журнал можно просматривать как в окне, открывающимся кнопкой *Журнал обмена* в разделе *Обмен данными* окна *Кластерный режим* (см. рис. ниже), так и в отдельном разделе *Журнал обмена* этого же окна.



8.2 Программный контроллер

Программный контроллер позволяет вместе с другими средствами системы обеспечивать сложные схемы управления доступом, например, для автомобильных проходных или шлюзов. Программный контроллер представляет собой программную реализацию обыкновенного контроллера: он имеет свою базу данных субъектов доступа, как и обычный контроллер, он входит в группы доступа.

Основное отличие от аппаратно реализованных контроллеров в том, что сам он не имеет исполнительных устройств (реле), но через менеджер заданий может управлять любым другим аппаратным контроллером.

Другой важной особенностью программного контроллера является возможность работы с любыми типами идентификаторов - со стандартными картами доступа, с автомобильными номерами, и в дальнейшем - с любыми идентификаторами, поддерживаемыми системой.

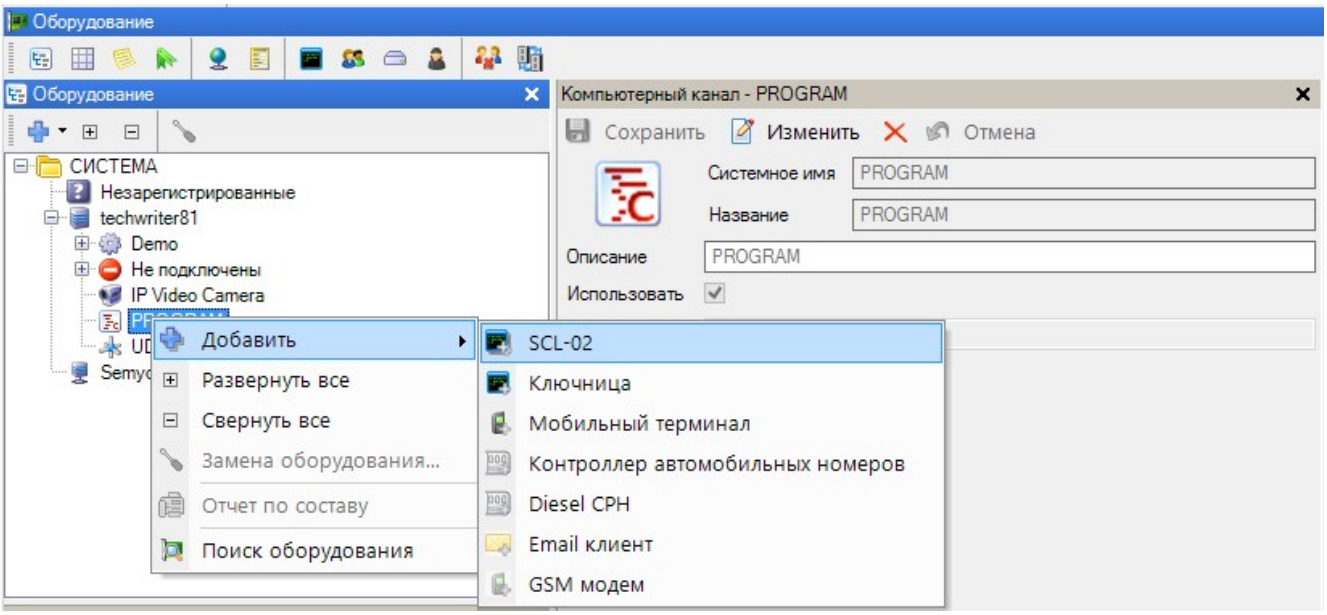
Далее в качестве примера мы покажем, как можно управлять, например, входной дверью с настольного считывателя, подключенного к ПК.

Пример программного контроллера

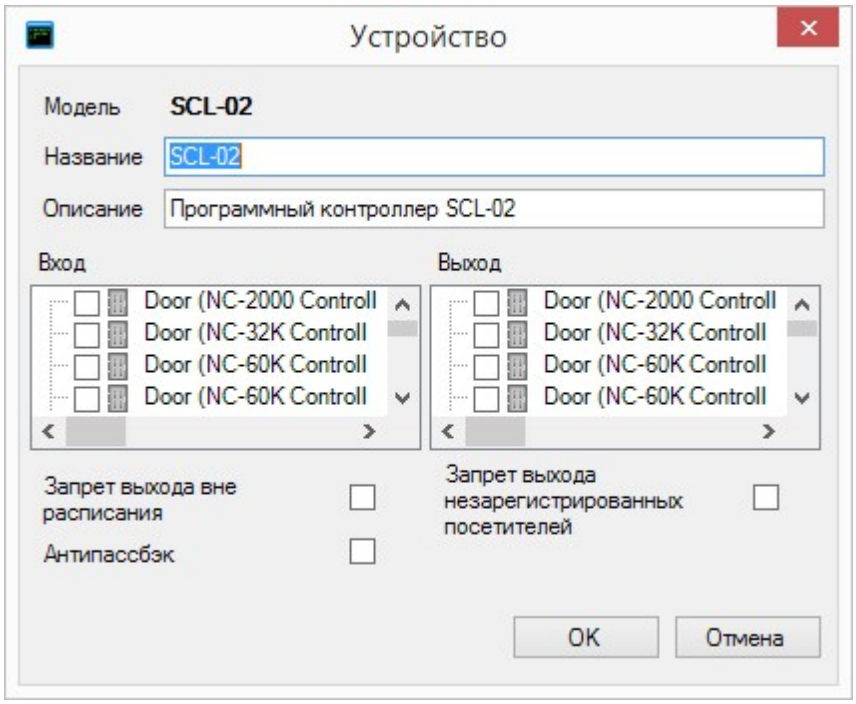
Итак, создадим программный контроллер для управления дверью с настольного считывателя.

Шаг 1. Создание контроллера

В редакторе оборудования в канале PROGRAM создайте программный контроллер:

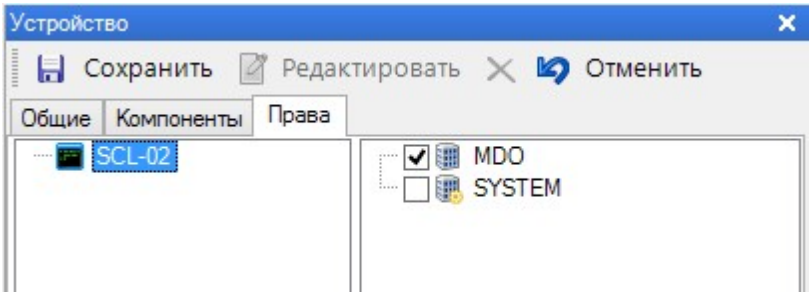


Как и обычный контроллер, программный контроллер может осуществлять идентификацию на вход и на выход. Назначьте в качестве источника идентификационных данных настольный считыватель:



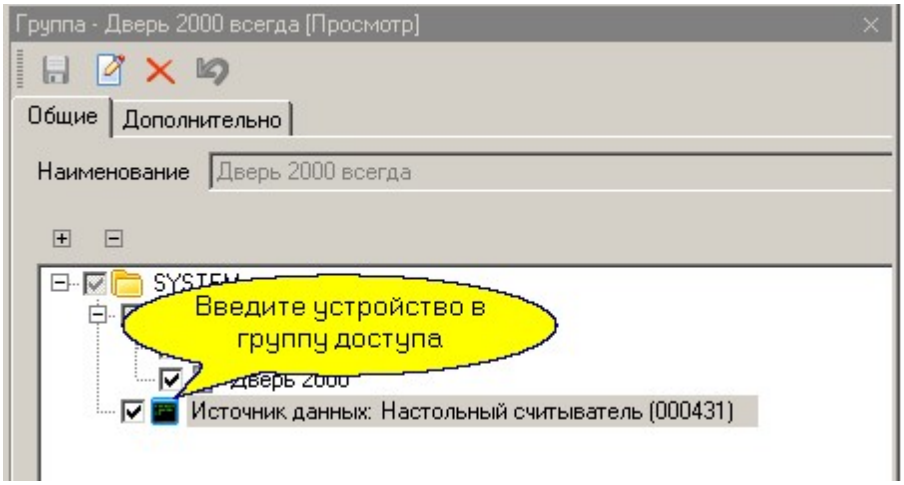
При необходимости установите нужные флажки и произведите настройку[161] группы АПБ. Описание функций "Запрет выхода вне расписания[78]" и "Запрет выхода незарегистрированных пользователей[78]" можно прочитать в разделе, посвященном настройкам контроллера NC-8K. Флажки можно поставить и позже, в карточке оборудования.

Проверьте, что контроллер будет доступен в вашей организации:



Шаг 2. Присвоение группы доступа

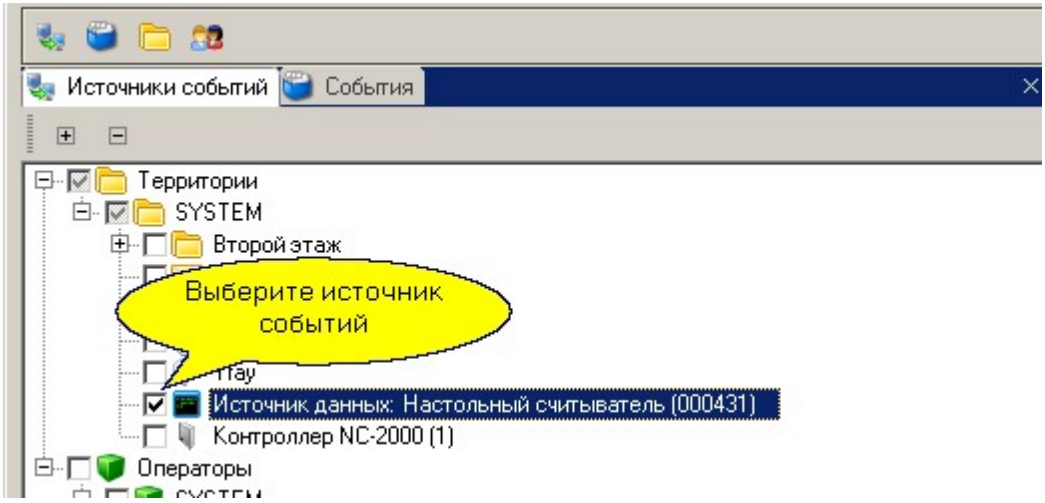
Для дальнейшей работы созданный программный контроллер (источник данных) введите в группу доступа (либо создайте для него отдельную группу доступа) как показано ниже:



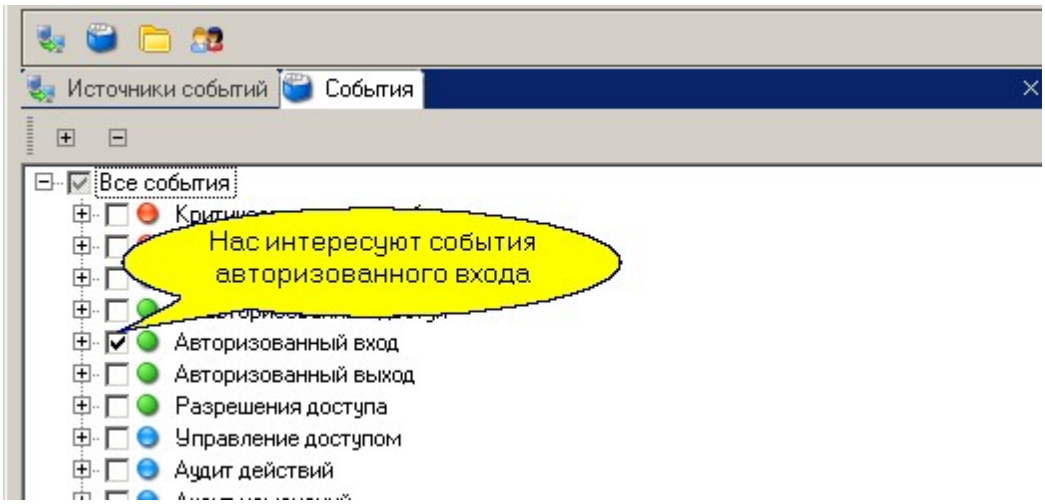
Теперь в базу данных программного контроллера попадут все субъекты, которым приписана группа доступа с программным контроллером.

Шаг 3. Назначение управляемого устройства

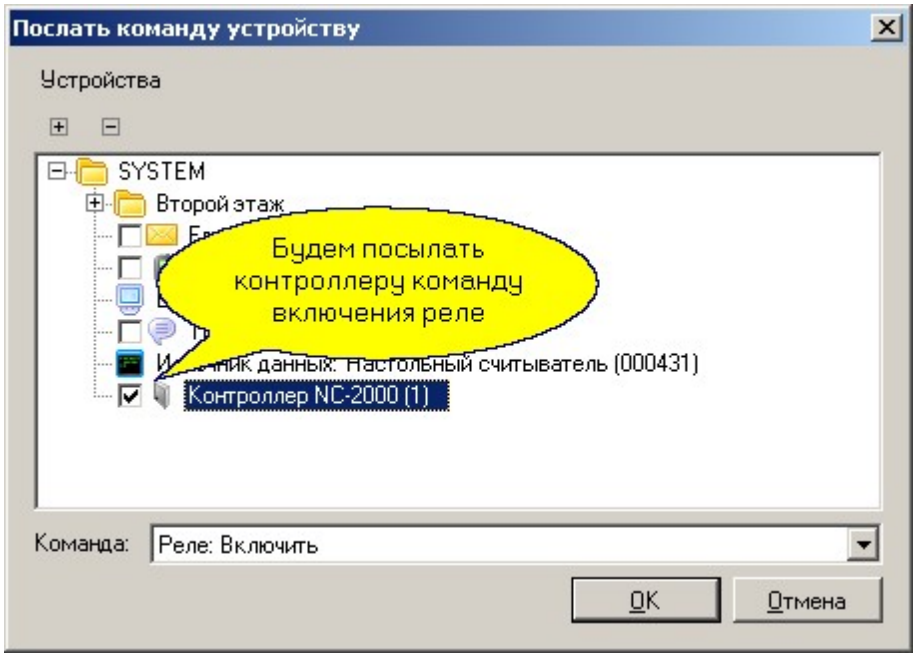
После предыдущего шага программный контроллер будет формировать транзакцию входа по карте после поднесения карты к настольному считывателю. Далее на основании этой транзакции можно с помощью менеджера заданий сформировать команду управления любому контроллеру или исполнительному устройству. Например, нужно управлять дополнительным реле контроллера NC-2000-IP. Создайте новое задание, работающее по событию от устройства, и в качестве такого устройства назначьте Ваш источник данных:



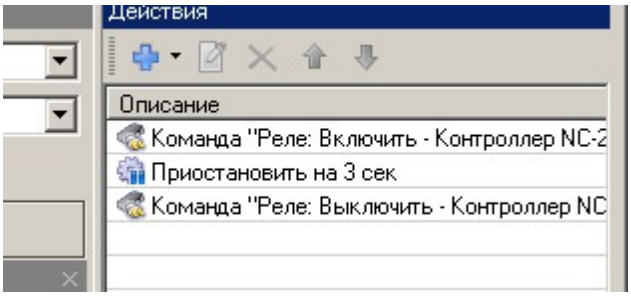
Также отметьте, на какие события будет реагировать Ваша задача:



Теперь назначьте, какая команда и кому будет посылаться при получении транзакции авторизованного входа:

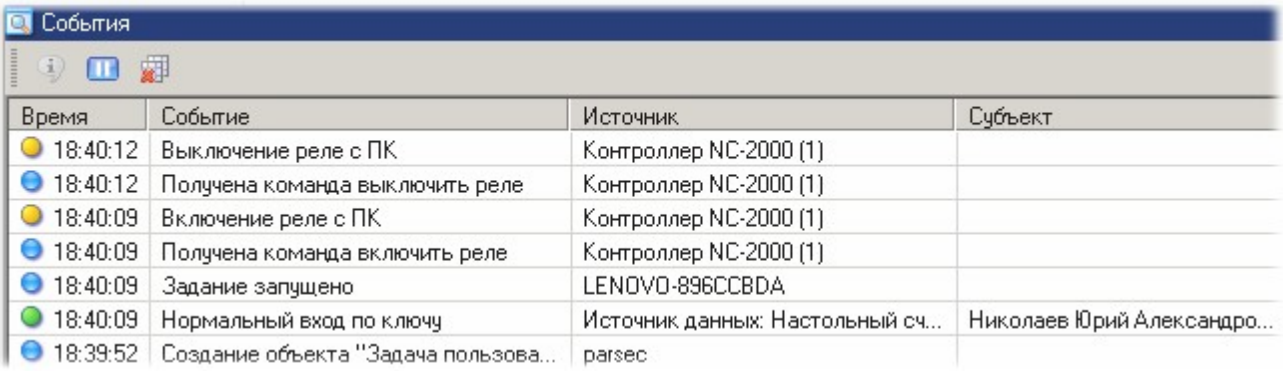


Последнее, что осталось сделать - это в задании добавить еще две задачи: задержку (время работы включенного реле) и команду выключения реле. Полный список действий нашей задачи будет теперь выглядеть так:



Шаг 4. Проверка работы

Включите монитор событий (если он не был запущен) и поднесите карту с требуемой группой доступа к настольному считывателю. В результате получим последовательность событий, показанную на рисунке ниже:



Время	Событие	Источник	Субъект
18:40:12	Выключение реле с ПК	Контроллер NC-2000 (1)	
18:40:12	Получена команда выключить реле	Контроллер NC-2000 (1)	
18:40:09	Включение реле с ПК	Контроллер NC-2000 (1)	
18:40:09	Получена команда включить реле	Контроллер NC-2000 (1)	
18:40:09	Задание запущено	LENOVO-896CCBDA	
18:40:09	Нормальный вход по ключу	Источник данных: Настольный сч...	Николаев Юрий Александро...
18:39:52	Создание объекта "Задача пользова...	parsec	

Если к дополнительному реле контроллера NC-2000-IP подключить исполнительное устройство (например, замок), то Вы сможете управлять точкой прохода с настольного считывателя.

Выше был рассмотрен конкретный пример, который показывает принцип создания заданий автоматизации с использованием программного контроллера. Вы можете реализовывать различные алгоритмы работы, используя различные источники идентификационных данных, различные наборы действий и комбинацию устройств управления.

Важно помнить, что основной смысл программного контроллера - это идентификация субъекта доступа и формирование транзакций доступа или отказа в доступе (например, по временному профилю).

См. также:

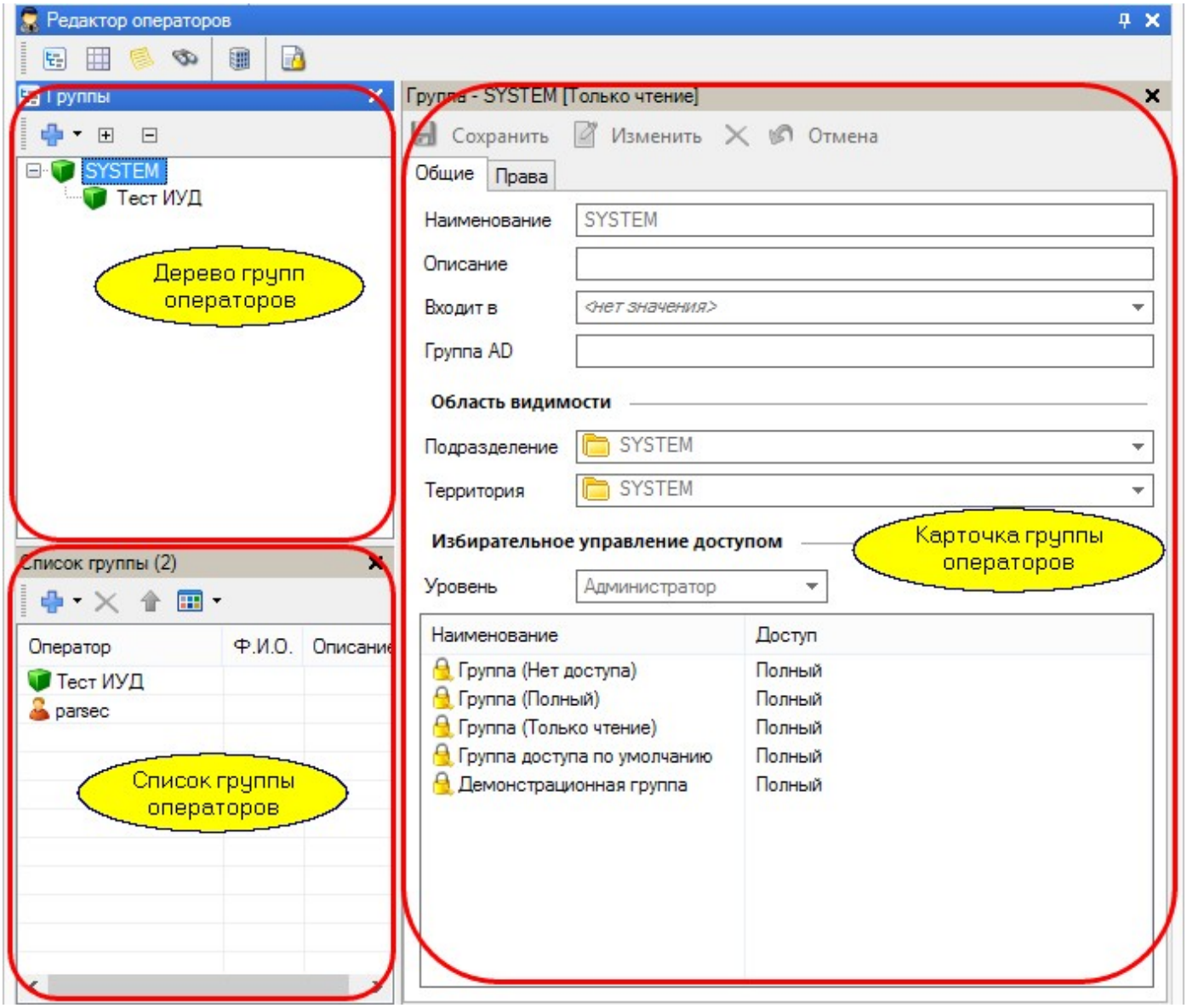
Редактор заданий[321]

8.3 Редактор операторов

Редактор операторов предназначен для создания групп операторов и создания операторов в группах. Права операторов и области видимости по территориям и персоналу задаются для группы операторов. Для конкретного оператора назначаются его имя в системе, пароль, код карты (если необходимо).

Панели редактора операторов

Редактор операторов имеет три основных рабочих панели, показанные ниже на рисунке.



Дерево групп операторов показывает структуру групп операторов текущей организации. На рисунке выше в дереве имеется корень организации SYSTEM и вложенную группу операторов: "Тест ИУД".

Список группы операторов отображает состав элемента, выбранного в дереве. В список могут входить вложенные группы и входящие в группу операторы.

Карточка группы операторов показывает свойства выбранного в списке или в дереве элемента. Для группы показываются общие свойства (на вкладке "Общие"), а на вкладке "Права" можно посмотреть и отредактировать права конкретной группы операторов. Для оператора в карточке показываются его свойства: имя (логин), пароль, полное имя и описание (как справочное поле).

Если вы только что установили систему, то в БД будет существовать единственный оператор с максимальными правами. Его имя и пароль - parsec.

Пошаговое создание группы операторов и самих операторов описано в разделе Безопасность[193]
.

См. также:

Инструкции оператору[212]

8.3.1 Безопасность

ParsecNET 3 представляет собой систему с богатым набором возможностей, при этом необходимо защититься от преднамеренных или непреднамеренных изменений параметров системы, которые могут привести к изменению работы или к частичной неработоспособности системы. Как обеспечить выполнение этого требования? - только за счет ограничения прав отдельных операторов, работающих с системой.

В простой одноорганизационной системе существуют операторы только этой системы. Если у вас профессиональная версия с поддержкой множественных организаций, то в каждой организации будут свои операторы со своими правами.



Операторы одной организации принципиально не могут иметь доступа к сущностям другой организации. Ввиду этого в каждой организации должен быть хотя бы один оператор с полными правами.

Операторы и группы

Для упрощения назначения прав при большом количестве операторов последние объединяются в группы. Именно группе назначаются конкретные права, а затем в эту группу вводятся операторы. При данном подходе легко изменить права оператора, перенеся его в другую группу, а также сменить одним щелчком права сразу всех операторов, входящих в конкретную группу. Количество операторов в системе или конкретной группе не ограничено.

Если вы только что установили систему, то в ней будет существовать единственный оператор с максимальными правами. Создание других операторов и назначение им прав ***является вашей задачей***.

Каждый оператор в организации имеет уникальное имя и может входить только в одну группу операторов данной организации. Однако любой оператор может иметь права доступа в разных организациях.

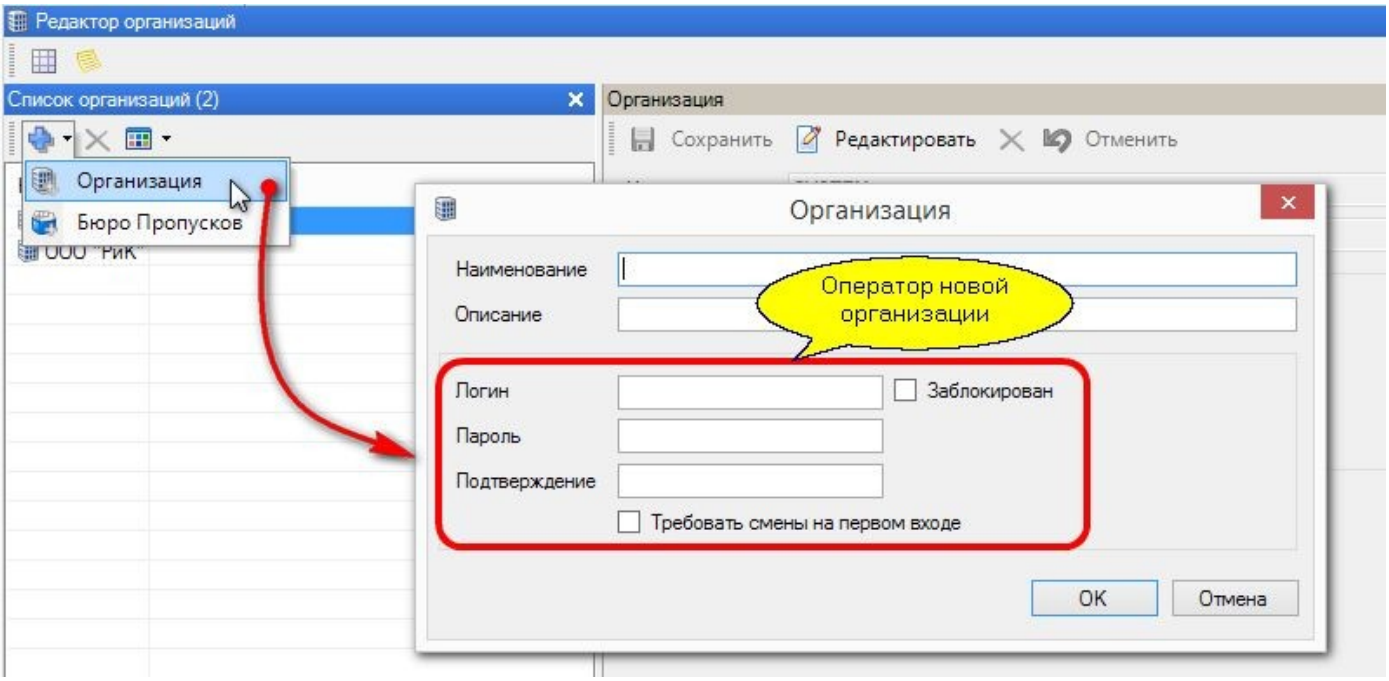
Области видимости

Группа операторов имеет ***набор прав*** (например, на использование того или иного инструмента системы), но кроме этого группе операторов можно назначить определенную ***область видимости*** объектов (территорий, подразделений). А также есть возможность определить уровень доступа операторов к группам доступа пользователей. Все это позволяет дополнительно разграничить права операторов внутри организации, если того требуют ваши задачи.

Разграничение прав между организациями

В системе в каждой организации определен свой состав операторов. Оператор одной организации не имеет доступа к данным другой организации.

Для вновь создаваемой организации при ее создании определяется ее оператор с максимальными правами. Ниже показан диалог создания новой организации, в котором создается и ее главный оператор:



Обратите внимание, что установлен флажок *Требовать смены при первом входе*, чтобы оператор новой системы поменял свой пароль при первом входе. После этого оператор организации SYSTEM, создавший оператора новой системы, теряет возможность контроля новой организации.

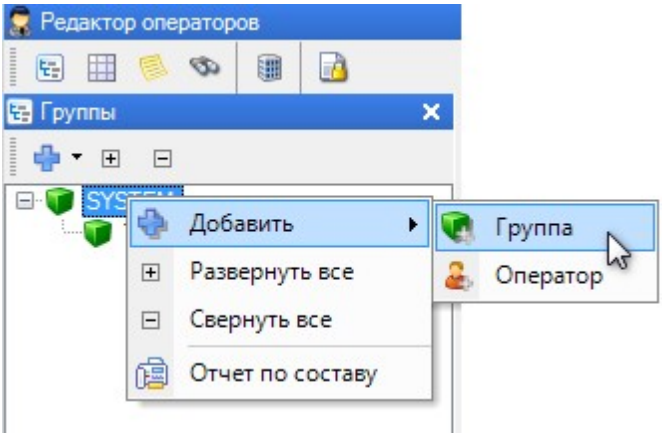
Главный оператор новой организации теперь сам создаст структуру операторов для своей организации.

8.3.2 Создание групп операторов

Ролевые права группы

Для создания и редактирования операторов и групп операторов служит "Редактор операторов", который показывает группы операторов и самих операторов только текущей организации (организации, выбранной при входе в систему).

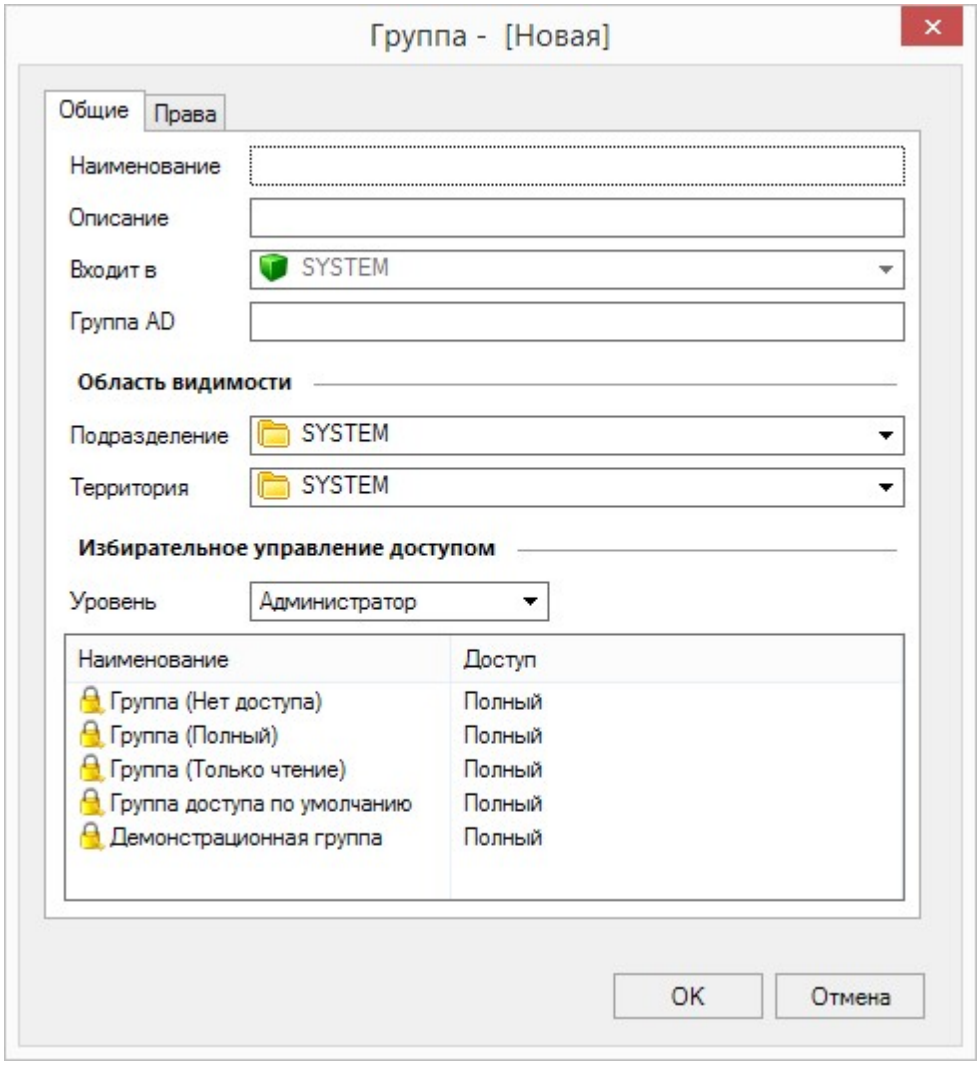
Изначально (после установки системы) существует только одна организация - SYSTEM, и один оператор, входящий в корень этой организации. Этот оператор имеет максимальные права. Чтобы создать операторов с ограниченными правами, сначала необходимо создать соответствующую группу. Для примера создадим две группы: "Пользователи" и "Только отчеты". Добавим группу:



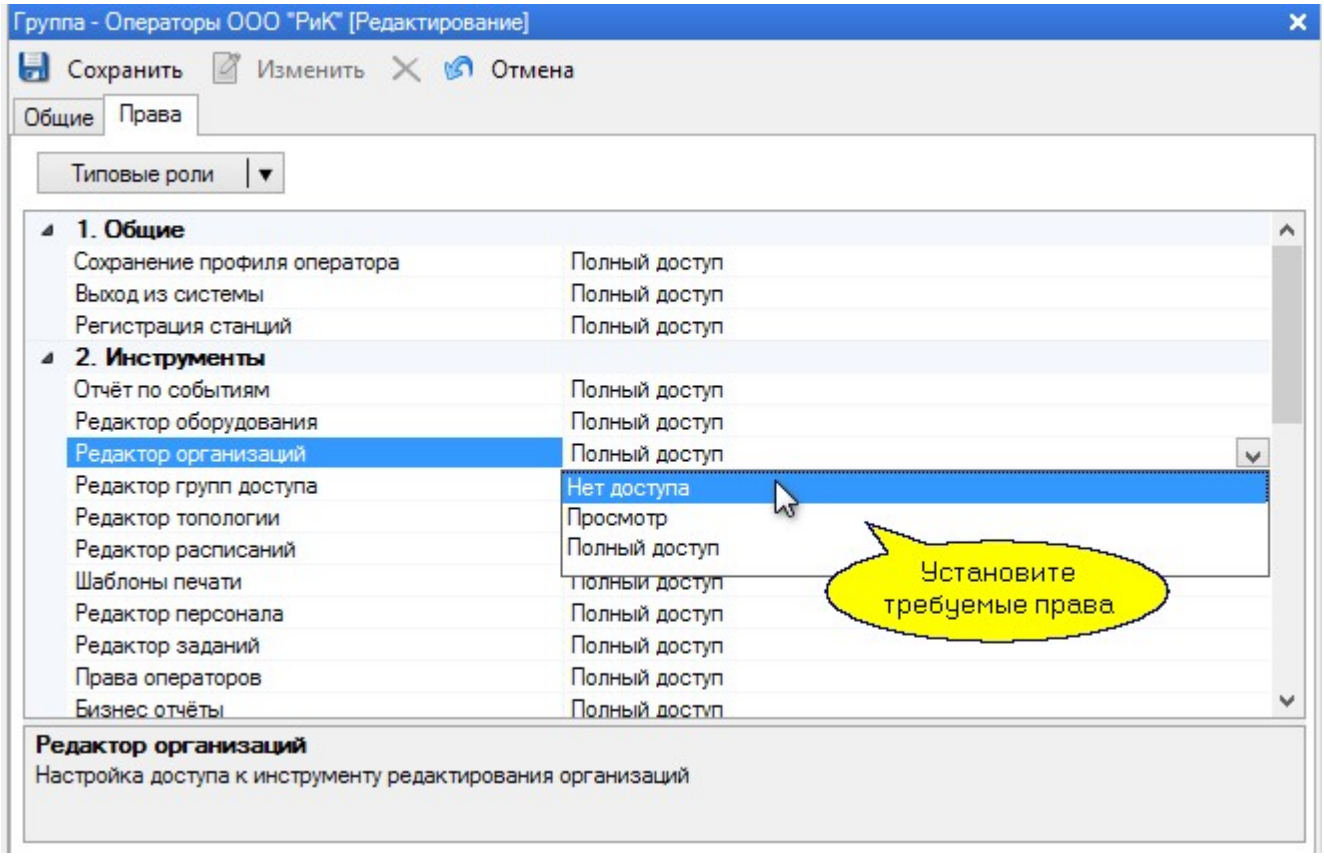
Теперь в открывшемся диалоге на вкладке "Общие" заполните поля:

- введите название и описание группы;
- при необходимости укажите группу AD (Microsoft Active Directory) (подробнее см. тут[201]);
- укажите, какие подразделения и территории[197] будут видны оператором данной группы;

- выберите уровень безопасности[197] для операторов данной группы.



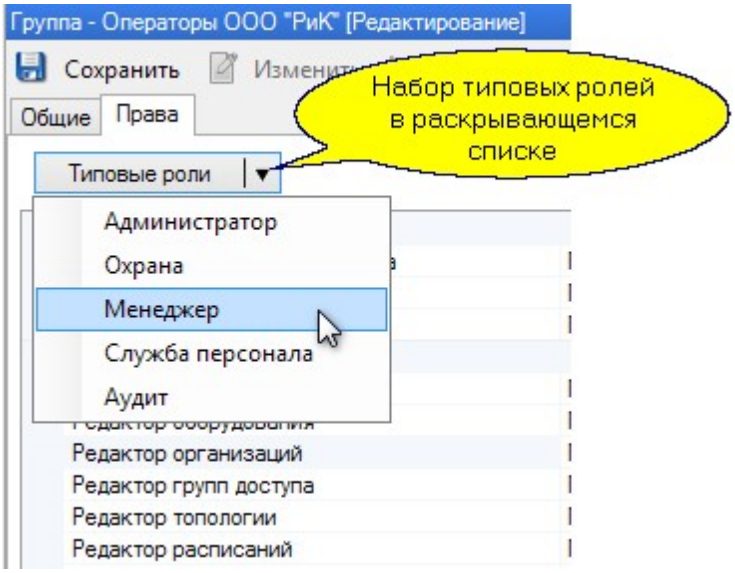
На вкладке "Права" определите набор прав этой группы:



Для большинства прав оператора существует три вида прав:

- "Полный доступ" - общие права по управлению системой;
- "Просмотр" - права просмотра оператором без управления системой;
- "Нет доступа" - данный раздел будет полностью недоступен оператору.

Для упрощения назначения прав группе можно воспользоваться типовыми ролями. Типовые роли – это готовые наборы прав для определенных типов сотрудников, например, охрана, администратор, аудит, менеджер, служба персонала. Вы можете выбрать наиболее подходящую роль, а затем при необходимости поправить отдельные права группы.

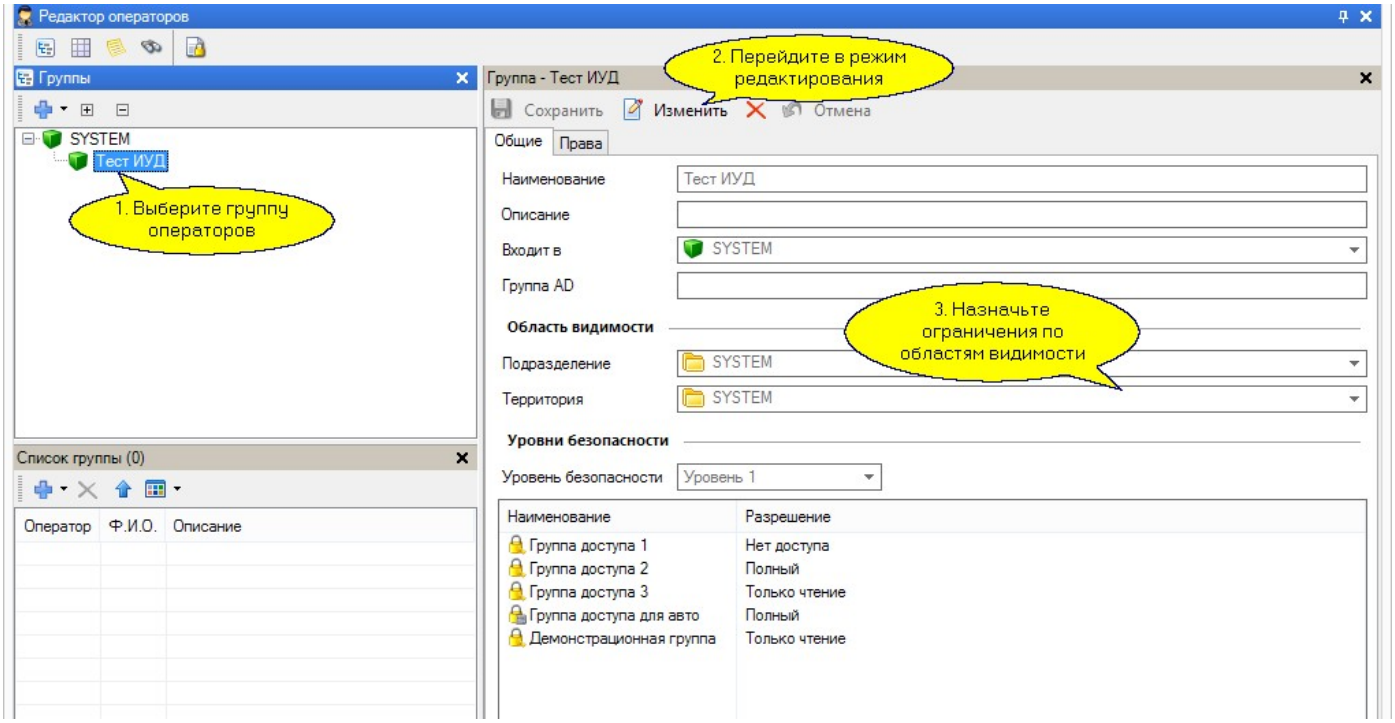


В дальнейшем вы всегда сможете с помощью редактора операторов скорректировать права группы, если это по каким - то причинам потребуется.

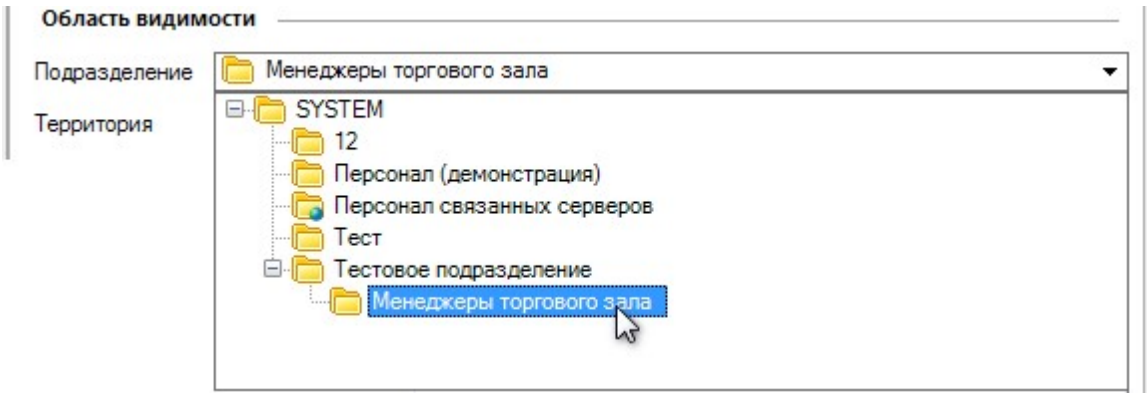
Ограничения по области видимости

Область видимости для группы задается из числа видимых элементов оператора, создающего группу. Каждая вложенная группа имеет такую же или меньшую область видимости. Набор прав может сохраняться или **уменьшаться** при вложениях. Все операторы одной группы имеют одинаковую область видимости и одинаковые права на использование инструментов системы.

Для ограничения прав группы операторов по области видимости в редакторе операторов на карточке группы на вкладке "Общие" можно задать в качестве корня по территориям и/или в качестве корня по подразделениям (персоналу) любую из папок соответствующего дерева. Для этого надо проделать следующие действия:



В открывшемся диалоге ограничим, например, данной группе видимость по персоналу только подразделением "Менеджеры торгового зала":

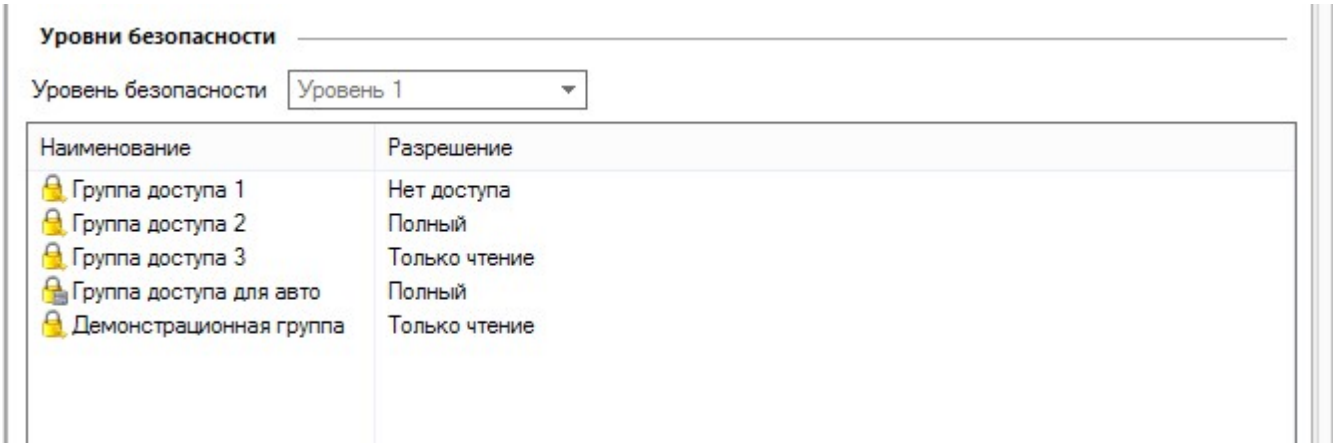


Теперь данная группа операторов будет видеть только персонал подразделения "Менеджеры торгового зала" и вложенных в него подразделений (при наличии таковых).

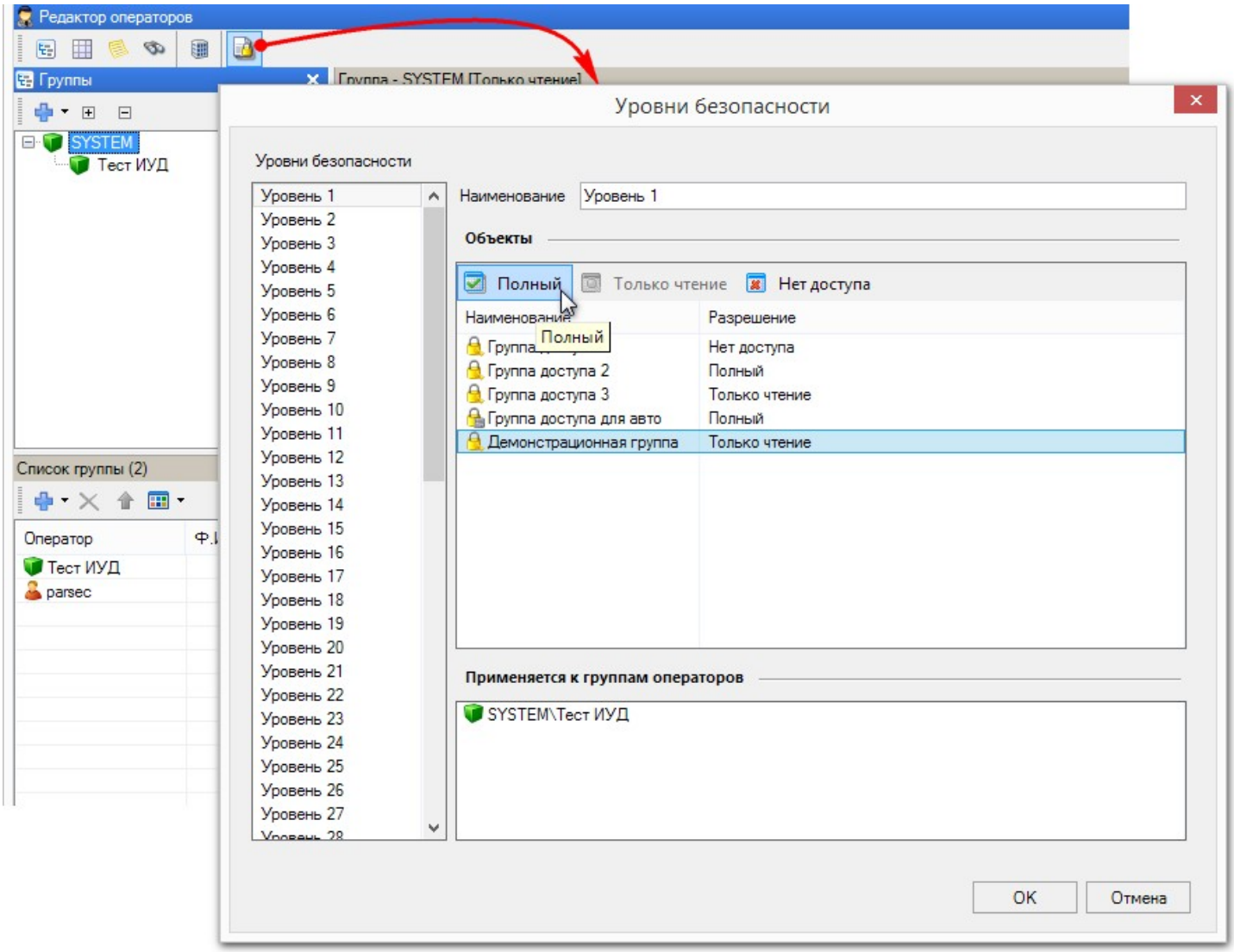
Уровень безопасности для групп операторов

Система позволяет задать для операторов подмножество групп доступа, с которыми они могут работать. Осуществляется это при помощи назначения группе операторов определенного уровня безопасности, который определяет, какие действия операторы этой группы могут совершать с группами доступа пользователей.

Уровень безопасности задает глобальный оператор организации в карточке группы операторов:



Набор действий с группами доступа для каждого уровня безопасности задается в отдельном окне, которое открывается при нажатии кнопки *Уровни безопасности* на панели инструментов Редактора операторов (рисунок ниже). Перед настройкой уровня безопасности в системе должны быть созданы группы доступа субъектов доступа (сотрудников, посетителей, автомобилей).



Слева на панели *Уровни безопасности* выберите нужный уровень (список не иерархический).

На панели *Объекты* отображаются все группы доступа.

На панели *Применяется к группам операторов* отображаются все группы операторов, которым назначен выбранный слева уровень безопасности.

Выберите на панели *Объекты* группу доступа и, нажимая на кнопки, определите уровень безопасности операторов по отношению к этой группе доступа (допуск к совершению действий с этой группой доступа):

- *Полный* - оператор сможет видеть эту группу, редактировать ее свойства, добавлять, удалять и изменять субъектов этой группы доступа;
- *Только чтение* - оператор сможет только видеть эту группу доступа и ее содержимое. Как-то изменять свойства такой группы доступа и ее содержимое оператор не сможет;
- *Нет доступа* - оператор не сможет видеть такую группу доступа и работать с ней, за одним исключением: если такая группа доступа назначена субъекту из его области видимости, то в его карточке субъекта доступа в Редакторе персонала она будет отображаться. И оператор даже сможет ее удалить. Но вернуть после этого не сможет, так как не имеет права по уровню безопасности. При этом субъекта доступа потеряет возможность прохода по правам этой группы доступа.

Пример:

1. В бизнес-центре есть группа доступа "VIP-вездеход", но руководитель СБ не хочет давать операторам бюро пропусков возможности работать с этой группой. Необходимо, чтобы они могли назначать посетителям только группу "Гости". Поэтому для операторов бюро пропусков устанавливается уровень безопасности "Нет доступа" для группы ""VIP-вездеход", а для группы доступа "Гости" - уроень безопасности "Полный".

2. У организации имеется несколько КПП и на каждом из них стоит АРМ выдачи гостевых пропусков. При помощи этого функционала можно обеспечить, что на "КПП-Северный" посетителям назначается одна из групп: Гости-Автостоянка, Гости-РиК, Гости-Общая, а на "КПП-Южный" - Гости-Склад и Гости-Общая.

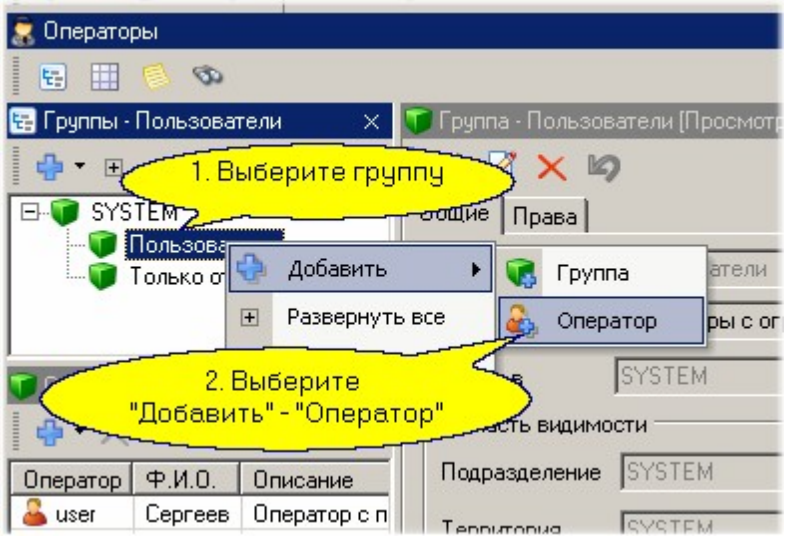
Оператор будет всегда видеть те группы доступа, которые ему доступны по уровню безопасности.

Кроме того, уровень безопасности сочетается с правом "Редактор групп доступа" (на вкладке *Права*) особым образом:

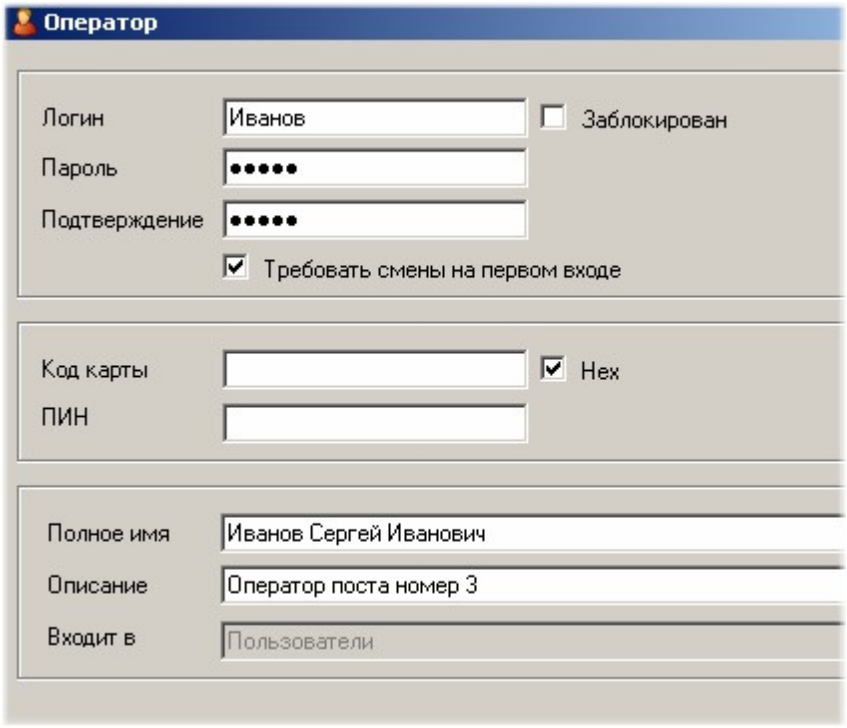
Если право "Редактор групп доступа" находится в состоянии "Нет доступа" (т.е. создавать новые группы доступа, редактировать их оператор не может), то в этом случае он все-равно может назначать пользователям любую из доступных ему по уровню безопасности групп доступа. Иными словами, оператор не может работать с Редактором групп доступа, но может назначать уже созданные группы доступа субъектам доступа из своей области видимости в Редакторе персонала.

8.3.3 Создание операторов

Когда соответствующие группы операторов созданы, ввод в группу нового оператора становится тривиальной задачей. Для этого на требуемой группе выберите "Добавить" - "Оператор":



... и в открывшемся диалоге задайте параметры оператора:



Ниже в таблице дана расшифровка всех полей показанного выше диалога:

Параметр	***Назначение***
Логин	Имя, под которым оператор будет входит в систему
Пароль	Пароль для входа в систему
Подтверждение	Повторно введенный пароль (для проверки на правильность ввода)
Требовать смены при первом входе	При установке этого флажка при первом входе в систему оператору будет предложено сменить первоначально заданный пароль
Код карты	Код карты. Позволяет входить в систему не только путем ввода имени и пароля, а также и поднесением карты к настольному считывателю

ПИН	Персональный Идентификационный Номер - используется на устройствах с клавиатурой
Hex	При установленном флажке код карты отображается в 16-ричном формате
Полное имя	Справочная информация: как правило, ФИО оператора
Описание	Справочное поле

После нажатия на кнопку *ОК* новый оператор будет введен в систему и сможет работать в ней в соответствии со своими правами.

8.3.4 Дополнительные возможности

Вход в систему по карте

Обычно вход в систему производится путем ввода имени оператора и пароля с клавиатуры. Однако имеется более простой и удобный способ входа в систему - по карте оператора. Для этого необходимо два условия:

1. К рабочей станции, на которой происходит вход в систему, должен быть установлен и зарегистрирован в системе настольный считыватель;
2. Оператору при его создании или редактировании должна быть назначена карта, по которой он будет осуществлять вход в систему.

Блокировка оператора

Если оператор **пять** раз подряд неправильно ввел свой пароль при входе в систему, то он автоматически получает статус заблокированного на 30 минут, после чего опять получает возможность входа в систему.

Иногда по разным причинам бывает просто необходимо на некоторое время лишить конкретного оператора прав пользования системой. В этом случае блокировка может быть осуществлена вручную (другим оператором с соответствующими правами). Для этого достаточно в редакторе операторов установить флажок *Заблокирован*, которая будет действовать до снятия ее вручную.

Смена пароля

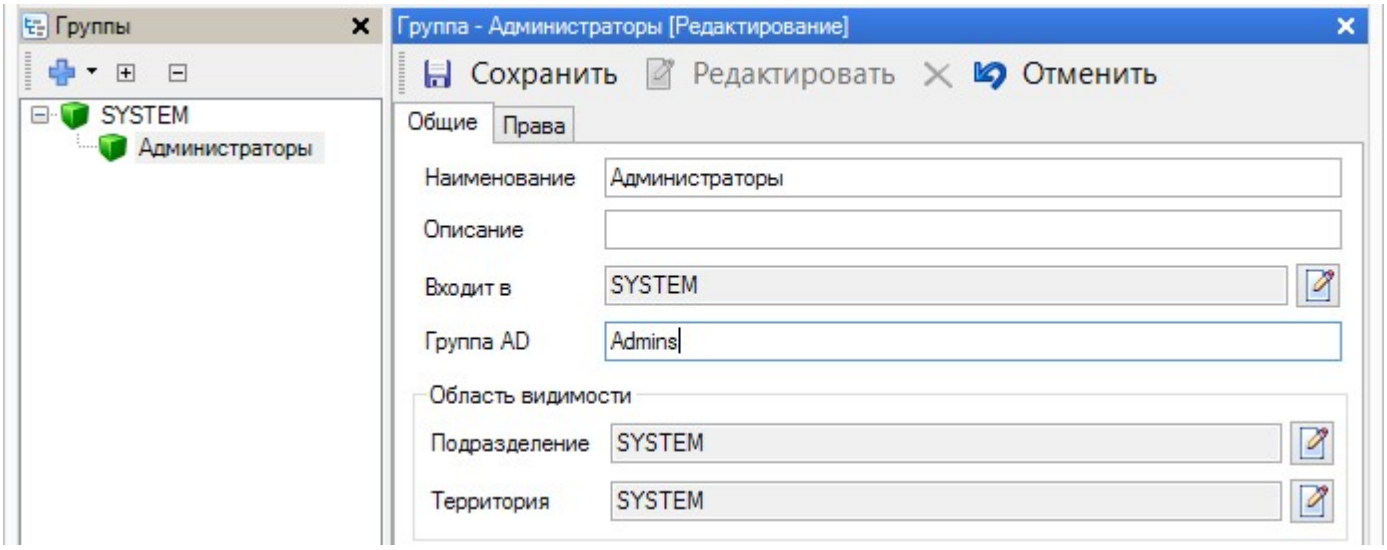
В целях повышения уровня безопасности система требует смены пароля оператора по истечении каждых 90 дней.

Вход в систему под учетной записью Windows

Система позволяет осуществлять вход пользователей с учетными данными своих аккаунтов в домене организации.

Для этого предварительно необходимо осуществить следующие настройки:

- создать группу операторов;
- связать ее с группой AD (Microsoft Active Directory). При необходимости обратитесь к своему системному администратору, он сообщит Вам, какие группы существуют в вашем домене. Наименование группы вносится в поле *Группа AD* на вкладке *Общие* свойств группы операторов. В примере ниже группа операторов связана с группой Admins в домене:

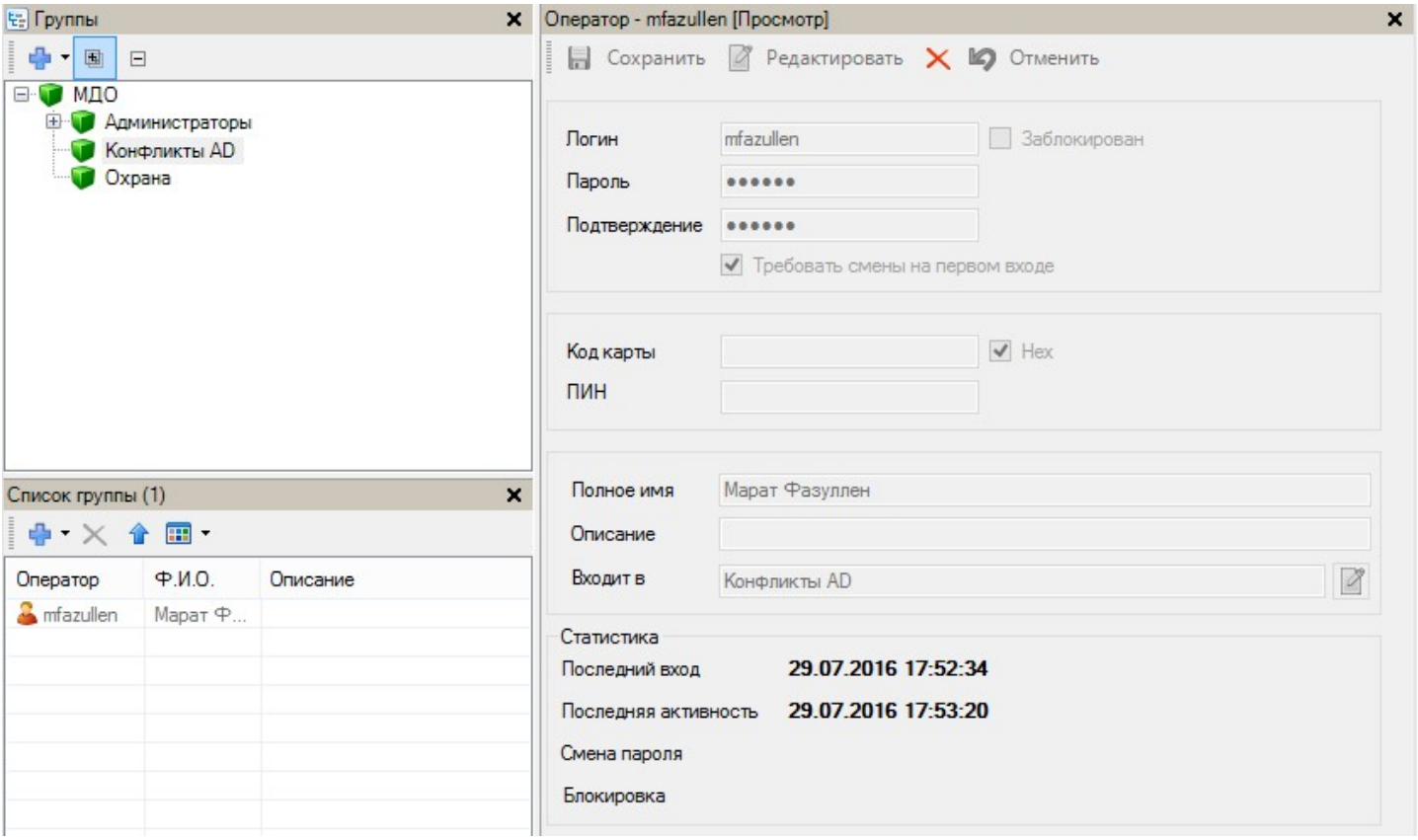


После этого все пользователи, входящие в привязанную группу AD, смогут входить в ParsecNET 3 под своими логином и паролем Windows. При этом система автоматически создаст для каждого из них оператора в той группе операторов, с которой связана их группа AD (в примере это группа операторов "Администраторы").

Конфликт групп AD и групп операторов

Пользователь Windows может входить в несколько групп AD в своем домене. Некоторые из этих его групп могут быть привязаны к разным группам операторов с системе ParsecNET 3. Если такой пользователь попытается войти в ParsecNET 3, то система не сможет определить, в какой группе операторов создавать нового оператора (оператор может входить только в одну группу операторов). Этому пользователю будет отказано во входе, а его учетная запись в системе ParsecNET 3 будет помещена в группу "Конфликты AD" (при этом она будет недоступна для редактирования, см. рис. ниже).

Администратор системы должен будет вручную перенести оператора из группы "Конфликты AD" в правильную группу операторов. Только после этого данный пользователь сможет воспользоваться входом в систему ParsecNET 3 под своими логином и паролем Windows.



8.4 Редактор топологии

Топология представляет собой иерархическую структуру (дерево) территорий, обслуживаемых системой ParsecNET 3 или ее частью (при наличии множественных организаций). Структура территорий создается в редакторе топологии системы.

В топологию могут входить как реальные элементы системы (двери, охранные области, турникеты, контроллеры), так и группирующие элементы, которые могут представлять организацию, здания, строения, этажи, комнаты.

Особенностью этого дерева является то, что одни и те же компоненты могут входить в разные ветки. Разграничение доступа для него задается на уровне узлов, которые могут присваиваться в качестве корневых для разных групп операторов. У одной группы может быть только один узел в качестве корня.

Назначение

Редактор топологии предназначен для создания структуры территорий вашей организации. В маленьких системах (на несколько дверей) структуру территорий можно и не создавать. Однако на больших объектах это делать целесообразно, поскольку:

- Упрощается поиск необходимых компонентов системы;
- Появляется возможность разграничить области видимости территорий для отдельных операторов.

Как правило, структура территорий привязывается к физической топологии объекта. Например, для здания можно в качестве единиц топологии назначать отдельные этажи здания. Для этажа с большим количеством подразделений структура территорий может отображать распределение территории между подразделениями.

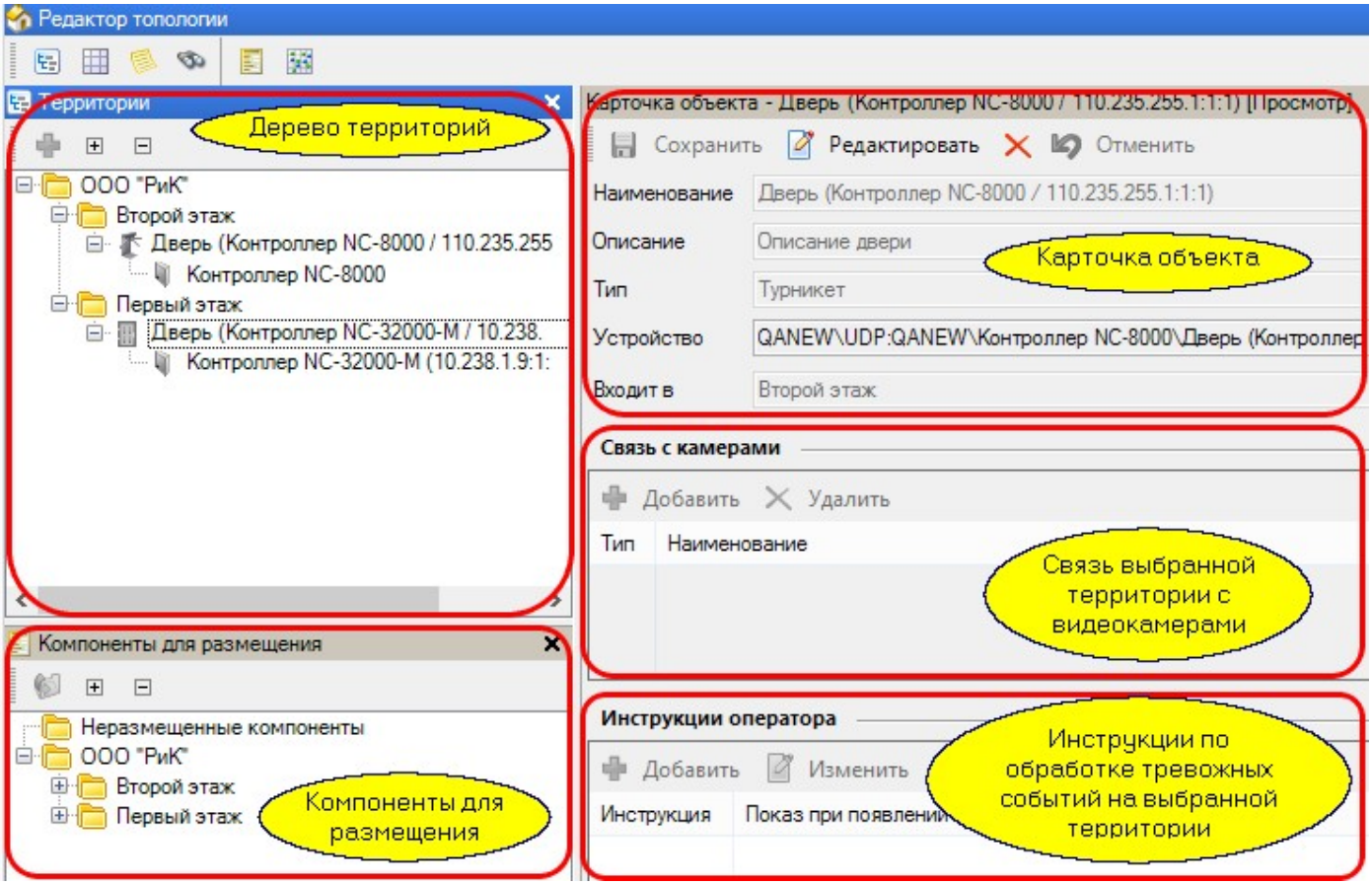
Структура территорий может иметь неограниченную вложенность уровней, причем каждый уровень может содержать как компоненты оборудования (двери, охранные области), так и другие группирующие элементы для внутреннего уровня вложенности.

Помимо создания структуры территорий, редактор топологии предоставляет возможность для каждой территории создать собственный графический план[208], который будет затем использоваться в окне монитора событий для визуального представления ситуации на конкретной территории.

Дополнительно в редакторе топологии для каждого компонента территории на определенную группу событий можно создать инструкции оператору[212] для помощи ему в принятии решений в конкретной ситуации.

Панели редактора топологии

Редактор топологии имеет следующие основные панели:



Дерево территорий показывает текущую топологию вашей организации. Топология других организаций не отображается. Добавленное для организации SYSTEM оборудование сразу попадает на панель дерева территорий.

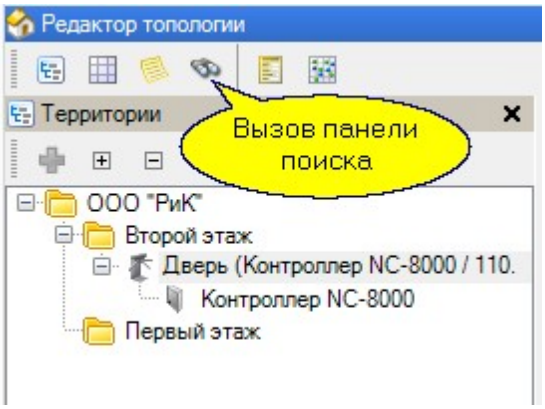
Компоненты для размещения. Данная панель отчасти дублирует панель дерева территорий, но в ней еще всегда имеется папка не размещенных компонентов. У иной, нежели SYSTEM, организации, в этой папке отображаются то добавленное оборудование, на просмотр которого у операторов этой организации есть права[71]. Оборудование, удаляемое из дерева территорий и организации SYSTEM, и других, также отображается в папке *Неразмещенные компоненты*. Помещенное в данную папку оборудование исключается из работы системы. Но его вновь можно разместить в своем дереве территорий.

Карточка объекта показывает свойства объекта, выбранного в дереве территорий или в компонентах для размещения. Карточка позволяет редактировать свойство выбранного объекта, а также "оснащать" его с видеокамерами и задавать инструкции оператору.

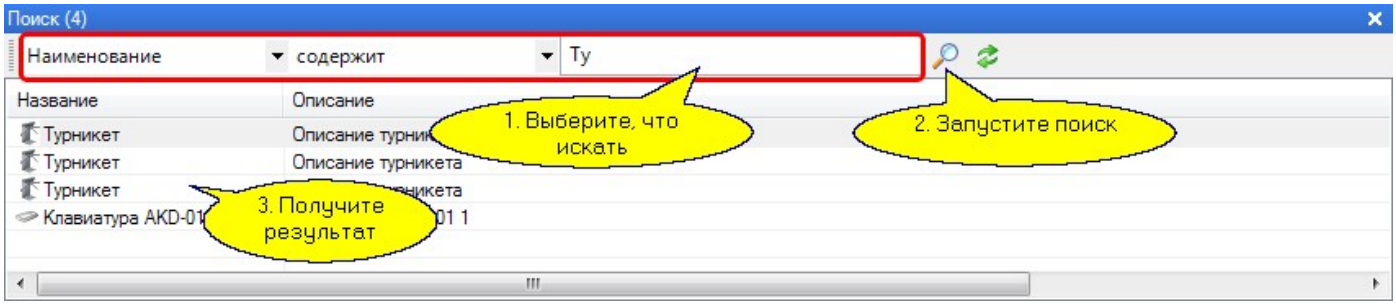
***Связь с камерами*.** На панели отображаются выбранные для данной территории видеокамеры. Панель доступна только для размещенной территории.

***Инструкции оператору*.** На этой панели выбираются тревожные события и пишутся инструкции, которые оператор должен выполнить при возникновении выбранных событий. Панель своя для каждой территории и настраивается отдельно. Панель доступна только для размещенной территории.

Редактор дополнительно имеет панель поиска, которая по-умолчанию скрыта, но открывается с панели инструментов редактора:



С помощью панели поиска можно найти элементы топологии (территории, оборудование и его компоненты). Для примера показан результат поиска турникета в нашей топологии:



Работа с редактором топологии рассмотрена в разделе Создание территорий[205] .

См. также:

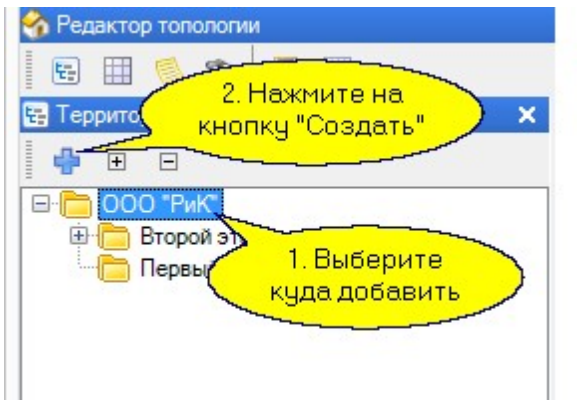
Создание графпланов[208]

Связь с камерами[211]

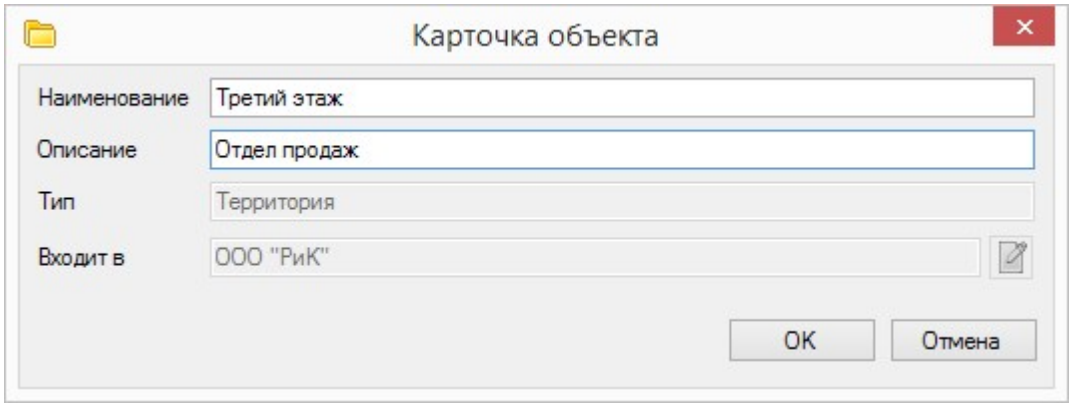
Инструкции оператору[212]

8.4.1 Создание территорий

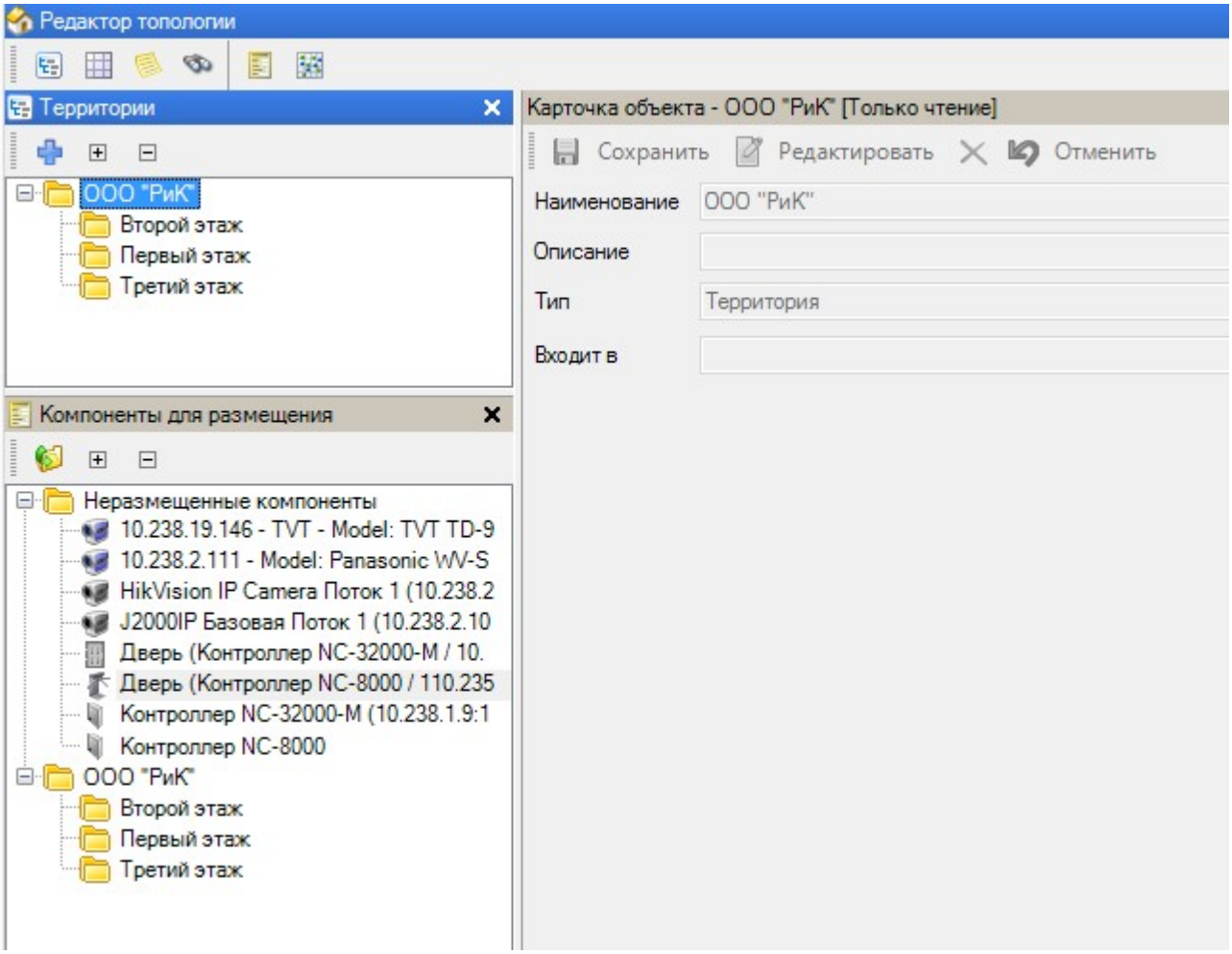
Для создания новой территории в Редакторе топологии выделите объект, под которым будет создана новая территория, и выберите команду "Создать" в контекстном меню или нажмите на кнопку "Создать":



В карточке новой территории введите ее название, и если необходимо - справочное описание:



После создания нескольких новых территорий получим следующую структуру:



Теперь логично разместить оборудование по принадлежности к этажам.

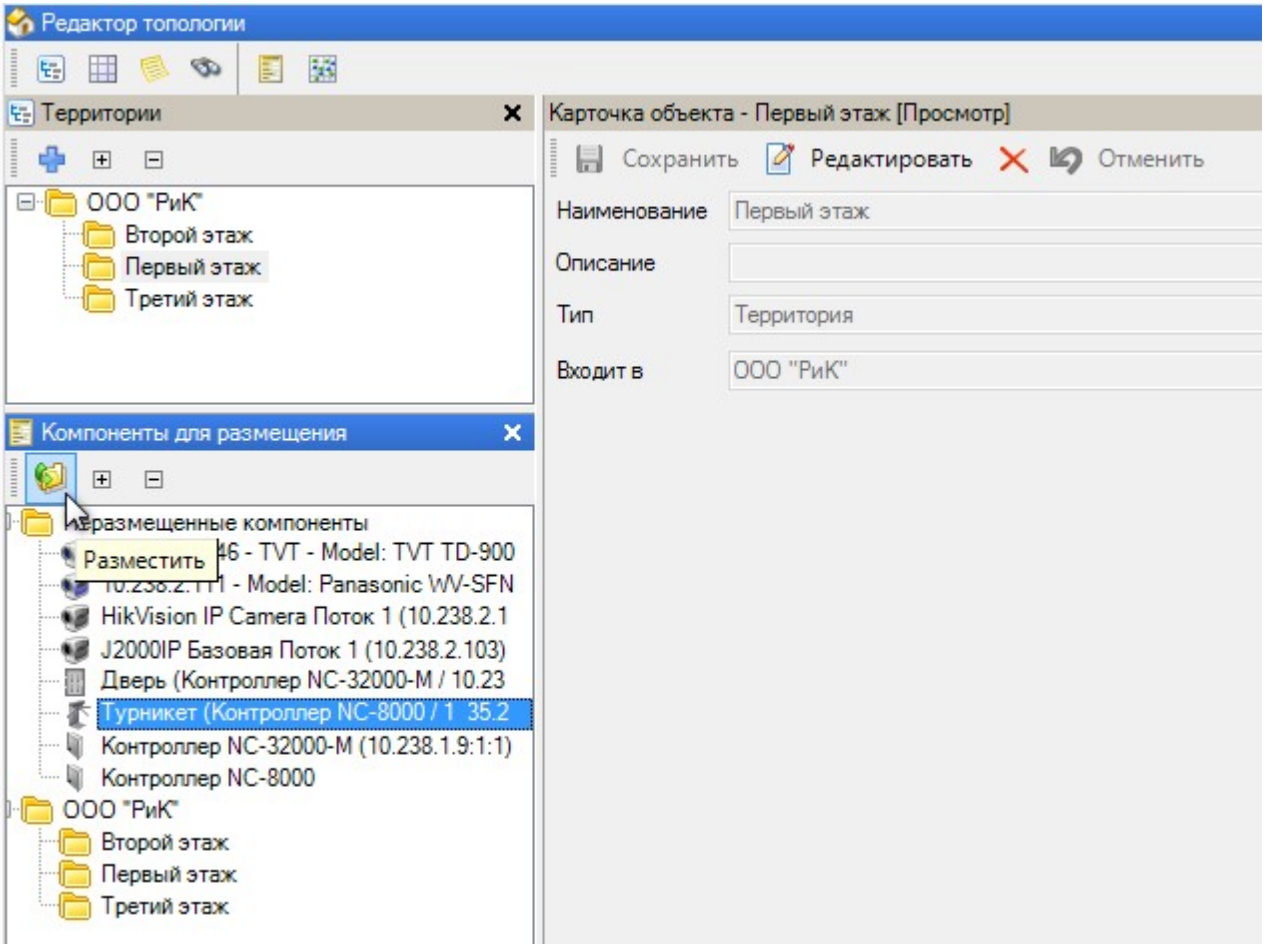
Территории, которые используются в группах доступа, удалить нельзя. Система выдаст предупреждающее сообщение.

Размещение оборудования

Оборудование можно перемещать между элементами топологии как перетаскивая мышкой из панели *Компоненты для размещения* в конкретный узел панели *Территории*, так и выполнив следующие действия:

1. Выделите на вкладке *Территории* требуемый объект;
2. Выберите в папке *Неразмещенные компоненты* элемент оборудования;
3. Нажмите на кнопку *Разместить* на панели инструментов вкладки *Оборудование*.

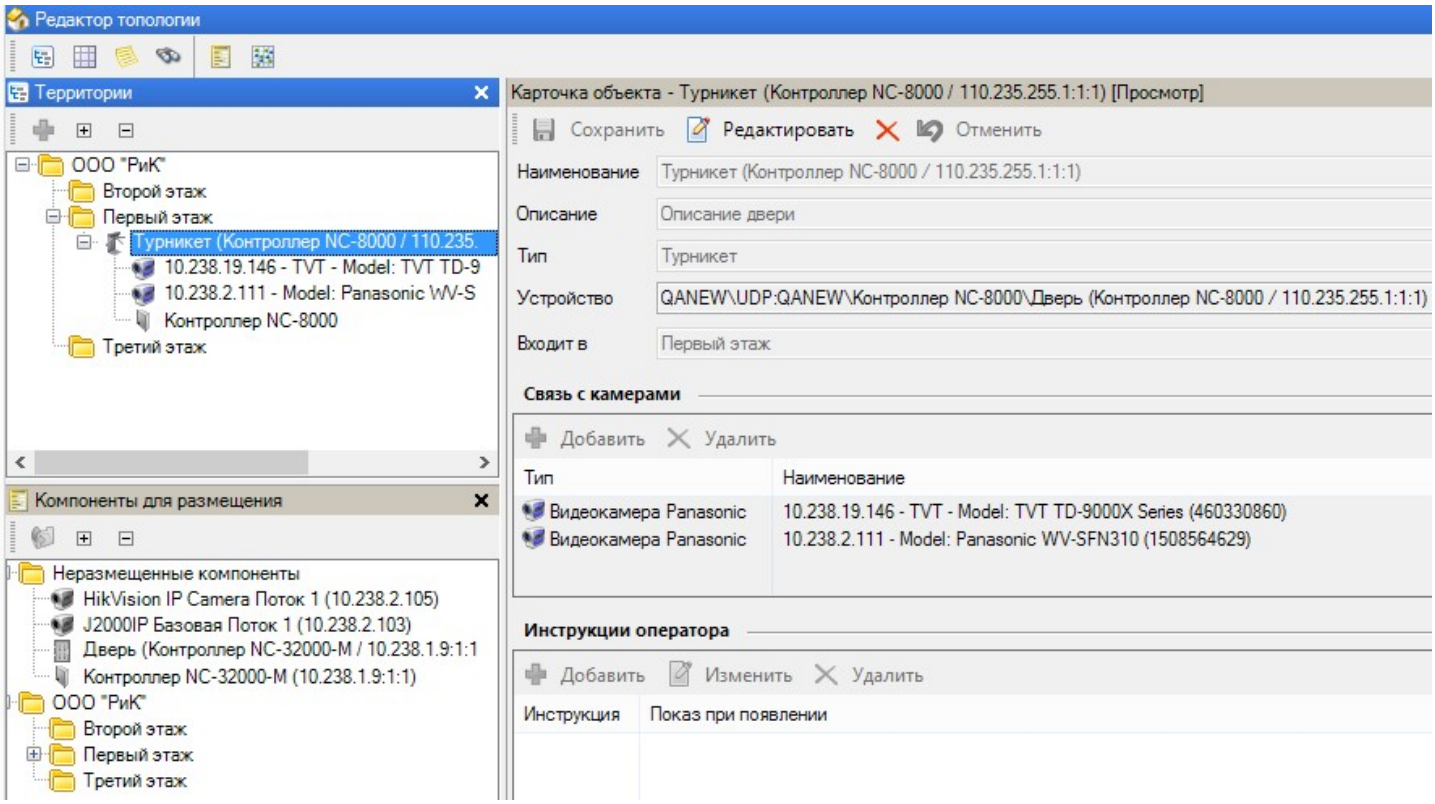
В примере на рисунке ниже "Турникет (Контроллер NC-8000 /1)" будет размещен в узле территорий *Первый этаж*:



Созданная таким образом структура используется конечными операторами для ссылки на объекты системы, навигации по объектам, управления объектами, конфигурирования областей, а также как источник событий для монитора событий.

Территориям типа "Дверь" и "Турникет" обязательно соответствует элемент "Контроллер". для удобства эти связанные элементы можно сгруппировать в дереве панели *Территории*. Для этого контроллер мышкой перетащите на дверь с тем же IP-адресом (на "чужую" дверь контроллер не перетащится). Вернутся к раздельному отображению этих элементов можно, перетащив контроллер обратно - в тот же или другой узел территорий.

Кроме того, связанные с дверью (турникетом) камеры также отобразятся в группе этой двери (турникета):



См. также

Создание графпланов[208]

Связь с камерами[211]

Инструкции оператору[212]

8.4.2 Создание графпланов

Компоненты графического плана

Графический план может включать в себя следующие компоненты:

- ***Подложка***. Графическое изображение, составляющее основу плана - например, план этажа, комнаты или другой территории. Поддерживаются подложки следующих форматов: *.bmp, *.gif, *.jpg, *.png, *.tif, *.emf, *.wmf.
  Если у вас подложка в другом формате, то с помощью любого графического редактора сконвертируйте ее в один из перечисленных форматов.

  Замечание: Предпочтительнее использовать растровые форматы - они компактнее и лучше масштабируются.

  Подложка на графическом плане может быть только одна.

- ***Текст***. Позволяет делать на плане текстовые пометки.

- ***Значок***. Используется для формирования статических изображений, поясняющих план.

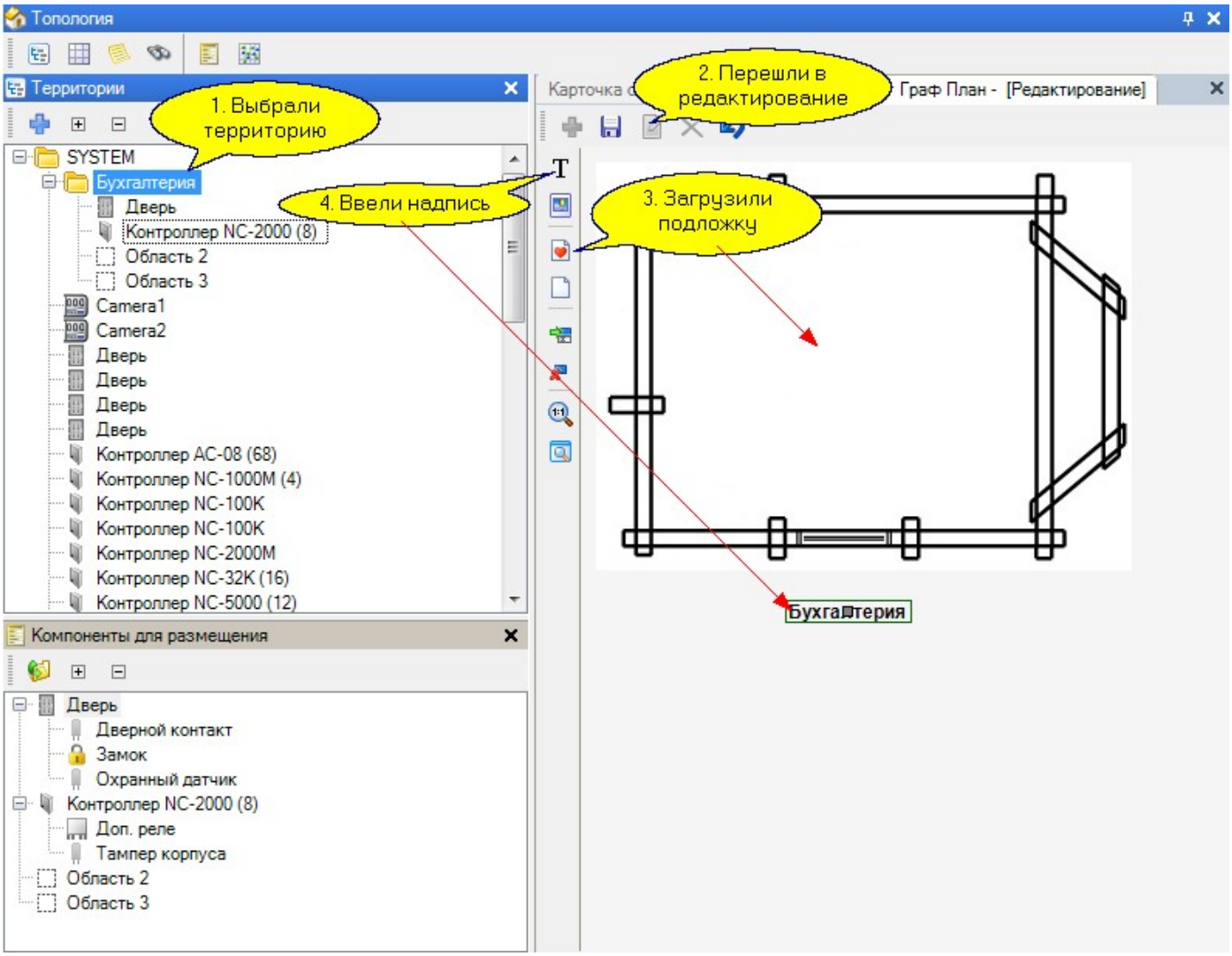
- ***Компонент***. Любой из компонентов, доступных в вашей системе - дверь, контроллер, дверной контакт и так далее. Любой компонент на конкретном графплане может присутствовать только один раз. Компоненты анимируются в реальном времени в соответствии с их статусом: например, дверь открывается и закрывается.

  Замечание: Поскольку анимированная графика требует достаточно много ресурсов от компьютера, старайтесь не "утяжелять" план ненужными компонентами.

Создание графплана

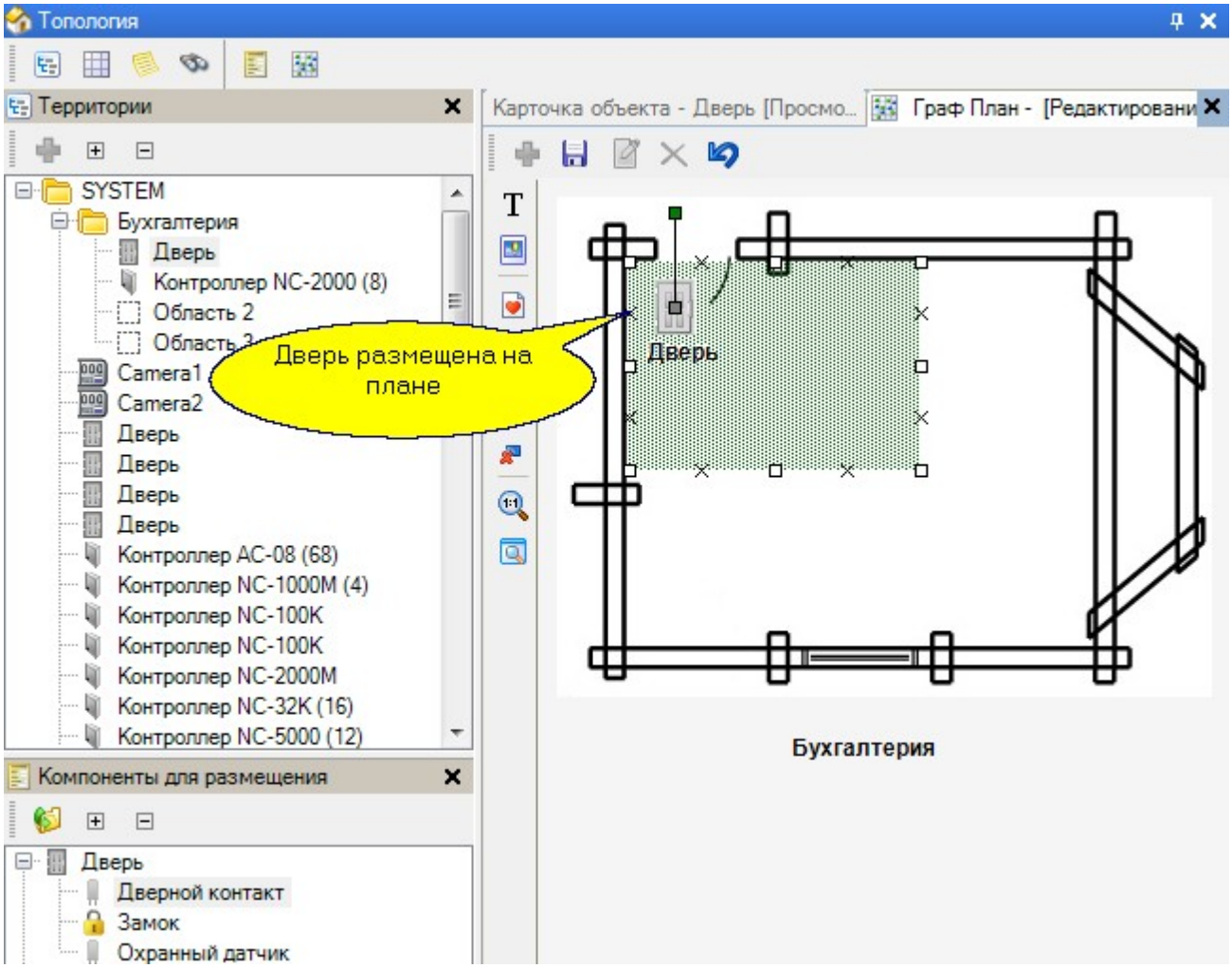
Для создания графплана в редакторе топологии перейдите в дереве топологии на территорию, для которой создается графплан, затем перейдите на вкладку *Граф План* с помощью соответствующего значка в панели инструментов редактора или щелкнув по заголовку вкладки.

После этого на панели редактора графплана нажмите на кнопку (*Создать*).



Загрузите заранее подготовленную подложку, при необходимости нанесите надписи и расставьте значки. Теперь можно размещать на графплане компоненты системы. В режиме редактирования графплана на панели компонентов для размещения будут доступны все компоненты системы, находящиеся на данном уровне иерархии и на всех вложенных уровнях. Например, для территории "SYSTEM" будут доступны все компоненты (они уже будут размещены на графплане), в том числе и территория "Бухгалтерия".

Для размещения компонента на плане просто перетащите его мышкой в нужное место. На рисунке ниже на графплане размещена дверь в бухгалтерию:



Надписи компонентов можно отредактировать, щелкнув правой кнопкой мышки на компоненте, размещенном на графплане.

При размещении на графплане территорий и дверей вокруг значков этих компонентов отображается зеленая сетка. С помощью нее можно отметить область, которая будет охраняться посредством данного компонента: охранной системой, размещенной на территории, или охранным датчиком контроллера двери. Для этого наведите курсор и потяните за маркеры на краях области. Двигая маркер в виде зеленого квадратика можно поворачивать всю зеленую область. Сетка будет изменять свой цвет при изменении статуса компонента.

(Если после обновления системы зеленая сетка у двери не появляется, удалите, а затем снова разместите ее на графплане).

После сохранения плана можно посмотреть его работу в Мониторе событий[287].

Значки компонентов графплана и принадлежащие им области имеют цвет, соответствующий состояниям:

Тревоги: Охранная, Пожар, Паника, Принуждение, Технологическая - красный (RGB 255, 0, 0)	
Пожарное внимание - оранжевый (RGB 255, 204, 0)	
Активация (реле, устройство и т.п.) - красный (RGB 255, 0, 0)	
Блокировка - оранжевый (RGB 255, 204, 102)	
Неисправность - желтый (RGB 255, 255, 100)	
Взлом - голубой (RGB 0, 153, 255)	
Норма, раздел не на охране - серый (RGB 127, 127, 127)	

Раздел на охране с пропуском зон (ШС) (RGB 0, 255, 255)	
Норма, раздел взят на охрану - зеленый (RGB 0, 204, 0)	
Состояние не определено - коричневый (RGB 102, 102, 51)	
Задержка (на взятие/снятие с охраны) - салатовый (RGB 127, 204, 127)	

8.4.3 Связь с камерами

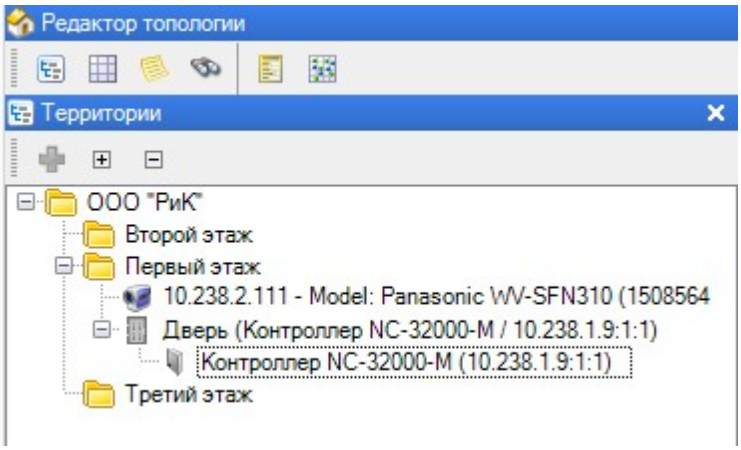
Если на точку прохода направлена одна или несколько видеокамер, то логично объединить эти компоненты системы в одну группу.

Связанные камеры позволяют просматривать архивированный видеофрагмент, начинающийся в момент события на точке прохода (при условии, что для камеры проинтегрированной системы видеонаблюдения настроена запись архива; для IP-камер, подключенных напрямую к ParsecNET 3 архив не записывается). Просмотр доступен[301] из ленты событий Монитора событий и из Отчета по событиям.

Кроме этого связанные камеры позволяют просмотреть "живое" видео точки прохода в Мониторе событий на графическом плане[291] или в дереве территорий[294].

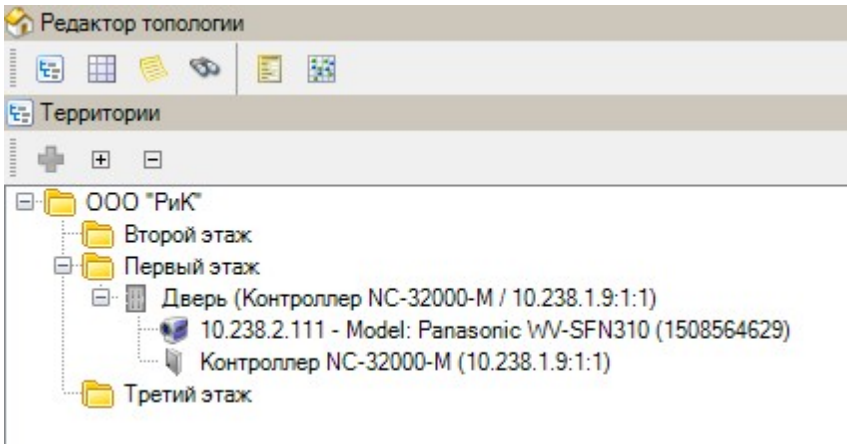
Для привязки камер к двери выполните следующие шаги:

1. Разместите дверь и направленную на нее камеру в одном и том же узле территорий:



2. Перетащите камеру на дверь и подтвердите свое действие.

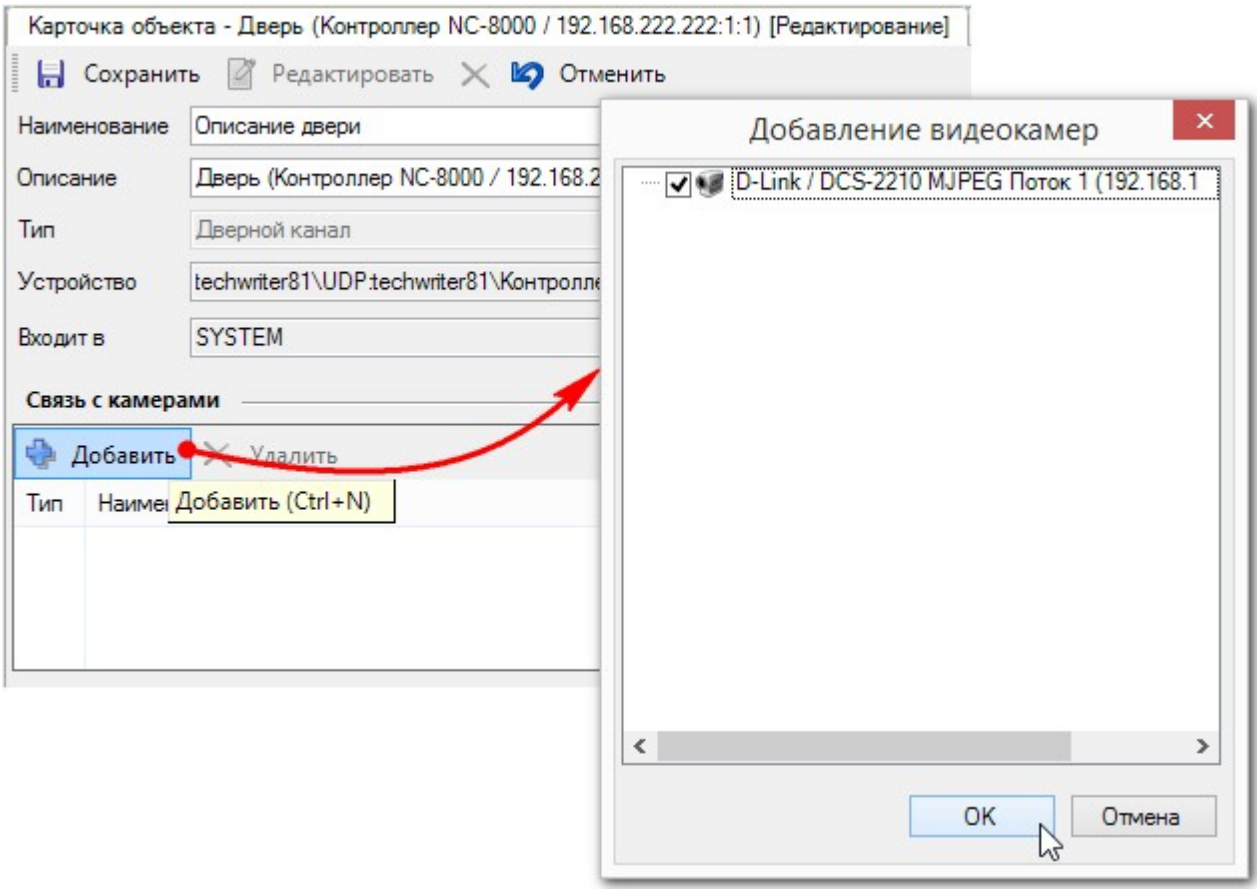
Теперь камера входит в группу двери:



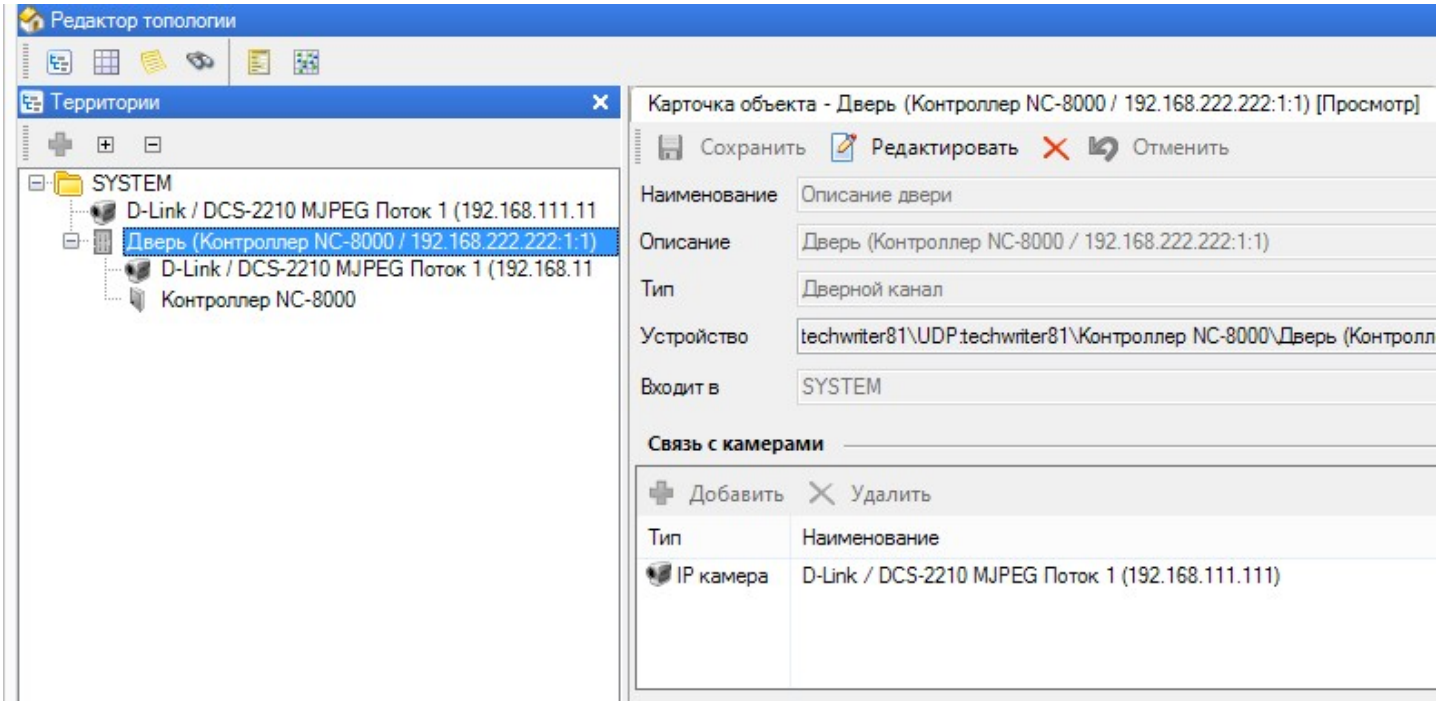
Вывести камеру из группы можно обратным действием - перетащив камеру в тот же или другой узел территорий.

Вместо описанного выше, можно связать камеру с дверью другим способом. При этом в топологии камера будет отображаться и в группе двери, и в корневой директории дерева территорий, что позволить, например, разрешить оператору в топологии видеть камеру, но не

видеть дверь. Для такого варианта связи используйте панель *Связь с камерами* в карточке объекта *Дверь*:



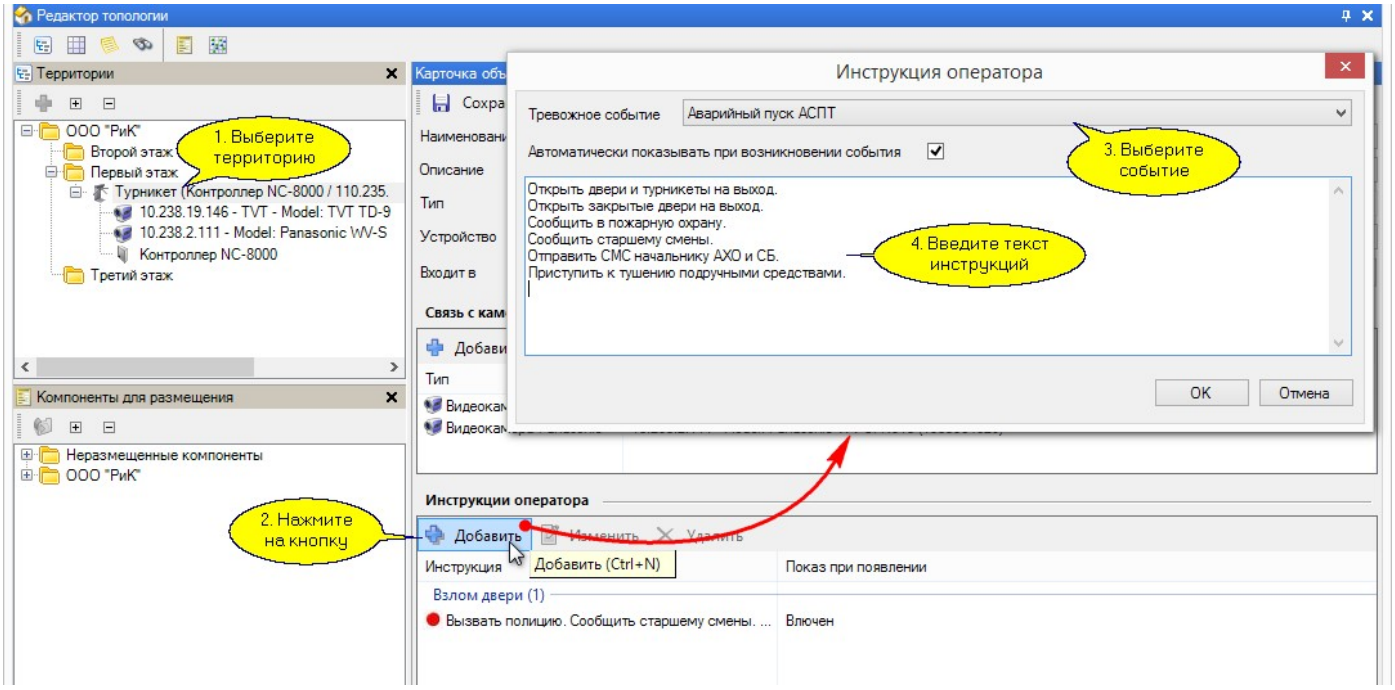
Дерево территорий после добавления таким способом будет выглядеть так:



8.4.4 Инструкции оператору

Инструкции оператору позволяют при возникновении тревожного события на определенной территории выдать визуальную информацию, помогающую оперативно выполнить необходимые в такой ситуации действия.

Для задания инструкции оператору выберите необходимый компонент в дереве территории, перейдите на панель карточки объекта и перейдите в режим редактирования. Теперь выберите из раскрывающегося списка тревожное событие, а ниже в окне введите инструкцию оператору.



После сохранения данная инструкция будет автоматически появляться в отдельном окне в Мониторе событий при возникновении тревожного [события](#)[300] с выбранного источника (в нашем случае инструкции будут появляться при взломе турникета и при включении автоматической системы пожаротушения). Автоматическое появление инструкций во всплывающем окне возможно только при запущенном Мониторе событий и установленном флажке *Автоматически показывать при возникновении события*.

Если флажок не установлен, то инструкции появятся при двойном щелчке на событии в Мониторе событий.

8.5 Редактор расписаний

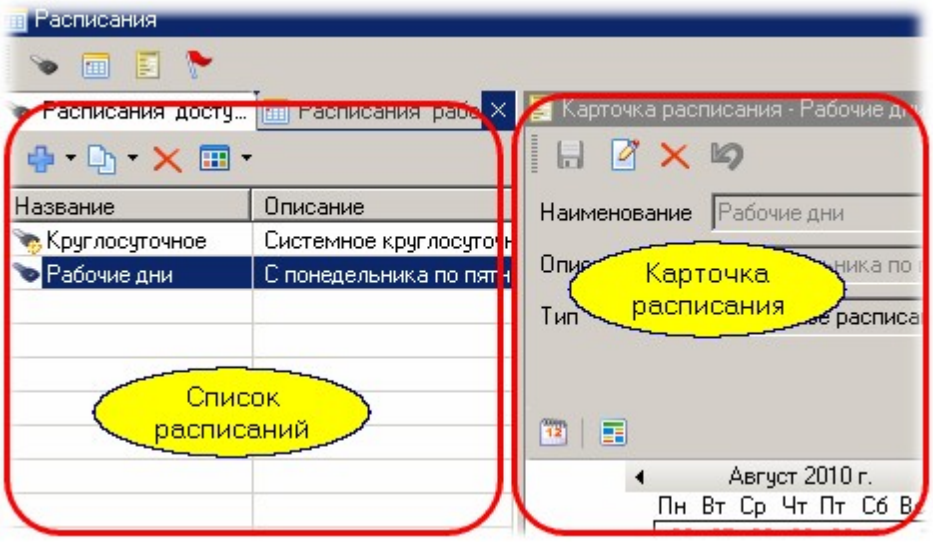
Назначение

Редактор расписаний позволяет создавать два типа расписаний:

- ***Расписания доступа***. Используются для ограничения доступа на территорию по времени, если это необходимо. Если ограничивать доступ не требуется, то можно использовать всегда существующее в системе круглосуточное расписание. Расписание доступа в дальнейшем используется при создании групп доступа.
- ***Расписания рабочего времени***. Используются только в подсистеме учета рабочего времени персонала. Имеют больше настроек для описания специфики рабочего времени в разных режимах: обычная рабочая неделя, сменные графики работы, свободные графики.

Панели редактора расписаний

Поскольку расписания не образуют иерархических структур, редактор расписаний имеет две панели: панель списка расписаний и карточку расписания, которая отображает свойства выбранного на данный момент расписания. В карточке также осуществляется создание и редактирование выбранного расписания.



Типы расписаний

Система ParsecNET 3 поддерживает расписания различной структуры - как недельные[216], привязанные к календарю, так и сменные[219], которые привязки к календарю не имеют.

Кроме того, расписания подразделяются на расписания доступа, которые определяют временные интервалы, когда субъект доступа может заходить в помещение, так и расписания для подсистемы учета рабочего времени (УРВ). Расписания УРВ используются для определения отработанного времени с учетом правил его подсчета. Подробнее об этом можно посмотреть в разделе Модуль учета рабочего времени[456]. Расписания УРВ имеют целый ряд специфичных именно для данного применения параметров. Если вы не используете УРВ, то расписания данного типа вам не потребуются.

Расписания доступа используются для следующих целей:

- Назначаются группе доступа для определения прав доступа на территорию во времени.
- Для автоматизации поведения оборудования, если данное оборудование поддерживает такие функции. Например, по расписанию область охраны может ставиться на охрану и сниматься с нее.

В дополнение к расписаниям редактор позволяет задавать праздничные дни, а также создавать дни-исключения (например, рабочий день в выходной при переносе праздника).

В примерах создания расписаний доступа (как недельного, так и сменного) для простоты не добавлялось запасное время. При создании реальных расписаний следует помнить, что если рабочее время начинается в 8 утра, то сотрудник должен иметь как минимум 15-минутный запас для входа, то есть должен иметь возможность прохода на территорию уже с 7 часов 45 минут.

Сказанное относится и к окончанию рабочего времени. Величину запаса вы должны определять сами.

Круглосуточное расписание

Круглосуточное расписание представляет собой особый тип расписания - оно действует всегда. Если вы назначаете для доступа круглосуточное расписание, то вход в помещение по времени никак не ограничивается.

Это расписание всегда присутствует в системе. Если вам не требуется ограничений во времени, вы можете назначать это расписание для любой группы доступа.

Создание расписаний

Все создаваемые расписания могут использоваться всей организацией. При этом расписание можно использовать "как есть", а можно на основе расписания для организации создать модифицированный вариант расписания для подразделения или даже для конкретного человека.

1. ***Обратите внимание, нецелесообразно создавать персональное расписание для каждого сотрудника, поскольку оборудование, в отличие от ПК, поддерживает весьма ограниченное количество расписаний.***



2. ***При создании сложных групп доступа следите за тем, чтобы в разных расписаниях не конфликтовал такой параметр, как использование праздников - контроллеры не в состоянии разрешить такие конфликты.***
3. ***Учитывайте, что большинство типов контроллеров поддерживают только недельные расписания доступа.***

См. также:

Недельное расписание доступа[216]

Сменное расписание доступа[219]

Расписание рабочего времени[221]

Праздничные дни[238]

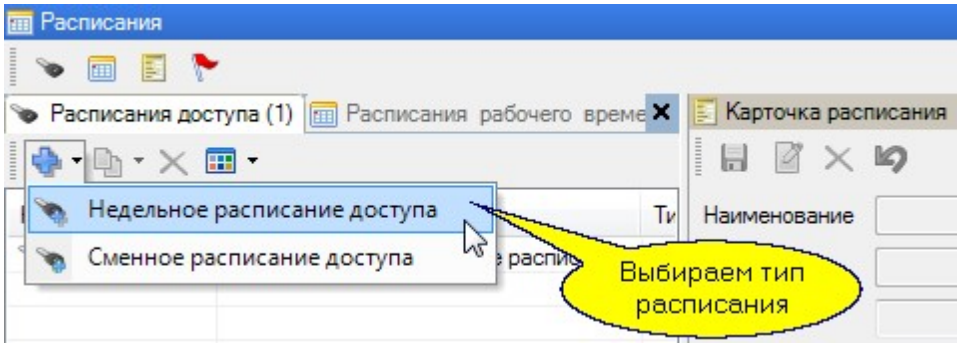
Дни-исключения[241]

Копии ранее созданных расписаний[243]

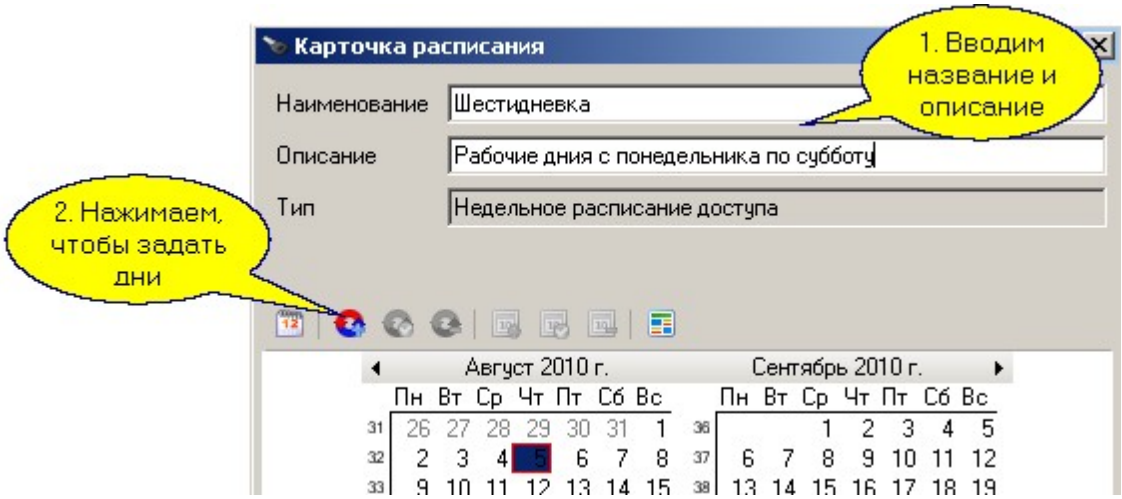
8.5.1 Недельное расписание доступа

Создание недельного расписания доступа

В панели списка расписаний выбираем тип расписания, которое будем создавать:

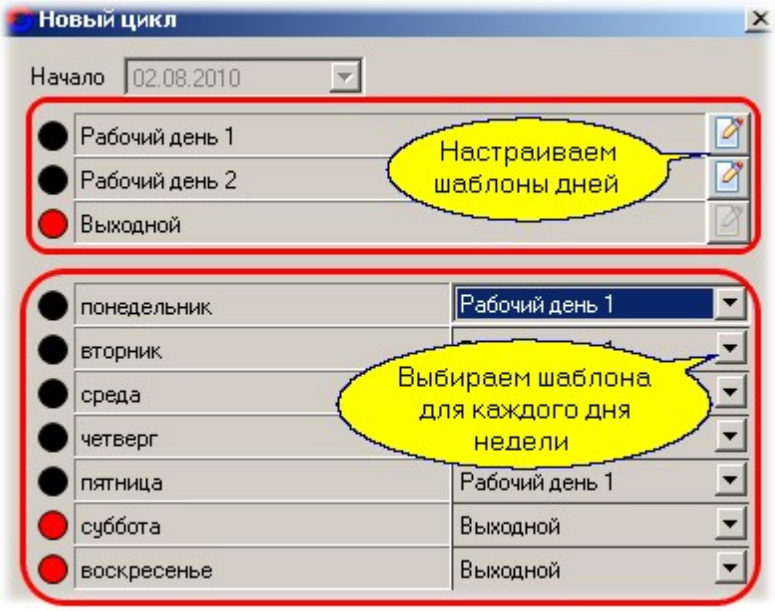


В появившемся диалоге вводим название расписания и опциональное описание (комментарий). Для недельного расписания доступа праздники применяются с заменой рабочего дня на выходной.

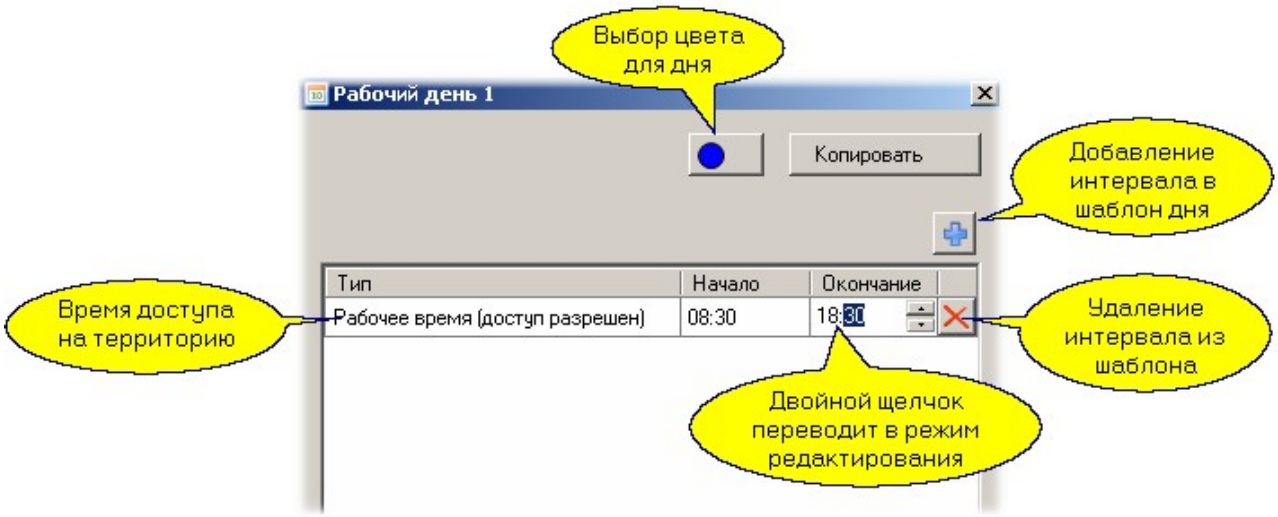


Обратите внимание, при создании нового расписания автоматически создается цикл с началом в текущую дату. Если начало цикла не совпадает с датой создания расписания, то перед заданием цикла надо на календаре выбрать нужную дату, а затем уже создавать цикл.

После нажатия на кнопку *Назначить цикл* (или *Редактировать цикл*) появляется диалог для формирования расписания по дням. В недельном расписание сразу формируется семь дней с началом в ближайший прошедший понедельник. Эти дни используем при создании расписания:



Нажав, например, на кнопку редактирования шаблона "Рабочий день 1", получаем возможность установить интервалы доступа для первого шаблона рабочего дня:



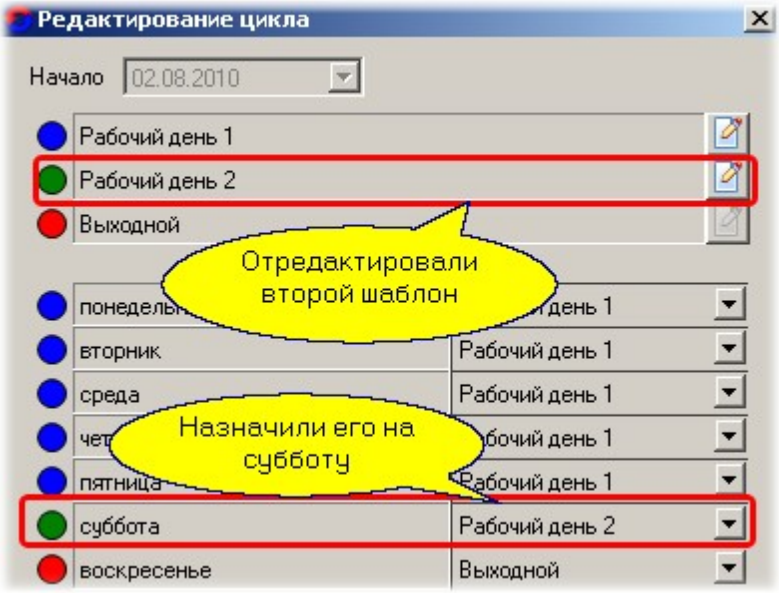
На рисунке выше виден диалог настройки шаблона после того, как мы изменили рабочее время с установленного по-умолчанию (с 9:00 до 18:00) на интервал с 8:30 до 18:30, дав запас времени по полчаса на приход до начала рабочего дня и уход после его окончания. Кроме того, можно сменить цвет для редактируемого шаблона, а также добавить интервалы.

Важно: контроллеры могут поддерживать в течение одного дня до четырех временных интервалов, но из-за ограничений в размере памяти это приведет к уменьшению количества шаблонов. Другими словами, в расписании можно использовать либо два шаблона настроек дней с двумя временными интервалами, либо один шаблон с четырьмя интервалами.

Реально два интервала полезны при назначении ночной смены, как это будет показано ниже при создании сменного расписания доступа.

Скорректировав первый шаблон рабочего дня, назначаем его с понедельника по пятницу.

Допустим, что в субботу у нас укороченный на час рабочий день. Для такой ситуации редактируем шаблон "Рабочий день 2", установив время доступа на территорию с 8:30 до 17:30, после чего назначаем этот день на субботу, как показано ниже:



После сохранения расписания его можно будет использовать при создании групп доступа.

См. также:

- Сменное расписание доступа[219]
- Расписание рабочего времени[221]
- Праздничные дни[238]
- Дни исключений[241]
- Копии ранее созданных расписаний[243]

8.5.2 Сменное расписание доступа

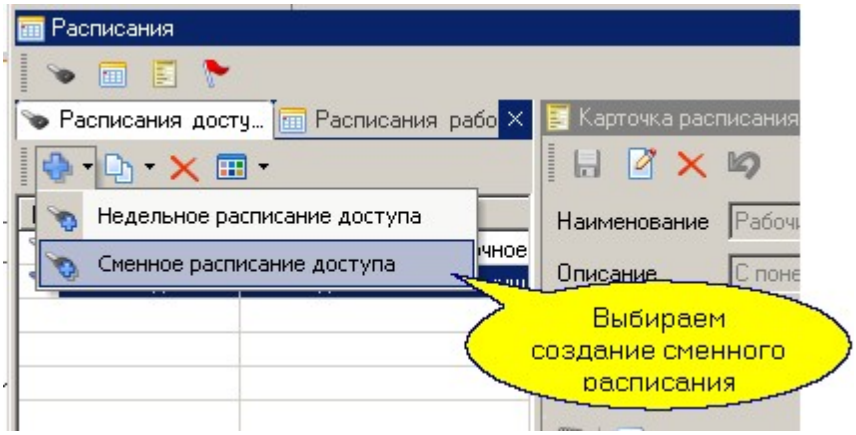
Сменные расписания позволяют задавать временные интервалы для доступа без привязки к календарной неделе. Такие расписания можно использовать, например, для описания сменных графиков типа "сутки через двое" и аналогичных.В принципе, с помощью последовательности сменных расписаний можно задать графики доступа любой сложности, однако следует помнить, что в контроллерах поддержка таких расписаний ограничена. В частности, контроллеры NC-1 000, NC-2000, NC-5000 поддерживают только недельные расписания.

Для аппаратной поддержки сменных расписаний необходимо использовать контроллеры NC-32K.M/NC-32K-IP, NC-8000(-D, -I), NC-60K/NC-60K.M и NC-100K-IP.

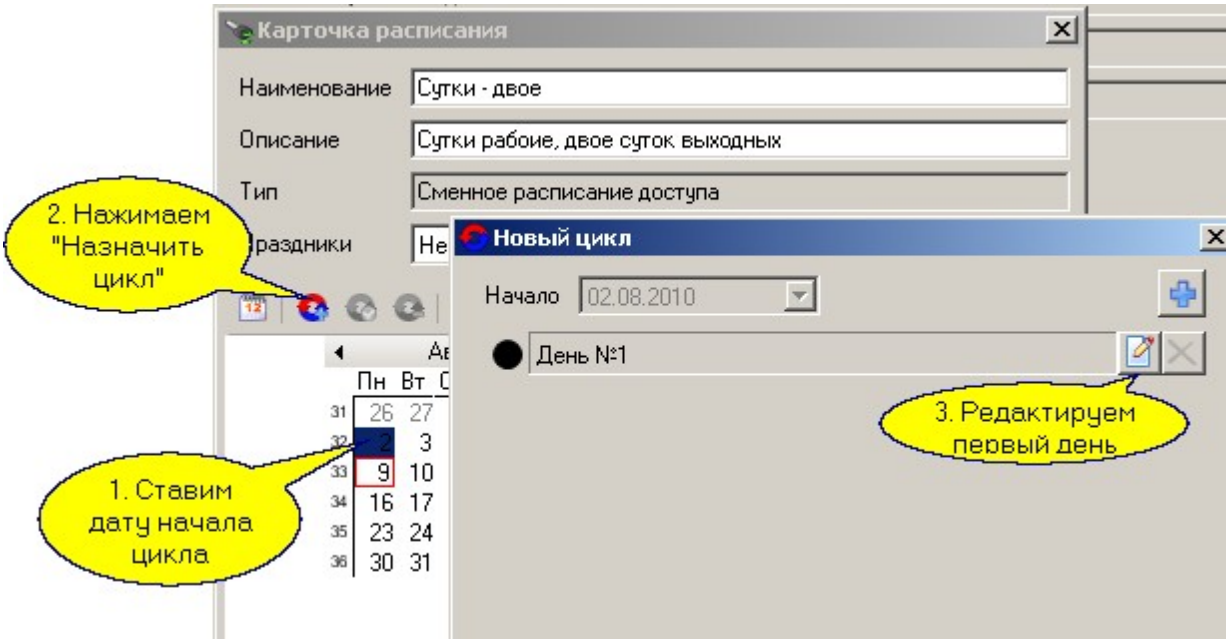
Создание сменного расписания доступа

Сменные расписания доступа поддерживаются не всеми контроллерами. Контроллеры NC-1000/2000/5000 поддерживают только недельные расписания и праздники.

Для создания сменного расписания выберите из меню редактора расписаний *Сменное расписание* доступа, как показано ниже:



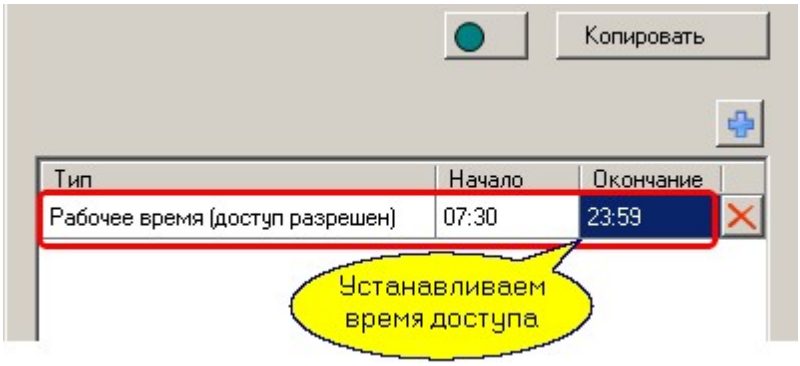
В карточке расписания введите название, описание и укажите, как учитывать праздники. В нашем случае мы выбрали "Не учитывать", как это обычно бывает при сменном графике работы. Создадим цикл "сутки через двое" с использованием ночной смены, выбрав начальный день цикла:



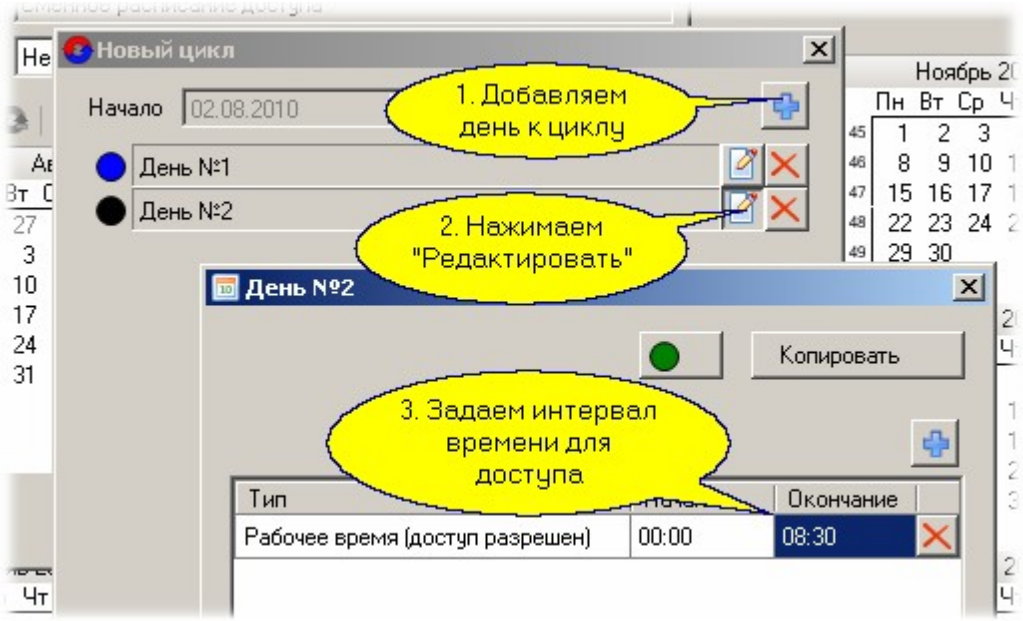
Обратите внимание, при создании нового расписания автоматически создается цикл с началом в текущую дату. Поэтому, когда маркер календаря установлен на "сегодня", кнопка *Создать цикл* неактивна. Можно только отредактировать созданный по-умолчанию цикл или удалить его, а потом создать заново (как на рисунке выше).

Если начало цикла не совпадает с датой создания расписания, то перед заданием цикла надо на календаре выбрать нужную дату, а затем уже создавать цикл.

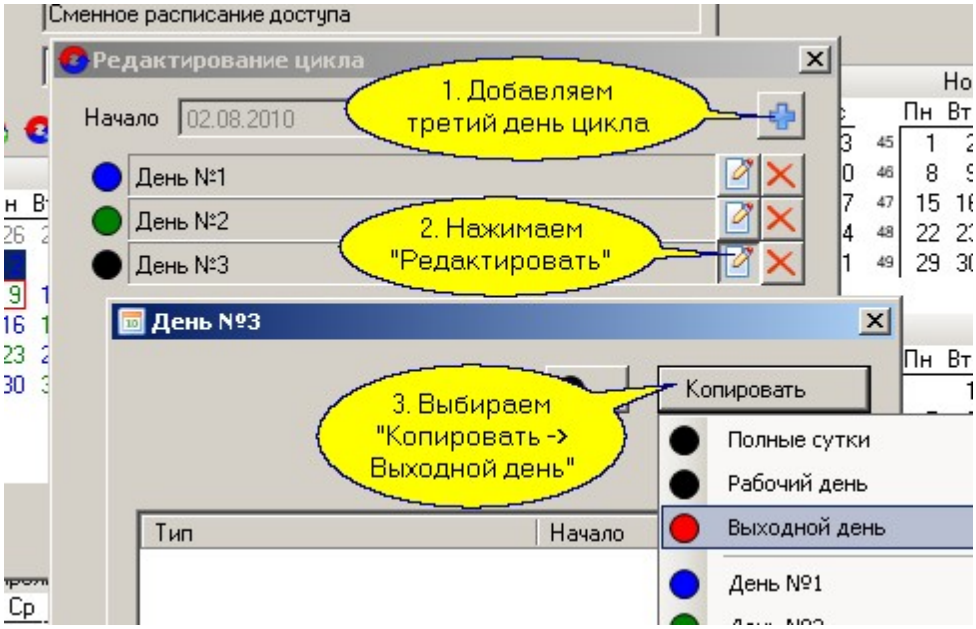
Начинаем цикл с даты, даты сотрудник заступает на смену, при этом считаем, что смена продолжается с 8:00 до 8:00 следующего дня. В первый день назначаем интервал с 7:30 до 23:59. Отредактируем первый день цикла нашего расписания:



Второй день начинается с полуночи и заканчивается в 8:00, но мы даем получасовой запас для ухода с работы, то есть ставим 8:30. Добавляем второй день с интервалом от 00:00 (полночь) до 8:30 утра:



Теперь добавляем третий день, который будет целиком выходным, и наше расписание готово. Обратите внимание, что выходной день не содержит никаких интервалов.



То есть сотрудник начинает работать с 8 утра в понедельник 2 августа, во вторник 3 августа в 8 утра он заканчивает работу, затем до 8 утра среды (4 августа) у него первые сутки отдыха, вторые сутки отдыха - до 8 утра четверга (5 августа), когда он опять заступает на смену.

Естественно, что для работников остальных двух смен надо также создать аналогичные расписания, но только со сдвигом на один и на два дня, что удобно делать копированием[243] текущего расписания.

См. также:

- Недельное расписание доступа[216]
- Расписание рабочего времени[221]
- Праздничные дни[238]
- Дни исключений[241]
- Копии ранее созданных расписаний[243]

8.5.3 Расписания рабочего времени

Лицензируемый модуль учета рабочего времени[456] (УРВ) анализирует данные, связанные с персоналом предприятия: количество отработанных часов, время прихода и ухода, опоздания, прогулы и прочее, позволяя создавать бизнес-отчеты.

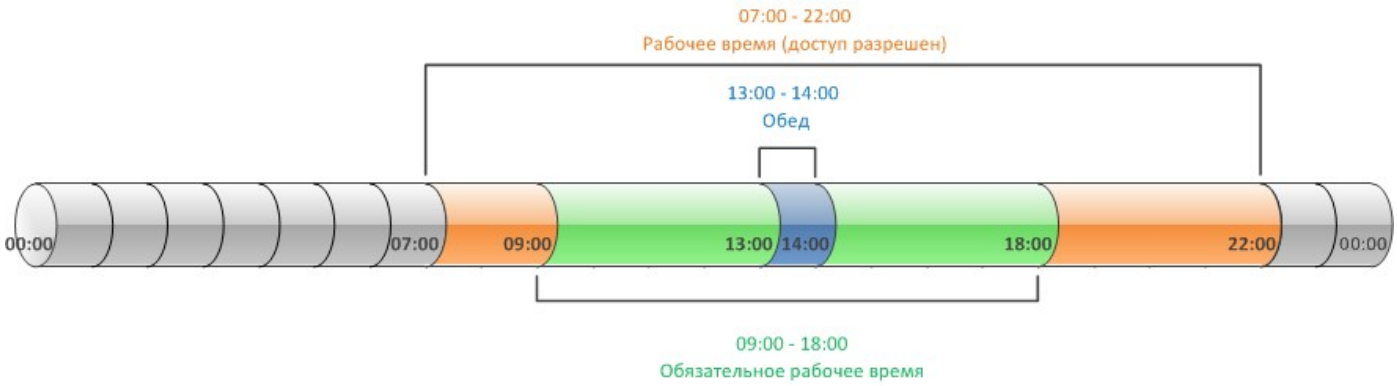
Для получения отчета УРВ используется много исходных данных, часть из которых может настраиваться оперативно при создании отчета (правила подсчета и некоторые другие), а часть задается практически один раз после установки системы. К редко настраиваемым параметрам относятся расписания рабочего времени, создаваемые в редакторе расписаний (запускается кнопкой ).

При составлении расписания рабочего времени обратите особое внимание на следующие важные моменты:

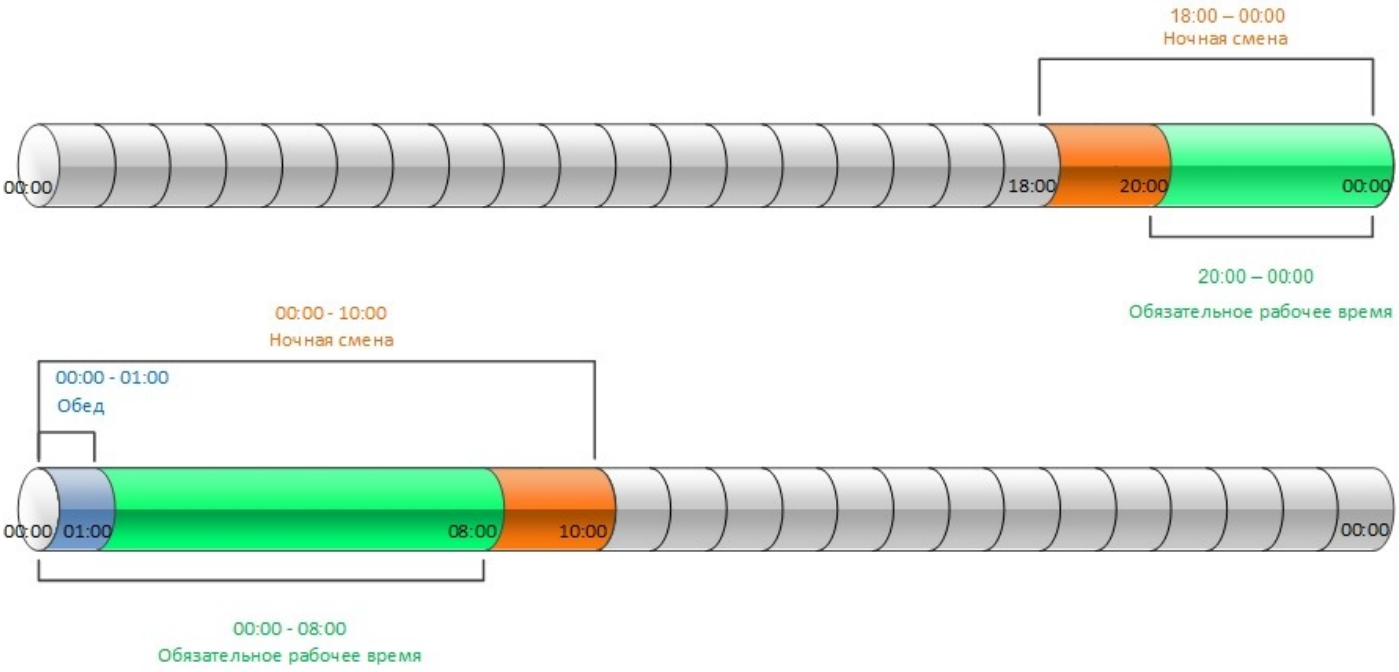
- На отчетный период (периоды) необходимо заранее составить расписание, соответствующее графику работы подразделения. Если это стандартное недельное расписание, то оно может быть единственным и действовать без изменений достаточно долго;
- Не забудьте в редакторе расписаний ввести праздники, а также дни-исключения (например, рабочий день в выходной при переносе праздника), и указать вариант использования праздников в конкретном расписании (см. раздел[238] настройки праздников);

- Обязательно укажите нормы отработки за день и за неделю, чтобы обсчет отработанного времени и анализ различных отклонений проводился корректно;
- Учитывайте, что существуют два типа рабочего времени:
  - простое, когда человек может находиться на рабочем месте (но не обязан, например ввиду свободного графика), и не должен находиться на рабочем месте в нерабочее время;
  - обязательное, когда человек обязан быть на работе (например сотрудник службы технической поддержки). Учитываются отклонения и нарушения именно этого типа рабочего времени.

На рисунке ниже приводится пример соотношения типов рабочего времени:



На следующем рисунке отображен пример соотношение типов рабочего времени для случая ночной смены:



Расписания рабочего времени никак не влияют на доступ в помещения. Они используется только для расчета отработанного времени в модуле УРВ. Расписания рабочего времени могут быть как недельными, привязанными к календарю, так и сменными, привязки к календарю не имеющими.

Все создаваемые расписания могут использоваться всей организацией. При этом расписание можно использовать "как есть", а можно на основе расписания для организации создать модифицированный вариант для подразделения или даже для конкретного человека.

От назначенных типов временных интервалов и норм отработки будет зависеть расчёт рабочего времени сотрудника.

Необходимо помнить, что от правильности настроек расписания рабочего времени будет зависеть правильность построения бизнес-отчётов.

При создании расписаний используются следующие понятия:

Типы временных интервалов:

- *Рабочее время (доступ разрешён)* – в рамках данного типа указывается допустимое время пребывания сотрудника на рабочем месте. Работник может не присутствовать в течение всего указанного интервала, при этом нарушения не фиксируются, если не нарушены иные условия;
- *Обязательное рабочее время* – в рамках данного типа указывается обязательное время пребывания сотрудника на рабочем месте. Отсутствие в это время засчитывается как нарушение, если время отсутствия превышает заданное в шаблоне отчета (в редакторе Бизнес-отчётов);
- *Перерыв на обед* – если интервал обеденного перерыва задан, то это время не засчитывается в отработанное время;
- *Ночная смена* – при добавлении данного типа появляется временной интервал, в котором указывается начало работы (например: с 20:00 до 00:00). Во втором дне указывается окончание работы (например: с 00:00 до 08:00).

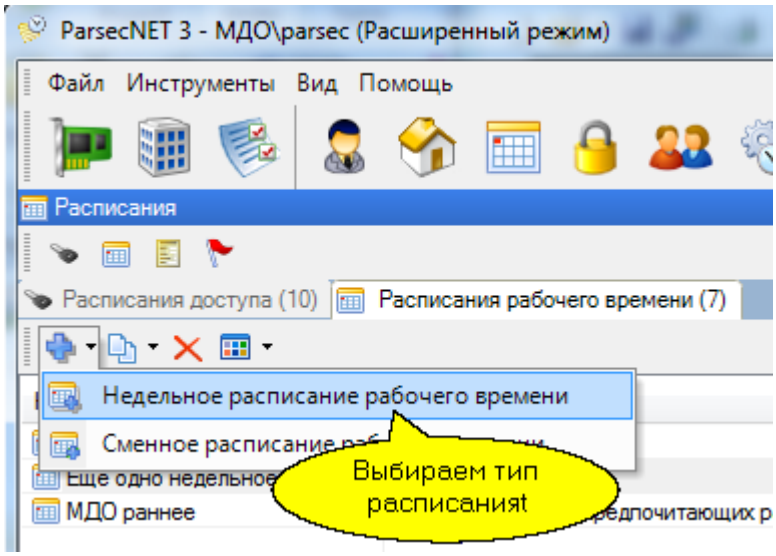
Норма отработки. Указываются обязательные часы отработки в день и в неделю. Эти параметры учитываются как норма, в частности, в недельных табелях. Данные значения используются при сопоставлении с временем, фактически отработанным за выбранный период, для принятия решения о недоработке, переработке и нарушениях.

8.5.3.1 Недельное расписание рабочего времени

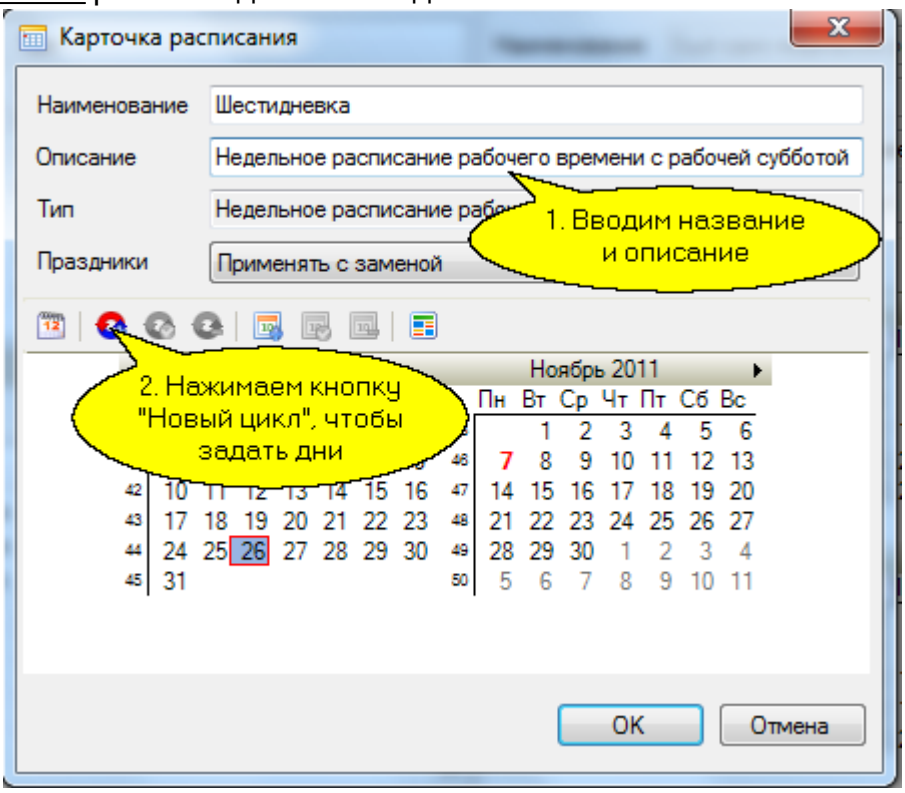
Расписание рабочего времени никак не влияет на доступ в помещения. Он используется только для расчета отработанного времени в Модуле учета рабочего времени[456].

Создание недельного расписания рабочего времени

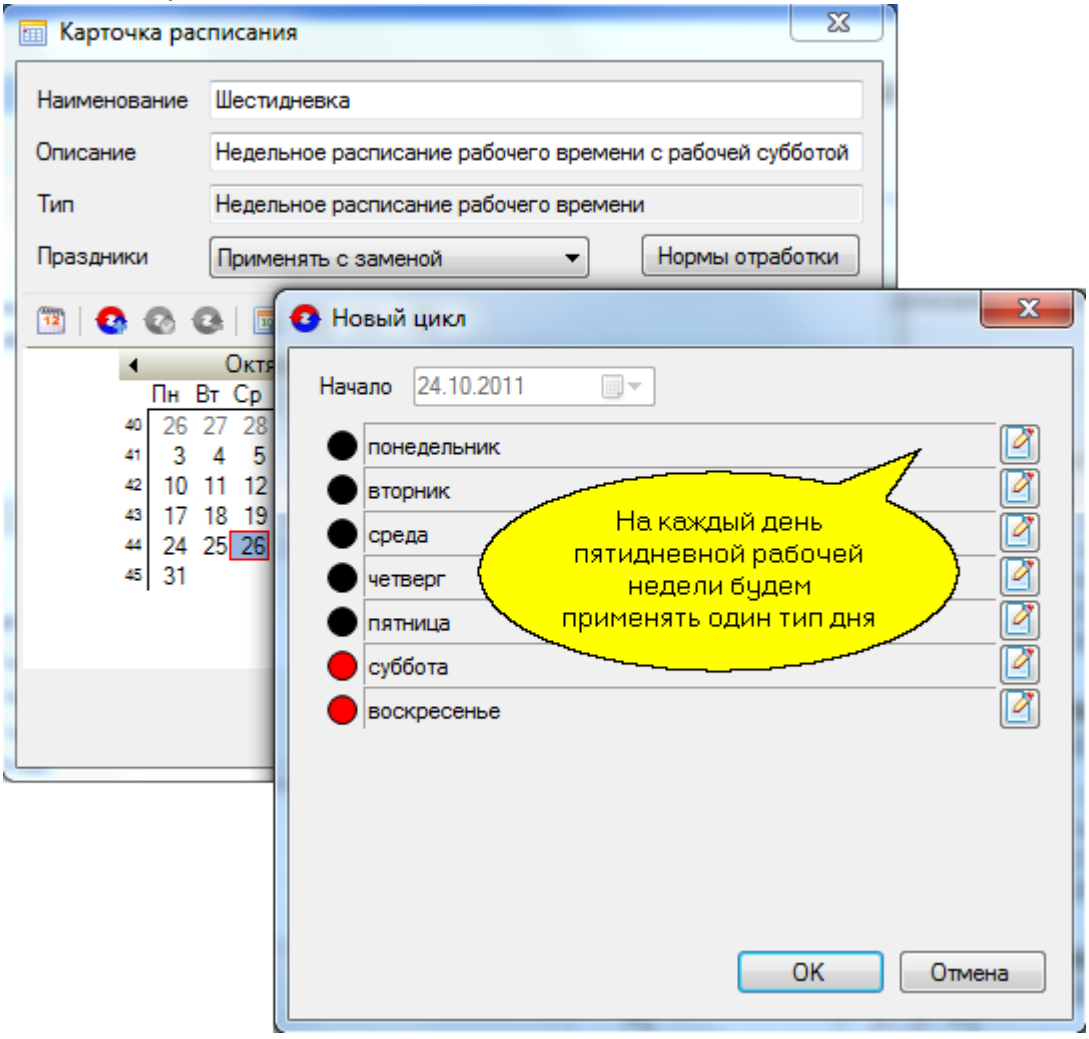
На вкладке *Расписания рабочего времени* в раскрывающемся списке кнопки *Добавить* выберите тип "Недельное расписание рабочего времени".



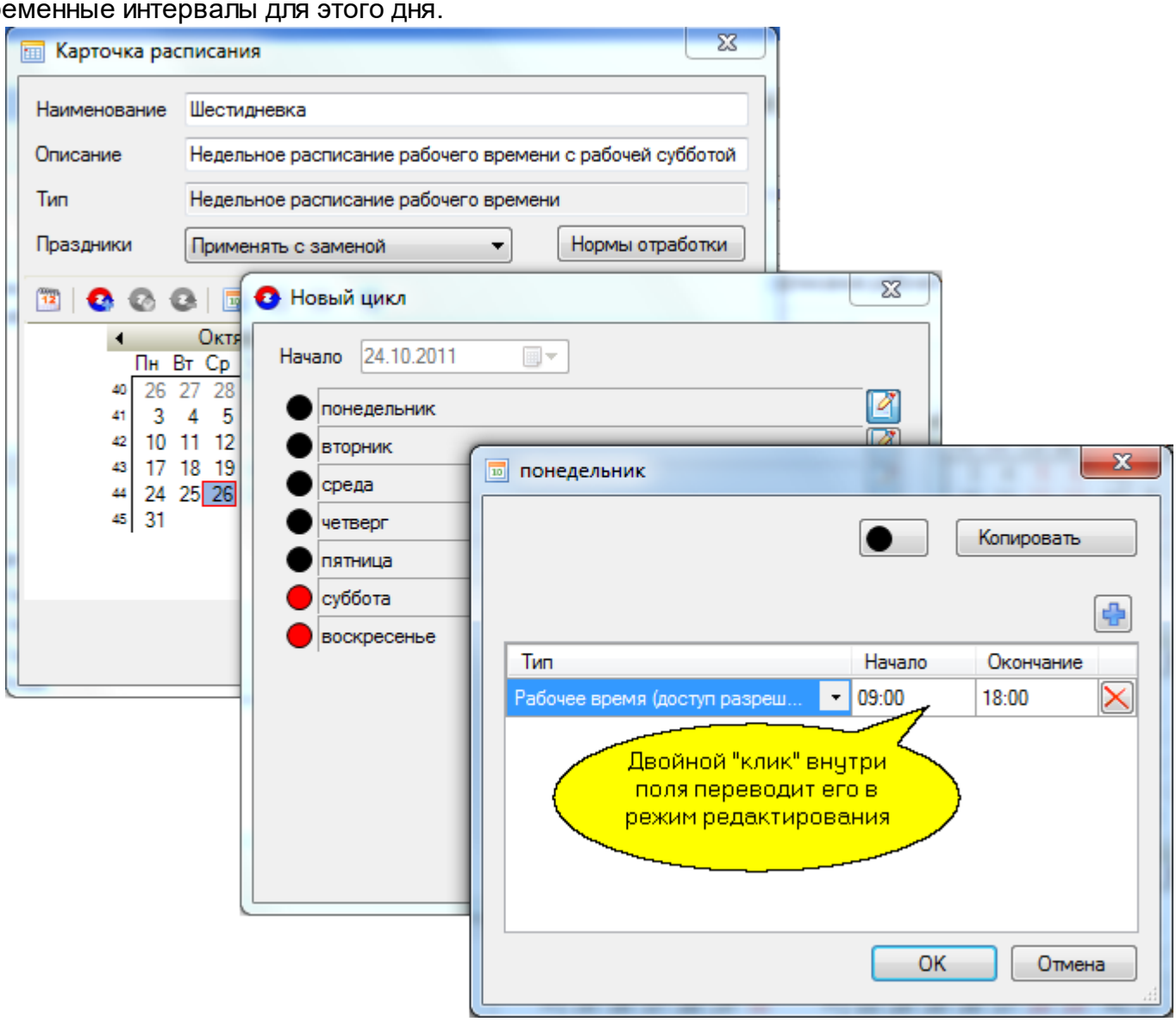
В появившемся диалоге введите название расписания, предположим, шестидневной рабочей недели и, по желанию, описание. Для недельного расписания рабочего времени праздники применяются с заменой рабочего дня на выходной.



После нажатия на кнопку *Назначить цикл* появляется диалог для формирования расписания по дням. В недельном расписании рабочего времени автоматически формируется семь дней с началом в ближайший прошедший понедельник.



Нажав на кнопку редактирования понедельника мы получаем возможность установить временные интервалы для этого дня.



В поле *Тип* из раскрывающегося списка можно выбрать:

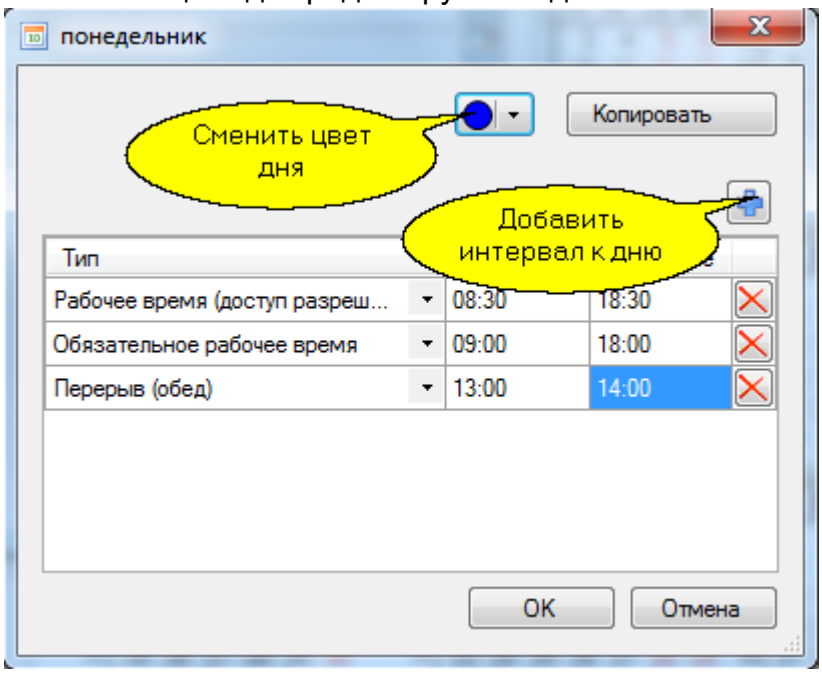
- "Рабочее время (доступ разрешен)" - для задания временного периода, когда пользователь может находиться на рабочем месте. Обычно совпадает с расписанием доступа;
- "Ночная смена" - особый тип рабочего времени для учета ночной смены. Если рабочее время сотрудника должно считаться как ночная смена, выберите этот тип для временного периода, когда он может находиться на рабочем месте. При этом интервал с типом "Рабочее время (доступ разрешен)" устанавливать не нужно;
- "Перерыв (обед)" - для задания времени перерыва;
- "Обязательное рабочее время" - для задания временного периода, когда пользователь должен находиться на рабочем месте.

  В общем случае задаются два интервала - "Рабочее время" и "Обязательное рабочее время". Первый, чтобы не учитывалось слишком долгое пребывание на работе, например, когда сотрудник не отметился при уходе. Второй интервал - для учета отклонений;

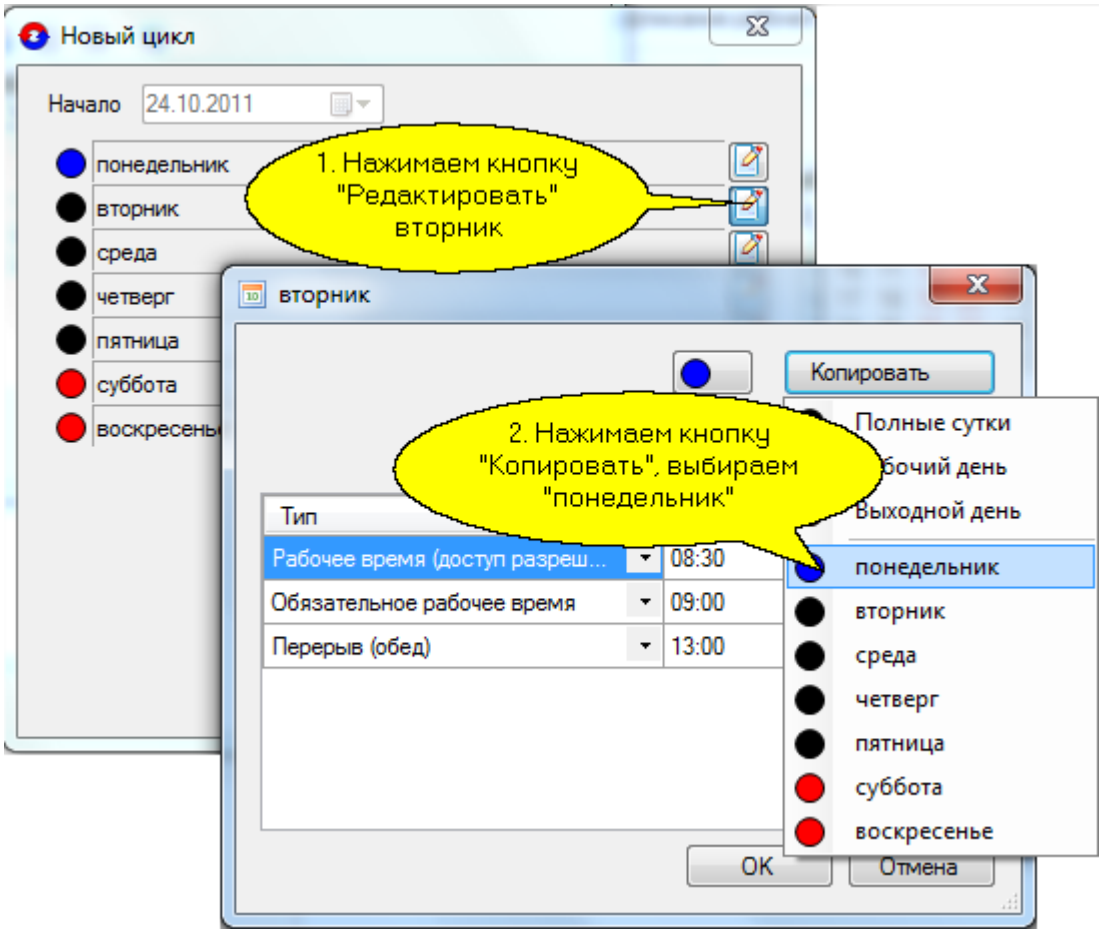
Ниже показан диалог настройки дня после того, как мы изменили интервал рабочего времени (доступ разрешён) с установленного по-умолчанию (с 9:00 до 18:00) на интервал с 8:30 до 18:30,

дав запас времени по полчаса на приход до начала рабочего дня и уход после его окончания. Также нужно ввести интервал обязательного рабочего времени, и, при необходимости, интервал перерыва (обед).

Кроме того, вы можете сменить цвет для редактируемого дня.

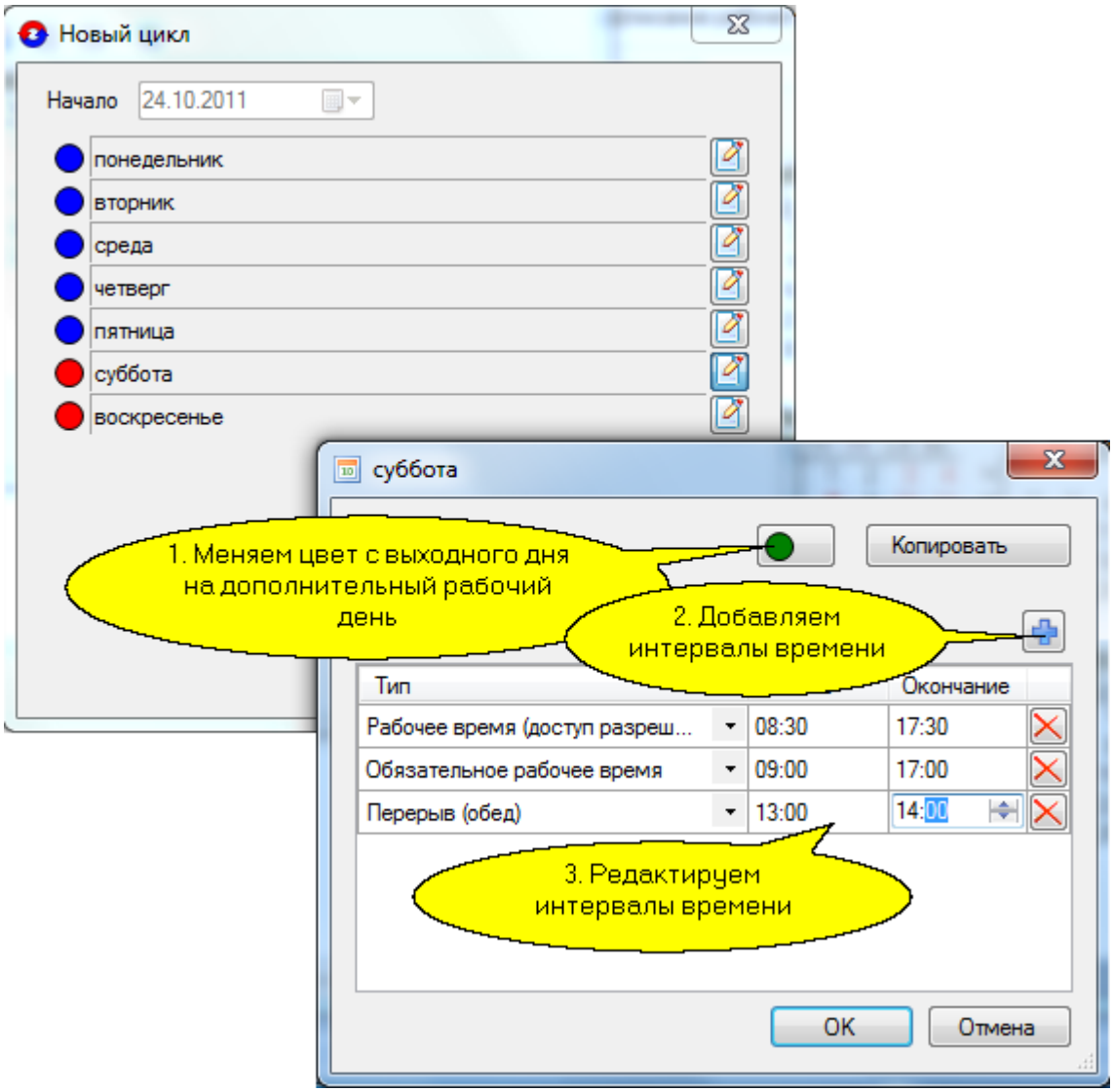


Скорректировав понедельник, мы можем применить его в качестве шаблона ко всем рабочим дням со вторника по пятницу. Делается это при помощи кнопки *Копировать* в окне настройки каждого дня недели.

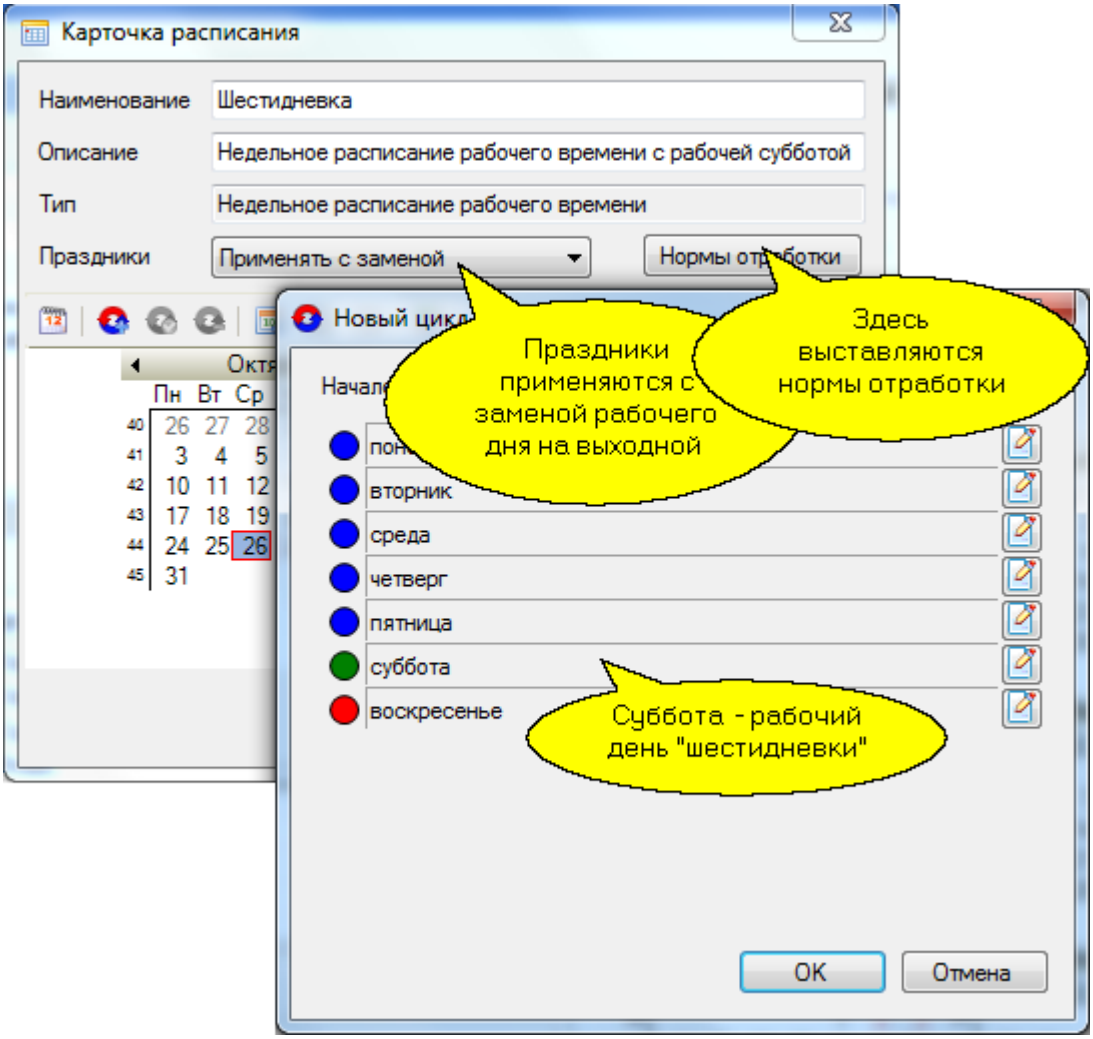


Процедуру назначения скорректированных интервалов времени понедельника на оставшиеся дни недели до пятницы повторяем описанным выше образом.

Допустим, поскольку мы рассматриваем "шестидневку", что в субботу у нас укороченный на час рабочий день. Для такой ситуации мы редактируем субботу отдельно, установив время доступа на территорию с 8:30 до 17:30, интервал обязательного рабочего времени с 09:00 до 17:00, перерыв (обед) с 13:00 до 14:00.

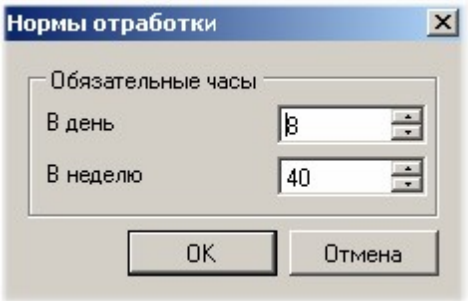


В итоге получаем следующее недельное расписание "шестидневки".



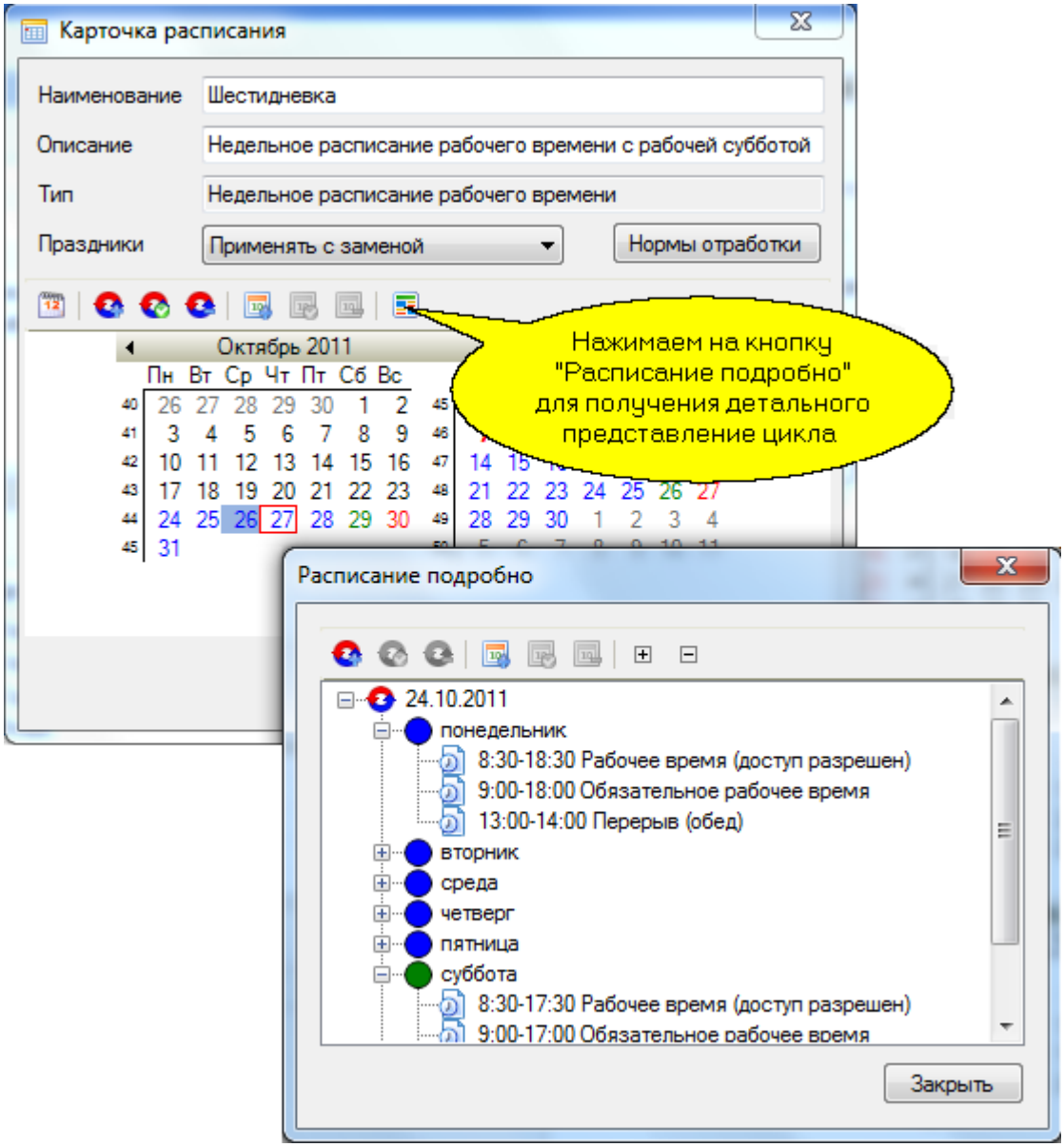
После настройки всех дней нажмите на кнопку *OK* в окне *Новый цикл*.

В карточке расписания выберите правило учета праздников - для недельного расписания используется "Применять с заменой" (см. рис. выше).
В окне, открывающемся при нажатии на кнопку *Нормы отработки* опишите правила обязательной отработки за день и за неделю. При этом, если заданы такие правила, то допустимое рабочее время каждый день, как правило, увеличивают, чтобы можно было, например, один день отработать 4 часа, а потом в другие дни компенсировать это отработкой по 9 часов с тем, чтобы недельная норма была выполнена.



Норма отработки: Указываются обязательные часы отработки в день и в неделю.

Нажатием на кнопку *Расписание подробно*, получаем детальное представление цикла недельного расписания "шестидневки".



Нажмите на кнопку *ОК* в окне *Карточка расписания*.

Недельное расписание рабочего времени готово и отобразится в списке расписаний.

Различие между сменными и недельными расписаниями рабочего времени заключается в том, что в недельном расписании назначен недельный цикл – с понедельника по воскресенье, здесь нет возможности добавлять или удалять дни.

Удобство применения сменных расписаний рабочего времени в том, что, на их основе, возможна реализация самых различных графиков работ сотрудников – "сутки-двое", "день-через-день" и т.д.

См. также:

- Недельное расписание доступа[216]
- Сменное расписание доступа[219]
- Сменное расписание рабочего времени[231]
- Праздничные дни[238]
- Дни исключений[241]

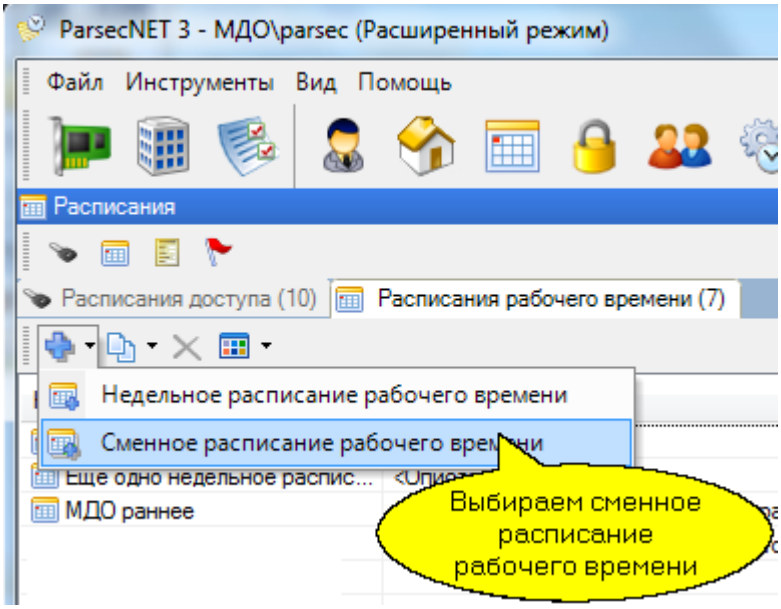
Копии ранее созданных расписаний[243]

8.5.3.2 Сменное расписание рабочего времени

Описанные ниже действия предназначены для создания сменного расписания, которое будет использоваться для учета рабочего времени инструментом "Бизнес-отчеты (версия 4)". Предыдущая версия этого инструмента больше не поддерживается.

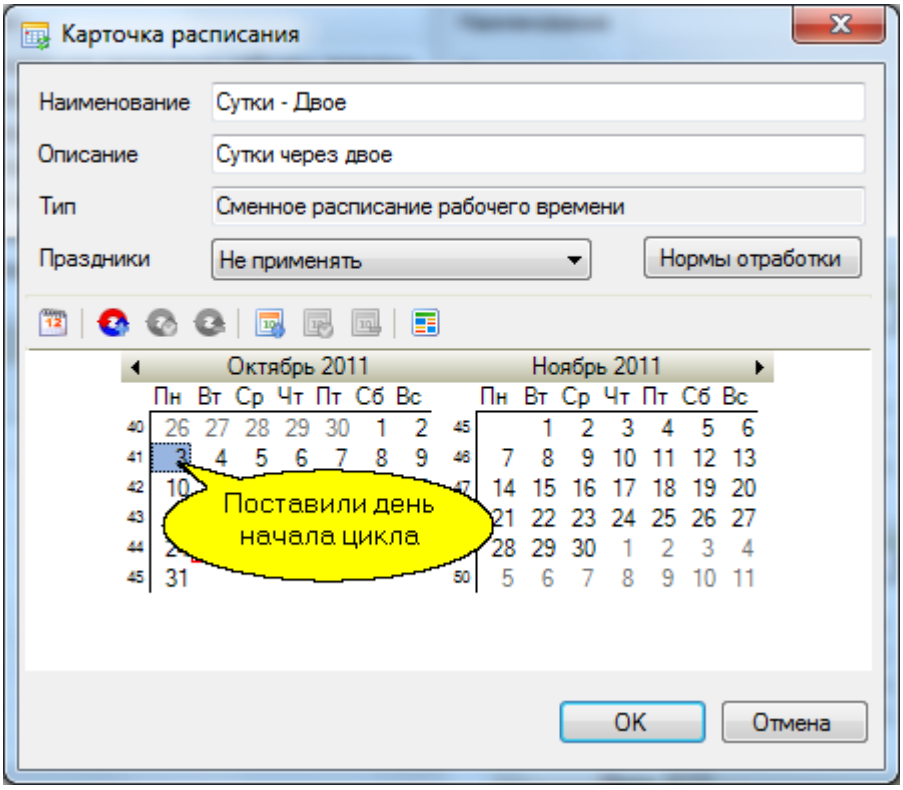
Создание сменного расписания рабочего времени

Перейдите на вкладку *Расписание рабочего времени* и в раскрывающемся списке кнопки *Добавить* выберите "Сменное расписание рабочего времени":

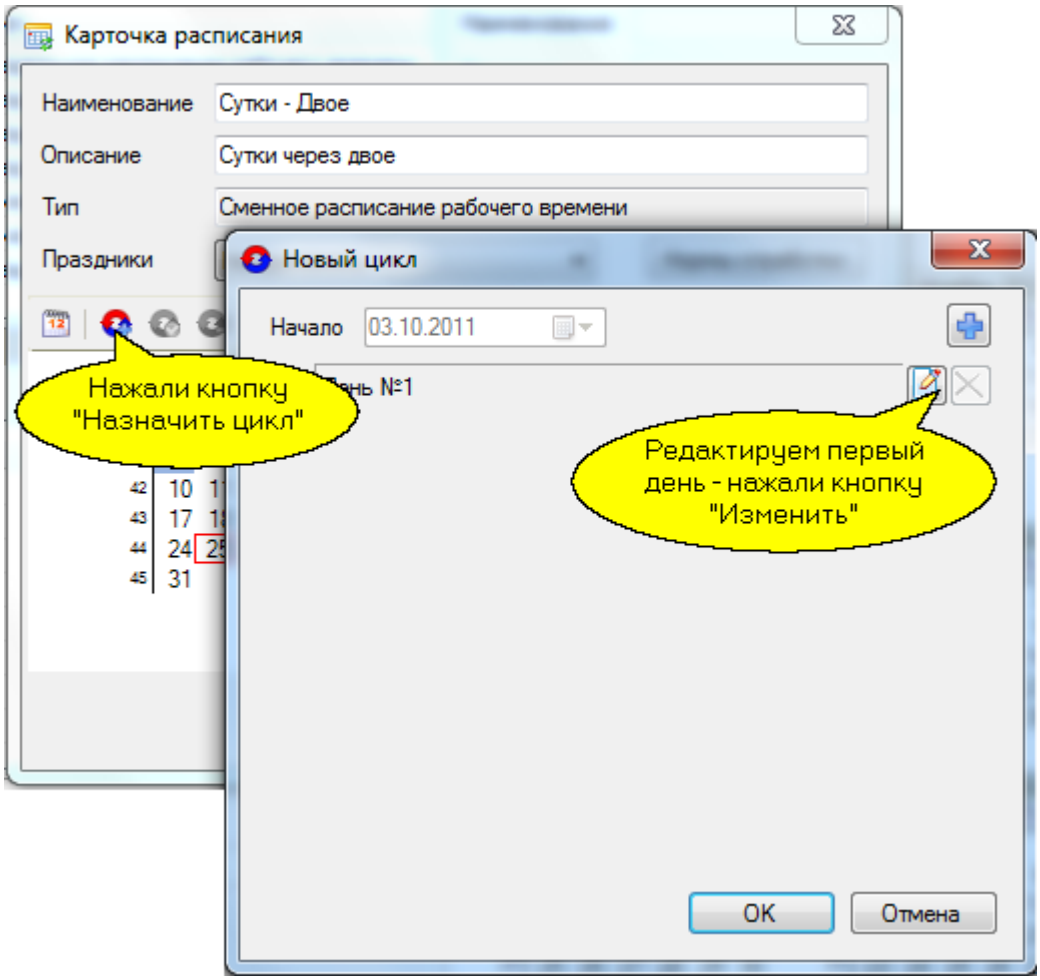


Откроется новое окно *Карточка расписания*. В поле *Название* введите название расписания. В поле *Описание* введите описание расписания (данное поле заполняется по желанию). Щёлкните по дате в календаре, с которой Вы хотите начать цикл.

Обратите внимание, по-умолчанию для этого расписания уже заданы временные интервалы. Это расписание начинается в понедельник текущей недели. Чтобы создать полностью свое расписание, нужно удалить автоматически созданные циклы и интервалы. Для этого нажмите на кнопку  ***(Удалить цикл).***



Нажмите на кнопку *Назначить цикл*. Откроется окно *Новый цикл*. Перейдите к первому дню и нажмите на кнопку *Изменить*.



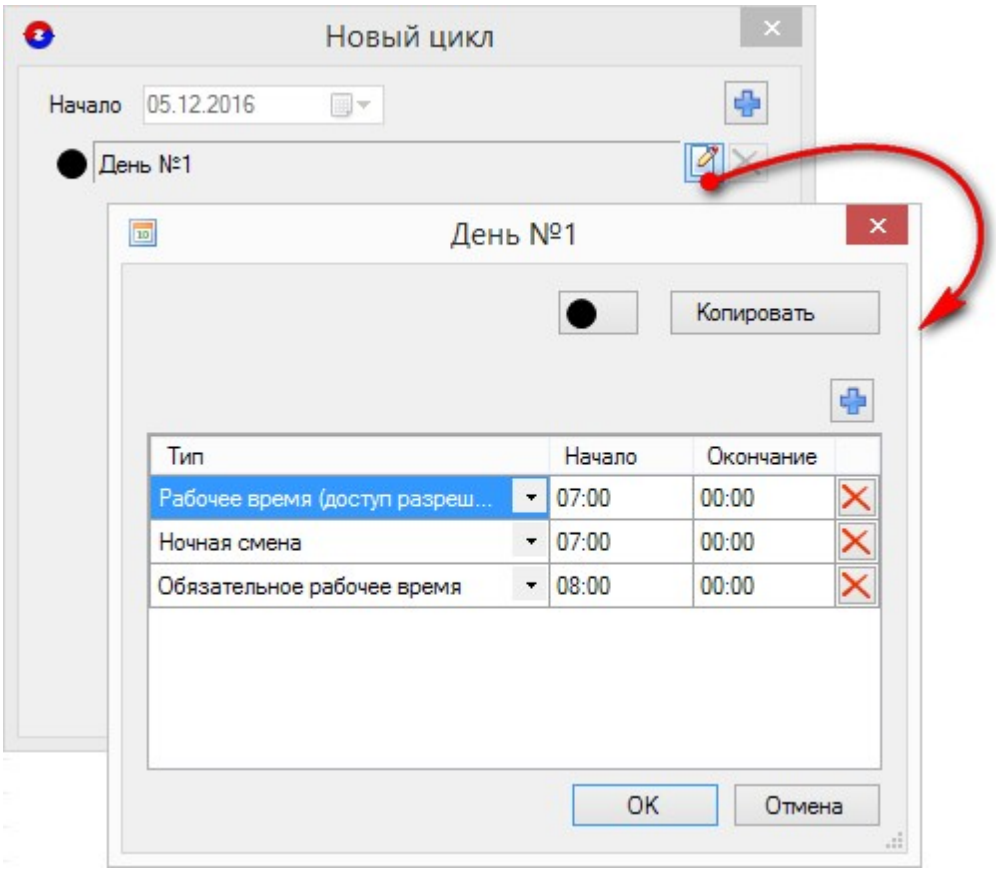
Откроется окно *День №1*. Здесь необходимо определить интервалы – выбрать тип и указать время начала и конца. Можно выбрать цветовую гамму для дня. Воспользуйтесь кнопкой

Копировать. Она открывает доступ к системным шаблонам дней: "Полные сутки", "Рабочий день", "Выходной день". Также, если создано несколько дней, Вы можете скопировать их.

Мы начинаем цикл с дня, в который пользователь заступает на смену, при этом считаем, что смена продолжается, например, с 08:00 до 08:00.

В первый день назначаем следующие интервалы:

- "Рабочее время (доступ разрешен)" с 07:00 до 00:00 - интервал доступа, по которому считается отработанное время (даём часовой запас для прихода на работу);
- "Ночная смена" с 07:00 до 00:00 - признак ночной смены;
- "Обязательное рабочее время" с 08:00 до 00:00 - период, относительно которого будут считаться опоздания, уходы раньше времени и другие отклонения.

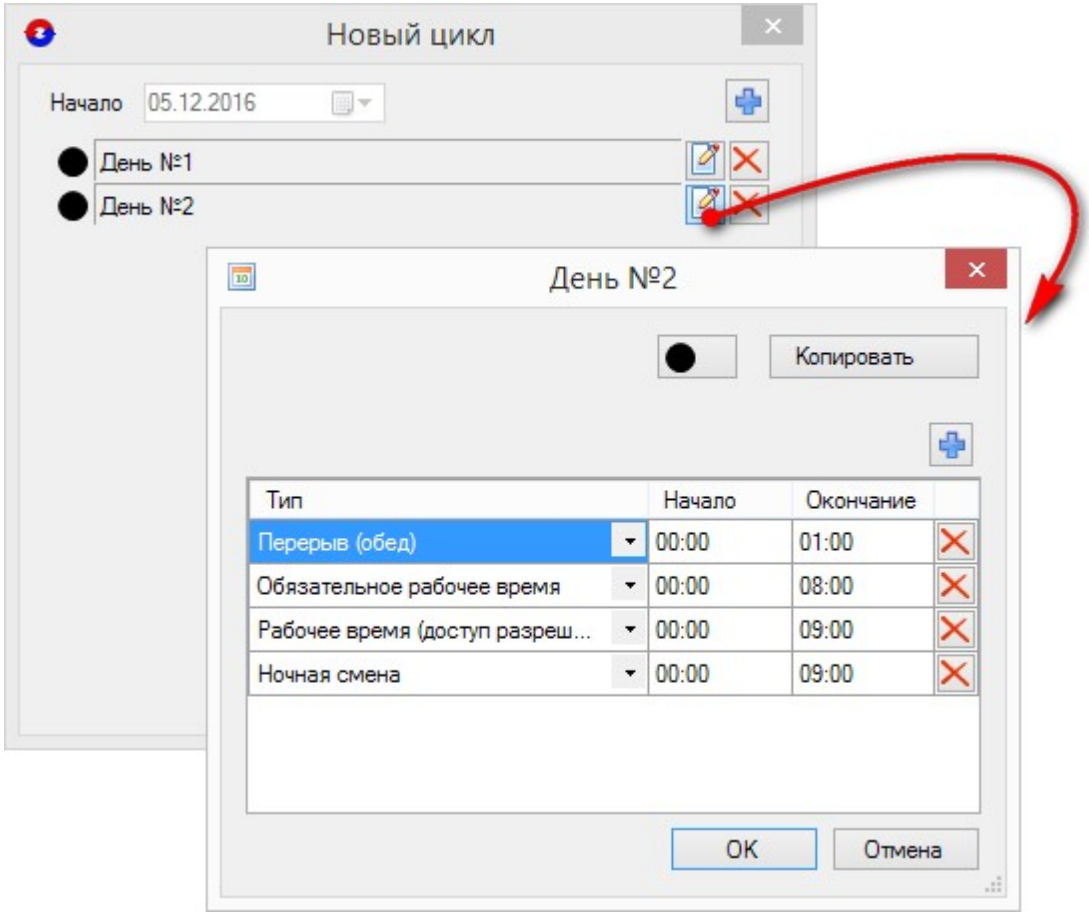


После настройки всех необходимых интервалов нажмите на кнопку *OK*, завершая, тем самым, настройку первого дня цикла сменного расписания рабочего времени "Сутки через двое".

Далее процедура настройки повторяется для каждого дня смены. Нажмите на кнопку *(Добавить)* в окне *Новый цикл* и к циклу добавится новый день (таким образом можно добавить нужное количество дней для Вашего цикла). После добавления дней в новый цикл их можно настраивать в любом порядке, но лучше делать это последовательно.

Второй день начинается с полуночи и заканчивается в 08:00, но можно дать часовой запас для ухода с работы, то есть поставить 09:00. Добавьте второй день с интервалами:

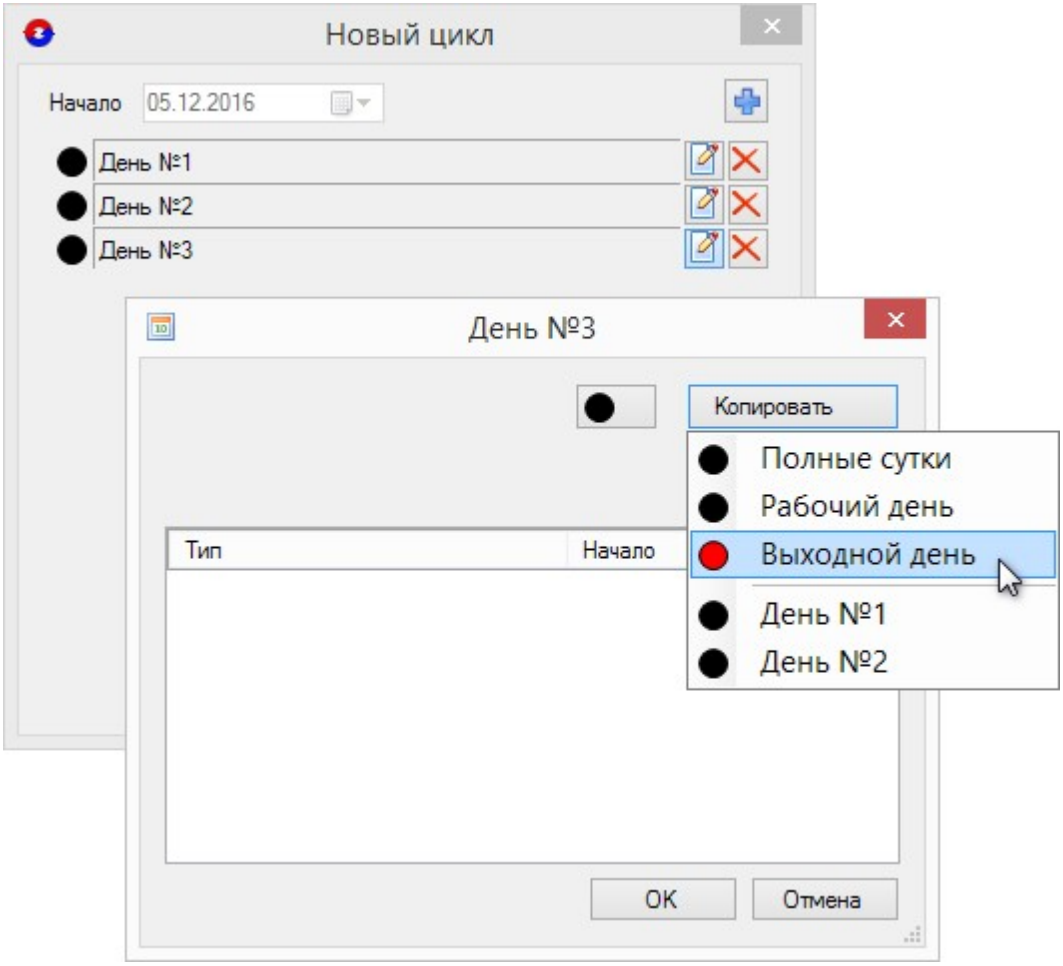
- "Рабочее время (доступ разрешен) с 00:00 до 09:00 - интервал доступа, по которому считается отработанное время (даём часовой запас для ухода с работы);
- "Ночная смена" с 00:00 до 09:00 - признак ночной смены;
- "Обязательное рабочее время" с 00:00 до 08:00 - период, относительно которого будут считаться опоздания, уходы раньше времени и другие отклонения;
- "Перерыв (обед)" с 00:00 до 01:00.



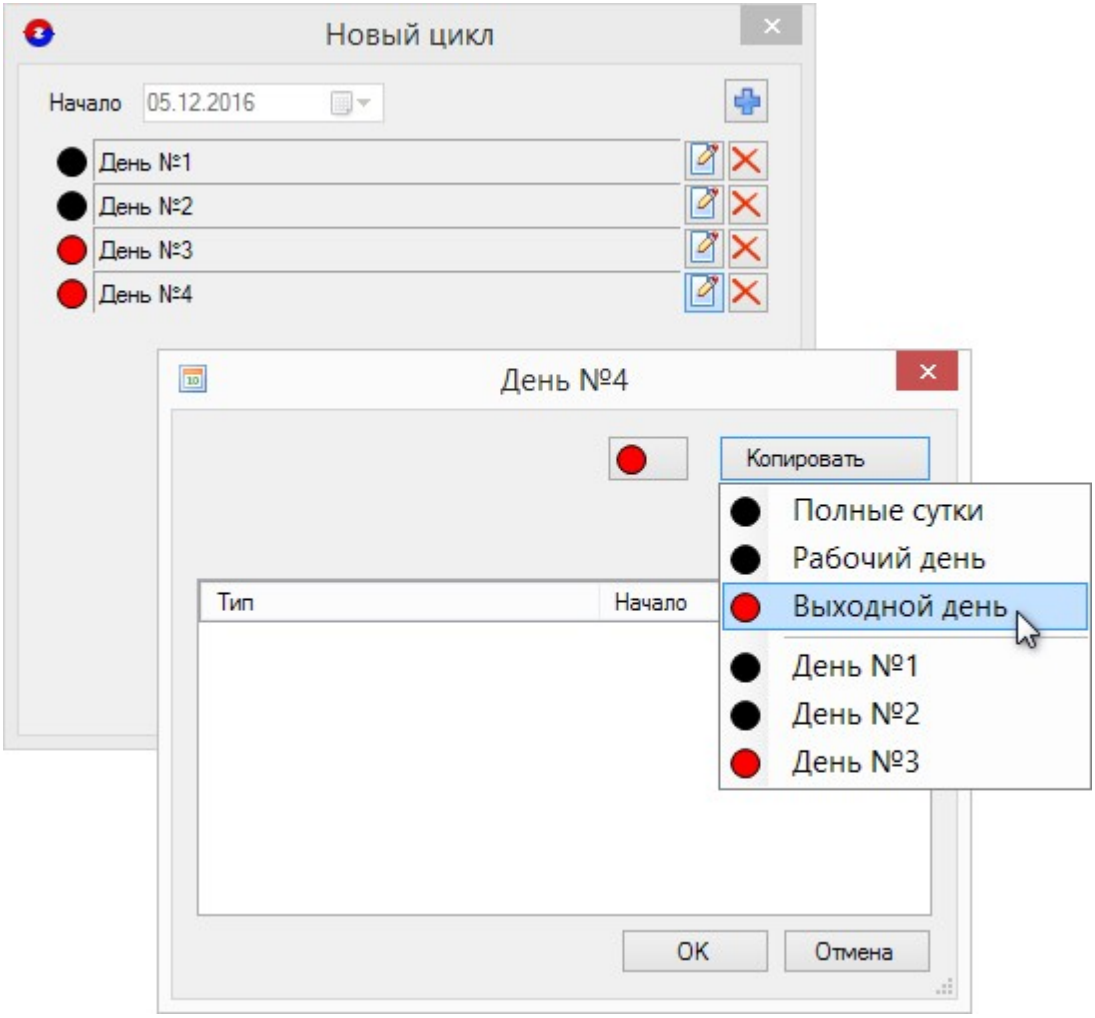
После настройки второго дня нажмите на кнопку *OK*.

Теперь добавьте третий день, который будет целиком выходным. Обратите внимание, признаком выходного дня является отстутствие интервала "Обязательное рабочее время".

Однако, в выходной день можно назначить интервал "Рабочее время (доступ разрешен)" и тогда сверхурочно отработанные часы зачтутся работнику.



Затем добавьте четвёртый день, который также будет целиком выходным, и расписание готово.



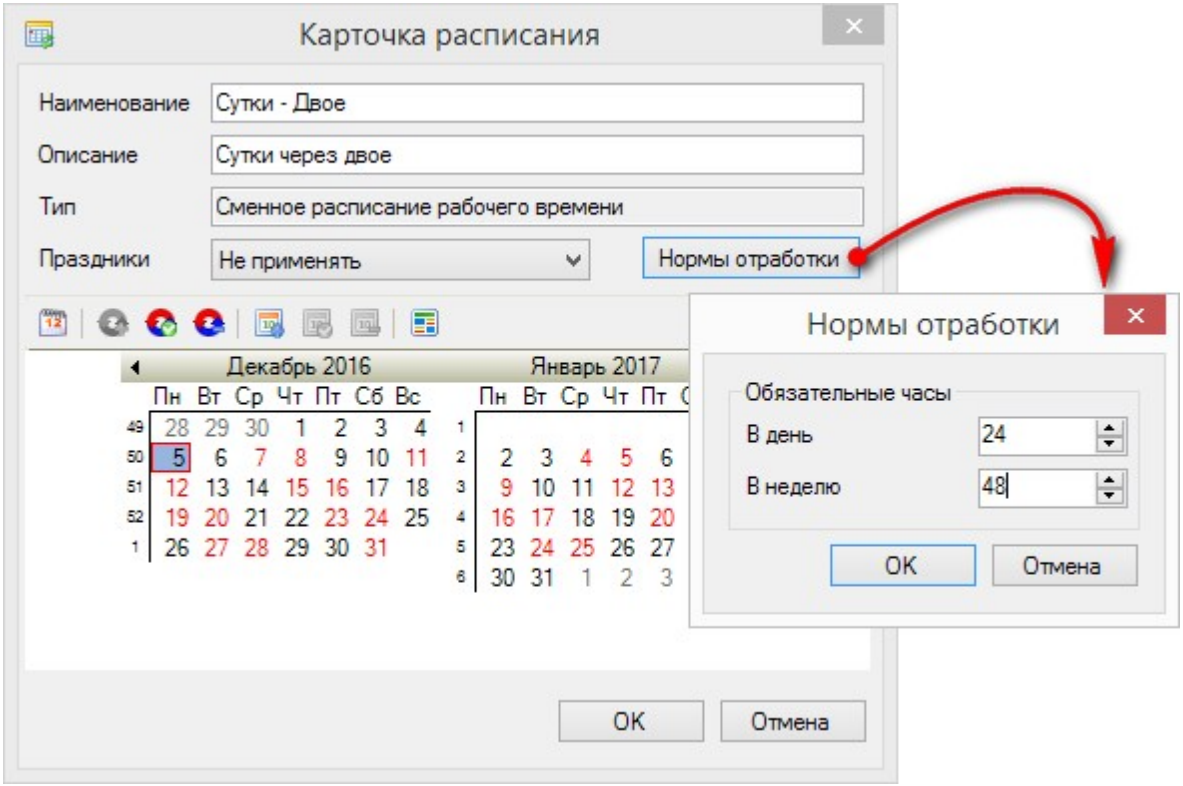
Таким образом, пользователь начинает работать с 8 утра в понедельник 5 декабря, 6 декабря, во вторник, в 8 утра заканчивает работу, затем до 8 утра в среду, 7 декабря, у него первые сутки отдыха, а до 8 утра четверга, 8 декабря - вторые сутки отдыха, после чего он опять заступает на смену в пятницу, 8 декабря.

То есть, "День №1" и "День №2" вместе составляют полные сутки, а "День №3" и "День №4" – выходные.

После настройки всех дней нажмите на кнопку *OK* в окне *Новый цикл*.

Праздники: к сменным расписаниям обычно праздники не применяются.

Норма отработки: указываются количество обязательных часов отработки в день и в неделю. Для сменного расписания, скорее всего, количество отработанных часов будет разным от недели к неделе, поэтому можно указать минимальное обязательное количество часов отработки.



Закончив создание расписания, нажмите на кнопку *ОК* в окне *Карточка расписания*. Сменное расписание рабочего времени готово и отобразится в списке расписаний.

Как и недельное расписание, сменное расписание УРВ никак не влияет на проход субъектов доступа на территорию, а используется только для подсчета отработанного времени в Модуле учета рабочего времени[456].

См. также:

- Недельное расписание доступа[216]
- Сменное расписание доступа[219]
- Недельное расписание рабочего времени[223]
- Праздничные дни[238]
- Дни исключений[241]
- Копии ранее созданных расписаний[243]

8.5.3.3 Присвоение расписания рабочего времени подразделению или сотруднику

Присвоение расписания необходимо для того, чтобы определить отработанное время с учётом правил его подсчёта.

Для присвоения расписания необходимо зайти в Редактор персонала[255].

Необходимо помнить, что подразделения и сотрудники должны быть уже созданы.

Присвоение расписания подразделению:

- В дереве подразделений выберите нужное подразделение;
- Перейти в карточку подразделения;
- Нажмите на кнопку *Изменить*, область подразделения перейдет в режим редактирования;
- В строке расписания нажмите на кнопку *Выбрать*. Откроется диалоговое окно *Список расписаний*;
- Выберите нужное расписание, затем нажмите на кнопку *Выбрать*;
- Нажмите на кнопку *Сохранить*.

В итоге, добавленное расписание сохраняется и отображается в области просмотра.

После назначения подразделению расписания сотрудник, принадлежащий к данному подразделению, наследует расписание подразделения, если у него явно не определено другое конкретное расписание.

Присвоение расписания сотруднику:

- В дереве подразделений выберите нужное подразделение;
- В области *Состав подразделения* выберите сотрудника;
- Перейдите в карточку сотрудника, нажмите на кнопку *Изменить*, карточка перейдёт в режим редактирования;
- Перейдите в закладку *Расписание*, нажмите на кнопку *Выбрать*. Откроется диалоговое окно *Список расписаний*.
- Выберите нужное расписание и нажмите на кнопку *Выбрать*;
- Нажмите на кнопку *Сохранить*.

Добавленное расписание отображается в области просмотра.

Если сотрудник унаследовал расписание от подразделения, то при изменении расписания у сотрудника, подразделение не наследует назначенное расписание. Каждый сотрудник может работать по индивидуальному расписанию.

8.5.4 Создание праздников

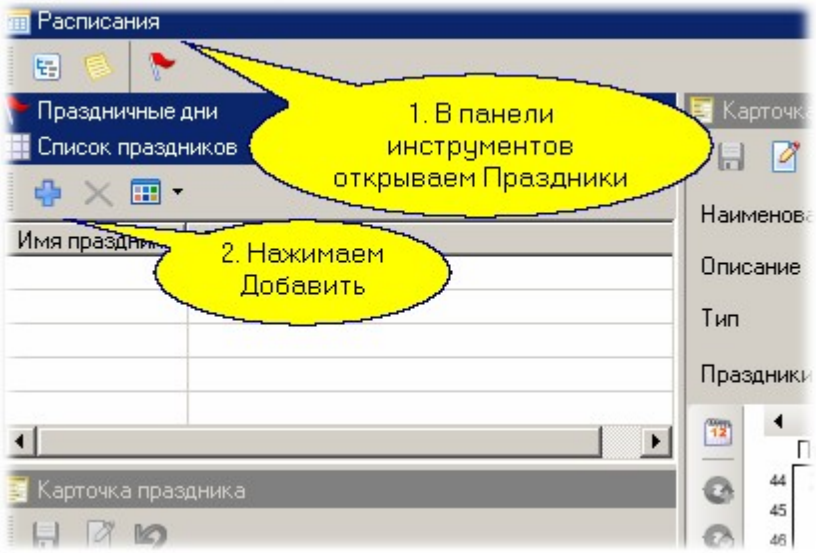
Если вы хотите аккуратно организовать доступ на территорию или подсчитывать отработанное время (учет рабочего времени), то необходимо ввести таблицу праздников с тем, чтобы система могла их учитывать в своей работе.

С точки зрения доступа праздник приравнивается к воскресенью, и контроллеры сами при наступлении праздничного дня автоматически будут работать по расписанию воскресного дня.

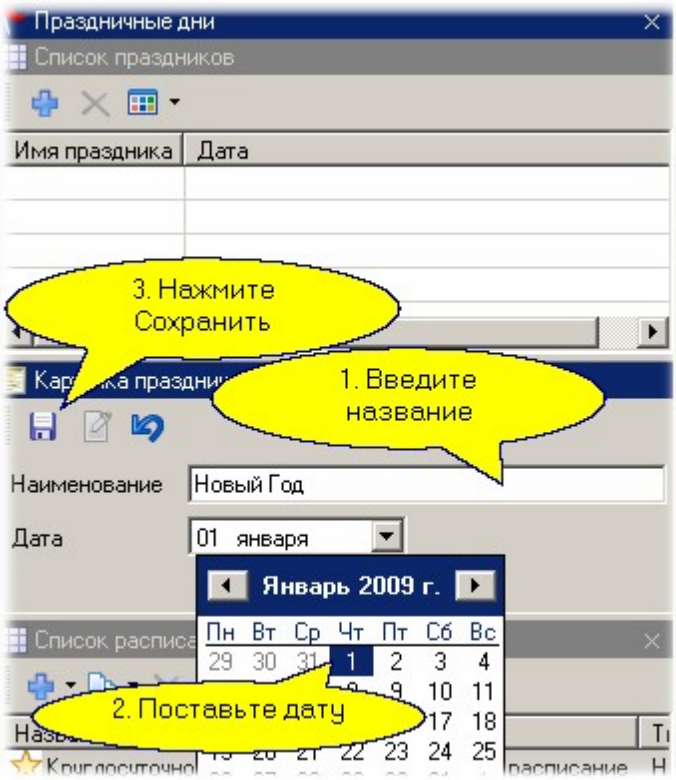
Т.е. если в расписании на воскресенье разрешен доступ, то и в выходной день доступ будет разрешен в то же время.

1. ***В недельных расписаниях доступа праздники всегда применяются и всегда с заменой (исключение - Круглосуточное системное расписание).***
2. ***В сменных расписаниях доступа праздники применяются в соответствии с настройкой для каждого из расписаний. Варианты использования дней-исключений для сменного расписания доступа:***
   - ***Не применять;***
   - ***Применять с заменой;***
   - ***Применять со вставкой.***
3. ***К "Круглосуточному системному расписанию" праздники никогда не применяются.***

Для добавления праздника необходимо открыть панель праздников, как показано ниже:



После нажатия на кнопку *Добавить* в карточке праздника надо ввести его название и назначить дату:



Повторите эту последовательность действий для всех остальных праздников на текущий год.

См. также:

- Недельное расписание доступа[216]
- Сменное расписание доступа[219]
- Расписание рабочего времени[221]
- Дни исключений[241]
- Копии ранее созданных расписаний[243]

8.5.5 Дни-исключения

Понятие исключительного дня позволяет задать нестандартный день в цикле любого расписания. Примером исключительного дня может служить рабочий день в воскресенье при переносе выходного из-за праздников.

Пример применения исключительных дней

Например, 23 февраля 2017 года - четверг. Чтобы получить три дня выходных подряд, воскресенье делается рабочим днем, а пятница выходным вместо воскресенья. Таким образом, получаем три выходных подряд: праздничный день 23 февраля, пятницу 24 февраля и субботу 25 февраля. Соответственно, воскресенье 26 февраля становится рабочим днем.

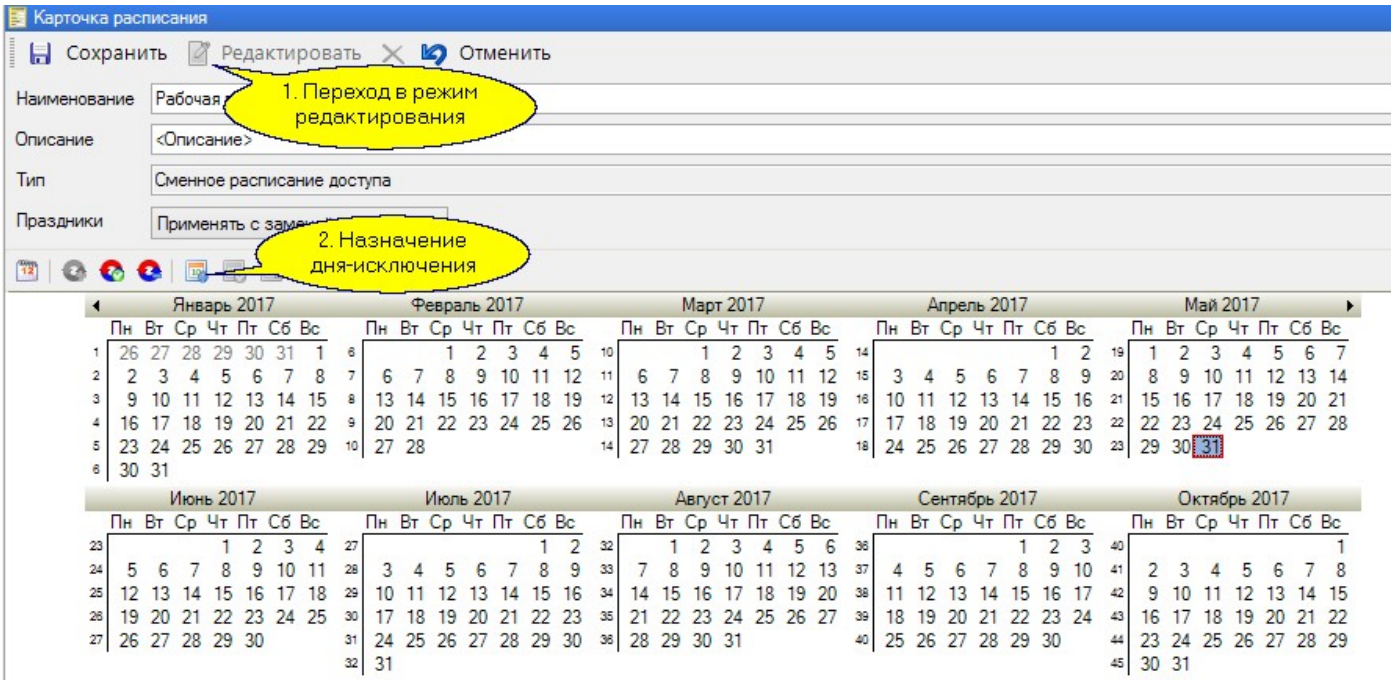


недельном расписании дост упа назначит ь день-исключение нельзя.

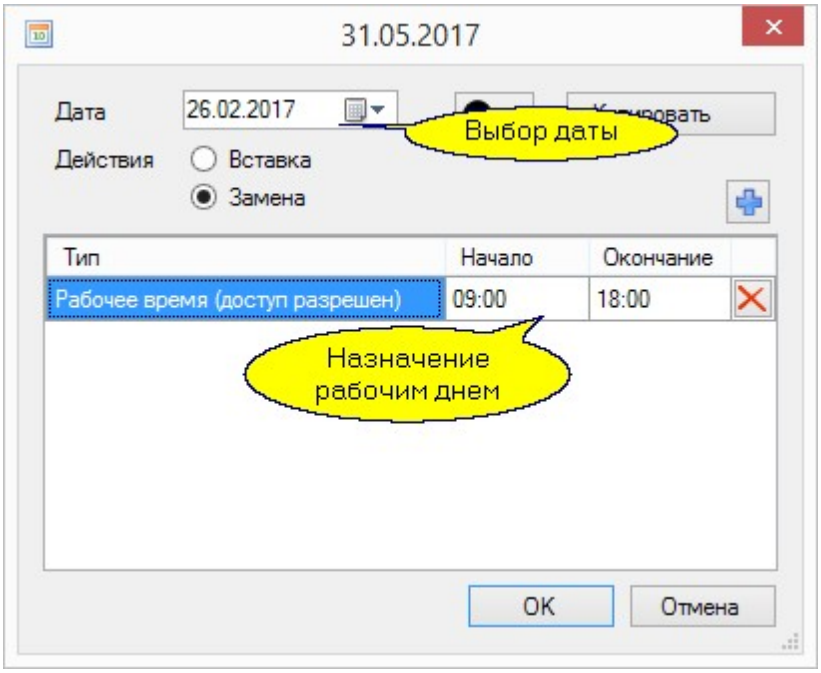
Внесение исключительных дней в расписание

Внесём рассмотренный выше пример исключительного дня в сменное расписание доступа.

Выберите в списке расписаний сменное расписание и перейдите в режим редактирования:



При назначении исключительного дня надо указать дату и назначить тип дня. В нашем примере, субботу 3 июня назначаем рабочим днем:



Пятницу 24 февраля назначаем выходным днем, удалив строку "Рабочее время (доступ разрешен)". Теперь наше расписание максимально соответствует действительности нашего примера.

- ***Для расписаний доступа надо знать, какие из контроллеров[696] поддерживают исключительные дни. Если ваши контроллеры их не поддерживают, то нет смысла вводить исключения в расписания доступа.***
- ***В учете рабочего времени исключительные дни обеспечивают формирование корректных отчетов об отработанном времени.***

См. также:

Недельное расписание доступа[216]

Сменное расписание доступа[219]

Расписание рабочего времени[221]

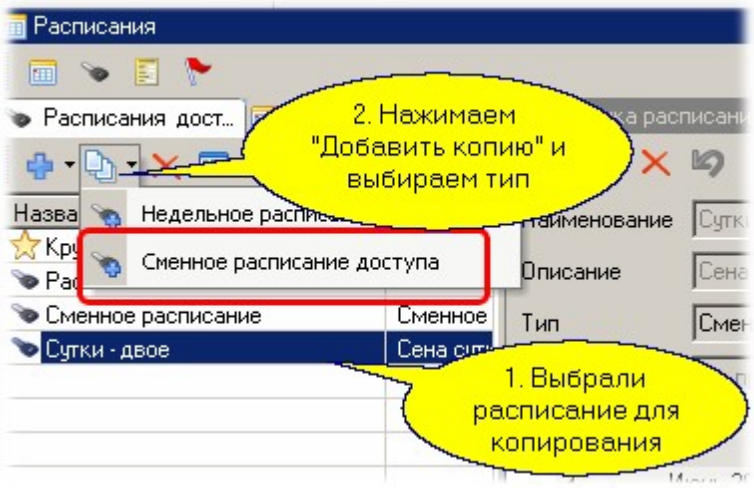
Праздничные дни[238]

Копии ранее созданных расписаний[243]

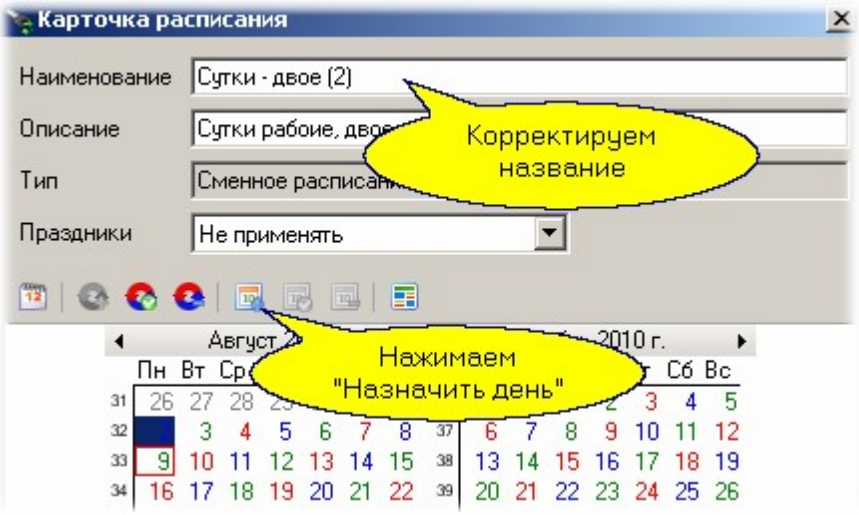
8.5.6 Создание расписания из копии

При создании сменных расписаний (типа сутки - через - двое и аналогичных) необходимо создать расписание для каждой смены. Чтобы не создавать расписание каждой смены заново воспользуемся возможностью копирования расписаний.

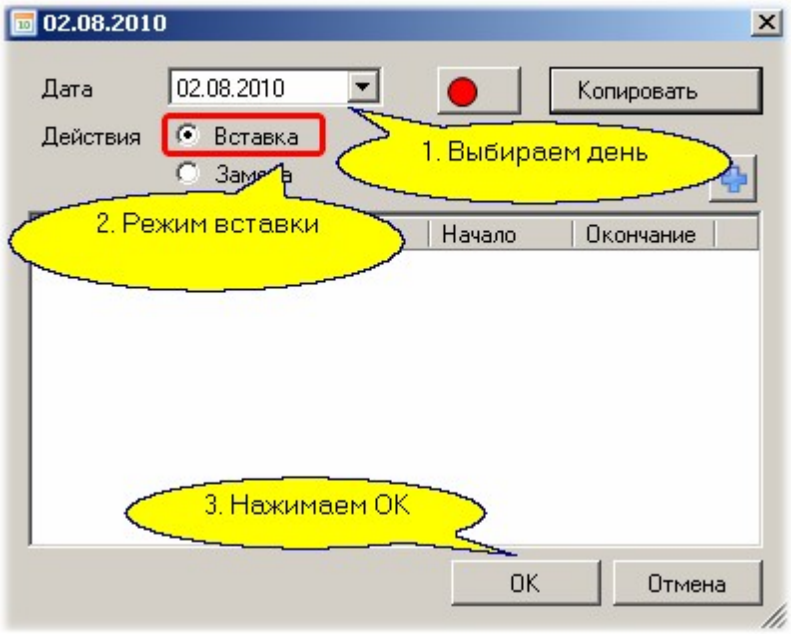
У нас было создано расписание для одной смены. сделаем из него копию и отредактируем как нам требуется:



Корректируем название расписания. У нас смена начиналась 2 августа. Для второй смены надо сдвинуть начало цикла на один день, для чего на 2 августа просто вставляем день:



В диалоге назначения дня ставим число, на которое вставляется лишний день, выбираем режим вставки и нажимаем ОК. Задавать интервалы на этот день нет необходимости, так как его назначение - просто сдвинуть расписание, что вы и увидите после нажатия ОК.



Теперь таким же образом можно сделать расписания на остальные дни смены.

См. также:

- Недельное расписание доступа[216]
- Сменное расписание доступа[219]
- Расписание рабочего времени[221]
- Праздничные дни[238]
- Дни исключений[241]

8.6 Редактор групп доступа

Группа доступа – это совокупность групп компонент (например, дверей) с назначенными им расписаниями и привилегиями. Созданные группы доступа будут назначаться субъектам доступа. На текущий момент система поддерживает четыре типа групп доступа в соответствии с их назначением:

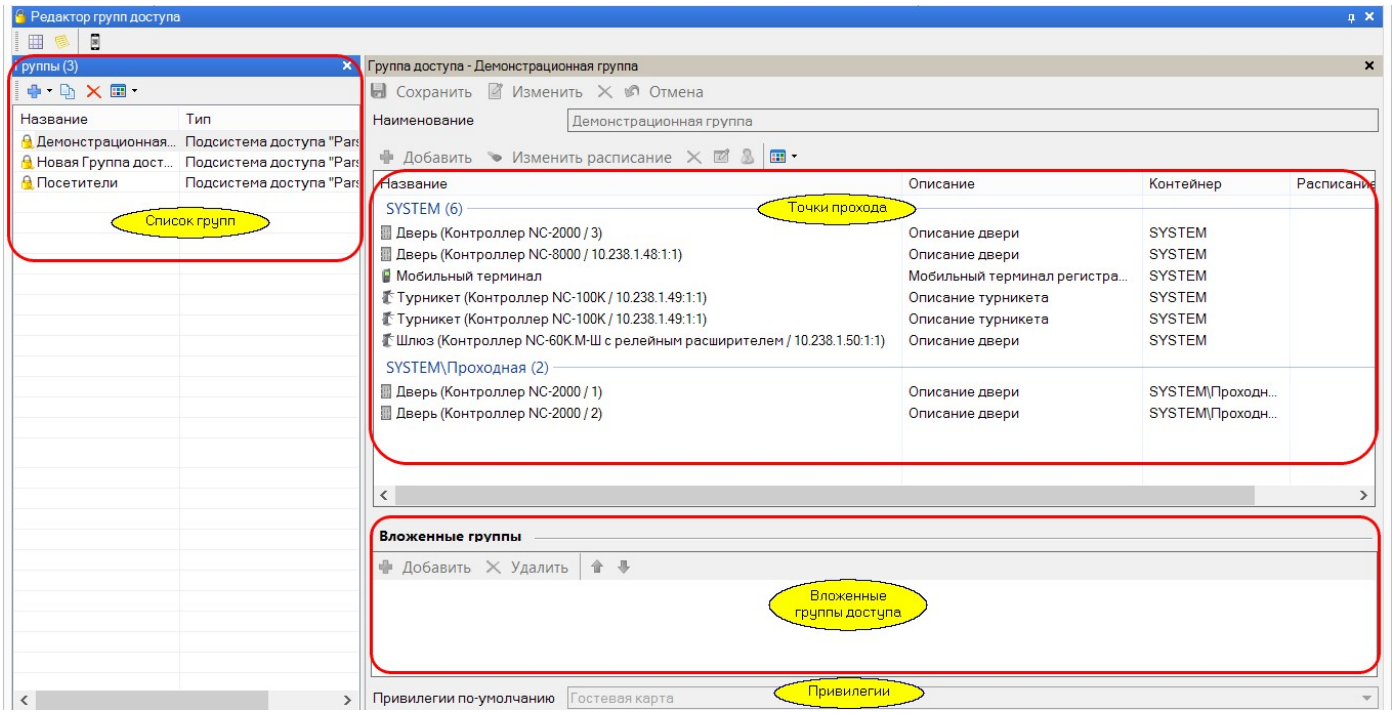
- Группа доступа для охранно-пожарной системы Стрелец;
- Группа доступа для охранной подсистемы Parsec;
- Группа доступа для подсистемы доступа Parsec;
- Группа доступа для автомобильных номеров.

Редактор групп доступа предназначен для создания и изменения групп доступа, которые определяют для субъектов доступа права на проход на территорию в определенное время. Дать пользователю права доступа на территорию можно только через назначение ему определенной группы доступа, созданной заранее.

Группы доступа типизированы, т.е. при создании субъекта доступа того или иного типа назначить ему можно только группу доступа соответствующего типа. Это связано с тем, что для пользования разными подсистемами требуется различный набор параметров.

Панели редактора групп доступа

Редактор групп доступа имеет всего две панели, поскольку группы доступа не образуют иерархий. Левая панель показывает список имеющихся в данной организации групп доступа, а правая панель (карточка группы) позволяет просматривать и редактировать свойства группы:



Карточка группы, в свою очередь, состоит из трех панелей:

- на первой отображаются основные свойства группы: точки прохода, входящие в группу, и расписания доступа через эти точки;
- на второй - вложенные группы, параметры которых "наследуются" выбранной на левой панели группой;
- третья позволяет выбрать привилегии для членов группы.

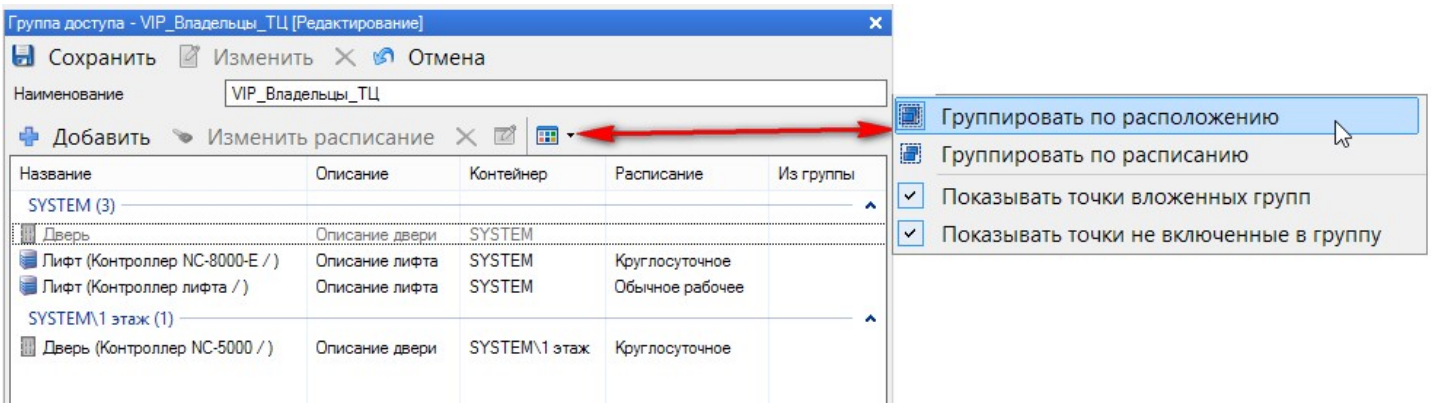
В карточке группы доступа можно добавить точки доступа и соответствующие им расписания для сложной группы[253], когда в разные помещения доступ будет разрешен по разным расписаниям.

Табличная часть панели точек доступа содержит следующие колонки:

- "Название" и "Описание" - колонки редактируются в карточке устройства в редакторе оборудования;
- "Расписание" - отображает расписание, по которому работает точка прохода;
- "Контейнер" - папка в редакторе топологии, в которой содержится данная точка прохода. Другими словами, это территория, доступ на которую защищает данная точка прохода;
- "Из группы" - показывает, из какой вложенной группы унаследовано правило доступа.

Кнопка "Список" на первой панели карточки группы доступа раскрывает список следующий команд:

- Группировать по расположению - в одну категорию объединяются точки доступа, расположенные в одной и той же папке топологии;
- Группировать по расписанию - в одну категорию объединяются точки доступа, работающие по одному и тому же расписанию;
- Показывать точки вложенных групп - управление отображением точек доступа групп, вложенных в текущую группу доступа;
- Показывать точки, не включенные в группу - управление отображением точек доступа, не входящих в текущую группу доступа (отображаются серым).



См. также:

Группы доступа[247]

Расписания[213]

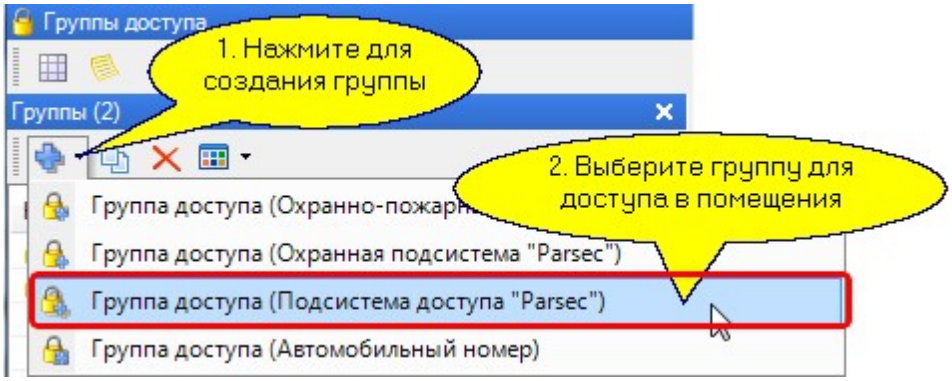
Создание сложных групп доступа[253]

Расширенные QR-коды[253]

8.6.1 Создание группы доступа

Чтобы создать группу доступа, выполните следующие действия:

- Нажмите на панели инструментов редактора групп доступа на кнопку *Добавить*, в раскрывшемся списке выберите тип группы доступа:

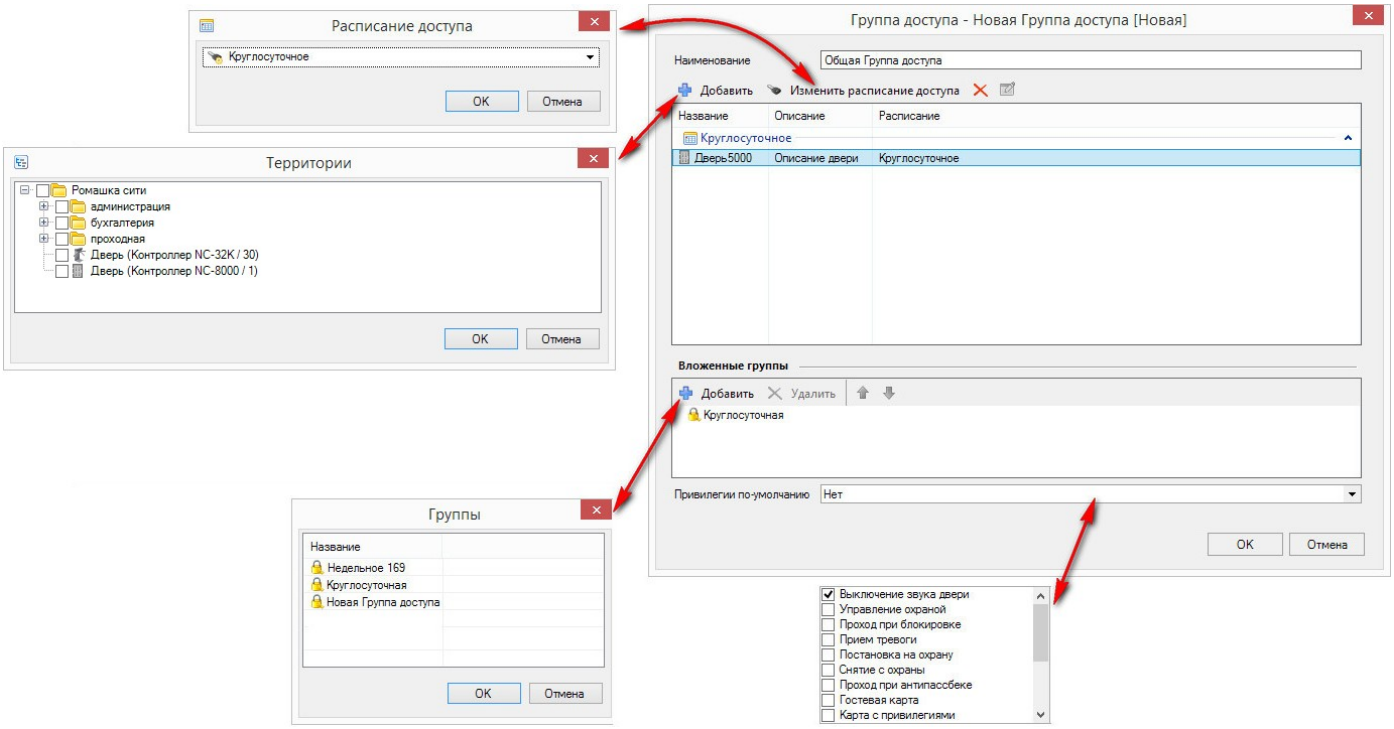


- В карточке новой группы доступа введите название;
- Нажав на кнопку *Добавить*, укажите точки прохода (двери, в которые персонал данной группы сможет ходить);
- При необходимости измените установленное выбранное по умолчанию расписание доступа;
- При необходимости в разделе *Вложенные группы* укажите группу, правила которой будут действовать одновременно с создаваемой новой группой. Например, группа "Общая Группа доступа" (рисунок ниже) обеспечивает доступ в офис организации в здании бизнес-центра. Тогда во вложенные нужно будет добавить группу доступа в здание БЦ, например, *Круглосуточная*. В случае конфликтов параметров групп (например, расписаний), приоритет определяется следующим образом:
  - высший приоритет - текущая группа (в примере это "Общая Группа доступа");
  - самая верхняя в списке вложенных групп (в поле *Вложенные группы*);
  - ...
  - самая нижняя в списке вложенных групп.

  При добавлении вложенной группы, в текущую группу добавляются правила только этой вкладываемой группы. Если такая вложенная группа, в свою очередь, тоже имеет вложенные группы, то правила последних НЕ копируются в текущую группу.

  В нашем примере, "Общая Группа доступа" будет наследовать правила вложенной группы "Круглосуточная". Но если у группы "Круглосуточная" есть какие-то свои вложенные группы, то их правила будут наследоваться только ею, но не группой "Общая Группа доступа".

- В нижней части карточки добавьте, при необходимости, привилегии.



После сохранения созданной группы доступа кнопкой *OK* ее можно назначать субъектам доступа.

Копирование группы доступа

Для облегчения создания групп доступа, незначительно отличающихся друг от друга, рекомендуется использовать функцию копирования. Для этого выделите нужную группу доступа, нажмите на кнопку  , внесите необходимые изменения и сохраните новую группу доступа.

См. также:

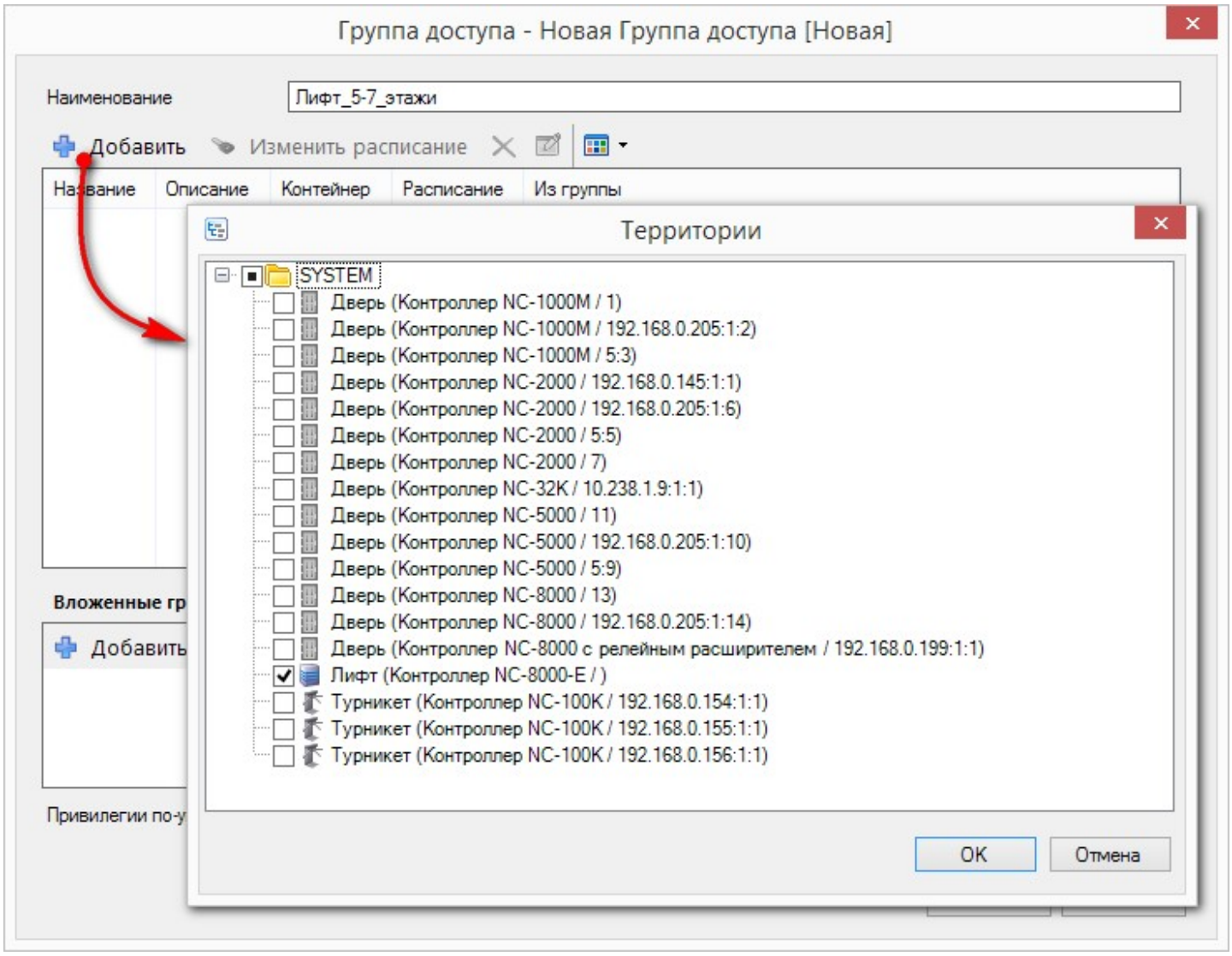
Редактор персонала[255]

Редактор расписаний[213]

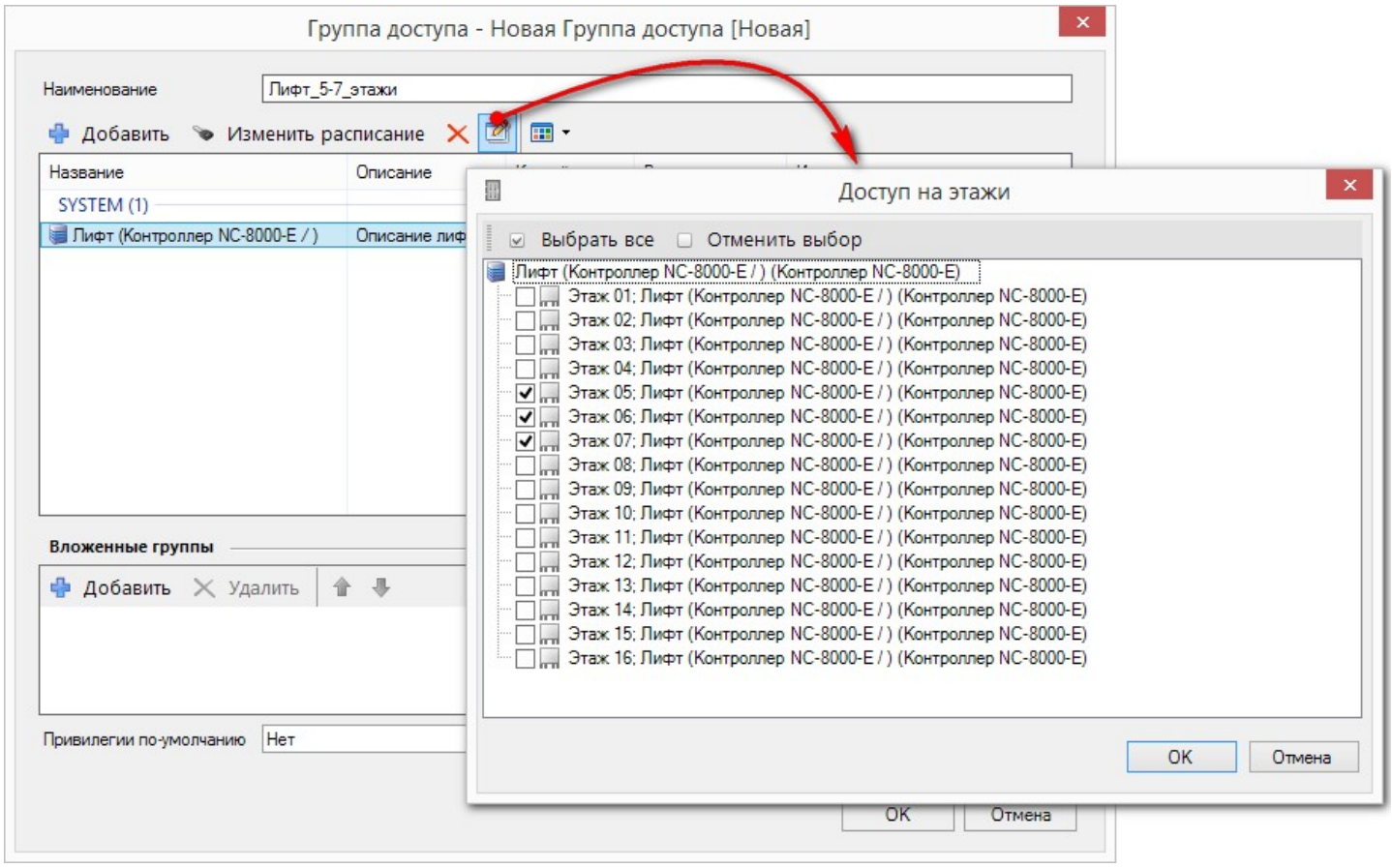
8.6.1.1 Особенности лифтового контроллера

Чтобы предоставить пользователям право доступа на определенные этажи, необходимо создать отдельную группу доступа.

При выборе территории укажите лифтовый контроллер:



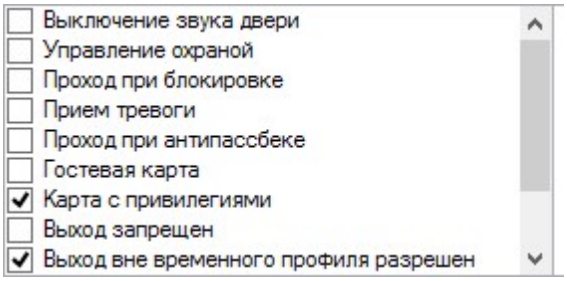
После добавления точки прохода "Лифт" выделите ее и нажмите на кнопку *Настройка*. В раскрывшемся списке удалите флажки у всех этажей, на которые доступ для данной группы запрещен (по умолчанию все флажки проставлены):



Теперь эта группа может использоваться как отдельная группа доступа или в качестве вложенной группы доступа для для других групп.

8.6.2 Привилегии

Обратите внимание, что назначенные группе доступа привилегии предоставляются всем субъектам, приписываемым к этой группе доступа. При этом при создании новой персоны у нее присутствуют только привилегии, который определены для группы доступа. Но любому субъекту доступа можно назначить любые привилегии, которые существуют в системе и поддерживаются контроллерами. Диалог выбора привилегий показан на рисунке ниже. Флажками отмечены привилегии, характерные только для контроллеров NC-100K-IP, предназначенных для обслуживания турникетов на проходных.



Привилегии и поддерживающие их контроллеры описаны ниже:

- "Выключение звука двери" - позволяет поднесением ключа к считывателю выключить звуковой сигнал незакрытой двери;
- "Управление охраной" - позволяет ставить помещение на охрану и снимать с охраны для всех контроллеров, кроме NC-100K-IP. Для контроллеров NC-2000xx, NC-8000xx и NC-32K.M позволяет пользователю отключать абсолютную блокировку в режиме offline;

- "Проход при блокировке" - обеспечивает доступ в помещение при включенной аппаратной блокировке или относительной блокировке, установленной с ПК. Преодоление абсолютной блокировки обеспечивается только в режим offline, при этом абсолютная блокировка не отменяется;
- "Прием тревоги" - позволяет снимать локальный сигнал тревоги на охранном контроллере. Привилегия предоставляется не доступному идентификатору, а пин-коду для охранного контроллера;
- "Проход при антипассбэке" - по-умолчанию, при наличии в системе точек прохода с включенным режимом "антипасбэк"-а, все сотрудники не имеют привилегии повторного прохода через эти точки (область). Если в данной строке поставить флажок, то "антипассбэк" на данного сотрудника не распространяется и по его карте возможен многократный вход или выход даже через точки прохода, на которых действует режим "антипассбэк"-а;
- "Гостевая карта" - по данной привилегии контроллер при выходе пользователя дает картоприемнику команду забрать карту;
- "Карта с привилегиями" работает по разному для разных контроллеров:
  - для NC-100K-IP привилегия позволяет пользователю отключать абсолютную блокировку в режиме offline, снимать звук тампера корпуса;
  - для NC-8000 всех модификаций и NC-60K/NC-60K.M привилегия позволяет проходить по одному идентификатору при включенной двухфакторной идентификации.
- "Выход вне временного профиля разрешен" - для контроллеров NC-100K-IP, данная привилегия позволяет преодолеть настройку "Запрет выхода вне расписания";
- "Управление доступом" - открывает точку прохода с помощью идентификатора (карты). Формирует транзакцию "Доступ предоставлен <<имя пользователя>>". Проходы по карте с данной привилегией не учитываются подсистемой УРВ. Также используется для разблокировки идентификатора[283];
- "Не использовать счетчик проходов" - привилегия прекращает подсчет проходов идентификатора (также см. Использовать персональный счетчик проходов[83]);
- "Проход без сопровождения запрещен" - привилегия предназначена для использования со шлюзом с весовой платформой. После того, как "претендент" на проход приложил свою карту к считывателю, проход не будет предоставлен, если сопровождающее его лицо не приложит к считывателю свою карту в течение заданного времени. После прохода посетителя сопровождающий также должен пройти через шлюз в течение другого временного периода;
- "Строго проверять время возврата ключа" - привилегия для ключницы. При установленном флажке система сформирует сигнал тревоги, если ключ не сдан вовремя (по истечению периода, на который ключ был выдан, или при наступления момента времени к которому ключ должен был быть сдан);
- "Постановка на охрану" (для групп доступа категории "Охранная подсистема Parsec") - позволяет ставить охранный контроллер на охрану. Привилегия предоставляется не доступному идентификатору, а пин-коду для охранного контроллера;
- "Снятие с охраны" (для групп доступа категории "Охранная подсистема Parsec") - позволяет снять охранный контроллер с охраны. Привилегия предоставляется не доступному идентификатору, а пин-коду для охранного контроллера;
- "Просмотр конфигурации" (для групп доступа категории "Охранная подсистема Parsec") - предоставляет возможность просмотреть статусы охранных областей контроллера AC-08 при помощи клавиатуры AKD-01;

- Флажки *Вход запрещен и Выход запрещен* (карточка субъекта доступа в Редакторе персонала) - при установке какого-либо флажка или обоих флажков идентификатору с признаком "Первичный" (отображается в поле *Код карты*) будет заблокировано соответствующее действие. Если у субъекта доступа более одного идентификатора, с ними можно произвести аналогичную блокировку, перейдя на вкладку *Идентификаторы*, переведя нужный идентификатор в режим редактирования, после чего установив нужные флажки;
- Флажок *Владелец кабинета* (карточка субъекта доступа в Редакторе персонала) - это сама по себе не привилегия, но функционал аналогичен. Установка этого флажка в карточке субъекта доступа[263] приводит к тому, что при его входе на территорию или в помещение дверь будет оставаться открытой, вплоть до его выхода.

Не все контроллеры поддерживают перечисленные привилегии, в таблице ниже приведена сводка:

Привилегия	Контроллеры					
	NC-100K-IP	NC-60K/ NC-60K.M	NC-32K/32K.M	NC-8000/D/E	NC-1k/2k/5k	AC-08
Выключение звука двери	●	●	-	●	●	-
Управление охраной	-	●	●	●	●	-
Проход при блокировке	●	●	●	●	●	-
Проход при антипассбэке	●	●	●	●	●	-
Гостевая карта	●	●	●	●	-	-
Карта с привилегиями	●	-	-	-	-	-
Флажок *Выход запрещен*	●	●	-	●	-	-
Выход вне временного профиля разрешен	●	●	-	●	-	-
Управление доступом	●	●	●	●	●	-
Не использовать счетчик проходов	-	●	-	●	-	-
Флажок *Вход запрещен*	●	●	-	●	-	-
Прием тревоги	-	●	●	●	-	●
Постановка на охрану	-	●	-	●	-	●
Снятие с охраны	-	●	-	●	-	●
Просмотр конфигурации	-	-	-	-	-	●
Флажок *Владелец кабинета*	-	●	-	●	-	-

8.6.3 Сложные группы доступа

Система позволяет создать достаточно сложные правила доступа для персонала с жестким ограничением времени доступа, причем с дифференциацией по помещениям.

У любой группы доступа можно выбрать любые точки прохода, и назначить им свое расписание. При этом удобно помнить правило: что одиному идентификатору присваивается только одна группа доступа, одной точке прохода можно назначить только одно расписание.

Создавая множество подгрупп с множеством расписаний, учитывайте, что количество расписаний, хранимых в контроллерах, ограничено. Кроме того, многие контроллеры поддерживают только недельные расписания - смотрите документацию на соответствующие типы контроллеров.

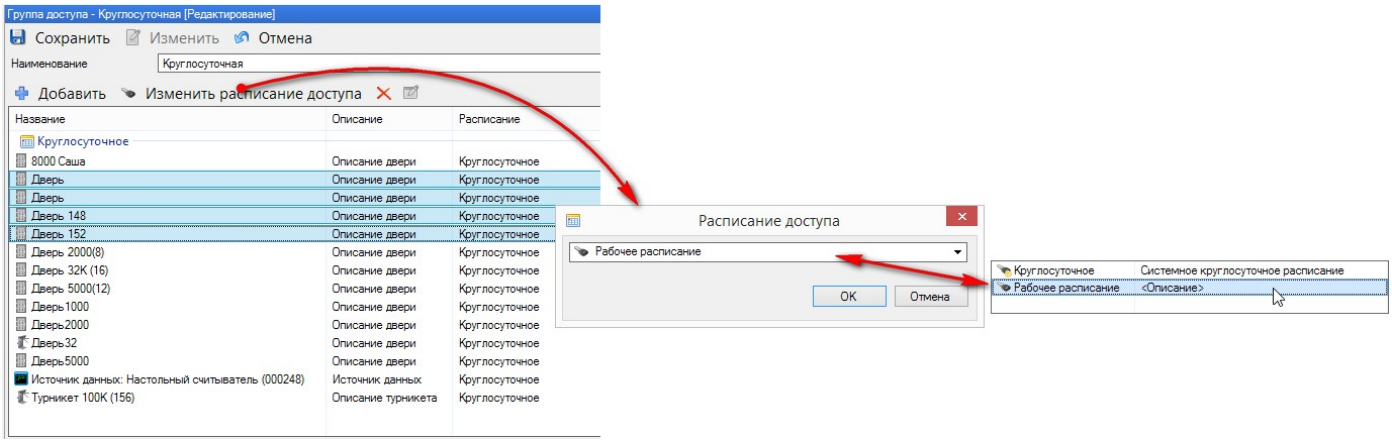
Система загружает в контроллеры только расписания, требуемые для данной группы доступа, даже если к этой группе пока не приписан ни один субъект, поэтому при большом количестве расписаний может возникнуть ситуация, когда в контроллер потребуется занести больше расписаний, чем он может реально хранить.

parsec

Создание подгруппы доступа

Предположим, что у нас есть группа доступа с набором точек прохода и круглосуточным доступом через них. Создадим подгруппу с доступом только по рабочим дням с 9:00 до 18:00. Предварительно для этого необходимо создать соответствующее недельное расписание доступа, после чего можно создавать подгруппу доступа.

1. Выберите точки прохода, которым необходимо назначить новое расписание доступа;
2. Нажмите на кнопку *Изменить расписание доступа*. Откроется *окно* расписаний доступа;
3. В раскрывающемся списке укажите нужное расписание и нажмите на кнопку *ОК*:



4. Сохраните сделанные изменения.

8.6.4 Расширенные QR-коды

Расширенные QR-коды доступны для работы только с контроллерами NC-60K и NC-60K.M.

Для внешних интегрированных систем доступна возможность создания расширенных QR-кодов (кодов с правами доступа). Иными словами, в сгенерированном QR-коде будут содержаться все настройки доступа и ID субъекта доступа. Это позволяет организовать доступ без загрузки кодов карт в контроллеры.

Общий алгоритм работы выглядит следующим образом:

- В ПО ParsecNET 3 создаются группы контроллеров, охраняющие доступ к тем или иным территориям;

- Средствами внешней интегрированной системы доступа выбирается та или иная группа контроллеров (до четырех групп), указывается время, в которое через них возможен проход и ID пользователя, после чего генерируется QR-код, содержащий эти данные;
- По факту прохода/запрета на проход в СКУД Parsec формируется событие с указанием ID субъекта доступа.

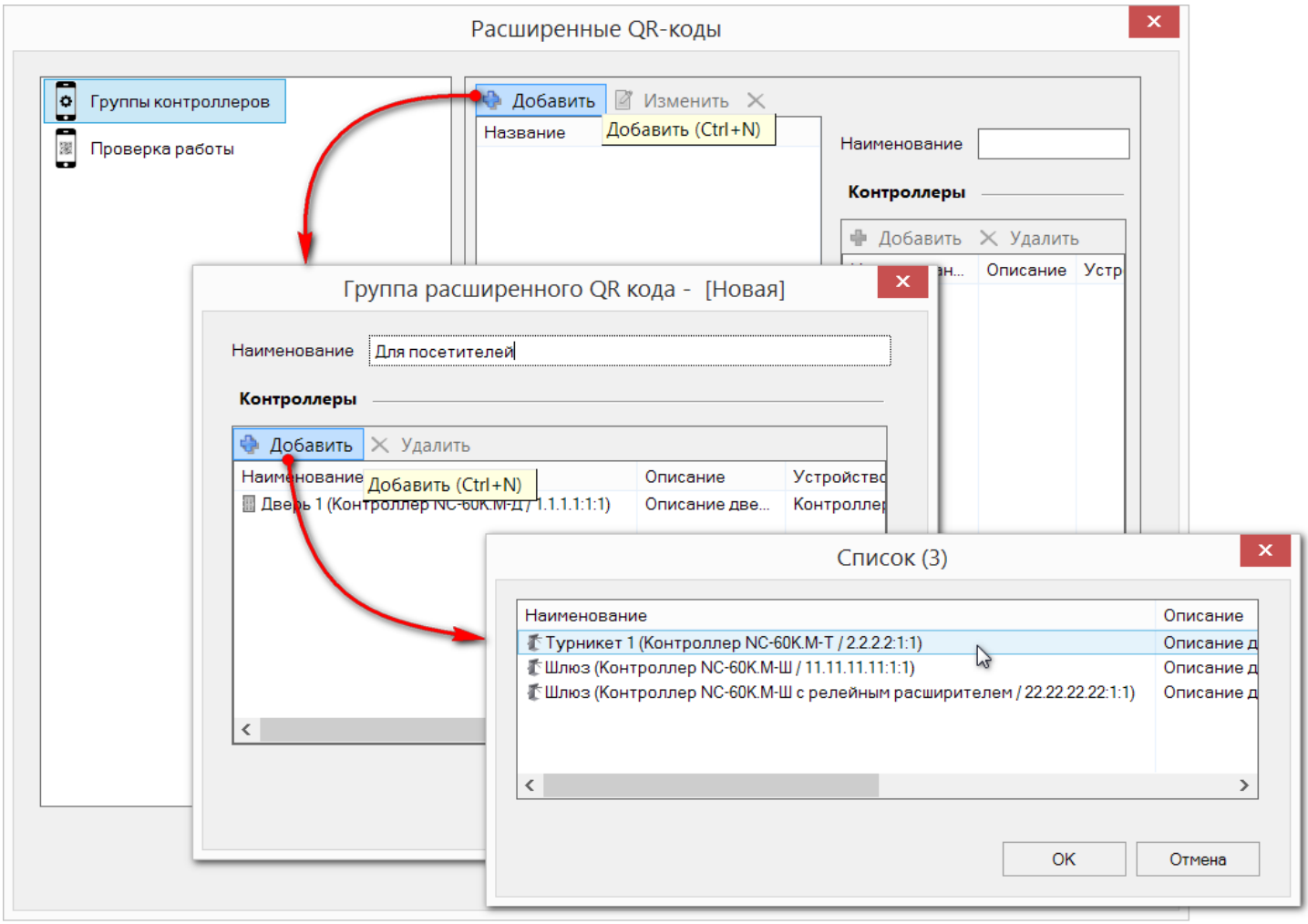
Количество QR-кодов с разными группами контроллеров и/или временем доступа - не ограничено.

Количество групп контроллеров - не более 32000. Один контроллер может состоять не более чем в 32 группах.

Нажмите на кнопку *Расширенные QR-коды* на панели инструментов Редактора групп доступа, чтобы открыть окно настроек.

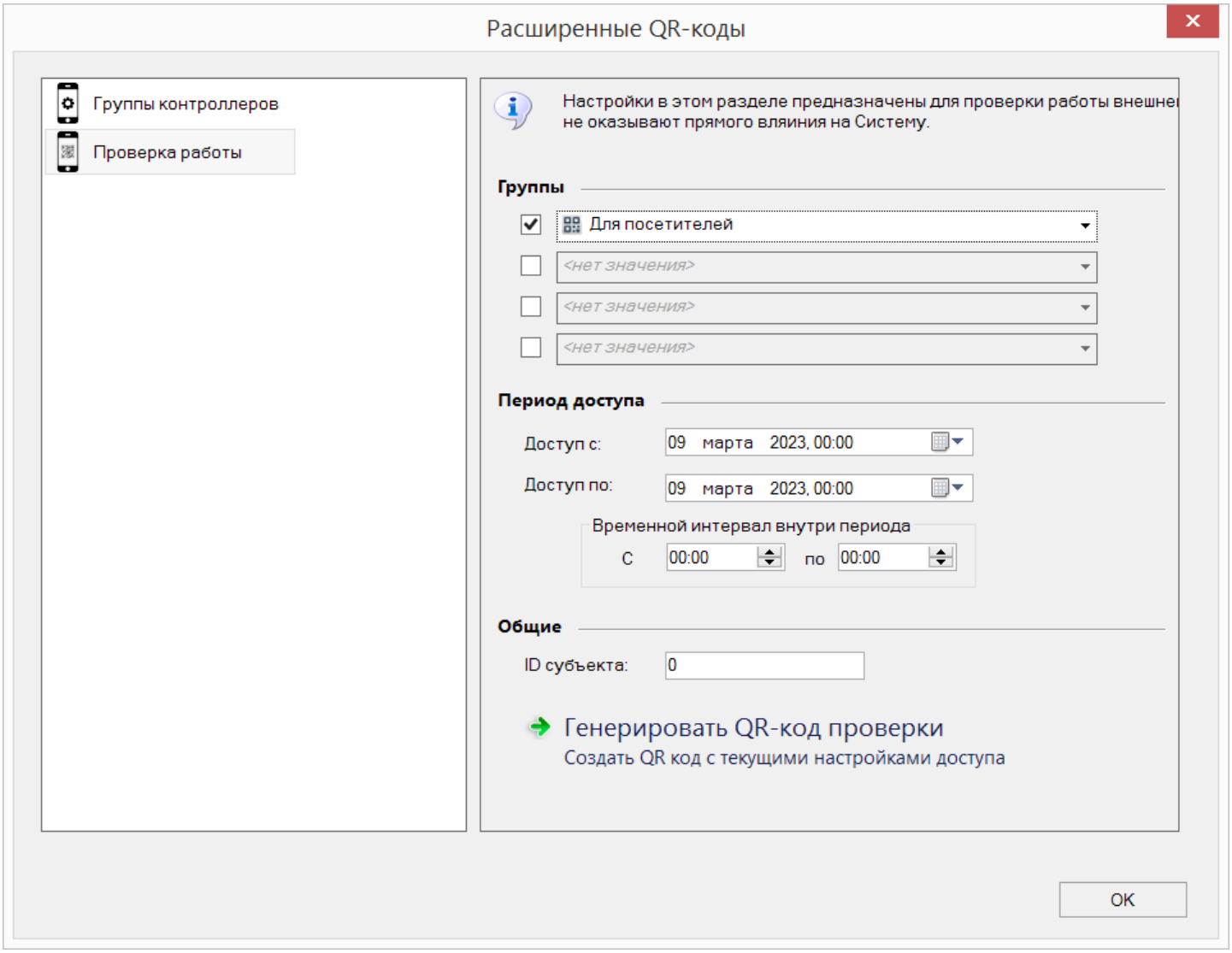
Группы контроллеров создаются на вкладке *Группы контроллеров*. Для этого выполните шаги:

- Нажмите на кнопку *Добавить* вкладки *Группы контроллеров*. Откроется окно *Группа расширенного QR кода*;
- Введите наименование группы и нажмите на кнопку *Добавить* для отбора контроллеров в состав группы;
- В открывшемся окне выберите контроллеры, защищающие территории, на которые предоставляется доступ. Т.е. пользователь должен иметь право доступа на все эти территории в любой последовательности в рамках разрешенного временного периода:



На вкладке *Проверка работы* можно проверить работоспособность функции с созданными группами контроллеров. Для этого необходимо выбрать группы (до 4) и указать период доступа. Затем нажать на кнопку *Генерировать QR-код проверки*.

Далее рекомендуется проверить, как срабатывает QR-код на точках прохода, охраняемых входящими в выбранные группы контроллерами, в направлении как на вход, так и на выход.



- *ID субъекта* - если указанный ID имеется в БД Системы, то при проверке будет сформировано событие с указанием данных соответствующего субъекта доступа. В противном случае в сообщении о событии будет указан только введенный в поле ID. Поле не обязательно для заполнения.

8.7 Редактор персонала

Редактор персонала предназначен для создания и редактирования подразделений и субъектов доступа системы. Понятие подразделений является чисто логическим группирующим понятием, помогающим систематизировать всех субъектов доступа.

Для того, чтобы субъект имел права доступа на определенные территории в определенное время, ему требуется присвоение группы доступа.

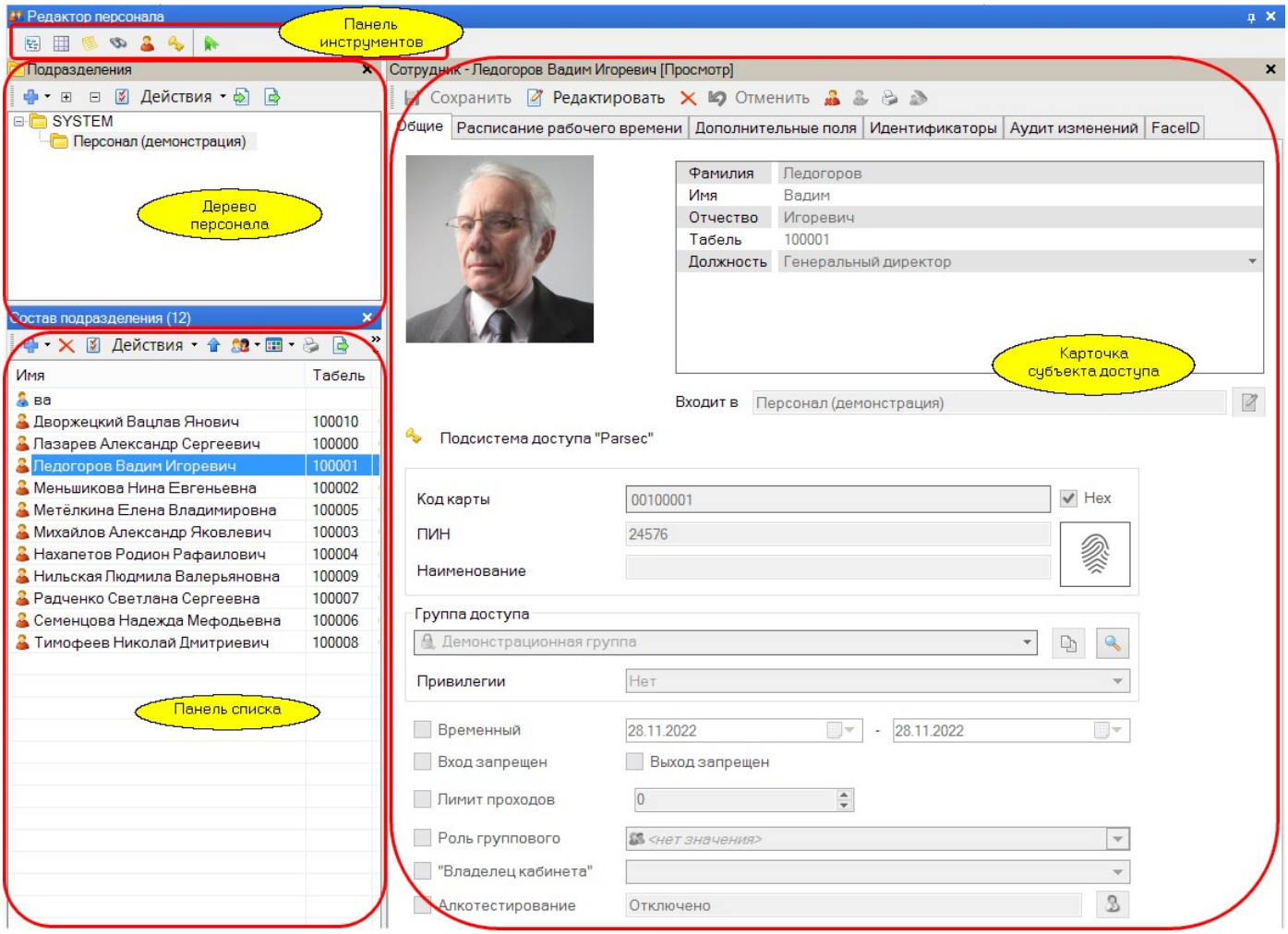
Все субъекты являются владельцами идентификаторов со своими группами доступа (набором элементов оборудования с привилегиями и временем доступа) и могут быть одного из трех типов:

- ***Сотрудник***. Основные его характеристики - ФИО и табельный номер. Имеет все возможности, предусмотренные в системе.
- ***Посетитель***. Поддерживает только один идентификатор доступа, причем всегда временный. У посетителя отсутствует закладка расписание рабочего времени, и он не может учитываться в УРВ.
- ***Автомобиль*** (транспортное средство). В карточке отсутствует закладка расписание рабочего времени, он не учитываются в УРВ. Также отсутствует возможность ввода данных со сканера и добавляется идентификатор типа автомобильный номер.

Следует отметить, что экспорт и импорт возможен только для однотипных субъектов. Также в других инструментах добавляется выбор категории (типа) субъекта доступа. Групповая печать карточек возможна также только для субъектов одного типа, поскольку они имеют свои наборы шаблонов для печати карт.

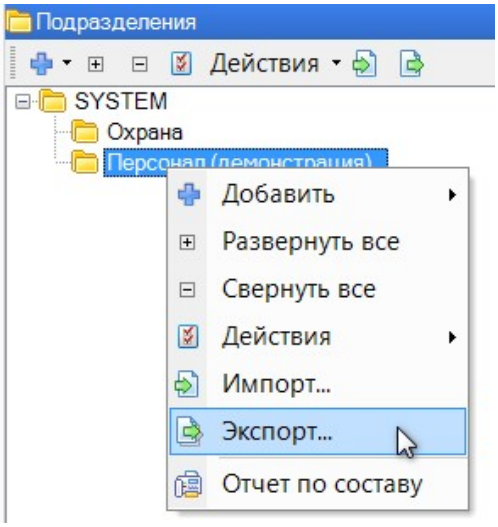
Панели редактора персонала

Редактор персонала имеет панель инструментов и три рабочие панели, показанные ниже:

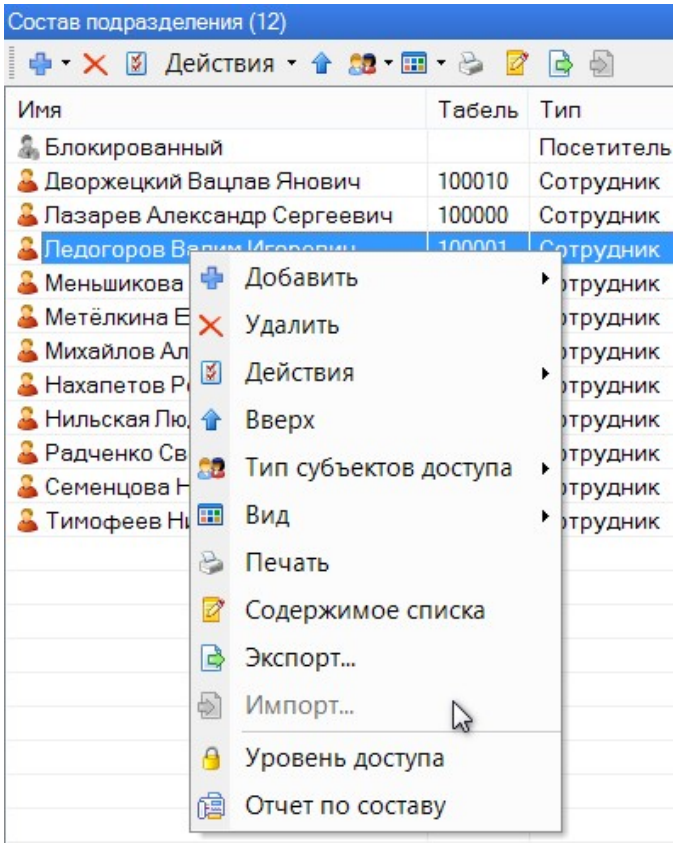


Работа с персоналом - создание подразделений, создание и редактирование сотрудников - описаны в разделе Создание карточек персонала и подразделения[258].

Контекстные меню



Контекстное меню панели "Подразделения"



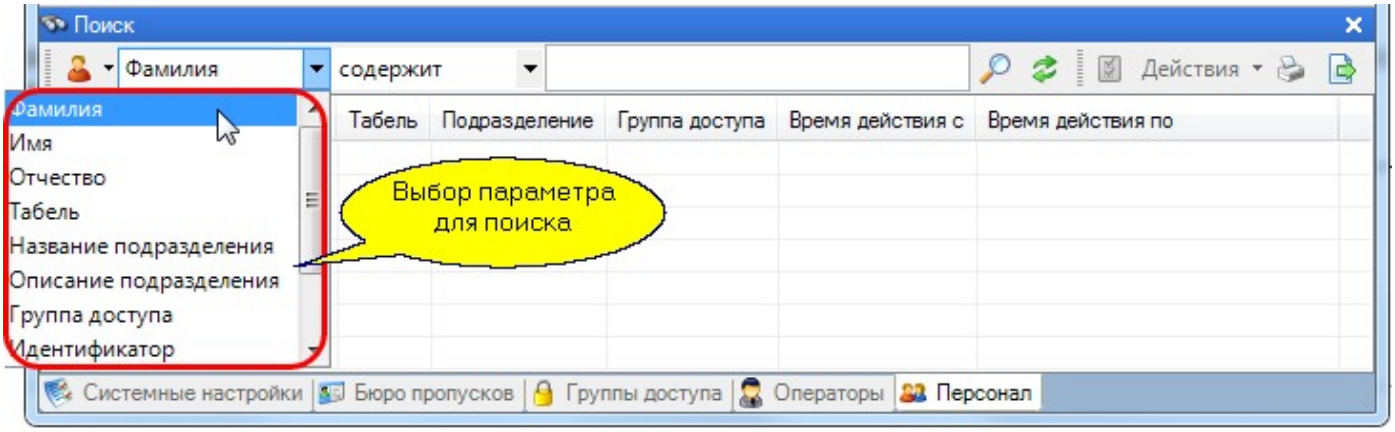
Контекстное меню панели "Состав подразделения"

Общий состав команд контекстных меню:

- *Вверх* - переход на вышестоящий уровень в дереве иерархии подразделений;
- *Вид* - выбор способа отображения списка субъектов доступа;
- *Действия* - список доступных действий[279] с персоналом и подразделениями;
- *Добавить* - добавление нового подразделения или субъекта доступа: Сотрудника, Посетителя, Автомобиль;
- *Импорт... / Экспорт...* - запуск процедуры импорта/экспорта[272] данных о подразделении/субъектах доступа;
- *Отчет по составу* - печать карточек выбранных субъектов доступа;
- *Печать* - вывод на печать данных о субъекте доступа. Шаблон печати настраивается в отдельном редакторе[417] ;
- *Развернуть все*/*Свернуть все* - команды раскрывают/скрывают все подуровни иерархического дерева;
- *Содержимое списка* - печать отображаемых в данный момент элементов списка. Доступен на панели "Состав подразделения" и "Поиск";
- *Тип субъекта доступа* - фильтр отображения на панели субъектов доступа выбранного типа;
- *Удалить* - удаление субъекта доступа из Системы;
- *Уровень доступа* - создание отчета с указанием, на какие территории выбранный субъект имеет доступ и его расписания доступа.

Панель поиска

Панель поиска открывается нажатием на кнопку *(Поиск)* на панели инструментов. В панели поиска мы можем найти сотрудника по различным критериям: фамилии, имени и другим полям:

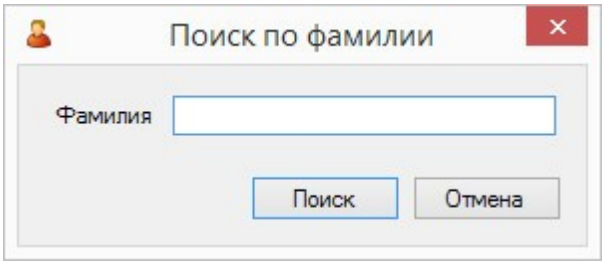


После выбора критерия следует выбрать правило анализа заданного поля (содержит или равно) и ввести искомое сочетание букв, после чего нажать на кнопку *Поиск* в верхней части панели поиска. Результат будет выведен в список, по которому можно перейти к карточке любой персоны из этого списка.

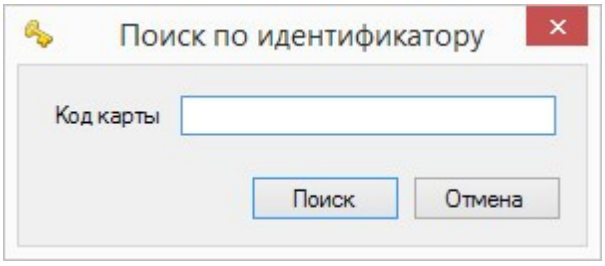
Если сотруднику назначена "Особая" группа доступа, то используя поиск по критерию "Группа доступа" с правилами анализа "Равно" и "Содержит" данного сотрудника найти будет невозможно. Воспользуйтесь правилом "не пусто" и вручную отсортируйте в полученном списке сотрудников с группой доступа "Особая".

Кроме этого, существуют варианты "быстрого" поиска:

- по фамилии (номеру автомобиля). Окно поиска вызывается кнопкой :



- по коду идентификатора. Окно ввода кода открывается кнопкой :



8.7.1 Создание карточек персонала и подразделения

В общем случае любое предприятие имеет деление на структурные подразделения (отделы, цеха и так далее). Вы можете создать иерархическую структуру персонала в соответствии с вашими потребностями. Если у вас совсем маленькая организация, то структуру подразделений можно не

создавать, а весь персонал заносить непосредственно в корень структуры - в нашем случае в SYSTEM.

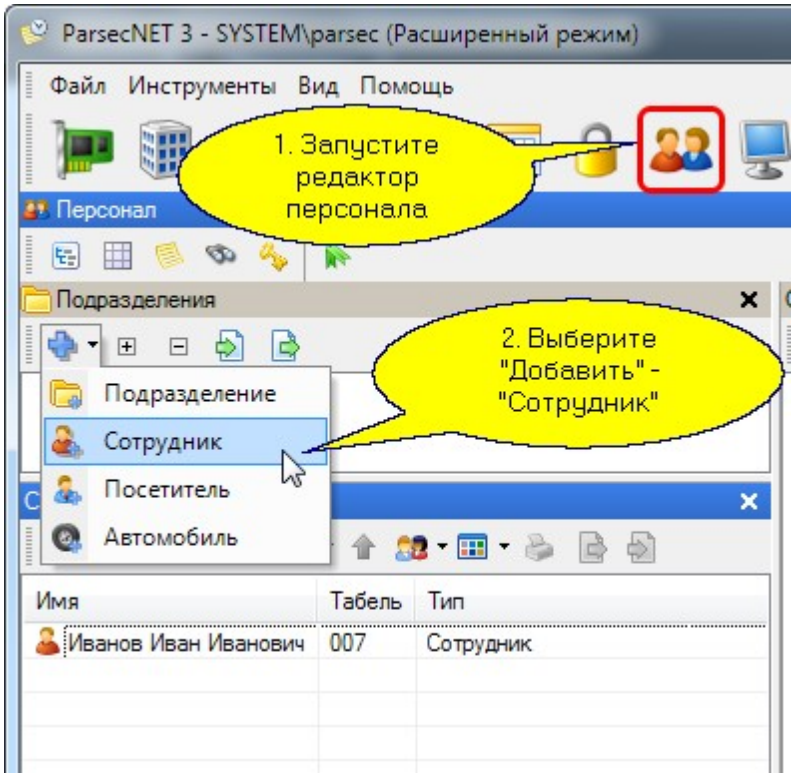
Все субъекты доступа делятся на следующие группы (или типы):

- **Сотрудники**. Постоянные пользователи системы (даже если время действия их карт ограничено некоторым конкретным сроком).
- **Посетители**. Используются, в основном, для бюро пропусков. По ним не могут создаваться отчеты по рабочему времени.
- **Автомобиль**. Трактуется как отдельный субъект доступа с номером в качестве идентификатора. **Обратите внимание, автомобильные номера пишутся с использованием латинского алфавита!**

Чтобы избежать дублирующих записей сотрудников рекомендуется настроить функцию Контроль уникальности сотрудников[355] .

Новый сотрудник в простой системе

Добавить сотрудника в корень персонала системы можно непосредственно в дереве персонала:



Ниже будут описаны шаги по вводу необходимых данных сотрудника на примере добавления его в конкретное подразделение.

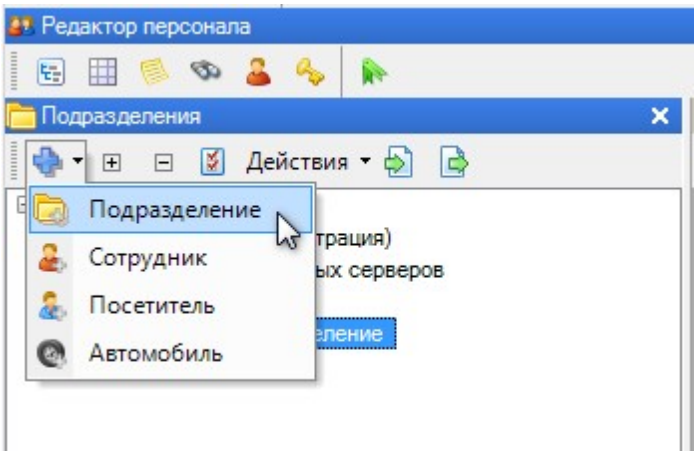
Ввод данных сотрудника со сканера возможен только при наличии модуля сканирования и распознавания документов[671] , который лицензируется отдельно.

Добавление подразделений

При добавлении подразделения создается группирующий элемент (папка), в который потом смогут входить как люди, так и вложенные подразделения. Для добавления подразделений выполните следующие действия:

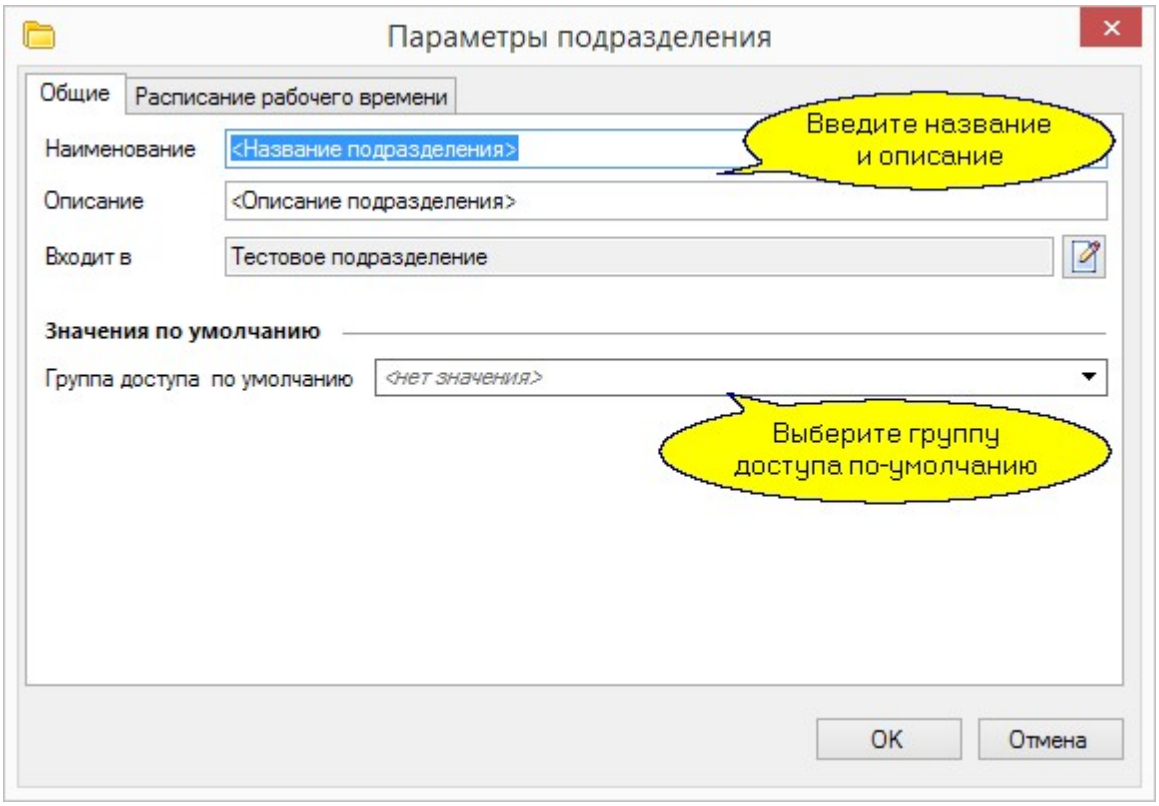
1. Установите курсор на то подразделение, в состав которого хотите добавить новое подразделение.

2. Нажмите на кнопку *Добавить* и выберите *Подразделение*:

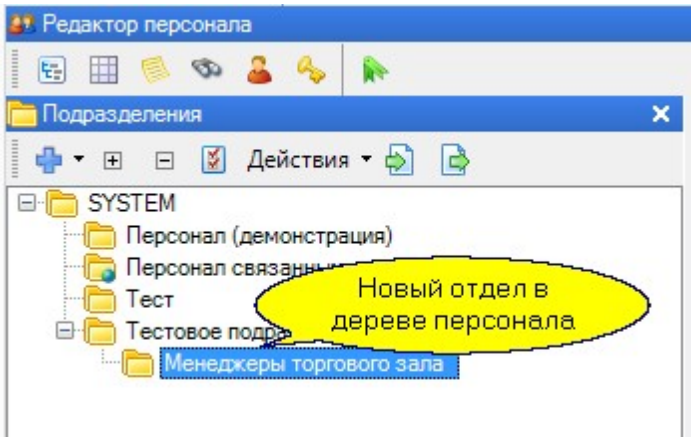


3. В открывшемся диалоге введите название. Описание не является обязательным - это ваша справочная информация.

   При необходимости укажите группу доступа по-умолчанию, она будет автоматически назначаться всем новым субъектам, добавляемым в это подразделение:



4. На вкладке "*Расписание рабочего времени*" при необходимости укажите расписание, которое будет автоматически назначаться всем новым субъектам, добавляемым в это подразделение.
5. Нажмите на кнопку "*OK*" и в результате в дерево персонала будет добавлено новое дочернее подразделение:

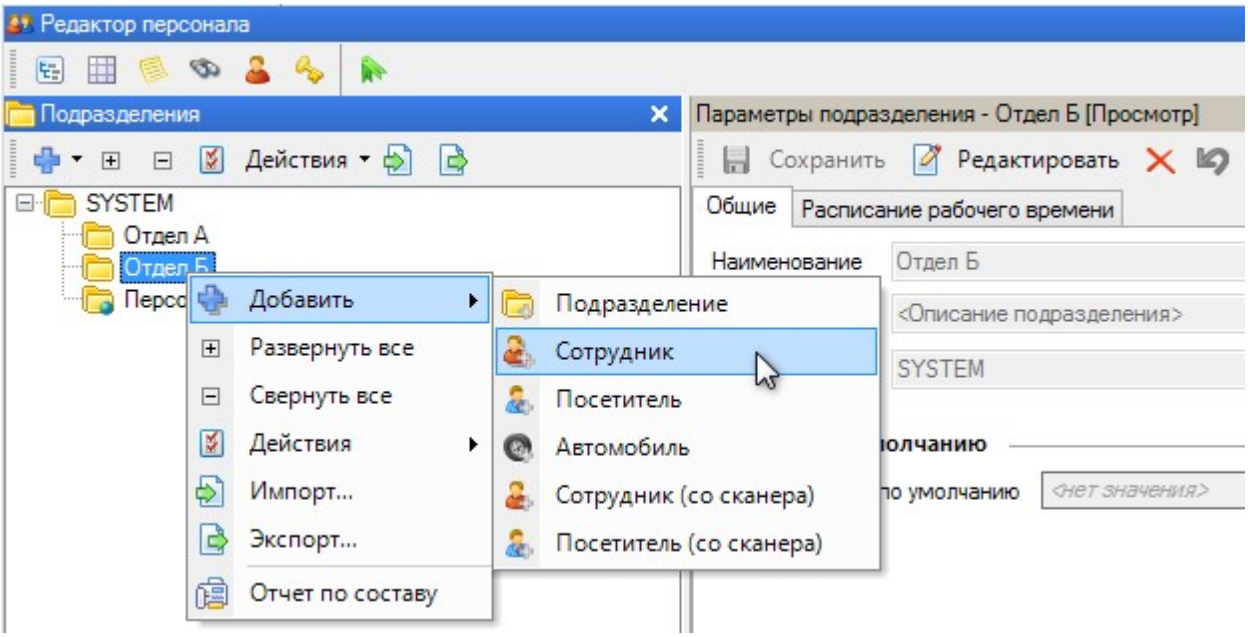


Далее мы можем добавлять персонал как в корень нашей структуры (в SYSTEM), так и в любой из отделов.

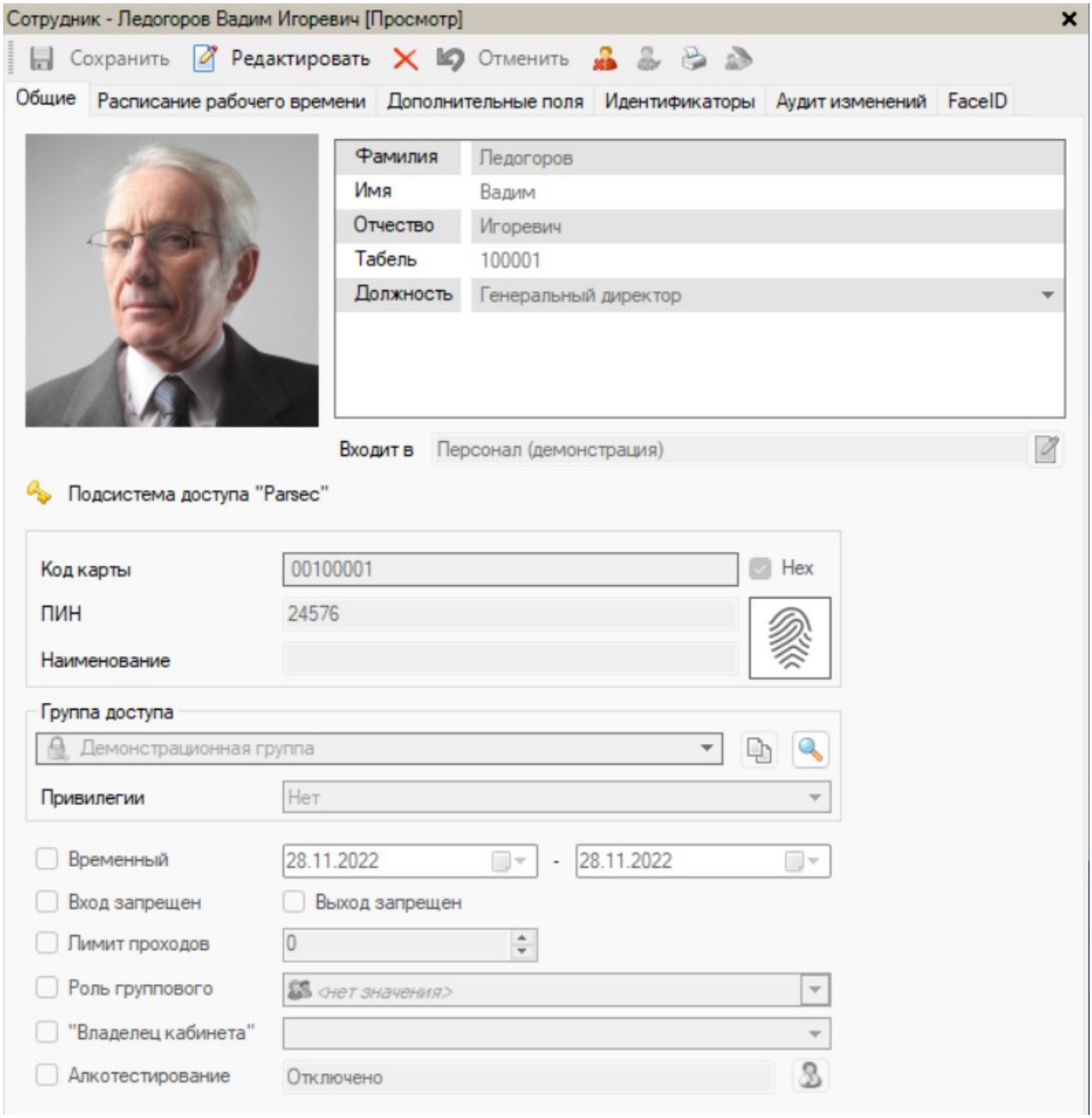
При создании подразделения на отдельной вкладке диалога параметров подразделения можно назначить подразделению расписание рабочего времени. Об этом подробнее сказано при описании модуля учета рабочего времени[456].

Добавление сотрудника

Для добавления сотрудника в конкретное подразделение надо установить в качестве текущего соответствующее подразделение. Например, выберите "Отдел Б" и добавьте туда сотрудника:



В появившейся карточке персоны введите необходимые данные:



Необходимо, как минимум, ввести фамилию; имя и отчество не обязательны.

Добавьте фотографию, если есть такая возможность.

Положите карту на подключенный настольный считыватель. Если у вас нет настольного считывателя, то его функцию при добавлении персонала может выполнять считыватель на двери (об этом в разделе Настольные считыватели[123]). В поле *Код карты* отобразится UID карты (если она уровня SL0, иными словами - чистая) или номер, заданный через утилиту SePro 3 (для уровня SL1), либо через диалоговое окно[125] Редактора оборудования (для уровня SL3).

При необходимости и если установлена какая-либо биометрическая система распознавания, отсканируйте и сохраните отпечаток пальца[654] сотрудника или скан его радужных оболочек глаз[350] .

Если для подразделения, куда добавляется сотрудник, по-умолчанию не указана группа доступа, обязательно укажите корректную группу доступа, иначе человек не сможет ходить ни в одну из дверей.

При необходимости укажите остальные параметры:

- *Временный* - если карточка выдается посетителю, то установите флажок и укажите время действия идентификатора;
- *Вход запрещен, Выход запрещен* - (привилегии[250]) при установке какого-либо флажка или обоих флажков идентификатору с признаком "Первичный" (отображается в поле Код карты) будет заблокировано соответствующее действие (Вход запрещен - только для NC-8000/D/E). Если у субъекта доступа более одного идентификатора, с ними можно произвести аналогичную блокировку, перейдя на вкладку Идентификаторы и переведя нужный идентификатор в режим редактирования;
- *Лимит проходов* - количество разрешенных входов через точку прохода. Учитывается общее количество проходов за все время использования карты. Функция работает только на точках прохода, которые оборудованы контроллерами поддерживающими использование индивидуальных счетчиков проходов. Учет проходов ведется независимо на каждой отдельной точке прохода;
- *Роль группового прохода* - выбор роли для группового прохода[115];
- *Владелец кабинета* - в раскрывающемся списке выбирается одна или несколько точек прохода, которые оборудованы контроллерами, поддерживающими функцию отслеживания владельца (см. флажок *Не закрывать, пока владелец внутри*[83]);
- *Алкотестирование* - настройка[141] параметров проверки наличия паров алкоголя в выдыхаемом субъектом доступа воздухе.

Расписания на вкладке *Расписания рабочего времени* предназначены для системы учета рабочего времени, его можно назначить позже. На доступ они не влияют.

Если оборудование подключено и система функционирует, то, в соответствии с группой доступа, информация о субъекте доступа будет отправлена в контроллеры и через пару секунд он уже сможет ходить в назначенные ему двери.

На вкладке *Дополнительные поля*[264] можно создать набор дополнительных полей для отображения специфической информации о субъектах доступа.

На вкладке *Идентификаторы*[268] имеется возможность добавить новые идентификаторы для данного субъекта доступа.

На вкладке *Аудит изенений* отображаются все события из категории "Аудит изменений", относящиеся к данному субъекту.

На вкладке *FaceID* отображаются привязанные к текущему субъекту доступа кадры, сделанные с Мобильного терминала, терминалов биометрической идентификации или камер СРЛ. Они используются для идентификации по лицу.

8.7.1.1 Дополнительные возможности

Для наиболее опытных пользователей могут оказаться полезными такие особенности, как:

- ***Дополнительные поля персонала***. Вы можете создавать свои собственные дополнительные поля[264] персонала, причем с группировкой и типизацией. Например, можно создать группу полей *Паспортные данные*, занести туда номер паспорта как строку, дату выдачи как дату и так далее.
- ***Множественные карты доступа***. Каждый субъект доступа в ParsecNET 3 может иметь более одной карты доступа, что может оказаться полезным, например, при использовании отдельных идентификаторов для распознавания принадлежащего субъекту автомобиля.
- ***Печать карт персонала***. Вы можете напечатать на доступном вам принтере карточку персоны, в частности, напечатать необходимую информацию, включая ФИО, фотографию и так далее на карте доступа, если имеете соответствующий принтер. Карты печатаются на основании шаблонов, создаваемых в Редакторе шаблонов печати[417].

- ***Расписание рабочего времени***. Его назначают при наличии Модуля учета рабочего времени[456]. В этом случае вы сможете получать отчеты об отработанном сотрудниками подразделения рабочем времени, о нарушениях графика рабочего времени.
- ***Привилегии***[250] ***пользователя***. Наряду с группой доступа уточняют права субъекта доступа по управлению охраной и другие особенности поведения системы.
- ***Персональная группа доступа***. Создание[270] группы доступа для одного сотрудника.

Использование указанных возможностей подробнее описано в разделе Редактор персонала[255].

8.7.2 Дополнительные поля

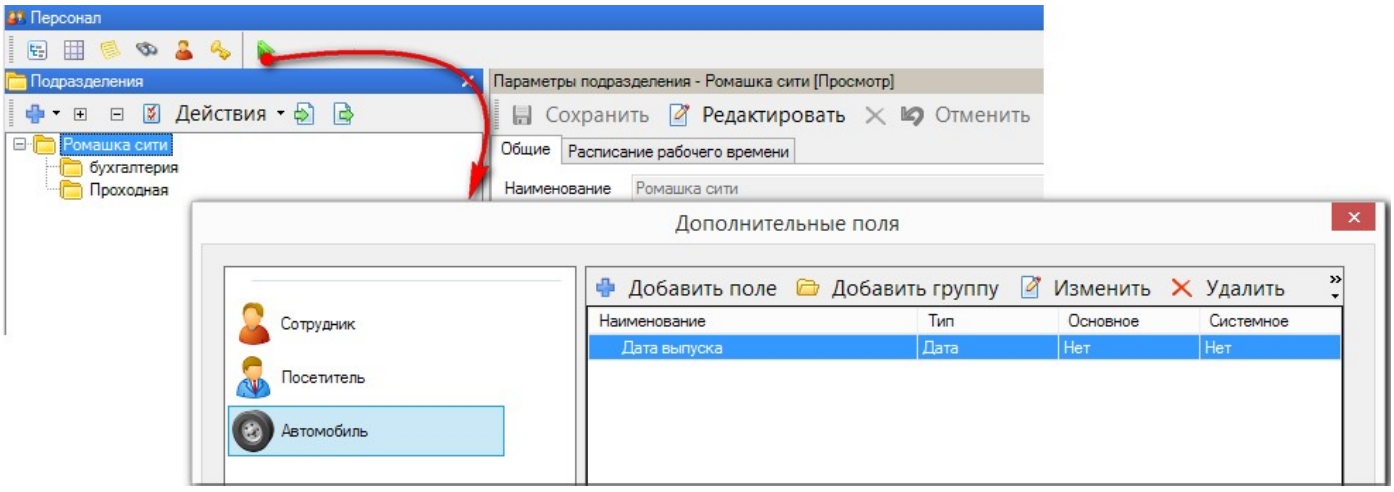
Если вам необходимо заносить в базу данных специфическую дополнительную информацию о субъектах доступа помимо той, что рассматривалась в основном описании редактора персонала, то потребуется создать набор дополнительных полей. Такие дополнительные поля используются только для информирования и не могут быть использованы Системой для каких-либо операций. В целях использования содержимого дополнительных полей, например, при создании заданий и т.п. необходимо создавать системные дополнительные поля[155].

Дополнительные поля имеют следующие свойства:

- Отображаются на вкладке *Дополнительные поля* карточки субъекта доступа;
- Для каждого субъекта доступа создается свой набор дополнительных полей;
- Их можно группировать (например, сделать группу "Паспортные данные" и "Цвет глаз" для сотрудников и/или посетителей, группы "Модель", "Госномер" и "Цвет" для автомобилей и т.п.;
- Дополнительные поля имеют типизацию (строковое, числовое, дата/время и так далее);
- Могут быть основными (показываются на первой вкладке карточки субъекта доступа), а также системными[155] (возможно использование при работе с оборудованием).
- Поле типа "Ссылка" может ссылаться[266] на другие субъекты доступа (например, сотрудник может ссылаться на автомобиль и наоборот, автомобиль может ссылаться на сотрудника).

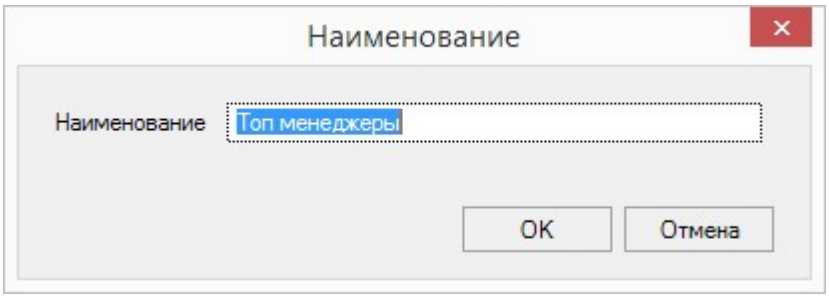
Создание дополнительных полей

Для примера создадим дополнительные поля для автомобиля. Открываем панель дополнительных полей и переходим в раздел "Автомобиль":



Можно начать как с создания групп полей, а потом внутри этих групп создавать дополнительные поля, так и сначала создать все поля, а потом, создав группы, распределить между ними созданные дополнительные поля при помощи стрелок *Вверх* и *Вниз*. Рассмотрим сначала создание групп.

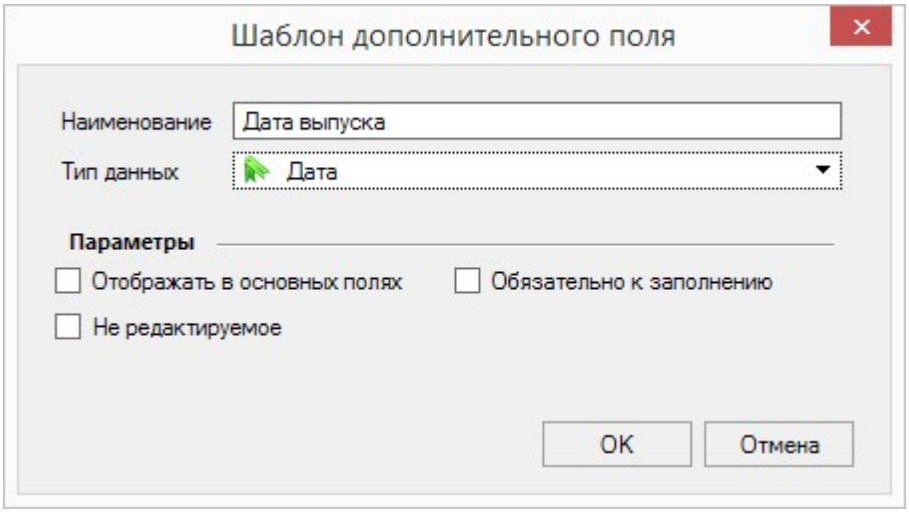
Для создания группы дополнительных полей нажмите на кнопку *Добавить группу* и в открывшемся диалоге введите название группы, затем нажмите на кнопку *ОК*:



Теперь внутри группы создайте нужное количество дополнительных полей, нажимая на кнопку *Добавить поле*, вводя названия и задавая параметры в открывшейся форме.

Дополнительные поля не могут иметь одинаковое наименование. Даже если они находятся в разных группах.

Для ФИО владельца, если он присутствует в системе, можно выбрать тип "Ссылка", для даты рождения владельца или даты выпуска автомобиля выберите тип "Дата":



Настройте параметры поля, которые соответствуют выбранному типу. Для нашего примера:

- *Отображать в основных полях* - при установке флажка созданное дополнительное поле будет отображаться в карточках субъектов доступа на первой вкладке *Общие*;
- *Обязательно к заполнению* - при установленном флажке, если при создании карточки нового или изменении существующего субъекта доступа оставить это поле незаполненным, система выдаст предупреждающее сообщение;
- *Не редактируемое* - при установке флажка содержимое поля в карточках субъектов доступа нельзя будет изменить.

Аналогично вводятся другие поля, например, *Расход топлива* и т.д. После нажатия на кнопку *ОК* у всех субъекта доступа "Автомобиль" (как новых, так и уже существующих в системе) в карточке субъекта появится новое поле.

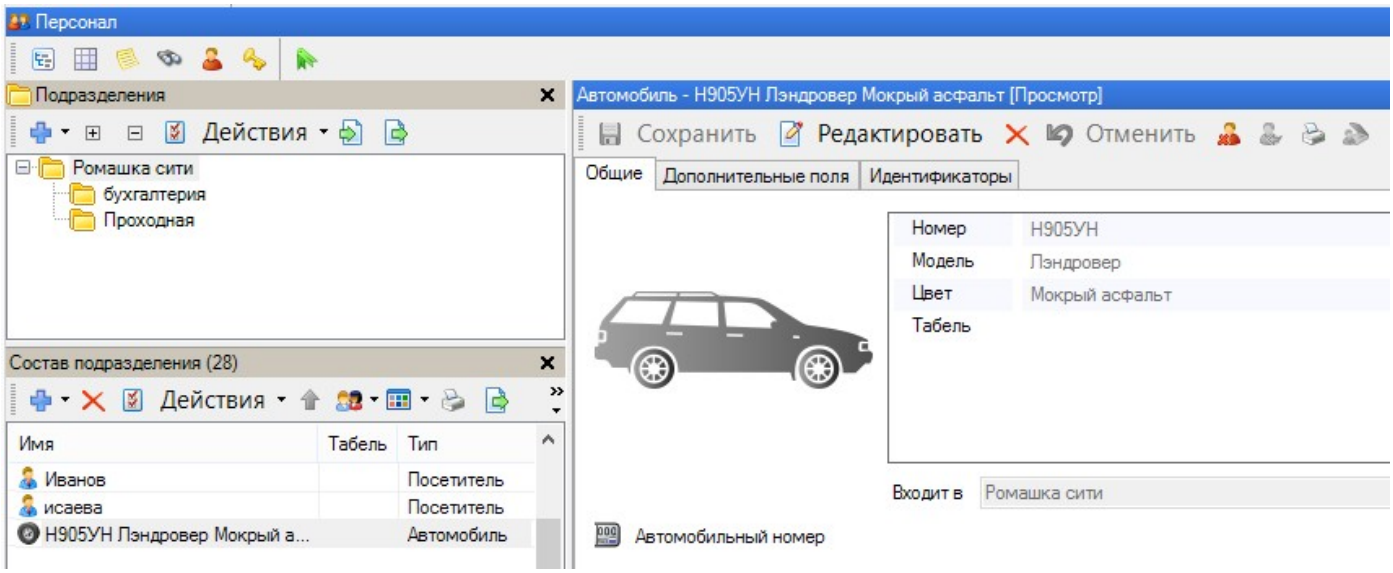
Для субъектов доступа "Сотрудник" и "Посетитель" действия по созданию дополнительных полей полностью аналогичны.

Дополнительные поля создаются отдельно в каждой организации. Как и остальные данные, они не доступны в других организациях. Исключения составляют системные дополнительные поля, у которых структура общая для всех организаций.

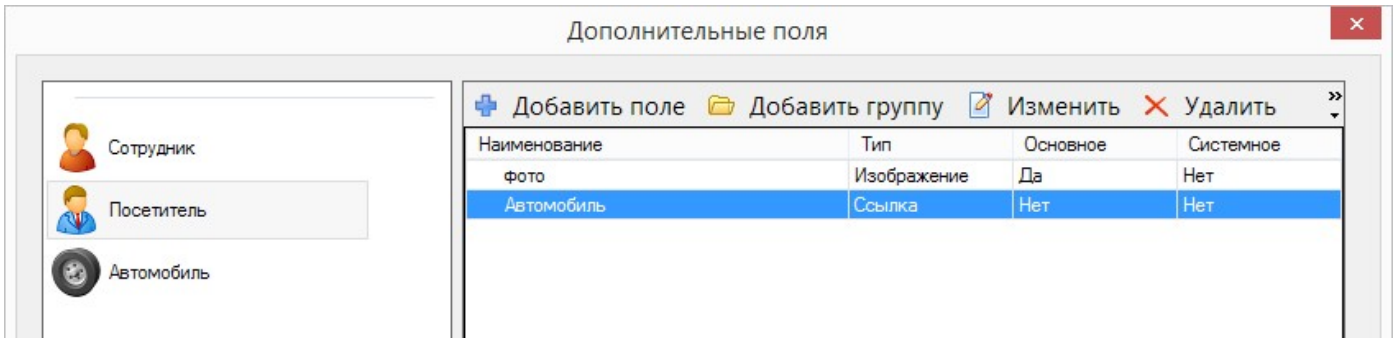
Ссылочные дополнительные поля

Для демонстрации принципов использования ссылочных дополнительных полей рассмотрим создание ссылки для посетителя на автомобиль.

Предварительно и посетитель, и конкретный автомобиль должны быть занесены как субъекты доступа в БД системы:

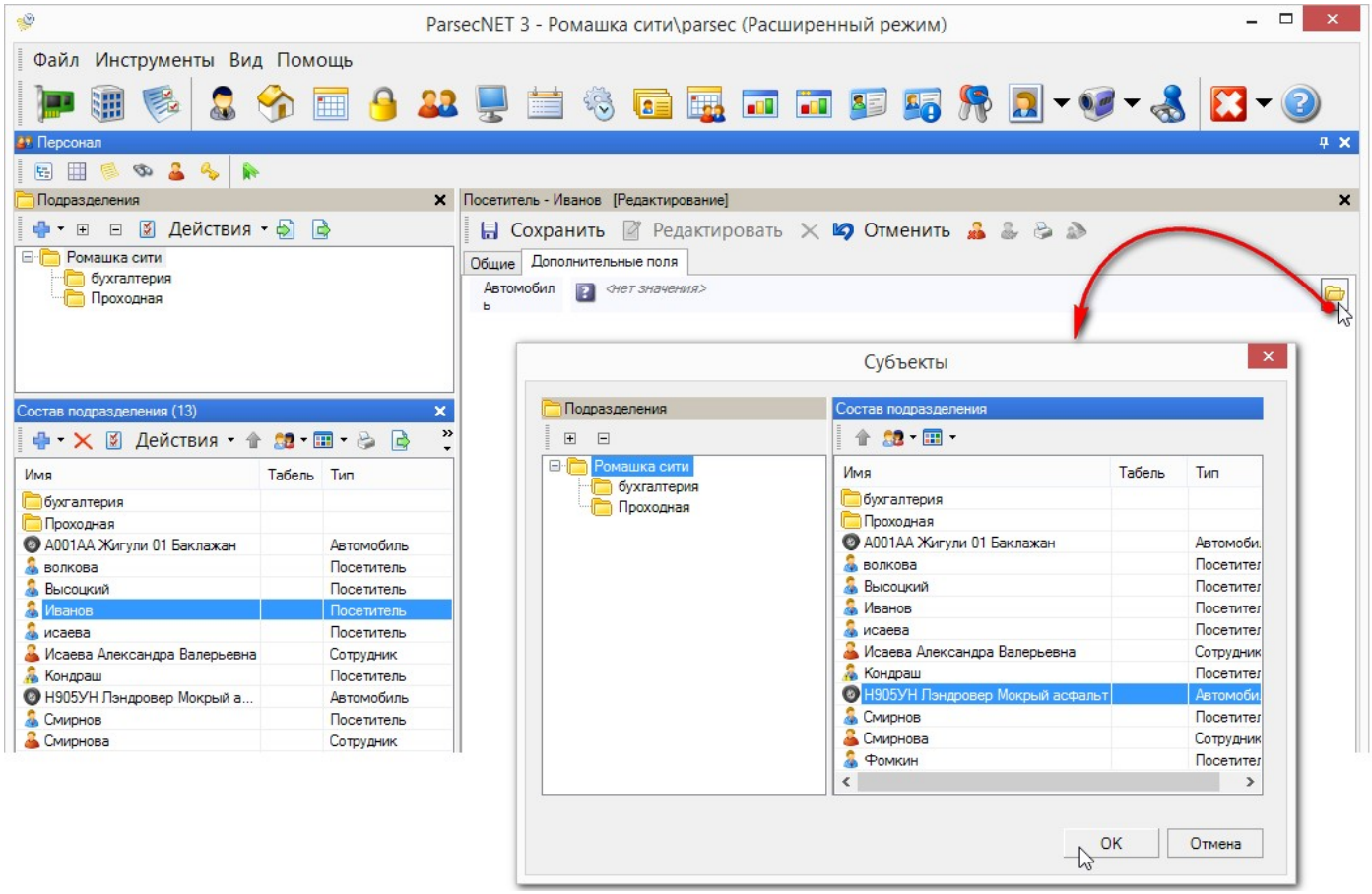


С использованием панели дополнительных полей для посетителей создается дополнительное поле *Автомобиль* ссылочного типа:



Теперь конкретному посетителю назначается ссылка на конкретный автомобиль:

- переведите карточку посетителя в режим редактирования;
- на вкладке *Дополнительные поля* нажмите на значок папки в ссылочном поле *Автомобиль*;
- в открывшемся окне выберите нужное транспортное средство и нажмите на кнопку *ОК*:

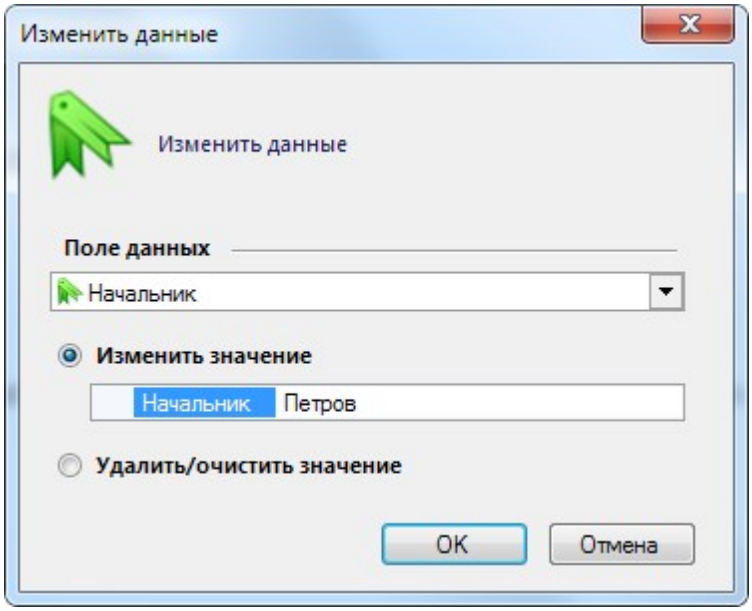


Не забудьте нажать на кнопку *Сохранить* в карточке сотрудника для сохранения изменений в базе данных. Если дополнительное поле сделать основным, то оно появится на первой вкладке карточки сотрудника.

Изменение значения дополнительного поля

Значение дополнительного поля можно изменить (очистить) как у одного, так и у группы субъектов доступа. Для этого:

1. Выберите одну или несколько записей субъектов доступа, либо папку подразделения, в котором нужно изменить дополнительные данные;
2. Выберите пункт "Действия - Изменить данные" в контекстном меню или в раскрывающемся списке на панели *Состав подразделения*. Откроется диалоговое окно;



3. В раскрывающемся списке *Поле данных* выберите дополнительное поле, значение которого нужно изменить;
4. Установите переключатель:
   - "Изменить значение" - в поле ниже можно будет ввести новое значение;
   - "Удалить/очистить значение" - значение будет удалено из поля (поле останется пустым).
5. Если выбрано изменение значения, установите новое значение выбранного дополнительного данного;
6. Нажмите на кнопку *OK*.

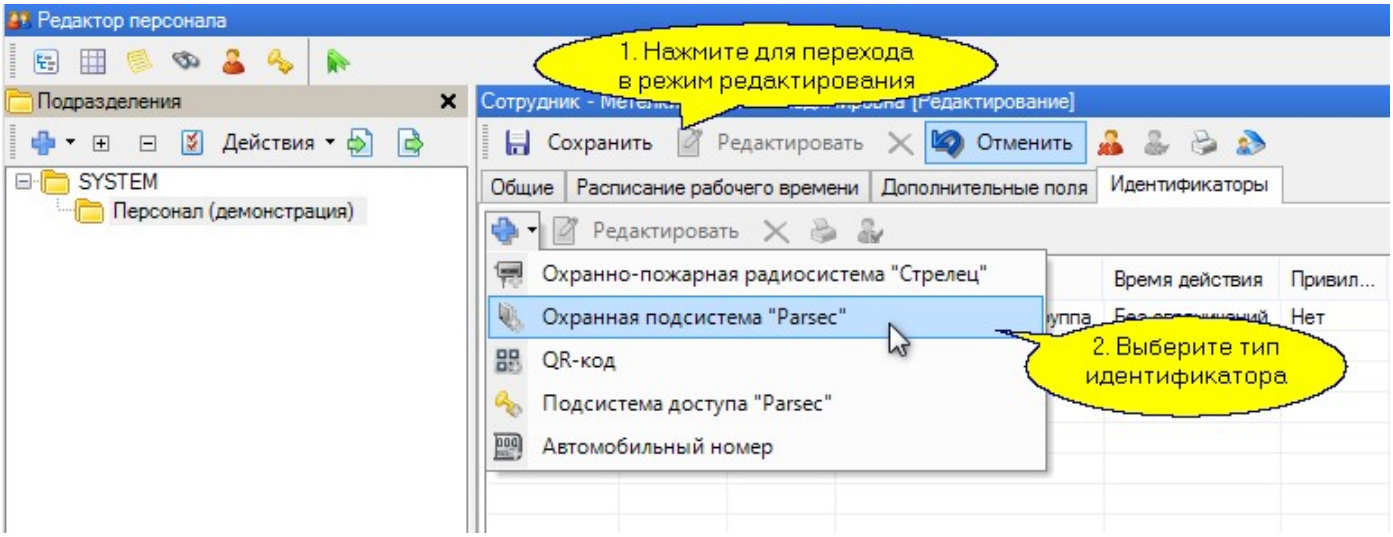
Изменение данных у подразделения приведет к установке нового значения в выбранном поле дополнительного данного у <u>всех</u> сотрудников этого подразделения.

Изменение значений основных данных (ФИО и табельный №) производится индивидуально в карточке сотрудника в режиме редактирования.

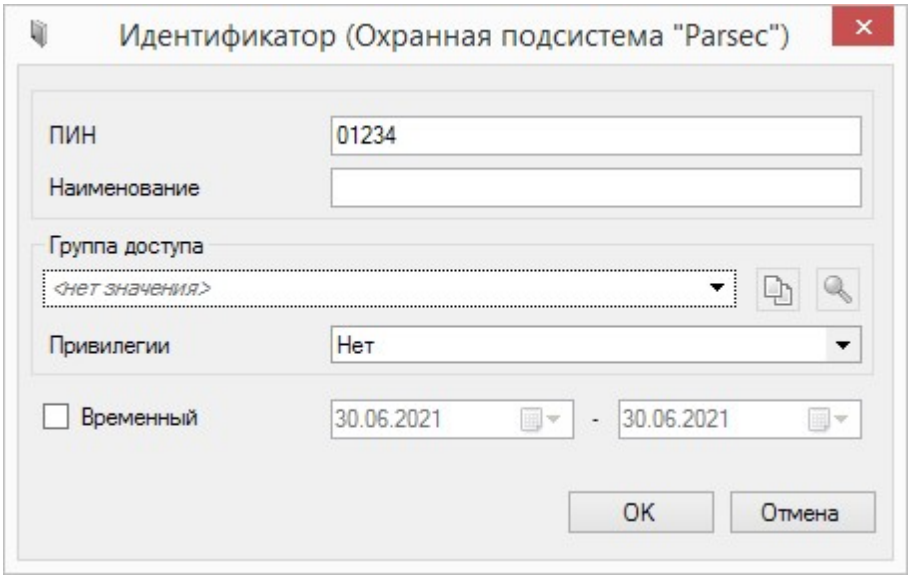
8.7.3 Идентификаторы

Каждому субъекту доступа в ParsecNET 3 можно назначить любое количество идентификаторов, причем различного типа: для доступа на территорию, для доступа к функциям охраны и так далее. Это доступно только в расширенном режиме работы.

Для добавления субъекту доступа идентификатора в редакторе персонала перейдите на вкладку *Идентификаторы*, войдите в режим редактирования и нажмите на кнопку *Добавить*:



В нашем примере мы хотим ввести идентификатор для доступа к управлению охранным контроллером AC-08. Для ввода идентификатора открывается следующий диалог:



Введите ПИН-код.

Назначьте группу доступа и привилегии (если необходимо). Естественно, соответствующую группу доступа следует создать предварительно.

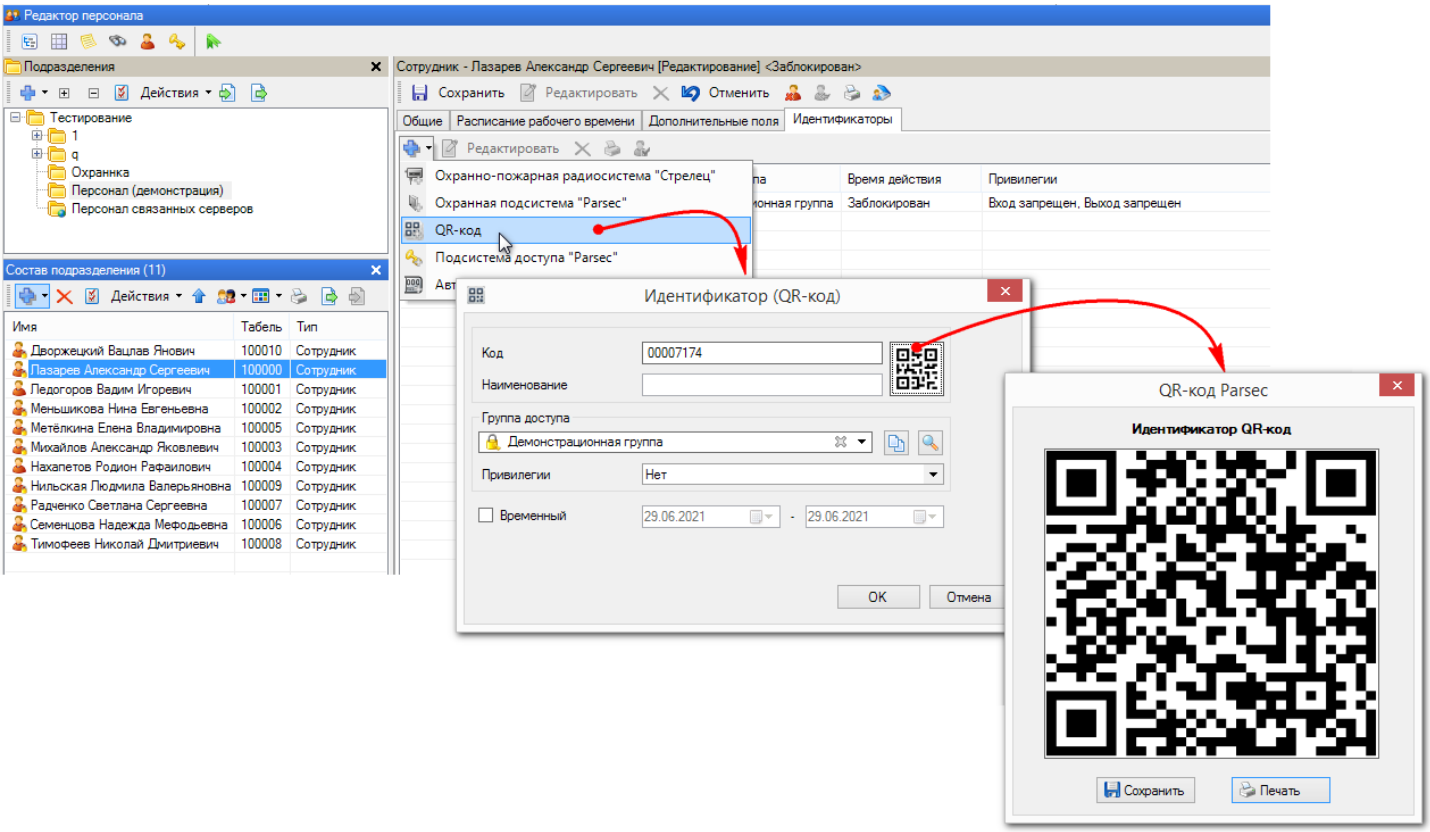
Укажите срок действия идентификатора, если он временный.

По завершению работы нажмите на кнопку *OK* для сохранения результатов.

Идентификаторы "QR-код Parsec"

В Системе можно использовать идентификаторы типа QR-код, информация в которых зашифрована специальным ключом шифрования[157]:

1. В режиме редактирования нажмите на кнопку *Добавить* и выберите из списка "QR-код Parsec";
2. В открывшемся окне заполните нужные поля, руководствуясь информацией из раздела Добавление сотрудника[261] ;
3. Для просмотра QR-кода, сформированного при помощи текущего ключа шифрования, нажмите на его значок в окне *Идентификатор (QR-код)* (рисунок ниже). Шифруется только значение из поля *Код* этого окна. Остальные данные (Группа доступа, Привилегии, срок действия временного идентификатора) не попадают в QR-код:



Сохраните сгенерированный QR-код или распечатайте на удобном носителе. Для печати на пропусках средствами СКУД ParsecNET 3 предварительно требуется создание шаблона печати[424].

Для использования идентификаторов этого типа необходимы считыватели, имеющие возможность чтения QR-кодов (например, PNR-QX29). Их также необходимо настроить как описано в разделе[157].

8.7.4 Персональная группа доступа

Общие положения

В некоторых случаях права доступа для сотрудников отличаются настолько незначительно, что не имеет смысла создавать отдельные группы доступа. Например, все сотрудники имеют доступ в общее здание, но дальше каждый имеет доступ только в свой кабинет. В таком случае имеет смысл создать общую группу доступа, а затем для каждого сотрудника - персональную группу доступа на основе общей.

Персональная группа не видна в редакторе групп доступа. Просмотреть ее можно только в карточке субъекта доступа - там же, где она создается.

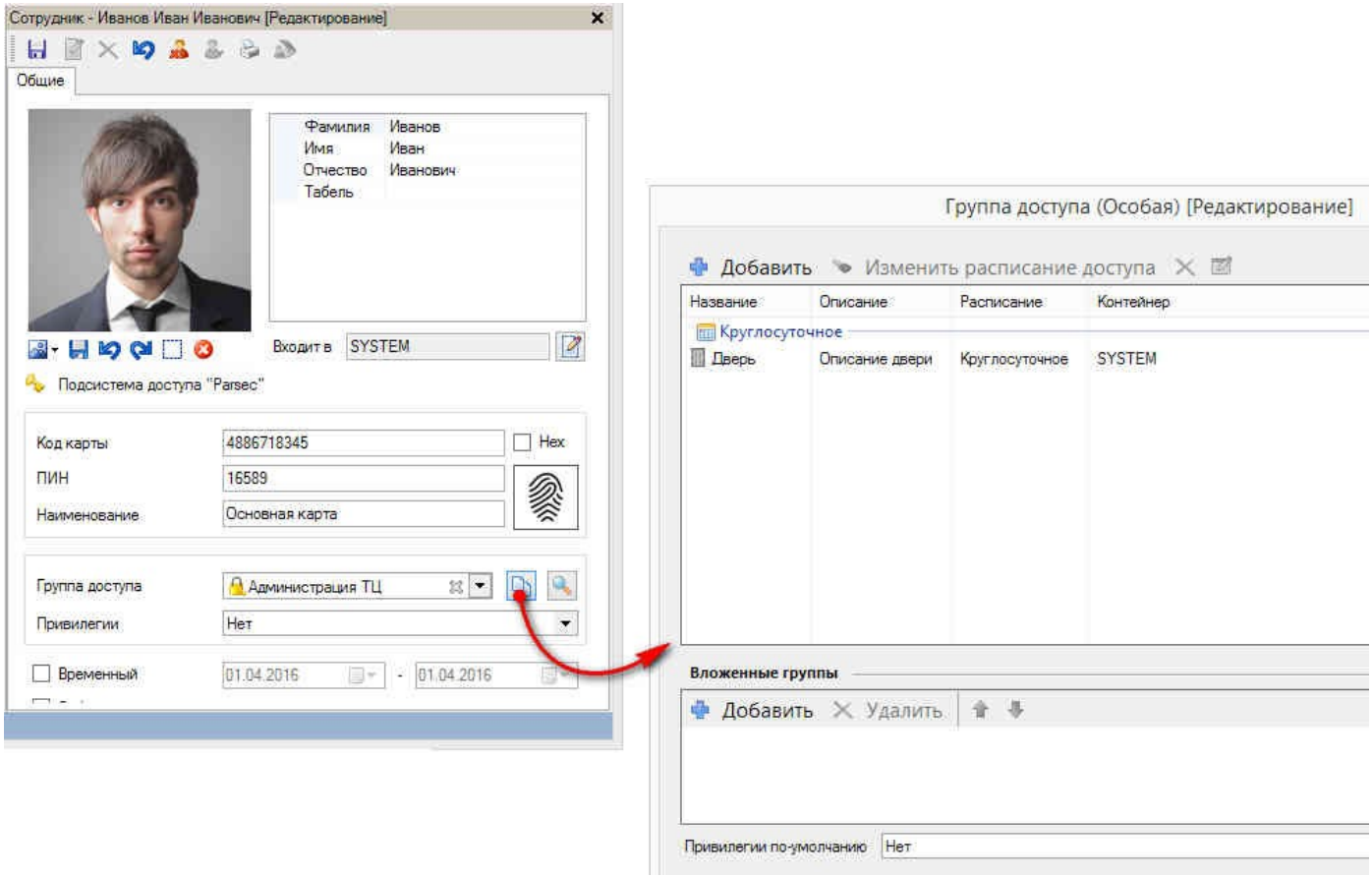
Персональная группа доступа существует до тех пор, пока в БД существует запись о субъекте доступа или идентификаторе, для которого она была создана. При отзыве идентификатора, группа персональная удаляется. При удалении сотрудника из БД, все его персональные группы также удаляются.

Создание персональной группы

Создать персональную группу можно только на основе существующей обычной группы доступа. Чтобы создать персональную группу, выполните следующие действия:

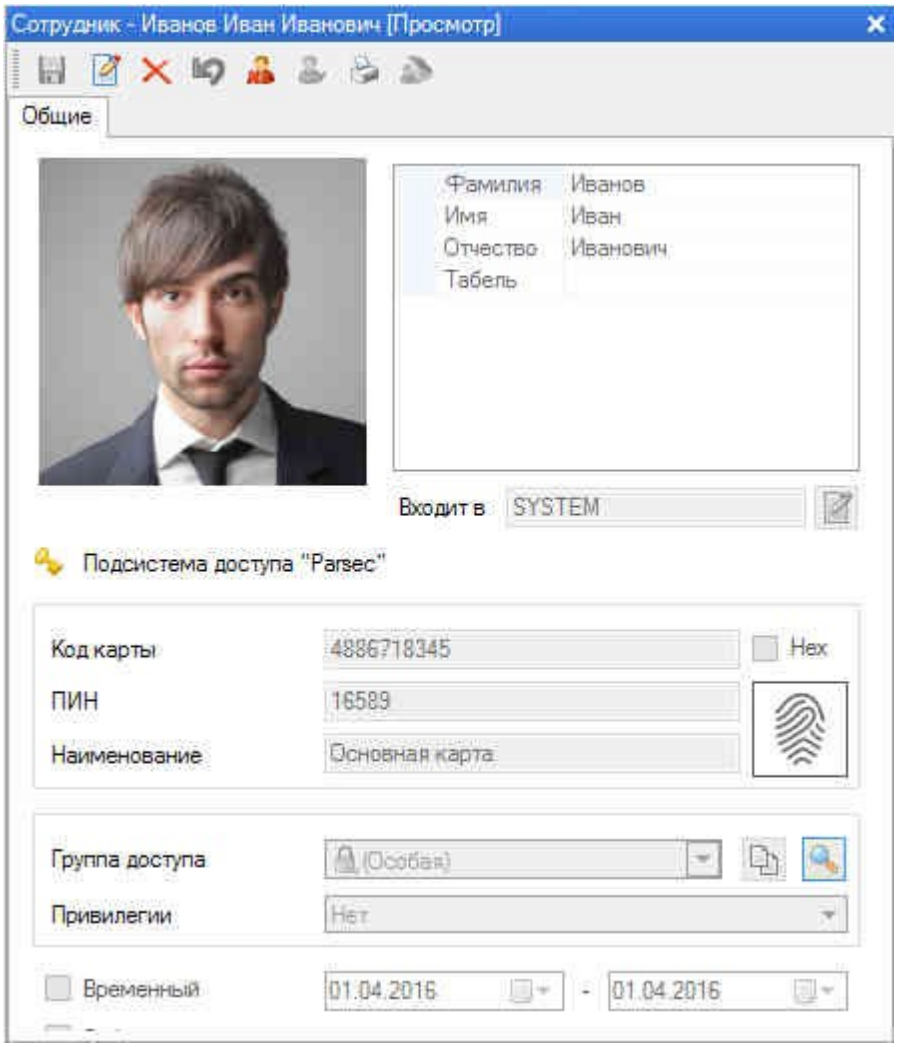
1. В карточке субъекта доступа в режиме редактирования нажмите на кнопку  в строке *Группа доступа*;

2. В открывшемся окне отметьте те точки прохода, через которые данный субъект имеет право доступа. На вкладке *Дополнительно* можно назначить подгруппы доступа. (Описание дополнительных групп доступа см. в разделе 253).



3. Нажмите на кнопку *ОК* в окне *Группа* и сохраните результаты редактирования карточки.

В результате данному субъекту будет назначена особая группа доступа:

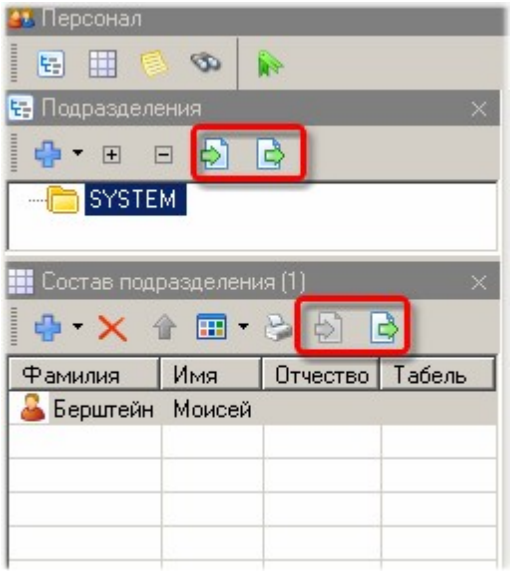


8.7.5 Экспорт и импорт персонала

Иногда требуется перенести данные о персонале из одной программной среды в другую с тем, чтобы не осуществлять ввод одних и тех же данных несколько раз и не порождать на этом дополнительных ошибок ручного ввода. Примером подобной задачи является импорт данных о персонале из кадровой системы в систему доступа или наоборот.

При импорте[274] и экспорте поддерживаются форматы XML и CSV.

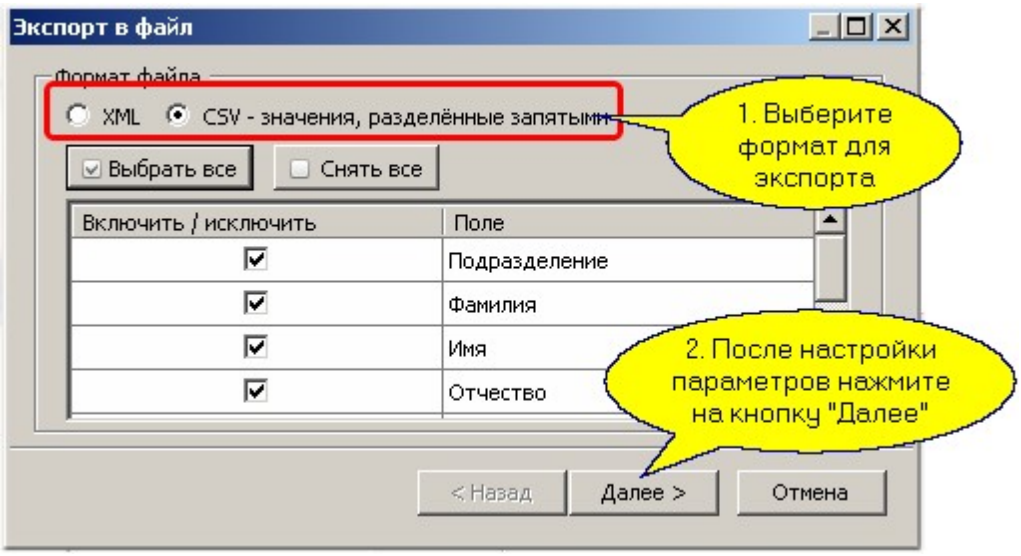
Для решения подобных задач в редакторе персонала ***Parsec*** имеется возможность импорта и экспорта персонала. Для инициирования процессов импорта или экспорта необходимо воспользоваться соответствующими кнопками в панелях редактора персонала, показанными на рисунке:



Кроме того, опции импорта и экспорта доступны из контекстного меню, открывающегося по нажатию правой кнопки мышки.

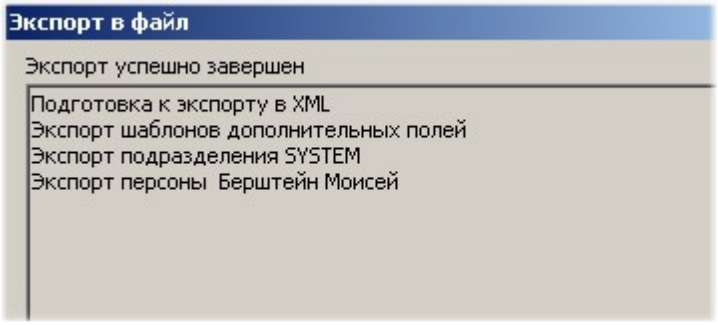
Экспорт персонала

Для примера рассмотрим экспорт персонала подразделения SYSTEM. Для этого на панели подразделений выделите требуемое подразделение и нажмите кнопку *Экспорт*. Откроется диалоговое окно, которое помогает настроить параметры экспорта:



После нажатия на кнопку *Далее* будет выведен стандартный диалог Windows для сохранения файла, при этом расширение имени файла формируется автоматически в соответствии с выбранным форматом.

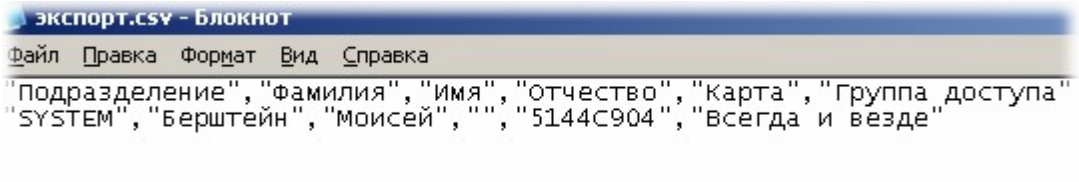
Процесс экспорта отображается в диалоговом окне, как показано, например, ниже для экспорта в формат XML:



Фрагмент файла экспорта для формата XML показан на рисунке ниже:

```
<?xml version="1.0" standalone="yes"?>
<Personel xmlns="http://tempuri.org/Personel.xsd">
  <PERSON>
    <LAST_NAME>Берштейн</LAST_NAME>
    <FIRST_NAME>Моисей</FIRST_NAME>
    <MIDDLE_NAME />
    <TAB_NUM />
    <PHOTO></PHOTO>
    <PERS_ID>e9b52847-08d1-4686-a224-3c3fd3a04890</PERS_ID>
    <ORG_ID>903cc83c-c354-4927-a97e-a9acdd6827b1</ORG_ID>
```

При экспорте в формат CSV в первой строке приводятся названия полей базы персонала, а в остальных строках последовательно идут данные персонала, по одной строке на сотрудника (если не экспортируется фотография). Пример файла с экспортом одного сотрудника в формате CSV показан ниже:



В случае, если экспорт производится из внешних систем, в поле "*Фотография* каждого экспортируемого сотрудника можно указать:

- полный путь к папке, где лежат (или будут лежать) файлы с изображениями сотрудников, или
- название файла изображения сотрудника, при условии, что при импорте csv-файл будет находиться и выполняться в той же директории, что и файлы изображений.

В этом случае при импорте фотографии автоматически будут импортированы в создаваемые карточки субъектов доступа.

Импорт персонала

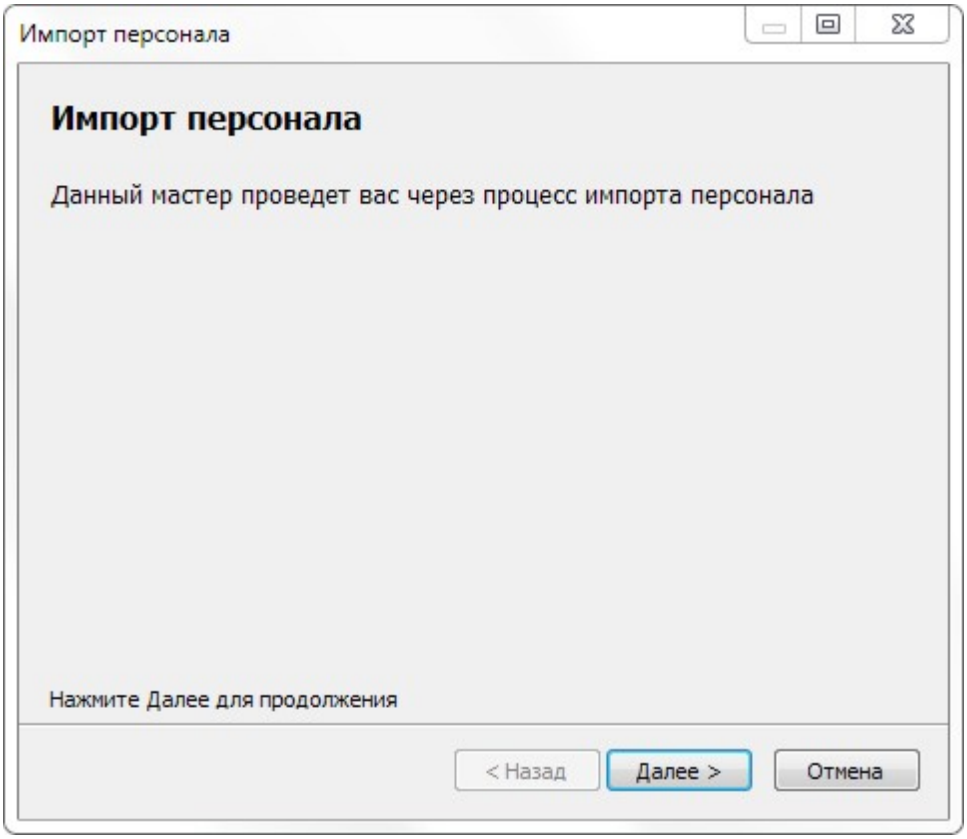
ParsecNET 3 поддерживает импорт данных в форматах XML и CSV.

Файл импорта должен содержать данные только однотипных субъектов доступа: сотрудников, посетителей или автомобилей.

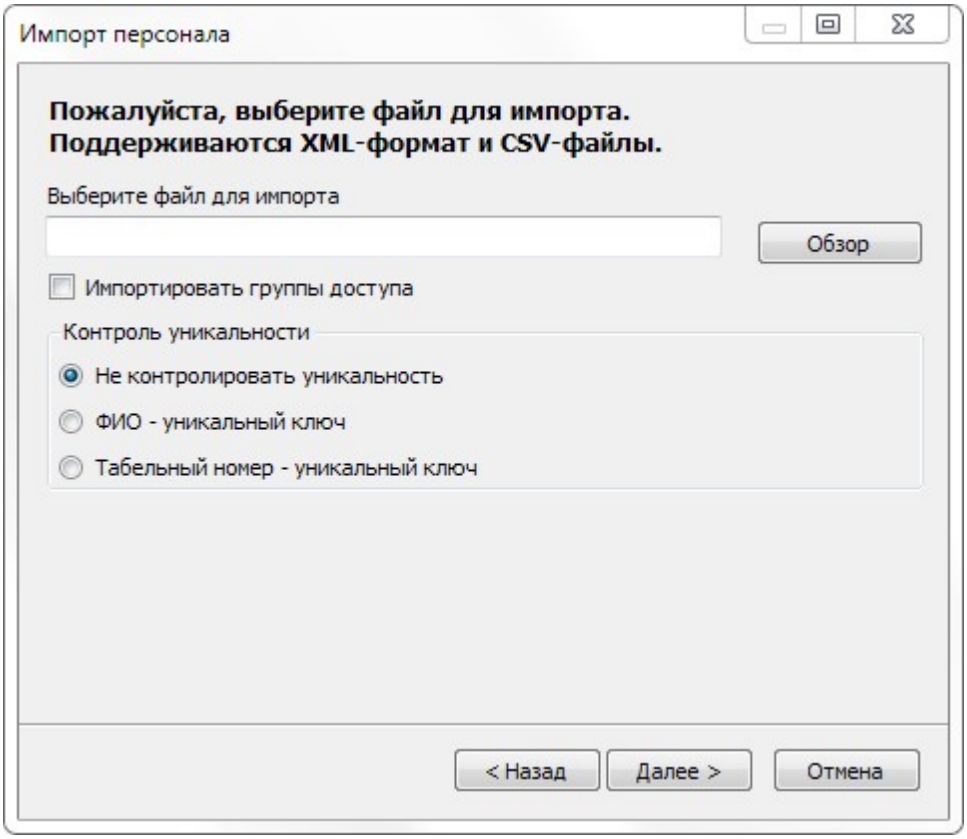
Процедуры импорта для обоих случаев описаны ниже (перейти к импорту из XML 277).

Чтобы импортировать данные в **формате CSV**, выполните следующие действия:

1. Выберите папку подразделения и нажмите на кнопку *Импорт* на панели инструментов персонала или в контекстном меню. Откроется стартовое окно мастера импорта;



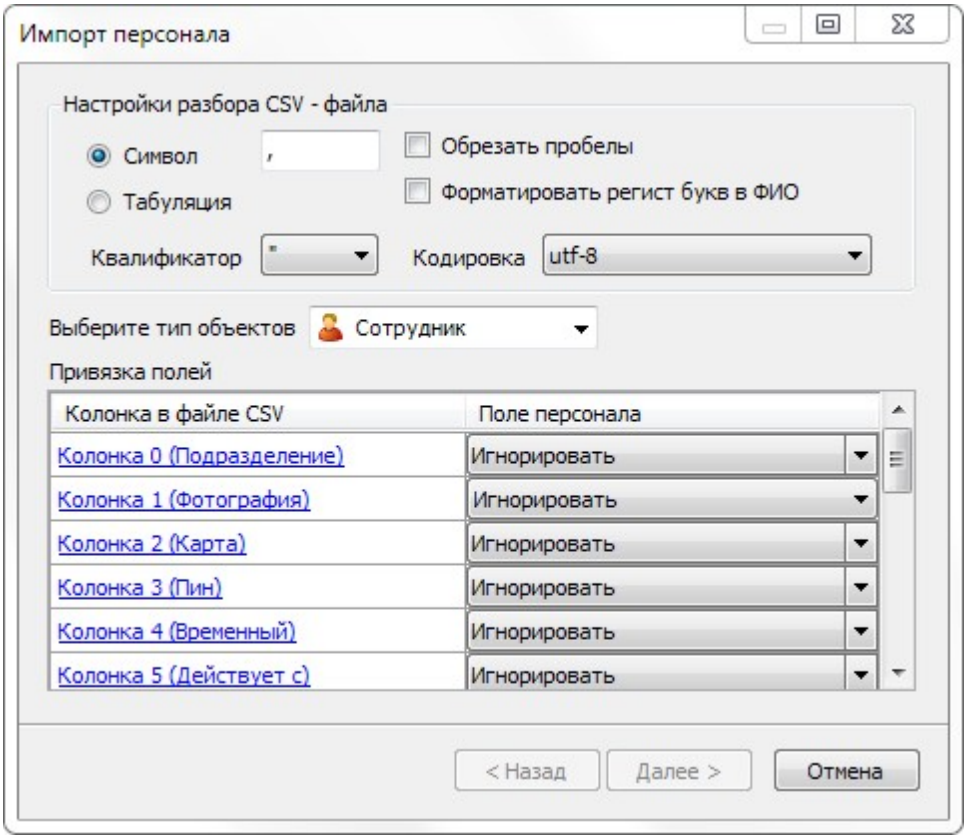
2. Нажмите на кнопку *Далее*. Откроется окно выбора файла;



3. Нажмите на кнопку *Обзор* и укажите из какого файла нужно производить импорт сведений;
4. Выберите способ контролировать уникальность импортированных записей:

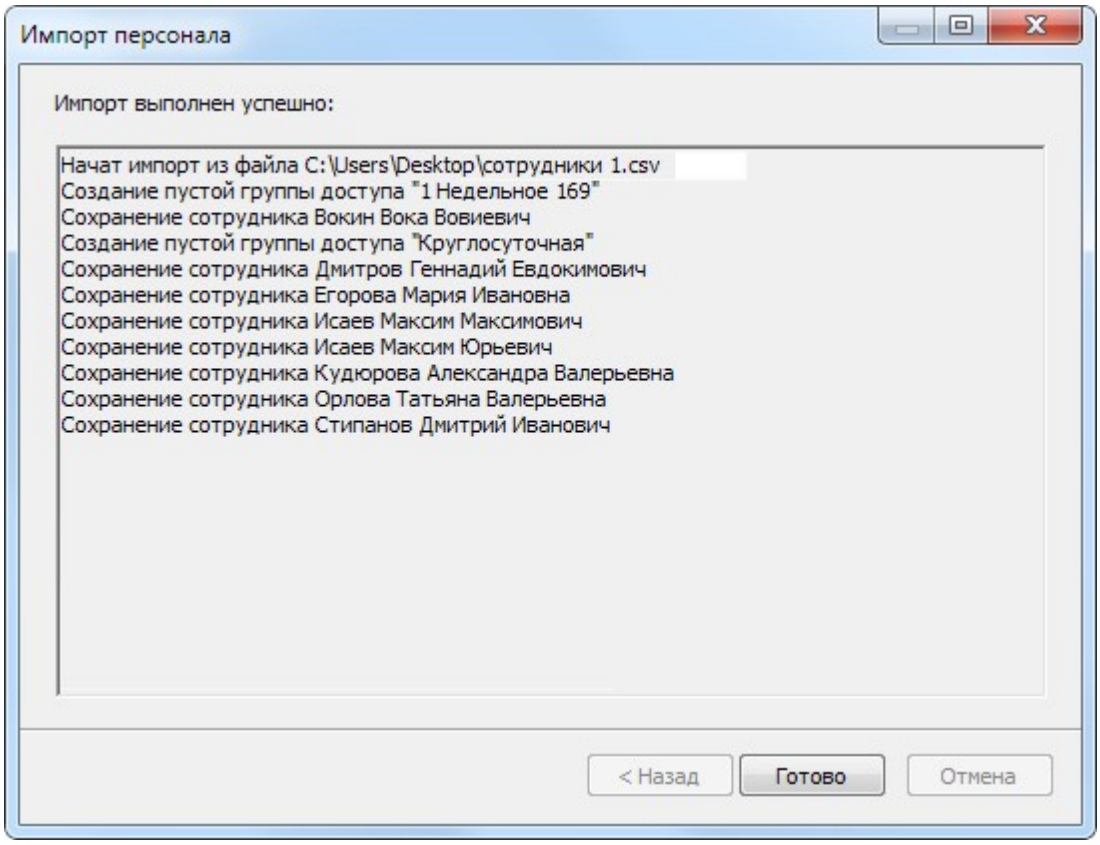
- *Импортировать группы доступа* - при установленном флажке в систему будут импортированы находящиеся в файле группы доступа. Если в системе нет группы доступа с аналогичным наименованием, то будет создана новая группа, для которой потребуется указать компоненты;
- *Не контролировать уникальность* - система импортирует все записи из файла, даже если подобные записи уже есть в системе;
- *ФИО-уникальный ключ* - система импортирует из файла первую запись с конкретными ФИО, а все последующие с такими же ФИО будут проигнорированы;
- *Табельный номер-уникальный ключ* - система импортирует из файла первую запись с конкретным табельным номером, а все последующие с таким же номером будут проигнорированы.

5. Нажмите на кнопку *Далее*. Откроется окно настройки параметров импорта;



6. Установите переключатель в значение "Символ" или "Табуляция" в зависимости от того, как разделяются значения в файле CSV. Если нужно, укажите иной символ, нежели используемая по-умолчанию запятая;
7. Если используется квалификатор, укажите какой: двойные или одинарные кавычки. Квалификатор - это символы, обрамляющие значения импортируемых данных. Обычно применяются тогда, когда значения могут содержать знаки препинания, например, в текстовых полях. Иначе система будет воспринимать все запятые как разграничения между значениями соседствующих полей данных. по-умолчанию выбраны двойные кавычки;
8. При установке флажка *Обрезать пробелы* система будет удалять пробелы между символом квалификатора и ближайшим символом значения данного. Если квалификаторы не используются, то будут удаляться пробелы между символами значения и запятыми;
9. Если установить флажок *Форматировать регистр букв в ФИО*, то текст ФИО будет написан "как в предложениях": первая буква заглавная, остальные - строчные. Если флажок не установлен, то ФИО будет импортированы так, как они записаны в файле импорта;
10. Выберите кодировку текста в файле импорта;
11. Выберите тип импортируемых субъектов доступа;

12. В таблице *Привязка полей* укажите в какие колонки системы должны импортироваться данные из колонок файла CSV. При этом обратите внимание на следующие нюансы:
    - В раскрывающемся списке отображаются все поля карточки персонала: как основные, так и дополнительные[264] . Не обязательно связывать все, но системе требуется, как минимум, указать привязку поля *Фамилия*;
    - Запись о сотруднике будет помещена в папку его подразделения, но иерархия подразделений не сохраняется. Ее необходимо будет настроить вручную;
    - Чтобы автоматически корректно импортировать изображение сотрудника в карточку субъекта, при создании файла необходимо выполнить дополнительные условия[274] ;
    - Шестнадцатиричный код идентификатора должен предоставляться в формате 0x00112233. Если он будет предоставлен в формате 00112233 (т.е. не будет иметь префикса 0x и не будет содержать букв A, B, C, D, E, F, то система при импорте распознает его как десятеричный).
13. Нажмите на кнопку *Далее*. Откроется окно и запустится процедура импорта, о завершении которой сообщит появившаяся кнопка *Готово*;



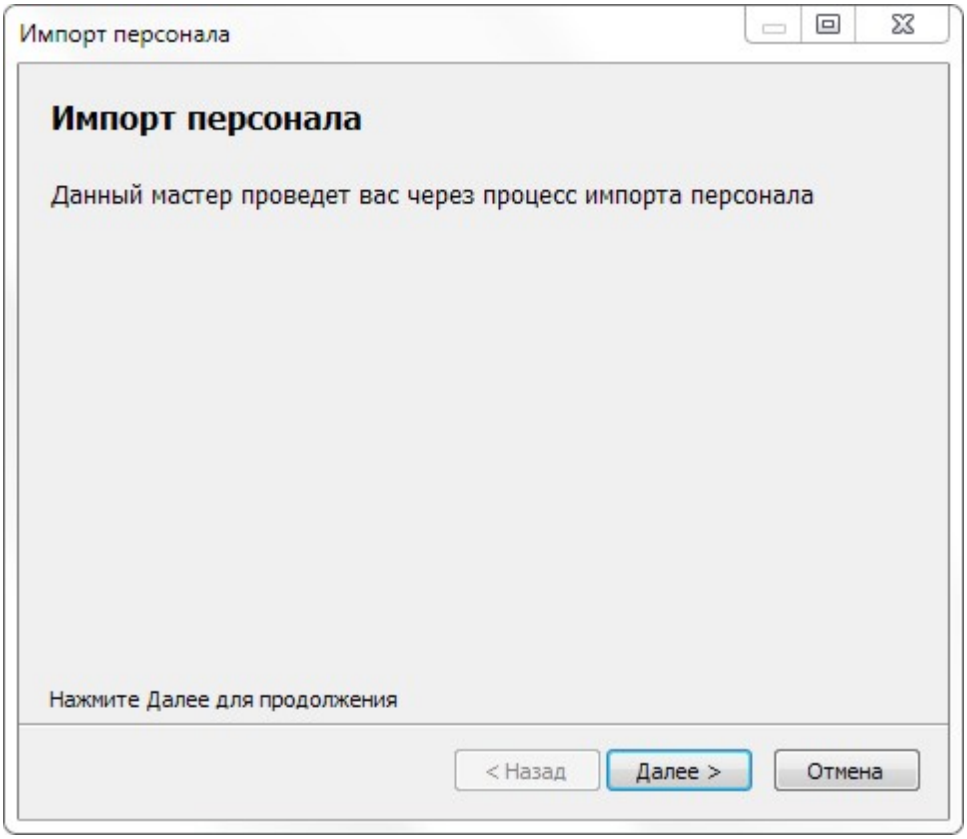
В случае возникновения ошибки импорта в этом окне будет представлено описание ошибки.

1. Для завершения процедуры нажмите на кнопку *Готово*.

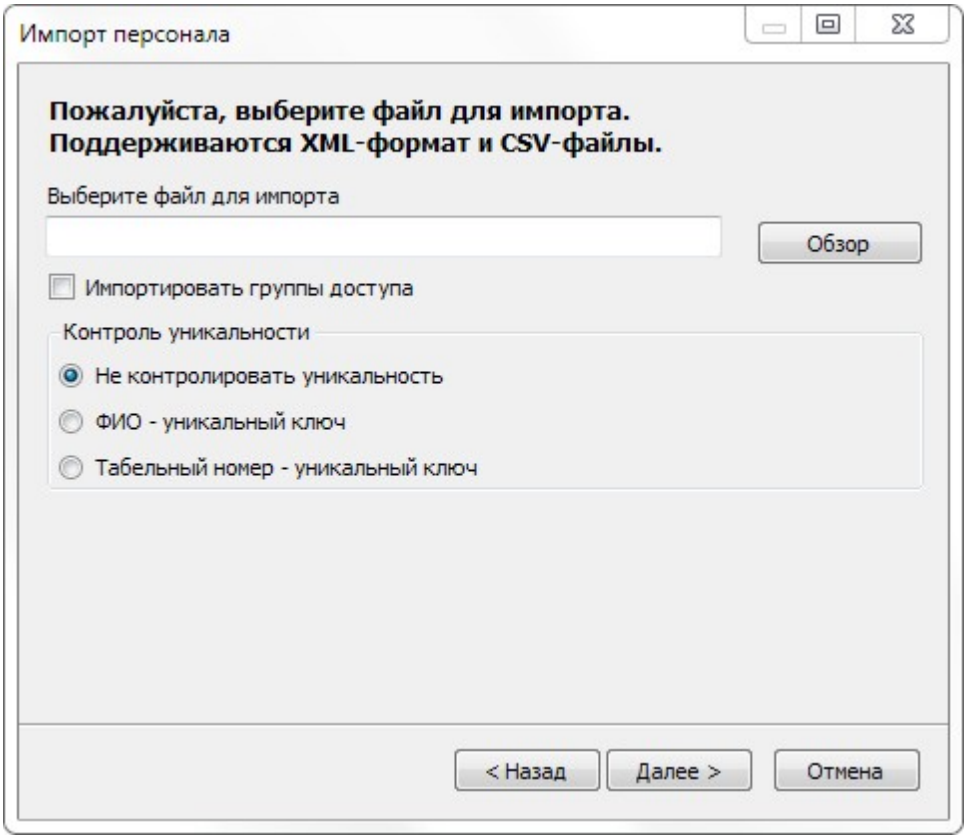
Если при импорте персонала окажется, что указанный в файле идентификатор уже принадлежит другому пользователю, то карточка субъекта доступа будет создана, но идентификатор присвоен ему не будет. Также об этом будет выдано системное сообщение.

Чтобы импортировать данные из файла **в формате XML**, выполните следующие действия:

2. Выберите пункт "Действия - Импорт" в контекстном меню или в раскрывающемся списке на панели инструментов персонала. Откроется стартовое окно мастера импорта;



3. Нажмите на кнопку *Далее*. Откроется окно выбора файла;

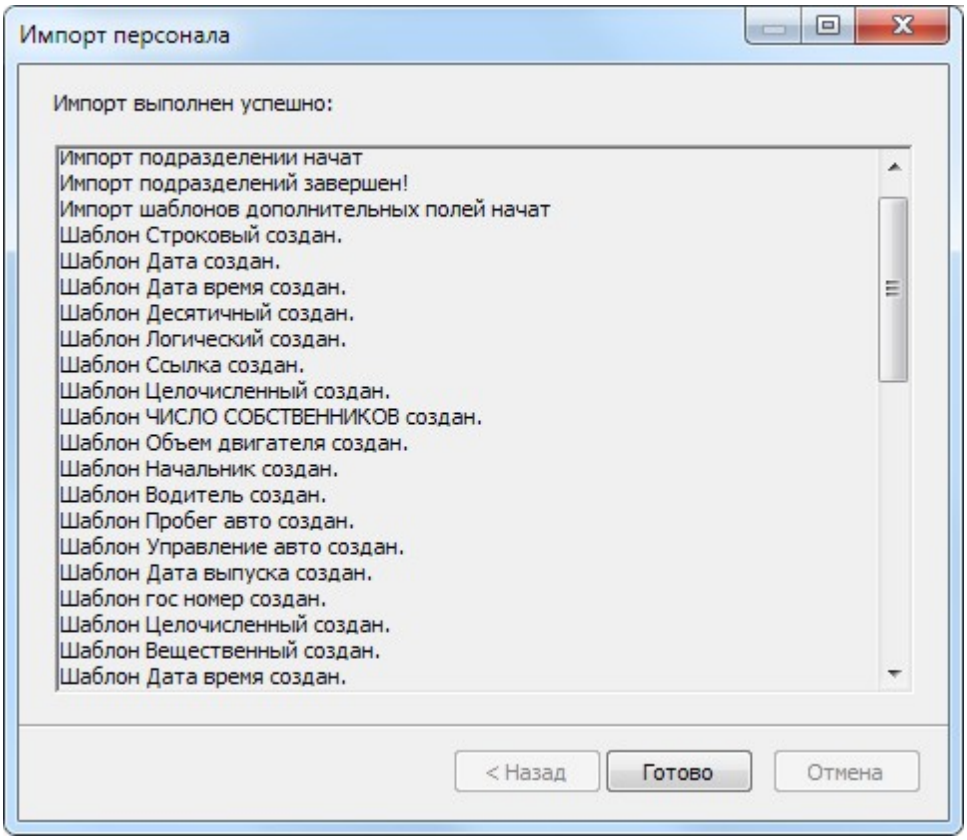


4. Нажмите на кнопку *Обзор* и укажите из какого файла нужно производить импорт сведений;
5. Выберите способ контролировать уникальность импортированных записей:
   - *Импортировать группы доступа* - при установленном флажке в систему будут импортированы находящиеся в файле группы доступа. Если в системе нет группы

доступа с аналогичным наименованием, то будет создана новая группа, для которой потребуется указать компоненты;

- *Не контролировать уникальность* - система импортирует все записи из файла, даже если подобные записи уже есть в системе;
- *ФИО-уникальный ключ* - система импортирует из файла первую запись с конкретными ФИО, а все последующие с такими же ФИО будут проигнорированы;
- *Табельный номер-уникальный ключ* - система импортирует из файла первую запись с конкретным табельным номером, а все последующие с таким же номером будут проигнорированы.

6. Откроется окно и запустится процедура импорта, о завершении которой сообщит появившаяся кнопка *Готово*;



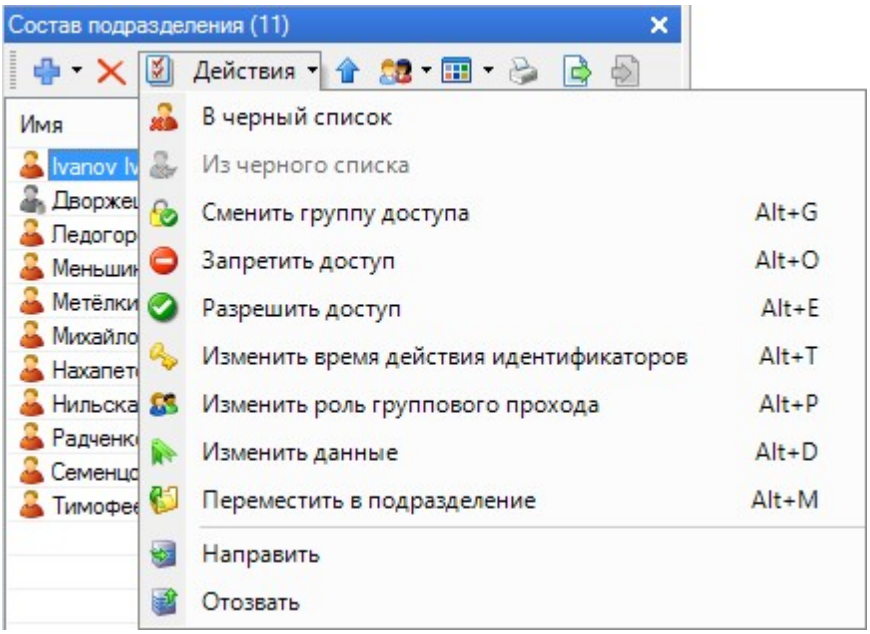
В случае возникновения ошибки импорта в этом окне будет представлено описание ошибки.

7. Для завершения процедуры нажмите на кнопку *Готово*.

8.7.6 Действия с персоналом и подразделениями

Перечень возможных действий с записью практически одинаков как для одного сотрудника, так и для нескольких или целиком подразделения. Принципиальное отличие состоит в том, что действия с папкой подразделения являются групповыми, т.е. они применяются к записям всех сотрудников, входящих в это подразделение. Естественно, к группе нельзя применить перемещение в черный список.

Список действий можно раскрыть кнопкой на панели инструментов персонала или подразделения либо через их контекстные меню.



Ниже приведены описания действий:

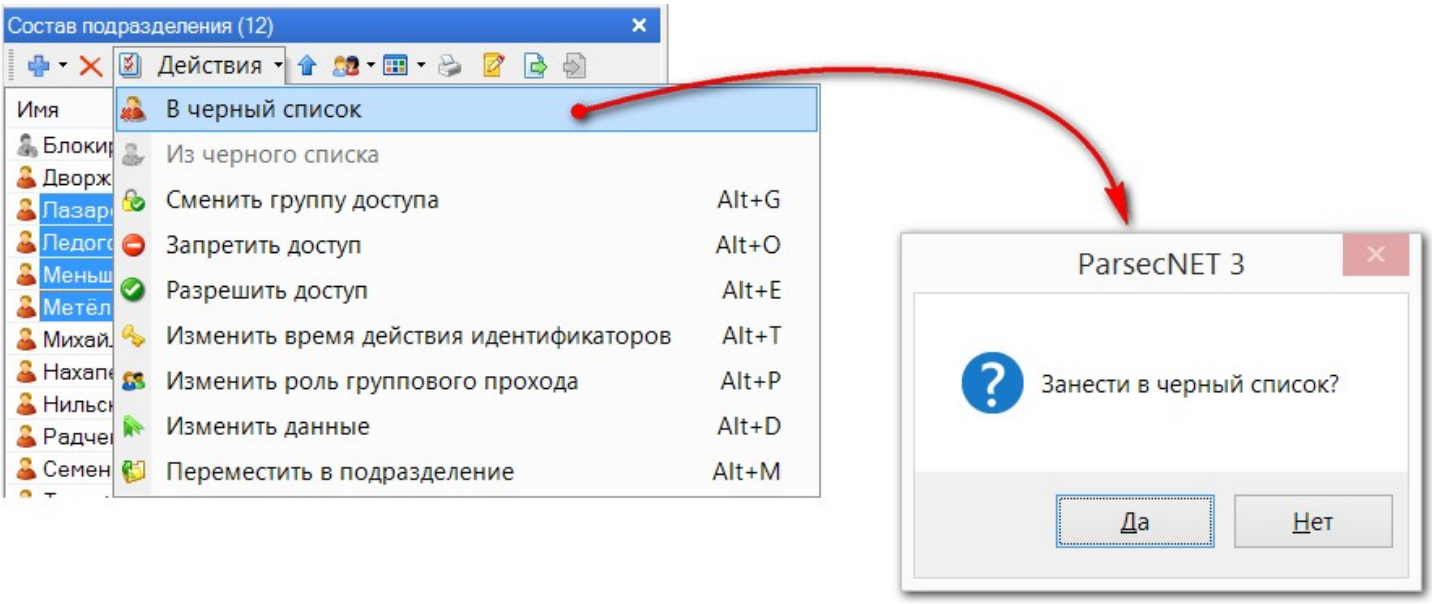
- "В черный список" - помещение субъекта доступа в черный список[280];
- "Из черного списка" - удаление субъекта доступа из черного списка[280];
- "Сменить группу доступа" - изменение[283] группы доступа;
- "Запретить доступ" - запрет прохода[281] пользователю по любому его идентификатору. Возможно помещение в черный список;
- "Разрешить доступ" - восстановление разрешения[281] пользователю на проход;
- "Изменить время действия идентификаторов" - изменение срока[284] действия временных идентификаторов;
- "Изменить роль группового прохода" - изменение[285] роли сотрудника в групповом проходе;
- "Изменить данные" - изменение[286] данных в дополнительных полях;
- "Направить" - назначение[183] совместной группы доступа первичному идентификатору сотрудника. Опция становится доступной при включении кластерного режима[164];
- "Отозвать" - удалить[186] идентификатор сотрудника с одного или всех связанных серверов. Опция становится доступной при включении кластерного режима[164];
- "Переместить в подразделение" - перемещение[286] записи(-ей) субъекта(-ов) доступа в другое подразделение.

Управление неактивными идентификаторами и субъектами доступа осуществляется посредством скрипта[333], выполняемого в рамках созданного задания[322].

8.7.6.1 Управление черным списком

Помещение субъекта доступа в черный список приводит к тому, что его данные будет нельзя редактировать (например, выдать ему новый идентификатор для прохода). Однако, выданные ему ранее идентификаторы сохранять останутся в силе. Поэтому, чтобы запретить такому субъекту передвижение по территории, необходимо перед занесением в черный список удалить или заблокировать все его идентификаторы.

Чтобы перенести один или несколько субъектов доступа в черный список, выделите их в редакторе персонала и выберите пункт "Действия - В черный список". Подтвердите действие в появившемся окне запроса:



После перемещения в черный список значок субъекта становится серым.

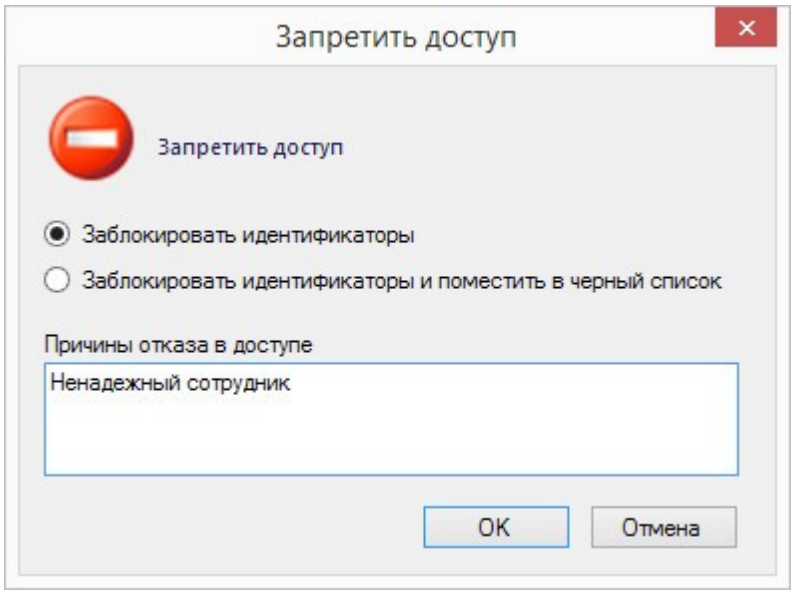
Для удаления субъекта доступа из черного списка выберите его и выберите пункт "Действия - Из черного списка". Подтвердите действие в появившемся окне запроса.

8.7.6.2 Запрет и разрешение доступа

Система ParsecNET 3 предоставляет возможность запретить доступ как отдельным пользователям, так и целым подразделениям. Для этого применяется функция "Запретить доступ".

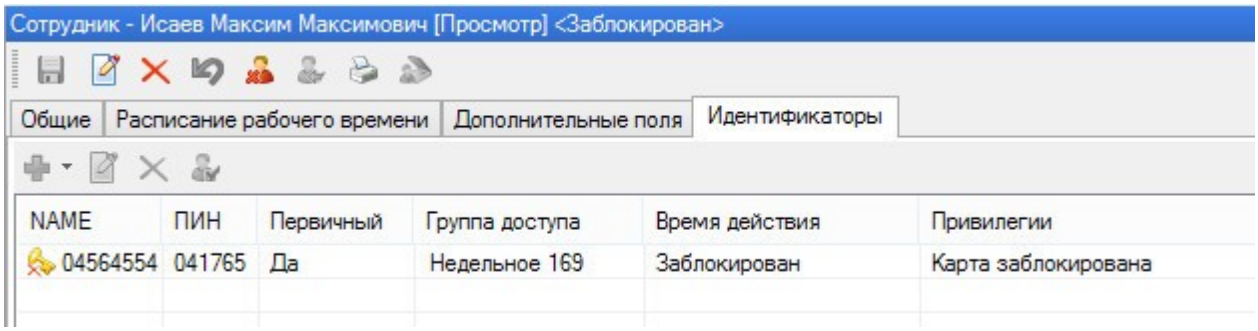
Для запрета доступа выполните следующие действия:

1. Выберите одну или несколько записей пользователей, либо папку подразделения, для персонала которого нужно запретить доступ;
2. Выберите пункт "Действия - Запретить доступ" в контекстном меню или в раскрывающемся списке на панели инструментов персонала. Откроется диалоговое окно *Запретить доступ*;
3. Установите переключатель:
   - "Заблокировать идентификаторы" - будет запрещен проход по всем идентификаторам выбранных пользователей. Запрет обратим;
   - "Заблокировать идентификаторы и поместить в черный список" - выбранные пользователи помещаются в черный список, идентификаторы блокируются, но могут быть использованы впоследствии для новых карт. Если пользователи будут удалены из черного списка, то им, вероятно, нужно будет назначить новые идентификаторы.
4. В текстовом поле, при необходимости, введите причины, по которым доступ запрещен;
5. Нажмите на кнопку *ОК*. Система произведет необходимые действия, и выбранные пользователи теперь не смогут пройти через точки прохода при помощи своих карт.



В случае блокировки идентификаторов в карточке сотрудника на вкладке *Идентификаторы* появятся отметки:

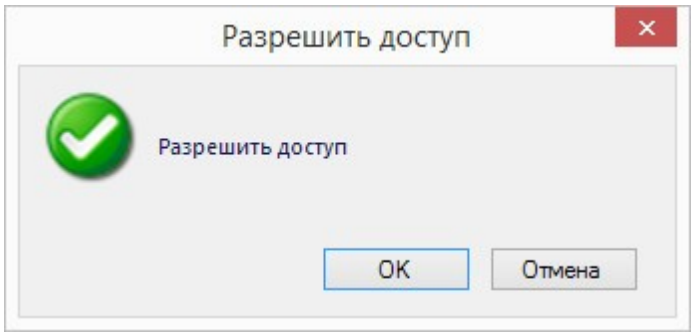
- в колонке "Время действия" - Заблокирован;
- в колонке "Привилегии" - "Карта заблокирована".



В карточках заблокированных субъектов доступа у всех идентификаторов имеются флажки[263] *Вход запрещен* и *Выход запрещен*. При помощи манипуляций с этими флажками каждому из заблокированных субъектов доступа блокировку можно снять полностью (и на вход, и на выход) или частично, для одного или нескольких идентификаторов.

В любом случае пользователям можно снова разрешить проход. Для этого выполните шаги:

1. Выделите пользователя или папку подразделения и выберите пункт "Действия - Разрешить доступ";
2. Нажмите на кнопку *OK* в окне запроса подтверждения.



Если у пользователя идентификатор был заблокирован, то он разблокируется и его можно будет использовать дальше.

Если во время пребывания в черном списке идентификаторы субъекта были использованы для другого субъекта, то при восстановлении из черного списка субъекту будет необходимо присвоить новый идентификатор, распечатать и выдать карту, а также, возможно, подписать новое соглашение об обработке персональных данных.

Снятие блокировки картой оператора

Если идентификатор субъекта доступа был заблокирован, то его можно восстановить при помощи идентификатора, имеющего привилегию "Управление доступом". Для этого необходимо создать задание[322] с указанием следующих параметров:

- тип запуска - "По событию устройства";
- выберите одну точку прохода;
- выберите всех сотрудников, чьи карты должны разблокировываться этим способом;
- на вкладке *События* установите флажки:
  - *Нет доступа по блокировке*;
  - *Нет входа - режим блокировки*;
  - *Нет выхода - режим блокировки*;
  - *Доступ предоставлен*;
  - *Нет входа - карта в черном списке (блокирована)*;
  - *Нет выхода - карта в черном списке (блокирована)*.
- исполняемые действия - "Выполнить код". Укажите для выполнения скрипт "AccessControl_ActivateBlockedCardByOperator" из папки "..\Program Files\MDO\ParsecNET 3\Scripts".

После успешной компиляции скрипта нажмите на кнопку *ОК* и введите логин и пароль оператора, имеющего привилегию "Управление доступом".

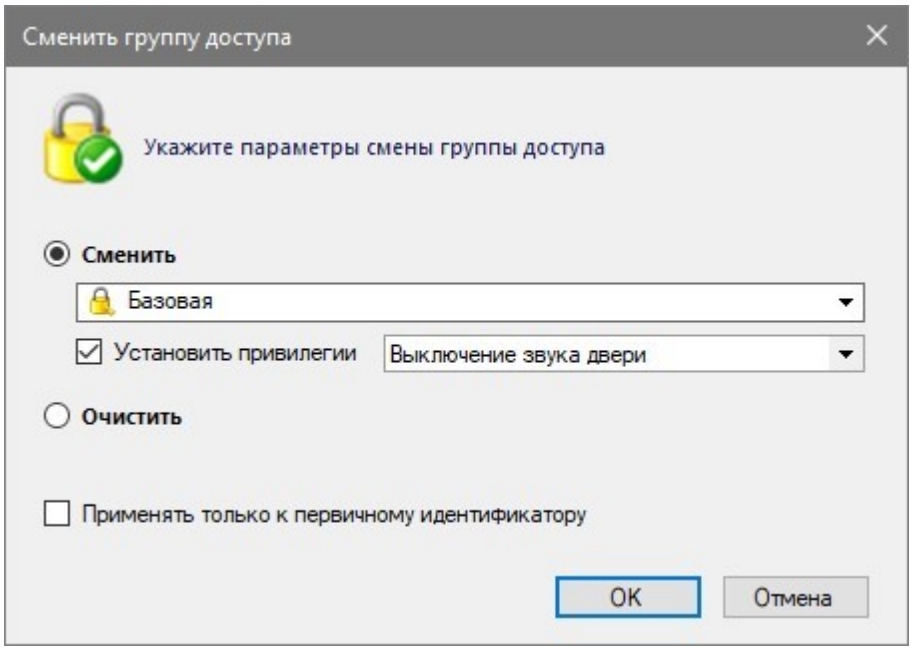
После того, как задача будет создана, оператор с данной привилегией, сможет снимать блокировку карты субъекта доступа, используя считыватели выбранной точки доступа. Для этого первым к считывателю подносится заблокированный идентификатор, а затем, не позже 15 секунд, - идентификатор с привилегией "Управление доступом".

При этом разблокируется не только поднесенный идентифкатор, но и все ранее заблокированные идентификаторы этого субъекта .

8.7.6.3 Изменение группы доступа

Система ParsecNET 3 предоставляет возможность переназначить группу доступа у идентификаторов выбранных субъектов доступа или подразделений.

Для этого выделите субъектов доступа или папку подразделения и выберите пункт "Действия - Сменить группу доступа". Откроется окно:



Выберите новую группу доступа и, если необходимо, привилегии.

Если флажок «Установить привилегии» снят, текущие привилегии идентификаторов сохранятся.

По завершении настроек нажмите на кнопку *OK*. Выбранному субъекту доступа или подразделению будет назначена новая группа доступа и/или привилегии.

При выборе значения "Очистить" группы доступа у субъектов будут удалены. Обратите внимание, без группы доступа проход через точки прохода будет невозможен.

При установке флажка «Применять только к первичному идентификатору» выбранное действие (Сменить или Очистить) будет применено только к первичному идентификатору субъектов. Остальные идентификаторы останутся без изменений.

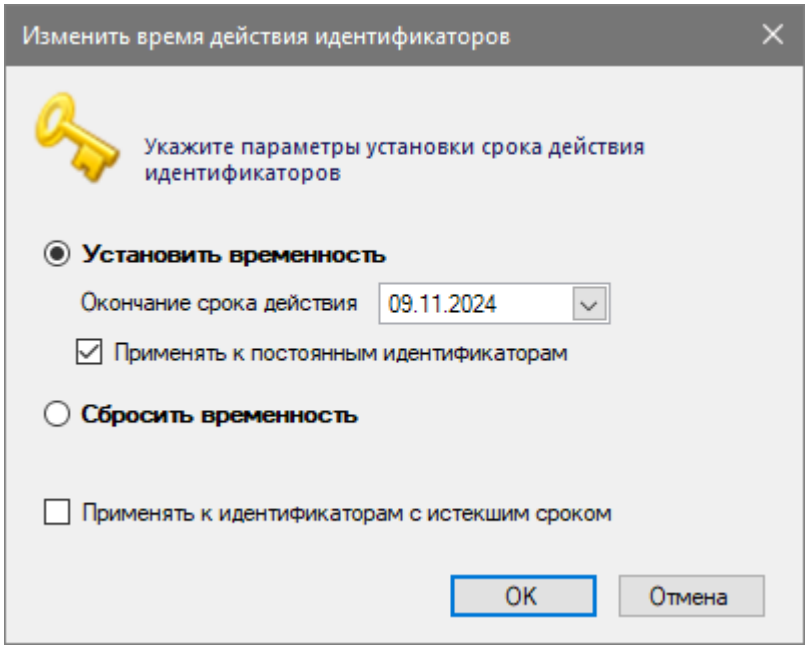
8.7.6.4 Изменение времени действия идентификаторов

Для изменения времени действия временных идентификаторов выполните следующие действия:

1. Выберите одну или несколько записей субъектов, либо папку подразделения, для субъектов которого нужно изменить срок действия идентификаторов;
2. Выберите пункт "Действия - Изменить время действия идентификаторов" в контекстном меню или в раскрывающемся списке на панели инструментов персонала. Откроется диалоговое окно;
3. В раскрывающемся календаре выберите дату, до которой должны действовать идентификаторы. Установкой даты можно как продлить, так и сократить время действия идентификатора. Даже можно отменить действующие идентификаторы, указав прошедшую дату;
4. При установке флажка "Применять к постоянным идентификаторам" те идентификаторы, которые не имели окончания срока действия, станут временными со сроком действия до указанной даты;
5. Нажмите на кнопку *OK*. Срок действия временных идентификаторов у выбранных субъектов будет установлен до указанной даты.

При выборе значения «Сбросить временность», текущие временные идентификаторы станут постоянными. То есть не будут иметь срока действия.

При установке флажка "Применять к идентификаторам с истекшим сроком" выбранное действие («Установить временность» или «Сбросить временность») будет применено так же к идентификаторам, срок действия которых истек.

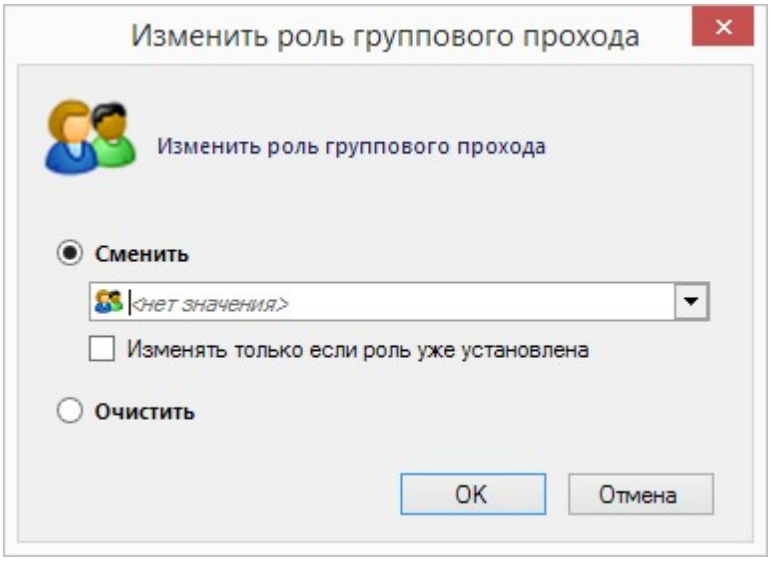


8.7.6.5 Изменение роли группового прохода

Список ролей для групового прохода[115] создается в редакторе оборудования[115].

При занесении сотрудника в БД ParsecNET 3, ему может быть назначена[263] какая-то из этих ролей.

Впоследствии роль можно сменить у одного или у группы сотрудников при помощи команды "Изменение роли группового прохода" меню *Действия* редактора персонала.



Если выбрана операция *Сменить*, выберите нужную роль из раскрывающегося списка.

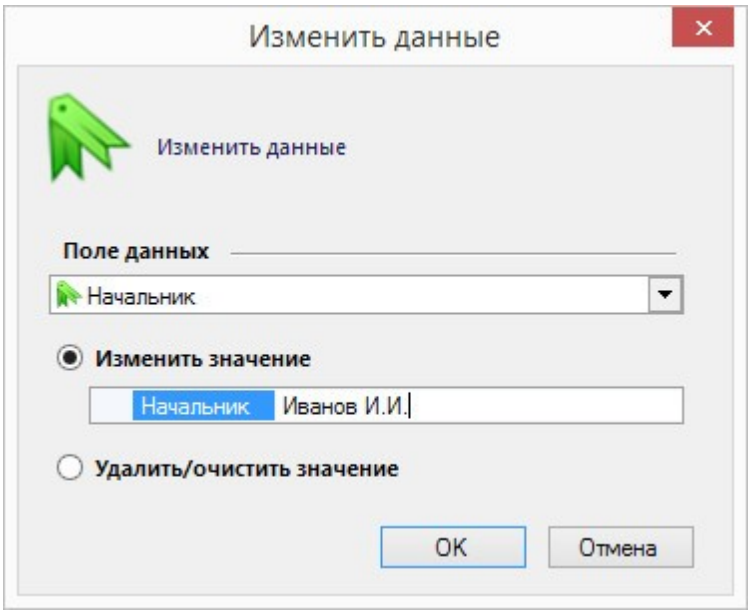
Установка флажка приведет к смене ролей только у тех сотрудников, которым ранее уже была назначена какая-то роль. В противном случае, выбранная из списка роль будет назначена всем сотрудникам, с которыми производится это действие.

Выбор операции *Очистить* приведет к удалению ролей у всех обрабатываемых записей сотрудников.

8.7.6.6 Изменить данные

Система позволяет изменить значения дополнительных полей данных. Особенно удобно это для группового ввода/изменения данных, например, изменения в карточках сотрудников адреса подразделения или фамилии руководителя.

Для изменения значения данного выделите один или несколько субъектов доступа и выберите пункт "Действия - Сменить группу доступа". Откроется окно:



Выберите поле, нуждающееся в изменении, в раскрывающемся списке *Поле данных*.

Установите переключатель в одно из двух положений:

- "Изменить значение" - значение поля у выбранных субъектов будет заменено значением, введенным в этом поле;
- "Удалить/очистить значение" - старое значение будет удалено. Поле будет пустым.

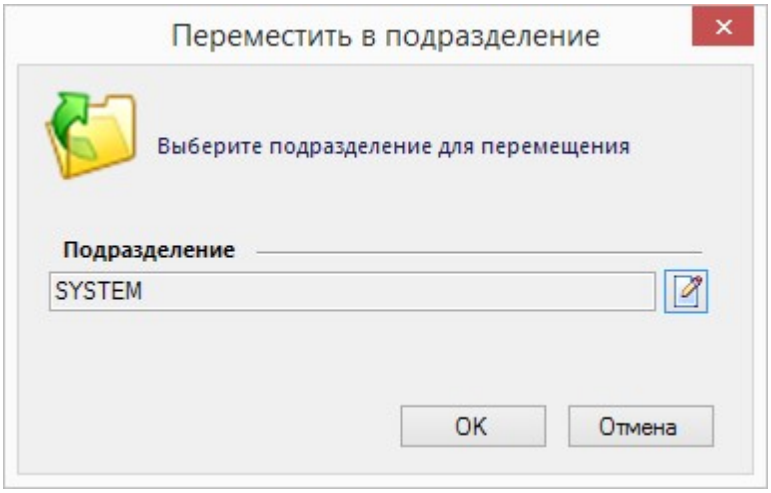
Нажмите на кнопку *OK*. Система выполнит заданные действия.

8.7.6.7 Переместить в подразделение

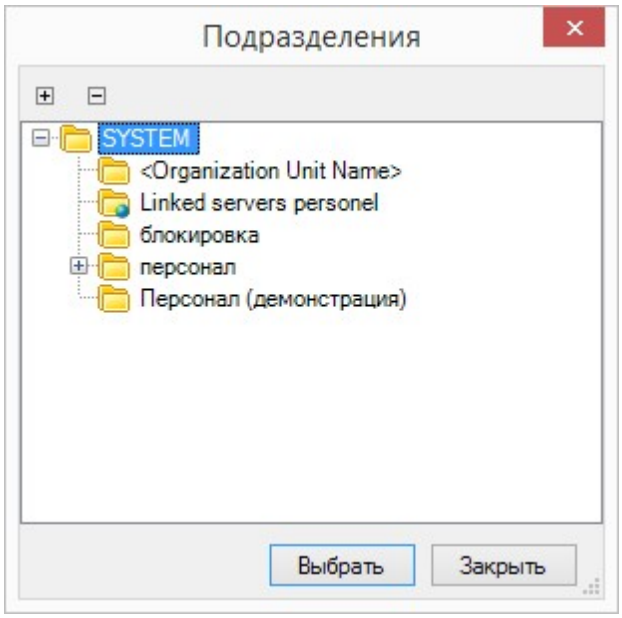
Данная команда позволяет переместить выбранный субъект доступа или группу субъектов доступа в существующее подразделение.

Для перемещения выполните следующие шаги:

1. В редакторе персонала выделите один или группу субъектов доступа (можно использовать клавиши Shift и Ctrl). Также можно сформировать список на перемещение, воспользовавшись функцией поиска[56];
2. Откройте список *Действия* и выберите команду "Переместить в подразделение". Откроется окно:



3. Нажмите на кнопку  . Откроется окно:



4. Выберите подразделение, в которое необходимо переместить субъектов доступа и нажмите на кнопку *Выбрать*;
5. Нажмите на кнопку *ОК* в первом открывшемся окне.

Выбранные субъекты доступа будут перемещены в указанное подразделение.

8.8 Монитор событий

Общие положения

Монитор событий предназначен для наблюдения за состоянием системы и событиями в реальном времени, а также прямого управления оборудованием. Вот некоторые из особенностей монитора событий:

- Возможность иметь несколько панелей событий с различными фильтрами в рамках одного монитора событий;
- Возможность одновременной работы с несколькими мониторами на одном ПК, в том числе в многомониторной системе, если это поддерживается видео картой ПК;
- Гибкая настройка фильтров событий для каждой панели и/или окна монитора;
- Временная "заморозка" окна событий для тщательного анализа конкретного события;
- Расширенная поддержка анимированных графических планов;
- Постоянный контроль статуса выбранных устройств в панели статуса;
- Возможность создания пользовательских команд для выбранных единиц оборудования с назначением отдельной кнопки в панели инструментов с выбранной пользователем пиктограммой;
- Оперативный отчет по любому выбранному объекту системы;
- Возможность использования в рамках одного монитора нескольких панелей видеоверификации с индивидуальными настройками;
- Интеграция с системами видео наблюдения (связка событий с видео, просмотр видео, как в реальном времени, так и ретроспективный по связке с событием);

- Подсчет количества входов и выходов (только для контроллера NC-8000).

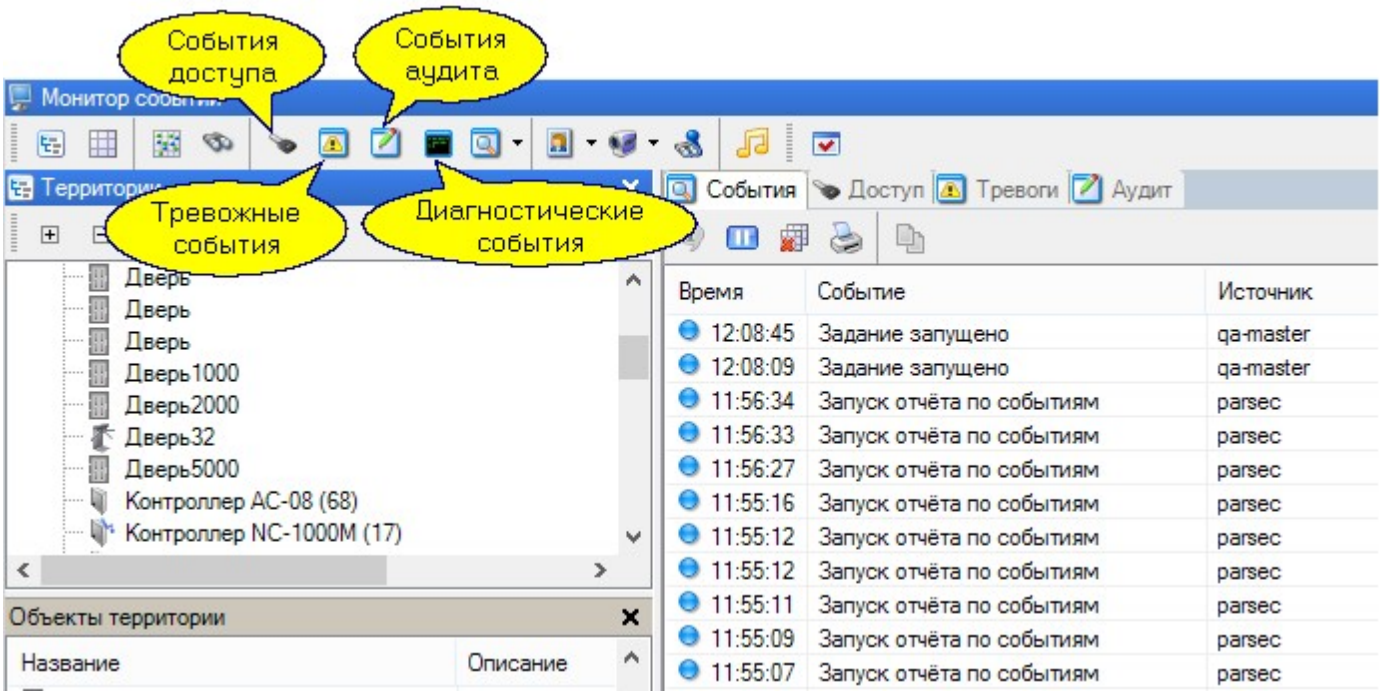
Панели монитора

Монитор событий содержит три основные панели:

- *Территории* - отображает дерево территорий организации;
- *Объекты территории/Состояние* - при позиционировании в дереве на территории отображает список ее объектов, при позиционировании в дереве на оборудовании показывает статус компонентов этого оборудования;
- Панель с 4 вкладками, на которых, в зависимости от категории, отображаются события:
  - *Доступ* - вкладка активна по-умолчанию после установки системы;
  - *Тревоги*. Если вкладка тревожных событий отсутствовала на панели, то с приходом тревоги оно может автоматически активироваться (опция указывается в настройках списка);
  - *Аудит*. В карточке субъекта доступа на вкладке *Аудит изенений* отображаются все события из категории "Аудит изменений", относящиеся к данному субъекту;
  - *Диагностика*.

  Для указанных вкладок список отображаемых событий (фильтрация событий) жестко фиксирован и не может изменяться пользователем (на вкладке *Фильтр* окна настроек изменения невозможны). Но для вкладок можно настроить колонки табличной части и особые для каждой вкладки параметры.

  На следующем рисунке показаны кнопки, с помощью которых открываются соответствующие вкладки:



Если вкладки с предопределенными событиями вас не устраивают, можно открыть дополнительные окна с событиями и настроить каждое из них (см. параграф ниже).

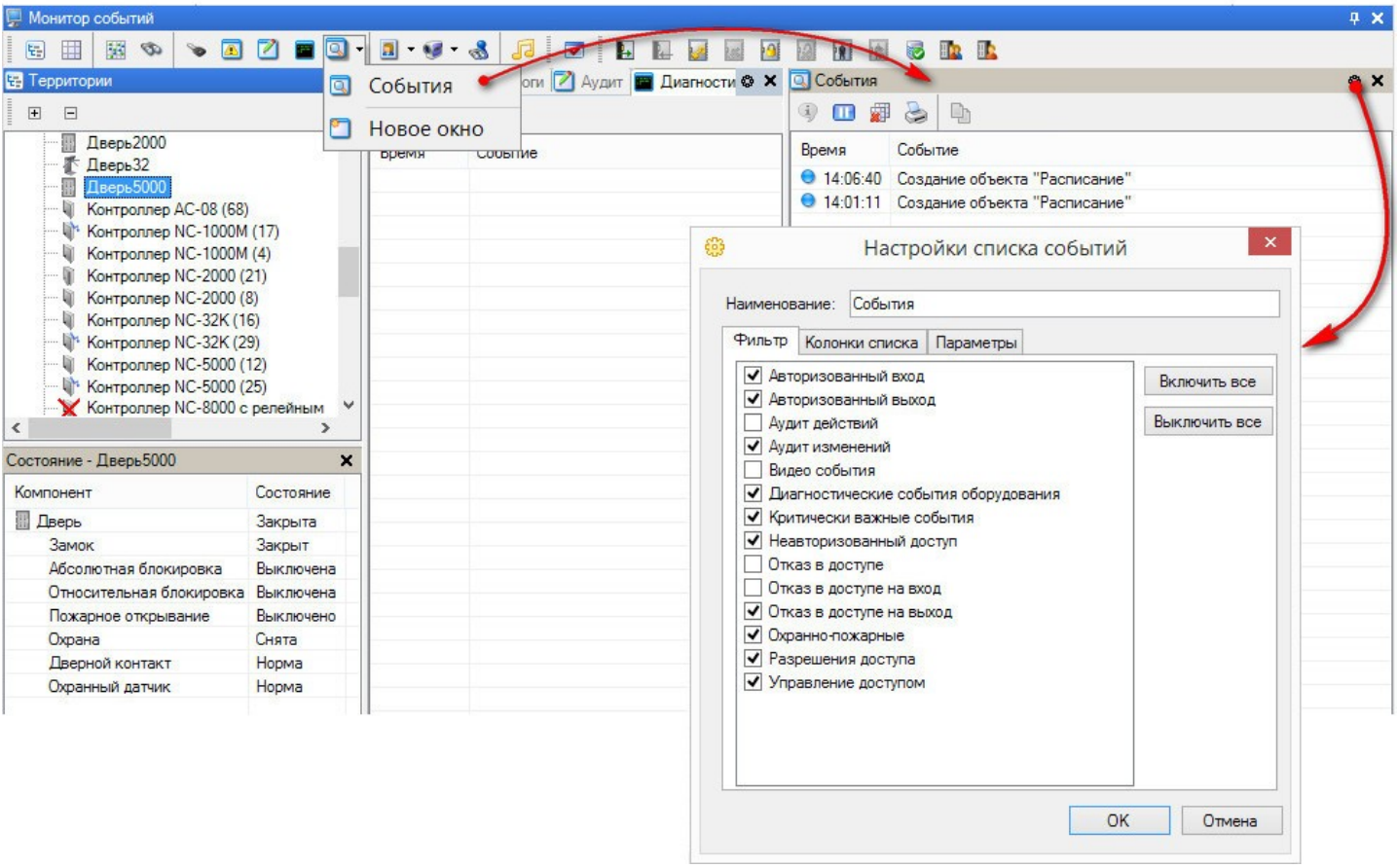
Кроме этого, в консоли монитора можно использовать следующие панели[291] :

- *Граф план;*
- *Поиск персонала;*
- *Видеоверификация* (если приобретена лицензия на данный модуль[506]);

- *Видеонаблюдение* (если приобретена лицензия на данный модуль[515]);
- *Количество людей в помещении.*

Настройка списка событий

Отображаемые монитором события можно гибко настраивать (фильтровать) в соответствии с задачей, которая выполняется на конкретном рабочем месте. Более того, в рамках одного окна монитора событий можно организовать несколько дополнительных окон с событиями, и каждое окно настроить на отображение своего списка событий: в одном можно показывать авторизованные проходы, в другом - события от оборудования и так далее:

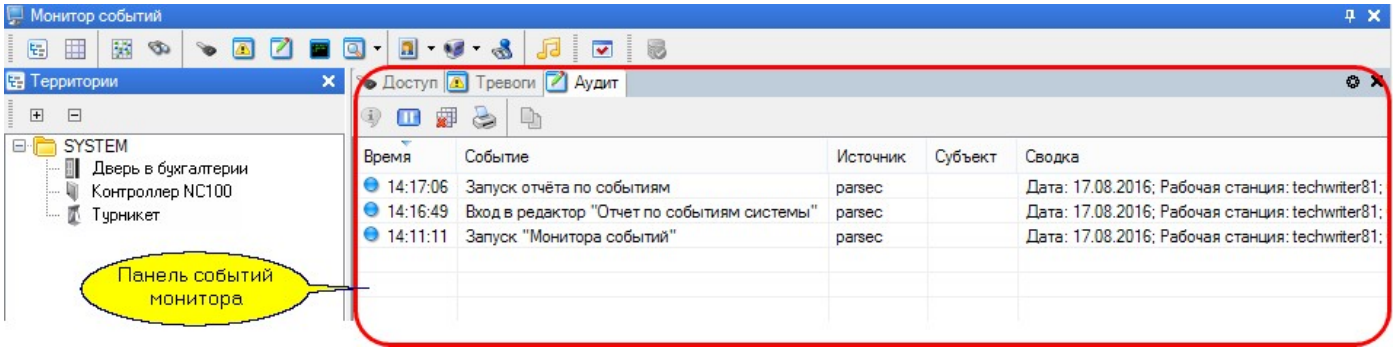


Окно *Настройки списка событий* имеет три вкладки:

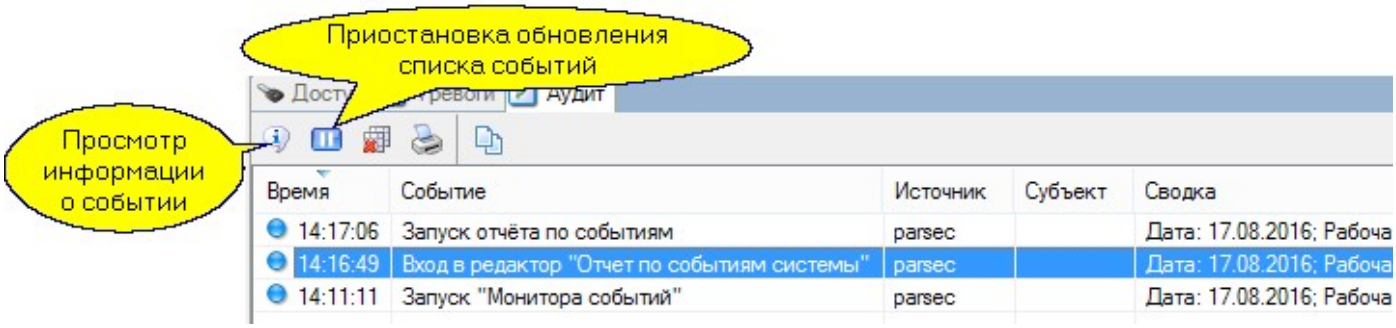
- *Фильтр* - настройка типов событий (на уровне категорий), которые будут отображаться в списке событий. по-умолчанию отображаются все категории событий;
- *Колонки списка* - определение набора колонок (по-умолчанию изначально показываются все колонки). Здесь же можно определить порядок колонок в списке;
- *Параметры* - устанавка максимального количества событий в списке, по достижении которого старые события будут вытесняться из списка (естественно, они сохранятся в базе данных транзакций системы). Кроме того, если вы включаете приостановку прокрутки событий, чтобы рассмотреть что-то более детально, можно настроить интервал времени, после которого прокрутка автоматически включится (чтобы случайно не остановить монитор событий на постоянно).

Просмотр данных и связанных данных события

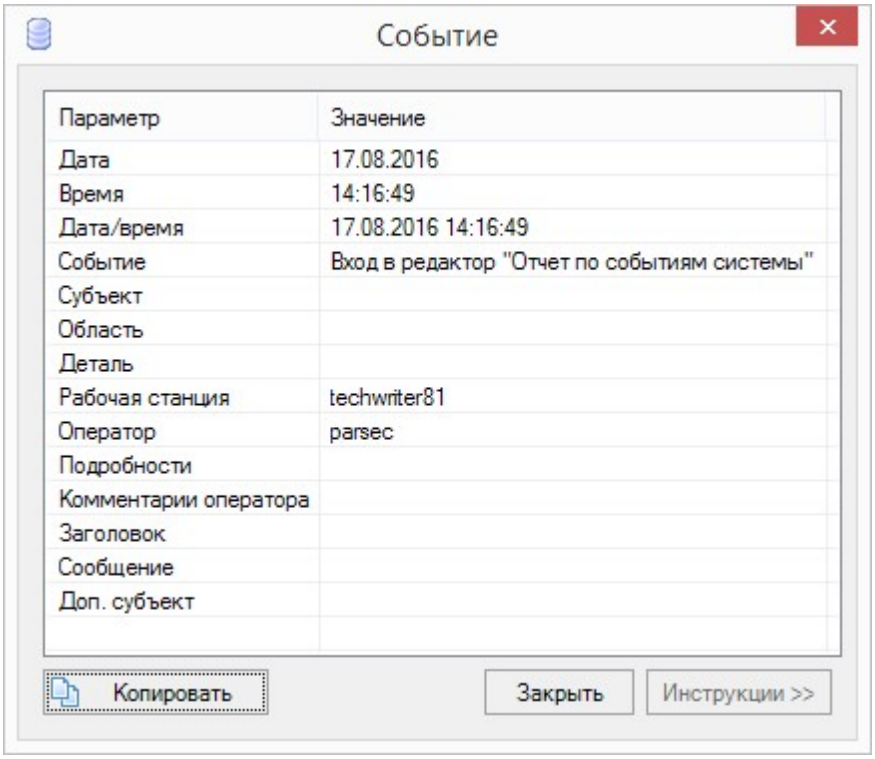
Текущие транзакции системы отображаются на панели событий, пример которой показан ниже:



Предположим, при интенсивно поступающих сообщениях, чтобы детально изучить какое-то конкретное событие, требуется приостановить обновление списка. Для этого нажмите на кнопку *Пауза*, и список не будет обновляться в течении времени, заданного в конфигурации панели. Для детального просмотра всех параметров события выделите его, а затем дважды щелкните по нему или нажмите на кнопку просмотра информации:

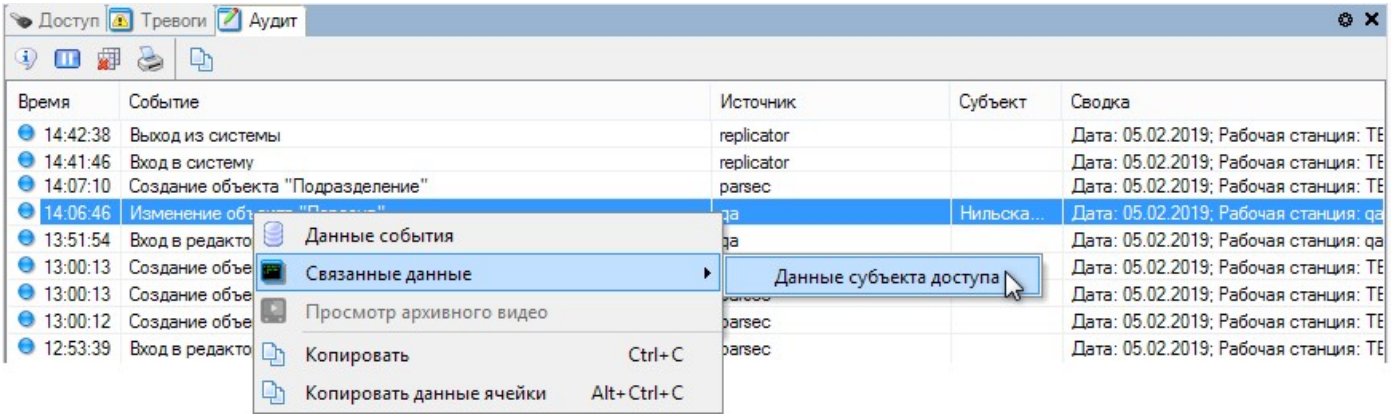


В результате появится диалог примерно следующего вида:

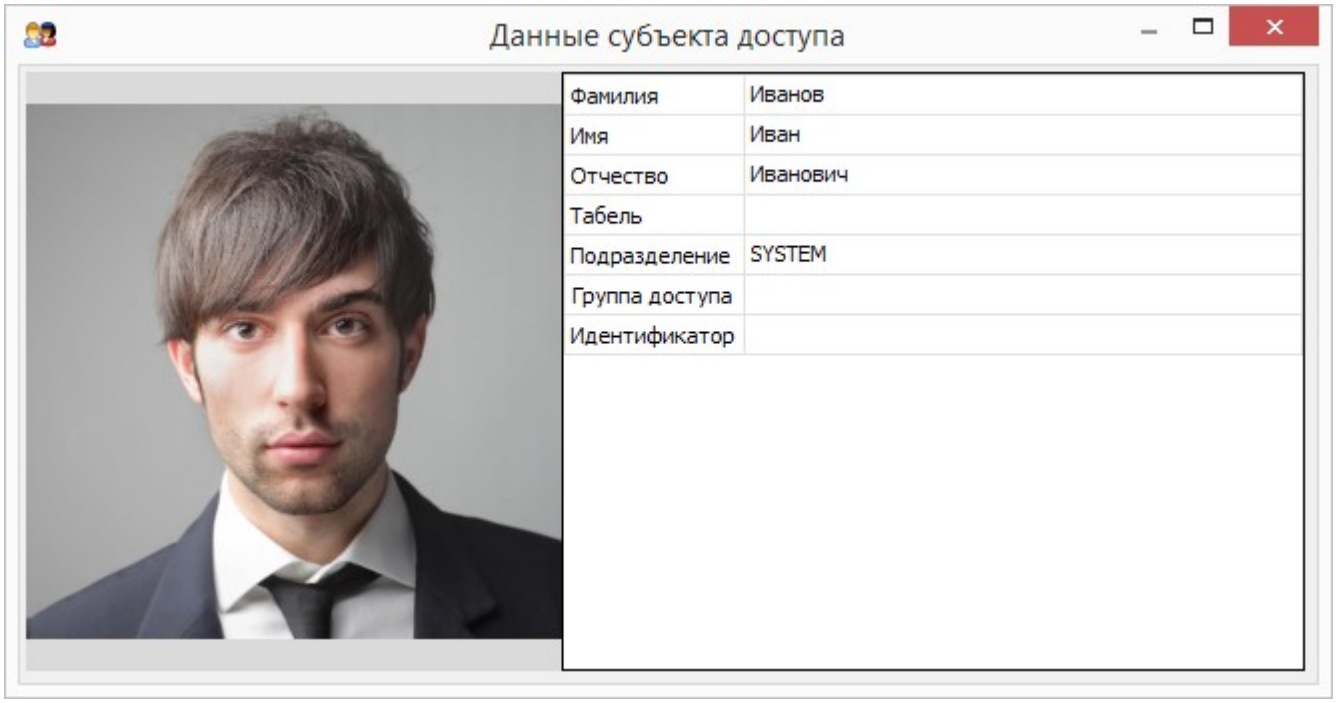


Для связанных событий также будет присутствовать ссылка на связанное событие (например, ссылка на снимок с камеры, произведенный по данному событию). Связанные данные можно просмотреть для любого события в панелях монитора и в отчетах по событиям системы. В зависимости от типа события это может быть карточка сотрудника, снимок с видеокамеры, видеофрагмент и так далее.

Для просмотра связанных с событием данных вызовите контестное меню и выберите пункт "Связанные данные", а в подпункте - интересующие вас данные, как показано на рисунке:



Для нашего примера будет показана карточка сотрудника примерно такого вида:



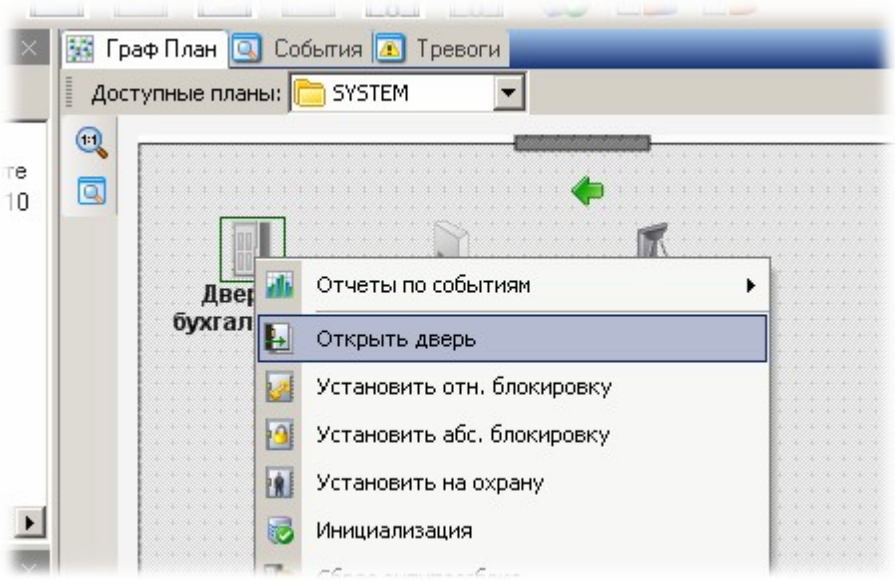
Обратите внимание, команда *Копировать* копирует всю выделенную строку, а команда *Копировать данные ячейки* копирует данные выделенной ячейки в том столбце, в котором находится курсор мышки.

8.8.1 Особые панели монитора событий

Графические анимированные планы

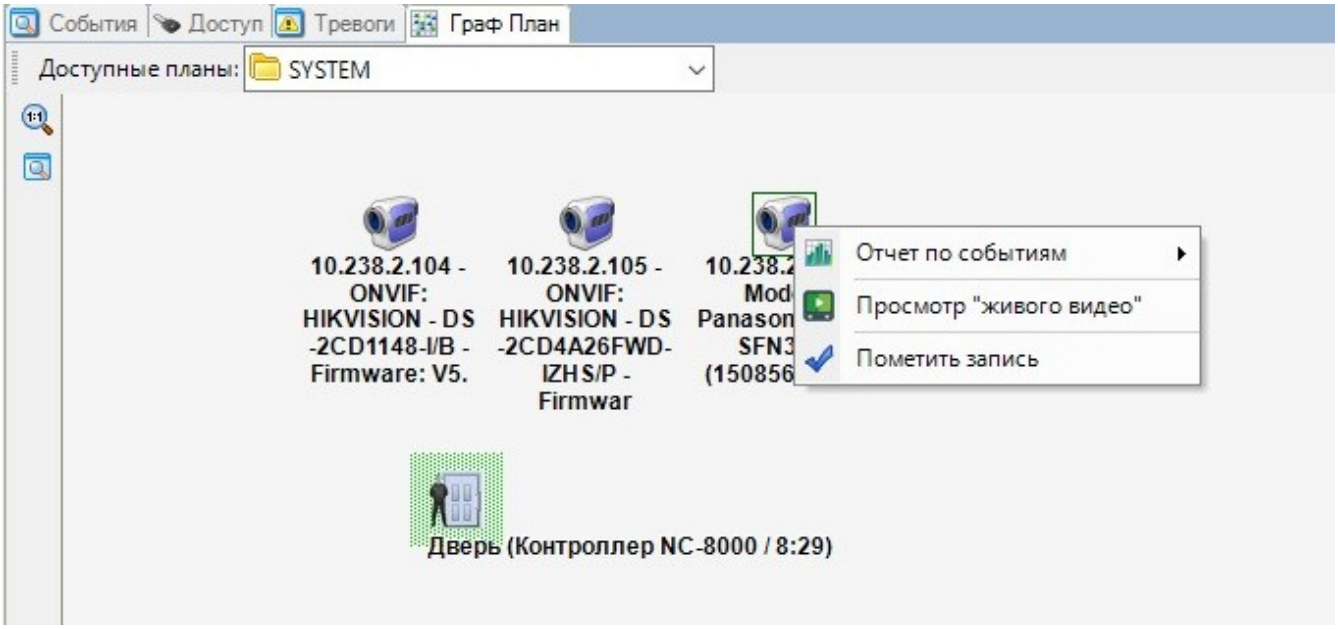
Графические планы иногда дают более наглядное представление об объекте мониторинга, чем обычный список событий - все зависит от выполняемой данным оператором работы. Графический план позволяет наблюдать за состоянием объектов территории, получать по ним отчеты и осуществлять прямое управление с помощью контекстного меню.

Графические планы создаются в Редакторе топологии[203]. Ниже показан пример простого графического плана с контекстным меню управления объектом "Дверь в бухгалтерию":



На графический план можно наносить[208] следующие элементы:

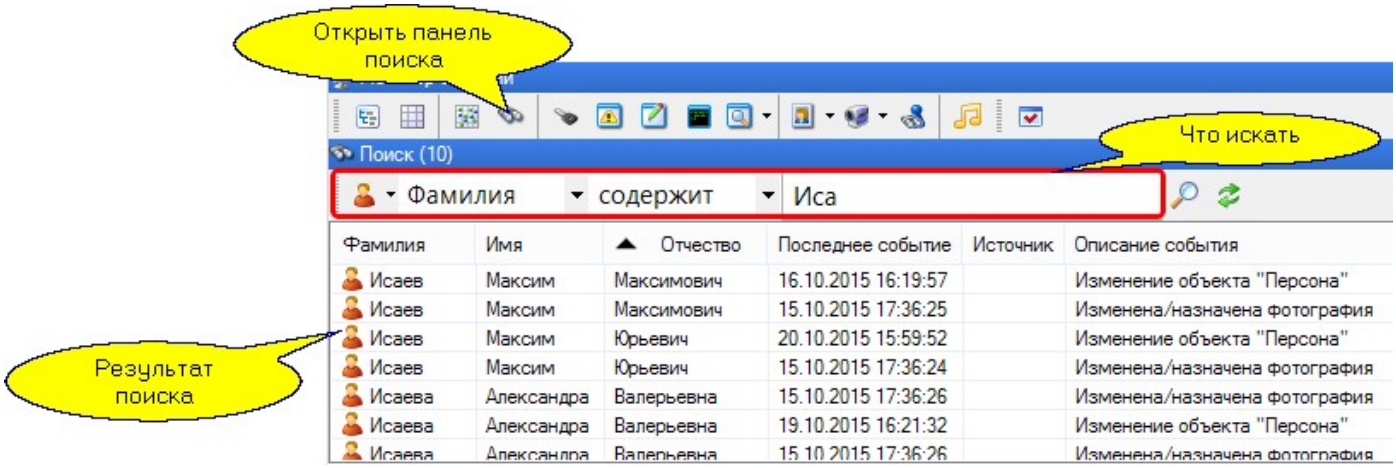
- Подложка. Как правило, это чертеж территории, выполненный в каком-либо графическом редакторе. Подложка всегда располагается на заднем плане.
- Компоненты оборудования. Вы можете разместить на плане только те компоненты, которые для вас важны. Если на графплане размещена видеокамера, то во всплывающем окне можно посмотреть изображение с нее, передающееся в реальном времени. Для этого дважды щелкните по ней или выберите пункт контекстного меню *Просмотр "живого видео"*:



- Текст. Позволяет нанести надписи, которые помогают понять назначение элементов плана.
- Значки. Позволяют добавлять некоторые небольшие изображения, также помогающие в работе оператору.

Поиск персонала

В ParsecNET 3 в мониторе событий реализован поиск субъекта в пределах доступной вам территории - событий, зафиксированных системой для конкретного субъекта доступа. Пользование панелью поиска поясняется следующим рисунком:

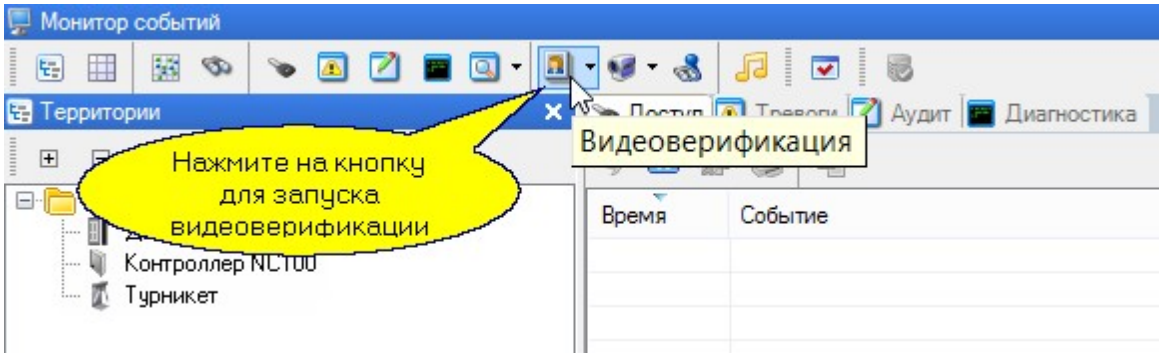


Видеоверификация

Модуль видеоверификации позволяет для выбранных точек прохода в реальном времени выводить указанный заранее набор информации о субъекте доступа, который в настоящий момент времени пытается войти на территорию.

Модуль видеоверификации является лицензируемой опцией.

Окно видеоверификации открывается кнопкой, показанной на рисунке ниже. Настройка панели и работа с модулем видеоверификации описаны в разделе[506].

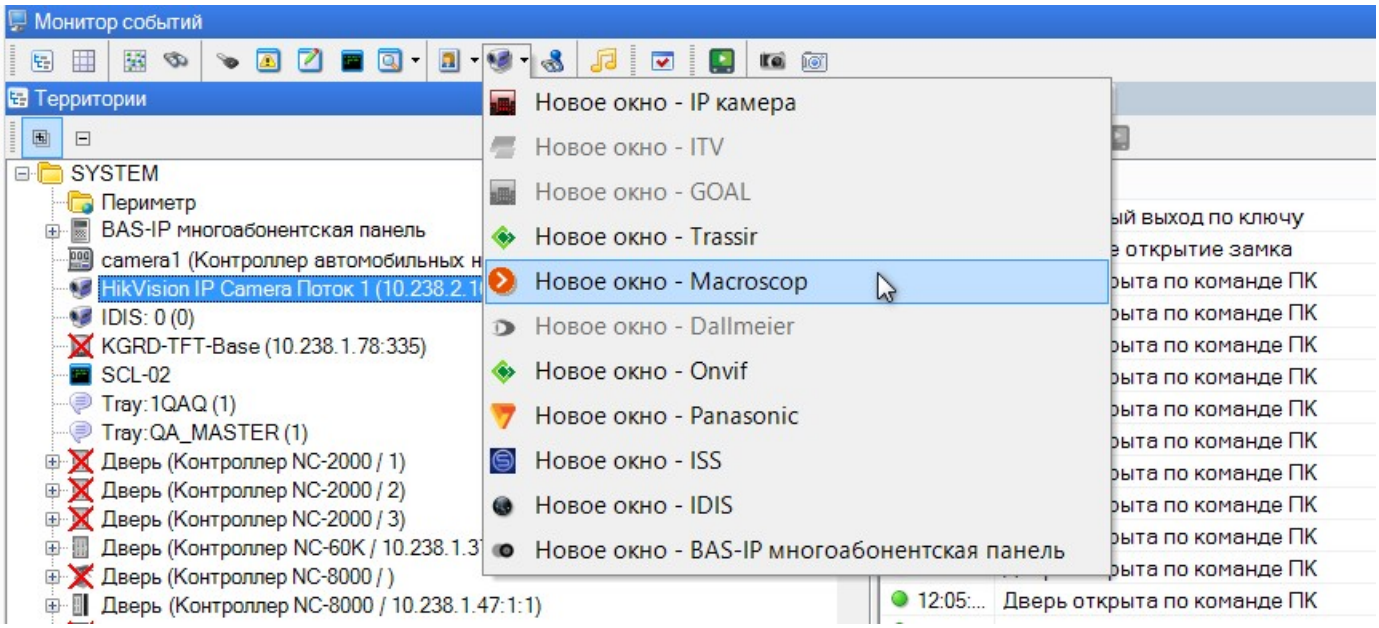


Видеонаблюдение

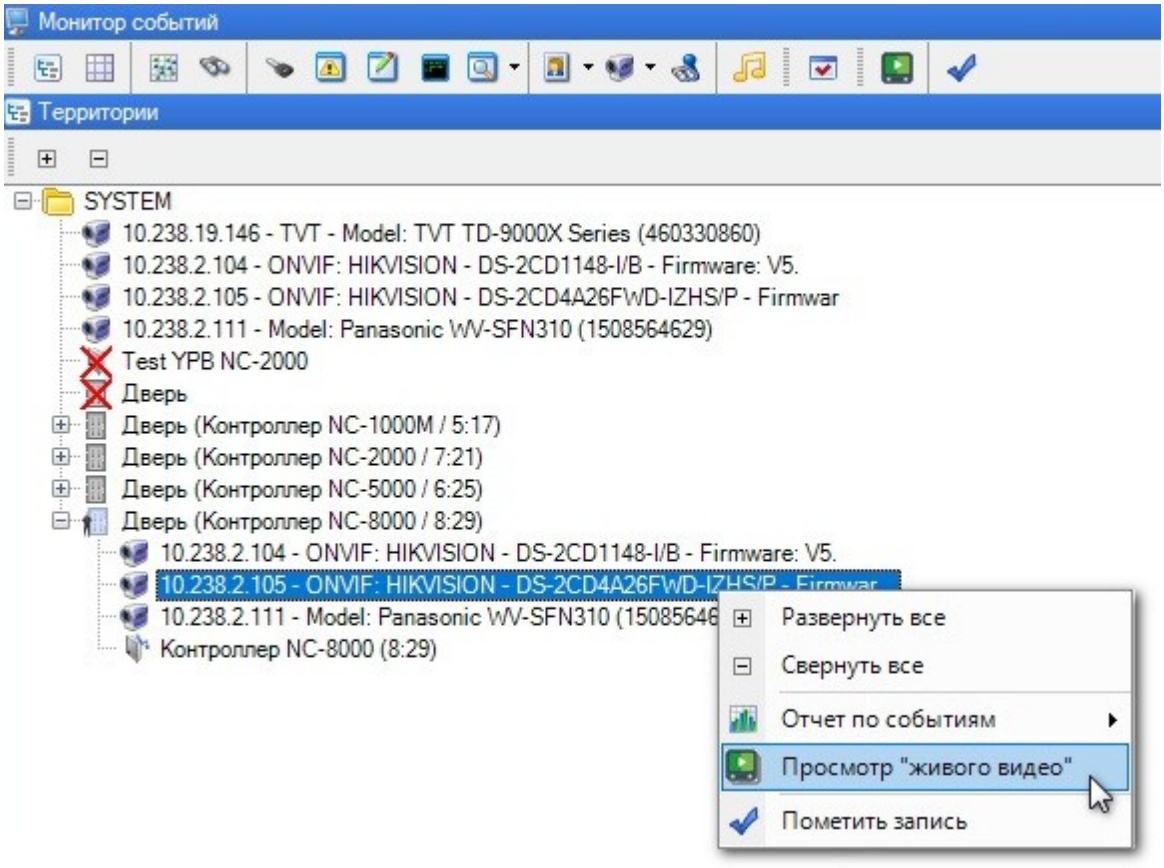
Модуль видеонаблюдения необходим для работы внешних систем видеонаблюдения в рамках СКУД ParsecNET. Подробно о модуле, системах видеонаблюдения и работе с ними написано в разделе[515].

Модуль видеонаблюдения является лицензируемой опцией.

Окно для каждой отдельной системы видеонаблюдения открывается кнопкой, показанной на рисунке ниже.



С любой работающей камеры в дереве территорий можно просмотреть изображение, передающееся в текущем времени. Для этого нажмите на одноименную кнопку на панели инструментов Монитора событий или выберите пункт контекстного меню *Просмотр "живого видео"*:



Мониторинг количества людей в помещении

Консоль монитора позволяет вести учет людей в помещении.

Функция работает только с контроллерами NC-8000.

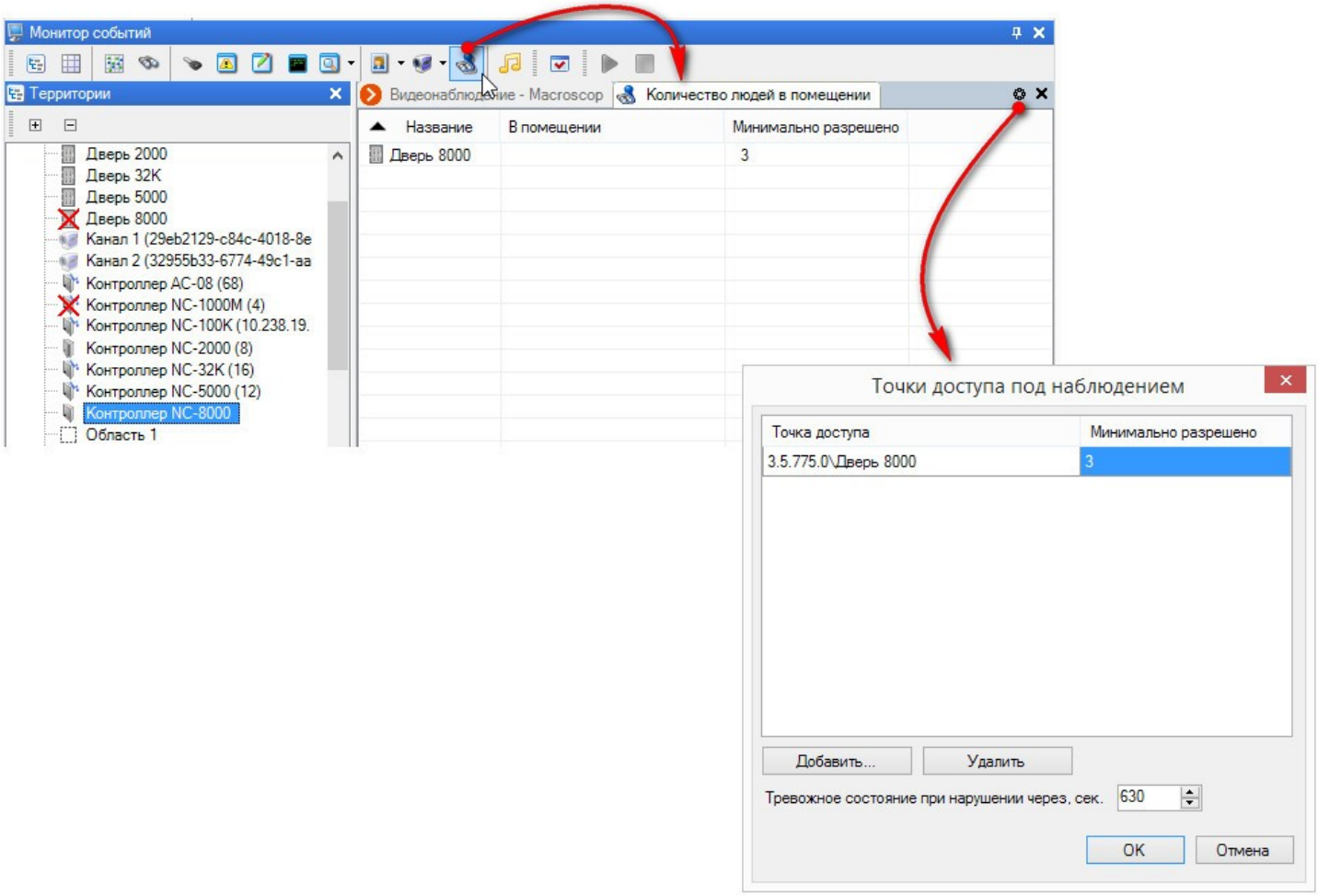
Для корректного подсчета людей в помещении точка прохода должна быть оборудована двумя считывателями.

Панель *Количество людей в помещении* в консоли монитора открывается при нажатии на кнопку на панели инструментов.

Монитор, на основании анализа количества входов и выходов, следит за тем, сколько человек находится в помещении. Если это количество равно или меньше заданного, запускается таймер, по истечении которого соответствующая строка подсвечивается красным. Отсутствие людей в помещении считается нормой и такого события не вызывает.

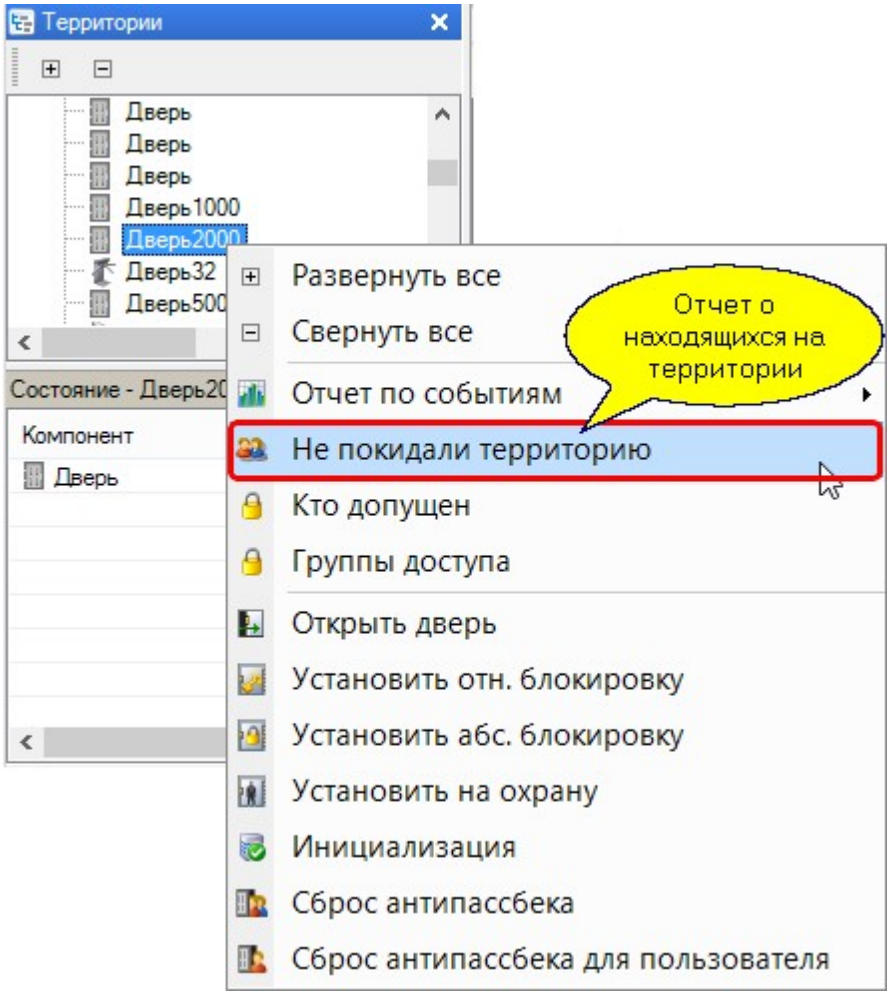
Для изменения минимально разрешенного количества человек, выполните следующие шаги:

1. Нажмите на кнопку (*Настройки)* на панели *Количество людей в помещении*. Откроется окно *Точки доступа под наблюдением;*
2. Нажмите на кнопку *Добавить* и выберите нужную точку доступа;
3. Задайте в поле *Минимально разрешено* количество людей в помещении;
4. Установите время, по истечении которого будет возникать подсветка строки;
5. Нажмите на кнопку *ОК*.



8.8.2 Отчеты монитора событий

Команда контекстного меню *Не покидали территорию* дает возможность получить список тех, кто находится на заданной территории со вчерашнего дня. В качестве объекта, по которому осуществляется поиск, выступает как конкретная точка прохода - отдельная дверь или турникет, так и составная территория. Отчет может быть распечатан на принтере или экспортирован в несколько популярных форматов.На рисунке ниже показано контекстное меню при формировании отчета о находящихся на территории "Дверь2000":

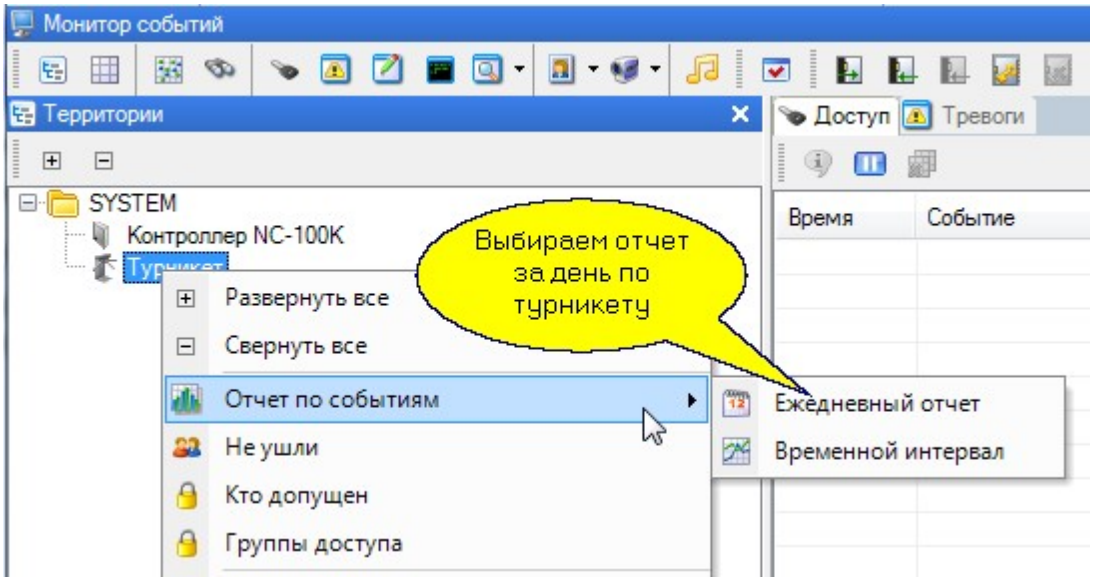


Следует иметь в виду, что корректная информация в отчете будет получена только для двухсторонних точек прохода.

Аналогичным образом можно получить отчеты:

- *Кто допущен* - список субъектов доступа, имеющих право прохода через одну или все точки прохода на территории. При создании этого отчета отдельным диалогом предоставляется выбор, какие субъекты отображать:
  - *Доступ разрешен* - отображаются субъекты доступа, имеющие действующий доступ через выбранные точки прохода;
  - *Идентификатор заблокирован* - отображаются те субъекты доступа, доступ которых через выбранные точки прохода запрещен (в карточках субъектов стоят флажки *Вход запрещен* и *Выход запрещен*);
  - *Временный идентификатор вне срока действия* - отображаются те субъекты доступа, чей период доступа уже закончился или еще не начался;
  - *Все субъекты доступа* - отображаются все субъекты доступа, имеющие право на проход через выбранные точки прохода.
- *Группы доступа* - список групп доступа, в которые включена выбранная точка прохода.

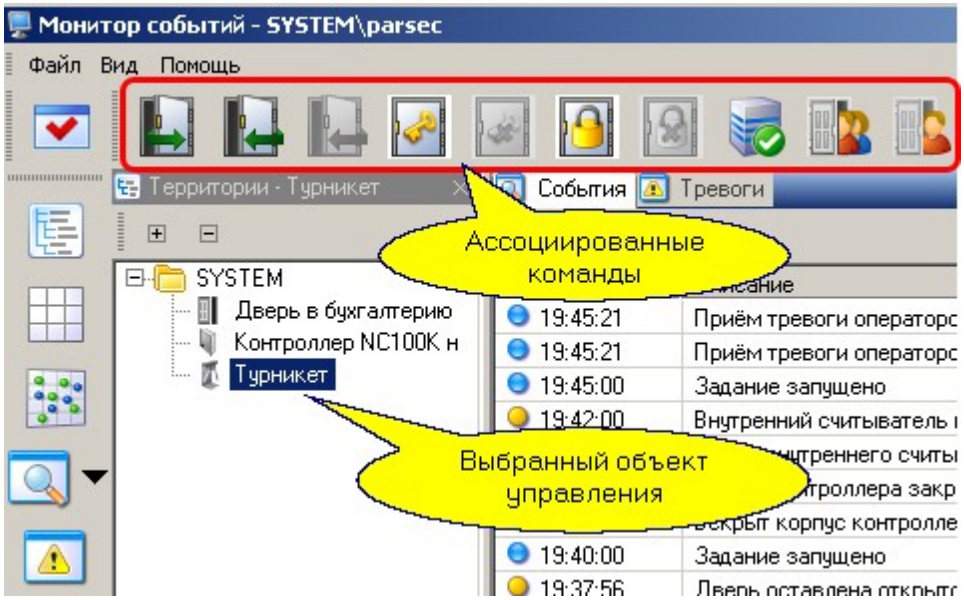
Обратите внимание, перечисленные выше отчеты доступны только в контекстном меню дверей и территорий. Контекстное меню контроллеров, охранных областей и т.д. содержит только пункт получения отчетов по событиям за текущий день или за выбранный интервал времени:



8.8.3 Прямое управление устройствами

С помощью монитора событий можно непосредственно управлять оборудованием (например, открыть и закрыть выбранную дверь).

Панель управления оборудованием предоставляет только те команды, которые могут исполняться выбранным в топологии оборудованием. Например, при выборе в качестве объекта управления точки прохода набор инструментов позволяет открыть или закрыть дверь, включить или выключить блокировку, как показано на рисунке ниже (панель основных команд для удобства сдвинута на левую сторону экрана):



Абсолютную блокировку можно установить и снять только с помощью ПО ParsecNET 3. При этом через точку прохода не может пройти ни один идентификатор, независимо от данных ему привилегий[250].

Однако, если во время абсолютной блокировки контроллер перейдет в режим работы off-line из-за потери связи с сервером, то с выходом сотрудников может возникнуть проблема. В СКУД Parsec эта проблема решена следующим образом:

- Контроллеры моделей NC-1000/5000 в подобном случае самостоятельно меняют абсолютную блокировку на относительную;
- Абсолютную блокировку контроллера NC-100K-IP может снять идентификатор с привилегией "Карта с привилегиями";

- Абсолютную блокировку контроллеров NC-2000/8000/32k снимает идентификатор с привилегией "Управление охраной".

Инициализация

После того, как в систему был добавлен новый контроллер или была произведена замена контроллера, необходимо проинициализировать его базу данных. Помимо этого инициализация может потребоваться после длительного пребывания контроллера в режиме офф-лайн. Например, когда пользователь получает "нормальный доступ по ключу", но отсутствует в БД системы и т.п.

Инициализация - это операция, которая заключается в том, что база данных контроллера (расписания доступа, коды идентификаторов, привилегии и т.п.) полностью очищается, а затем наполняется данными из БД системы ParsecNET 3.

Чтобы в новую точку прохода загрузить пользователей, эту точку нужно добавить в соответствующие группы доступа. Делать это необходимо перед проведением инициализации.

Во время проведения инициализации контроллер будет недоступен и точка прохода, которой он управляет, будет заблокирована. В зависимости от количества пользователей, имеющих доступ через точку прохода, типа контроллера и загруженности системы процесс инициализации может занять от нескольких секунд до нескольких минут.

Настоятельно рекомендуется не проводить одновременно инициализацию нескольких контроллеров.

Инициализацию проводите при условии, что с контроллером есть устойчивая связь.

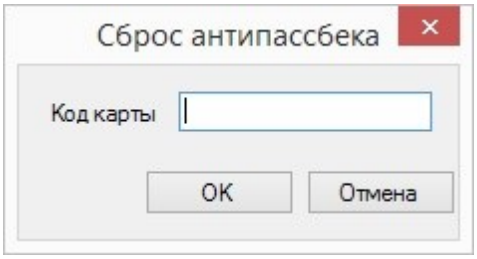
После успешного завершения инициализации в системе генерируется сообщение об этом.

Сброс антипассбэка для пользователя

Если пользователь приложил карту к считывателю, но не получил доступа из-за срабатывания антипассбэка (АПБ), то может возникнуть необходимость сброса АПБ.

Для этого выполните следующие действия:

1. В мониторе событий на панели территорий выделите точку прохода (дверь) того контроллера, для которого производится сброс АПБ;
2. Нажмите на кнопку  (*Сброс антипассбэка для пользователя)* на панели команд (см. рис. выше). Откроется окно ввода кода карты:



3. Приложите к считывателю контроллера (см. шаг 1) карту, для которой сбрасывается АПБ, - код карты отобразится в окне. Либо введите код карты вручную в **шестнадцатиричном** виде. После ввода кода нажмите на кнопку *OK*.

Система сбросит антипассбэк для этого идентификатора и при следующем его прикладывании к считывателю доступ будет предоставлен.

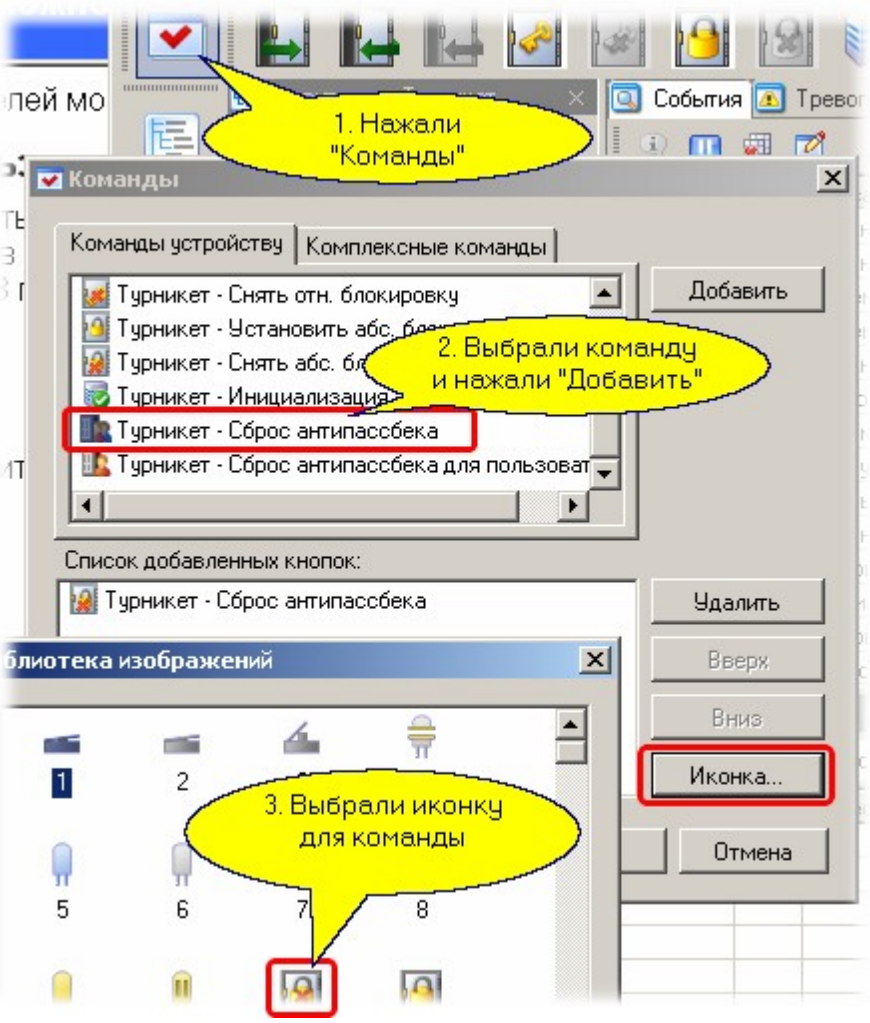
Сброс антипассбэка

Помимо сброса АПБ для пользователя, можно произвести сброс АПБ точки прохода. А если она входит в группу АПБ[161], сброс будет осуществлен у всех точек прохода данной группы. Для этого выделите на панели территорий монитора событий точку прохода и нажмите на кнопку 

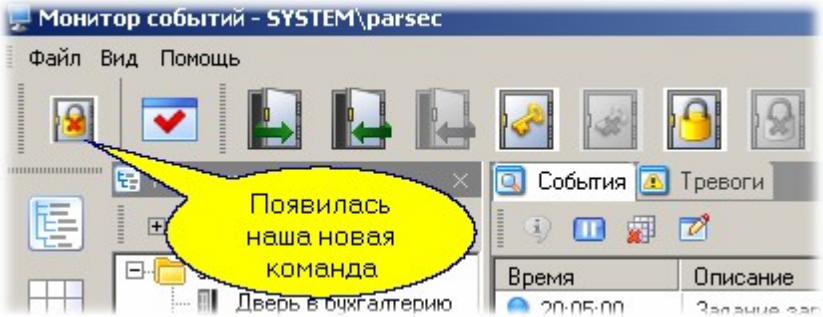
(Сброс антипассбэка). У всех субъектов доступа, прошедших через любую точку прохода данной группы АПБ, будет снят бит антипассбэка.

8.8.4 Часто используемые команды

Если вам часто надо подавать конкретную команду конкретному оборудованию, вы можете сформировать для этих целей отдельную кнопку в панели инструментов монитора. Для этого выберите в панели топологии нужный объект (в нашем примере это турникет), нажмите на кнопку *Команды*. В появившемся окне выберите нужную команду, присвойте ей значок и нажмите на кнопку *ОК*.



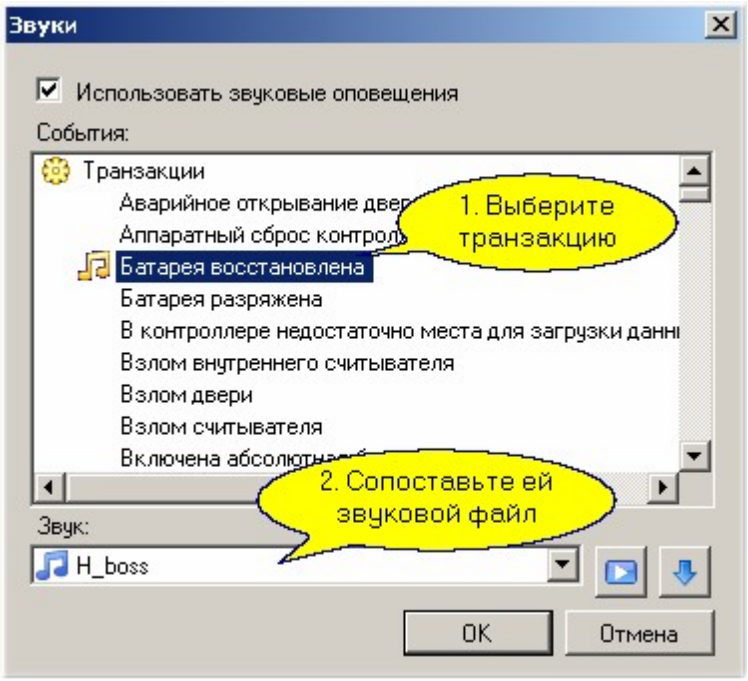
В панели инструментов появится новая кнопка, по которой будет исполняться ваша команда.



Подобным образом можно выносить на панель монитора событий и сложные комплексные команды, созданные с помощью менеджера заданий.

8.8.5 Настройка звуков

Можно индивидуально озвучить все транзакции, отображаемые в мониторе событий. Для этого служит диалог выбора звуковых файлов, доступный из панели инструментов монитора. В диалоговом окне выберите транзакцию и поставьте ей в соответствие звуковой файл, затем нажмите на кнопку *OK*:



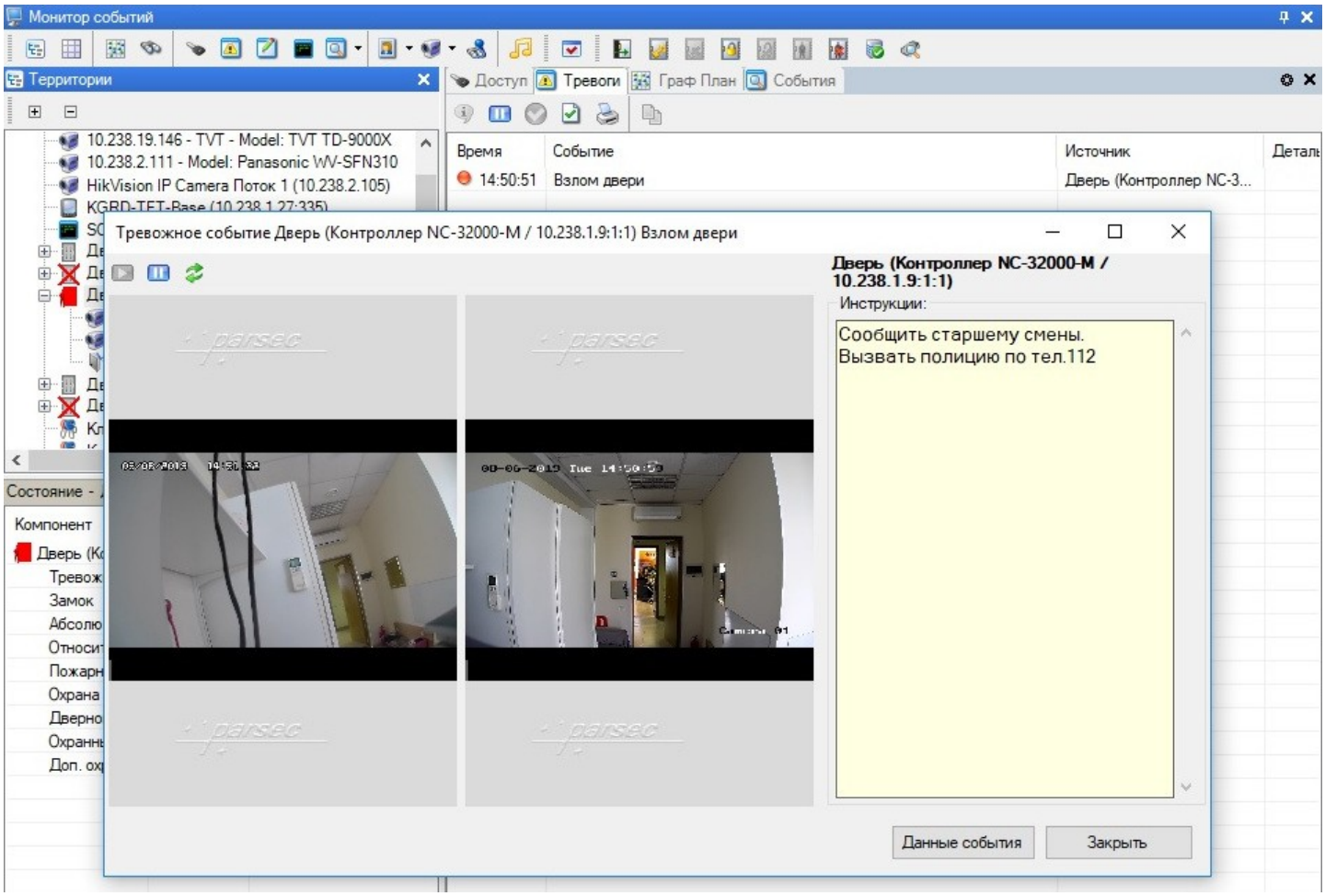
8.8.6 Тревожные события

Настоятельно рекомендуется для тревожных событий создать инструкции оператору[212] .

Инструкции будут появляться во всплывающем окне, если:

- Установлен флажок *Автоматически показывать при возникновении события*;
- Запущен Монитор событий (при этом можно находиться на вкладке любого другого инструмента Системы).

Кроме того, если на территорию с которой поступило тревожное событие, направлена и настроена видеокамера, то во всплывающем окне, помимо инструкций, будет отображаться и видеофрагмент, начинающийся за 20 секунд до возникновения этого тревожного события, при условии, что такую возможность используемая видеосистема предоставляет. Если видеосистема такого функционала не имеет, то отображается живое видео в текущем времени.

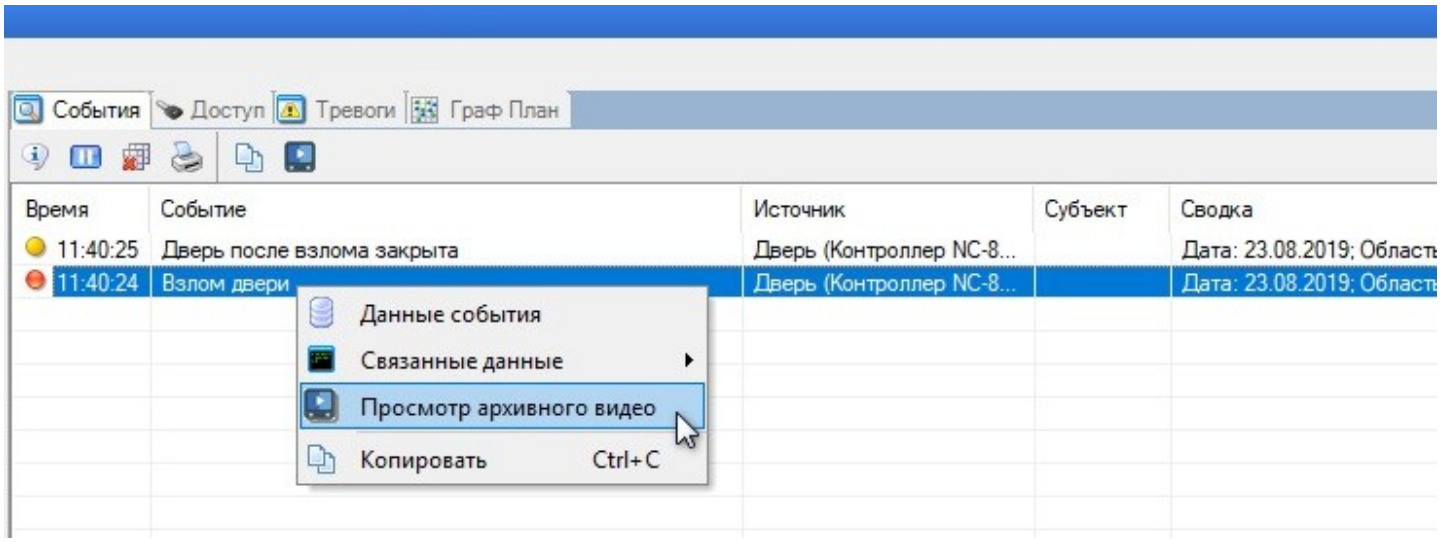


Элементы управления:

- останавливает показ видеофрагмента;

- повторяет видеофрагмент.

Аварийное событие позднее можно найти в окне *События*, либо составив отчет по событиям. При наличии у двери связанных камер[211] выбором команды контекстного меню *Просмотр архивного видео* можно будет во всплывающем окне просмотреть видеофайл из архива, начинающийся за 20 секунд до возникновения этого тревожного события. Ведение видеоархива, время начала фрагмента и его длительность зависят от функционала используемой видеосистемы.



Чтобы принять тревогу, нажмите на кнопку на панели инструментов окна *Тревоги*. Список тревог очистится, аварийная сигнализация отключится.

8.9 Отчеты по событиям

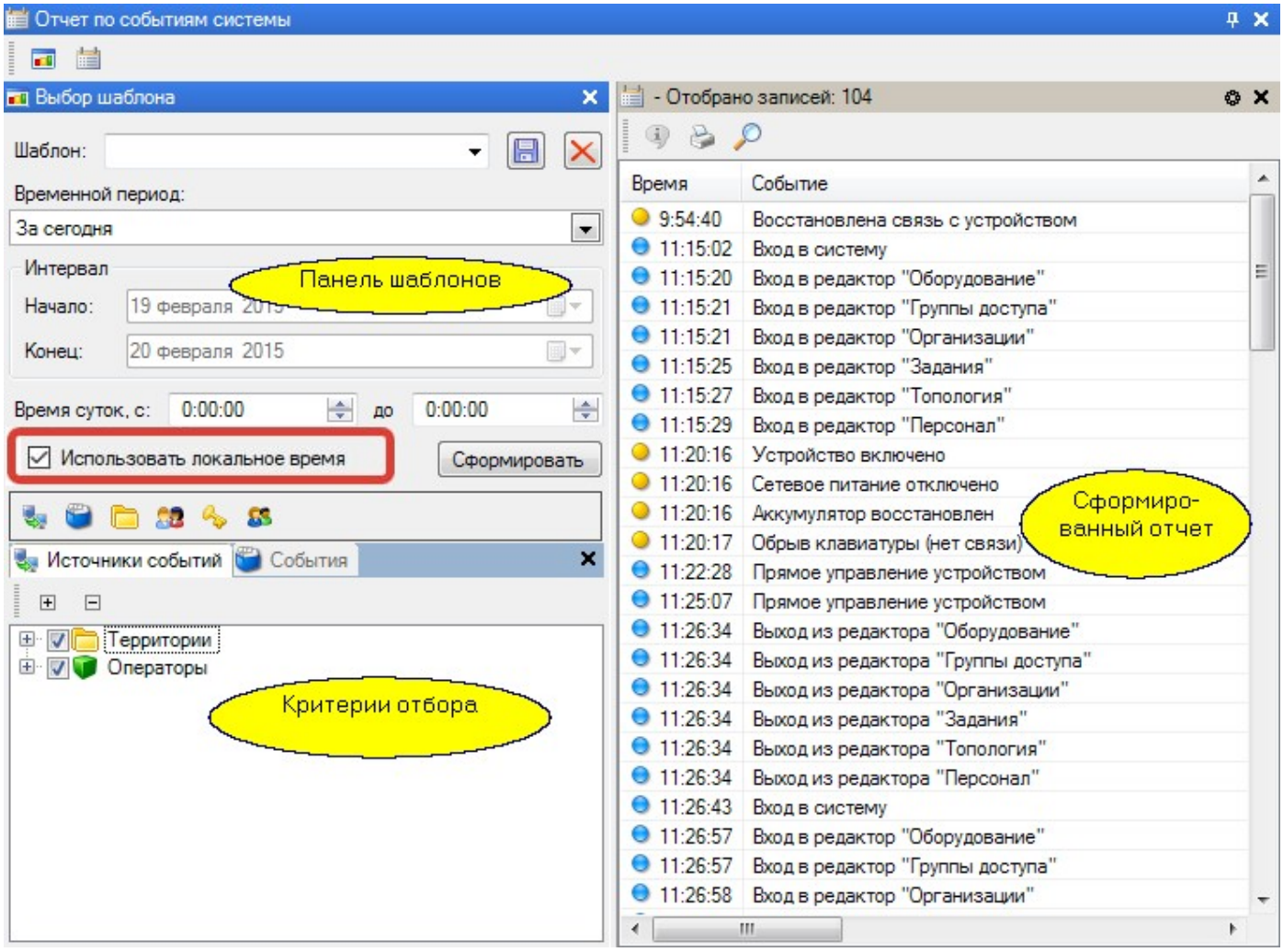
Назначение

Генератор отчетов по событиям предназначен для ретроспективного анализа событий системы. Он имеет развитую систему фильтров, позволяющих сформировать требуемый набор критериев отбора событий в отчет по территории, персоналу, идентификаторам, типам событий и по времени. Кроме того, вы можете отсортировать события в отчете по любому полю или набору полей.

Панели генератора отчетов

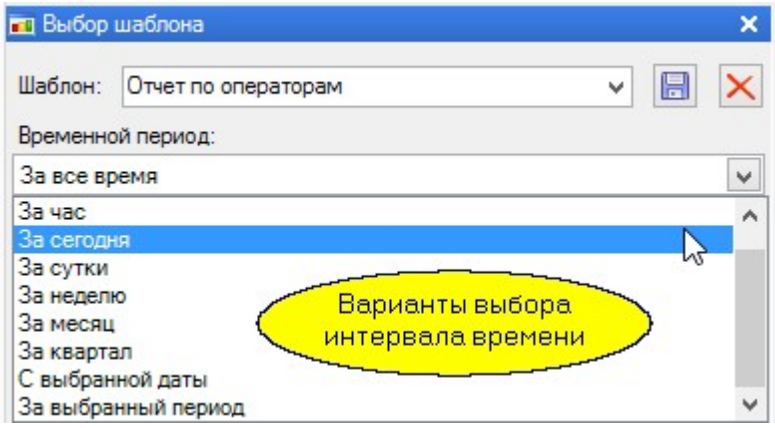
Генератор отчетов имеет три основные панели: панель выбора временного интервала с возможностью выбора ранее созданного шаблона, панель критериев отбора и панель результирующего отчета.

В свою очередь, панель критериев имеет вкладки: источники событий, типы событий, пользователи по подразделениям и персонально, идентификаторы и дополнительные субъекты. по-умолчанию на вкладках отмечены все источники, все события и все пользователи.

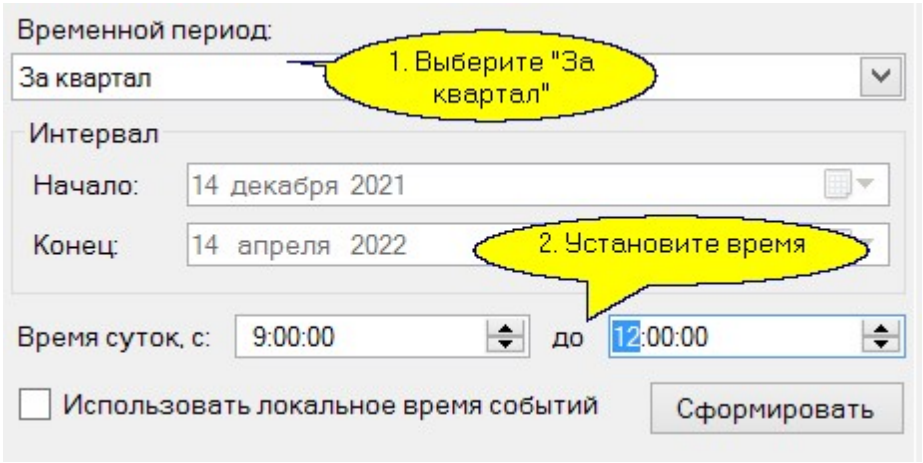


Выбор критериев для отчета

В первой вкладке мы можем настроить временной интервал, за который будут отбираться события. Возможные варианты показаны на рисунке ниже:

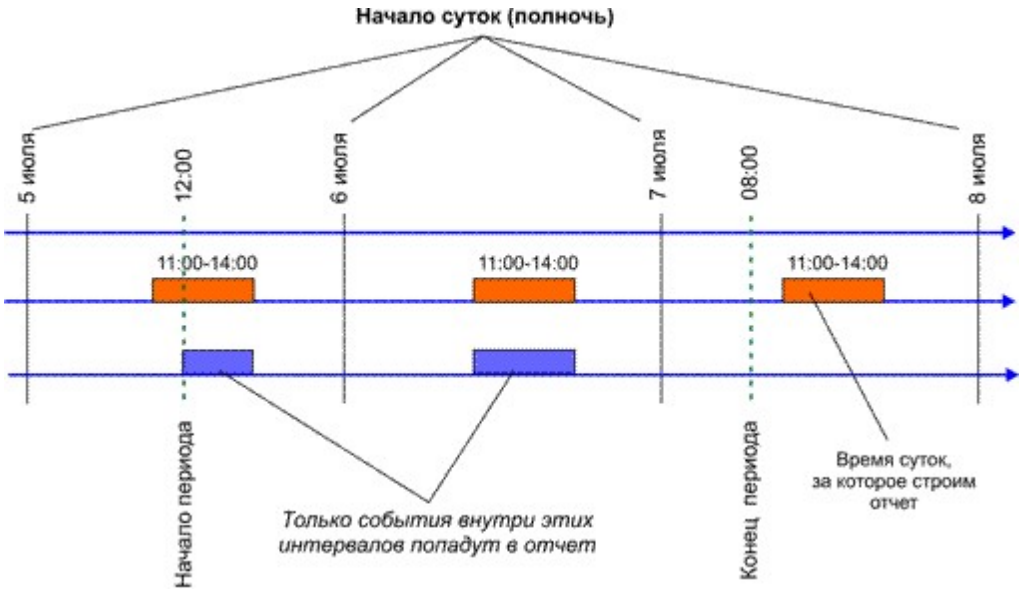


Кроме того, можно выбрать интервал времени внутри каждого из дней, для которых нужно отобрать события. Например, интересуют события за текущий квартал с 9 утра до полудня - в этом случае установите критерии, как показано на рисунке:

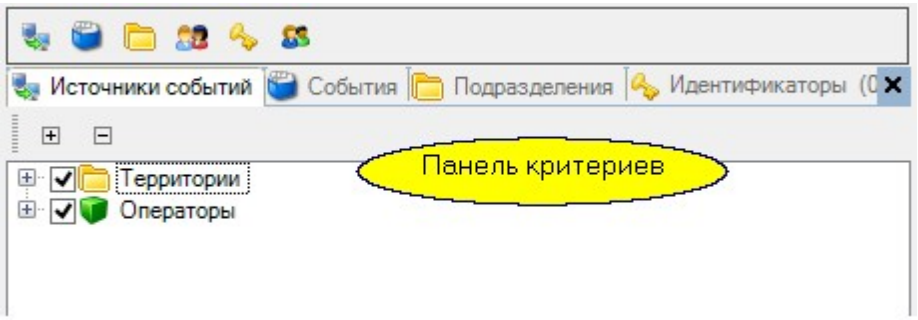


При установке флажка *Использовать локальное время событий* отчет будет сформирован с указанием времени тех часовых поясов, в которых находятся контроллеры, породившие события.

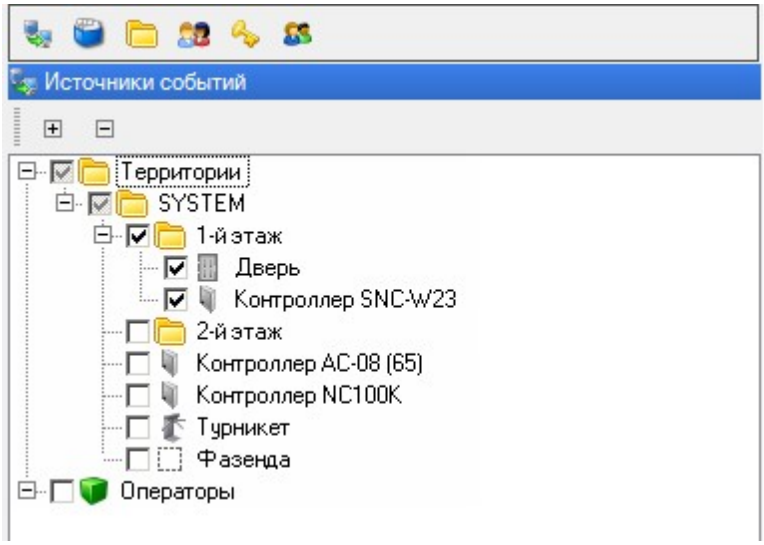
Если выбирается не предопределенный, а **произвольный период для отчета** (опция "За выбранный период"), то необходимо понимать, как работает критерий отбора по времени. Например, при выборе в качестве начала интервала 5 июля 12 часов дня, конец интервала 7 июля в 8часов утра и установке времени суток с 11:00 до 14:00 в отчет попадут только события, показанные внизу следующего рисунка синим цветом.



Особенностью панели критериев является наличие вкладок, из которых как минимум одна остается всегда открытой.

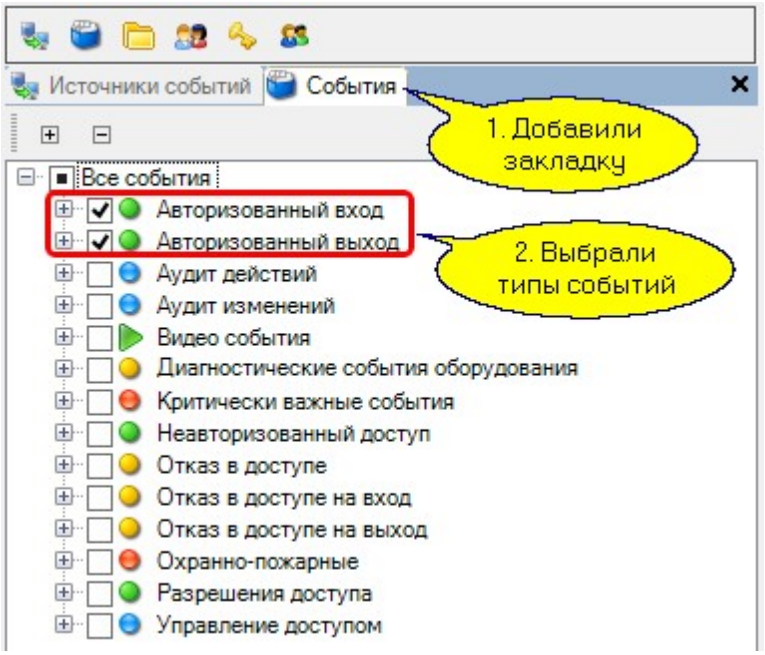


Закрытые вкладки на результат отчета не влияют. Например, если оставить открытой только вкладку источников и указать в ней конкретный источник, события от которого нас интересуют, как показано ниже, то критерии отбора закрытых вкладок использоваться не будут. Это равнозначно тому, что на каждой из закрытых вкладок отмечены все входящие составляющие (в нашем случае - все события, все подразделения и все пользователи). Для рисунка ниже выбор можно трактовать так: "требуются все события, связанные с территорией "1-й этаж" (независимо от того, какое это событие, с каким пользователем связано):

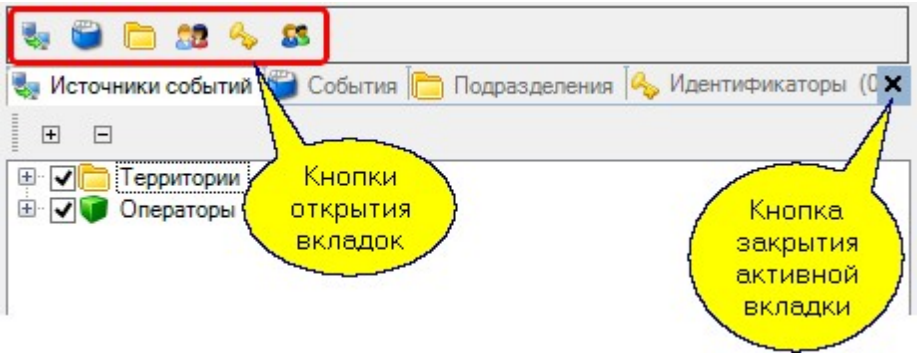


Обратите внимание: если в открытой вкладке не выбран ни один критерий, то отчет формироваться не будет. Все неиспользуемые вкладки необходимо закрыть.

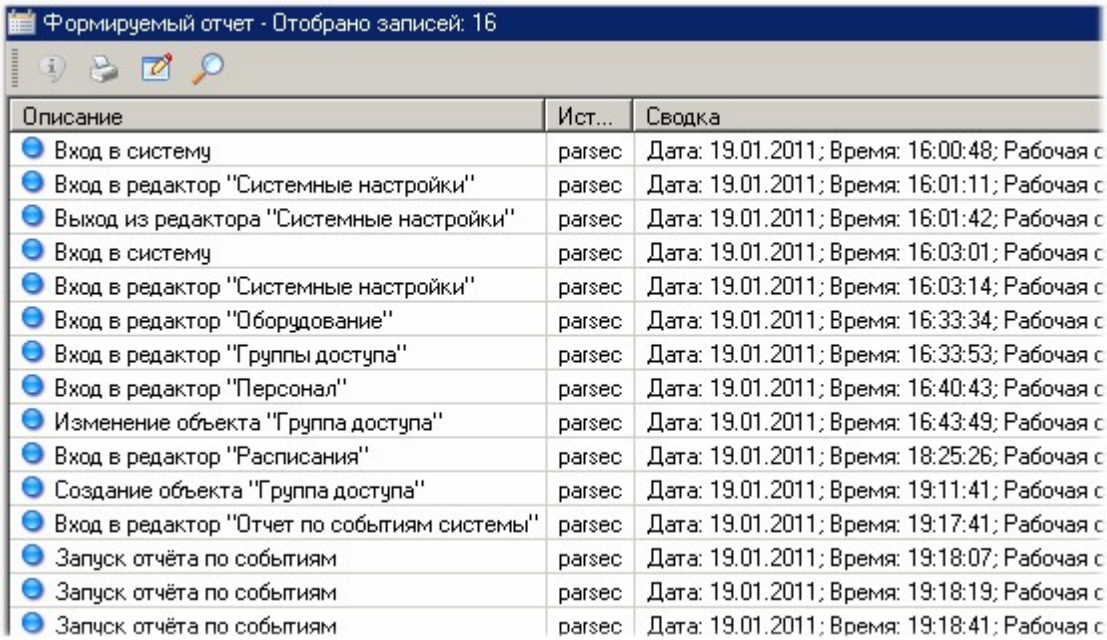
Если мы к вкладке *Источники событий* добавим вкладку *События* и выберем события авторизованного доступа, как показано на рисунке ниже, то в отчет попадут все события входа и выхода с территории "1-й этаж" (с любыми пользователями):



Аналогично можно ввести отбор по подразделениям и (или) отдельным пользователям, открыв соответствующие вкладки. Активная вкладка закрывается "крестиком" справа, а открываются с помощью кнопок в верхней части панели критериев отбора:

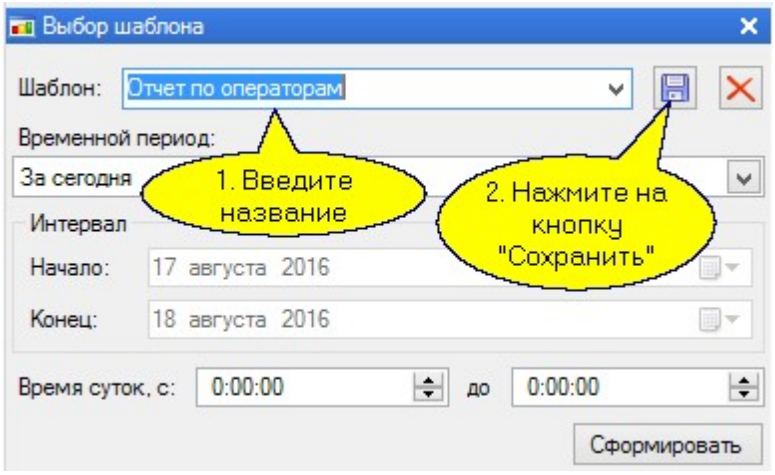


Если после установки критериев и временного интервала на панели шаблонов нажать на кнопку *Сформировать*, то через некоторое время в правой панели получаем отчет по желаемым событиям:



Использование шаблонов

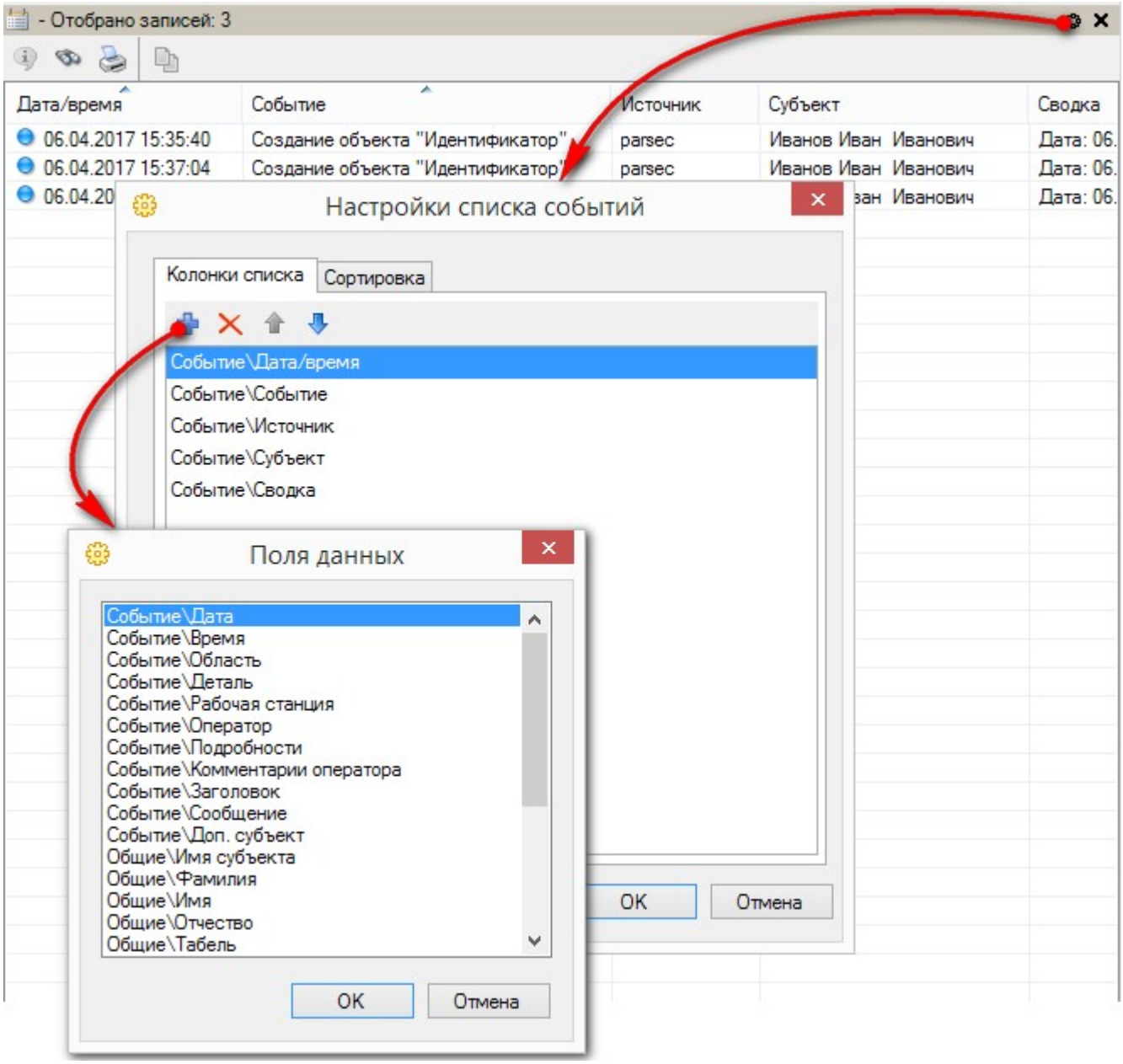
Предположим, что каждое утро в понедельник нужно формировать один и тот же отчет. Набирать все критерии каждый раз - не самое разумное решение. Лучше воспользоваться шаблоном. Все настройки сохранятся в шаблоне с именем "Отчет по операторам":



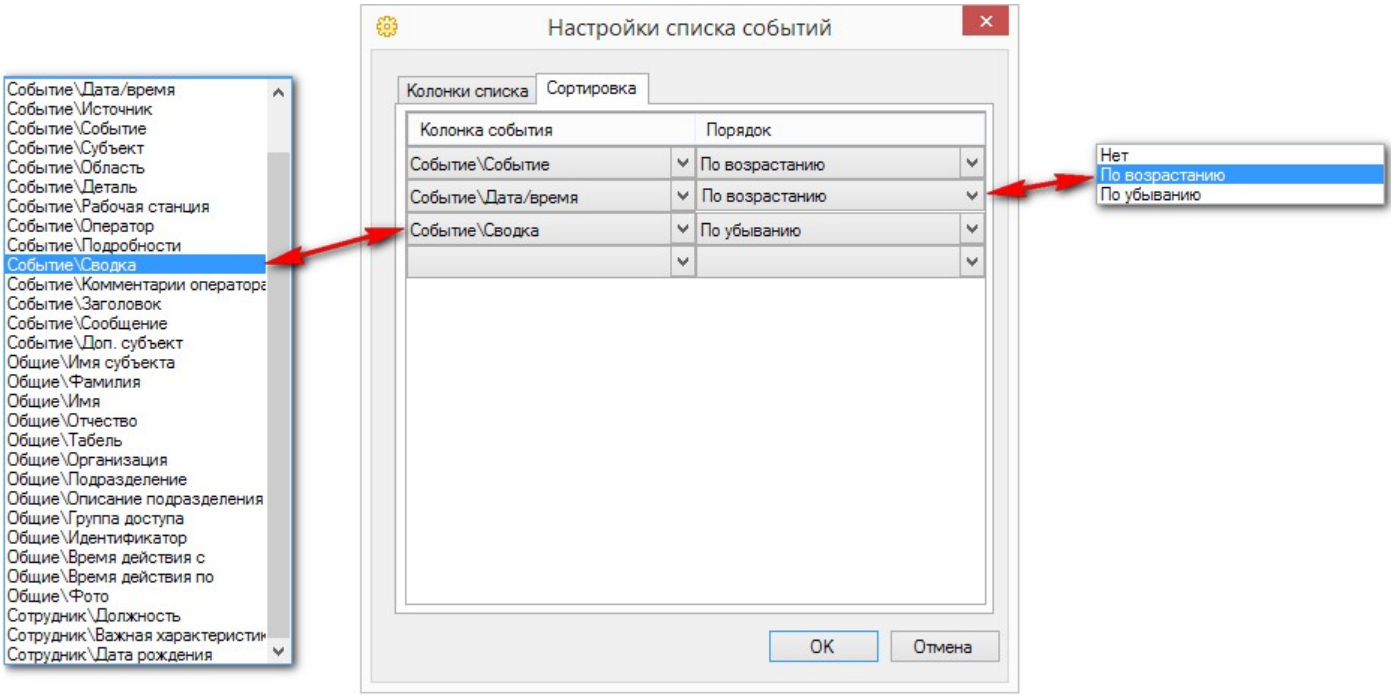
Теперь каждый раз, когда потребуется данный отчет, выберите его из списка сохраненных шаблонов, и просто нажмите на кнопку *Сформировать.*

Настройка колонок отчета

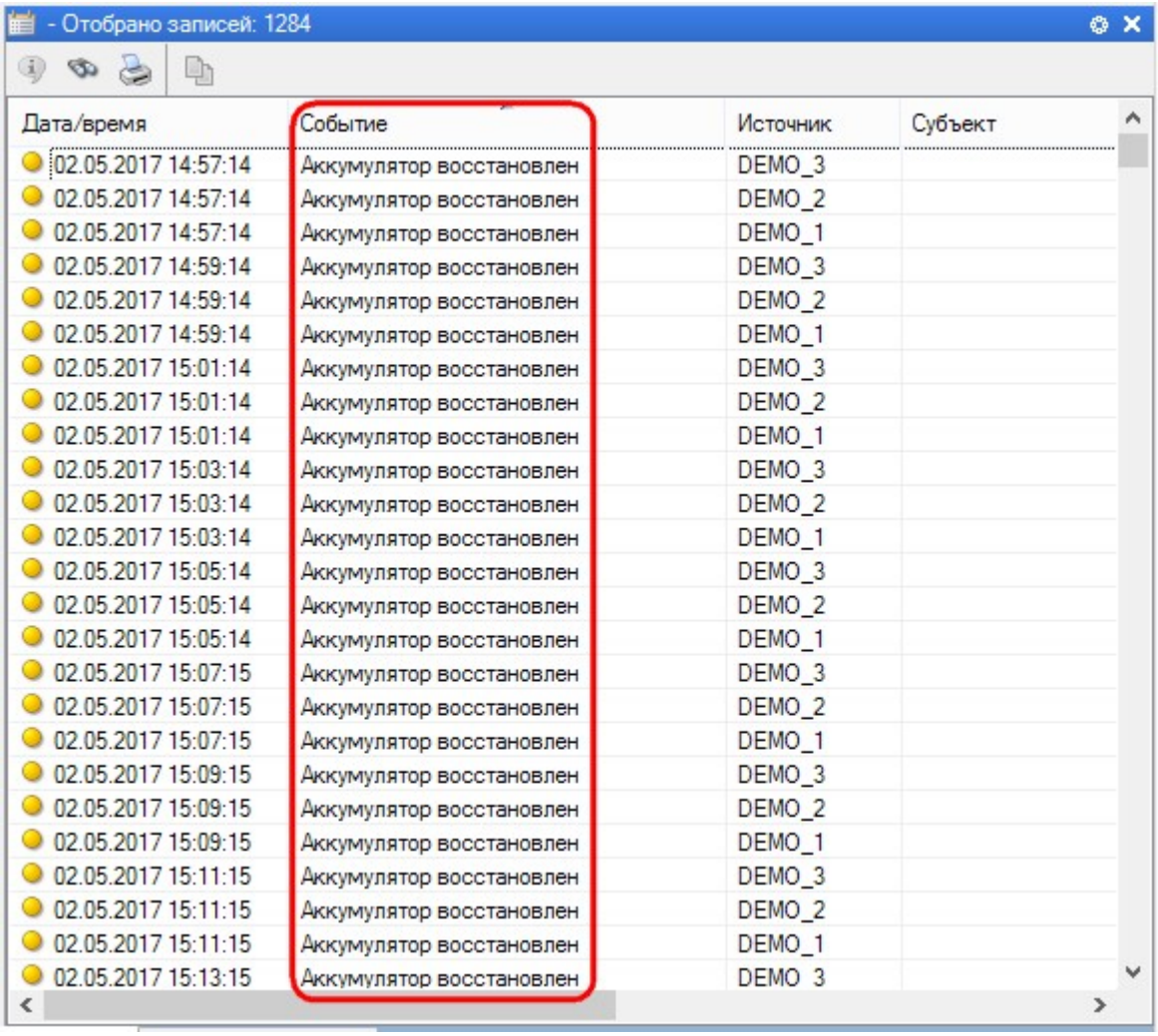
Все доступные колонки результирующего отчета не всегда нужны, каждому пользователю может потребоваться свой набор и порядок расположения колонок. Для настройки колонок нажмите на кнопку *Настройки* вверху справа на панели отчета. В открывшемся диалоге можно удалить ненужные колонки и добавить нужные, нажав на кнопку *Добавить*. При этом откроется окно *Поля данных*, в которых можно выбрать нужные колонки и добавить их, нажав на кнопку *ОК*. Кроме того, колонки списка можно пересортировать, используя стрелки *Вверх* и *Вниз*:



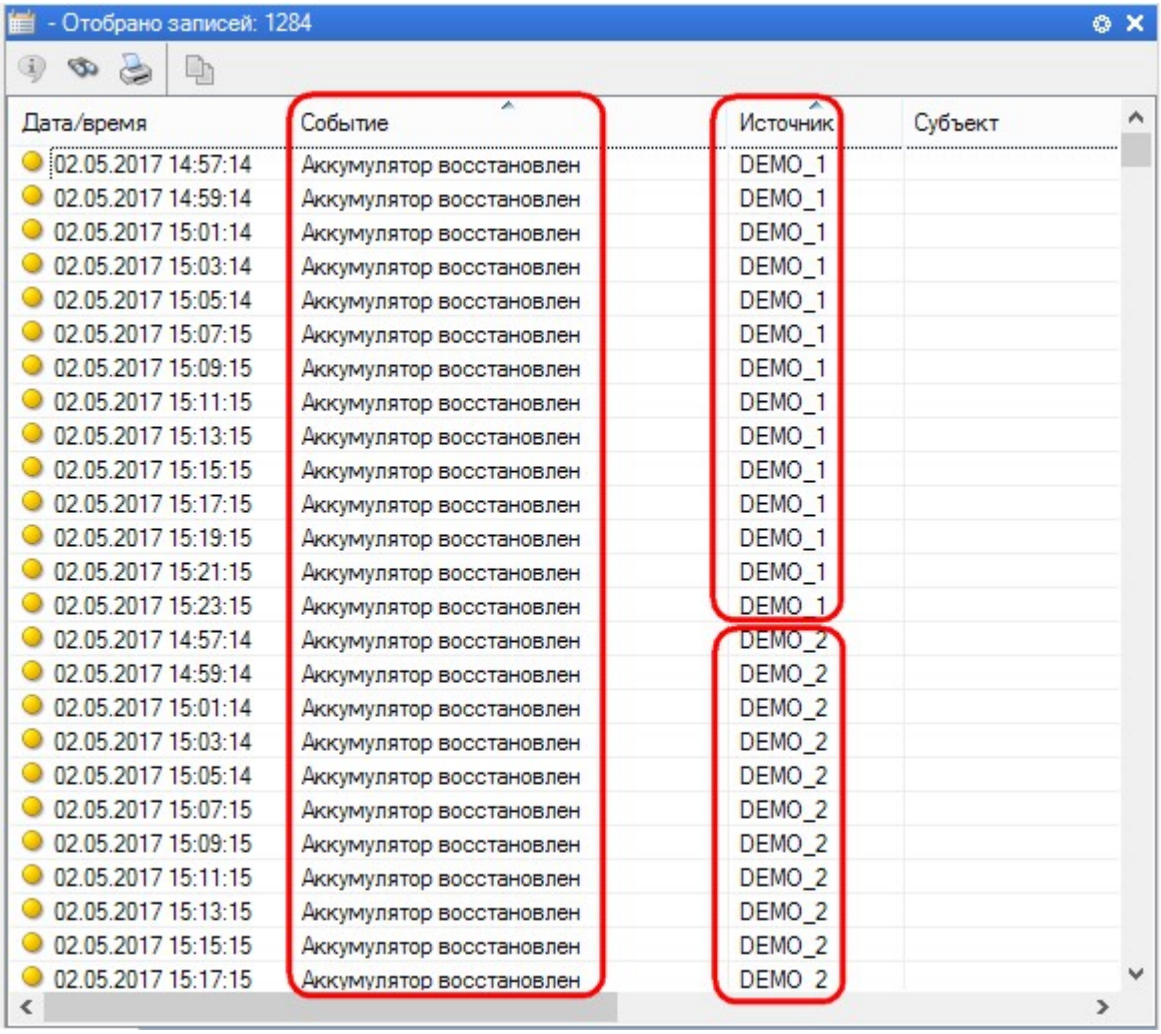
На вкладке *Сортировка* можно задать порядок сортировки строки в колонках.



Заданным образом сведения будут сортироваться по-умолчанию при формировании отчета. Оперативно сортировку можно осуществлять по нескольким столбцам или строкам (например, как, в таблицах MS Excel). Это позволяет сгруппировать данные с одинаковыми значениями в одном столбце, а затем отсортировать данные в другом столбце в этих группах с одинаковыми значениями. Например, в отчете имеются столбцы "Источник" и "Событие", сначала отсортируем строки в столбце "Событие" (для группировки всех одинаковых событий)

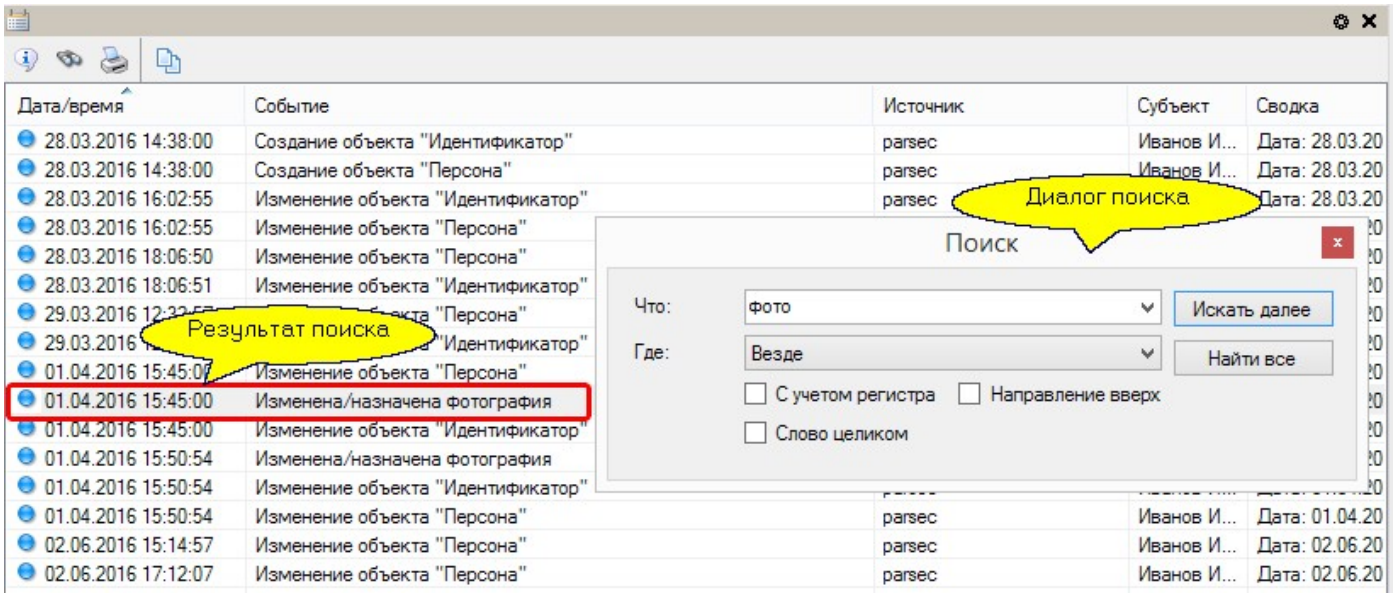


а затем по источнику события. Для этого, удерживая клавишу Control, последовательно нажимайте на заголовки столбцов, по которым нужно сделать сортировку. В итоге мы получим сначала одинаковые события из одного источника, потом те же события из другого источника и т.д.



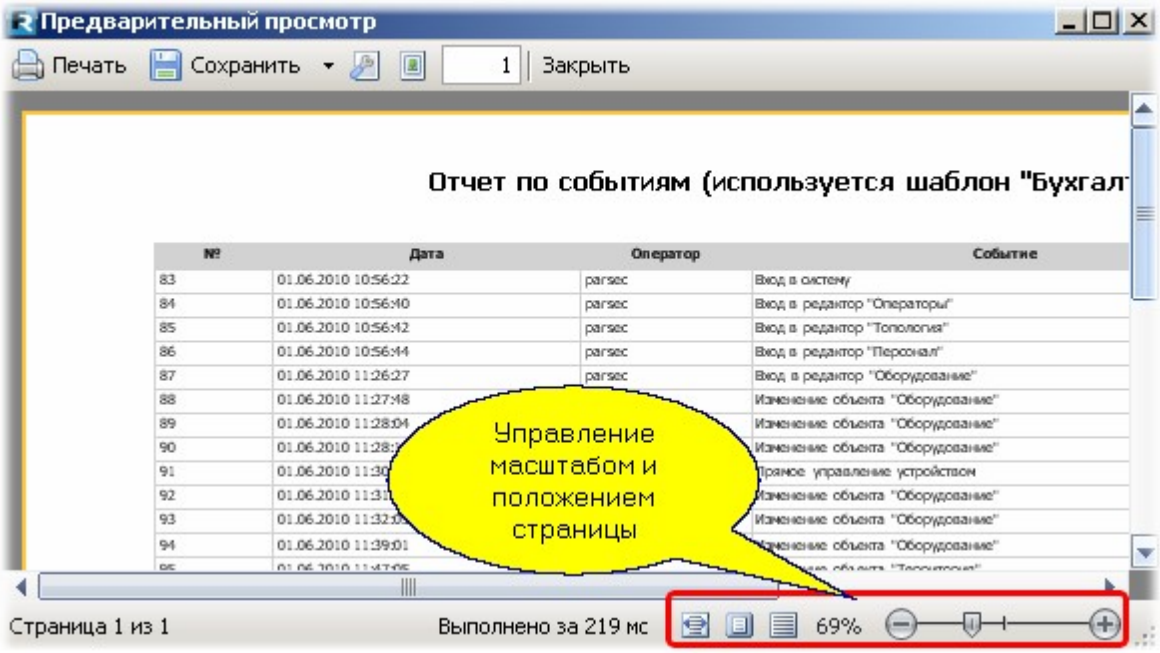
Поиск событий

В сформированном отчете можно искать отдельные события, содержащие в полях заданные слова (части слов, словосочетания). Для этого в верхней части панели отчета нажмите на кнопку *Найти* с изображением бинокля, установите критерии поиска и нажмите на кнопку *Искать далее* или *Найти все*.

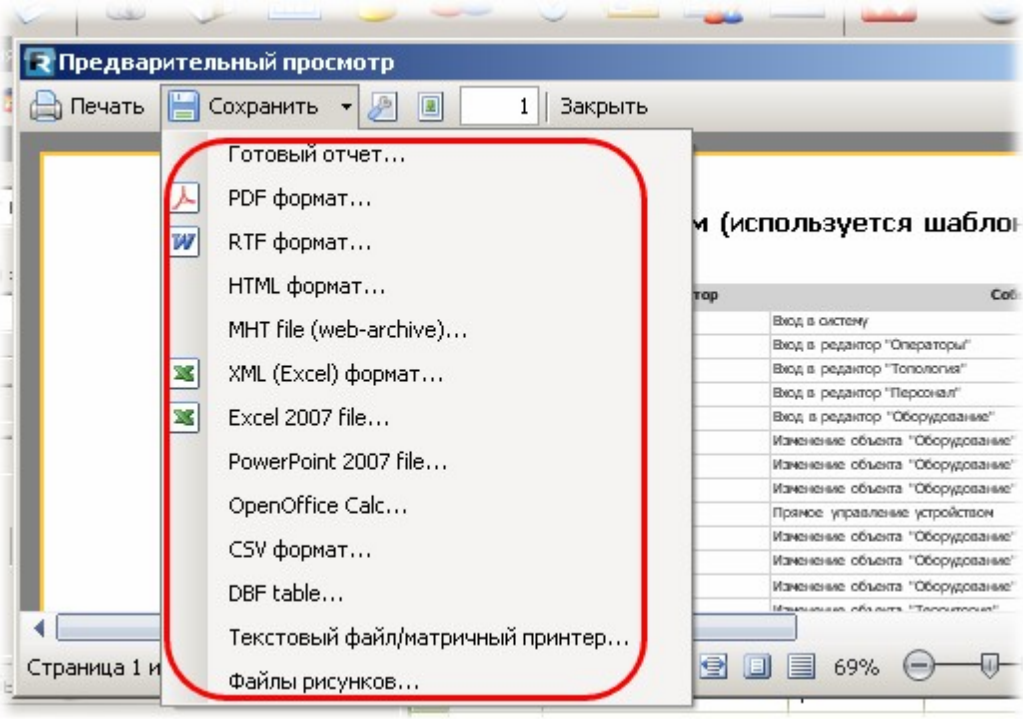


Печать отчета

Сформированный отчет можно вывести на принтер или сохранить в файл. Для этого нажмите на кнопку с изображением принтера в верхней части панели отчета. Откроется окно предварительного просмотра отчета перед печатью.



Вы можете масштабировать страницу отчета и позиционировать ее в окне с помощью отмеченных на рисунке органов управления. Готовый отчет можно напечатать, либо сохранить в файл в одном из показанных на следующем рисунке форматов:

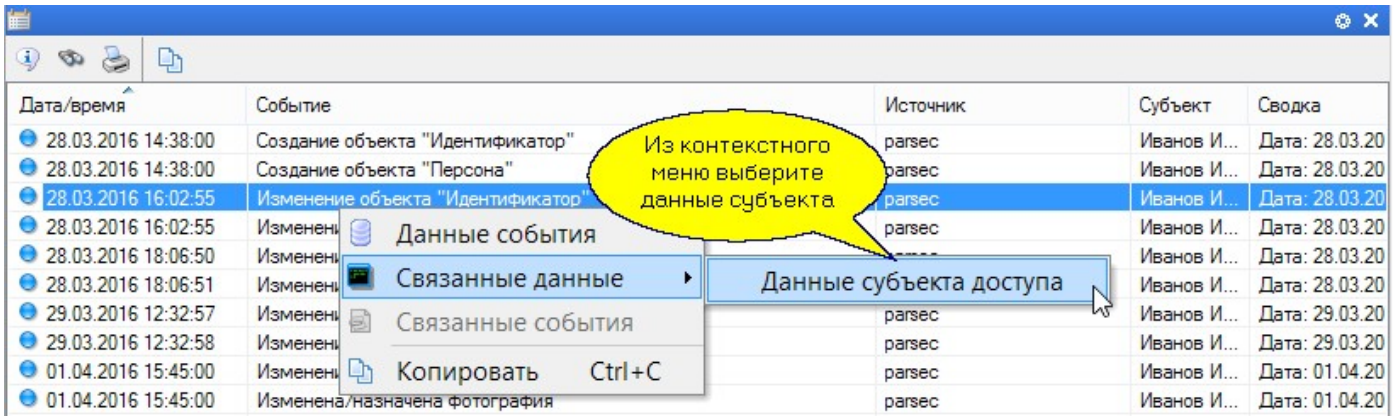


Естественно, что перед печатью можно выбрать тип принтера, бумагу и другие параметры из стандартного диалога настройки печати Windows.

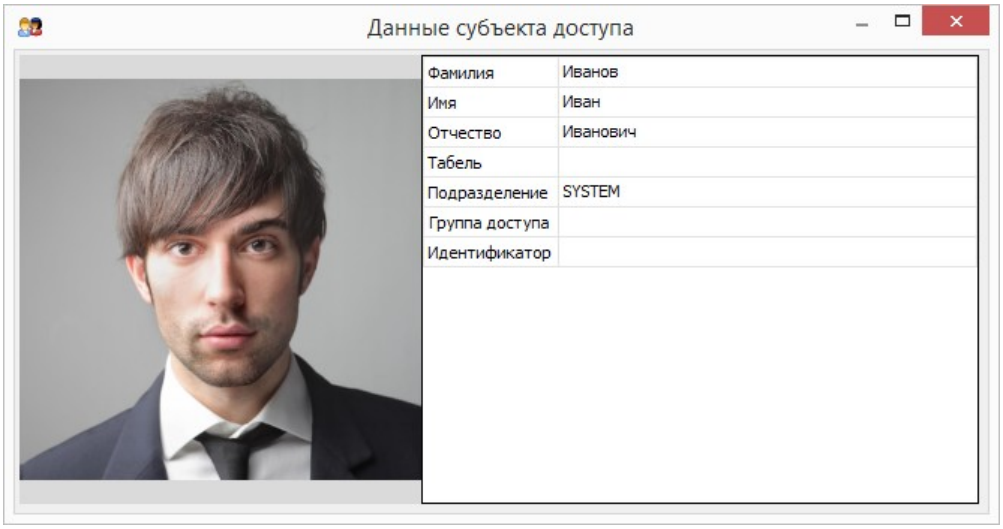
Получение деталей события

В сформированном отчете, как и в мониторе событий, по каждому событию можно получить полные данные (независимо от набора колонок в форме отчета), связанные события (если

таковые имеются, например, записанный видеофрагмент), а также связанные данные (если таковые есть, например, данные субъекта доступа). Пример приведен на рисунке ниже.



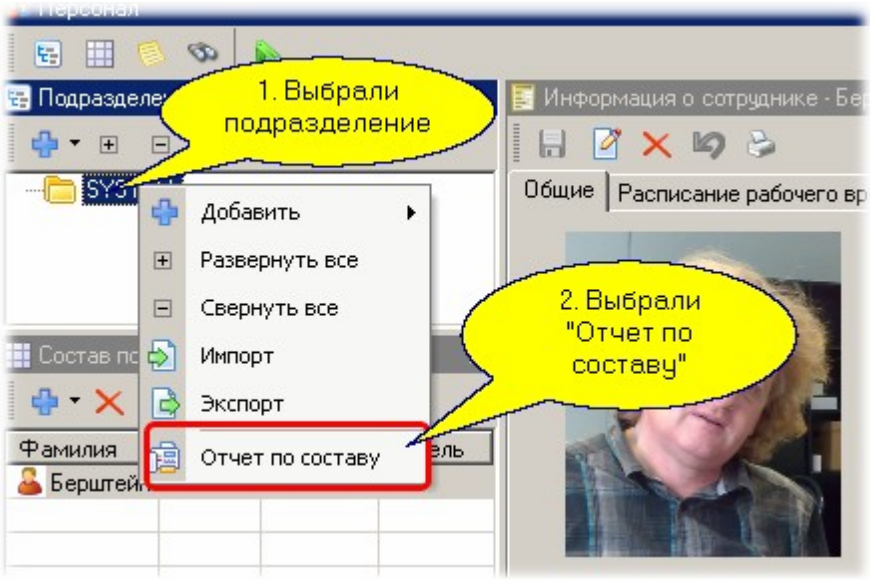
При выборе связанных данных для изменения идентификатора получаем карточку субъекта:



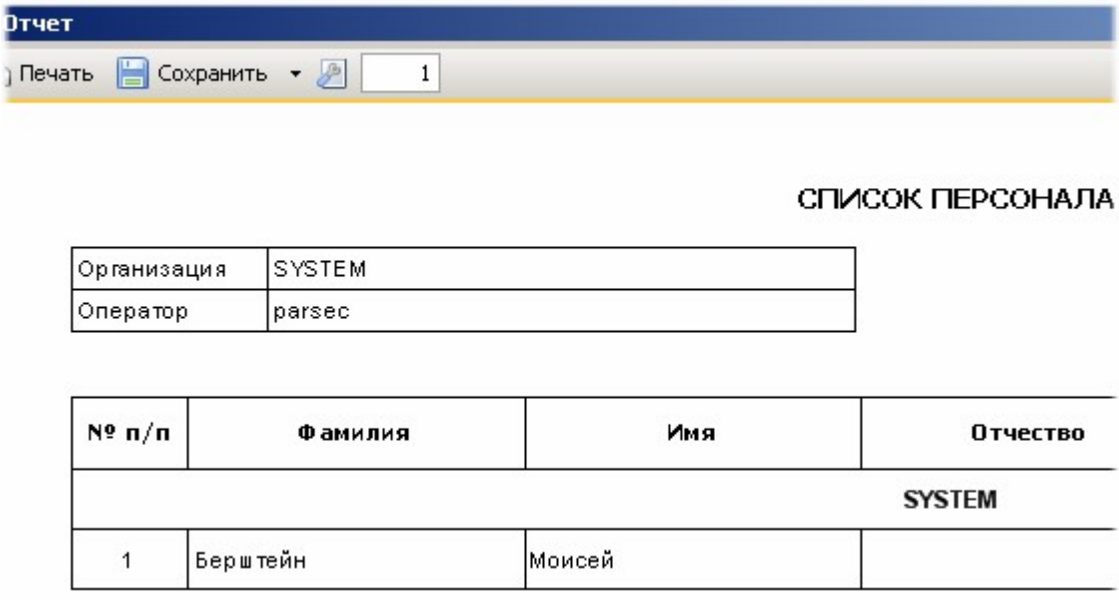
8.10 Отчеты по составу

Во всех инструментах, оперирующих с хранящимися в базе данных компонентами системы, имеется возможность сформировать так называемый отчет по составу. Такие отчеты можно получить для оборудования, групп доступа, персонала, операторов, расписаний.

Покажем на примере формирование подобного отчета для редактора персонала. Если выбрать подразделение в дереве персонала и нажать правую клавишу мыши, то в контекстном меню можно выбрать "Отчет по составу":



В результате появится окно с отчетом по персоналу выбранного подразделения примерно такого вида:


Отчет

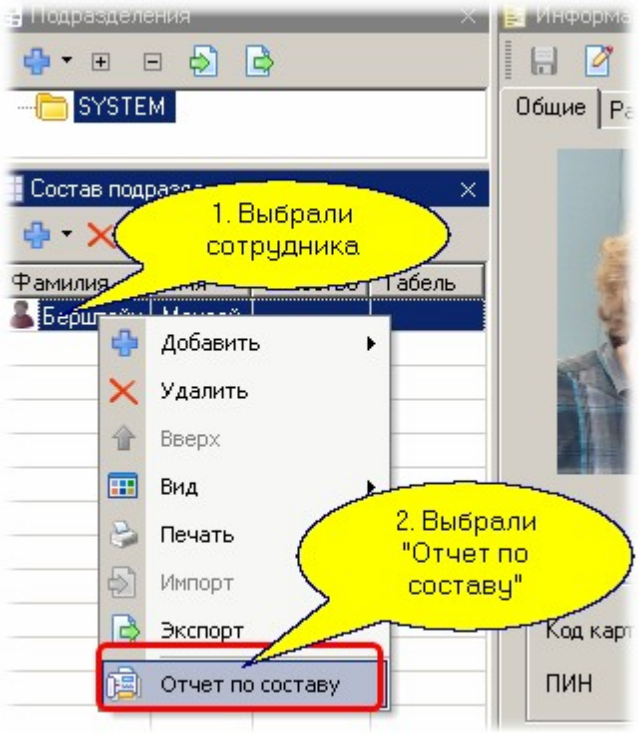
Печать Сохранить 1

СПИСОК ПЕРСОНАЛА

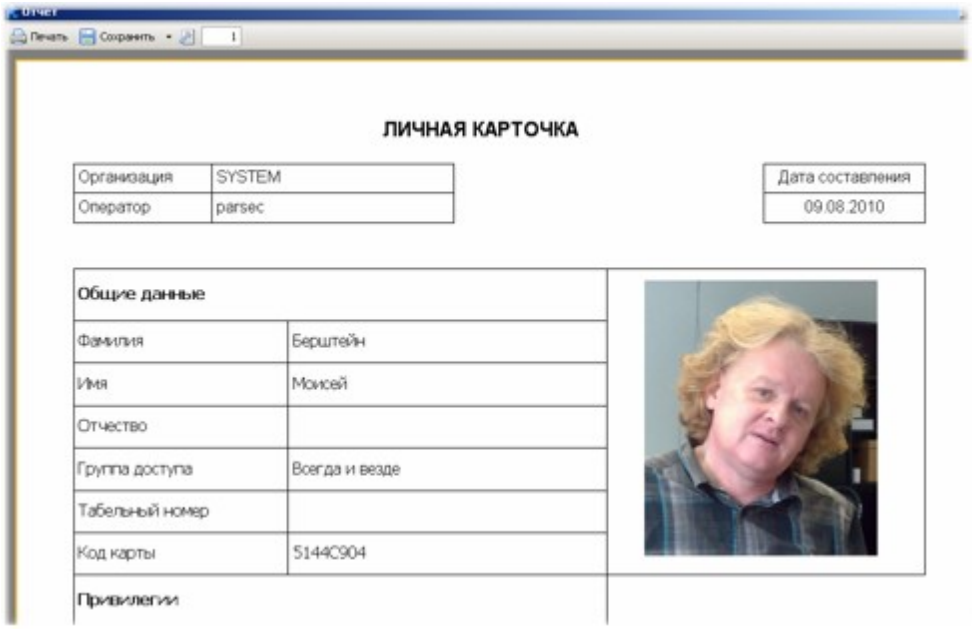
Организация	SYSTEM
Оператор	parsec

№ п/п	Фамилия	Имя	Отчество
			SYSTEM
1	Берштейн	Моисей	

Если же мы в списке персонала подразделения выберем сотрудника, нажмем правую клавишу мыши и выберем "Отчет по составу", как показано ниже:



то появится окно отчета с личной карточкой сотрудника примерно такого вида:



ЛИЧНАЯ КАРТОЧКА

Организация	SYSTEM
Оператор	parsec

Дата составления
09.08.2010

Общие данные	
Фамилия	Берштейн
Имя	Моисей
Отчество	
Группа доступа	Всегда и везде
Табельный номер	
Код карты	5144C904
Привилегии	

В других редакторах отчеты по составу реализованы аналогичным образом.

8.11 Работа с шаблонами в отчетах

Общие положения

В ряде генераторов отчетов системы ParsecNET 3, таких, как учет рабочего времени, отчеты по событиям системы применена технология шаблонов, позволяющая заметно упростить процесс регулярного создания однотипных отчетов.

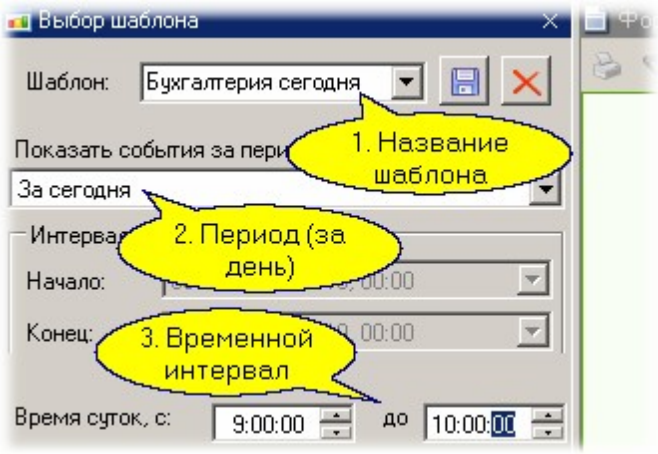
Принцип шаблонов основан на сохранении как параметров отчета (выбираемые территории, персонал, другие критерии), так и сохранении в относительном представлении отчетного периода

(например, "текущая неделя"). В дальнейшем с использованием подгружаемого шаблона можно в любой момент сформировать, например, "отчет по нарушениям за текущую неделю" буквально в два щелчка мышкой.

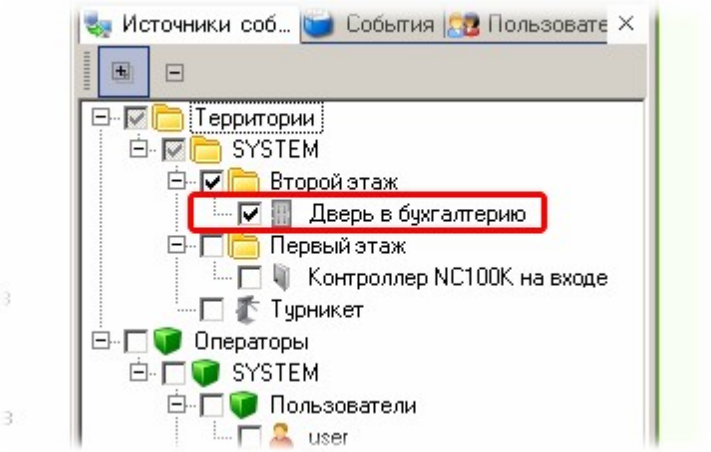
Создание шаблона

Рассмотрим пример использования шаблонов на примере отчета по событиям системы. Для этого воспользуемся соответствующим инструментом[302].

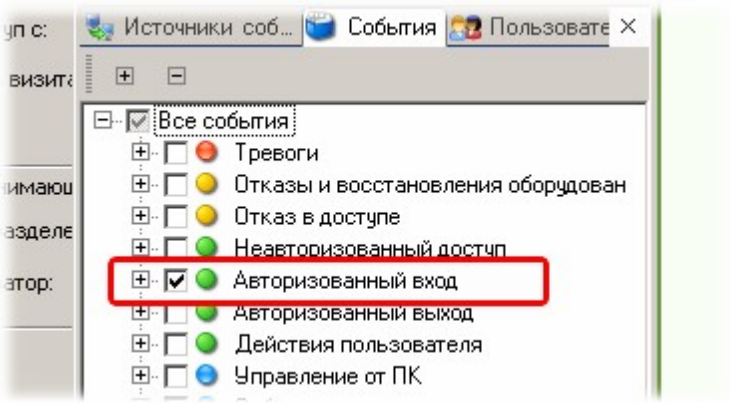
Создадим шаблон для ежедневного анализа прихода сотрудников подразделения "Бухгалтерия" в утренние часы с 9:00 до 10:00. Для этого в генераторе отчетов настроим требуемые нам параметры. В поле *Шаблон* введем его название, затем выберем период "За сегодня", зададим необходимый временной интервал, как показано на следующем рисунке:



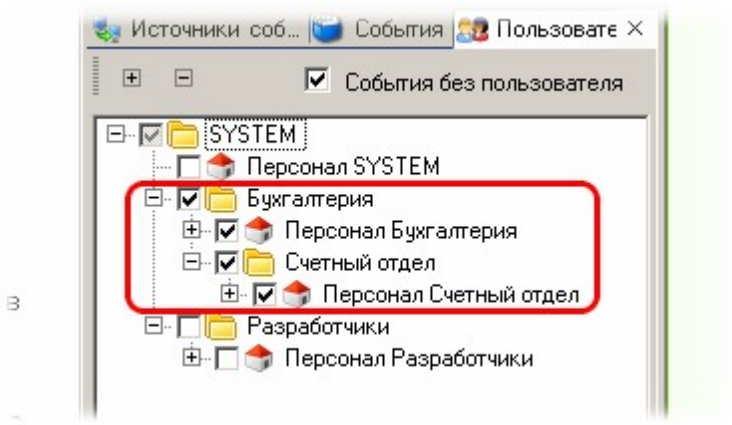
Теперь на вкладке *Источники событий* выберем интересующую нас дверь:



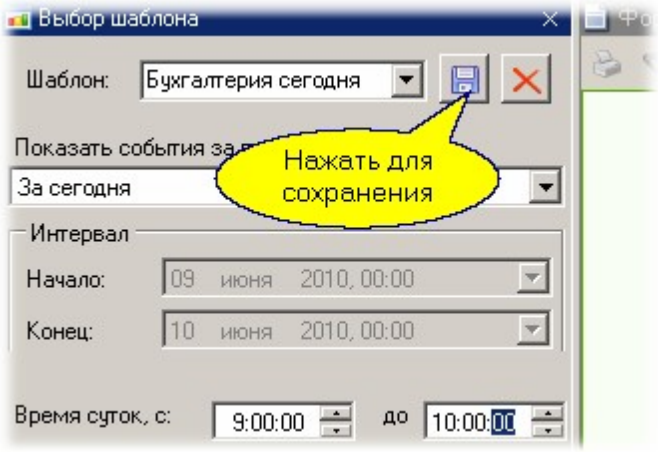
Далее на вкладке *События* отметим "Авторизованный вход":



... и последним шагом на вкладке *Пользователи* выберем свой персонал:



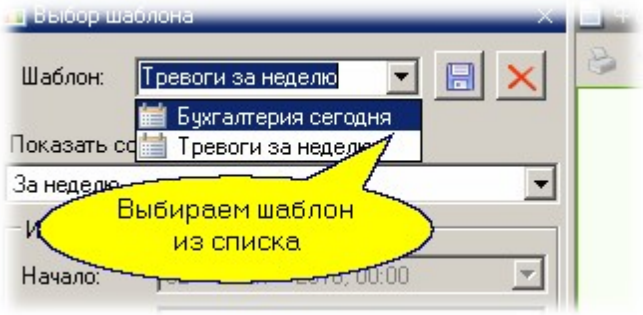
Теперь остается сохранить созданный шаблон, нажав на изображение дискеты рядом с названием нашего шаблона:



Наш шаблон готов, им можно пользоваться.

Использование шаблона

Использовать созданный шаблон очень просто. В генераторе отчетов достаточно выбрать шаблон из раскрывающегося списка, как он автоматически загружается без каких - либо дополнительных действий, что сразу будет видно по автоматической установке параметров шаблона в критериях отчета:



- Для формирования самого отчета теперь достаточно нажать на кнопку *Сформировать*, и вы получаете требуемый отчет на момент его формирования.

См. также:

Отчеты по событиям[302]

Модуль учета рабочего времени[456]

Отчеты бюро пропусков[447]

8.12 Специальные средства

В данном разделе приведено описание специальных средств системы ParsecNET 3. Эти средства предназначены для опытных пользователей, причем некоторые из них доступны только при наличии соответствующей лицензии.

- Редактор организаций[317] предназначен для крупных распределенных систем и позволяет в рамках одной физической системы ParsecNET 3 создать нужное количество виртуальных, полностью независимых систем с разделением по оборудованию, персоналу, операторам. Доступен только в профессиональной версии системы.
- Редактор системных настроек[341] позволяет управлять лицензиями продукта, определяемыми вашим ключом защиты. Кроме того, для опытных пользователей данный редактор даст возможность менять категории транзакций для адаптации системы под специфические нужды.
  - Работа с ключом[344] защиты познакомит вас с тем, как управлять вашими лицензиями на программное обеспечение;
  - Резервное копирование[346] позволит вам сделать резервные копии базы данных всей системы;
  - Система может синхронизироваться с Active Direcory[348];
  - Раздел *Настройка рабочей станции* позволяет выбрать систему распознавания документов[359].
- Редактор заданий[321] предназначен для автоматизации различных процессов в системе: управления оборудованием по времени или событиям.
- Интеграция с алкотестером[141] позволяет организовать особые режимы прохода.
- Для работы на устройствах под управлением ОС Android используется мобильный терминал доступа[360].
- Мобильное приложение Parsec Сотрудник предназначено для телефона в качестве идентификатора субъекта, контроля трудовой дисциплины сотрудников и для работы с заявками Бюро пропусков.



Настоятельно рекомендуется периодически делать резервную копию ваших баз данных на случай поломок оборудования (компьютеров).

8.12.1 Редактор организаций

После установки системы ParsecNET 3 в ней изначально присутствует организация SYSTEM (Система). Для небольших установок этого вполне достаточно. Если же система позиционируется для управления крупными распределенными объектами (например, бизнес-центр), то для полного разделения областей видимости отдельных групп пользователей (например, эксплуатирующая организация и арендаторы в бизнес-центре) потребуется создание дополнительных организаций.



Для работы с редактором организаций требуется специальная лицензия на профессиональную версию системы.

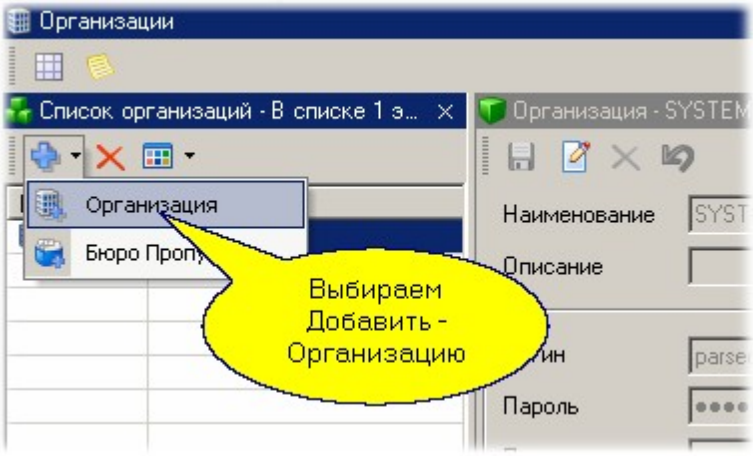
Переименовать системную организацию можно при помощи кнопки *(Переименование организации)*, расположенной на панели инструментов редактора операторов. Выбор размещения кнопки продиктован необходимостью предоставить возможность переименования владельцам всех лицензий, т.к. редактор организаций доступен только в профессиональной версии ПО.

Общие свойства организаций

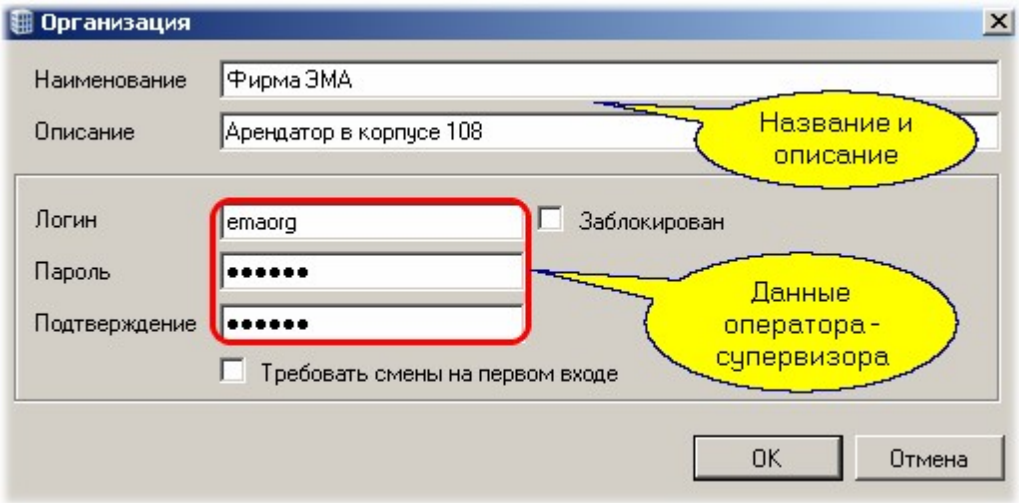
- Организации не образуют иерархии, поскольку они полностью отделены друг от друга;
- В каждой организации имеются свои операторы и свой персонал, недоступные более никому;
- Каждой организации предоставляется доступ к своему набору[71] контроллеров;
- У каждой организации своя внутренняя топология;
- Только главная организация (SYSTEM) имеет доступ к редактору оборудования, редактору организаций и системным настройкам. Как правило, это организация эксплуатирующей компании;
- В каждой организации создаются свои расписания, шаблоны печати, наборы дополнительных полей персонала и так далее.

Создание организации

В редакторе организаций на панели списка организаций выберите из раскрывающегося списка "Добавить - Организация":



В появившемся диалоге вводим следующие данные:



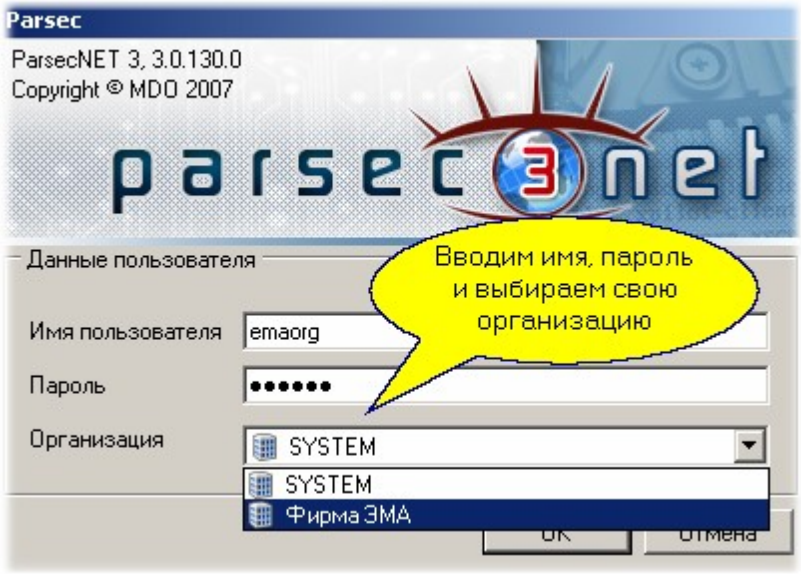
- *Наименование*. Под введенным названием организация будет существовать в системе.
- *Описание*. необязательное справочное поле.
- *Логин*. Имя главного оператора организации. Он создается автоматически и обладаем максимальным набором прав.
- *Пароль* (вводится с подтверждением). Этот пароль используется при входе в организацию.

Две дополнительные опции предназначены для следующих целей:

- *Требовать смены при первом входе*. Если опция отмечена, то после первого входа в систему она автоматически потребует смены пароля. Это может потребоваться, чтобы определенный при создании организации пароль, который может быть известен другим лицам, был заменен на конфиденциальный.
- *Заблокирован*. При отметке этой опции оператор будет заблокирован (то есть не получит входа в систему), пока ему не снимут отметку о блокировке.

Вход в организацию

Если оператор вновь созданной организации не заблокирован, то теперь он может войти в систему в свою организацию. Для этого надо запустить консоль оператора, ввести логин, пароль и выбрать свою организацию:



После входа у вас появится пустой рабочий стол с набором инструментов, за исключением редактора оборудования, редактора организаций и редактора системных настроек, которые доступны только в организации SYSTEM.

Замечания:

1. ***После первого входа рекомендуется сменить пароль оператора организации.***
2. ***Рекомендуется создать нового оператора с новым именем, чтобы он стал никому недоступным вне организации.***
3. ***Следует создать дополнительные группы операторов с ограниченными правами для выполнения отдельных ролей в вашей организации.***

Теперь вы можете создавать свою топологию, назначать операторов, вводить персонал и так далее - все ваши данные будут абсолютно недоступны извне, даже оператору организации SYSTEM.

Единственное, что возможно из организации SYSTEM - это удалить вашу организацию вместе со всеми ее данными.



Важно! Поскольку в вашу организацию более ни у кого нет доступа, тщательно храните пароли для доступа в нее - при утере пароля организация станет недоступной! Рекомендуется завести карточку для доступа оператора по карте, и эту карту хранить в надежном месте.

8.12.2 Редактор заданий

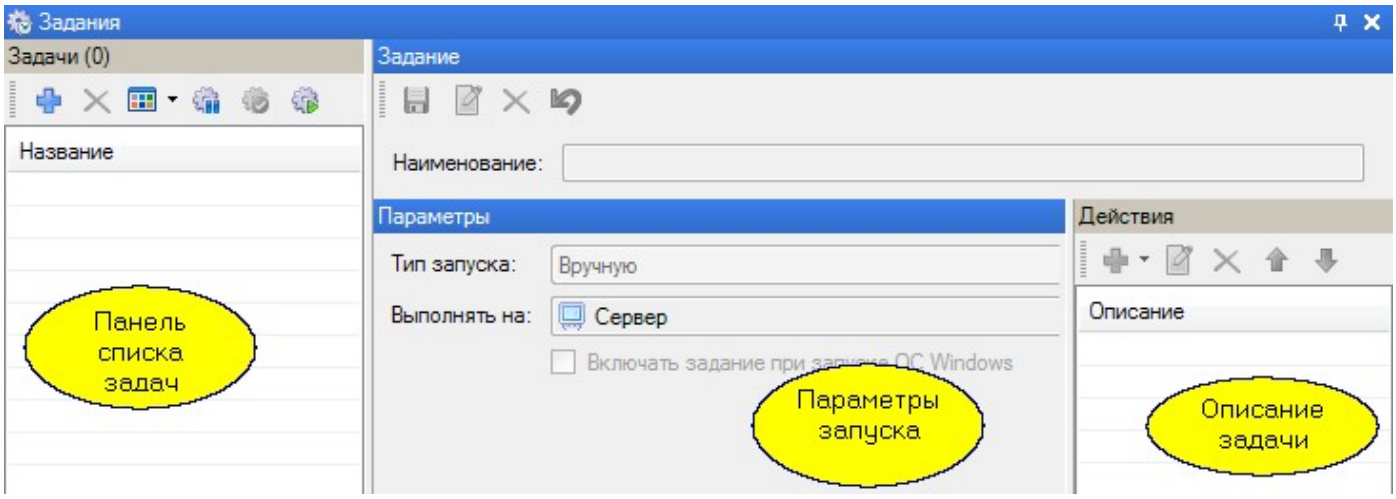
Назначение

Редактор заданий предназначен для создания структуры заданий системе, которые она будет выполнять в соответствии с вашими настройками. За исполнение заданий отвечает специальный сервис системы, который постоянно работает в фоновом режиме как служба Windows.

Частным случаем задания является автоматическое создание резервных копий баз данных системы (раздел Резервное копирование[346]).

Кроме того, Редактор заданий позволяет организовать по событиям или расписаниям рассылку уведомлений в Мини-консоль[394] системы, рассылку SMS - сообщений и электронной почты.

Панели редактора заданий



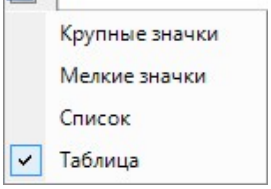
Редактор заданий имеет две панели:

- *Задачи* - содержит список всех задач и элементы управления ими:

  Открыть окно создания нового задания.

  Удалить выбранное задание.

  Выбор способа отображения списка заданий.

  Выключить (деактивировать) задание. Выключенное задание не будет выполняться даже при наступлении заданных условий запуска.

  Включить (активировать) задание.

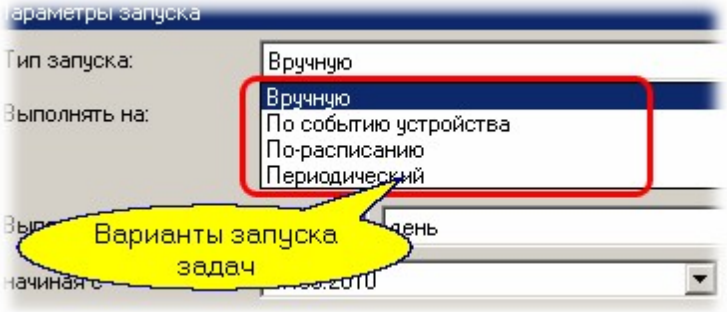
  Выполнить задание немедленно.

- *Задание* - карточка, позволяющая просматривать и редактировать выбранную задачу. Состоит, в свою очередь, из двух панелей:
  - *Параметры* - отображает параметры запуска задания. Набор параметров зависит от выбранного типа запуска задачи

    - Задачи для запуска вручную. Задачи этого типа могут запускаться по команде пользователя из Монитора событий[287] ;

    - Задачи по событию от устройств. Позволяют запрограммировать действие, инициируемое событием с устройства системы (например, событие от контроллера);

- Задачи, запускаемые по времени. К данной категории относятся задачи периодические и задачи, выполняемые по расписанию;



- *Действия* - отображает и позволяет редактировать действия, которые выполняются при запуске задания. Доступны следующие типы действий:

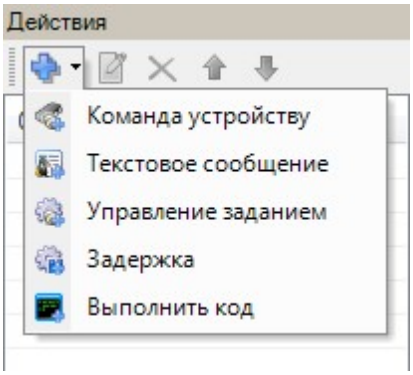
  - Команда устройству или нескольким устройствам;

  - Отправка текстового сообщения[394];

  - Управление другим заданием или несколькими заданиями;

  - Выполнение временной задержки между выполнением последовательных действий;

  - Выполнение стороннего кода[327].



Кнопки  и  перемещают выбранное действие, соответственно, вверх или вниз, позволяя настроить очередность их выполнения.

См. также:

Резервное копирование[346]

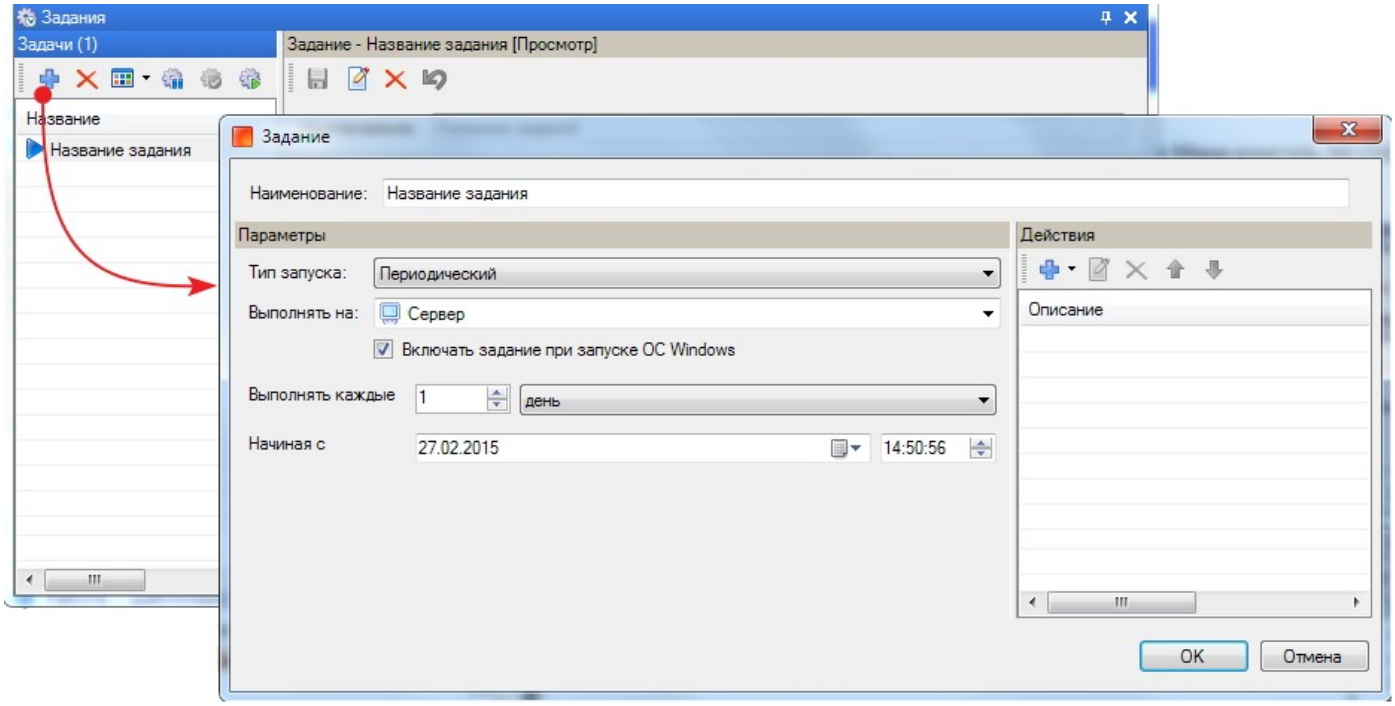
Редактор системных настроек[341]

Мини-консоль[394]

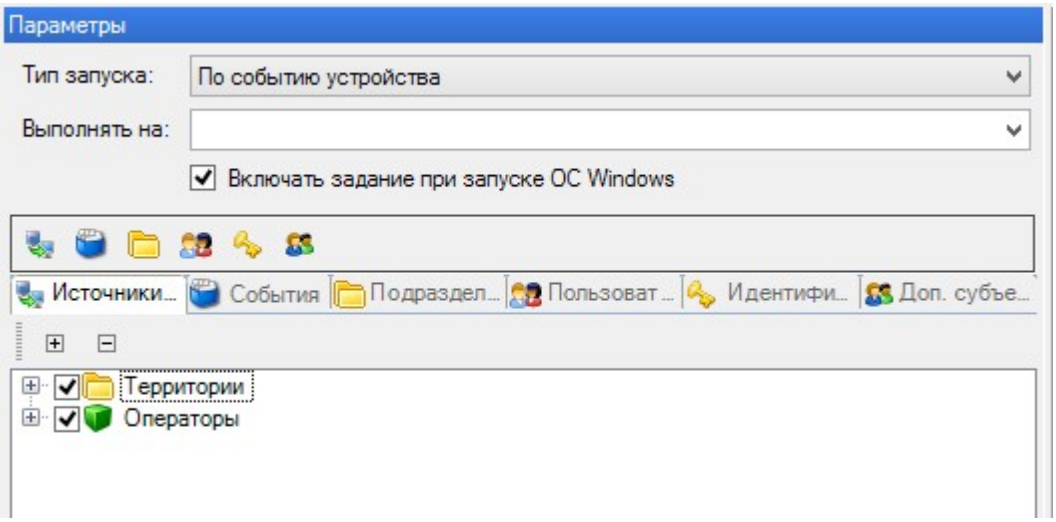
8.12.2.1 Создание задания

Чтобы создать задание выполните следующие шаги:

1. Процедура создания задания начинается с нажатия на кнопку *(Создать)* на панели *Задания* Редактора заданий. При этом открывается окно создания задания:



2. Введите наименование задания в соответствующее поле;
3. Из раскрывающегося списка *Тип запуска* выберите, как должно инициализироваться выполнение задания. От выбора типа зависит набор параметров настройки запуска:
   - **Вручную**. При ручном запуске задания дополнительных параметров настройки нет;
   - **По событию устройства**

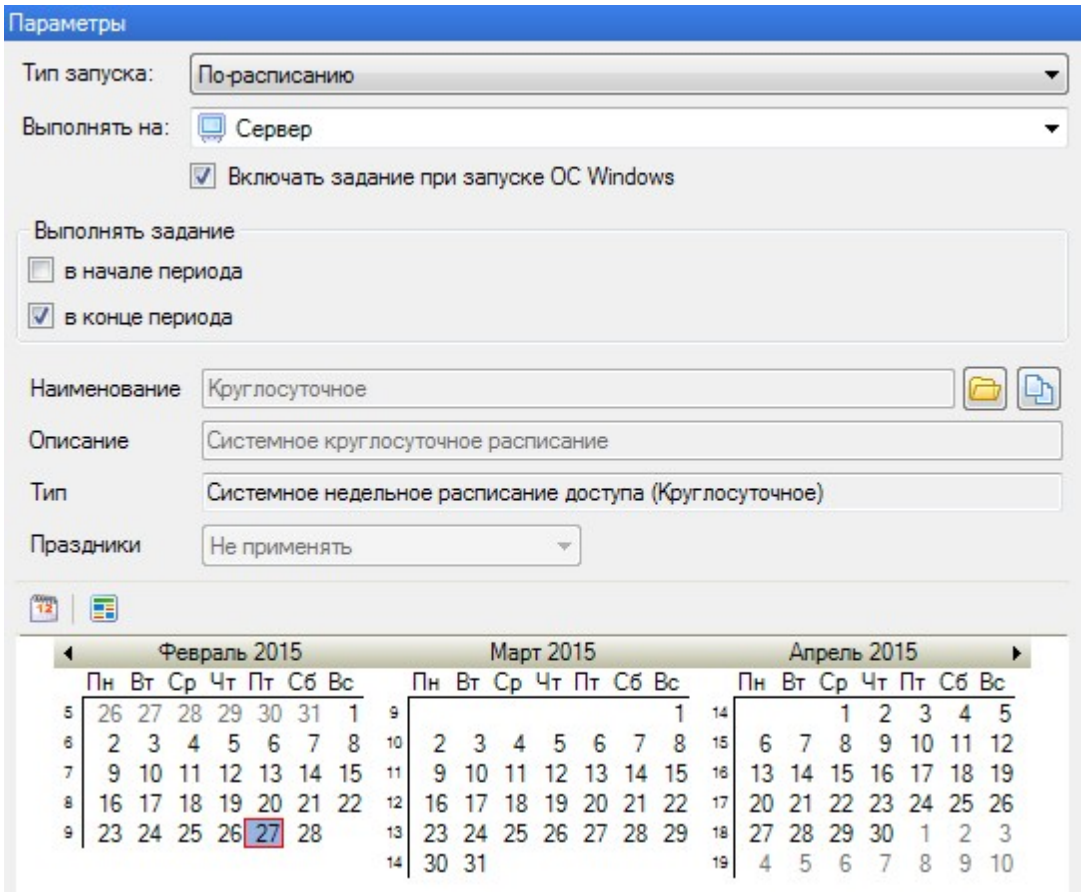


   - В раскрывающемся списке *Выполнять на* выберите, где должно быть выполнено задание: на сервере или на дополнительной рабочей станции;
   - Если задание должно активироваться при старте ОС, установите соответствующий флажок. В противном случае, его каждый раз придется включать кнопкой  на панели *Задания*;
   - Выбором элементов на вкладках формируется комплекс условий выполнения задания:

     - На вкладке *Источник события* указываются компоненты системы, которые порождают события. Данные события инициируют выполнение задания;
     - На вкладке *События* указывается какие события будут запускать выполнение задания. Если конкретные события не указаны, то задание будет выполняться по любому событию в системе;

- На вкладке *Подразделения* выбираются структурные единицы организации. События, в которых фигурируют субъекты доступа этих подразделений, будут запускать задание. Данная категория условий запуска задания может использоваться как отдельно, так и совместно с индивидуально выбранными на вкладке *Пользователи* субъектами доступа;
- На вкладке *Пользователи* выбираются конкретные субъекты доступа. События, в которых фигурируют эти субъекты доступа, будут запускать выполнение задания;
- На вкладке *Идентификаторы* выбираются конкретные идентификаторы. События, в которых фигурируют эти идентификаторы, будут запускать выполнение задания;
- На вкладке *Доп.субъекты* выбираются субъекты, наличие которых в качестве второго лица при групповом проходе (проходе с сопровождающим) будет запускать выполнение задания. Вместо конкретного субъекта можно выбрать подразделение. В этом случае любой сотрудник данного подразделения будет инициировать выполнения задания, при участии "вторым номером" в парном проходе.

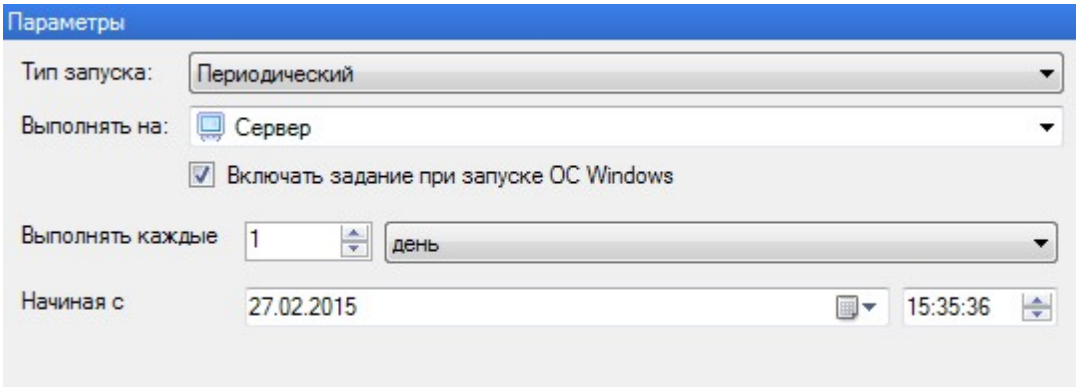
- **По расписанию**



- В раскрывающемся списке *Выполнять на:* выберите, где должно быть выполнено задание: на сервере или на дополнительной рабочей станции;
- Если задание должно активироваться при старте ОС, установите соответствующий флажок. В противном случае, его каждый раз придется включать кнопкой на панели *Задания*;
- В блоке *Выполнить задание* установите флажки в соответствии с тем, в какой момент временного периода, указанного в расписании, должно выполняться задание. Например, задание по постановке на охрану всех дверей привязано к расписанию, в котором доступ разрешен с 8.30 до 18.30. В этом случае устанавливается флажок *в конце периода*;
- Нажав на кнопку (*Выбрать...)* выберите расписание, которое будет использоваться для запуска выполнения задания. Если подходящего расписания нет,

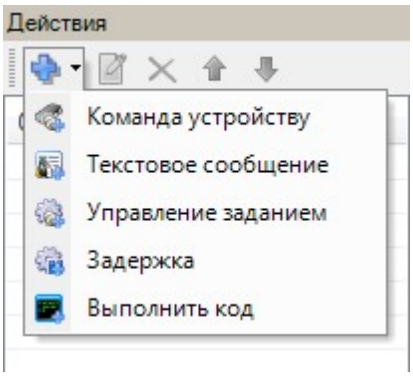
его можно создать, нажав на кнопку (*Создать копию...)* и внеся изменения в скопированное расписание (подробнее см. Редактор расписаний[213]);

- **Периодический**

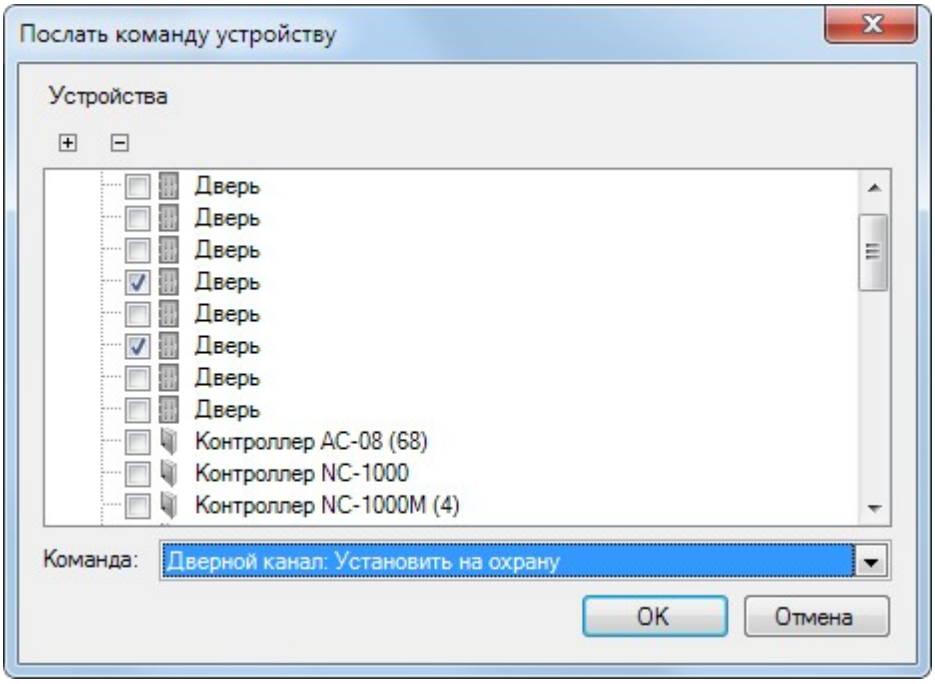


  - В раскрывающемся списке *Выполнять на:* выберите, где должно быть выполнено задание: на сервере или на дополнительной рабочей станции;
  - Если задание должно активироваться при старте ОС, установите соответствующий флажок. В противном случае, его каждый раз придется включать кнопкой на панели *Задания*;
  - В поле *Выполнять каждые* укажите частоту выполнения задания;
  - В поле *Начиная с* укажите дату и время с которого начнется отсчет периодичности выполнения задания.

4. Определите, какие действия должны быть выполнены в рамках данной задачи. Для этого нажмите на кнопку *(Добавить)* на панели *Действия*. В открывшемся списке выберите какой тип действия должен быть выполнен



- **Команда устройству**



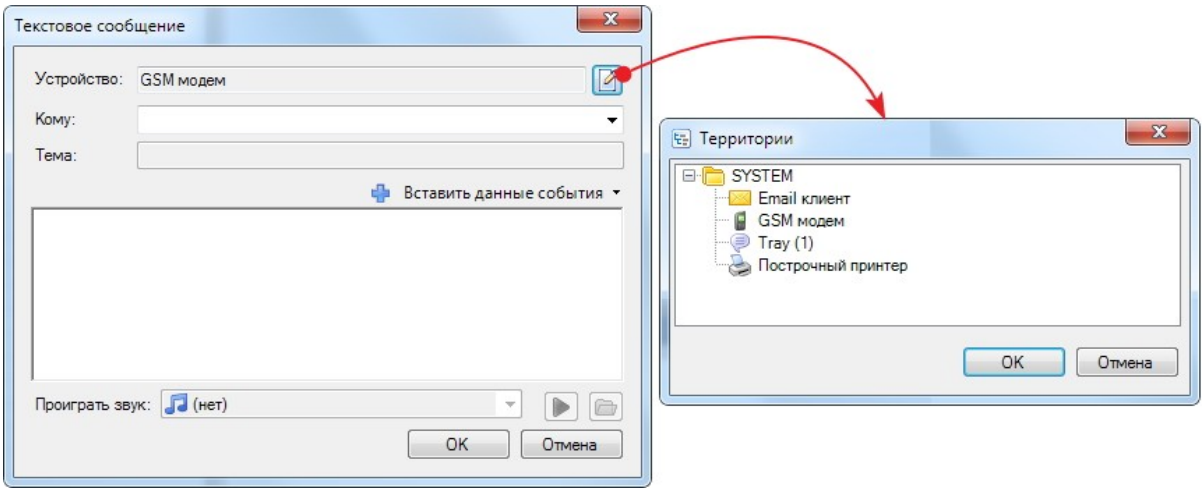
- Выберите одно или несколько однотипных устройств;
- В раскрывающемся списке *Команда* выберите, какую команду должны выполнить выбранные устройства.

- **Текстовое сообщение**

Текстовое сообщение можно послать 4 различными способами:

- на электронную почту;
- при помощи SMS;
- на распечатку на построчном принтере;
- как уведомление в мини-консоль.

Подробнее о текстовых сообщениях см. раздел Текстовые сообщения[394] .

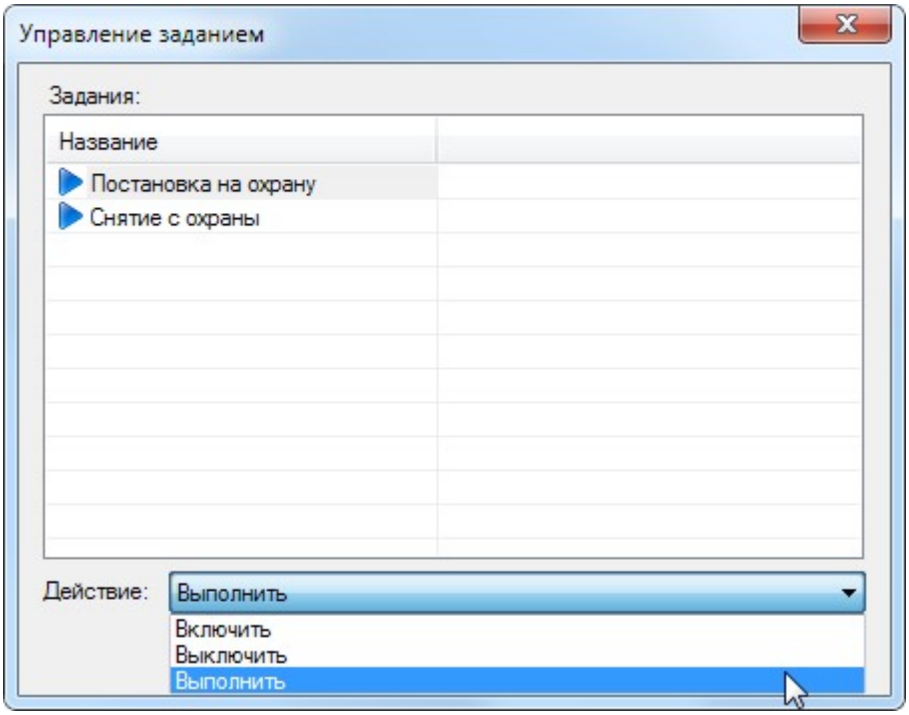


- Нажмите на кнопку (*Изменить)* в поле *Устройство* и в открывшемся окне *Территории* выберите, на какое устройство нужно отправить сообщение;
- Заполните активные поля в окне *Текстовое сообщение*:

  - *Кому* - введите e-mail адрес или телефон для SMS;

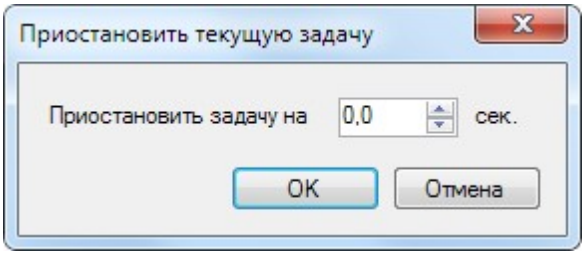
- Для e-mail можно ввести название темы сообщения;
- Нажав на кнопку (*Вставить данные события)* можно выбрать данные о событии, которые будут отображены в сообщении;
- Введите текст сообщения;
- Для извещения через мини-консоль можно указать звуковой файл, который будет проигрываться при появлении сообщения. Извещение будет появляться в той мини консоли, которая выбрана при создании задания.

- **Управление заданием**



- Выберите задание;
- Из раскрывающего списка *Действие* выберите, что нужно сделать с указанным заданием.

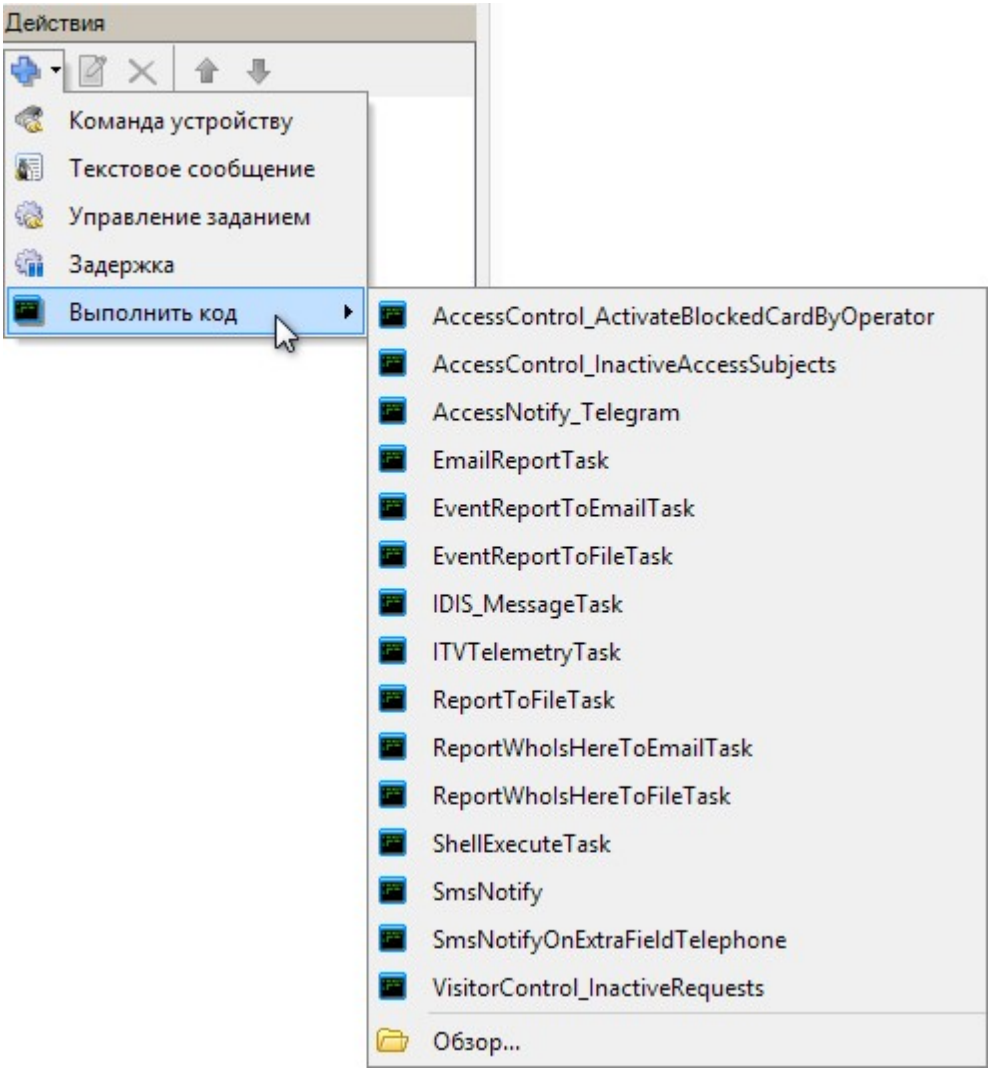
- **Задержка**



Установите время, которое система должна выждать, прежде чем выполнить следующее действие текущей задачи.

- **Выполнить код**

Набор исполняемых файлов, которые могут использоваться в заданиях, находится в папке SCRIPTS в каталоге установки Системы. Выполняемые файлы доступны в списке:



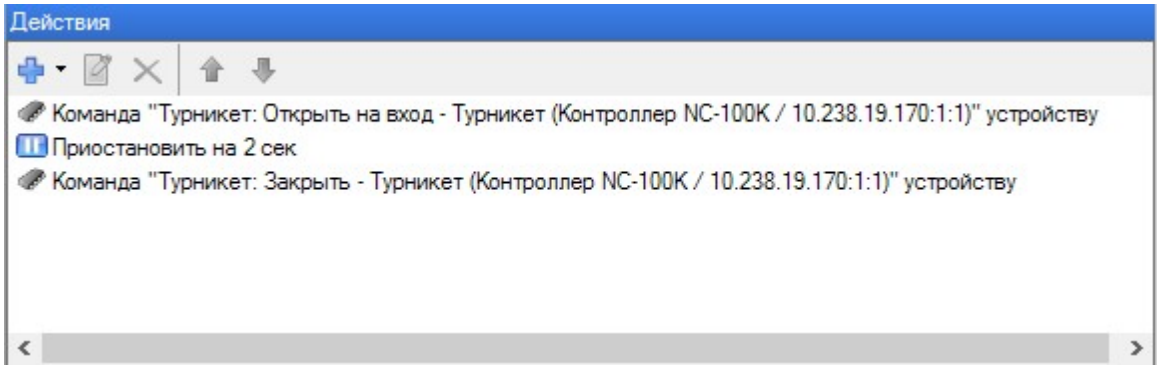
- Для выбора другого исполняемого файла нажмите на кнопку *Обзор...* и выберите нужный файл;

На текущий момент доступен следующий набор наиболее востребованных скриптов в формате cs:
- AccessControl_ActivateBlockedCardByOperator - снятие блокировки[283] картой оператора;
- AccessControl_InactiveAccessSubjects - управление неактивными субъектами доступа и идентификаторами[333];
- AccessNotify_Telegram - отправка уведомления[408] о событии в мессенджер Telegram;
- EmailReportTask - создание отчета УРВ и отправка[329] его на указанный адрес электронной почты;
- EventReportToEmailTask - создание отчета по событиям системы[336] и отправка его на указанный адрес электронной почты;
- EventReportToFileTask - создание отчета по событиям системы[336] и сохранение его в файл;
- IDIS_MessageTask - отправка сообщения в видеосистему IDIS[332];
- ITVTelemetryTask - автоматизация работы ИСБ "Интеллект"[525];
- ReportToFileTask - создание отчета УРВ и сохранение[331] его в выбранной директории;

- ReportWhoIsHereToEmailTask - создание отчета "Не покидали территорию"[339] и отправка его на указанный адрес электронной почты;
- ReportWhoIsHereToFileTask - создание отчета "Не покидали территорию"[339] и сохранение его в файл;
- ShellExecuteTask - запуск внешнего исполняемого файла;
- SmsNotify - отправка SMS сообщения через интернет-портал[402];
- SmsNotifyOnExtraFieldTelephone - отправка SMS сообщения на телефон, указанный в системном дополнительном поле;
- VisitorControl_InactiveRequests - управление заявками бюро пропусков[335].

- Для доступа к исполняемому файлу введите логин и пароль оператора, имеющего право на выполнение тех действий, которые автоматизированы этим исполняемым файлом.

5. Повторите шаг 4 столько раз, сколько действий должно быть выполнено в создаваемой задаче. Например, можно не просто выбрать одно действие, а описать последовательность действий, как показано на рисунке ниже. Здесь турникету подается команда "Открыть на вход", затем идет задержка в 2 секунды, а в заключение - команда закрыть турникет.



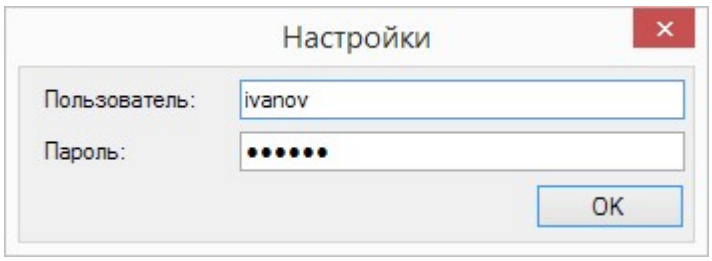
6. Закончив настройку задачи, нажмите на кнопку *OK*, оно появится на панели *Задачи*.

Не забывайте для создаваемого задания ставить флажок "Включать задание при старте ОС Windows" в параметрах запуска, иначе задача не будет работать.

8.12.2.1.1 Создание, сохранение и отправка на Email отчета УРВ

Система позволяет формировать отчеты УРВ и отправлять их на указанный почтовый адрес или сохранять в заданной директории.

В обоих случаях при выборе выполнения кода[327] на создание отчета и отправку на почту (EmailReportTask) или на создание и сохранение отчета УРВ в заданной директории (ReportToFileTask) на экране появится окно аутентификации:

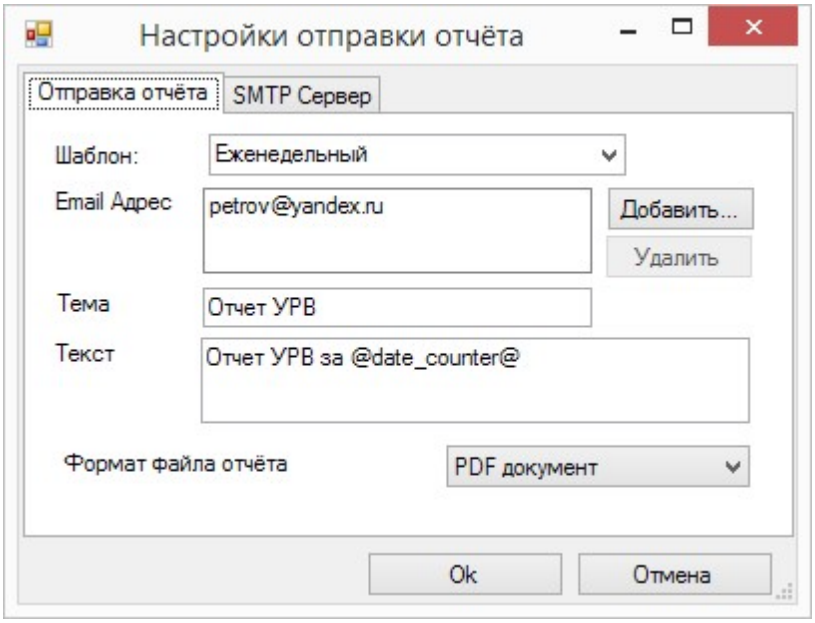


Введите имя и пароль пользователя, от имени которого будет запускаться задание (это не обязательно должен быть оператор, создающий данное задание).

Далее настройки отличаются.

Создание отчета УРВ и отправка его на электронную почту

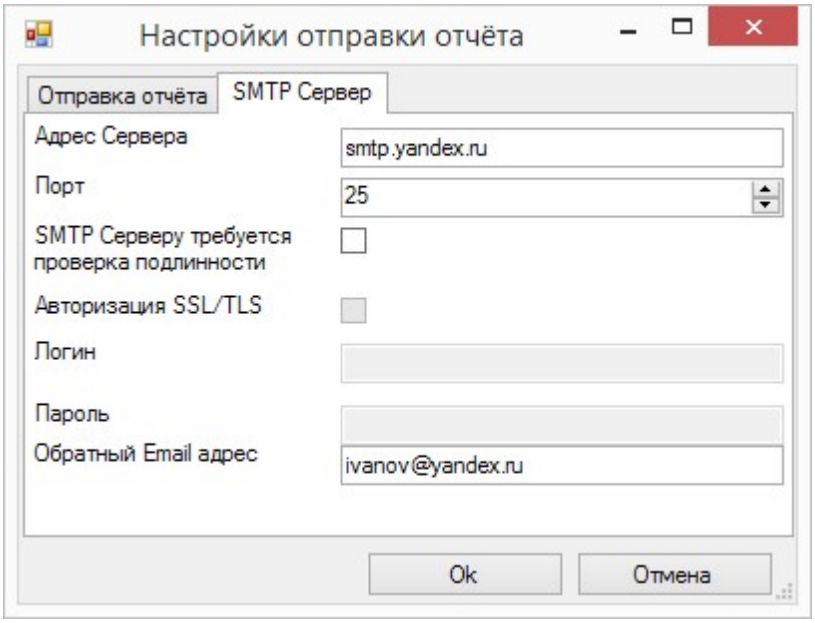
После нажатия на кнопку *ОК* в окне *Настройки*[329] появится окно *Настройки отправки отчета*:



Заполните поля:

- *Шаблон* - выберите шаблон отчета[473] ;
- *E-mail Адрес* - укажите адрес (несколько адресов) электронной почты, на который(-е) хотите получать отчет, нажав на кнопку *Добавить…;*
- *Тема* - введите тему, которая будет автоматически вставляться в отправляемое письмо;
- *Текст* - введите текст, который будет автоматически вставляться в отправляемое письмо;
- *Формат файла отчета* - выберите, в каком формате хотите получать отчет.

Перейдите на вкладку *SMTP Сервер*.



Заполните поля:

- *Адрес сервера* - введите адрес своего почтового сервера;
- *Порт* - введите номер порта для подключения к SMTP серверу;
- *SMTP серверу требуется проверка подлинности* - при установке флажка станут доступными поля:

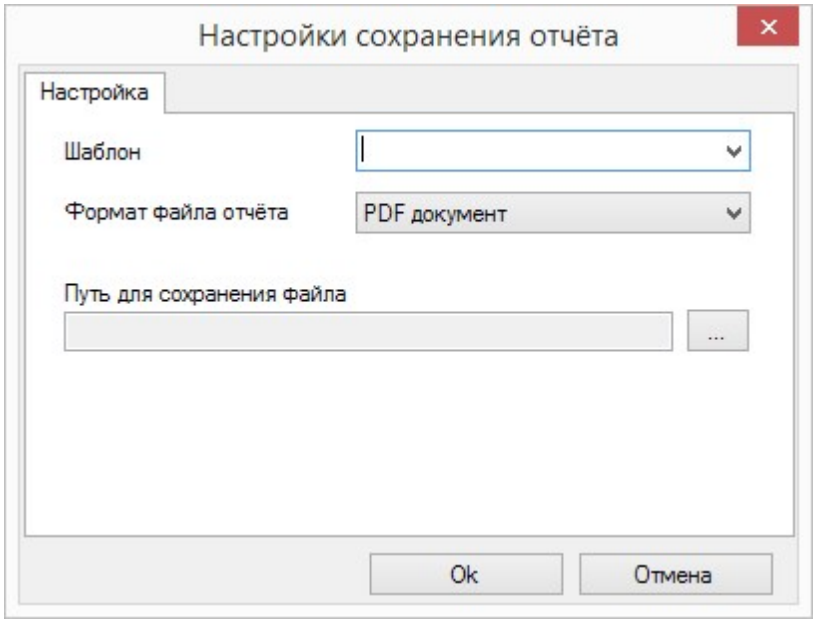
- *Авторизация SSL/TLS* - при установленном флажке авторизация будет производиться по клиентским TLS/SSL сертификатам. При установке флажка порт SMTP сервера выбирается автоматически, значение в поле *Порт* не учитывается;
- *Логин* - имя пользователя для SMTP сервера;
- *Пароль* - пароль для SMTP сервера;

- *Обратный E-mail адрес* - укажите адрес электронной почты для получения системных сообщений и т.п.

По завершении всех настроек нажмите на кнопку *ОК* и продолжите создание задания[322] .

Создание отчета УРВ и сохранение его в заданной директории

После нажатия на кнопку *ОК* в окне *Настройки*[329] появится окно *Настройки сохранения отчета*:



Заполните поля:

- *Шаблон* - выберите шаблон отчета[473] ;
- *Формат файла отчета* - выберите, в каком формате хотите получать отчет;
- *Путь для сохранения файла* - укажите директорию, в которой будет сохраняться отчет. При желании можно задать имя файла с использованием спец. символов, которые при выполнении задания будут трансформироваться в дату начала отчетного периода:

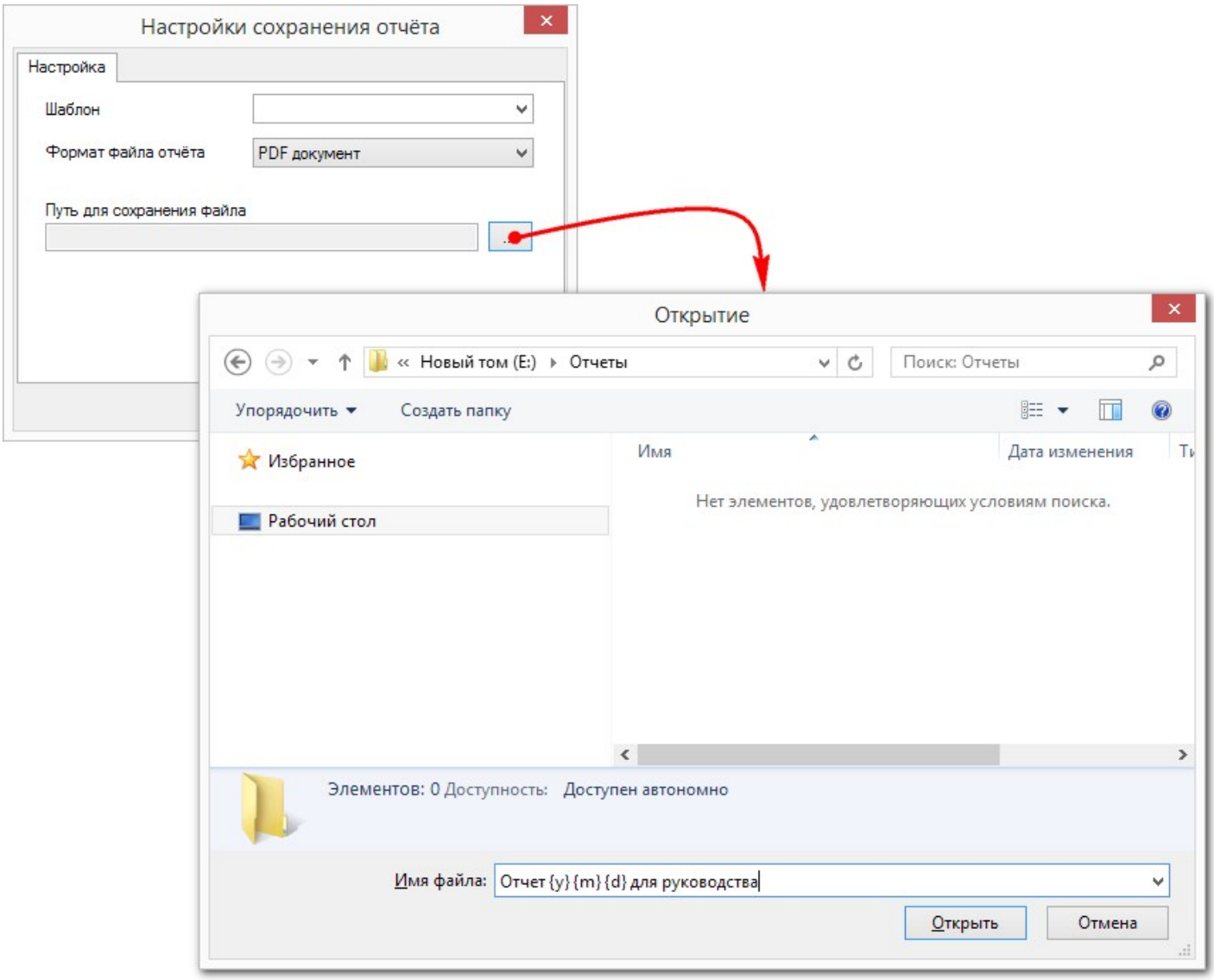
  {d} - день

  {m} - полный месяц

  {y} - год

  Имя файла при этом должно иметь вид, например, "Отчет {y} {m} {d} для руководства" как на рисунке ниже.

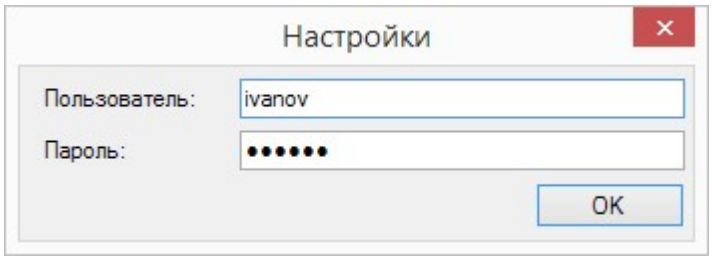
Сформированный отчет заменяет предыдущий отчет с таким же именем, если тот находится в той же директории.



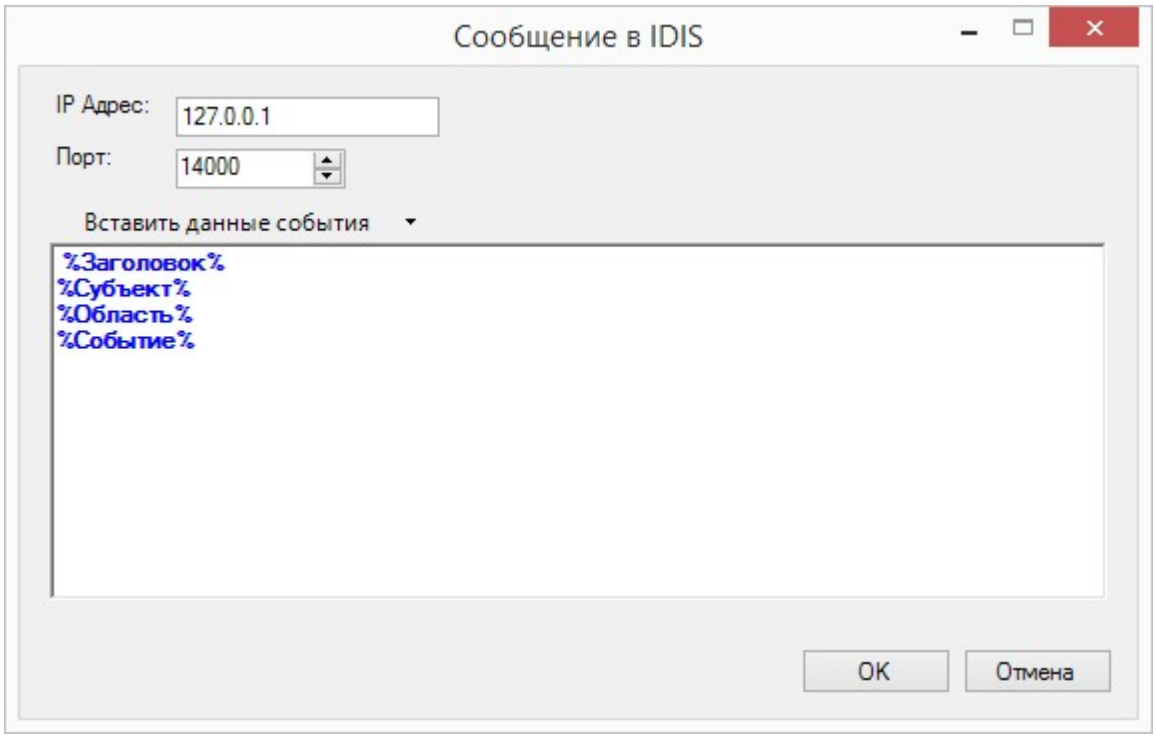
- Нажмите на кнопку *OK* и продолжите создание задания[322].

8.12.2.1.2 Сообщение в видеосистему IDIS

При выборе выполнения кода[327] на отправку сообщения в видеосистему IDIS (IDIS_MessageTask) откроется окно аутентификации:



Введите имя и пароль пользователя, от имени которого будет запускаться задание.
После нажатия на кнопку *OK* появится окно *Сообщение в IDIS*:



Заполните поля:

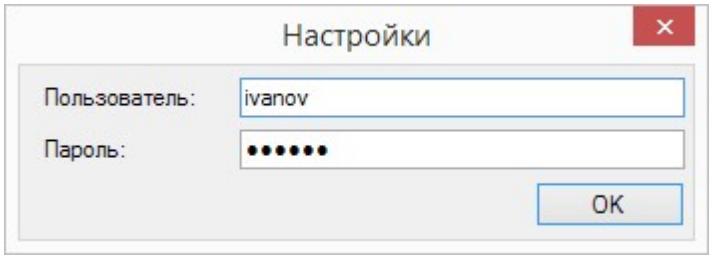
- *IP адрес* - укажите IP адрес сервера видеосистемы IDIS;
- *Порт* - порт, определенный за каналом записи, который соответствует контроллеру СКУД;
- В табличной части введите текст или выберите из раскрывающегося списка *Вставить данные события* нужный набор сведений о событии.

По завершении нажмите на кнопку *OK* и продолжите создание задания[322] .

8.12.2.1.3 Управление неактивными субъектами доступа и идентификаторами

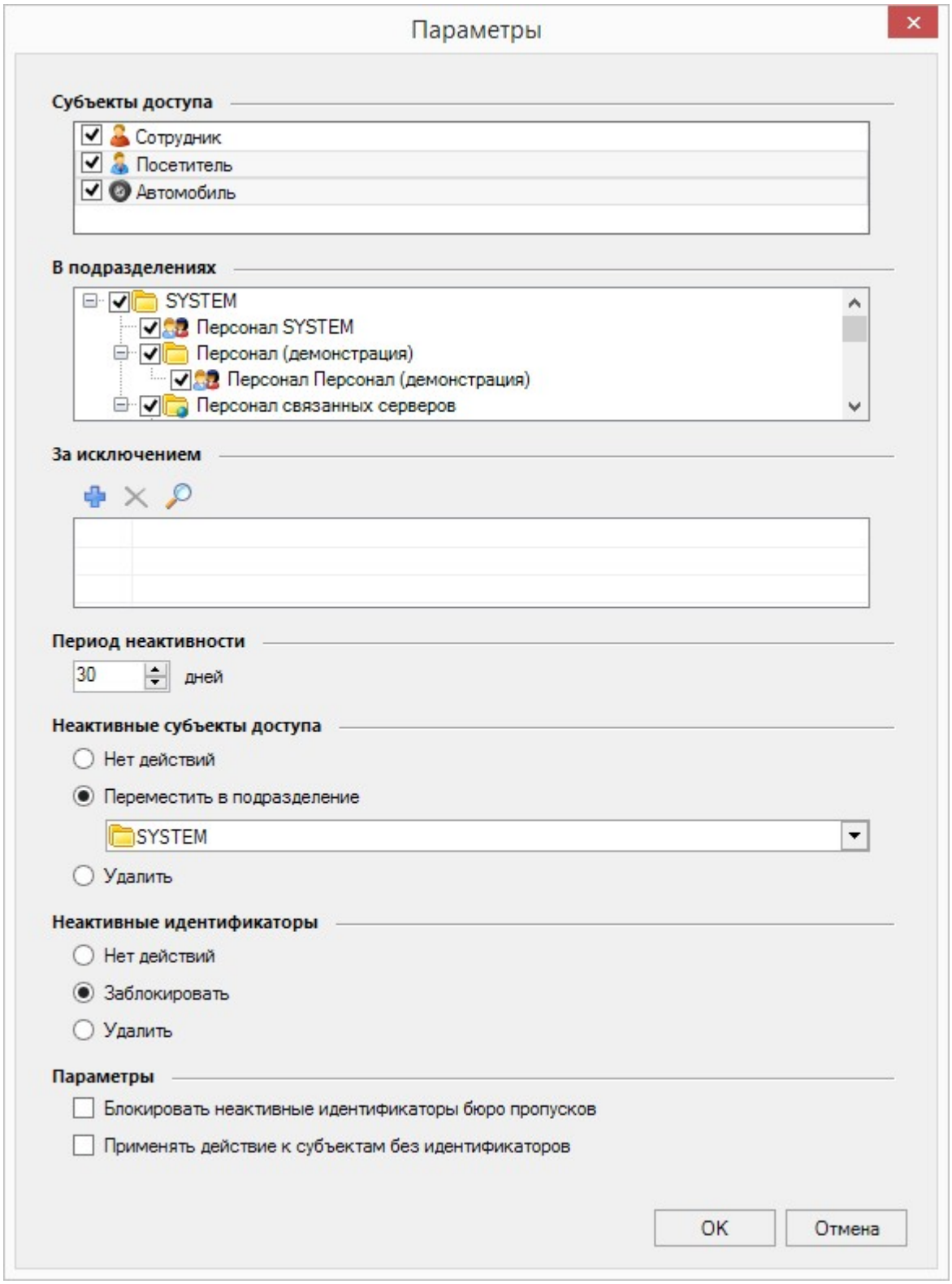
Обрабатываются только идентификаторы, входящие в группы доступа категории "Подсистема доступа Parsec".

При выборе выполнения кода[327] по управлению неактивными субъектами доступа и идентификаторами (AccessControl_InactiveAccessSubjects) откроется окно аутентификации:



Введите имя и пароль пользователя, от имени которого будет запускаться задание.

После нажатия на кнопку *OK* появится окно параметров:



Установите необходимые параметры для выбора субъектов доступа и/или идентификаторов и задайте срок неактивности. Определите, как должно поступить с выбранными субъектами и идентификаторами при превышении заданного времени неактивности, после чего нажмите на кнопку *ОК*.

Теперь вернитесь к созданию задания[322].

Термины, используемые при описании работы скрипта:

- *последняя активность идентификатора* - время создания идентификатора или последнего события доступа;

- *неактивный идентификатор* - идентификатор, с последней активности которого прошло большее количество дней, указанных в блоке *Период неактивности*;
- *неактивный субъект доступа* - субъект доступа, у которого **все** идентификаторы неактивны на момент фактического выполнения задания.

При выполнении скрипта, анализируются идентификаторы, входящие в группы доступа, созданные в категории "Подсистема доступа Parsec". Если с момента последней активности таких идентификаторов прошло больше времени, чем указано в настройках, то он признается неактивным. Причем период неактивности высчитывается с точного времени выполнения задания, т.е., например, если задан период неактивности 5 дней и задание выполняется в 12:00 10 октября, то неактивными будут все идентификаторы, последняя активность которых была ранее 12:00 5 октября.

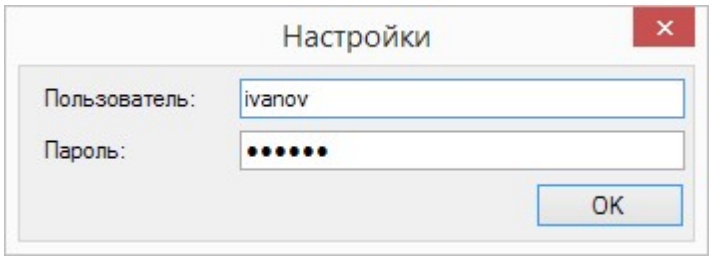
После определения неактивных идентификаторов и неактивных субъектов доступа скрипт выполняет с ними заданные в настройках действия.

Флажки:

- *Блокировать неактивные идентификаторы бюро пропусков* - если флажок не стоит, то идентификаторы из пула Бюро пропусков игнорируются.
  Субъекты доступа, созданные в Бюро пропусков (посетители), с которыми связаны какие-либо заявки (в любом статусе), не обрабатываются (для работы с заявками Бюро пропусков обратитесь к описанию соответствующего скрипта[335]).
- *Применять действие к субъектам без идентификаторов* - при установке флажка субъекты, которым не назначен ни один идентификатор, считаются неактивными и к ним применяются заданные настройками действия.

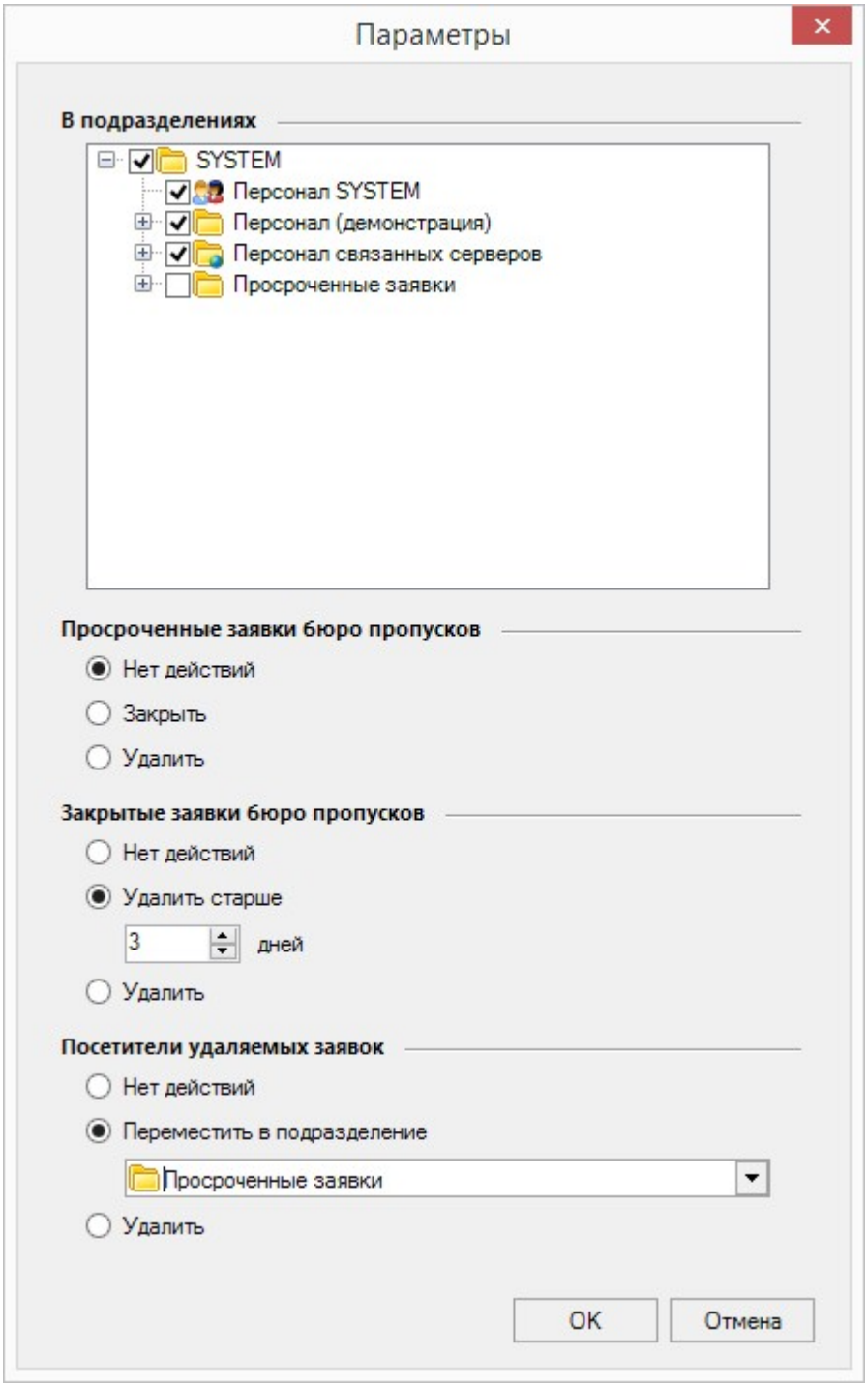
8.12.2.1.4 Управление заявками бюро пропусков

При выборе выполнения кода[327] по управлению заявками Бюро пропусков (VisitorControl_InactiveRequests) откроется окно аутентификации:



Введите имя и пароль пользователя, от имени которого будет запускаться задание.

После нажатия на кнопку *ОК* появится окно параметров:



Установите, заявки каких подразделений (указаны в блоке *Принимающая сторона* в заявке) необходимо проанализировать. Определите, как должно поступить с просроченными и/или закрытыми заявкам и их посетителями, после чего нажмите на кнопку *ОК*.

Теперь вернитесь к созданию задания[322].

При выполнении скрипта сначала обрабатываются заявки, затем субъекты доступа (посетители).

Если при выполнении данного скрипта с посетителями удаленных заявок никаких действий не выполнялось, они могут быть обработаны скриптом Управление неактивными субъектами доступа и идентификаторами[333], при условии установки флажка *Блокировать неактивные идентификаторы бюро пропусков.*

8.12.2.1.5 Создание отчета по событиям системы

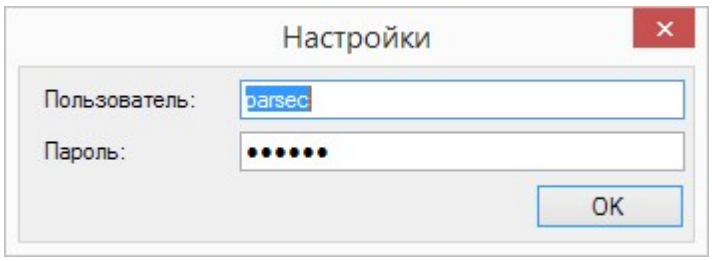
Отчет по событиям системы может быть сформирован при помощи задания, активирующего один из двух исполняемых файлов:

- EventReportToEmailTask - создание отчета по событиям системы и отправка его на указанный адрес электронной почты;

- EventReportToFileTask - создание отчета по событиям системы и сохранение его в файл.

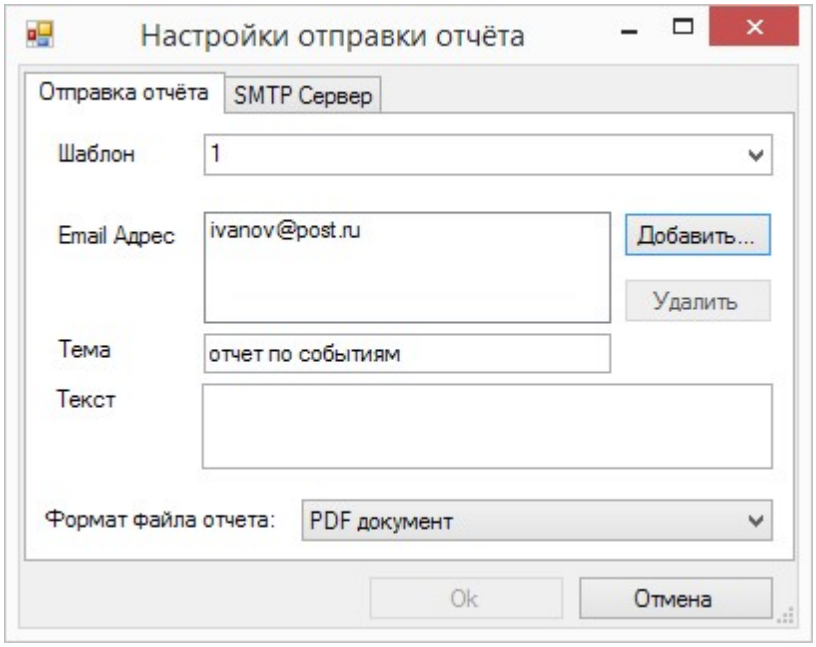
Прежде чем браться за настройку данного задания, необходимо при помощи инструмента Отчеты по событиям[302] создать шаблон отчета, который будет формироваться и отсылаться на почту либо сохраняться в файл.

При выборе выполнения кода[327] по созданию отчета, откроется окно аутентификации:



Введите имя и пароль пользователя, от имени которого будет запускаться задание.

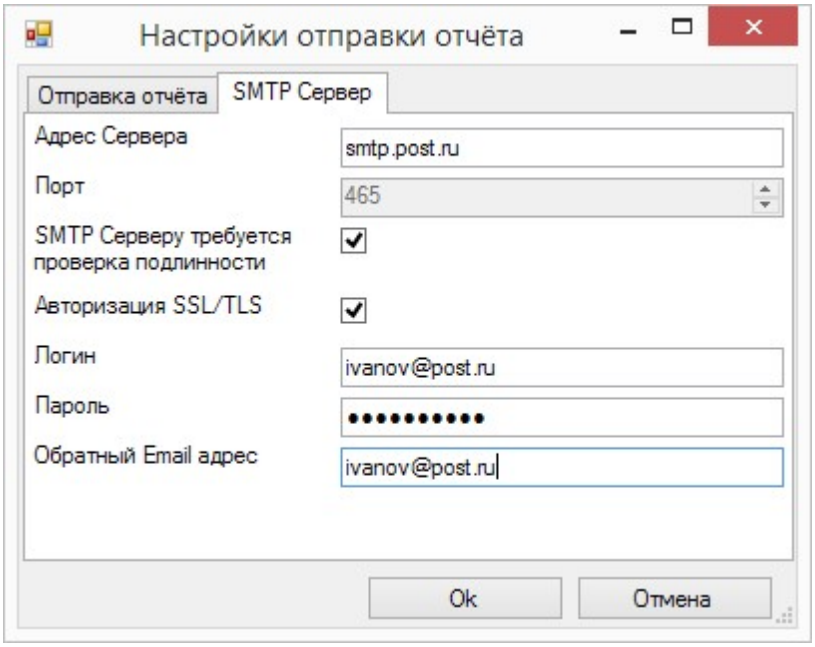
После нажатия на кнопку *ОК* появится окно настройки параметров отправки (если выбран скрипт EventReportToEmailTask) либо окно настройки параметров сохранения[338] (если выбран скрипт EventReportToFileTask):



Заполните поля:

- *Шаблон* - выберите шаблон отчета[302];
- *E-mail Адрес* - укажите адрес (несколько адресов) электронной почты, на который(-е) хотите получать отчет, нажав на кнопку *Добавить...;*
- *Тема* - введите тему, которая будет автоматически вставляться в отправляемое письмо;
- *Текст* - введите текст, который будет автоматически вставляться в отправляемое письмо;
- *Формат файла отчета* - выберите, в каком формате хотите получать отчет.

Перейдите на вкладку *SMTP Сервер*.

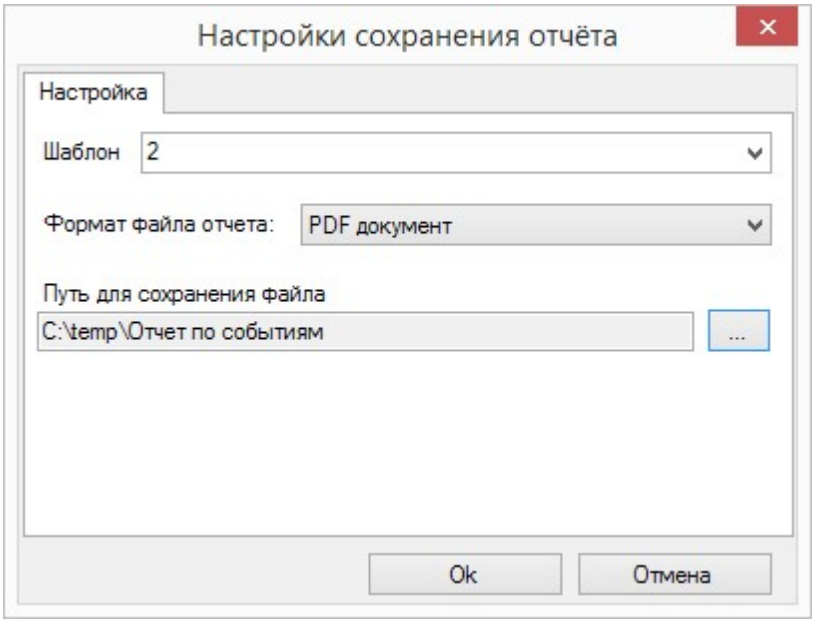


Заполните поля:

- *Адрес сервера* - введите адрес своего почтового сервера;
- *Порт* - введите номер порта для подключения к SMTP серверу;
- *SMTP серверу требуется проверка подлинности* - при установке флажка станут доступными поля:
  - *Авторизация SSL/TLS* - при установленном флажке авторизация будет производиться по клиентским TLS/SSL сертификатам. При установке флажка порт SMTP сервера выбирается автоматически, значение в поле *Порт* не учитывается;
  - *Логин* - имя пользователя для SMTP сервера;
  - *Пароль* - пароль для SMTP сервера;
- *Обратный E-mail адрес* - укажите адрес электронной почты для получения системных сообщений и т.п.

По завершении всех настроек нажмите на кнопку *ОК* и продолжите создание задания 322.

Если выбран скрипт EventReportToFileTask, то после аутентификации пользователя откроется окно настройки сохранения отчета:



Заполните поля:

- *Шаблон* - выберите шаблон отчета[302] ;
- *Формат файла отчета* - выберите, в каком формате хотите получать отчет.
- *Путь для сохранения файла* - укажите директорию, в которой будет сохраняться генерируемый файл, и его имя.

Файл отчета переписывается каждый раз при сохранении в указанной директории.

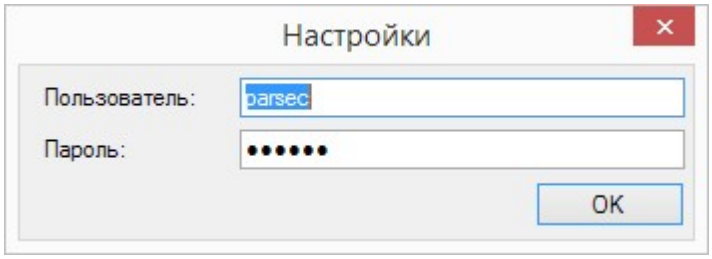
По завершении настройки нажмите на кнопку *ОК* и продолжите создание задания[322] .

8.12.2.1.6 Создание отчета "Не покидали территорию"

Отчет "Не покидали территорию" отображает список тех, кто находится на заданной территории со вчерашнего дня, и может быть создан не только в Мониторе событий, но и при помощи задания, активирующего один из двух исполняемых файлов:

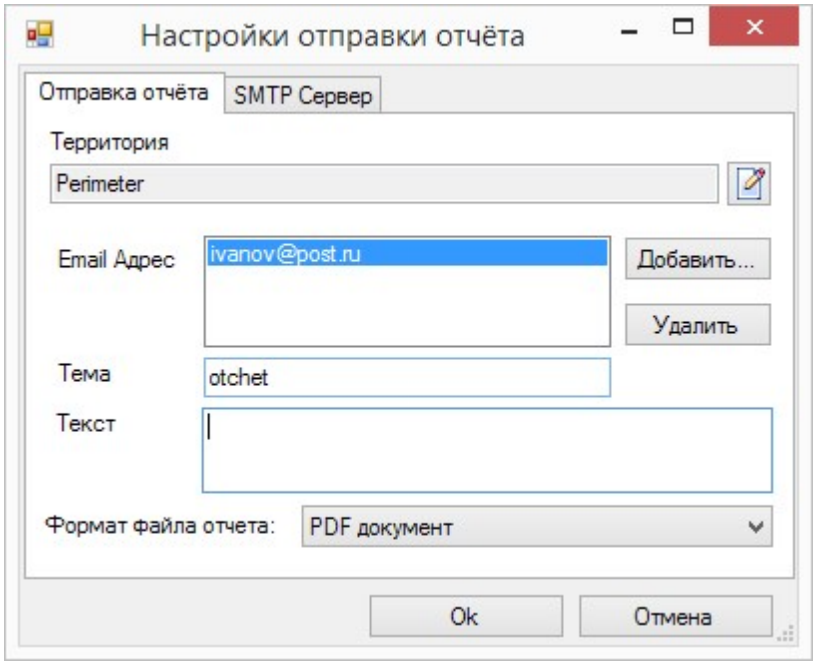
- ReportWhoIsHereToEmailTask - создает отчет и отправляет его на указанный адрес электронной почты;
- ReportWhoIsHereToFileTask - создает отчет и сохраняет его в файл.

При выборе выполнения кода[327] по созданию отчета, откроется окно аутентификации:



Введите имя и пароль пользователя, от имени которого будет запускаться задание.

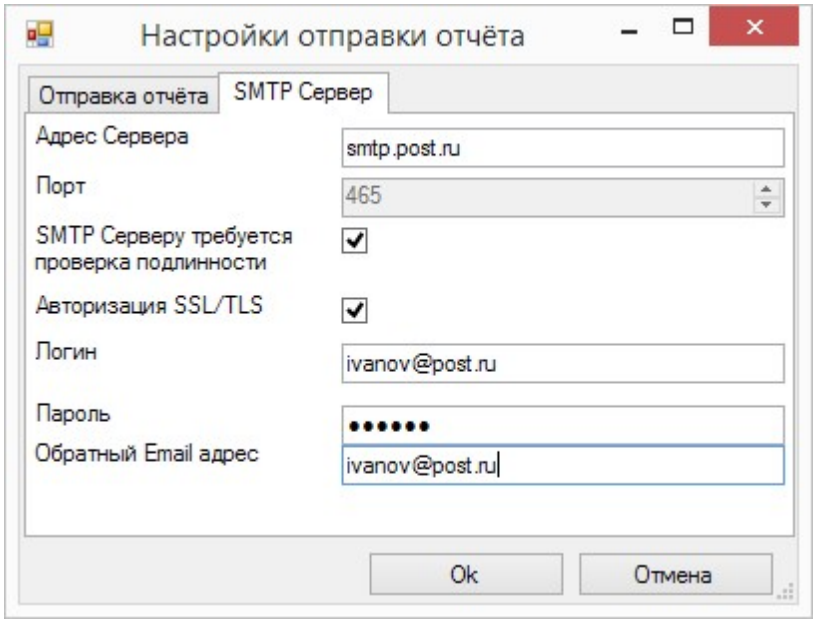
После нажатия на кнопку *ОК* появится окно настройки параметров отправки (если выбран скрипт ReportWhoIsHereToEmailTask) либо окно настройки параметров сохранения[340] (если выбран скрипт ReportWhoIsHereToFileTask):



Заполните поля:

- *Территория* - выберите территорию, которая будет проверена на наличие оставшихся с прошедшего дня субъектов доступа;
- *E-mail Адрес* - укажите адрес (несколько адресов) электронной почты, на который(-е) хотите получать отчет, нажав на кнопку *Добавить...;*
- *Тема* - введите тему, которая будет автоматически вставляться в отправляемое письмо;
- *Текст* - введите текст, который будет автоматически вставляться в отправляемое письмо;
- *Формат файла отчета* - выберите, в каком формате хотите получать отчет.

Перейдите на вкладку *SMTP Сервер*.

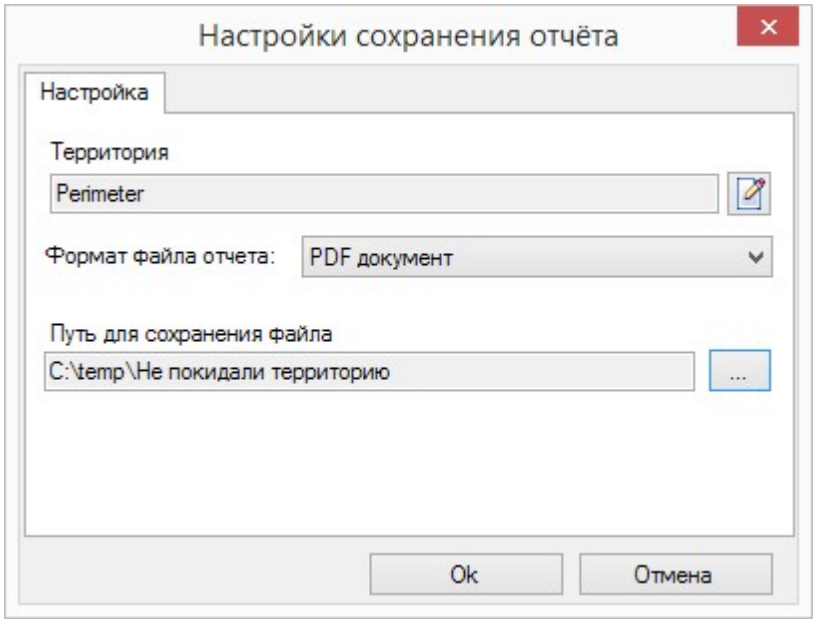


Заполните поля:

- *Адрес сервера* - введите адрес своего почтового сервера;
- *Порт* - введите номер порта для подключения к SMTP серверу;
- *SMTP серверу требуется проверка подлинности* - при установке флажка станут доступными поля:
  - *Авторизация SSL/TLS* - при установленном флажке авторизация будет производиться по клиентским TLS/SSL сертификатам. При установке флажка порт SMTP сервера выбирается автоматически, значение в поле *Порт* не учитывается;
  - *Логин* - имя пользователя для SMTP сервера;
  - *Пароль* - пароль для SMTP сервера.
- *Обратный E-mail адрес* - укажите адрес электронной почты для получения системных сообщений и т.п.

По завершении всех настроек нажмите на кнопку *ОК* и продолжите создание задания 322.

Если выбран скрипт ReportWhoIsHereToFileTask, то после аутентификации пользователя откроется окно настройки сохранения отчета:



Заполните поля:

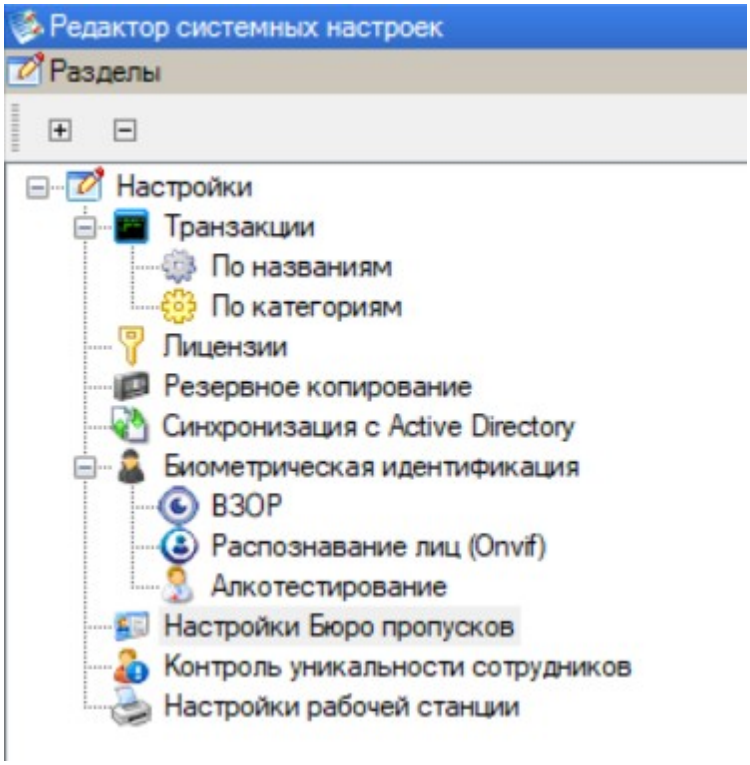
- *Территория* - выберите территорию, которая будет проверена на наличие оставшихся с прошедшего дня субъектов доступа;
- *Формат файла отчета* - выберите, в каком формате хотите получать отчет.
- *Путь для сохранения файла* - укажите директорию, в которой будет сохраняться генерируемый файл, и его имя.

Файл отчета переписывается каждый раз при сохранении в указанной директории.

По завершении настройки нажмите на кнопку *ОК* и продолжите создание задания[322] .

8.12.3 Редактор системных настроек

Редактор системных настроек позволяет выполнять различные вспомогательные операции, в том числе обслуживать ключ защиты[344] и базу данных системы. На рисунке ниже показана левая панель редактора, с помощью которой выбирается та или иная функция.



Если включен упрощенный интерфейс, то категории транзакций в редакторе не отображаются. Переход к расширенному интерфейсу осуществляется через меню "Файл - Расширенный режим".

Для лучшего понимания работы с системой следует знать, что в системе порождает то или иное событие. Все события системы, выводимые на ПК, делятся на две группы: аппаратные события и программные.

- ***Аппаратные события*** - это события генерируемые контроллером и описывающие непосредственно события, связанные с доступом через точку прохода, состоянием оборудования и самого контроллера.
- ***Программные события*** - генерируются программным обеспечением ParsecNET 3 и описывают события, связанные с подачей команд с ПК, действиями, производимыми оператором и так далее

Все события в системе разделены на категории, в соответствии с которыми они отбираются при составлении отчетов по событиям:

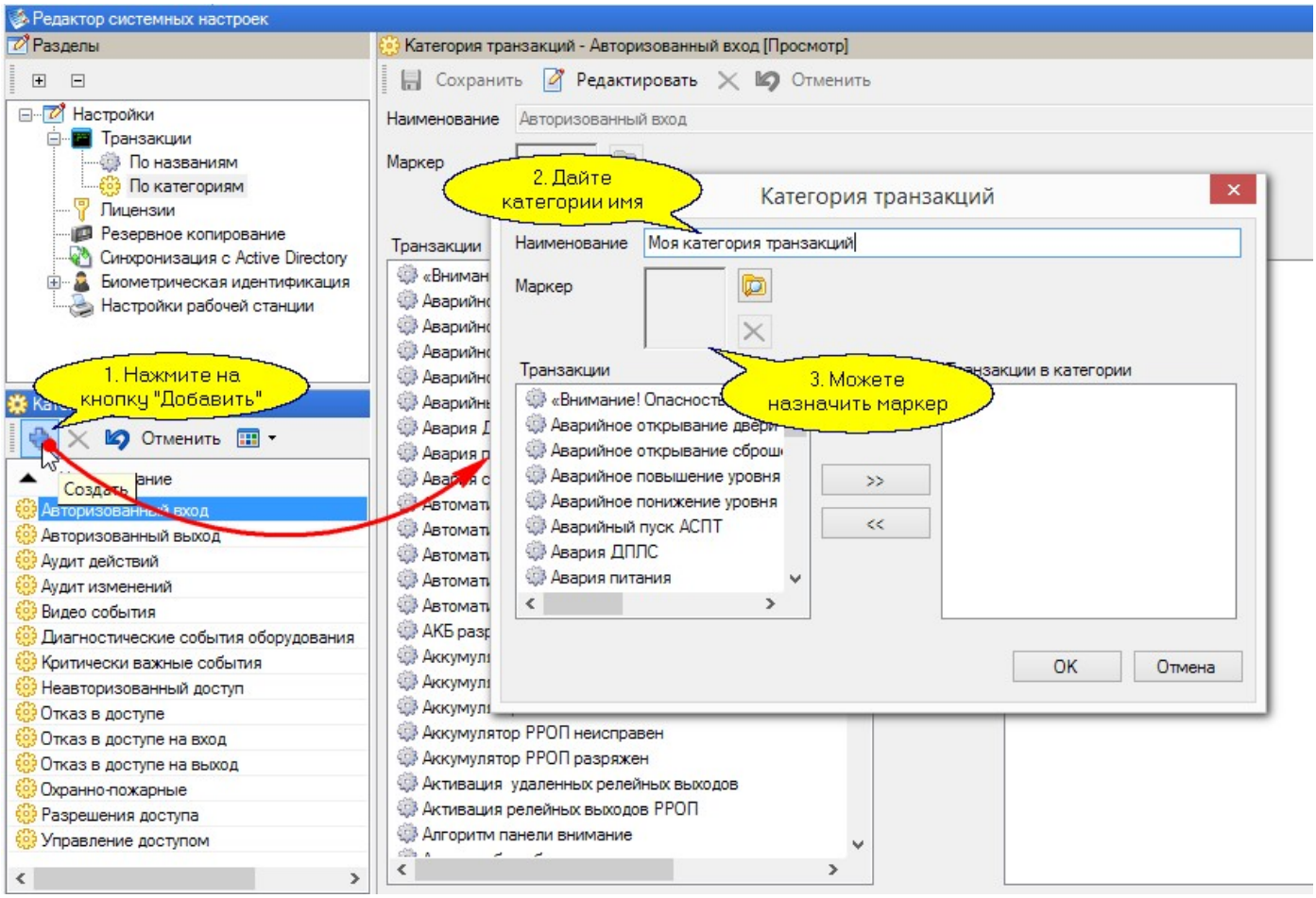
1. Авторизованный вход
2. Авторизованный выход
3. Аудит действий
4. Аудит изменений
5. Видео события
6. Диагностические события оборудования
7. Критически важные события
8. Неавторизованный доступ
9. Отказ в доступе
10. Отказ в доступе на вход
11. Отказ в доступе на выход

12. Охранно-пожарные
13. Разрешения доступа
14. Управление доступом

Редактирование категорий

Вы можете отредактировать существующие категории (перенести транзакции из одной категории в другую), а также добавить свои категории и перенести в них транзакции. Перенос транзакций в категорию и удаление из категории делается на правой панели редактора в режиме редактирования с использованием кнопок со стрелками. После переноса транзакций не забудьте сохранить результат.

Ниже на рисунке показаны действия, необходимые для добавления пользовательской категории.



Созданные пользователем категории можно редактировать и удалять, если надобность в них отпала.

Удалить системные категории невозможно.

См. также:

Лицензии и ключ защиты[344]

Резервное копирование[346]

Синхронизация с Active Directory[348]

Биометрическая идентификация[350]

Контроль уникальности сотрудников[355]

Настройки рабочей станции[359]

8.12.3.1 Лицензии и ключ защиты

Система лицензирования

Программное обеспечение ParsecNET 3 имеет две основные конфигурации:

- ***Standard***. Возможны практически все конфигурации, установка всех дополнительных модулей, выбор по количеству точек прохода и рабочих станций. Возможна установка связанного сервера (назначение мастер-сервера недоступно);
- ***Professional***. Максимальная версия с поддержкой виртуальных подсистем (множество организаций), максимальное количество точек прохода, большинство дополнительных модулей входят в поставку. Возможна установка как связанного сервера, так и назначение его мастер-сервером.

В дополнение к основному ПО, реализующему базовый набор функций, можно дополнительно покупать лицензии на следующие программные модули:

- ***PNSoft-WS*** – дополнительное рабочее место оператора (рабочая станция[34]);
- ***PNSoft-AR*** – модуль учета рабочего времени[456];
- ***PNSoft-VV*** – модуль видеоверификации[506];
- ***PNSoft-PI*** – разработка шаблонов карт-пропусков[417];
- ***PNSoft-PO*** – модуль бюро пропусков[432];
- ***PNSoft-DS*** – автоматическое распознавание документов[671]. Выбор из следующих модулей:
  - ***PNSoft-DS Cognitive*** – модуль Scanify (продажа прекращена с декабря 2019);
  - ***PNSoft-DS Regula*** – модуль Regula;
  - ***PNSoft-DS ABBYY*** – модуль ABBYY.
- ***PNSoft-VI*** – интеграция с системами видеонаблюдения[515];
- ***PNSoft-AI*** – интеграция с системами ОПС[603] (охранно-пожарной сигнализации);
- ***PNSoft-FR*** – интеграция с системами распознавания лиц[661] (СРЛ). Подключение до 100 биометрических терминалов (UniUbi, Hikvision) или серверных СРЛ (CVS, Ntechlab, VisionLabs, NeuroIO и др.);
  - ***PNSoft-FR1CH*** – подключение 1 терминала СРЛ или 1 канала серверной СРЛ.
- ***PNSoft-TA1CH*** – модуль алкотестирования[141]. Подключение 1 алкотестера;
- ***PNSoft-IC*** – интеграция с домофонными системами[684]. Одна лицензия на одну вызывную панель;
- ***Parsec.Сотрудник*** – отдельно приобретаемый модуль[380] для использования некоторых функций СКУД на мобильных устройствах. Лицензируется общее число зарегистрированных пользователей, а также число пользователей информационных сервисов.

Возможные комбинации версий программного обеспечения и дополнительных модулей показаны в таблице ниже.

Версия \ Модули		Точки прохода	WS	AR	VV	PI	PO	DS	VI	AI	FR	TA	CI
PNSoft-Standard	PNSoft-08	8	○	○	○	○	○	○	○	○	○	○	○
	PNSoft-16	16	○	○	○	○	○	○	○	○	○	○	○
	PNSoft-32	32	○	○	○	○	○	○	○	○	○	○	○
	PNSoft-MAX	Max	○	○	○	○	○	○	○	○	○	○	○
PNSoft-Pro		Max	○	✓	✓	✓	✓	○	✓	✓	○	○	○

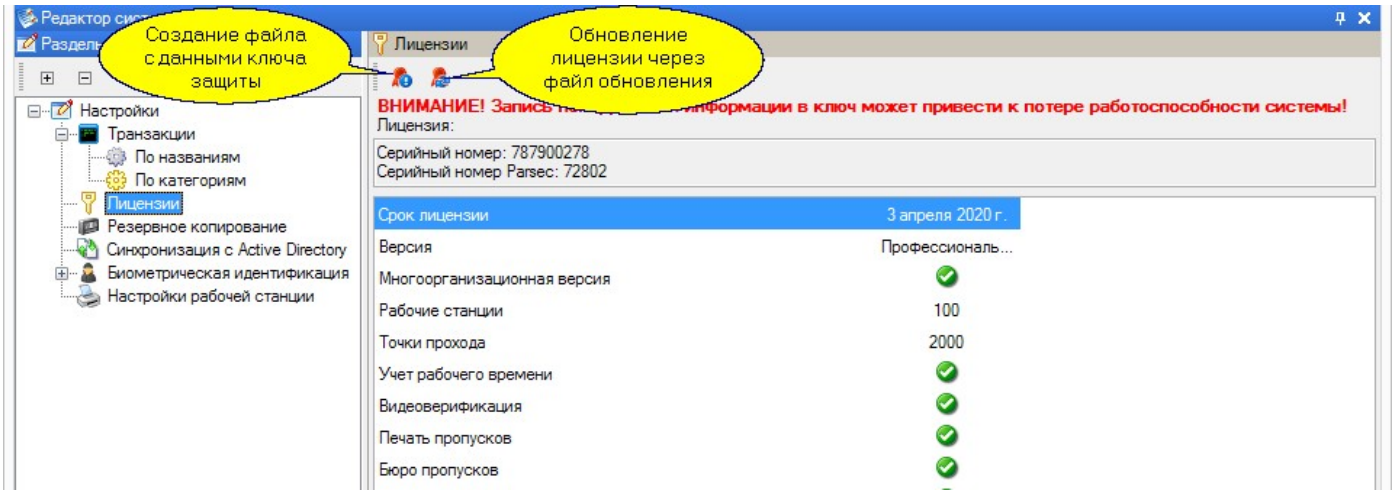
✓ *модуль входит в состав версии*

○ *модуль приобретается отдельно*

ВНИМАНИЕ! Для работы модуля распознавания документов требуется установка его собственного ключа защиты (в дополнение к ключу защиты Parsec).

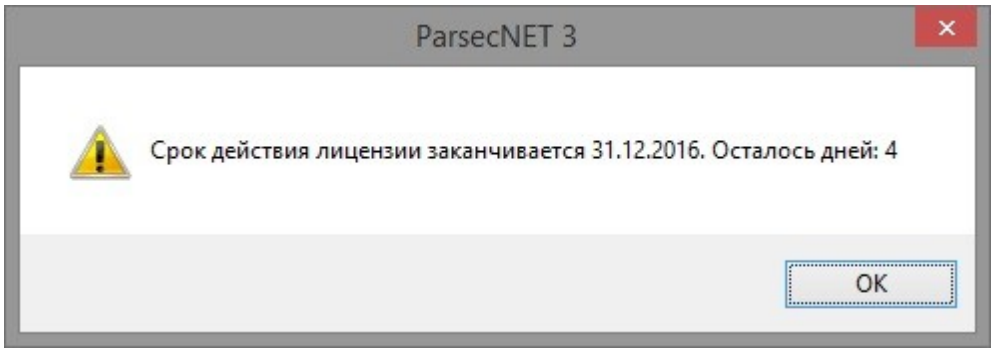
Работа с ключом защиты

Содержимое ключа защиты показывается в правой панели редактора системных настроек, если в левой панели выбрать "Лицензии". В верхней части карточки ключа защиты имеется две кнопки: с помощью левой кнопки можно создать копию данных ключа защиты в виде файла на диске (например, если вам надо отослать эту информацию вашему дилеру). При создании файла в качестве имени будет предложен серийный номер вашего ключа. Вы можете поменять или дополнить это имя по своему усмотрению.

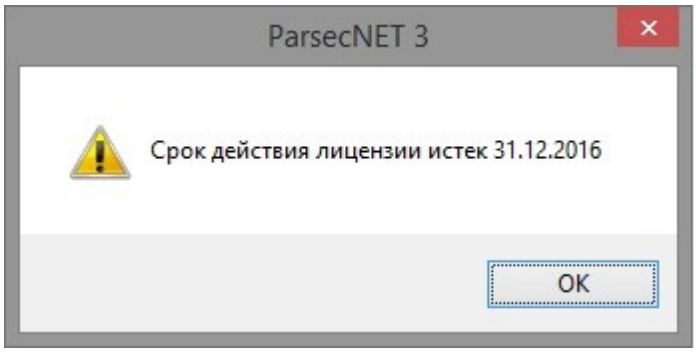


С помощью правой кнопки производится обновление вашей лицензии. Для этого необходимо получить файл с обновлением от вашего поставщика системы, поместить его в доступном месте на диске ПК, и оттуда загрузить в систему. Если данные в файле корректные, изменения вступят в силу после перезапуска программы.

За 14 дней до окончания срока действия ключа система при загрузке начнет выдавать предупреждающее собщение:



А по истечении срока действия ключа:



8.12.3.2 Резервное копирование

Резервное копирование баз данных системы является очень важным мероприятием, так как позволяет восстанавливать систему в случае отказа оборудования (например, при отказе ПК, на котором хранились данные).

Резервную копию можно сделать в любой момент вручную, но лучше делать это по расписанию, чтобы система сама об этом заботилась. Главным условием работы автоматического резервного копирования являются:

- Работа ПК, на которых работает сервер баз данных и сервер Parsec.
- Доступность директории для резервных файлов как для сервера Parsec, так и для MS SQL сервера (в соответствии с тем, под каким аккаунтом последний работает). При установке сервера Parsec папка для резервных копий создается в директории установки сервера. При установке по-умолчанию это будет директория C:\Program Files\MDO\ParsecNET 3\Backup.

Автоматическое копирование управляется сервисом, обслуживающим задания системы, то есть резервное копирование является просто специализированной задачей, выполняемой по расписанию.

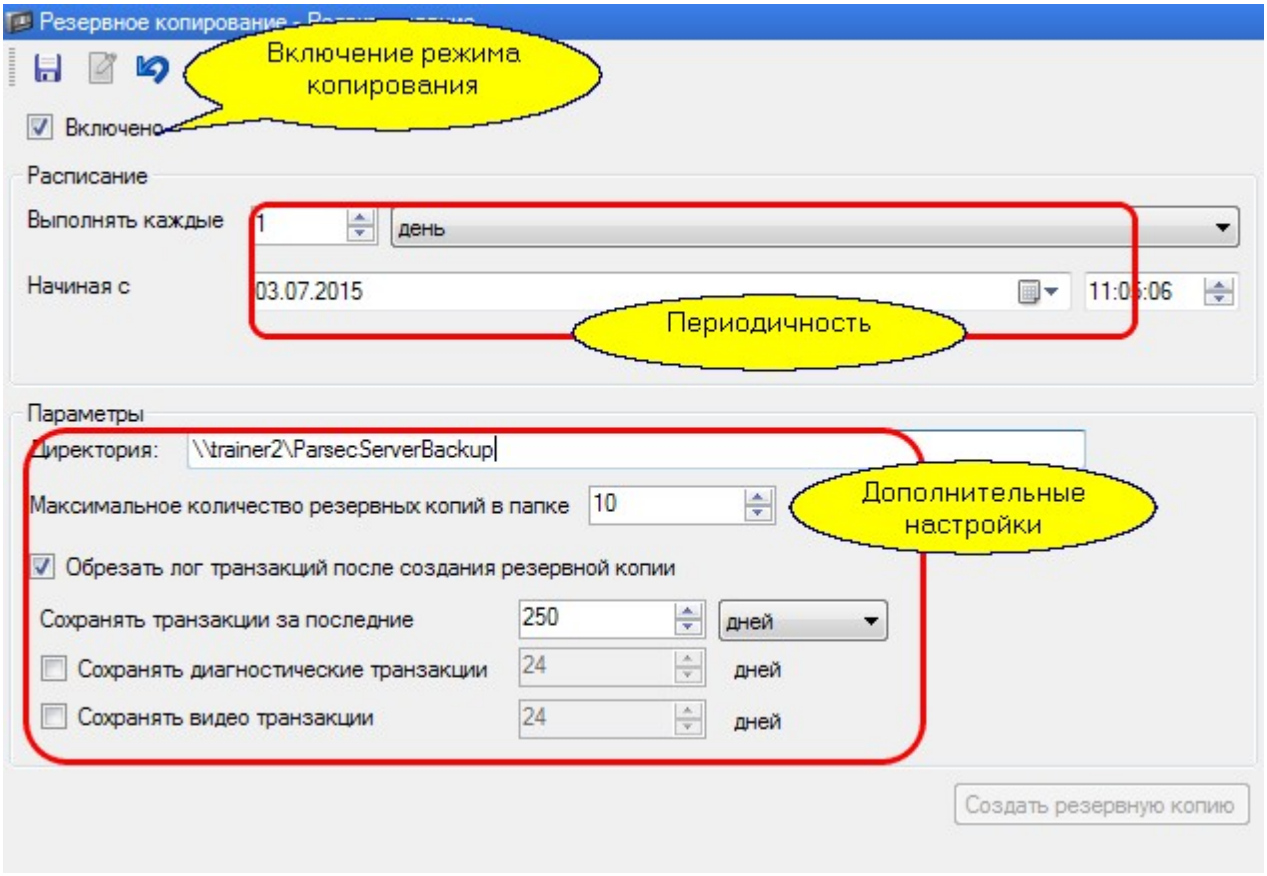


Важно! При отсутствии резервного копирования базы данных системы сбой жесткого диска или пожар приведет к неустранимой потере данных.

Запуск резервного копирования в пиковые часы работы приведет к ухудшению производительности работы системы на время, когда идет резервирование.

Настройка автоматического копирования

Для настройки резервного копирования зайдите в редактор системных настроек и выберите в левой панели раздел "Резервное копирование". В правой панели появятся параметры, которые можно настроить в соответствии со своими предпочтениями.



Перейдите в режим редактирования расписания копирования и установите параметры:

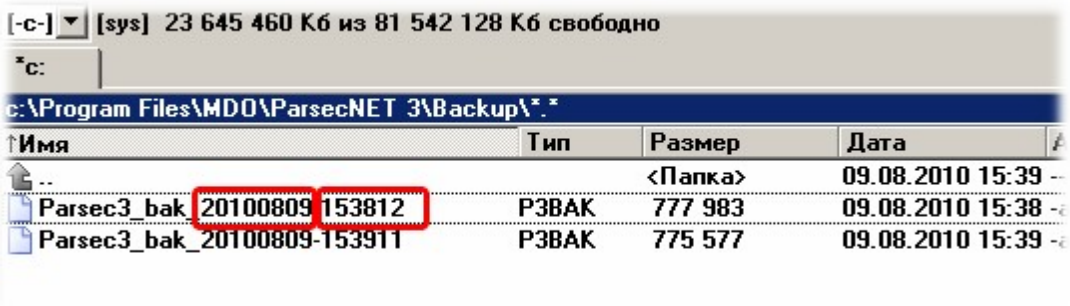
- Установите флажок *Включено*, чтобы задание по копированию выполнялось;
- Установите периодичность создания резервных копий. Рекомендуется делать копирование раз в сутки, но никак не реже одного раза в неделю;
- Время, в которое задача будет выполняться, лучше выбрать ночью, когда система находится в "холостом" (не нагруженном) режиме. Например, в час ночи;
- Если вас не устраивает директория по-умолчанию, как показано на рисунке выше, создайте и укажите системе сетевой путь к директории, куда будут складываться файлы резервных копий.

Важно! Директория для резервных копий должна быть доступна серверу системы и серверу баз данных. Работу архивирования можно проверить вручную, нажав кнопку "Создать резервную копию" и убедившись, что файл реально создан.

- Можно изменить количество файлов резервных копий, которое будет храниться. По достижении этого количества более старые файлы будут удаляться;
- Можно установить флажок *Обрезать лог транзакций после создания резервной копии*. В этом случае в основной рабочей БД системы старые транзакции, давность которых превышает заданное значение (250 дней на рисунке выше) будут удаляться. Это экономит размер дискового пространства, а также способствует более быстрому построению отчетов;
- Можно установить отдельные сроки для сохранения диагностических и видео транзакций. Для этого установите соответствующие флажки и укажите какой максимальной давности транзакции должны быть сохранены в резервной копии. Если флажки не установлены, то диагностические и видео транзакции будут сохраняться за срок, указанный в строке *Сохранять транзакции за последние...*.

После настройки всех параметров нажмите на кнопку *Сохранить*, чтобы изменения возымели силу.

Файлы резервных копий имеют следующую структуру имени: [Parsec3_bak_<дата>_<время>.P3BAK]. На рисунке ниже видно, что файл архива создан 9 августа 2010 года в 15 часов 38 минут 12 секунд.



Восстановление базы данных из резервной копии

Существует два способа восстановления данных из архивной копии:

- Запустить программу установки сервера Parsec setup.exe с командной строкой

setup.exe DB_BACKUP_FILE="C:\Program Files\MDO\ParsecNET 3\Backup\Parsec3_bak_20100317-094938.P3BAK" (то есть с именем файла архива)

- На компьютере с установленным сервером запустить setup.exe еще раз. Выбрать "Исправить". Выбрать "Из архива". Выбрать файл архива.

Все оборудование, рабочие станции и т.п., которые были подключены к серверу после создания установленной резервной копии, необходимо переустановить заново.

8.12.3.3 Синхронизация с Active Directory

Синхронизация системы ParsecNET 3 со службой Active Directory позволяет:

- автоматически блокировать доступ на территорию организации тем сотрудникам, которые блокируются в Active Directory;
- активировать\отключать запись пользователя в Active Directory по факту нахождения субъекта доступа внутри периметра (набора контроллеров). При выходе субъекта за указанный периметр запись в AD будет заблокирована, при входе запись активируется.

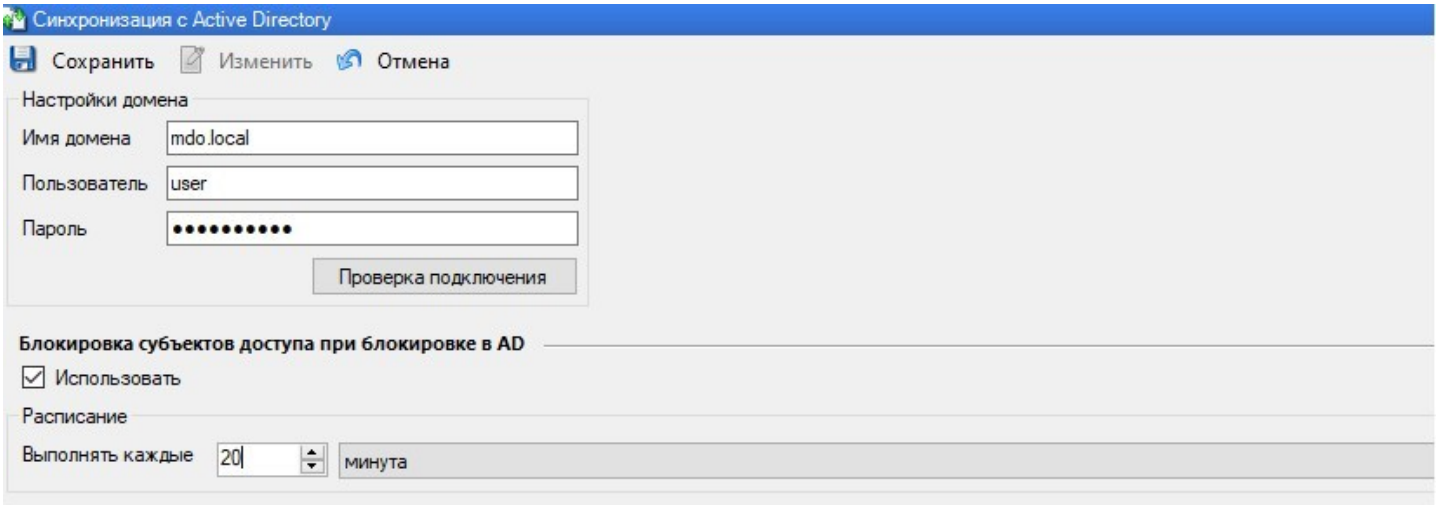
Для настройки подключения к Active Directory выполните следующие действия:

1. Перейдите в Редактор системных настроек, в раздел "Синхронизация с Active Directory";
2. Перейдите в режим редактирования;
3. Введите имя домена, а также логин и пароль для доступа к этому домену;
4. Проверьте подключение, нажав на одноименную кнопку;

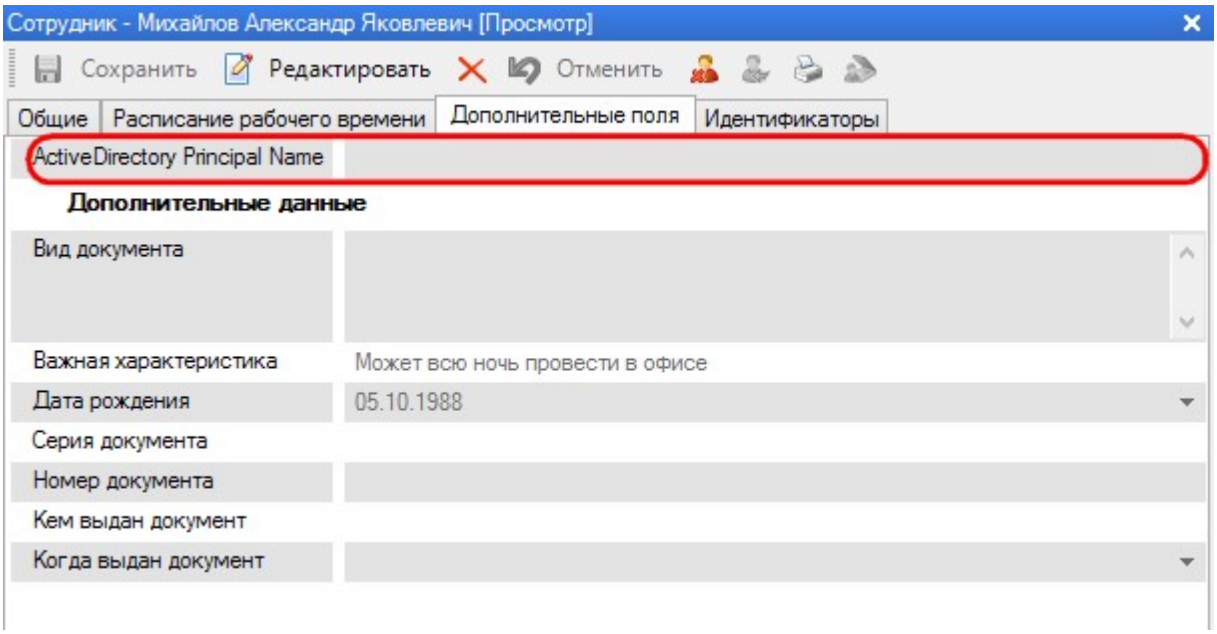
Для активации функции блокировки субъектов выполните следующие действия:

1. Настройте подключение к Active Directory (см. пункты 1-4 выше)
2. Установите флажок *Использовать* в разделе «Блокировка субъектов доступа при блокировке в AD»;

3. Установите периодичность синхронизации данных между Active Directory и системой ParsecNET 3;
4. Сохраните внесенные изменения, нажав на кнопку *Сохранить*.



После сохранения настроек в этом разделе, в карточке персонала на вкладке *Дополнительные поля* появится поле *ActiveDirectory Principal Name*:



В это поле каждому сотруднику необходимо ввести Principal Name из Active Directory, имеющее вид <user_login>@<domain_name>. Например, Principal Name пользователя со скриншотов выше будет a_mikhailov@mdo.local.

После выполнения этих шагов система ParsecNET 3 будет с указанной периодичностью проверять, есть ли у сотрудников с заданными Principal Name право на доступ к домену. Если учётная запись пользователя заблокирована, то таким сотрудникам будет запрещен доступ через все точки прохода.

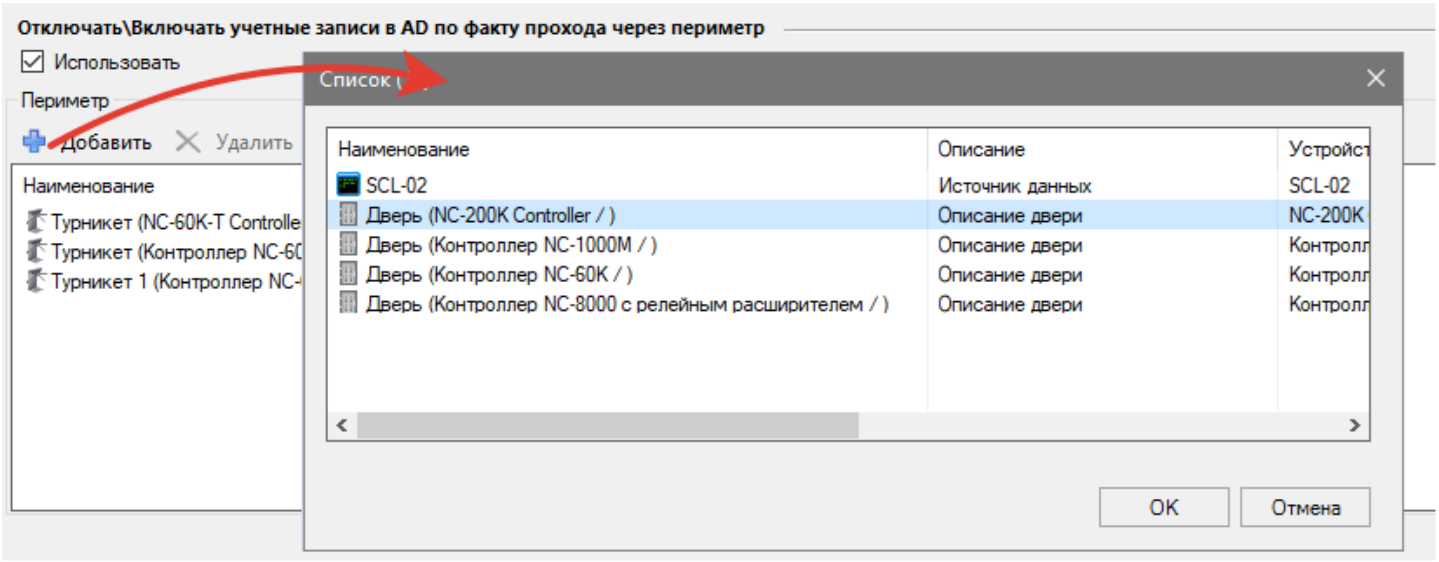
К блокируемым сотрудникам применяются действия аналогичные операции "Запретить доступ[281]". Статус персоны при этом меняется на "Заблокирован" (изменяется значок), а для всех идентификаторов персоны проставляются флажки "Вход запрещен" и "Выход запрещен", что приводит к удалению этих идентификаторов из баз данных контроллеров СКУД.

При разблокировке учётной записи в Active Directory автоматической разблокировки персоны в ParsecNET не происходит.

Для разблокировки персоны воспользуйтесь действием "Разрешить доступ[281] ", доступным из контекстного меню в Редакторе персонала.

Для активации функции контроля записей в AD по нахождению в периметре выполните следующие действия:

1. Настройте подключение к Active Directory (см. инструкцию выше);
2. Установите флажок *Использовать* в разделе «Отключать\Включать учетные записи в AD по факту прохода через периметр»;
3. Нажмите кнопку Добавить и выберите контроллеры, которые входят в необходимый периметр;
4. Сохраните внесенные изменения, нажав на кнопку *Сохранить*.



После этого при проходе субъектов с заполненным полем ActiveDirectory Principal Name через указанные контролеры будет произведен поиск учетной записи в AD и действие с ней в соответствии с направлением прохода: Отключение при выходе и Активация при входе.

8.12.3.4 Биометрическая идентификация

В ПО ParsecNET 3 интегрированы следующие системы биометрической идентификации:

- идентификация по отпечаткам пальцев[654] ZKTeco и ЛКД;
- идентификация по радужной оболочке глаз[350] "Взор";
- устройства идентификации по карте и/или лицу UniUbi[666] ;
- распознавание лиц на основании стандартов ONVIF[353] "Profile A" и "Profile C";
- алкотестирование[141] .

В текущей версии Системы включить можно только какой-то один из этих модулей интеграции. Однако, независимо от выбранной системы, пользователь также может организовать СКУД с использованием биометрической системы распознавания лиц[353] на основе технологий Onvif.

8.12.3.4.1 Система биометрической идентификации Взор

Интеграция ПО ParsecNET с системой биометрической идентификации Взор позволяет повысить безопасность доступа через точки прохода, организовав проход по радужной оболочке глаз (РОГ).

Сканеры для записи биометрических шаблонов передают их в систему ParsecNET через шину MQTT.

Биометрические сканеры для идентификации подключаются к контроллерам Parsec по стандарту Wiegand при помощи интерфейса сопряжения NI-TW.

Для включения модуля Взор произведите следующие действия:

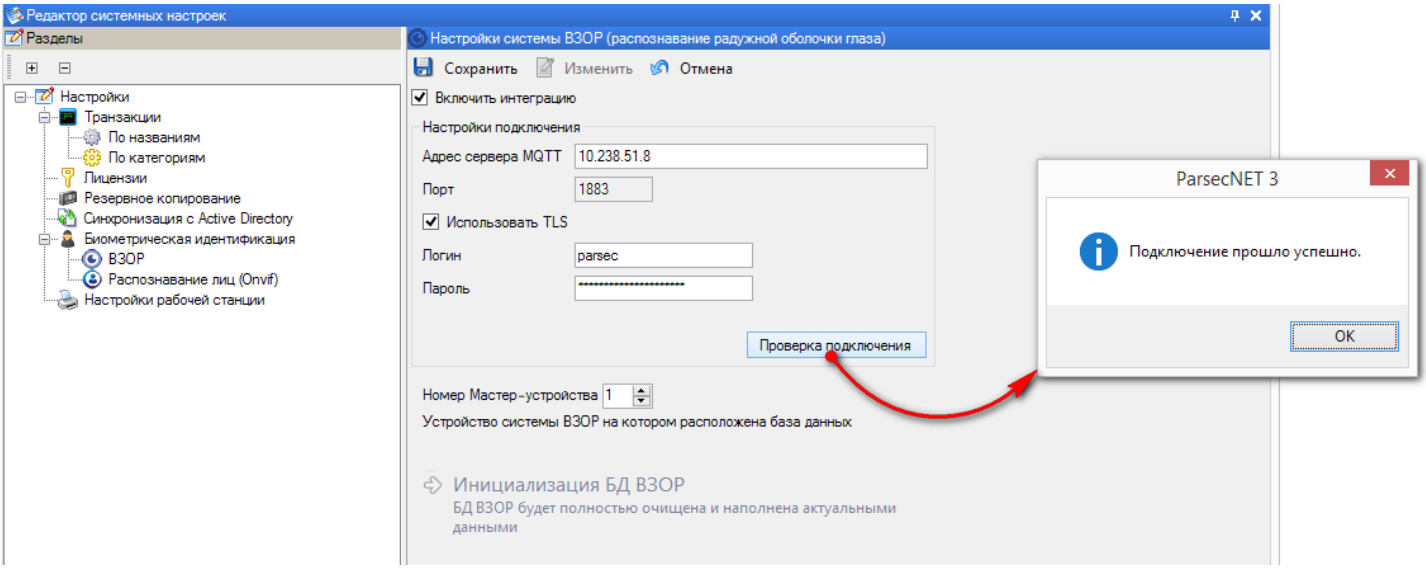
1. Установите и настройте оборудование компании VZOR SYSTEMS в соответствии с руководствами по эксплуатации. Запомните, а лучше запишите ID установленных устройств для дальнейшей настройки модуля интеграции;

2. Перейдите в раздел ВЗОР редактора системных настроек;

3. Перейдите в режим редактирования и установите флажок *Включить интеграцию*;

4. Укажите адрес сервера MQTT, порт, а также (если используется протокол аутентификации TLS) флажок *Использовать TLS* и введите логин и пароль;

5. Нажмите на кнопку *Проверка подключения*. Система выдаст сообщение об ошибке или успешном подключении:



Если появилось сообщение об ошибке, устраните ошибку и повторите проверку.

Если проверка прошла успешно, то кнопка *Биометрические данные...* в карточке субъекта доступа[262] будет активировать сканер РОГ.

6. В поле *Номер Мастер-устройства* укажите ID того устройства, на котором находится база данных;

7. Сохраните внесенные изменения, нажав на кнопку *Сохранить*;

8. Если есть сомнения в том, что БД подключенных(-ого) устройств(-а) пуста, нажмите на кнопку *Инициализация БД ВЗОР*.
В дальнейшем, эту кнопку необходимо нажимать, если Мастер-устройство заменяется. При нажатии на эту кнопку данные из БД ParsecNET 3 записываются в БД Мастер устройства ВЗОР. Базы данных всех биометрических считывателей ВЗОР синхронизируются между собой автоматически.

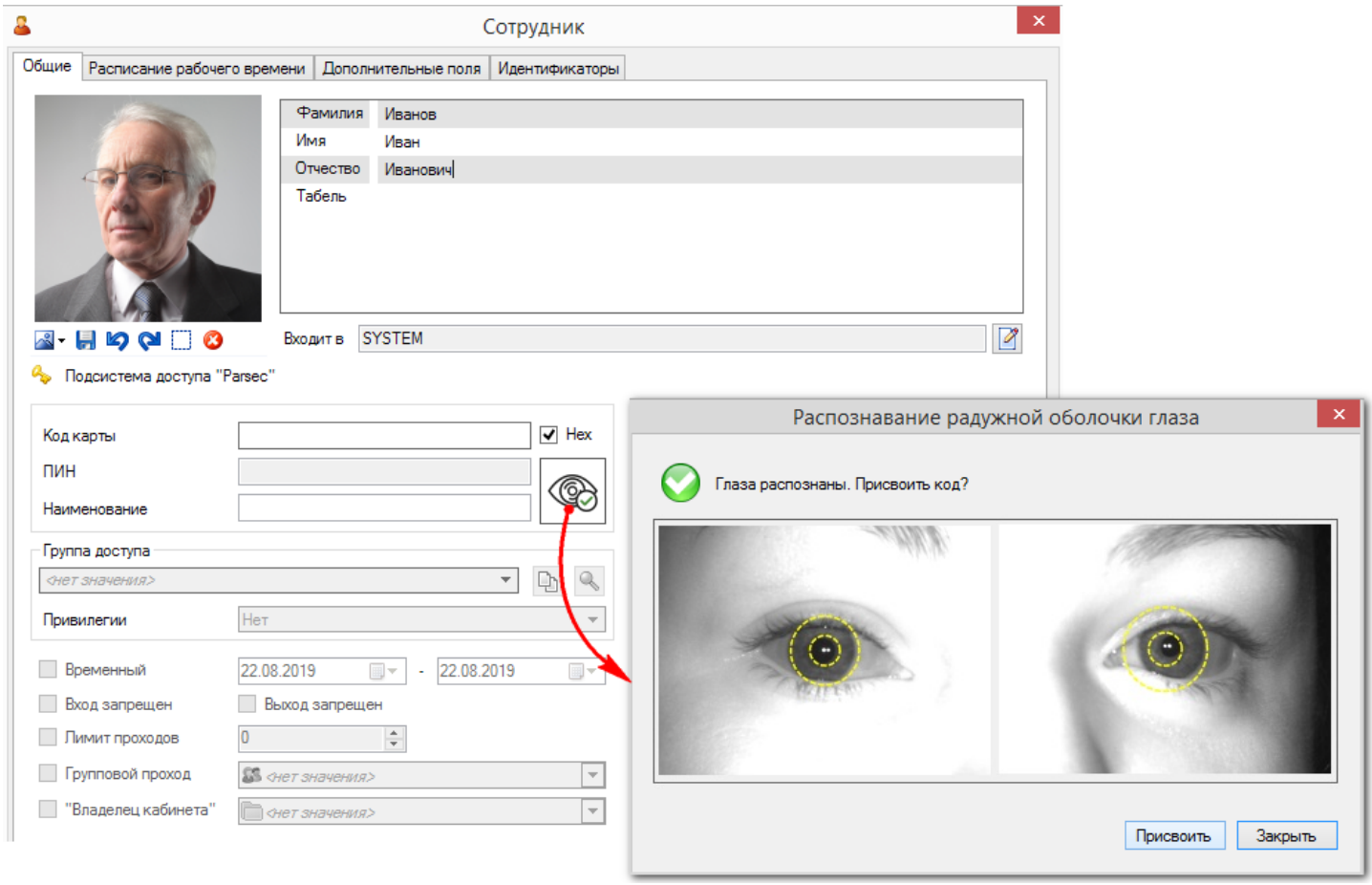
9. В ПО ParsecNET 3 на ПК, к которому подключен биометрический сканер Взор, использующийся для записи РОГ в БД, необходимо указать его номер. Для этого перейдите в раздел *Настройка рабочей станции*[359] и в поле *Номер подключенного устройства* задайте корректный номер (устройство должно быть подключено именно к данному локальному ПК).

Теперь модуль интеграции готов к работе.

При добавлении нового субъекта доступа в Редакторе персонала к его идентификатору можно добавить биометрические данные - математическую модель изображения его РОГ. Уже существующим в системе пользователям также можно добавить такие биометрические данные.

В обоих случаях выполните следующие действия:

1. Поместите карту доступа пользователя на настольный считыватель. Если проход будет осуществляться только по радужной оболочке, то можно обойтись без карты, в качестве идентификатора пользователю будет присвоен сгенерированный код;
2. Расположите субъект доступа на расстоянии около 40 см от сканера таким образом, чтобы отражении глаз на панели сканера были наложены на мигающие светодиоды индикации;
3. Нажмите на кнопку *Биометрические данные...* Появится окно распознавания радужной оболочки глаз (пустое), а цвет индикаторной панели сканера изменится с красного на белый;
4. Пусть субъект доступа медленно приближает лицо к сканеру, не изменяя наклона головы и не отклоняясь в стороны, при этом по белой индикаторной панели слева направо будет двигаться зеленая полоска. Приближаться необходимо до тех пор, пока зеленая полоска не достигнет правого края индикаторной панели. По завершении сканирования система обработает данные и в окне появятся изображения глаз;
5. Нажмите на кнопку *Присвоить*. При неудаче, повторите сканирование. Текущему идентификатору будет присвоен биометрический шаблон, который можно использовать для доступа по радужной оболочке глаз;



Для проведения успешного сеанса записи РОГ необходимо выполнить следующие рекомендации:

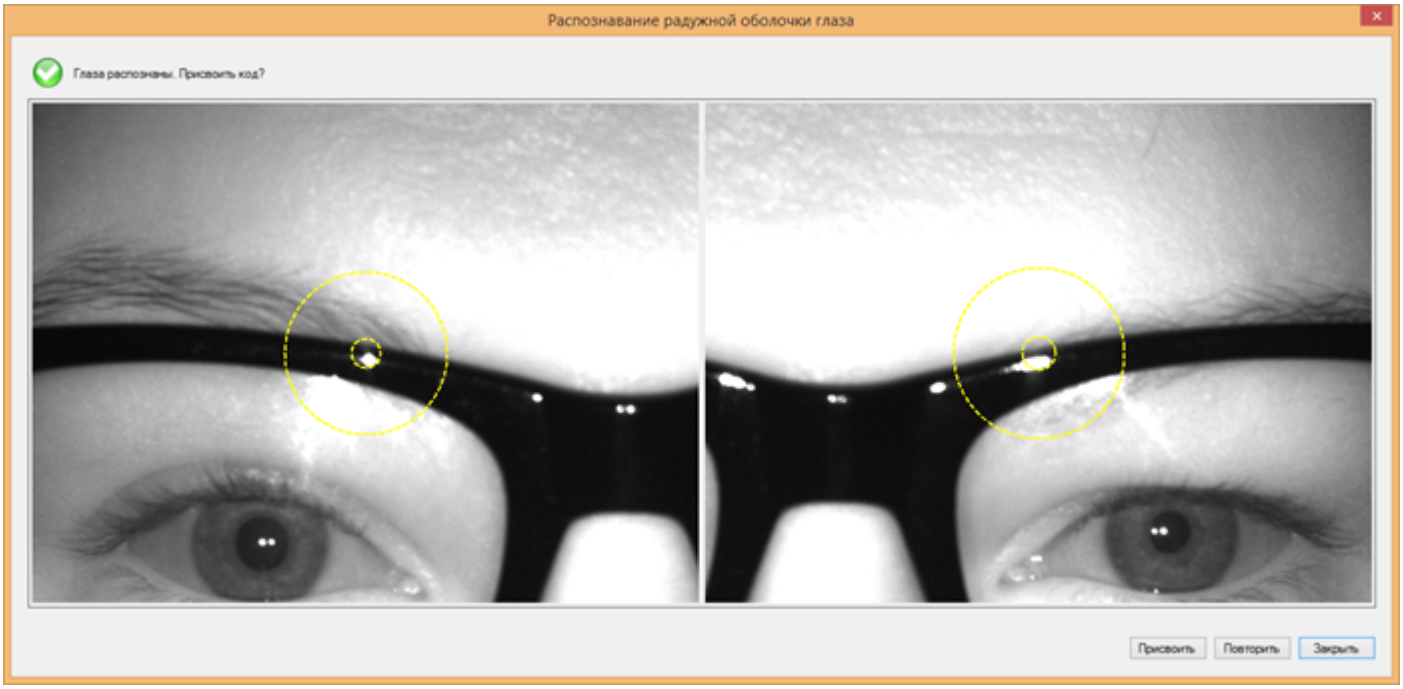
- Перед началом записи необходимо снять очки, солнцезащитные очки, контактные линзы (жесткие, с рисунком и применяемые для коррекции астигматизма);
- Пользователь должен стоять или сидеть, прямо обратившись лицом к лицевой панели сканера на расстоянии около 40 см, его глаза должны быть широко открыты и

располагаться на одном уровне со сканером таким образом, чтобы видеть отражение своих глаз на лицевой панели сканера;

- Приближаться к сканеру следует медленно и плавно, не смещаясь по вертикали и горизонтали;
- В случае, если пользователь сильно сместился в сторону, АРМ выдаст в строке состояния сообщение: «Смещение персоны от центра устройства слишком велико».

Чтобы создать новый снимок РОГ пользователю АРМ необходимо нажать кнопку «Присвоить».

Обратите внимание, при сканировании радужная оболочка и зрачок должны попадать в границы, очерченные пунктирными кругами. В противном случае, проход будет невозможен:



6. Далее завершите создание карточки пользователя системы как указано в разделе[258].

8.12.3.4.2 Распознавание лиц (Onvif)

Лицензируется как PNSoft-FR[344]

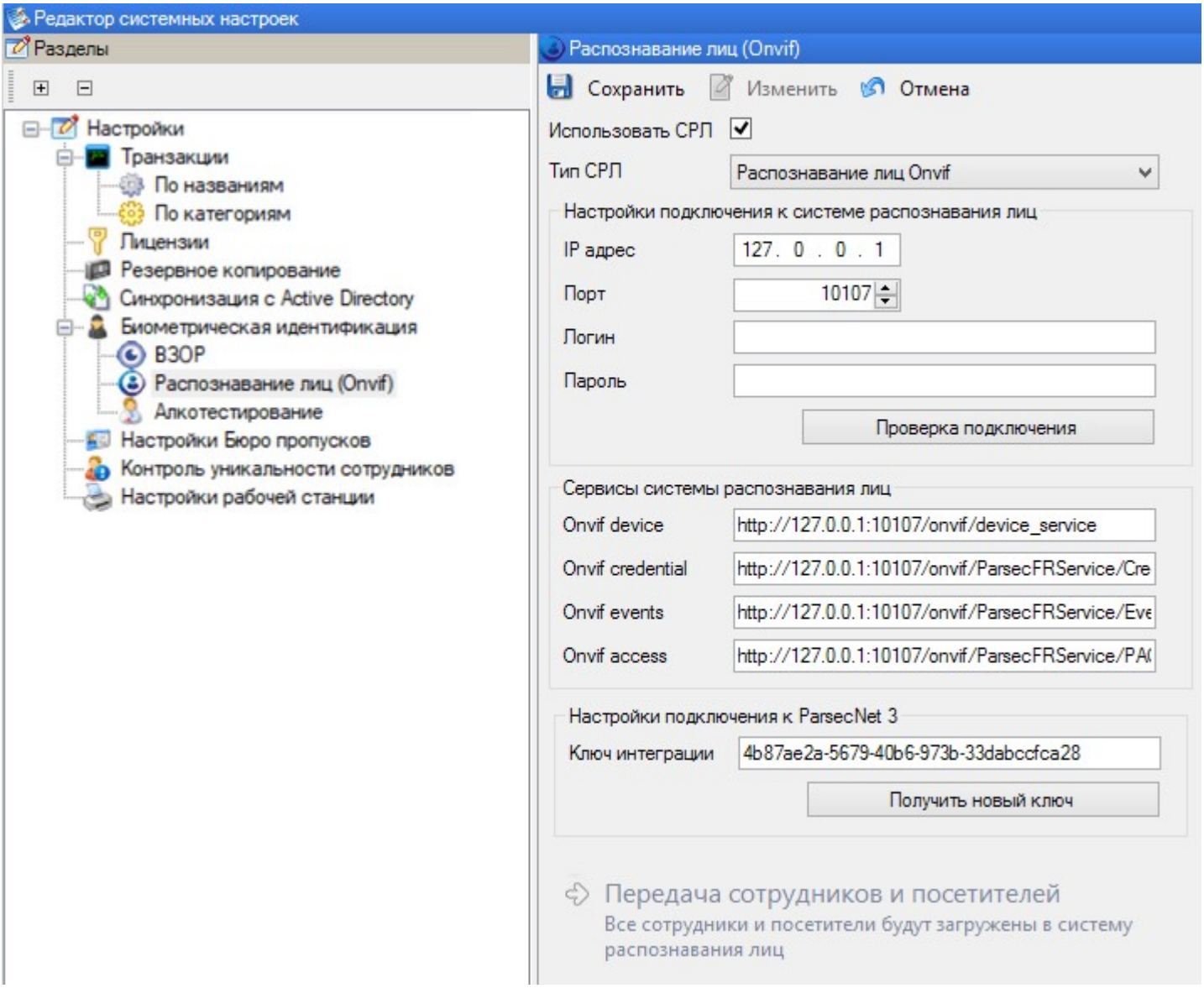
Интеграционный модуль распознавания лиц СКУД ParsecNET 3 позволяет сторонним разработчикам и интеграторам решать задачи по идентификации и контролю доступа на основании стандартов ONVIF "Profile A" и "Profile C". На этой основе реализованы, в частности, следующие отдельные модули:

- модуль распознавания лиц ISS (FaceX)[572].

Подробное описание механизмов интеграции содержится в документе "Описание API для интеграций с системами распознавания лиц".

Чтобы настроить ПО ParsecNET для взаимодействия с системой распознавания лиц (СРЛ) на основе технологий Onvif, выполните следующие шаги:

1. Перейдите в раздел *Распознавание лиц (Onvif)* Редактора системных настроек и установите флажок *Использовать СРЛ;*
2. Из раскрывающегося списка *Тип СРЛ* выберите "Распознавание лиц Onvif":



3. В блоке *Настройки подключения к системе распознавания лиц* укажите параметры для доступа к Onvif-серверу СРЛ;
4. Проверьте подключение к Onvif-серверу, нажав на кнопку *Проверка подключения*;
5. В случае успешного соединения с Onvif-сервером в полях блока *Сервисы системы распознавания лиц* появятся URL сервисов СРЛ.
   Если URL сервисов не появились или появились не все, обратитесь к поставщику СРЛ за уточнением и добавьте их вручную. Если сервис "Onvif access" поставщиком СРЛ не предусмотрен, то оставьте поле пустым;
6. После нажатия на кнопку *Получить новый ключ* СКУД ParsecNET сгенерирует цифро-буквенный код (ключ интеграции). Этот ключ используется в качестве пароля для оператора, от имени которого СРЛ будет подключаться к ПО ParsecNET;
7. Сохраните внесенные изменения, нажав на кнопку *Сохранить*;

После сохранения настроек станет активной кнопка *Передача сотрудников и посетителей*, при нажатии на которую сведения о субъектах доступа будут переданы из БД ParsecNET в БД СРЛ. Впоследствии все изменения в записях и вновь добавленные сотрудники будут передаваться в БД СРЛ автоматически.

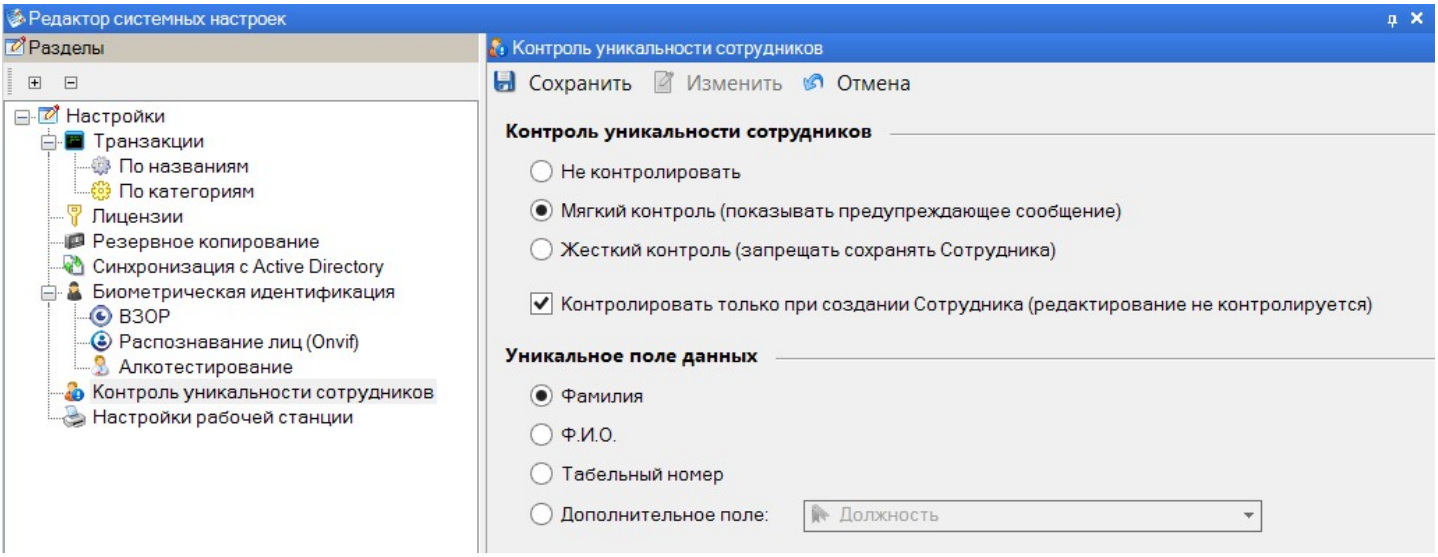
Теперь следует добавить в Систему и настроить контроллеры распознавания лиц[108].

8.12.3.4.3 Алкотестирование, системные настройки

Полное описание настроек алкотестирования, в том числе и системной их части, находится в разделе Алкотестирование[141].

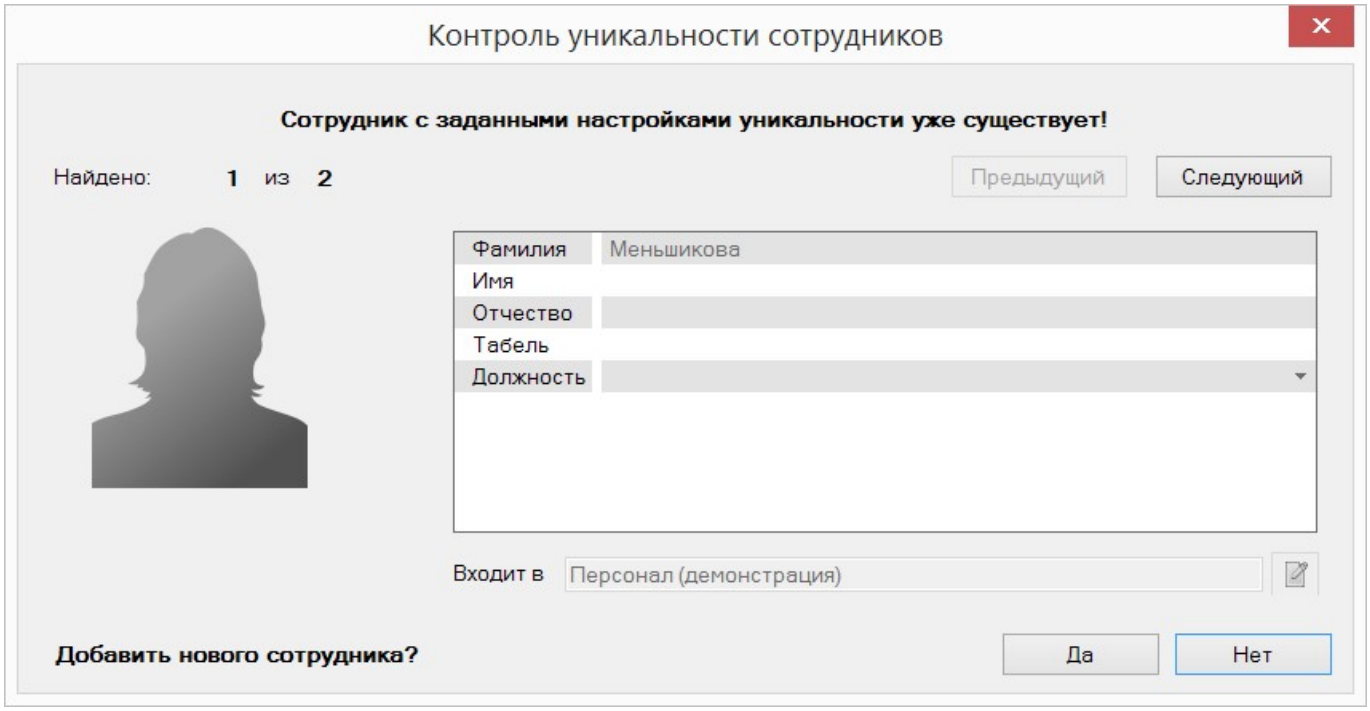
8.12.3.5 Контроль уникальности сотрудников

Функция контроля уникальности сотрудника позволяет исключить создание в Системе дублирующих записей субъектов доступа типа "сотрудник". Кроме того, контроль уникальности также производится при редактировании карточек сотрудников.

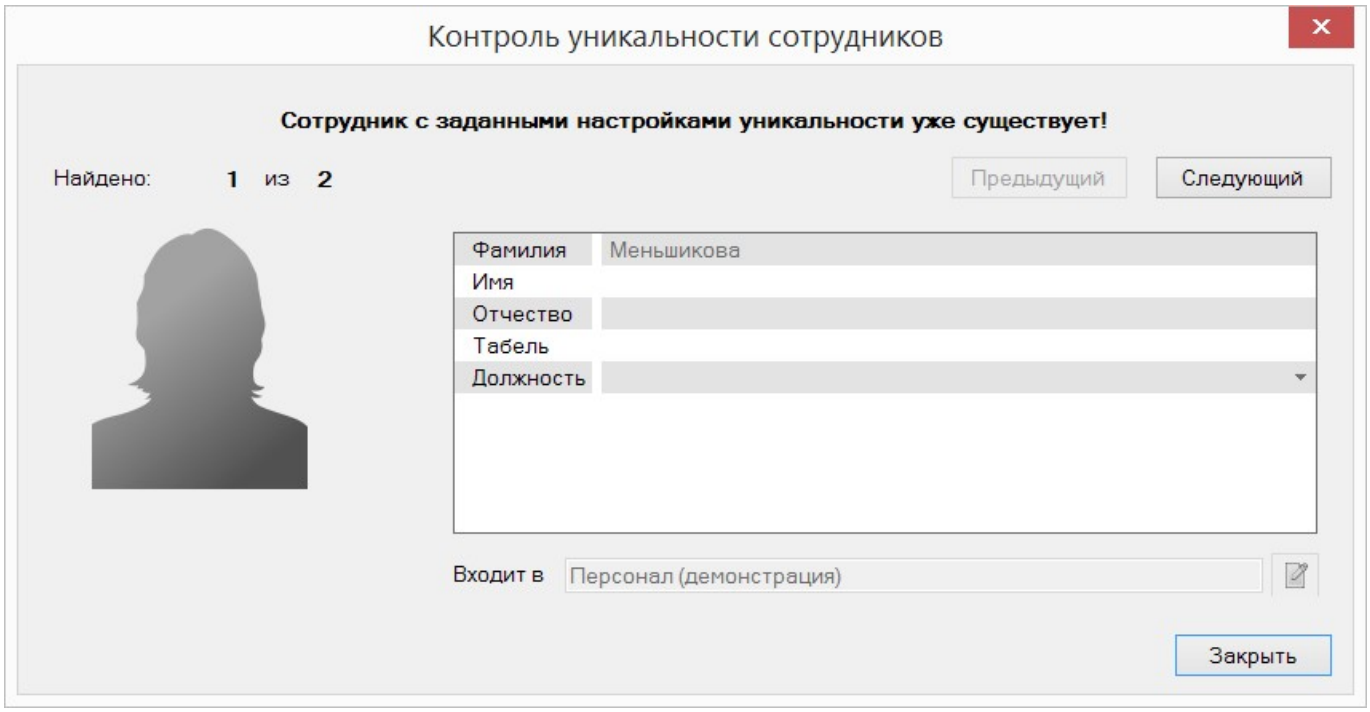


Параметры настройки контроля уникальности:

- *Не контролировать* - проверка на дублирование добавляемых сотрудников не производится;
- *Мягкий контроль* - при добавлении в Систему уже существующего в ней сотрудника появляется окно с предупреждающим сообщением:



  Нажатием на кнопки *Предыдущий* и *Следующий* можно просмотреть все уже существующие карточки сотрудников, не отвечающие критерию уникальности по заданному параметру. Оператор может проигнорировать предупреждение и добавить запись, нажав на кнопку *Да*;
- *Жесткий контроль* - при добавлении в Систему уже существующего в ней сотрудника процедура блокируется. Появляется окно с сообщением:



Оператор может только закрыть это окно. Добавление записи невозможно.

Проверка уникальности проводится по следующим полям карточки субъекта доступа:

- *Фамилия* - на уникальность проверяется только фамилия субъекта доступа;
- *Ф.И.О.* - добавляемая запись проверяется на совпадение по всем полям карточки сотрудника: *Фамилия*, *Имя* и *Отчество*;
- *Табельный номер* - на уникальность проверяется только табельный номер;
- *Дополнительное поле* - контроль уникальности производится по значению выбранного из раскрывающегося списка значения дополнительного поля[264].

8.12.3.6 Настройки Бюро пропусков

Начиная с версии 3.12.1117 появилась возможность выдавать посетителям идентификаторы типа "QR-код Parsec".

Чтобы начать использование QR-кодов в Бюро пропусков, необходимо задать настройки:

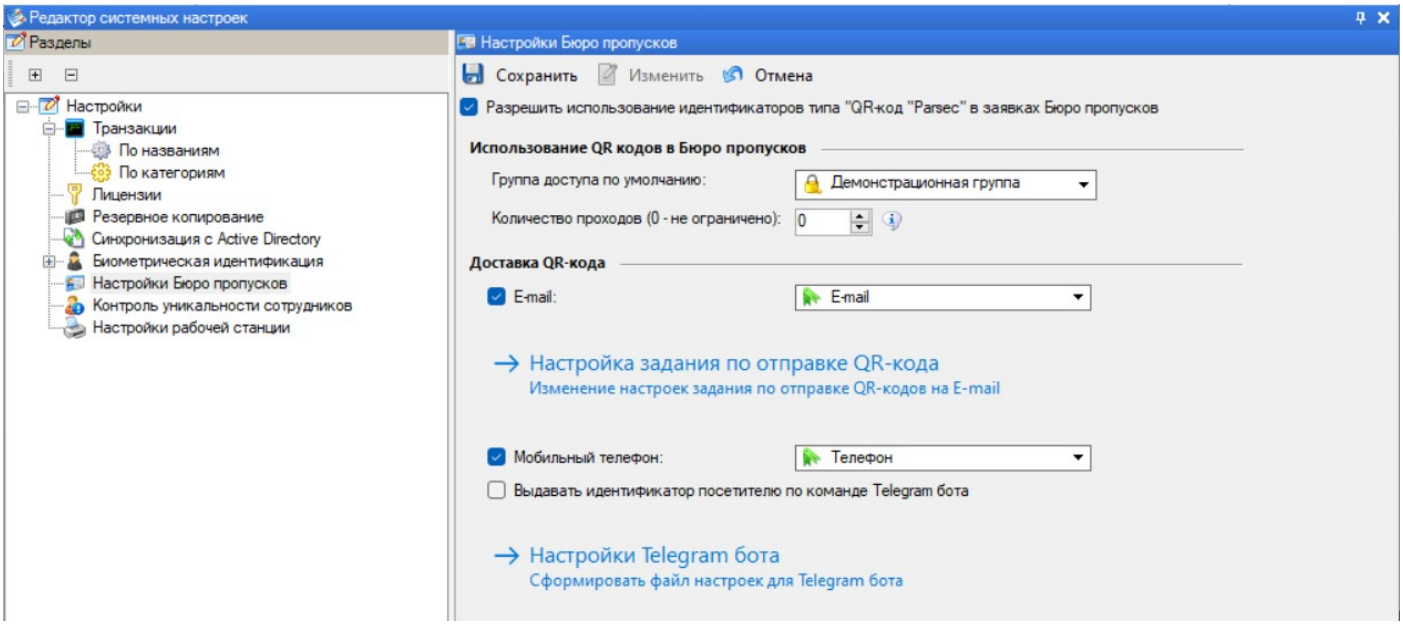
1. Откройте Редактор системных настроек и выберите раздел *Настройки Бюро пропусков*;
2. Установите флажок *Разрешить использование идентификаторов типа "QR-код "Parsec" в заявках Бюро пропусков*;
3. Выберите группу доступа, которая будет назначаться посетителям при выдаче идентификатора. Индивидуально для каждого посетителя можно изменить группу при создании заявки;
4. При необходимости укажите количество проходов, которые могут сделать посетители по своим QR-кодам. Это работает только для контроллеров, поддерживающих функцию "Использовать индивидуальные счетчики проходов";
5. Если QR-код не планируется выдавать в распечатанном виде, выберите способ его доставки посетителю: на E-mail или в систему мгновенного обмена сообщениями Telegram на мобильное устройство. Для этого в Модуле Бюро пропусков предварительно должны быть созданы дополнительные поля для указания адреса электронной почты и номера мобильного устройства посетителя.
   Для доставки кода на E-mail используется задание[454], которое создается автоматически, а настраивается в окне, открывающемся по нажатию кнопки *Настройка задания по отправке QR-кода*. Подробности в разделе Отправка QR-кода Parsec посетителям[454].
   Флажок *Мобильный телефон* активирует функцию отправки сгенерированного QR-кода в систему мгновенного обмена сообщениями Telegram на номер, указанный в дополнительном

поле карточки посетителя.

Флажок *Выдавать идентификатор посетителю по команде Telegram бота.* Если флажок не установлен, то при отправке любого сообщения в чат Telegram-боту[393] посетитель получит в ответ QR-код Parsec только в том случае, если он уже назначен ему в СКУД Parsec. Если флажок установлен, то посетителям, чьи заявки находятся в статусе "Согласована" (т.е. идентификатор еще не назначен), Telegram-бот самостоятельно выдает идентификатор "QR-код Parsec" в системе ParsecNET и передает его в чат.

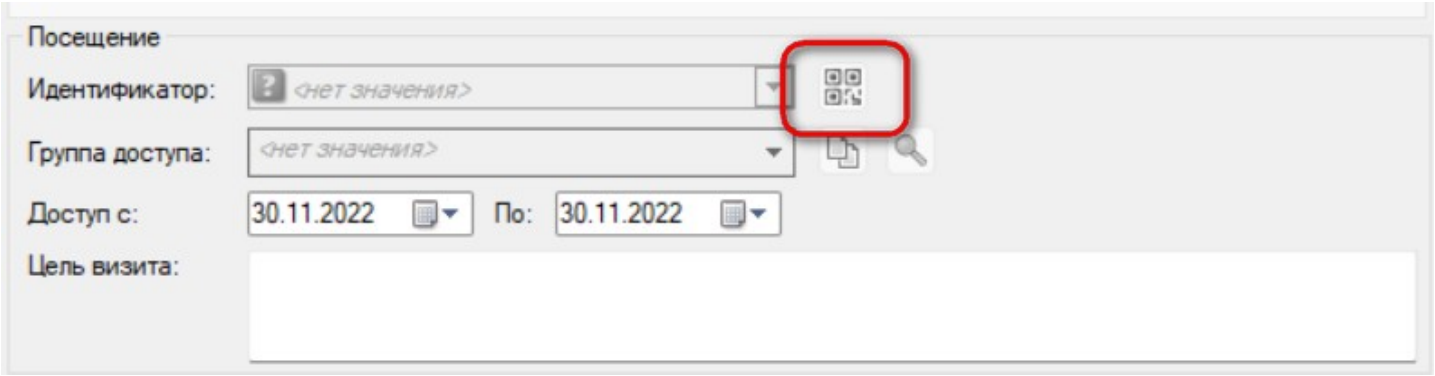
Кнопка *Настройка Telegram бота* позволяет сохранить файл с настройками *appsettings.json*, которые необходимо использовать для отправки QR-кодов на номер мобильного устройства в Telegram.

Для обеспечения корректного взаимодействия СКУД Parsec и мессенджера Telegram необходимо произвести дополнительные настройки (раздел Отправка QR-кода Parsec посетителям[454]).



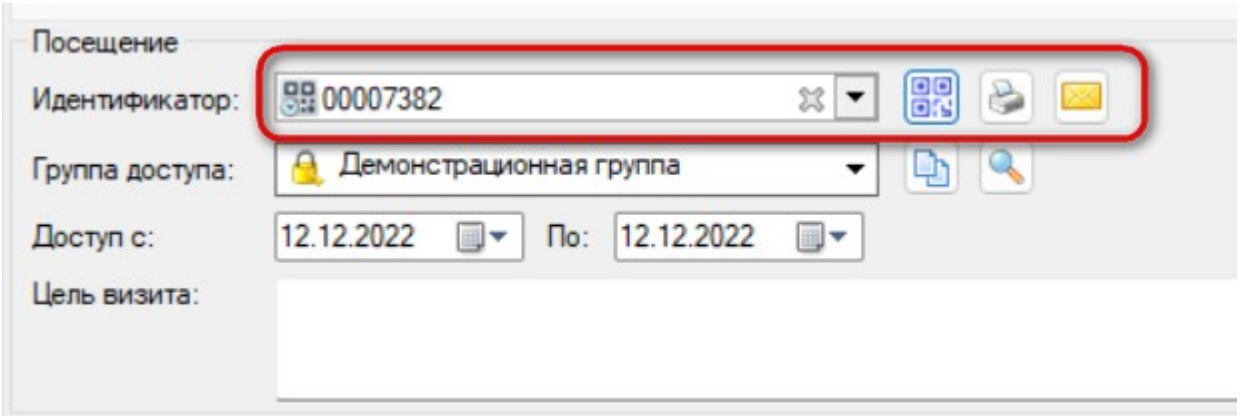
После завершения настройки появляется возможность выдавать посетителям идентификаторы типа "QR-коды Parsec". Конечно, точки доступа должны быть оборудованы считывателями QR-кодов, например, PNR-QX29.

При создании заявки справа от раскрывающегося списка *Идентификатор* теперь отображается кнопка *Выдать идентификатор типа QR код*:



Кнопка становится активной при получении заявкой статуса *Согласована*.

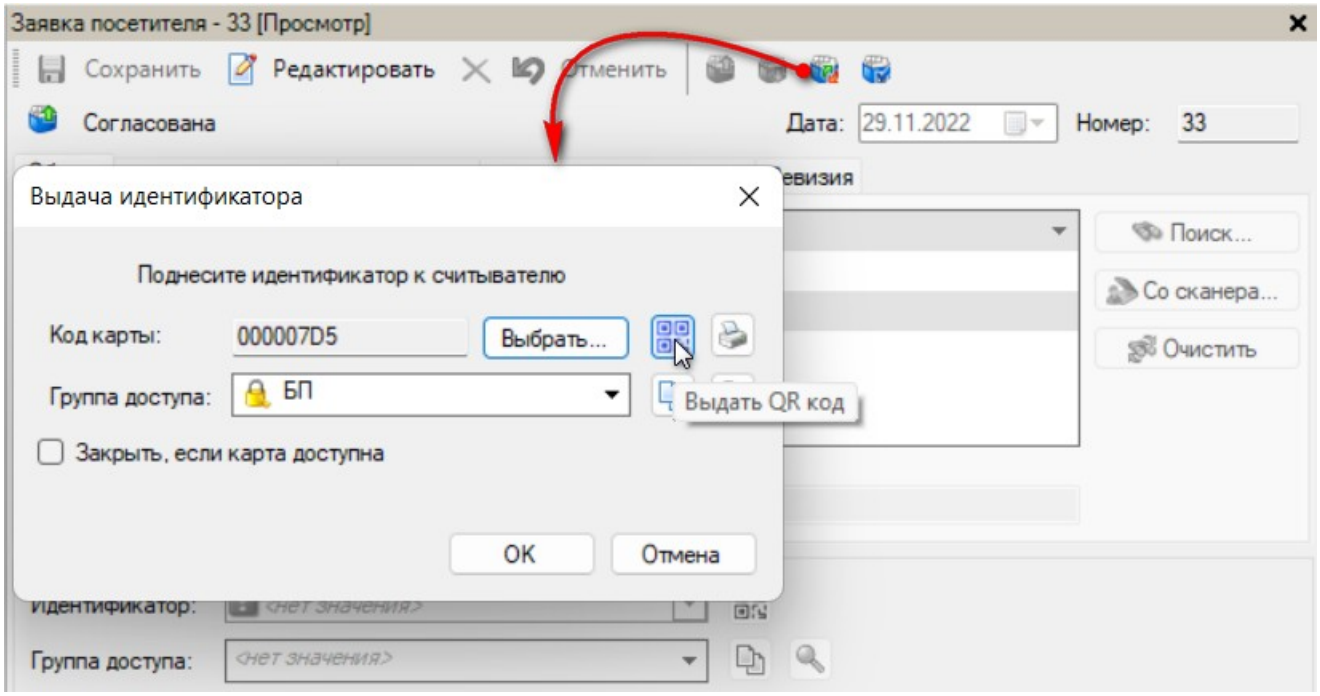
При нажатии на эту кнопку посетителю выдается идентификатор (его код генерируется рандомно и отображается в поле раскрывающегося списка) и появляется кнопка *Распечатать QR код*:



Повторное нажатие на кнопку *Выдать идентификатор типа QR код* открывает окно просмотра кода, из которого его можно сохранить или распечатать:



QR-код можно сгенерировать также в окне *Выдача идентификатора*. Кнопка для открытия этого окна становится доступной после согласования заявки:

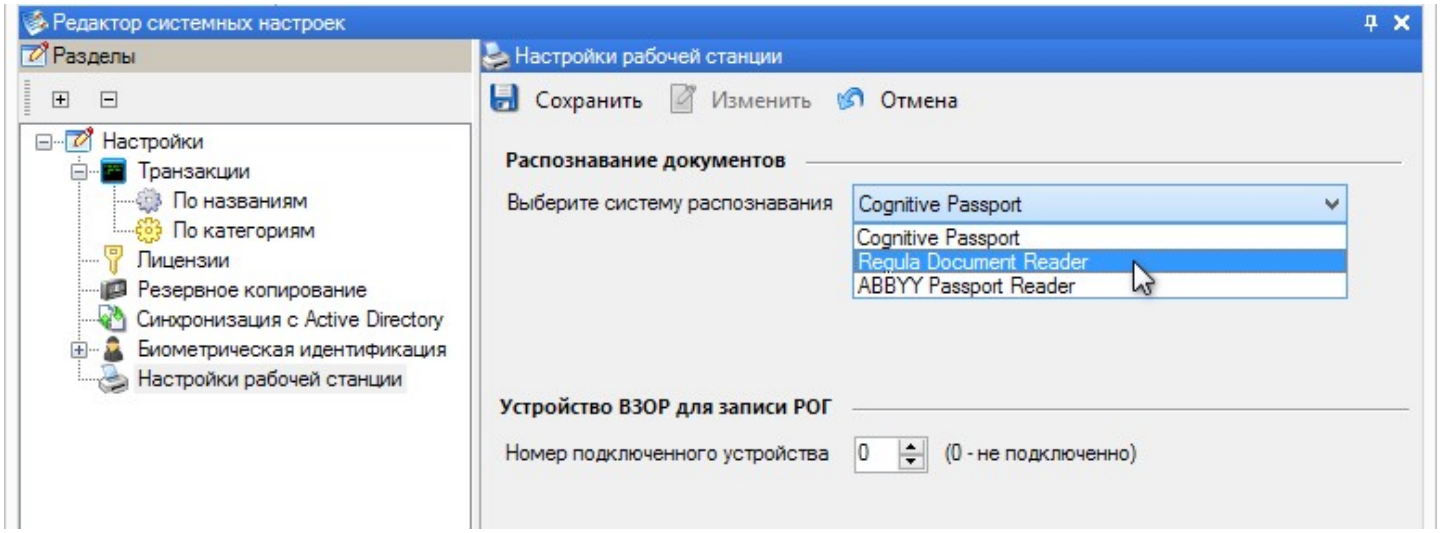


8.12.3.7 Настройки рабочей станции

В этом разделе отображаются настройки, относящиеся к тому ПК, на котором открыто данное ПО ParsecNET 3.

Распознавание документов

Если к Вашему компьютеру подключена какая-либо система распознавания документов[671], в этом разделе необходимо указать, какая именно:



При выборе ABBYY Passport Reader имеются особенности. Дальнейшие действия описаны в соответствующем разделе[675].

Устройство Взор для записи РОГ

Если к Вашему компьютеру подключен биометрический сканер Взор[350], который используется для записи сканов радужной оболочки глаз (РОГ) в БД, необходимо указать номер этого устройства. Номер устройства, которое используется только для идентификации по РОГ указывать не нужно.

8.12.4 Мобильный терминал доступа

Терминал удаленной регистрации субъектов доступа предназначен для регистрации проходов сотрудников и посетителей на территорию не на точке доступа (например, в автобусе).

Мобильный терминал представляет собой мобильное устройство на ОС Android версии не ниже 7 с установленным приложением "Parsec Access Terminal". Связь с сервером ParsecNET 3 осуществляется по сети посредством Wi-Fi соединения или мобильного интернета. Для чтения карт используется встроенный NFC-модуль смартфона или внешний RFID-модуль чтения карт. Для идентификации по QR коду приложение имеет встроенный сканер QR кодов.

Для работы мобильного терминала с сервером ParsecNET 3 они должны находиться в одной локальной сети.

Настройки для работы мобильного терминала с картами Mifare Plus задаются в ПО ParsecNET в разделе Работа с картами Mifare Plus[125].

При наличии связи с сервером события с мобильного устройства передаются в БД системы сразу. При отсутствии связи, транзакции накапливаются в буфере мобильного устройства. Передача происходит при восстановлении связи по нажатию кнопки внизу экрана приложения.

В общем, использование мобильного терминала выглядит следующим образом:

1. В ПО ParsecNET 3 создаются и настраиваются[360] точки доступа "Мобильный терминал" по количеству физических устройств, которые будут использоваться в качестве мобильных терминалов доступа;
2. Если планируется работа с картами Mifare Plus, производятся соответствующие настройки[125];
3. На смартфоны с ОС Android 7 или выше устанавливается[364] приложение "Parsec Access Terminal";
4. Мобильные терминалы регистрируются[371] в ПО ParsecNET 3;
5. Базы данных на мобильных терминалах и в ParsecNET 3 синхронизируются[364];
6. Операторы авторизуются в приложениях и осуществляют контроль за проходом субъектов доступа.



Мобильный терминал работает только при его создании на сервере ParsecNET 3.

Старые версии приложения "Parsec Access Terminal" (до версии 1.1.34) также поддерживаются, но не имеют возможности воспользоваться новым функционалом:

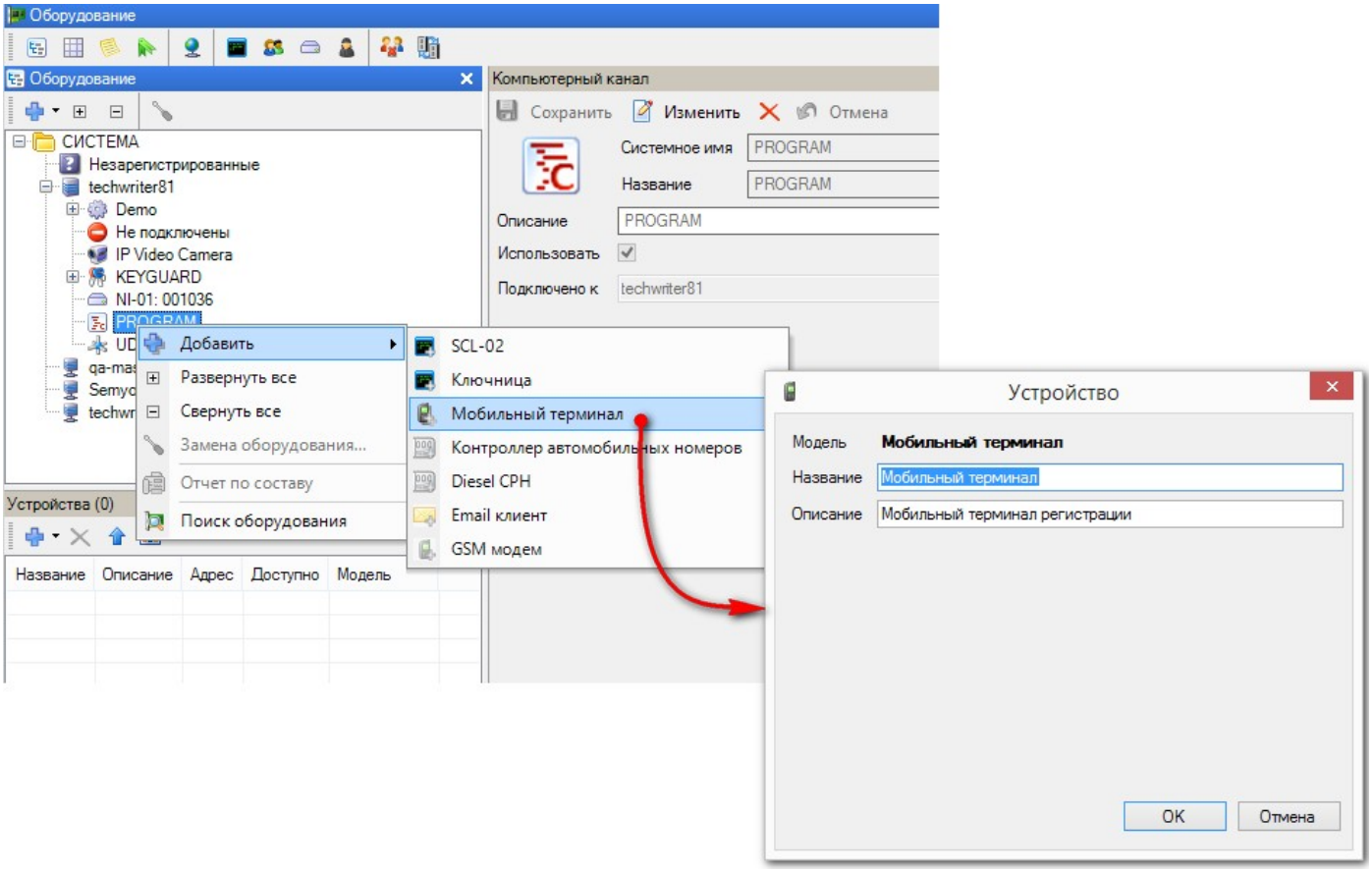
- работа с картами Mifare Plus SL1/SL3;
- шифрование персональных данных сотрудников в локальной Базе данных;
- автоматическое обновление данных по расписанию (в т.ч. в онлайн-режиме, не обязательно закрывать приложение);
- различные способы отображения фотографии субъекта доступа;
- QR сканер.

8.12.4.1 Создание и настройка мобильного терминала в ParsecNET 3

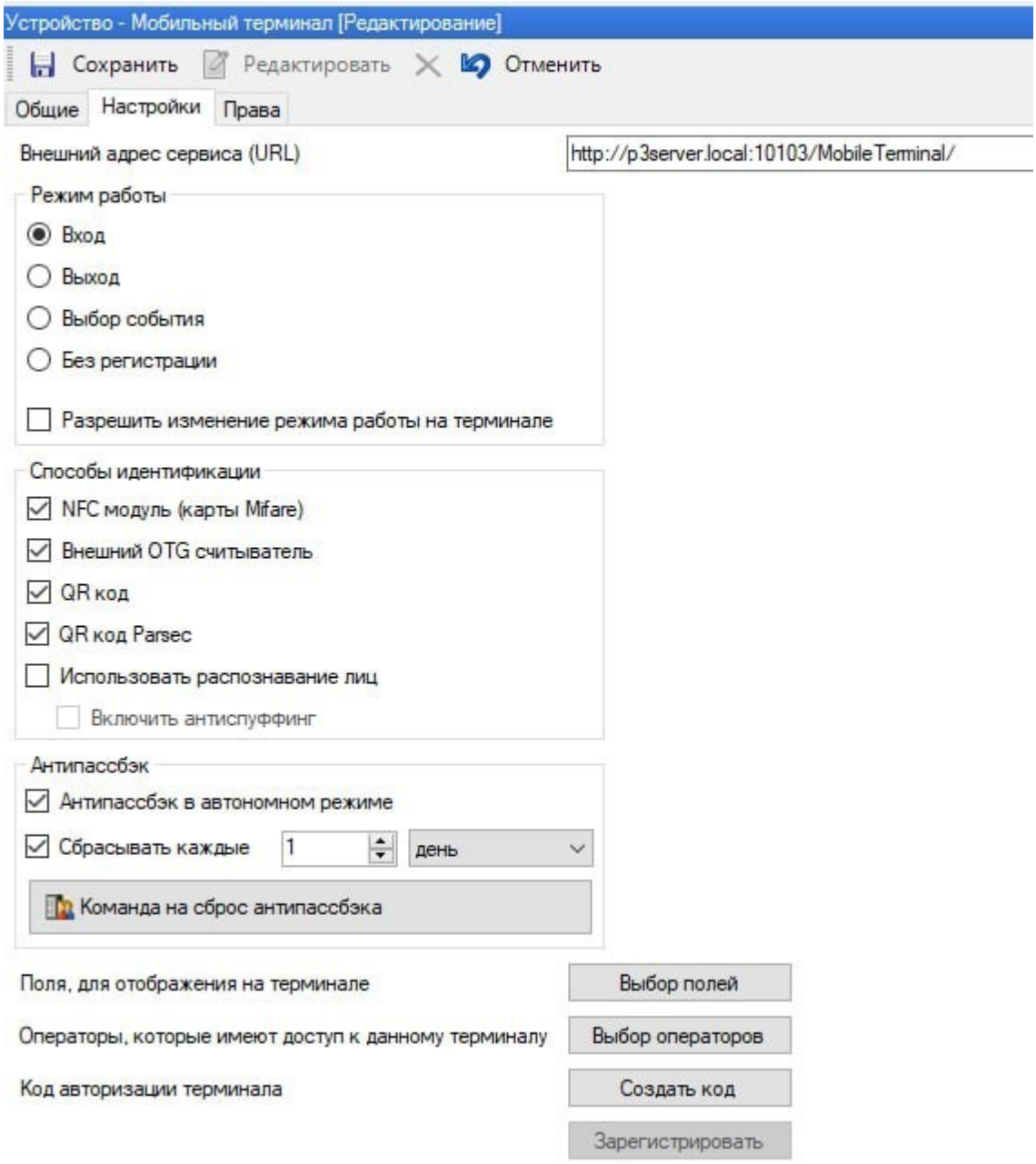
Чтобы создать в системе ParsecNET 3 мобильный терминал и настроить его, выполните следующие действия:

1. Перейдите в редактор оборудования и нажмите правой клавишей мыши на значок канала PROGRAM. Если такой канал не отображается на панели *Оборудование*, проведите поиск оборудования. Для этого откройте контекстное меню на значке сервера и выберите команду "Поиск оборудования";
2. В раскрывшемся списке выберите пункт *Добавить - Мобильный терминал*. Откроется окно *Устройство*;

3. Введите название и, при необходимости, описание устройства, которые в дальнейшем позволят его легко идентифицировать и нажмите на кнопку *ОК*. В системе будет создано устройство *Мобильный терминал*;



4. Перейдите на вкладку *Настройки*, а затем в режим редактирования:



5. Произведите настройку мобильного терминала:

В блоке *Режим работы* выбирается режим работы мобильного терминала, выбор которого определяет, какие решения оператор сможет принимать в отношении считанной терминалом карты пользователя:

- *Вход* - считанные карты автоматически регистрируются на вход, оператор может запретить вход;
- *Выход* - считанные карты автоматически регистрируются на выход, оператор может запретить выход;
- *Выбор события* - автоматическая регистрация события для карты отсутствует, от оператора требуется принятие решения для считанной карты: зарегистрировать вход, выход или запрет прохода;
- *Без регистрации* - просмотр карточки субъекта доступа, событие доступа не формируется;
- *Разрешить изменение режима работы на терминале* - при установленном флажке появляется возможность изменять режим работы в мобильном терминале. При этом выбор в мобильном терминале имеет приоритет.

В разделе *Способы идентификации* производится выбор способов, которыми мобильный терминал будет считывать идентификаторы пользователей:

- *NFC модуль (карты Mifare)* - мобильный терминал сможет читать карты семейства Mifare, при условии, что мобильное устройство имеет в своем составе модуль NFC;
- *Внешний OTG считыватель* - флажок ставится при использовании для чтения карт внешний считыватель, подключаемый в USB-порт мобильного устройства;
- *QR код* - идентификация осуществляется посредством чтения QR-кода при помощи камеры мобильного устройства;
- *QR код Parsec* - идентификация осуществляется посредством чтения камерой мобильного устройства QR-кода, сгенерированного[269] в ПО ParsecNET 3;
- *Использовать распознавание лиц* - при установке данного флажка идентификация может осуществляться путем распознавания лица субъекта доступа;
  - *Включить антиспуффинг* - установка флажка включает защиту при распознавании лиц. Суть защиты заключается в отслеживании движения лица по серии входных кадров с целью определения динамических признаков, позволяющих различать реальное и поддельное лицо (например, фотографию вместо реального лица).

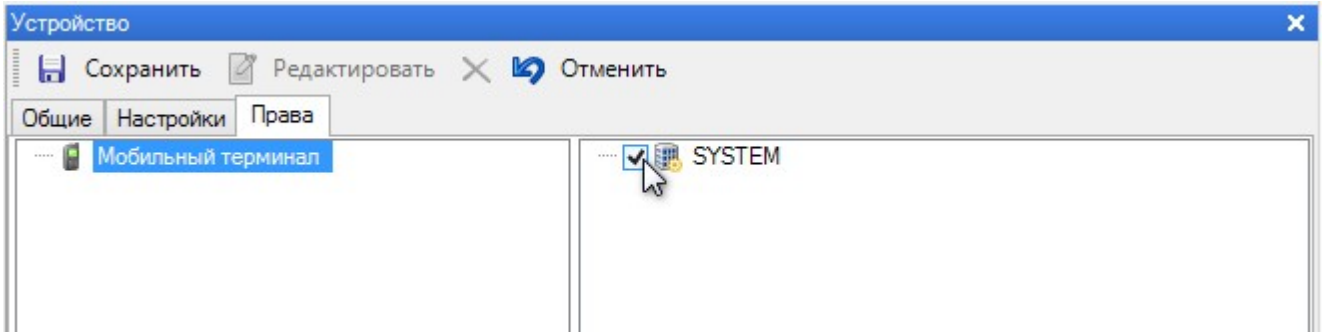
В разделе *Антипассбэк* производится настройка параметров запрета повторного прохода по одному и тому же идентификатору.

- *Антипассбэк в автономном режиме* - установка флажка включает режим запрета двойного прохода на данном терминале.
- *Сбрасывать каждые* (минута\час\день) - установка флажка разрешит проход в одном направлении по истечении указанного в параметре времени. Если флажок не установлен, двойной проход будет запрещен всегда.
- *Команда на сброс антипассбэка* - отправляет в терминал команду на принудительный сброс состояний АПБ у идентификаторов. Команда будет отправлена после сохранения карточки терминала. В момент отправки команды терминал может не иметь связи с сервером. В таком случае команда будет отправлена и обработана терминалом в момент возникновения связи с сервером. Все это время (пока команда не обработана) в карточке устройства будет видна кнопка «Команда на сброс антипасбэка».

Кнопки выбора настроек:

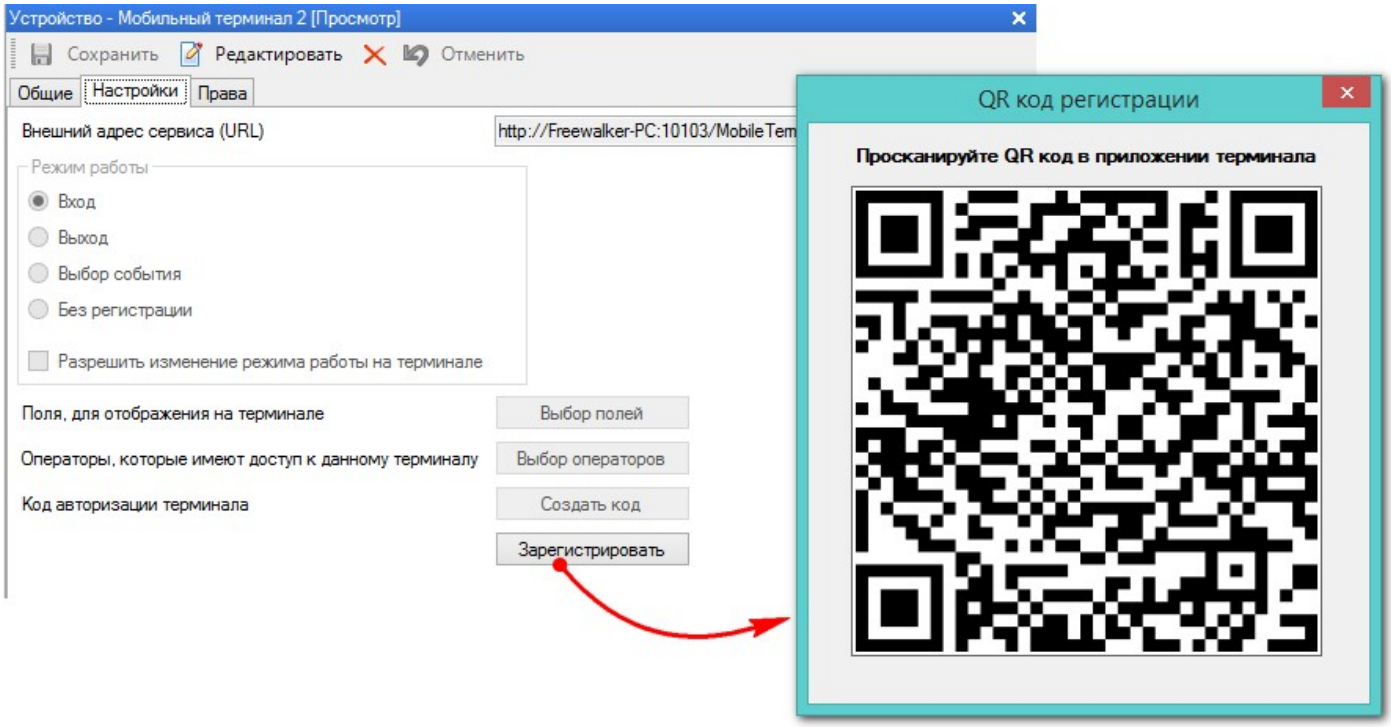
- *Выбор полей* - нажмите, чтобы добавить поля данных о субъекте прохода, которые будут отображаться в приложении "Parsec Access Terminal" на смартфоне. По умолчанию отображаются поля *Имя субъекта* и *Подразделение*;
- *Выбор операторов* - кнопка для добавления операторов, которые будут иметь право доступа в приложение "Parsec Access Terminal" на зарегистрированном для этой мобильной точки прохода смартфоне;
- *Создать код* - нажмите на кнопку после завершения настройки. Система создаст QR-код для регистрации мобильного терминала.

6. Перейдите на вкладку *Права* и выберите в левой части мобильный терминал;
7. Установите флажки у тех организаций, которые будут отображать мобильный терминал в своей топологии и назначать его своим группам доступа:



8. Нажмите на кнопку *Создать код*. Система сгенерирует QR-код, который используется приложением "Parsec Access Terminal" для регистрации мобильного терминала в системе;

9. Сохраните настройки, нажав на кнопку *Сохранить*. Карточка устройства выйдет из режима редактирования, а кнопка *Зарегистрировать* станет активной. При нажатии на нее появится созданный ранее QR-код, который требуется сосканировать приложением "Parsec Access Terminal":



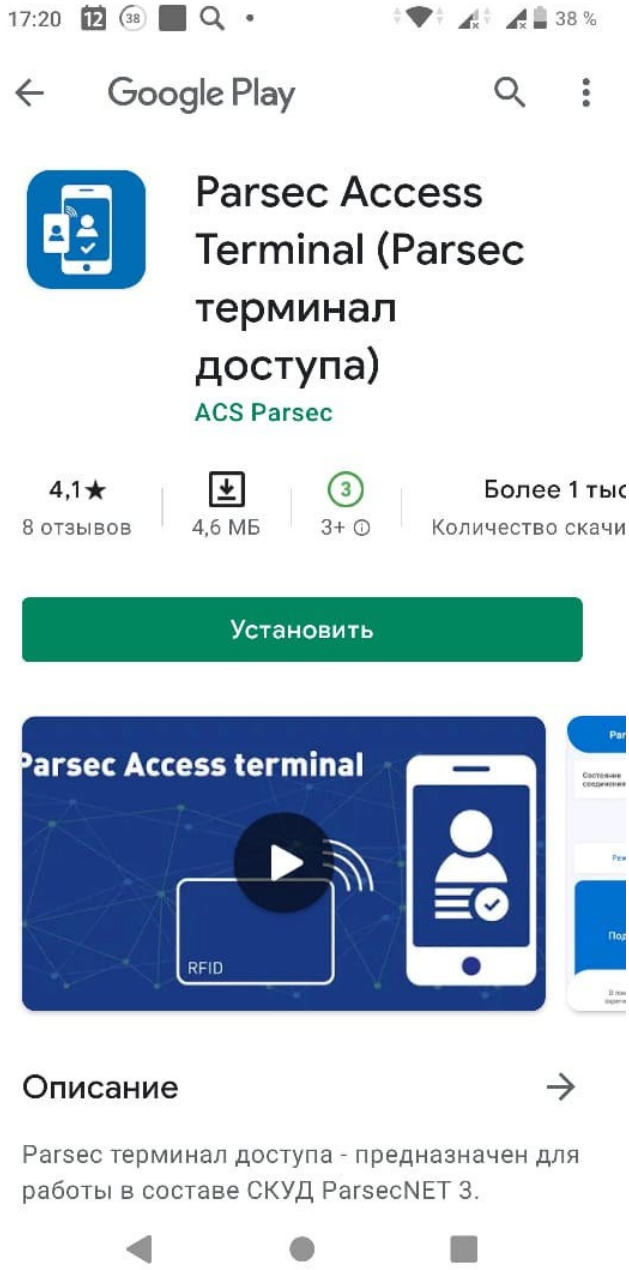
10. Назначьте устройство "Мобильный терминал" тем группам доступа, члены которых будут осуществлять проход при помощи смартфона или планшета с приложением "Parsec Access Terminal".

Далее с устройством "Мобильный терминал" работают так же как и с обычным контроллером: размещают на графпланах, следят за событиями в мониторе событий и т.п.

8.12.4.2 Установка приложения на смартфон

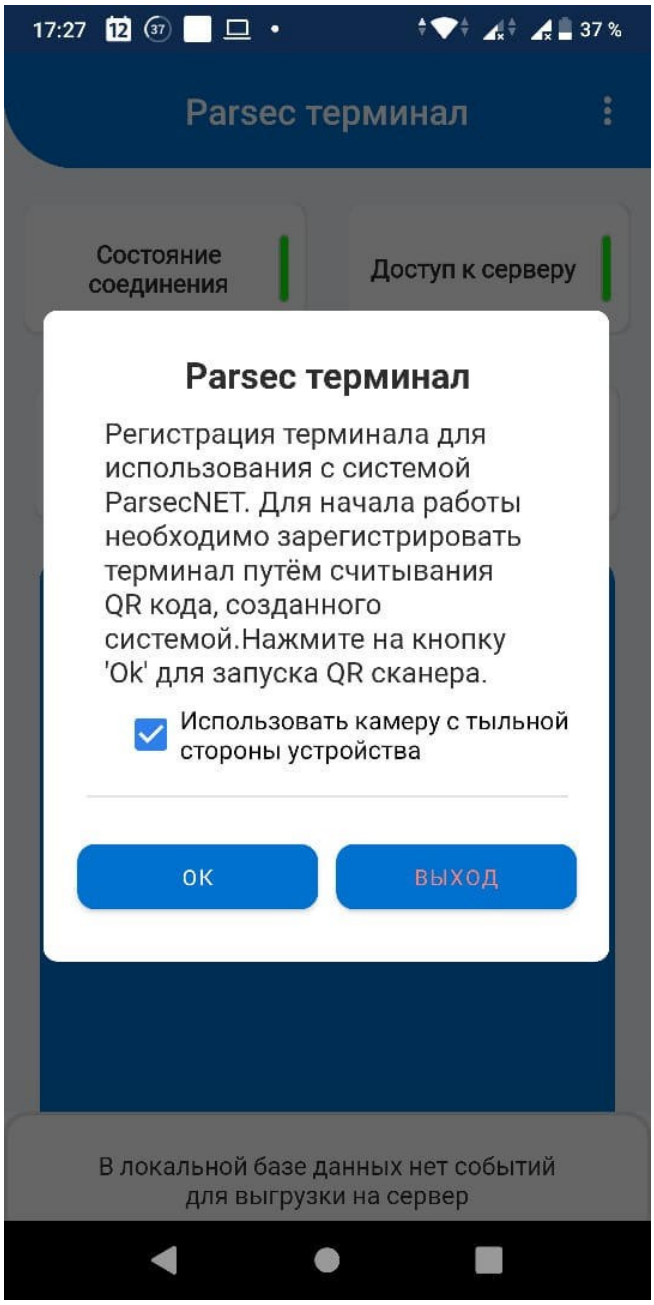
Перед установкой приложения убедитесь, что на Вашем мобильном устройстве установлена операционная система Android версии 7 или выше.

Установите приложение "Parsec Access Terminal" из магазина Google Play:

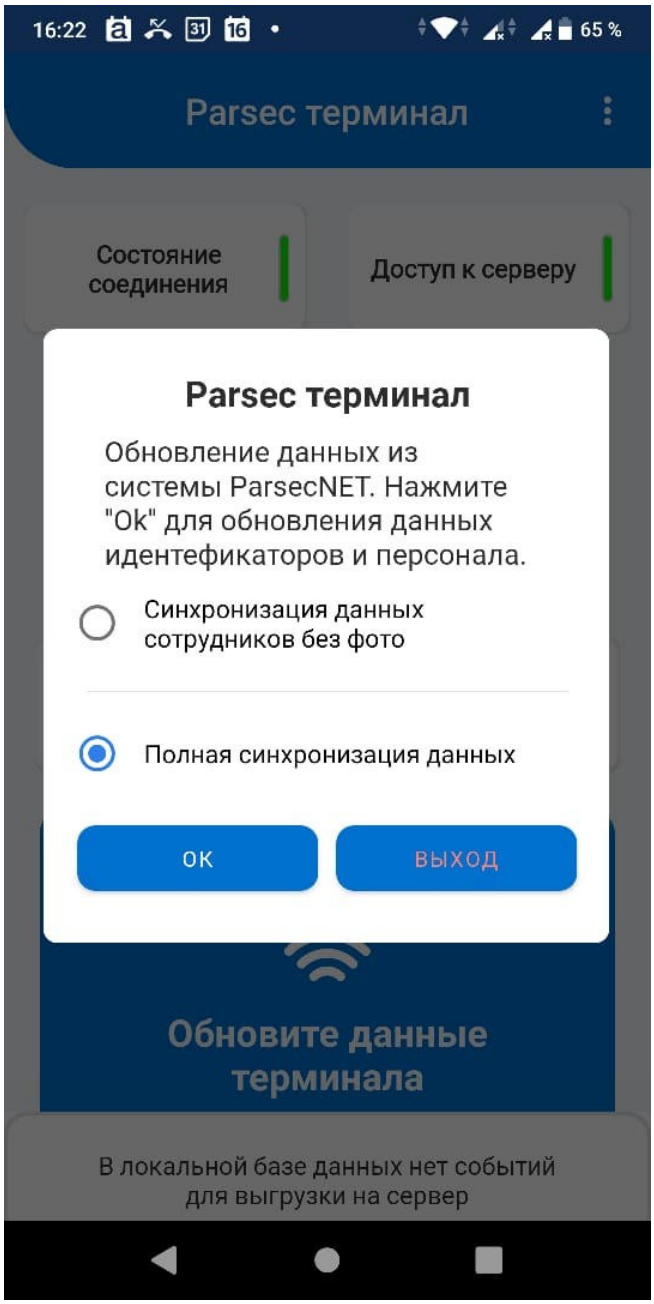


Для запуска приложения после установки нажмите на кнопку *Открыть* или коснитесь значка приложения на экране мобильного устройства.

Свежеустановленное приложение после запуска потребует зарегистрировать его в системе ParsecNET 3.



Нажмите на кнопку *ОК* и наведите сканер на окно с QR-кодом на экране монитора (о QR-коде см. шаг 9 364). Приложение автоматически зарегистрируется в системе ParsecNET 3, после чего будет предложено синхронизировать базы данных сервера системы и мобильного терминала:



Варианты синхронизации:

- *Синхронизация данных сотрудников без фото* - в локальную БД мобильного терминала поступают сведения о новых пользователях и их картах доступа. Фотографии не загружаются в мобильный терминал;
- *Полная синхронизация данных* - в БД мобильного терминала поступают полные данные: новые пользователи и их карты; логины и пароли операторов, имеющие доступ к терминалу и т.д. в том числе фотографии.

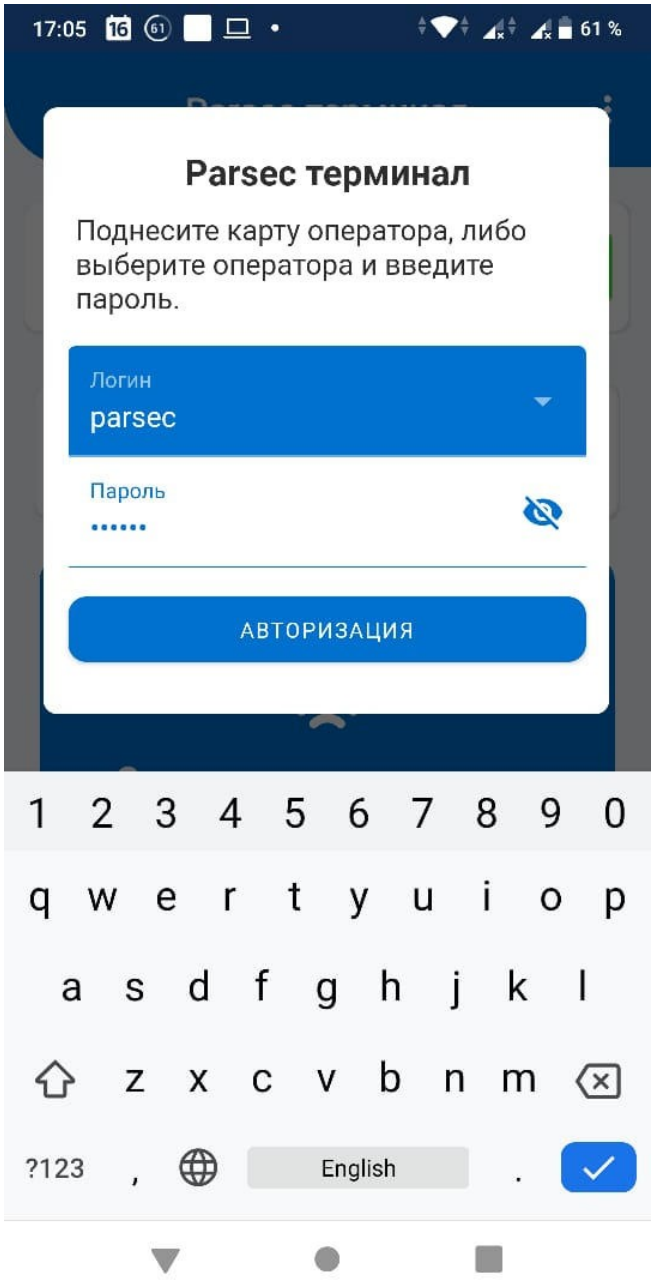
После новой установки мобильного терминала необходимо провести полную синхронизацию. Для этого выберите соответствующий вариант и нажмите на кнопку *OK*.

В случае ошибки при регистрации терминала или при синхронизации данных, приложение выводит информационное сообщение. Устраните описанные недостатки и повторите действие.

После того, как локальная база данных мобильно терминала и база данных сервера синхронизируются, пользователю будет предложено авторизоваться для входа.

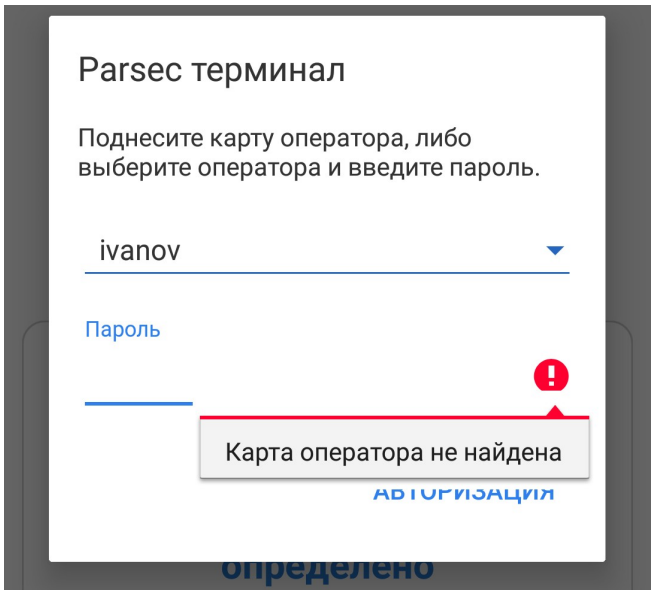
При нажатии на экран в поле логина оператора откроется список выбора операторов, имеющих право доступа в мобильный терминал.

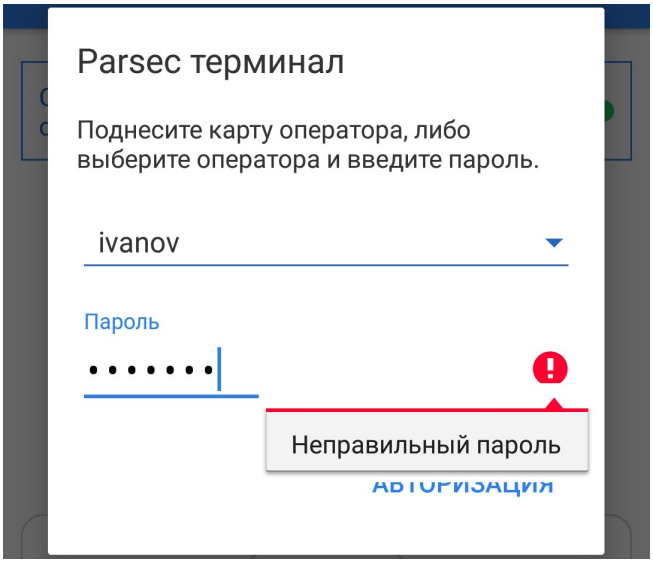
При нажатии на экран в поле пароля появится экранная клавиатура для набора пароля:



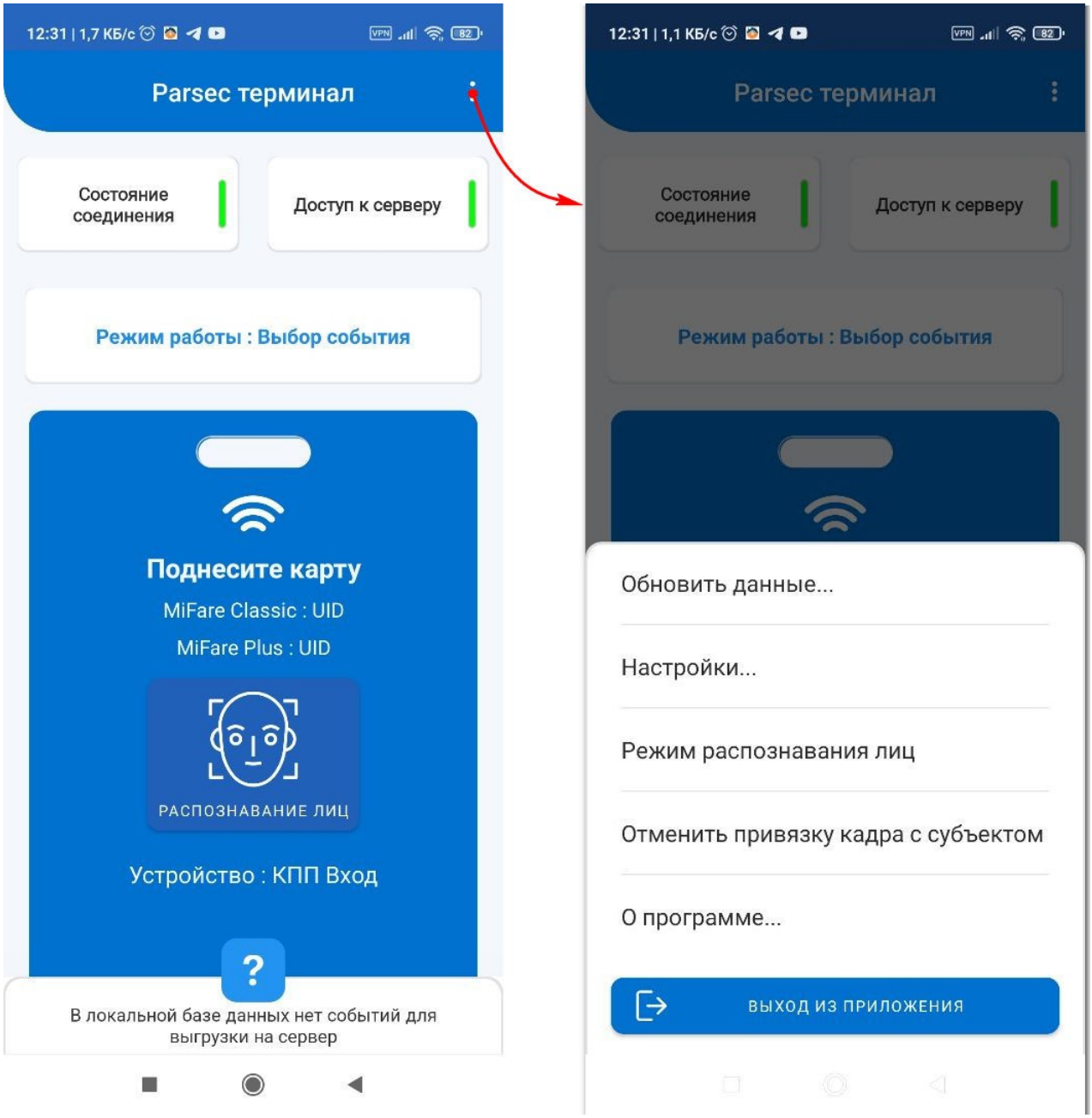
Также оператор может авторизоваться, поднеся свою карту к NFC или RFID считывателю.

При попытке авторизоваться при помощи некорректных карты или пароля приложение выдаст соответствующее сообщение:





После успешной установки, первой синхронизации и авторизации оператора экран мобильного терминала имеет следующий вид:

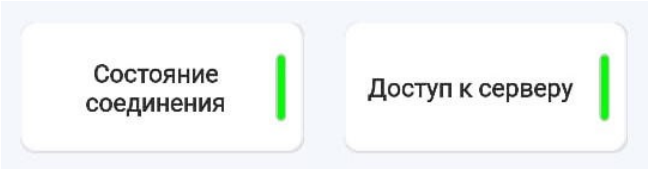


При нажатии на кнопку  открывается список команд:

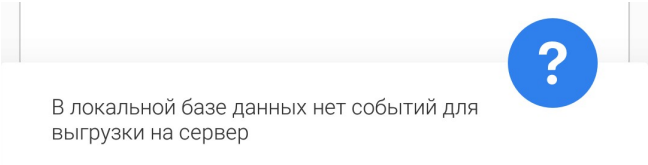
- *Обновить данные...* - открывается окно синхронизации[367] локальной и серверной баз данных;
- *Настройки...* - просмотр и редактирование параметров приложения:
  - *Регистрация терминала* - открывает окно регистрации[366] мобильного терминала при помощи QR-кода[364];
  - *Настройки соединения* - просмотр параметров соединения;
  - *Сменить оператора* - открывается окно авторизации[364] оператора;
  - *Параметры автообновления данных* - настраивается расписание и варианты обновления базы данных с сервера;
  - *Режим работы* - открывается окно, в котором оператор может выбрать, какие решения он сможет принимать в отношении считанной терминалом карты пользователя:
    - *Вход* - считанные карты автоматически регистрируются на вход, оператор может запретить вход;
    - *Выход* - считанные карты автоматически регистрируются на выход, оператор может запретить выход;
    - *Выбор события* - автоматическая регистрация события для карты отсутствует, от оператора требуется принятие решения для считанной карты: зарегистрировать вход, выход или запрет прохода;
    - *Без регистрации* - просмотр карточки субъекта доступа, событие доступа не формируется.
  - *Способ отображения фото* - выбор способа, которым будет размещаться фотография субъекта доступа в окне мобильного терминала:
    - *Вписать по центру* - фото масштабируется, чтобы вписаться в окно, пропорции могут не сохраняться;
    - *По центру (без скейла)* - фотография отображается в исходном размере, без масштабирования. Если фото большего размера, чем окно, то края обрезаются;
    - *По центру с обрезкой* - фото увеличивается или уменьшается так, чтобы ширина (или высота) картинки совпала с шириной (или высотой) окна, а остальное обрезается;
    - *Внутри по центру* - фото масштабируется, чтобы вписаться в окно, сохраняя пропорции.
  - *Задержка автозакрытия карточки* - настройка времени, в течение которого на экране приложения будет отображаться карточка субъекта доступа;
  - *QR сканер* - установите флажок в окне настройки, если идентификация субъектов доступа будет производиться по QR коду;
  - *Включить звуковое оповещение* - при установленном флажке мобильное устройство будет издавать звуковой сигнал при чтении карты как встроенным NFC модулем, так и внешним OTG считывателем;
  - *125Khz считыватель* - настройка используется только при установке приложения "Parsec Access Terminal" на мобильные устройства бренда KCOSIT со встроенным 125 KHz считывателем:
    - *Запуск чтения порта считывателя* - флажок устанавливается при использовании на устройствах KCOSIT;
    - *Номер порта* - выберите один порт из списка доступных;
    - *Скорость порта* - выберите значение из списка доступных скоростей: 1200, 2400, 4800, 9600, 14400, 19200, 38400, 56000, 57600, 115200, 128000, 256000 бит/с;
    - *Вольтаж порта* - выберите значение, соответствующее режиму работы вашего устройства.
- *Режим распознавания лиц* - переключение на процедуру[372] распознавания лица;
- *Отменить привязку кадра с субъектом* - отмена[377] привязки кадра, размещенного на вкладке *FaceID* карточки сотрудника в Редакторе персонала, к данному сотруднику.

- *О программе...* - сведения о версии программы;
- *Выход из приложения* - завершение работы.

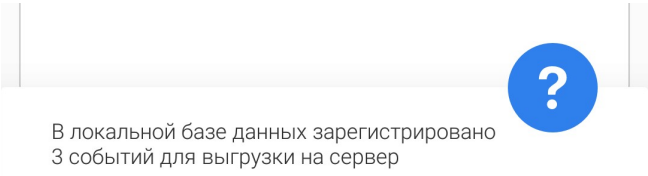
Зеленые сигналы вверху экрана говорят о наличии соединения и доступа к серверу. О потере соединения или доступа сигнализируют соответствующие красные сигналы.



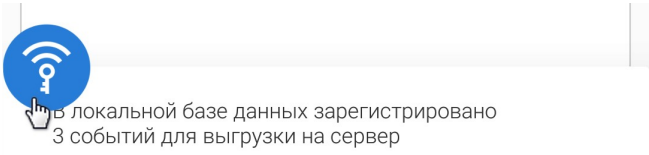
Надпись внизу экрана сообщает о состоянии локальной БД:



При потере связи с сервером , события будут накапливаться в мобильном терминале и надпись будет выглядеть примерно так:



После восстановления связи синяя кнопка изменит свой вид. Необходимо нажать на нее, чтобы синхронизировать данные локальной и серверной БД.

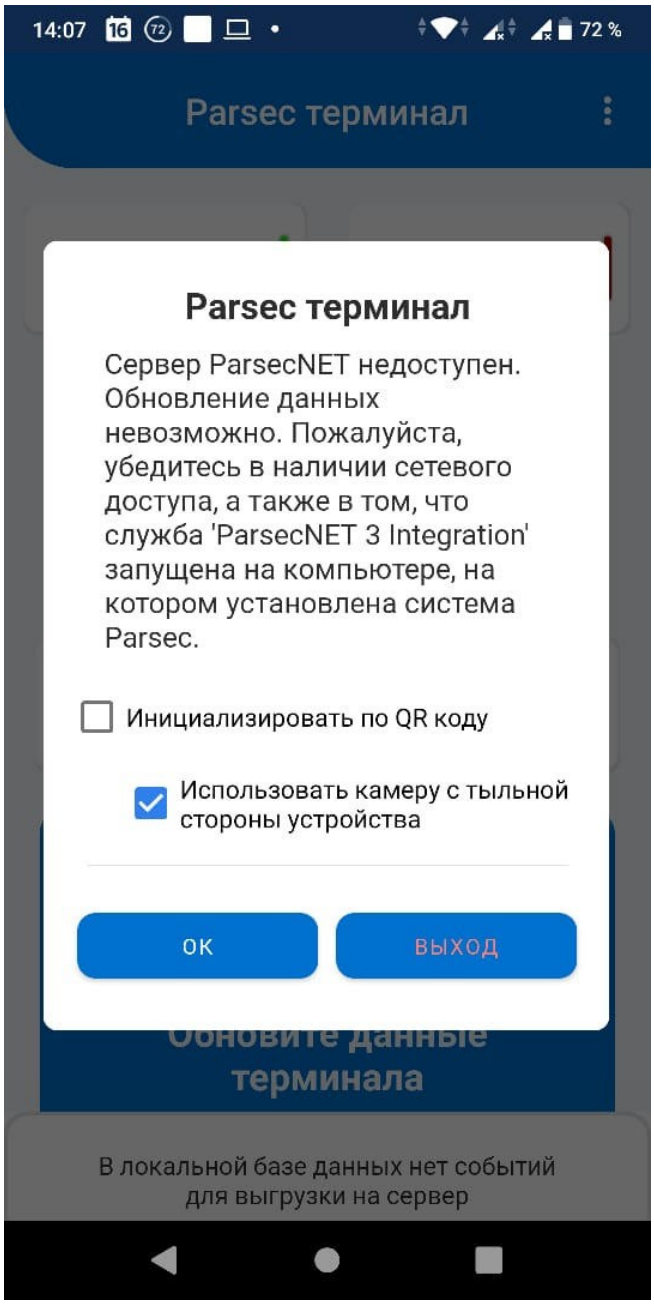


8.12.4.3 Инициализация мобильного терминала

Под инициализацией мобильного терминала подразумевается получение приложением "Parsec Access Terminal" данных о настройках мобильного терминала в ПО сервера ParsecNET 3. Первая инициализация происходит при первом установлении связи с сервером Parsec. Повторная инициализация потребуется в случаях, когда сервер сменил IP-адрес, мобильный терминал в Редакторе оборудования был удален, а затем создан новый и т.п. Во всех этих случаях у приложения "Parsec Access Terminal" доступ к серверу ParsecNET 3 будет отсутствовать.

Чтобы заново инициализировать мобильный терминал, выполните шаги:

1. Выберите *Обновление данных...* в меню. Откроется окно:



2. Установите флажок "Инициализировать по QR коду" и нажмите на кнопку *ОК*. Откроется окно сканера QR-кодов;
3. Отсканируйте QR код, сгенерированный[364] в настройках мобильного терминала в ПО ParsecNET 3. Настройки соединения обновятся, а база данных пользователей будет удалена и ее необходимо будет синхронизировать снова.

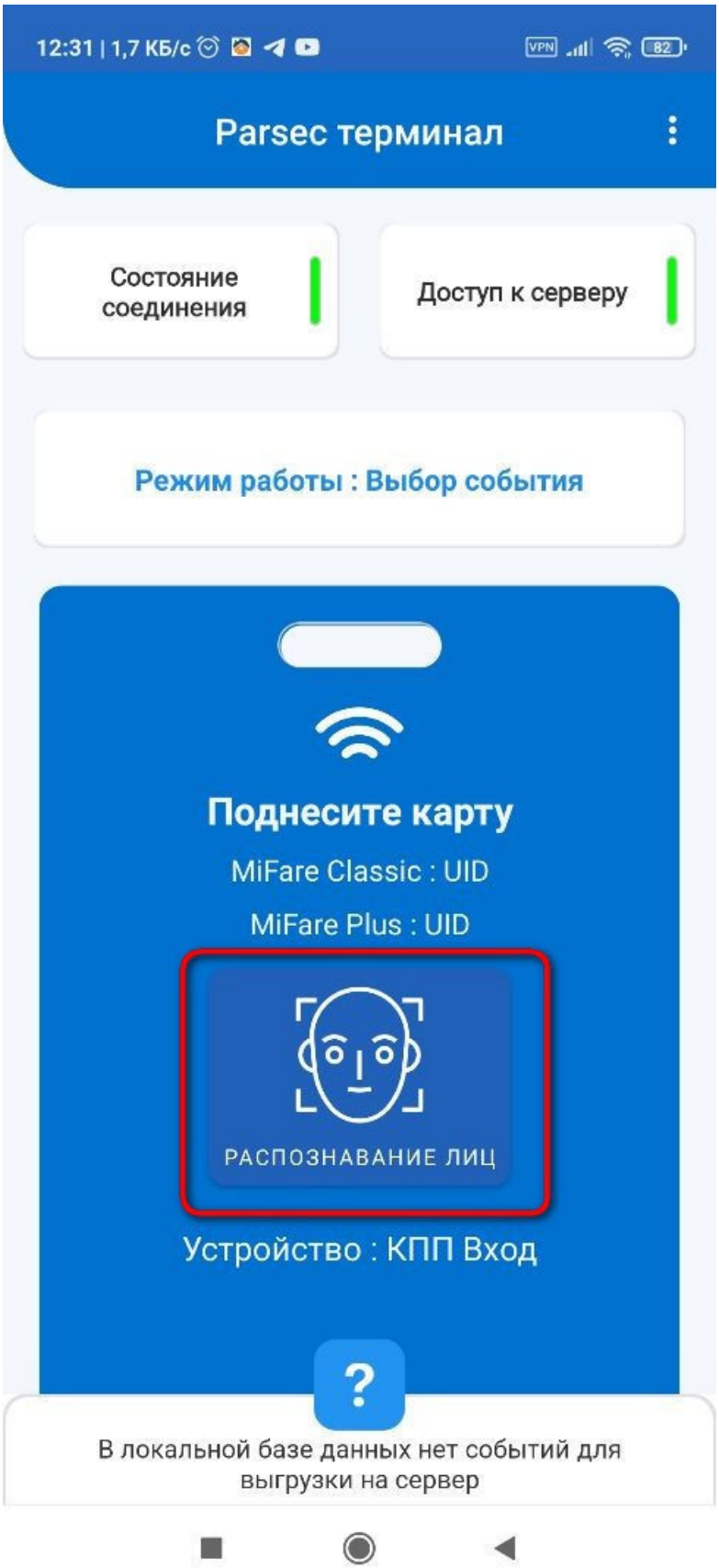
Далее действуйте как обычно после регистрации нового терминала.

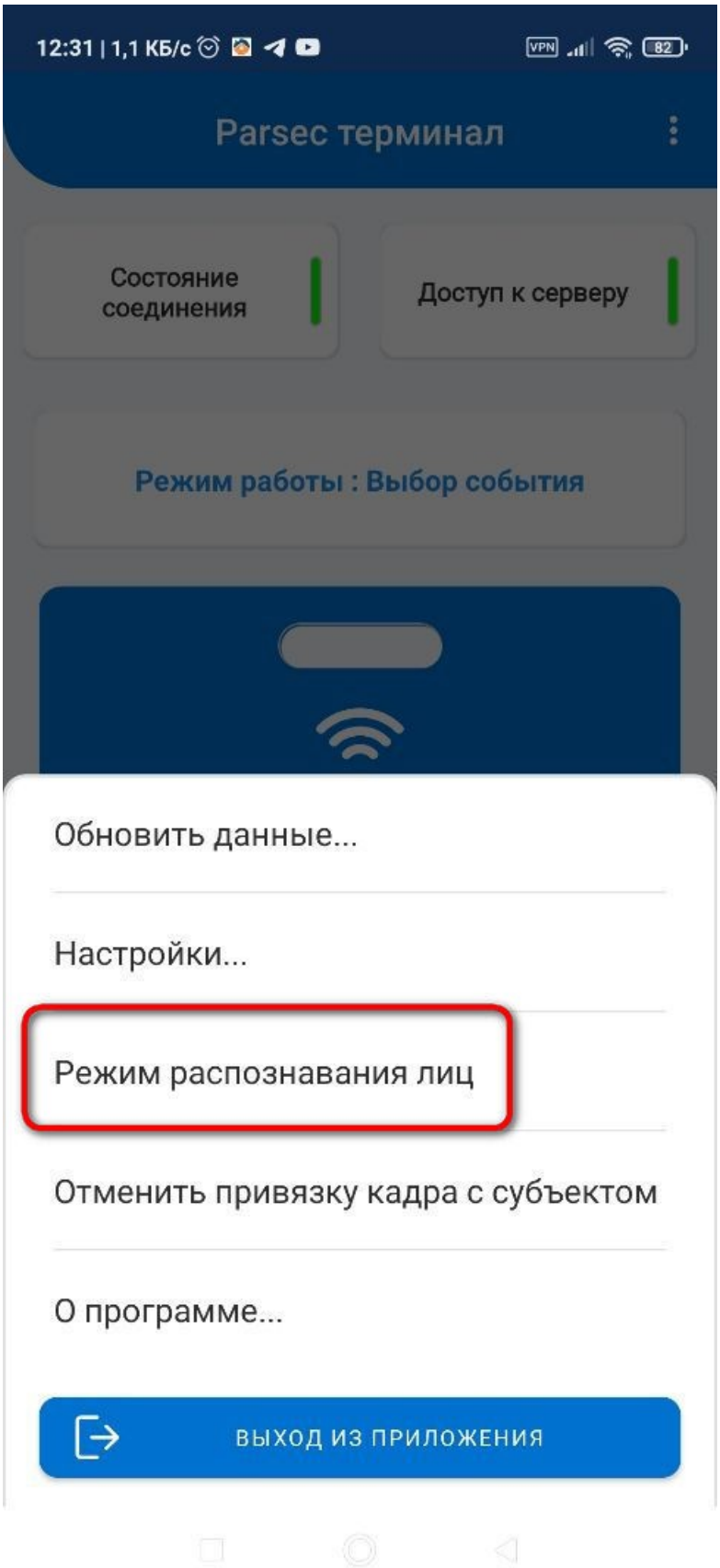
8.12.4.4 Идентификация по лицу

Мобильный терминал имеет возможность производить идентификацию субъекта доступа по лицу. Для этого в настройках[360] мобильного терминала в ПО ParsecNET должен быть установлен флажок *Использовать распознавание лиц* и, при необходимости, *Включить антиспуффинг*.

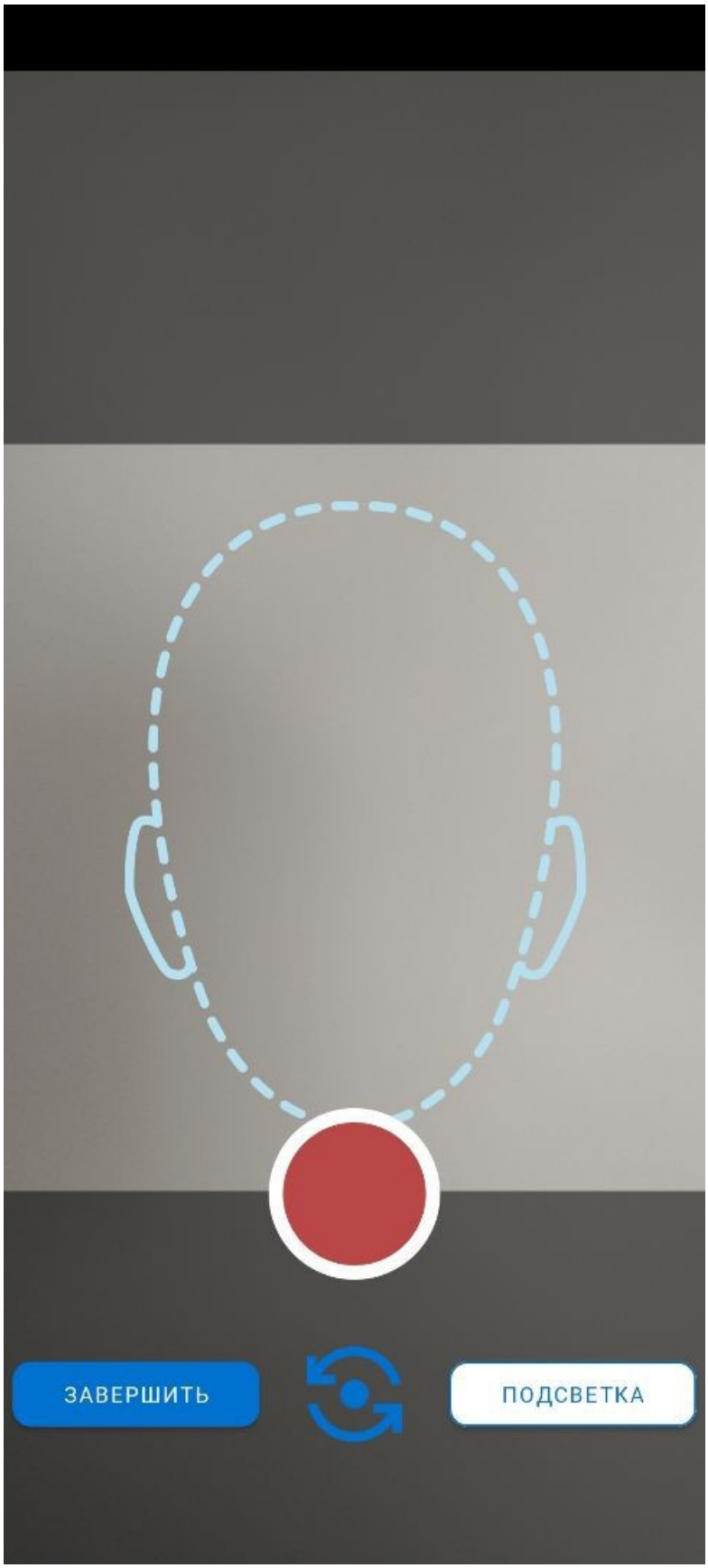
Для идентификации по лицу произведите следующие действия:

1. Нажмите на кнопку *Распознавание лиц* на главном экране мобильного терминала или выберите пункт "Режим распознавания лиц" в меню мобильного терминала:


12:31 | 1,7 КБ/с
Parsec терминал
Состояние соединения
Доступ к серверу
Режим работы : Выбор события
Поднесите карту
MiFare Classic : UID
MiFare Plus : UID
РАСПОЗНАВАНИЕ ЛИЦ
Устройство : КПП Вход
В локальной базе данных нет событий для выгрузки на сервер



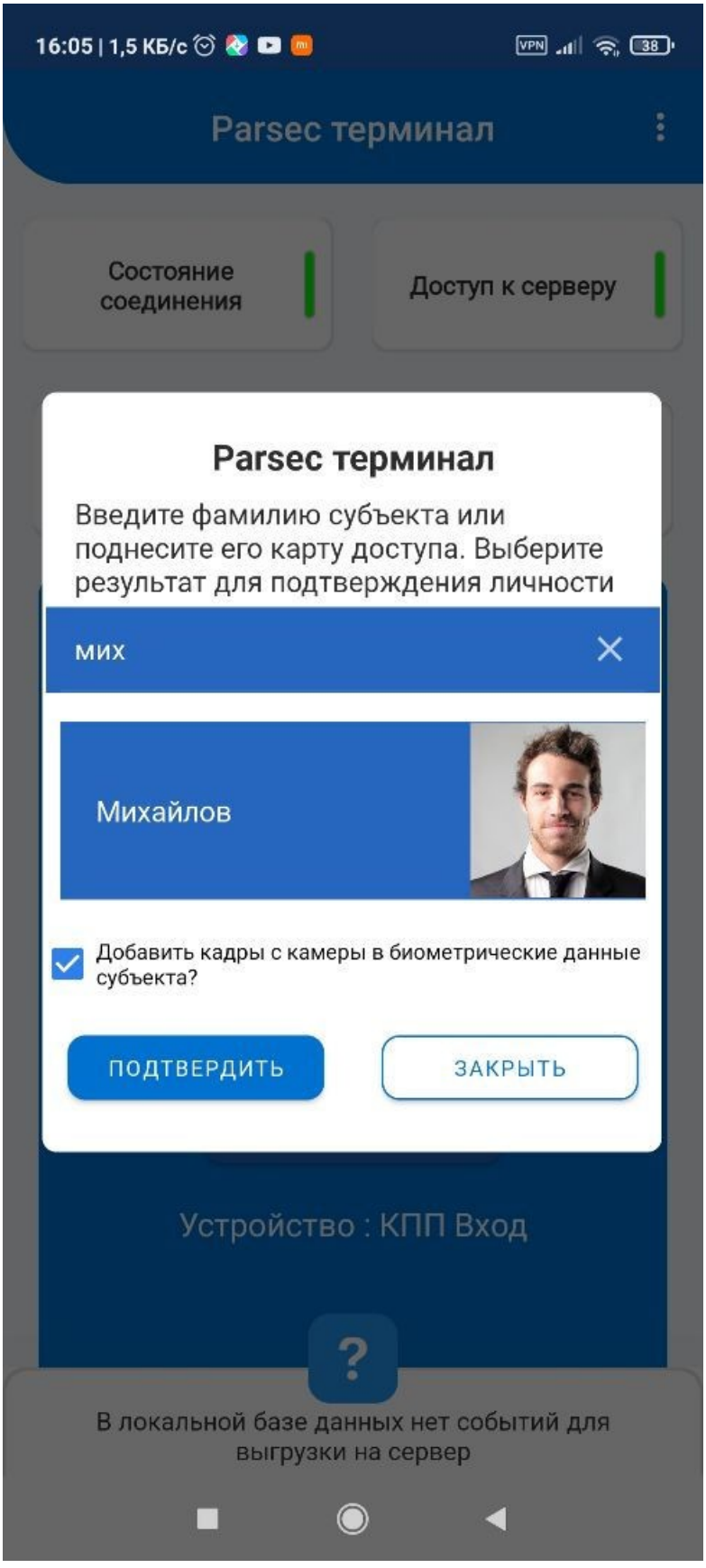
Откроется окно распознавания лица:



Элементы управления окна:

- *Завершить* - завершает процедуру распознавания и закрывает окно;
- Круговые стрелки - переключение между задней и фронтальной камерами мобильного устройства;
- *Подсветка* - включение светодиодов подсветки мобильного устройства.

2. Наведите камеру так, чтобы лицо субъекта доступа попадало в очерченную пунктирной линией область на экране мобильного устройства, и нажмите на красную кнопку, удерживая ее до тех пор, пока:
   - субъекту будет предоставлен доступ. При этом откроется карточка субъекта доступа, лицо которого было распознано. Либо,
   - доступ будет запрещен. При этом появится окно привязки кадра к записи субъекта доступа в БД СКУД. Проверка личности субъекта доступа и привязка изображения его лица к записи в БД СКУД возлагается на оператора мобильного терминал;



3. Введите в поле поиска начальные буквы фамилии субъекта доступа или пусть он приложит свой идентификатор к мобильному терминалу. В окне должна появиться запись (-си) из БД СКУД, включающие в себя введенные символы;
4. Если есть необходимость добавить к записи новое изображение субъекта доступа, установите флажок *Добавить кадры с камеры в биометрические данные субъекта?* Кадры хранятся на вкладке FaceID карточки субъекта в Редакторе персонала;
5. Нажмите на кнопку *Подтвердить*. проход будет предоставлен, а кадр с распознанным ранее лицом будет сохранен на вкладке FaceID карточки выбранного субъекта доступа. Если флажок не будет установлен, то проход предоставляется и кадр с распознанным лицом не сохраняется. Но в следующий раз распознанное лицо не будет обнаружено в БД СКУД с большей вероятностью;

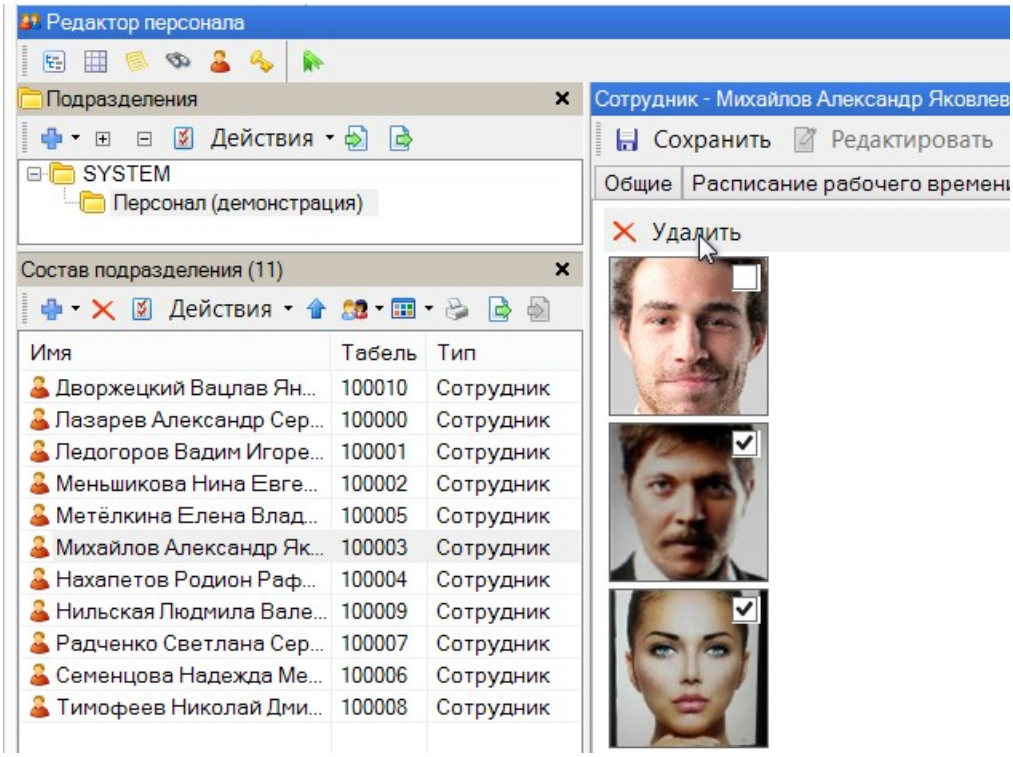
8.12.4.4.1 Отмена привязки кадра к субъекту доступа

В некоторых случаях необходимо отменить привязку кадра с распознанным лицом к субъекту доступа. Например, если кадр был привязан к не тому субъекту доступа.

Это можно сделать двумя способами: в ПО ParsecNET и в мобильном терминале.

Отмена привязки кадра в ПО СКУД ParsecNET производится следующим образом:

1. Запустите консоль *Администрирование* и откройте Редактор персонала;
2. Найдите субъект доступа, в биометрических данных которого хранятся некорректные кадры;
3. Перейдите на вкладку *FaceID* и перейдите в режим редактирования;
4. Установите флажок на тех кадрах, которые требуется удалить;
5. Нажмите на кнопку *Удалить*:

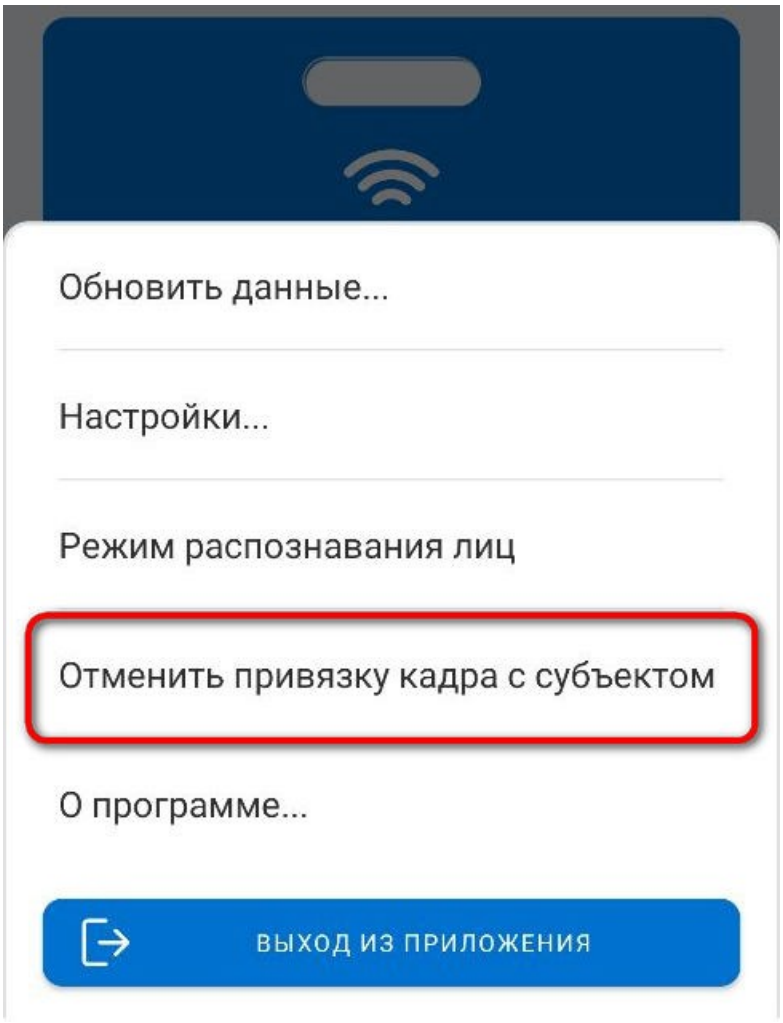


Отмена привязки кадра в мобильном терминале производится "по горячим следам". Например, когда изображение лица иванова было сохранено в карточке Михайлова. После того, как на

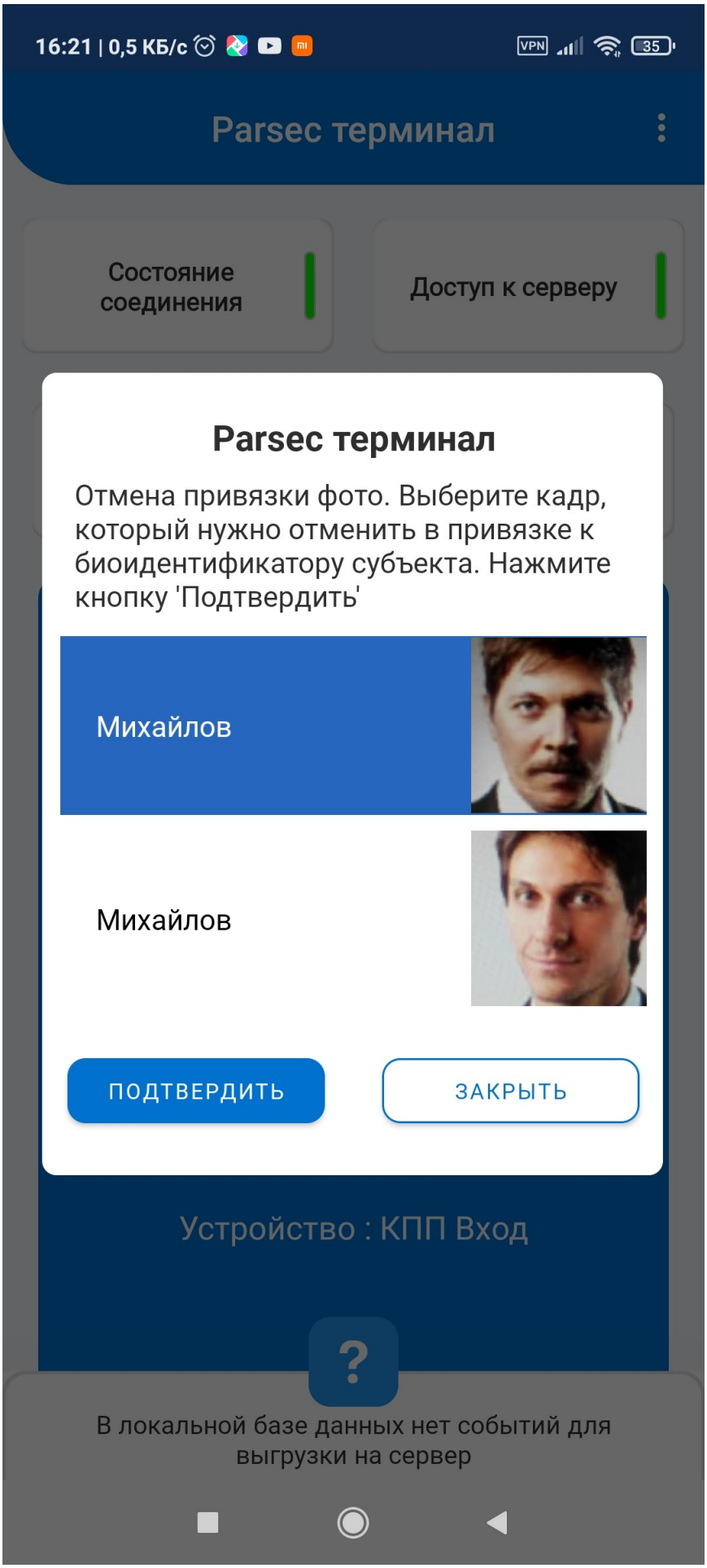
мобильном терминалу будет произведено обновление данных (вручную или по расписанию) отменить привязку кадра с субъекту доступа можно будет только в ПО ParsecNET.

Отмена привязки кадра в мобильном терминале делается следующим образом:

1. В меню выберите пункт "Отменить привязку кадра к субъекту":



Программа проанализирует все кадры во вкладках FaceID всех субъектов доступа, загруженных в мобильный терминал. Привязанные кадры, содержащие изображение, отличающееся от фотографии карточки субъекта доступа в Редакторе персонала, будут выведены списком на экран мобильного устройства:


16:21 | 0,5 КБ/с
VPN
35
Parsec терминал
Состояние соединения
Доступ к серверу
Parsec терминал
Отмена привязки фото. Выберите кадр, который нужно отменить в привязке к биоидентификатору субъекта. Нажмите кнопку 'Подтвердить'
Михайлов
Михайлов
ПОДТВЕРДИТЬ
ЗАКРЫТЬ
Устройство : КПП Вход
?
В локальной базе данных нет событий для выгрузки на сервер

2. Выделите ошибочно привязанный кадр, нажав на него и удержав нажатие. После чего нажмите на кнопку *Подтвердить*. Окно закроется, появится сообщение *Привязка кадра успешно отменена*;
3. При необходимости повторяйте процедуру, пока не будут удалены все некорректно привязанные кадры.

8.12.5 Приложение Parsec.Сотрудник

Лицензируется как Parsec.Сотрудник[344]

Для ознакомления с функционалом модуля пользователям СКУД ParsecNET 3 предоставляется 90-дневный бесплатный период.

Основное назначение мобильного приложения "Parsec Сотрудник" - использование определенных функций СКУД ParsecNET 3 в мобильных устройствах.

Приложение устанавливается на мобильные устройства с ОС Android версий 7.0 и выше. Для эмуляции карт доступа в мобильном устройстве необходимо наличие модуля NFC. В случае его отсутствия проход можно будет осуществлять только по QR-коду.
Мобильное приложение взаимодействует с сервером приложения. Сервер приложения устанавливается на ПК, который должен иметь надежную связь с сервером ParsecNET 3.

Приложение может быть использовано в двух вариантах:

1. Без авторизации на сервере. В этом случае приложение используется только для эмуляции карты доступа и прохода посредством NFC модуля или сгенерированного QR-кода. Идентификатор сотрудника автоматически формируется на основе Android ID* после установки приложения. Этот идентификатор заносится в СКУД Parsec и используется для определения его прав доступа;
2. С авторизацией на сервере приложения. Для этого пользователь должен быть предварительно занесен в СКУД Parsec. После авторизации на мобильное устройство пользователя будет автоматически передан его первичный идентификатор из СКУД, и он сразу сможет пользоваться этим устройством для прохода посредством NFC модуля или по QR-коду. Кроме этого, пользователь получает доступ к службам (в соответствии со своей ролью):
   - Заявка - просмотр, создание и удаление заявок Бюро пропусков. Изменение статуса заявки приходит в виде PUSH-уведомлений на мобильное устройство пользователя;
   - Опоздание - получение сведений об опоздавших сотрудниках видимых пользователю подразделений;
   - Присутствие - получение сведений о присутствии/отсутствии на рабочем месте сотрудников видимых пользователю подразделений.

   Сразу после авторизации пользователь по умолчанию получает роль "Сотрудник". Позднее его роль могут изменить операторы Parsec, обладающие правом "Администрирование "Parsec Сотрудник". Такое право доступно в ПО ParsecNET 3 начиная с версии 3.14.202.

*AndroidID - уникальный идентификатор устройства, формируемый OS Android.

8.12.5.1 Установка сервера приложения

Сервер приложения "Parsec Сотрудник" устанавливается только на ПК, на котором установлен сервер ParsecNET 3 или ПК, которые имеют надежную связь с этим сервером.

В качестве сервера приложения “Parsec Сотрудник” могут использоваться практически все современные компьютеры, имеющие не менее 4 Гб оперативной памяти. Требуемый объем жесткого диска определяется размерами развёрнутого сервера, размером лог-файла системы, и размером базы данных, содержащих текстовую и ссылочную информацию о зарегистрированных пользователях.

Размер развёрнутого сервера составляет около 120 Мб. Размер лог-файла системы по умолчанию установлен в 10 Мб (значение можно изменить в конфигурационном файле). Размер базы данных в типовой установке со 100 пользователями не превышает 3 Мб.

Сервер приложения “Parsec Сотрудник” работает на современных версиях Windows:

- Windows 7 (рекомендуется не ниже Professional, Service Pack 1); WindowsPower Shell версии 4 или выше;
- Windows 8/8.1; WindowsPower Shell версии 4 или выше;
- Windows 10;
- Windows 11.



Компьютер, на котором устанавливается сервер приложения должен иметь доступ в сеть интернет. Это необходимо для работы сервиса передачи PUSH-уведомлений.

Сервер приложения устанавливается только на 64 разрядные версии ОС.

Минимальная установленная версия ParsecNET к которой может подключаться “Parsec Сотрудник”: PNSoft 3.14.202

Поддерживаемые браузеры для доступа в консоль администратора:

- Google Chrome;
- Mozilla FireFox.



Для корректной работы функционала подачи заявок бюро пропусков в Вашем ключе лицензии СКУД ParsecNET 3 должен быть предусмотрен модуль PNSoft-PO.

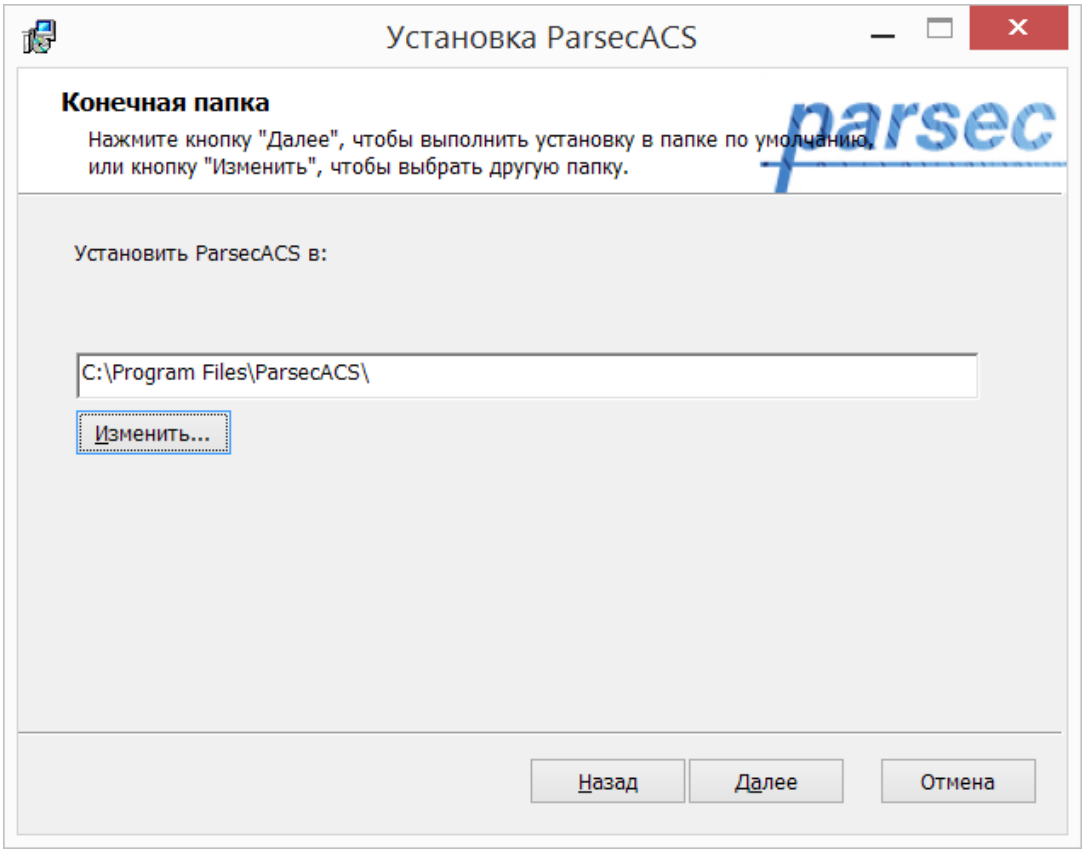


Приложение имеет ограничение в 1000 видимых субъектов СКУД ParsecNET 3.

Чтобы установить сервер приложения Parsec.Сотрудник на локальный ПК, запустите на нем установочный файл parsecACSInstaller.msi.

Следуйте указаниям мастера установки.

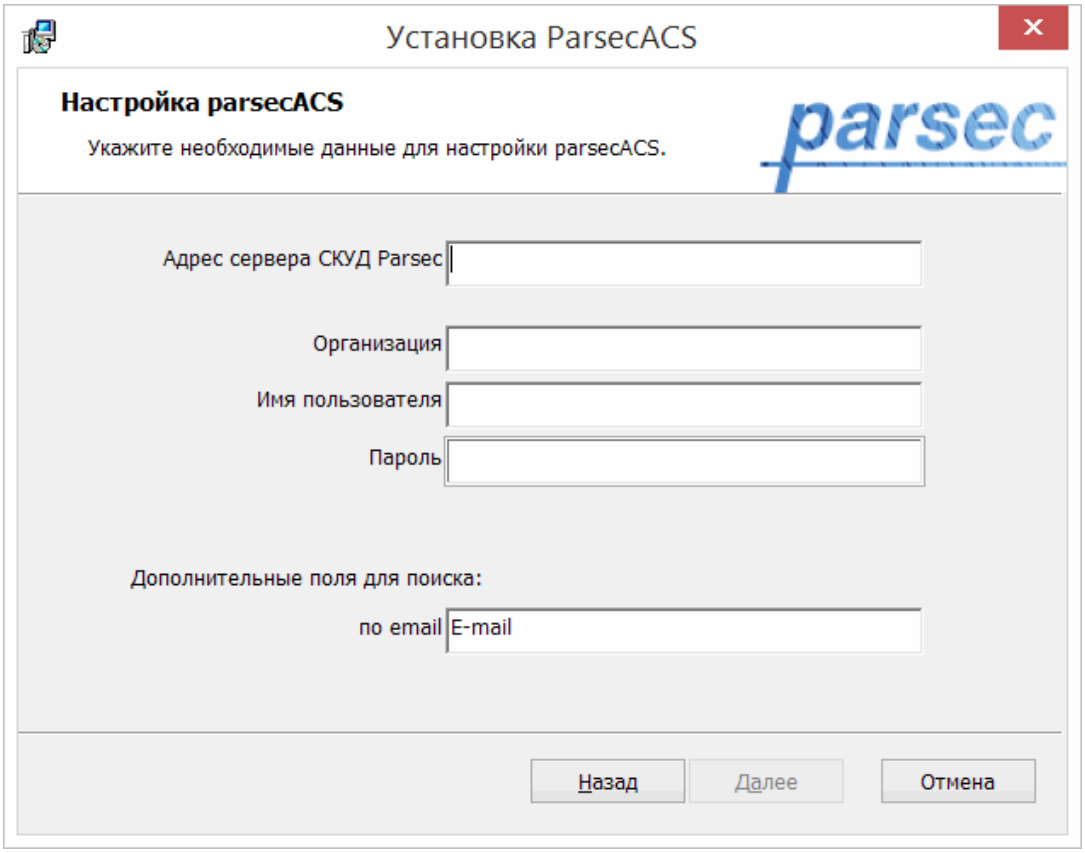
В окне выбора места установки укажите нужную директорию либо оставьте директорию по умолчанию:



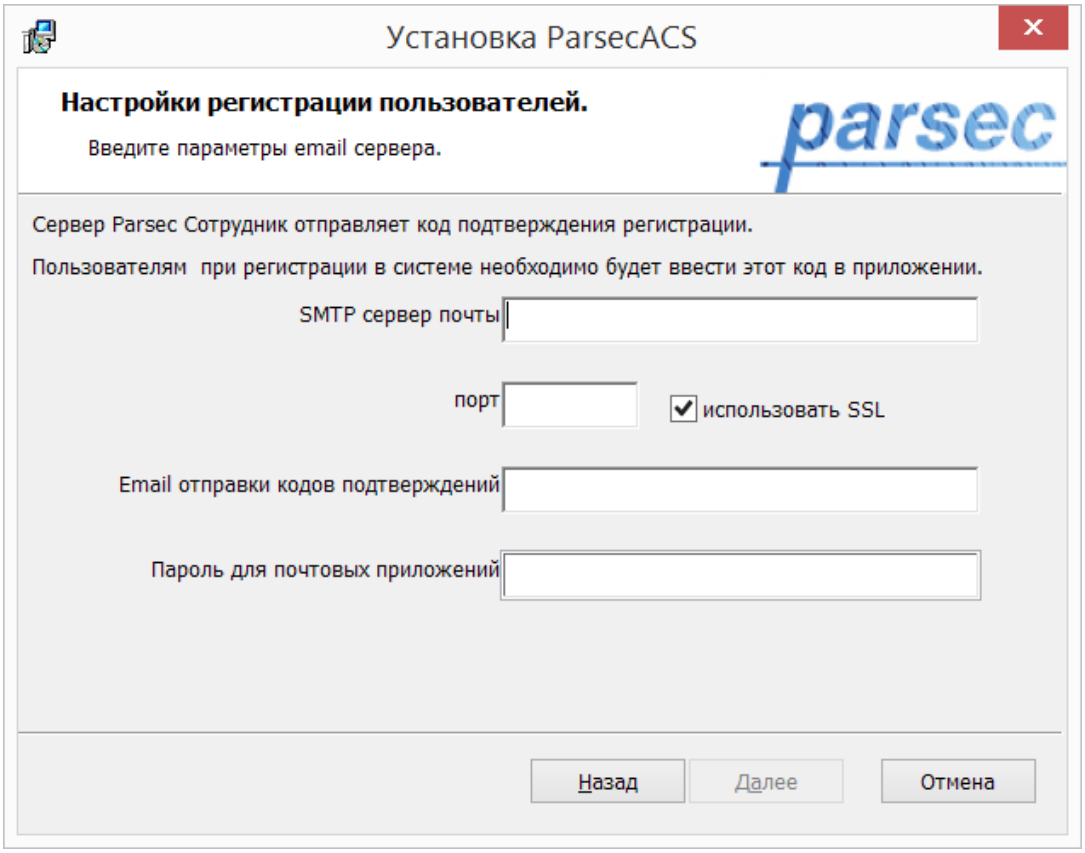
В окне установки данных укажите обязательные данные:

- IP-адрес сервера СКУД ParsecNET 3;
- Логин и пароль оператора для доступа к интеграционному сервису ParsecNET 3. Для корректной работы сервиса оператор должен иметь, как минимум, следующие права:
  - для Редактора персонала - Полный доступ;
  - для Бюро пропусков - Запуск и Подача заявок;
  - для Редактора расписаний - Просмотр;
  - для Монитора событий - Запуск;
  - для Отчетов по событиям - Доступ.

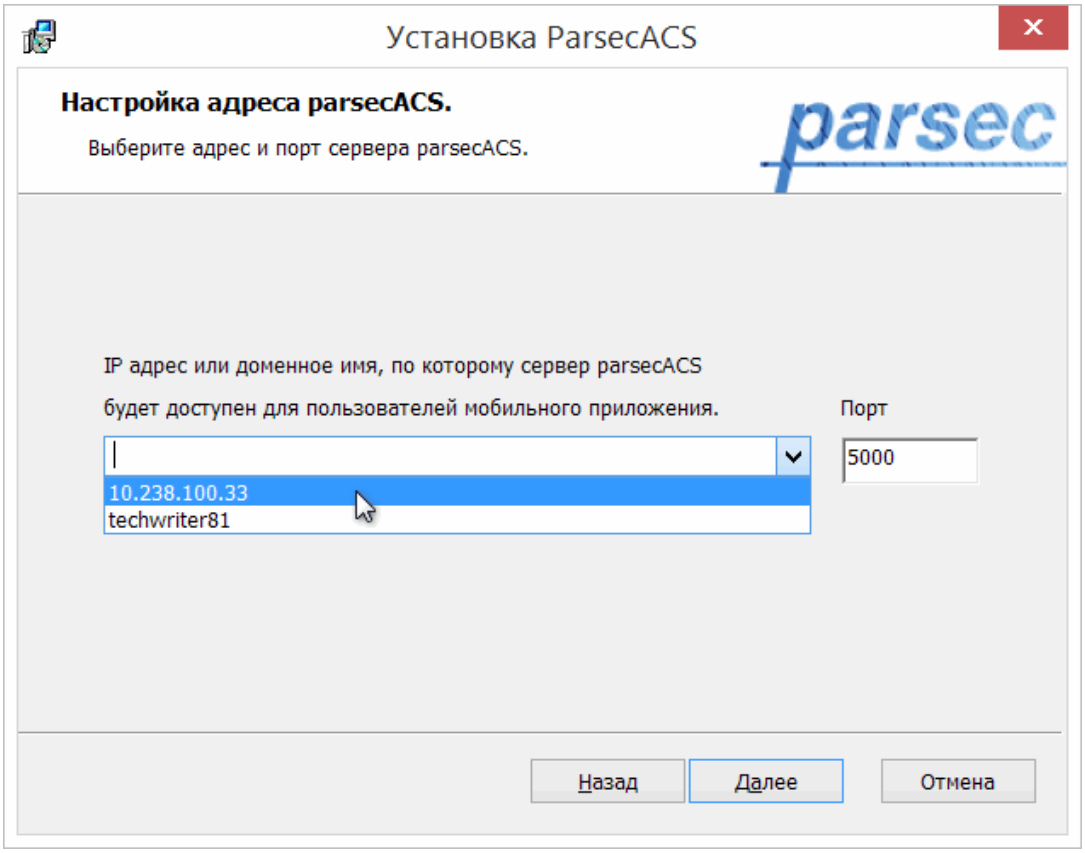
В разделе "Дополнительные поля для поиска" необходимо указать, как в ПО PNSoft названо дополнительное поле[264] для почтовых адресов пользователей. В этом поле сервер приложения будет производить поиск почтового адреса, который пользователь ввел при авторизации в приложении. На эти адреса пользователям будут рассылаться коды подтверждения при регистрации в приложении.



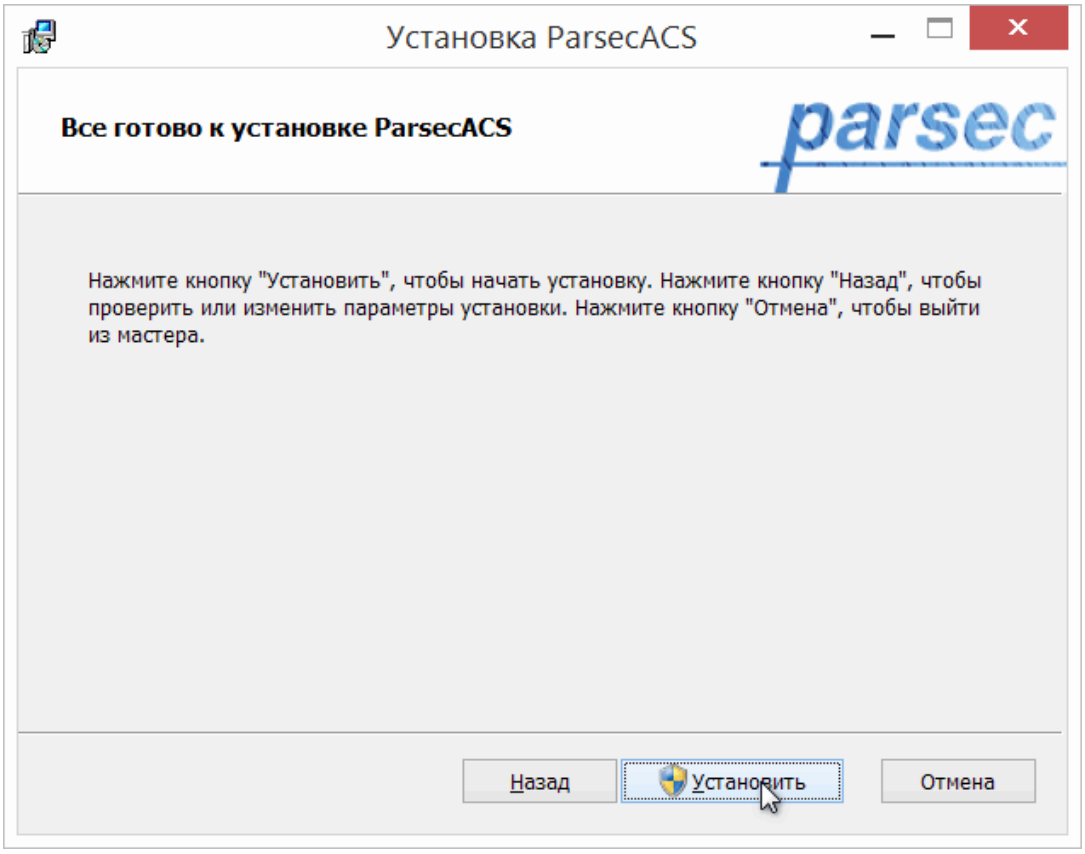
Далее необходимо настроить почтовый сервер, посредством которого пользователям будут рассылаться коды подтверждения регистрации:



В следующем окне из раскрывающегося списка выберите IP-адрес или доменное имя ПК, на который устанавливается сервер приложения "Parsec Сотрудник":



По завершении установки исходных данных нажмите на кнопку Установить. Начнется процедура установки сервера приложения.



После завершения установки можно переходить к [работе](#)[385] с сервером.

8.12.5.2 Настройка сервера приложения

После установки сервера приложения "Parsec Сотрудник" введите в адресной строке браузера IP-адрес того ПК, на котором он был установлен, с указанием заданного по умолчанию порта 5000 (<IP-адрес>:5000). Номер порта можно задать в конфигурационном файле[391] .

QR-код в появившемся окне используется для авторизации в мобильном приложении Parsec.Сотрудник.



Запуск сервера "Parsec Сотрудник" по протоколу HTTPS

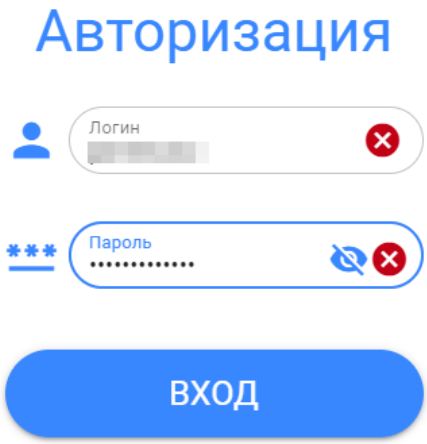
Функционал Системы предоставляет возможность для взаимодействия сервера “Parsec Сотрудник” с приложениями на мобильных устройствах пользователей и с сервером ParsecNET 3 по протоколу HTTPS. Для этого выполните следующие шаги:

1. Получите сертификат на Ваш сайт. (Обратитесь к своему сетевому администратору для помощи в этой процедуре);
2. Поместите файл сертификата в директорию установки приложения “Parsec Сотрудник”: C:\Program Files\ParsecACS;
3. Остановите службу приложения;
4. В файл ParsecACSServerSettings.json внесите следующие изменения:

- в секции "Connection" в поле "SSLCertificateFileName" введите имя файла сертификата. Например, "SSLCertificateFileName": "fullchain1_cert_out.pfx";
- в поле "SSLCertificatePassword" введите пароль сертификата;
- в поле "QR" введите адрес и порт, который работает по HTTPS. Например, https://stt.mdo.ru:5001;
- убедитесь, что в поле "URLs" установлен порт и протокол HTTPS для выбранного порта. Например, "URLs": http://*:5003,https://*:5001;

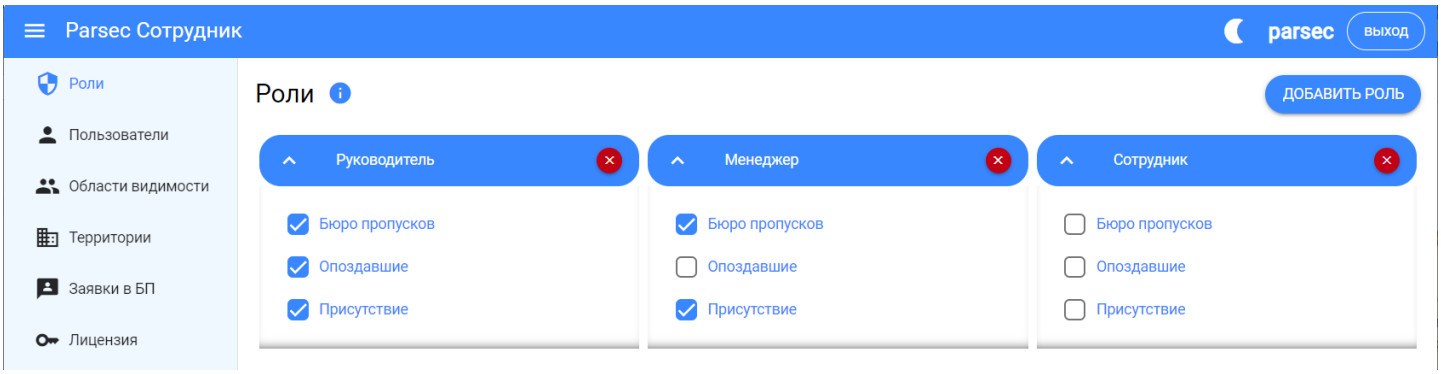
5. Сохраните изменения в файле json;
6. Запустите службу "Parsec Сотрудник";
7. Проверьте, что QR-код на главной странице указывает на новый HTTPS адрес.

При нажатии на ссылку *Администрирование* откроется окно авторизации на сервере. Введите в соответствующие поля логин и пароль оператора, обладающего правом "Администрирование Parsec Сотрудник". Только операторы с вышеуказанным правом имеют доступ к веб-интерфейсу сервера приложения. Операторы с правом "Администрирование "Parsec Сотрудник" всегда имеют полные права на доступ ко всем службам через веб-интерфейс (в мобильном приложении операторы с данным правом могут иметь ограниченный доступ в соответствии с назначенной им ролью, см. ниже).



Если авторизация успешна, откроется доступ к веб-интерфейсу сервера приложения.

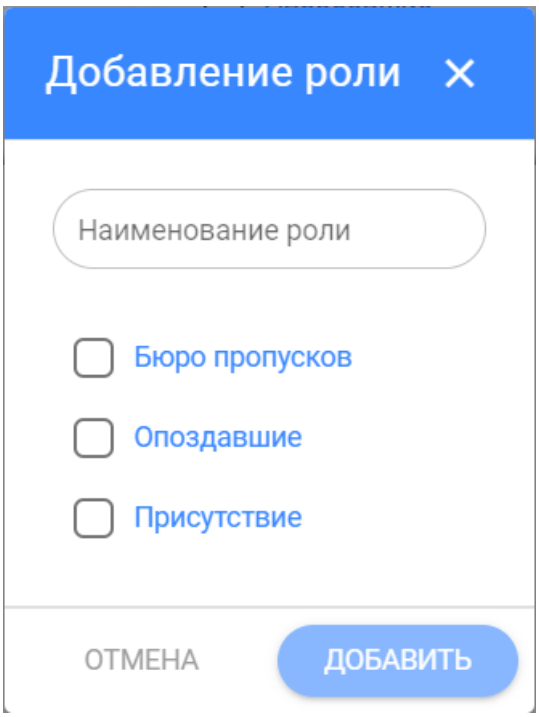
Раздел "Роли"



По умолчанию заданы три роли с доступом к службам, как показано на рисунке выше.

Добавление роли
Чтобы добавить новую роль, нажмите на кнопку *Добавить роль*.

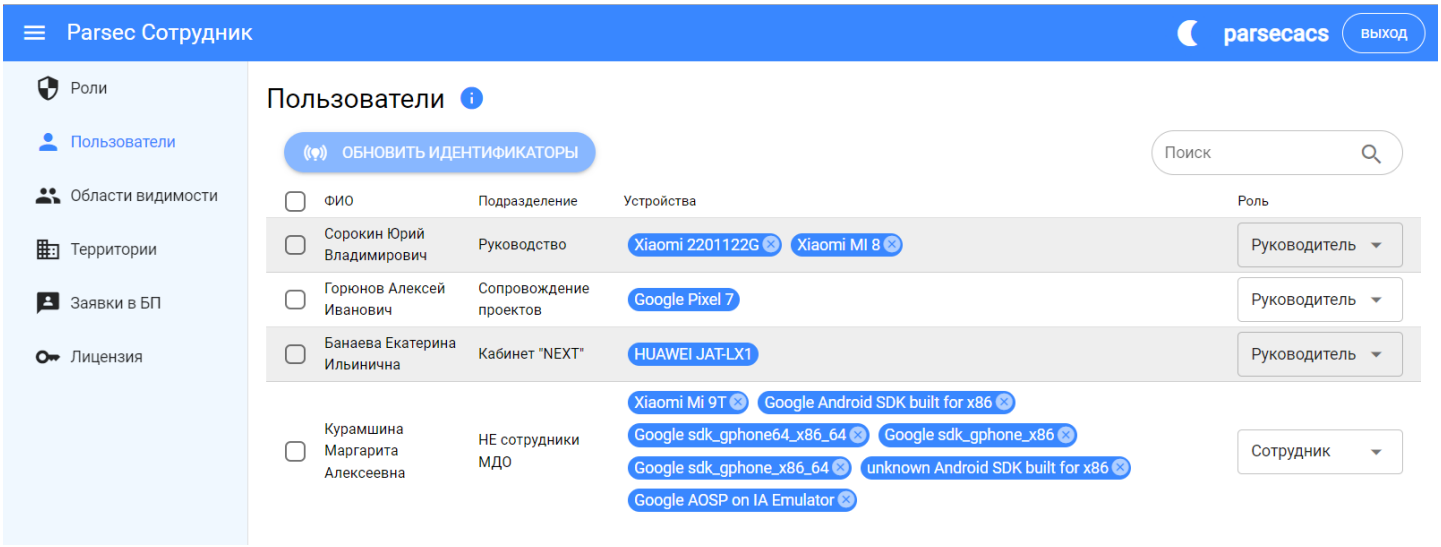
В открывшемся окне введите название роли и установите флажки у тех служб, которые будут доступны пользователям с этой ролью. После чего нажмите на кнопку *Добавить*:



- *Бюро пропусков* - просмотр, создание и удаление заявок Бюро пропусков. Изменение статуса заявки приходит в виде PUSH-уведомлений на мобильное устройство пользователя;
- *Опоздавшие* - получение сведений об опоздавших сотрудниках видимых пользователю подразделений;
- *Присутствие* - получение сведений о присутствии/отсутствии на рабочем месте сотрудников видимых пользователю подразделений.

Раздел "Пользователи"

В этом разделе отображаются только пользователи, авторизовавшиеся на сервере приложения "Parsec Сотрудник".



На этой странице можно выполнить следующие действия:

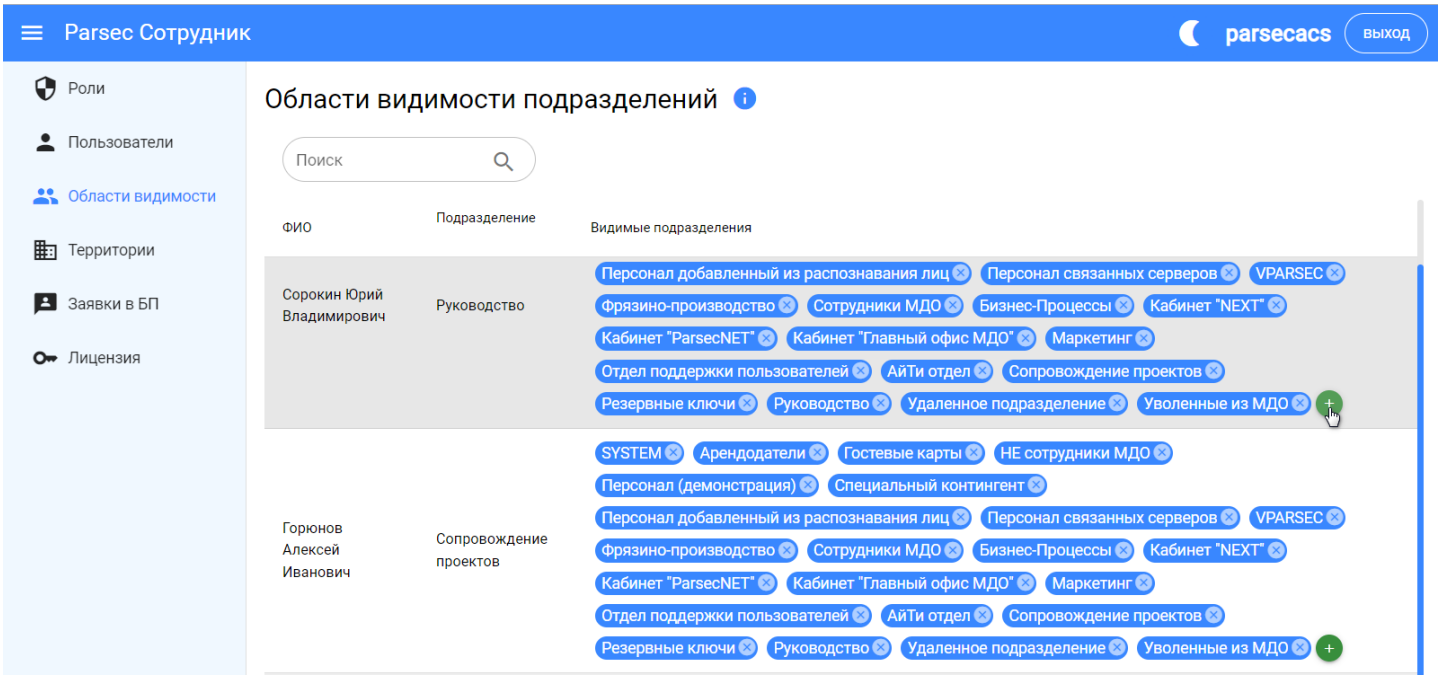
- Обновить идентификатор. Действие требуется в том случае, если идентификатор пользователя был изменен в ПО PNSoft. Для обновления нажмите на кнопку *Обновить идентификатор*, которая станет активной при установке флажка хотя бы у одного сотрудника;
  Кроме того, обновление идентификатора требуется, если в ПО PNSoft сменился ключ шифрования для QR-считывателей. До момента обновления идентификаторов QR-коды на мобильных устройствах пользователей будут недействительны;
- Удалить выбранного сотрудника. Кнопка *Удалить* появляется при установке флажка хотя бы у одного сотрудника;

- Удалить устройство сотрудника. Для этого нажмите на крестик справа от названия устройства. После удаления вход в приложение с данного устройства будет невозможен до повторной авторизации на сервере с этого устройства;
- Назначить роль сотруднику. Справа в строке сотрудника находится раскрывающийся список всех ролей, имеющихся в приложении.

Раздел "Области видимости подразделений"

Функционал раздела позволяет указать для каждого пользователя сотрудников каких подразделений он сможет видеть в своем приложении "Parsec Сотрудник" в разделах "Присутствие" и "Опоздание", а также получать уведомления о фактах входа этих сотрудников на территорию.

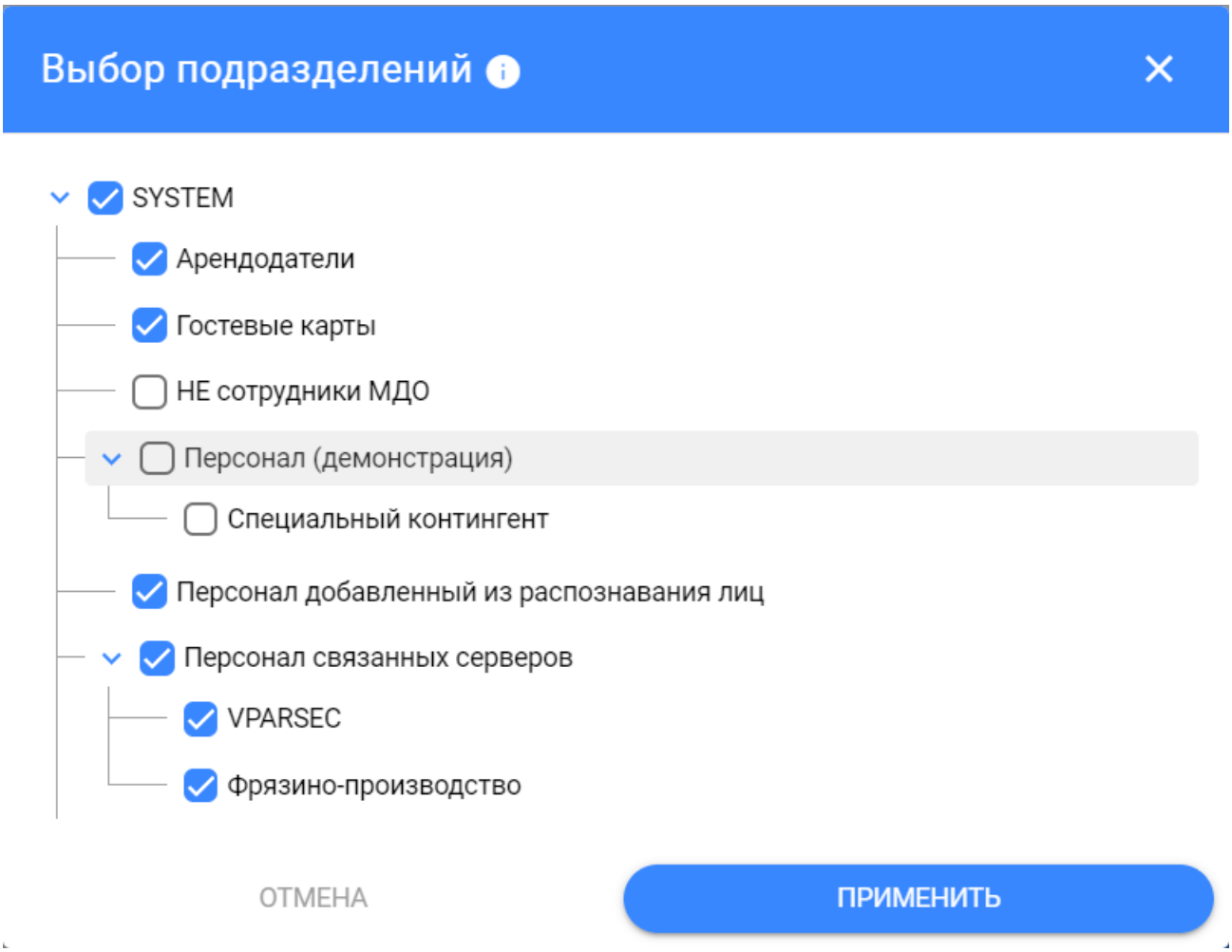
Наименования подразделений наследуются из Редактора организаций в ПО PNSoft.



Чтобы открыть пользователю видимость сотрудников какого-либо подразделения, нажмите на кнопку  в строке пользователя и в открывшемся окне выберите нужные подразделения:

- Чтобы выбрать/исключить один пункт, установите/удалите слева от него флажок;
- Чтобы выбрать/исключить пункт с подпунктами, нажмите на название пункта;
- Чтобы свернуть/развернуть пункт с подпунктами, нажмите на галочку слева от пункта или в области строки вне названия.

После выбора нажмите на кнопку *Применить*:



Чтобы удалить область видимости, нажмите на крестик справа от ее названия.

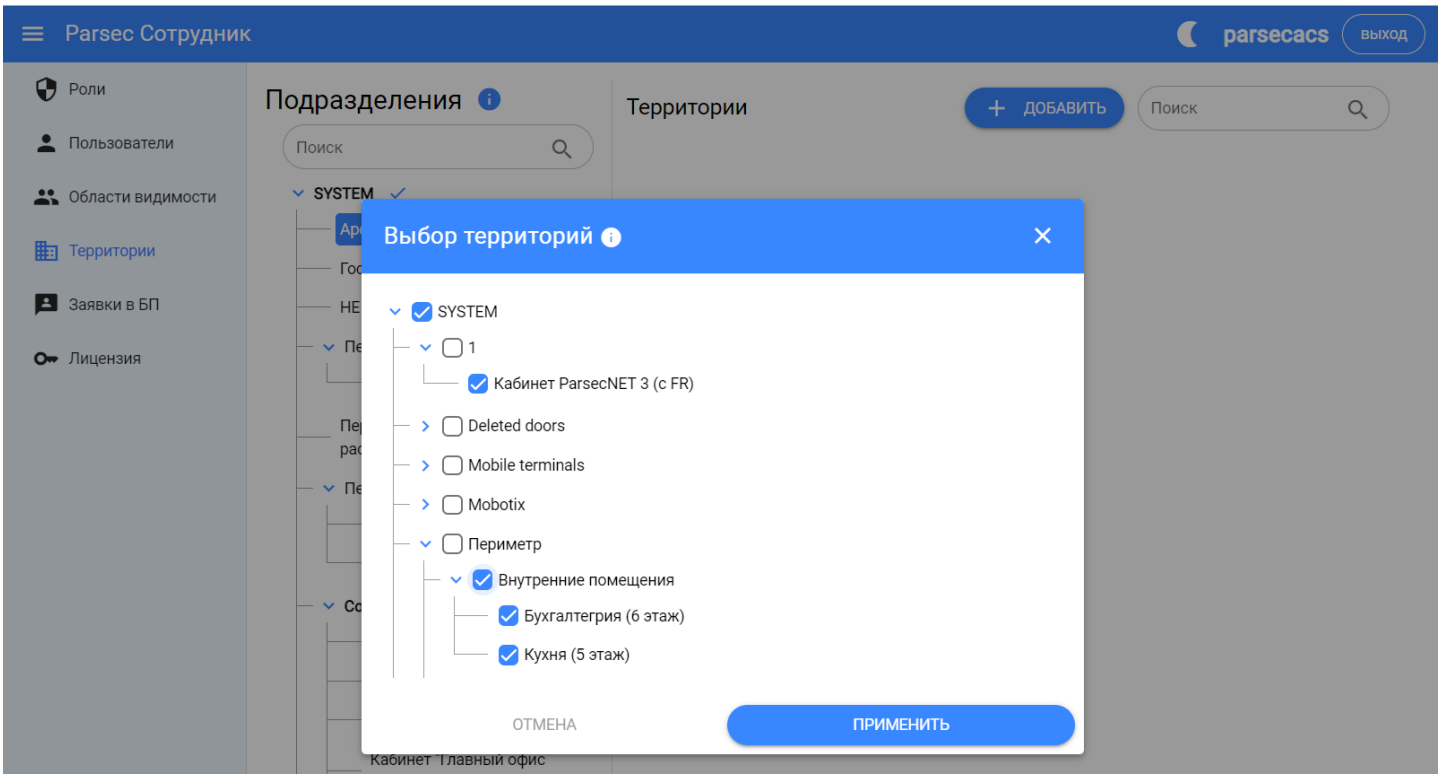
Раздел "Территории"

В этом разделе осуществляется взаимопривязка подразделений и территорий. Например, к подразделению можно привязать те помещения, которые оно занимает. И наоборот, одно помещение можно привязать к нескольким подразделениям, которые его делят.

Такая привязка требуется службе "Присутствие", чтобы определять, вошли ли сотрудники подразделения на территорию или нет. По входу на территорию определяется присутствие сотрудника на рабочем месте, по выходу - отсутствие. При проходе сотрудника на территорию сервер рассылает PUSH-уведомления всем, кто подписался на отслеживание входа этого сотрудника.

Служба "Опоздавшие" использует эту привязку, чтобы определить, прошел сотрудник на свое рабочее место до или после начала обязательного рабочего времени.

Наименования подразделений наследуются из Редактора организаций в ПО PNSoft, наименования территорий - из Редактора топологии.



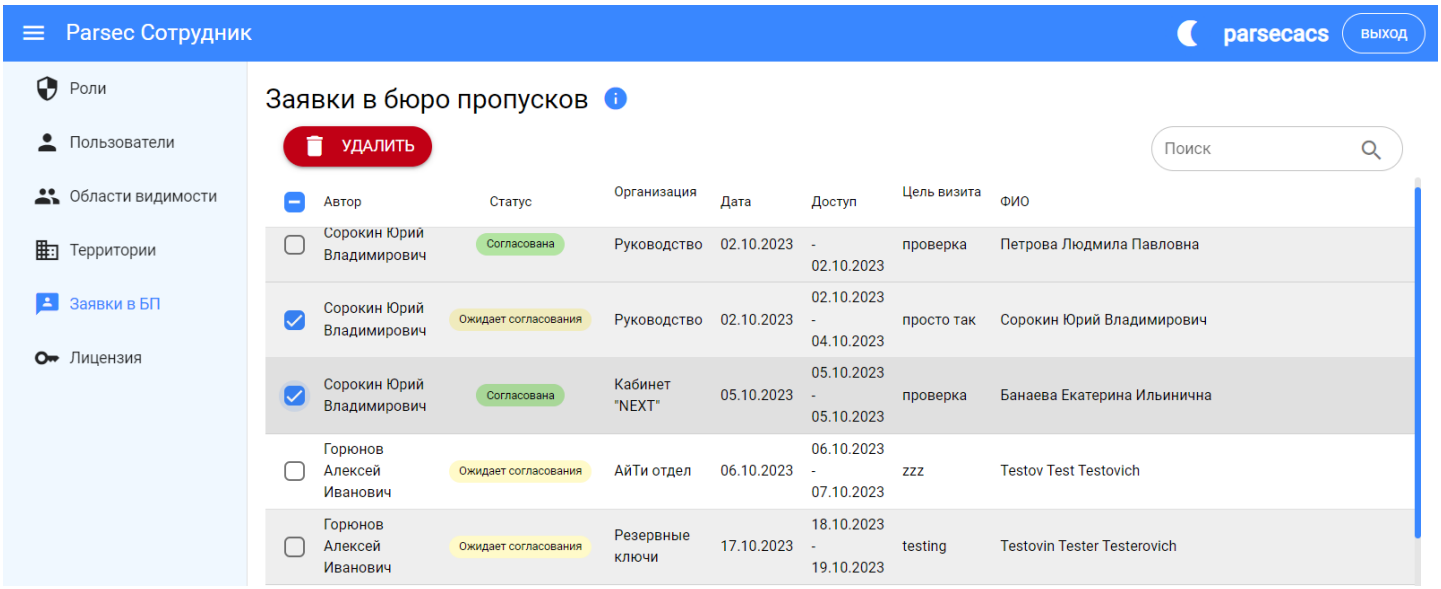
Чтобы привязать территорию к подразделению, выполните шаги:

- Выделите подразделение на панели *Подразделения* слева;
- Нажмите на кнопку *Добавить* на панели *Территории* справа;
- В открывшемся окне выберите нужную территорию(-ии):
  - Чтобы выбрать/исключить один пункт, установите/удалите слева от него флажок;
  - Чтобы выбрать/исключить пункт с подпунктами, нажмите на название пункта;
  - Чтобы свернуть/развернуть пункт с подпунктами, нажмите на галочку слева от пункта или в области строки вне названия.
- Нажмите на кнопку *Применить*.

Если подразделению не выбрана территория, то оно по умолчанию унаследует территории подразделения выше по иерархии. Это правило действует для всех уровней иерархии. Например: если имеются подразделения от 0 до 5 уровня иерархии, но территория назначена только подразделению 0 уровня (на изображении выше – это «SYSTEM»), то все подразделения унаследуют его территории. Если у какого-либо подразделения будут назначены свои территории, то правило наследования для них действовать не будет

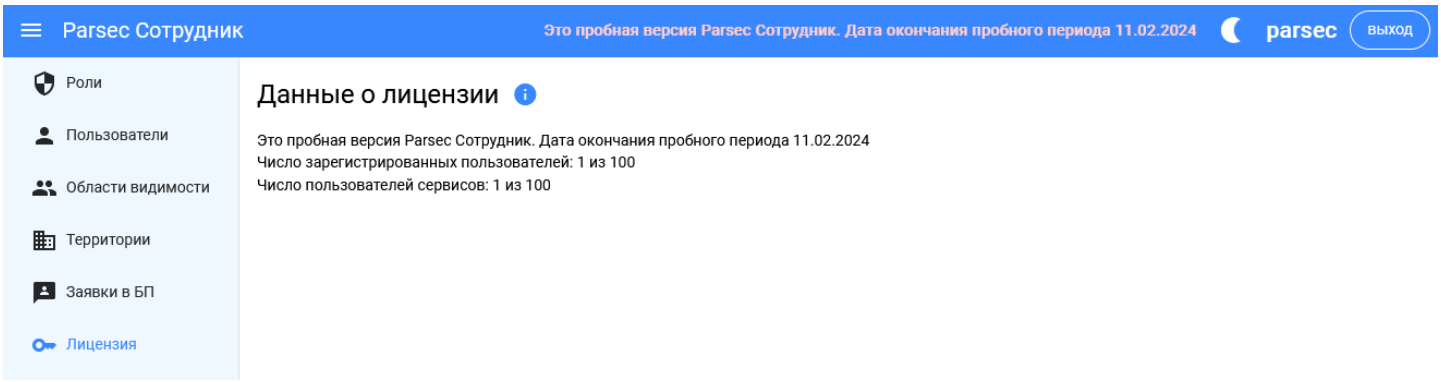
Раздел "Заявки в Бюро пропусков"

В разделе "Заявки в Бюро пропусков" оператор может просматривать статус заявок и удалять их. Удаление заявки на сервере приложения приведет к удалению заявки и в ПО PNSoft.



Раздел "Лицензия"

В разделе "Лицензия" отображаются данные о пробной версии приложения или приобретенной лицензии.



8.12.5.3 Конфигурационный файл

По умолчанию конфигурационный файл ParsecACSServerSettings.json находится в папке C:\Program Files\ParsecACS.

Редактируемые параметры и их значения по умолчанию приведены в таблице ниже.

Секция	Параметр	Тип	Описание	Значение по умолчанию	Примечание
Log	Name	Строка	Путь к файлу протокола (лога)	Log.txt	Будет создан в текущей папке
	MaxSize	Целое	Максимальный размер протокола (лога), по достижение которого происходит его переименование	104857600	100МБ

			(LogName_yyyy.MM.dd_HH.mm.ss.LogExt) и создание нового.		
	Error	Булево	Выводить в файл протокола ошибки	true	
	Warning	Булево	Выводить в файл протокола предупреждения	true	
	Debug	Булево	Выводить в файл протокола отладочную информацию	false	
	Info	Булево	Выводить в файл протокола информационные сообщения	false	
Connection	URLs	Строка	Протоколы и соответствующие им порты	http://*:5000, https://*:5001	Перечисляются через запятую.
	SSLCertificateFileName	Строка	Путь к SSL сертификату для HTTPS		
	SSLCertificatePassword	Строка	Пароль к SSL сертификату для HTTPS		
	UseHttpsRedirection	Булево	Перенаправлять с HTTP адреса на HTTPS	true	
	QR	Строка	Адрес в QR коде на первой странице мобильного приложения. Если не указан в конфиг.файле, то используется адрес для входа на сервер приложения	Первый адрес из URLs	
Database	FileName	Строка	Путь к файлу базы данных	database.db	Если базы нет, она будет создана
Parsec	Address	Строка	Адрес интеграционного сервиса PARSEC	http://localhost:10101/IntegrationService/IntegrationService.asmx	Заполняется в процессе установки
	Domain	Строка	Организация		Заполняется в процессе установки
	Login	Строка	Логин оператора для доступа к интеграционному сервису	parsec	Заполняется в процессе установки
	Password	Строка	Пароль оператора для доступа к интеграционному сервису	parsec	Заполняется в процессе установки

	EmailField	Строка	Поле для E-mail	Электронный адрес	Заполняется в процессе установки
	EventPollingInterval	Целое	Интервал опроса событий (изменение статуса заявок в бюро пропусков, присутствие, опоздавшие)	10000	В миллисекундах
Registration	Timeout	Целое	Таймаут ожидания ввода кода подтверждения при регистрации	120000	В миллисекундах
Email	ServerAddress	Строка	Адрес SMTP сервера рассылки кодов регистрации через электронную почту		Заполняется в процессе установки
	ServerPort	Целое	Порт SMTP сервера рассылки кодов регистрации через электронную почту	465	Заполняется в процессе установки
	UseSSL	Булево	Использовать безопасное соединение	true	
	SenderAddress	Строка	Адрес ящика отправителя		Заполняется в процессе установки
	SenderName	Строка	Имя отправителя	"Parsec Сотрудник"	
	SenderPassword	Строка	Пароль ящика отправителя		
	MessageTitle	Строка	Заголовок письма	Регистрация	
	MessageBody	Строка	Содержимое письма	Для подтверждения регистрации введите:	
	Timeout	Целое	Таймаут ожидания отправки письма	10000	В миллисекундах
Events	Entrance	Строка	Коды событий входа	590280,590266,590295,590262	Перечисляются через запятую.
	Exit	Строка	Коды событий выхода	590281,590267,590296,590263	Перечисляются через запятую.

8.12.6 Telegram бот

Для взаимодействия ПО ParsecNET 3 с приложением по обмену сообщениями (мессенджером) Telegram рекомендуется создать двух ботов, предназначенных для:

- отправки текстовых сообщений[408] о событиях на телефонный номер пользователя;

- отправки посетителям идентификаторов доступа в виде QR-кода[454]. Данный бот будет работать с заявками Бюро пропусков.

Для создания бота любого предназначения из перечисленных выше, необходимо выполнить следующие шаги:

1. Установите Telegram и зарегистрируйтесь в нем;
2. Перейдите в раздел Contacts и в строке поиска наберите @BotFather - это автоматический бот Telegram, позволяющий создать свои собственные боты;
3. Начните чат с @BotFather и на первой страничке чата нажмите на кнопку *Start* (или напишите боту команду /start). В ответ на это бот выведет список доступных команд;
4. Напишите команду /newbot. @BotFather попросит ввести имя, а потом имя пользователя для Вашего нового бота. В последнем случае оно должно оканчиваться на «bot» (возможно, над именем придется поломать голову). В случае успеха @BotFather возвращает токен бота;
5. В сообщении с токеном бота нажмите на ссылку с именем Вашего бота. Откроется чат с созданным ботом. Нажмите на кнопку *Start* или напишите команду /start.

Если Вы создавали бот для отправки QR-кодов, то на этом этапе создание бота завершено. Далее необходимо настроить ПО ParsecNET 3[454].

Если создавался бот для отправки текстовых сообщений, то дополнительно выполните следующие шаги:

1. Создайте группу отправки текстовых сообщений, например, с именем ParsecEvents. В группу, кроме созданного бота, должны входить те пользователи, кто будет получать уведомления о событиях;
2. В чате с @BotFather напишите команду /token. Внизу экрана выберите созданного бота и нажмите на него;
3. В этом же чате с @BotFather напишите команду /start и в списке выберите /setinline, либо напишите сразу команду /setinline. Внизу экрана нажмите на созданного бота;
4. Перейдите в созданный чат (в нашем примере это ParsecEvents) и также напишите команду /setinline.

На этом создание бота завершено и можно переходить к созданию задания[408].

9. Текстовые сообщения

Общие положения

Сообщения можно отправлять не только в Мини-консоль, также есть возможность отправки SMS и электронной почты. Далее мы рассмотрим все три варианта текстовых сообщений более подробно.

Перед созданием заданий по отправке сообщений в виде SMS или письма на e-mail адрес необходимо создать дополнительные устройства - GSM модем и E-mail клиент на канале PROGRAM. Их создание описано в разделах, посвященных отправке соответствующих сообщений:

Мини-консоль[395]

Настройка уведомлений[396]

Отправка SMS через GSM-модем[398]

Отправка SMS через интернет-портал[402]

Отправка сообщения в Telegram[408]

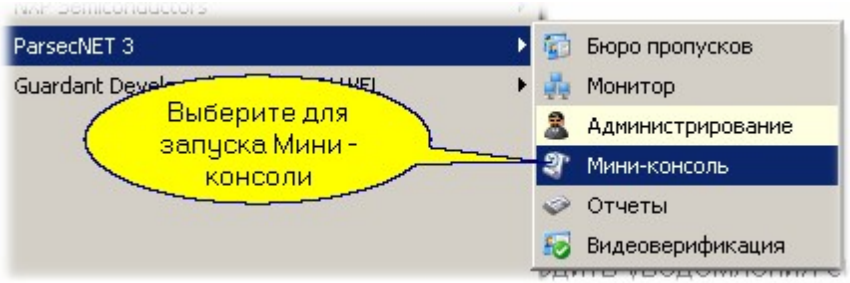
Отправка e-mail[409]

Печать уведомлений[411]

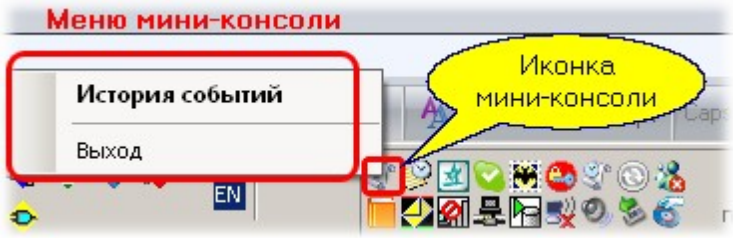
9.1 Мини-консоль

Мини-консоль является отдельным приложением системы и позволяет выдавать уведомления работающему за ПК пользователю при наступлении запрограммированных событий. по-умолчанию после установки системы Мини-консоль запускается автоматически при старте Windows.

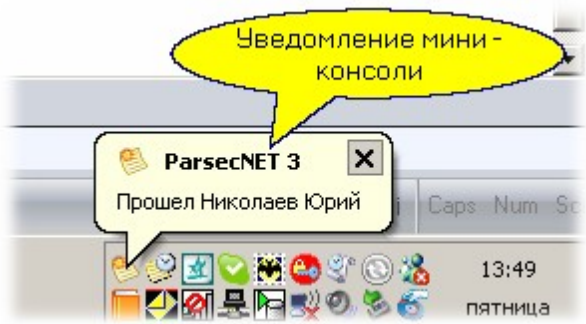
Если вы закрыли Мини-консоль, то ее можно перезапустить из папки с установленными компонентами системы:



При запущенной Мини-консоли в панели задач Windows вы сможете видеть ее значок, имеющий свое собственное контекстное меню:

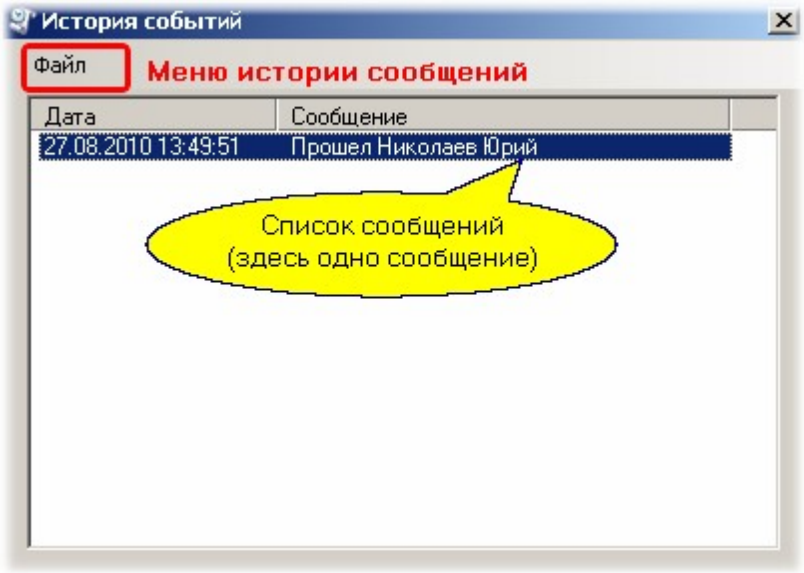


Мини-консоль позволяет выводить уведомления системы, порождаемые Менеджером заданий[321] системы. Уведомления представляют собой всплывающее текстовое сообщение с возможностью параллельного воспроизведения заданного звукового файла. Пример сообщения Мини-консоли показан на рисунке ниже:



Уведомления, как уже упоминалось, создаются с помощью Редактора заданий[321] системы. Всплывающее сообщение можно закрыть вручную, в противном случае оно закроется автоматически по истечении нескольких секунд.

Выбрав из меню Мини-консоли опцию "История событий" вы можете посмотреть список происходивших событий в диалоговом окне следующего вида:



С помощью меню *Файл* окна истории событий можно очистить все сообщения, а также сохранить их в назначенный пользователем текстовый файл.

Поскольку настройка текстовых уведомлений делается однотипно для всех устройств (Мини-консоль, GSM - модем, e-mail), данная процедура описана в отдельном разделе.[396]

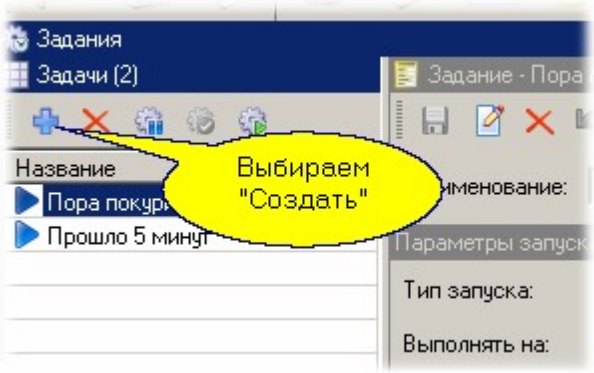
См. также:

- Настройка уведомлений[396]
- Отправка SMS через GSM-модем[398]
- Отправка SMS через интернет-портал[402]
- Отправка сообщения в Telegram[408]
- Отправка e-mail[409]
- Печать уведомлений[411]

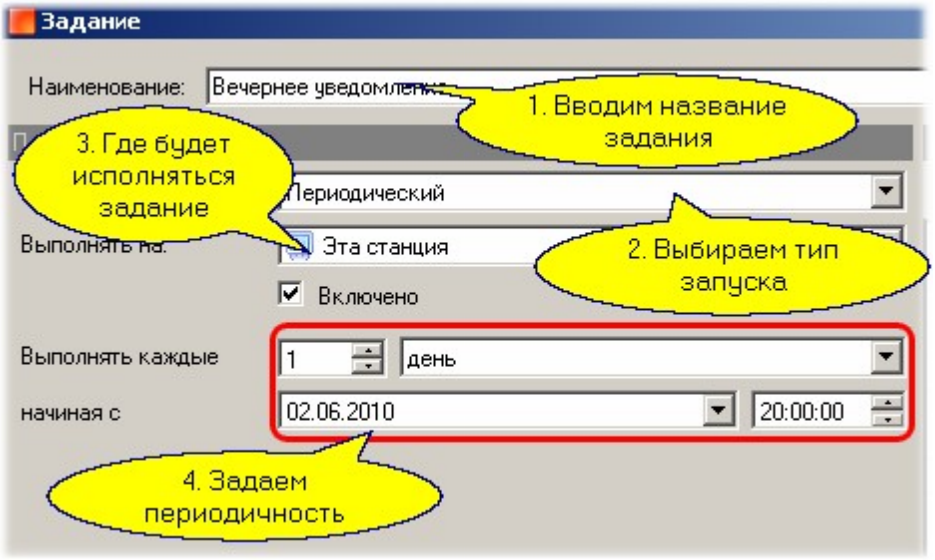
9.2 Настройка уведомлений

Текстовые уведомления о наступлении того или иного события могут быть отправлены в Мини-консоль, в виде SMS[398] через GSM-модем, либо по электронной почте[409] (e-mail), либо распечатаны[411] на построчном принтере. Настройку уведомлений рассмотри на примере создания сообщения для Мини-консоли. Делается это в редакторе заданий системы.

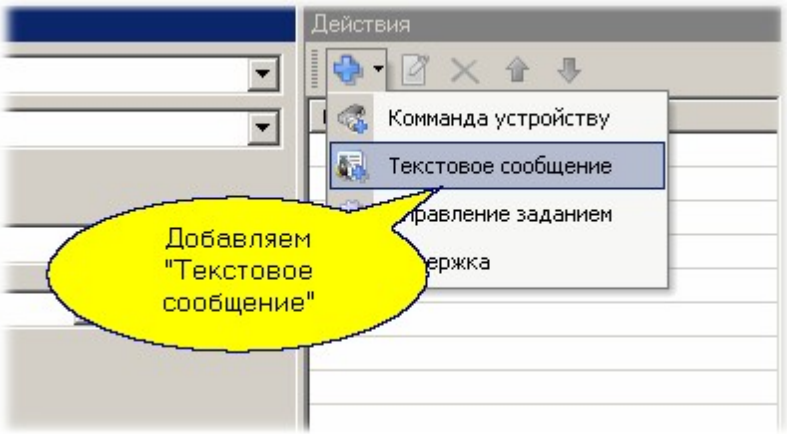
- Необходимо в редакторе выбрать "Создать"



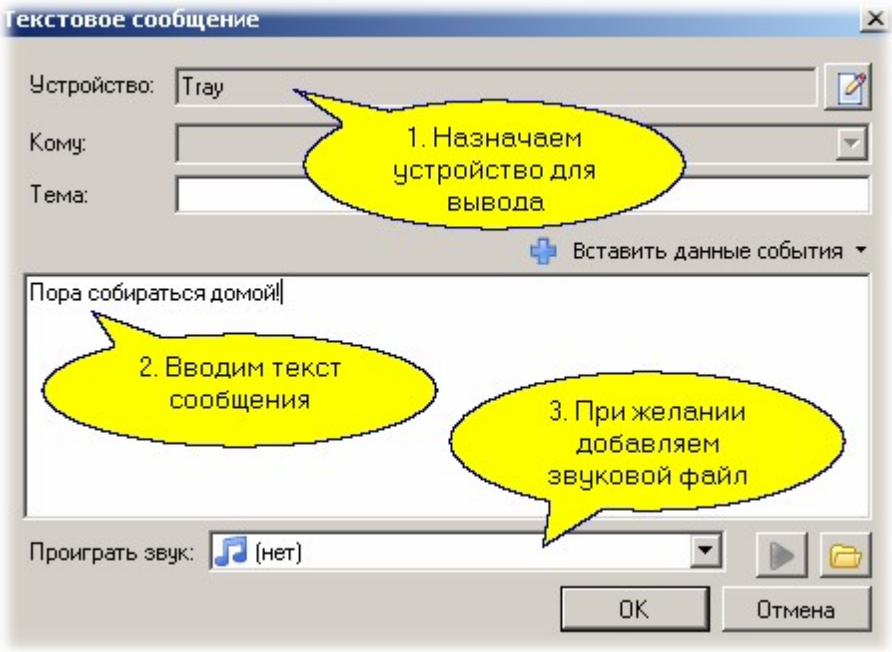
- и в открывшемся диалоге создать новое задание. Для примера создадим периодическое (выполняемое по времени) задание:



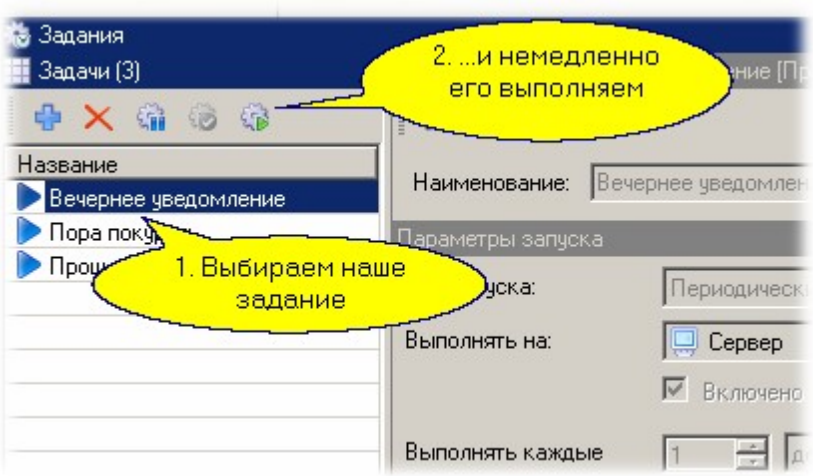
- теперь в правой части диалога добавим действие для задания:



- далее описываем действие:



После закрытия диалогов нажатием на кнопку *OK* наше задание готово. Теперь его можно проверить прямо из редактора заданий:



См. также:

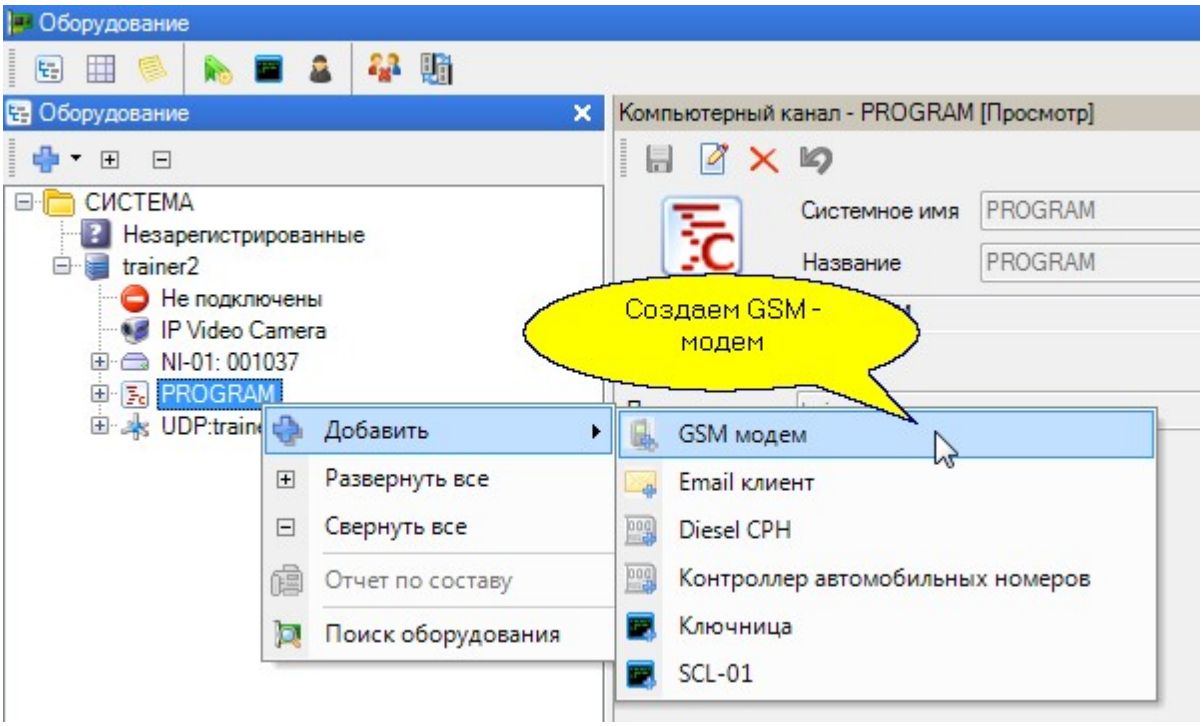
- Мини-консоль[395]
- Отправка SMS через GSM-модем[398]
- Отправка SMS через интернет-портал[402]
- Отправка сообщения в Telegram[408]
- Отправка e-mail[409]
- Печать уведомлений[411]

9.3 Отправка SMS через GSM-модем

При возникновении тревоги в заданной области, которую обслуживает контроллер доступа с функциями охраны, Система может отправить SMS-сообщение на заданный телефонный номер посредством GSM-модема или при помощи интернет-портала www.smsc.ru[402]

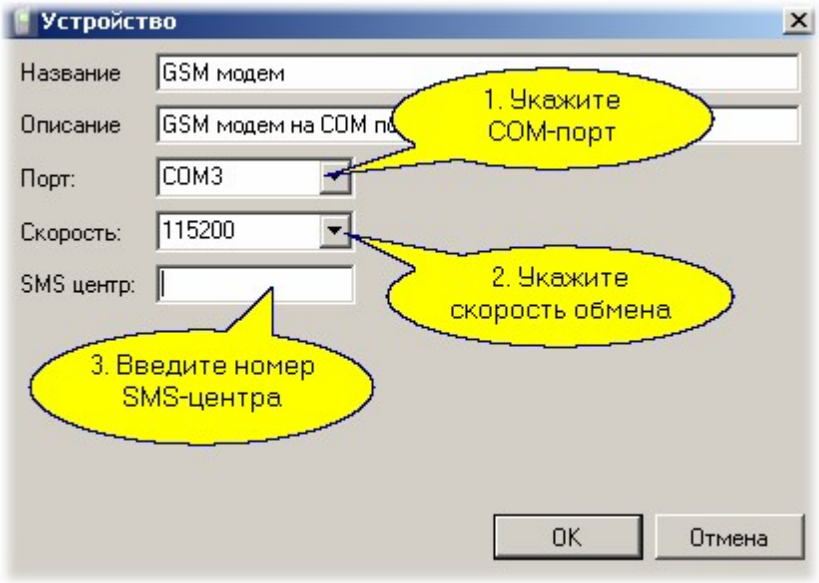
В этом разделе описаны действия по отправке SMS посредством модема.

Сначала необходимо на канале PROGRAM создать GSM модем. Делается это из контекстного меню (по правой кнопке мышки) при выборе канала PROGRAM, как показано на рисунке ниже:



Для отправки SMS-сообщений вам потребуется стандартный GSM-модем, подключаемый к COM-порту ПК (либо представляемый в Windows как виртуальный COM-порт). В качестве примера можно рекомендовать, например, внешние USB-модемы российского производства "Teleofis RX101" или аналогичные.

Для каждого устройства необходимо указать соответствующие ему параметры. Так, для GSM модема при его создании необходимо указать следующие параметры:



Для большинства модемов по-умолчанию используется скорость обмена 115200 бод. Для уточнения обратитесь к руководству пользователя своего модема.

Номер SMS-центра - это телефонный номер оператора связи, по которому отправляются SMS-сообщения. Его можно уточнить у оператора связи, чью SIM-карту вы будете использовать в модеме. Это номер достаточно ввести в модем один раз, и в дальнейшем он будет использоваться автоматически. Если номер уже записан в SIM-карту, соответствующее поле можно не заполнять.

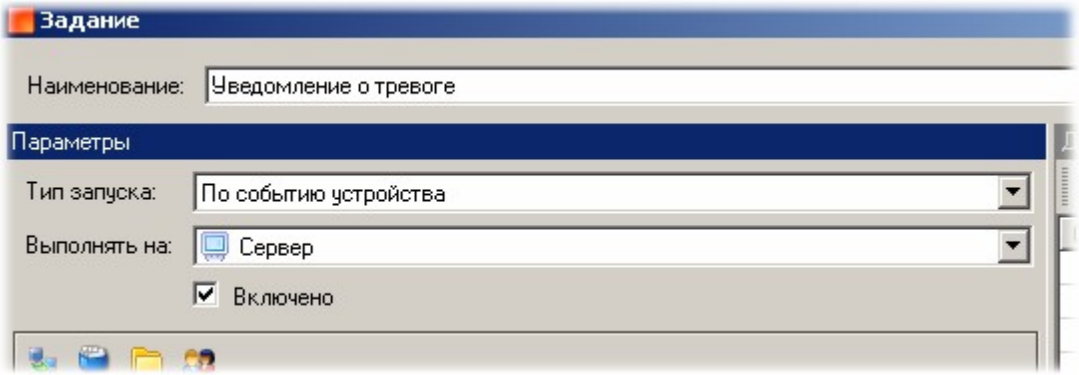
Перед использованием SIM-карты в модеме обнулите PIN-код, так как система при инициализации модема не может передать его модему.

После ввода всех требуемых параметров нажмите на кнопку *ОК* и в канале появится созданный GSM-модем.

Теперь создадим задачу в Менеджере заданий:

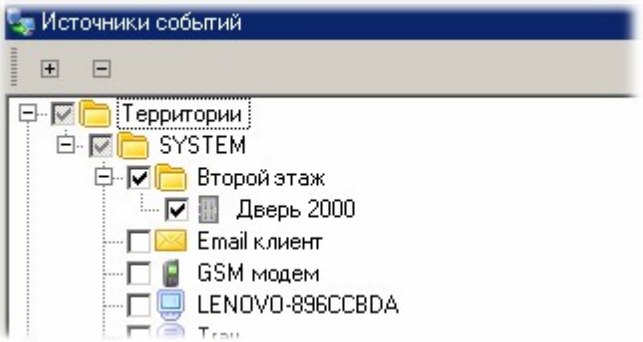
Шаг 1.

Создадим новое задание с именем "Уведомление о тревоге", тип запуска - по событию с устройства, исполнять на сервере системы:



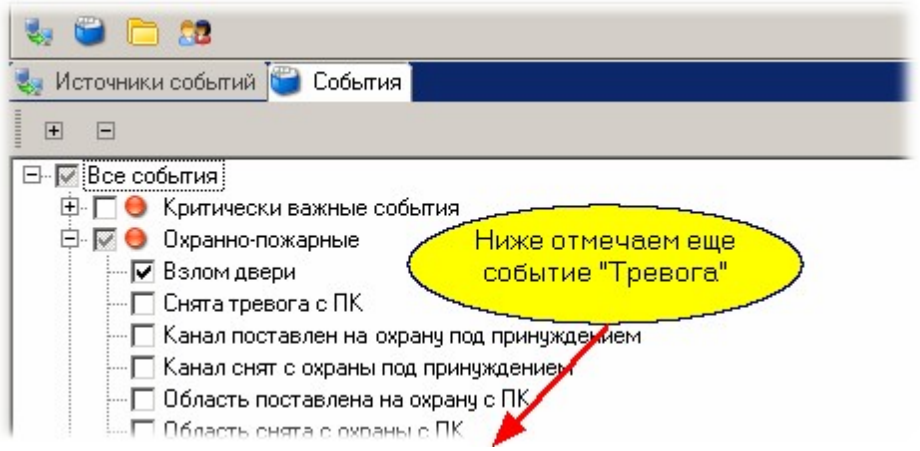
Шаг 2.

Определим территорию (устройство), события с которого нас будут интересовать:



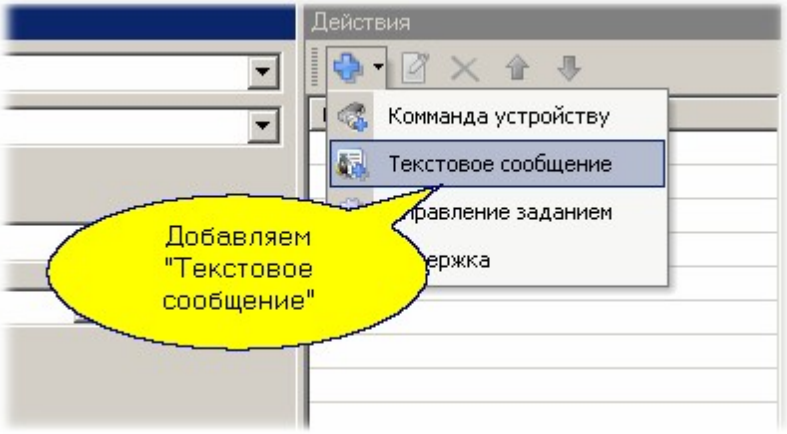
Шаг 3.

Определим, какие именно события нас будут интересовать. Если на контроллере задействован охранный датчик, то тревоги на охране будут порождать события "Взлом двери", "Тревога". Если используется шлейф с контролем четырех состояний, то тревогами можно также считать события "Обрыв охранного датчика" и "КЗ цепи охранного датчика".

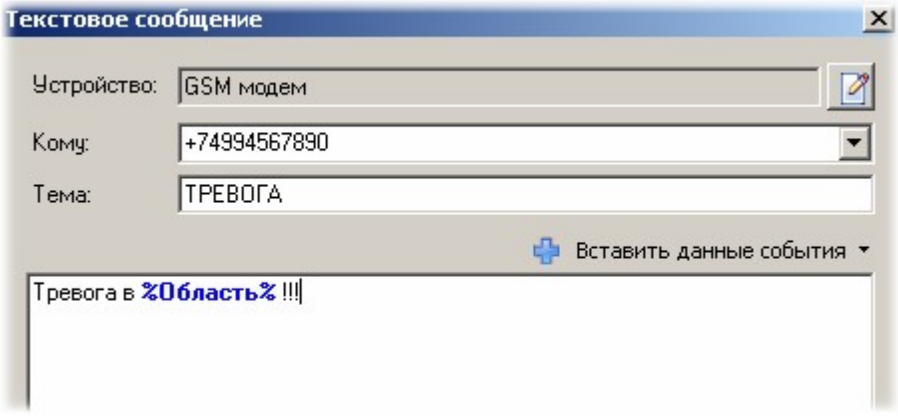


Шаг 4.

Переходим к формированию сообщения, для чего в правой панели диалога выбираем "Добавить" - "Текстовое сообщение":

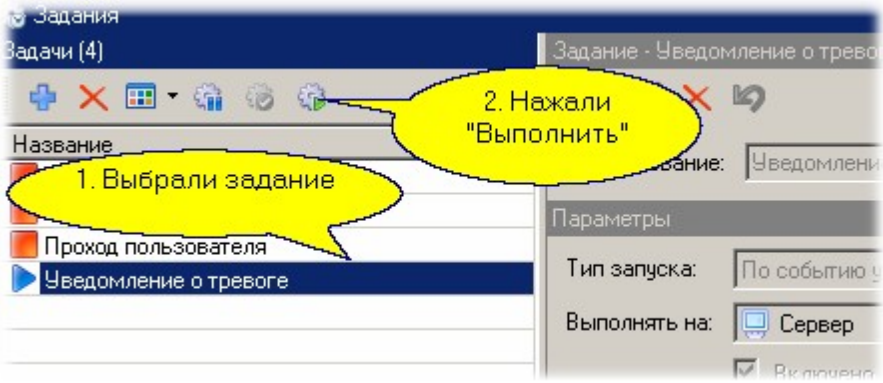


и в открывшемся диалоге выбираем GSM-модем, вводим номер телефона и текст сообщения:



Помимо ввода номера телефона можно выбрать предварительно созданное системное дополнительное поле[155], в котором у каждого сотрудника в карточке стоит свой номер телефона.

После нажатия "ОК" задание готово. Его можно его протестировать, запустив вручную с левой панели редактора заданий:



См. также:

- Мини-консоль[395]
- Настройка уведомлений[396]
- Отправка SMS через интернет-портал[402]
- Отправка сообщения в Telegram[408]
- Отправка e-mail[409]
- Печать уведомлений[411]

9.4 Отправка SMS через интернет-портал

Система может отправлять SMS-сообщения на заданный телефонный номер посредством GSM-модема[398] или при помощи интернет-портала www.smsc.ru при наступлении запрограммированных в задании событий, например, при возникновении тревоги.

В этом разделе описаны действия по отправке SMS посредством интернет-портала. SMS можно отправить на номера телефонов, заданные в настройках, а можно отправлять на номер телефона, указанный в дополнительном поле карточки субъекта доступа, который инициализировал событие.

Чтобы пользоваться данным функционалом Системы, требуется зарегистрироваться на портале smsc.ru.

Для настроек необходимо знать имя пользователя (логин) и пароль для входа в учетную запись портала.

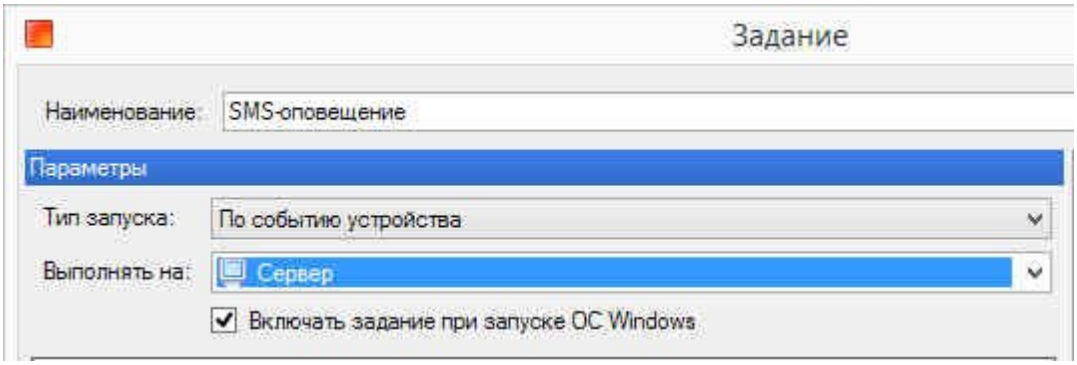
Отправка сообщения на телефоны, указанные в настройках

Такую функцию можно использовать, например, для информировании о возникновении тревожных событий.

В Менеджере заданий выполните следующие действия:

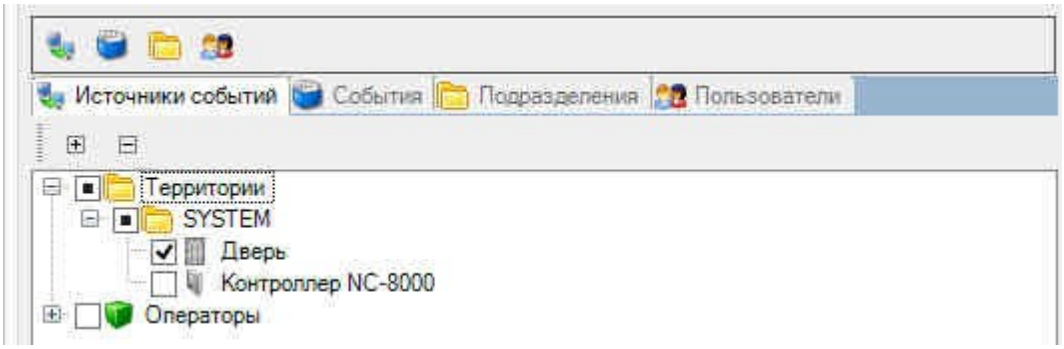
Шаг 1.

Создайте новое задание и задайте ему имя, например, "SMS-оповещение", тип запуска - по событию с устройства, исполнять на сервере системы:



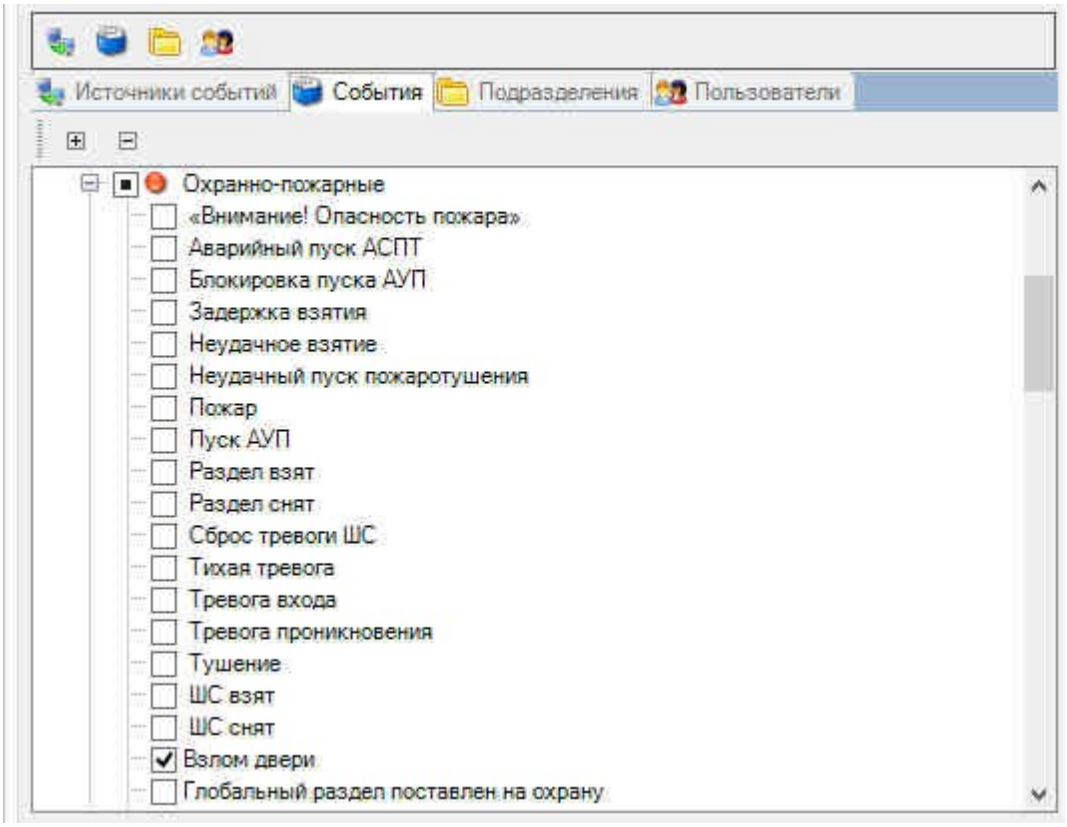
Шаг 2.

Определите территорию (устройство), события с которого будут вас интересовать:



Шаг 3.

Определите, какие именно события вас будут интересовать. Если на контроллере задействован охранный датчик, то тревоги на охране будут порождать события "Взлом двери", "Тревога". Если используется шлейф с контролем четырех состояний, то тревогами можно также считать события "Обрыв охранного датчика" и "КЗ цепи охранного датчика".



Флажки на вкладках *Подразделения* и *Пользователи* нужно снять, чтобы не вводить дополнительных ограничений на отправку сообщения.

Шаг 4.

В текст скрипта необходимо вставить логин и пароль для входа на портал.

по-умолчанию, при установке ПО ParsecNET 3 скрипты помещаются в директорию *C:\Program Files\MDO\ParsecNET 3\Scripts*. Перейдите в эту папку, откройте скрипт SmsNotify и найдите следующие строки:

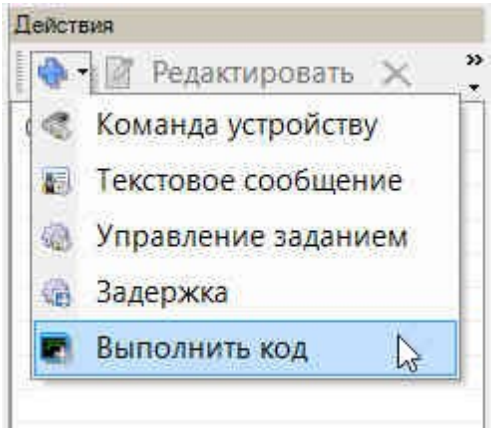
```
// Константы с параметрами отправки
        const string SMSC_LOGIN = "login";          // логин клиента
        const string SMSC_PASSWORD = "pass";        // пароль или MD5-хеш пароля в нижнем регистре
```

Вместо выделенных красным слов введите логин и пароль для входа на портал.

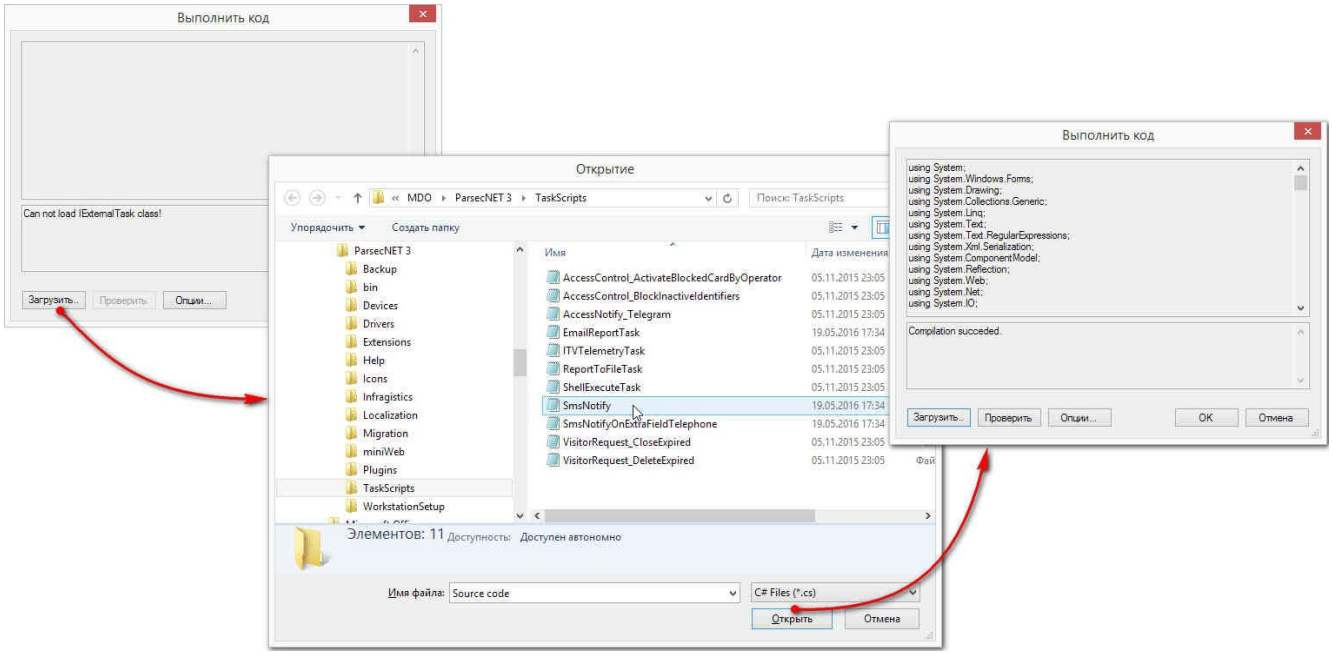
Сохраните изменения и закройте файл скрипта, не изменяя его местоположения.

Шаг 5.

Сформируйте сообщение, для чего в правой панели диалога нажмите на кнопку *Добавить* и выберите в раскрывшемся списке *Выполнить код*:



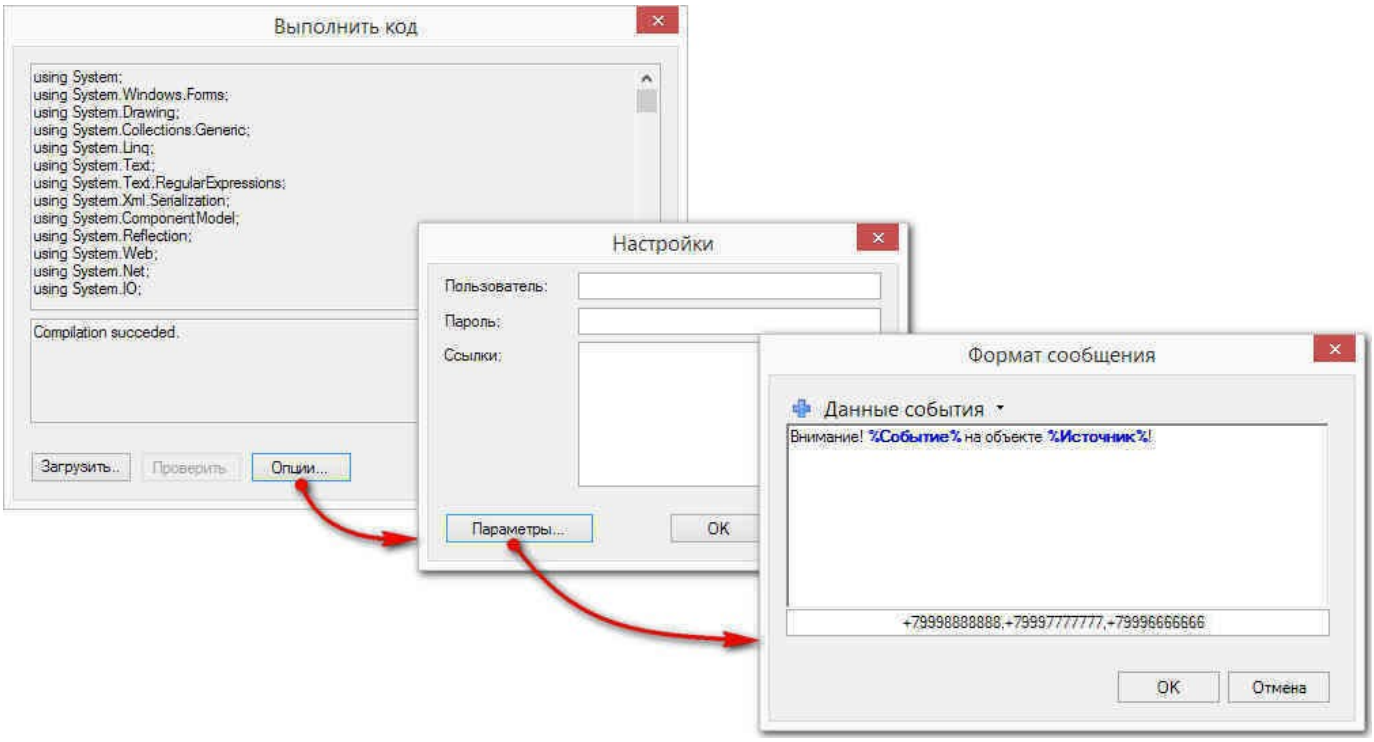
В открывшемся окне нажмите на кнопку *Загрузить...*, перейдите в папку со скриптами и выберите скрипт SmsNotify:



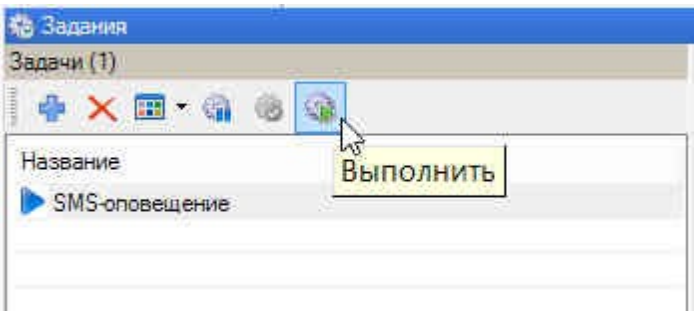
После успешной загрузки скрипта, о чем говорит надпись "Compilation succeded", нажмите на кнопку *Опции...*. В открывшемся окне *Настройки* нажмите на кнопку *Параметры* (все поля оставьте пустыми), откроется окно *Формат сообщения*.

В верхнем поле можно создать шаблон текстового сообщения, при этом из раскрывающегося списка *Данные события* можно выбрать те параметры события, которые будут передаваться в сообщении.

В нижнем поле через запятую или точку с запятой вводятся номера телефонов, на которые будет отправлено сообщение.



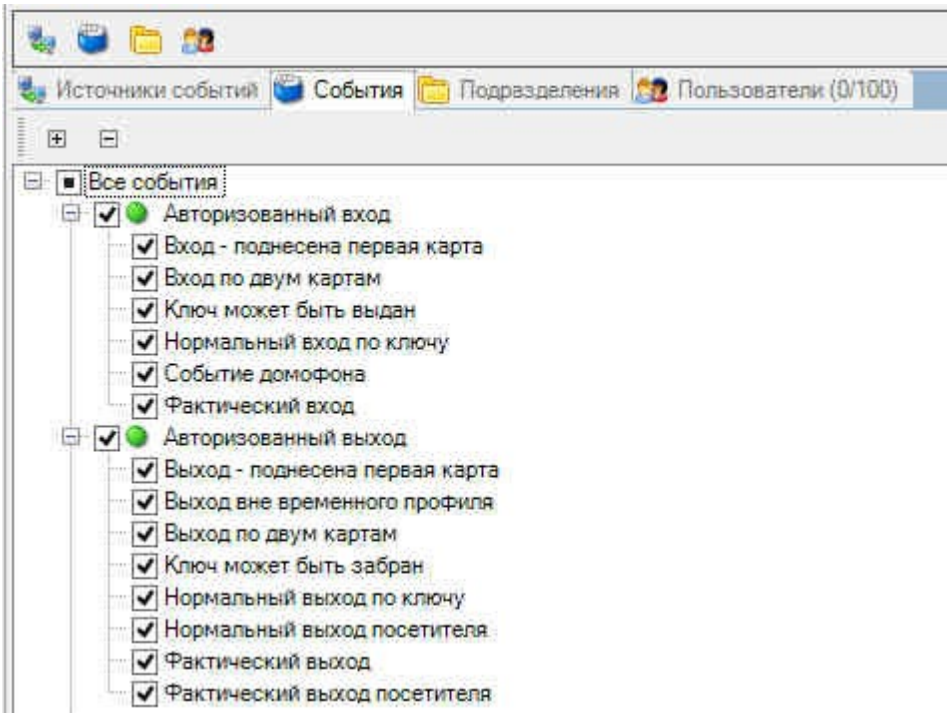
После создания сообщения, последовательно закройте окна, нажимая на кнопку *OK*. Задание готово. Его можно протестировать, запустив вручную с панели инструментов:



Отправка сообщения на телефон, указанный в системном дополнительном поле

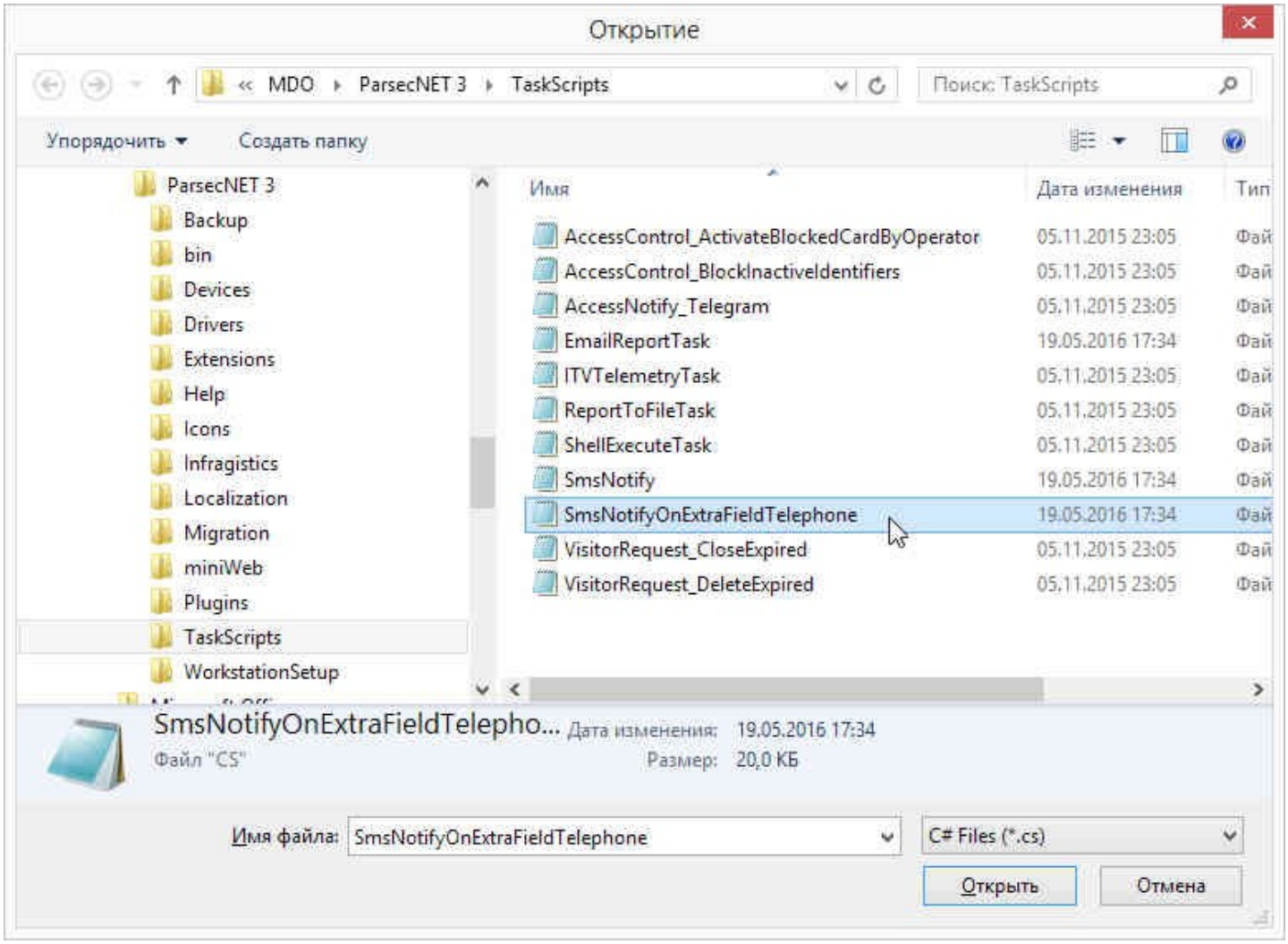
Такая функция может быть полезна, например, для информирования родителей о проходе ребенка через школьный турникет на вход и выход. При создании задания для данного случая в Менеджере заданий выполняются действия, аналогичные описанным выше, со следующими изменениями:

- На Шаге 3 выберите категории событий "Авторизованный вход" и "Авторизованный выход":



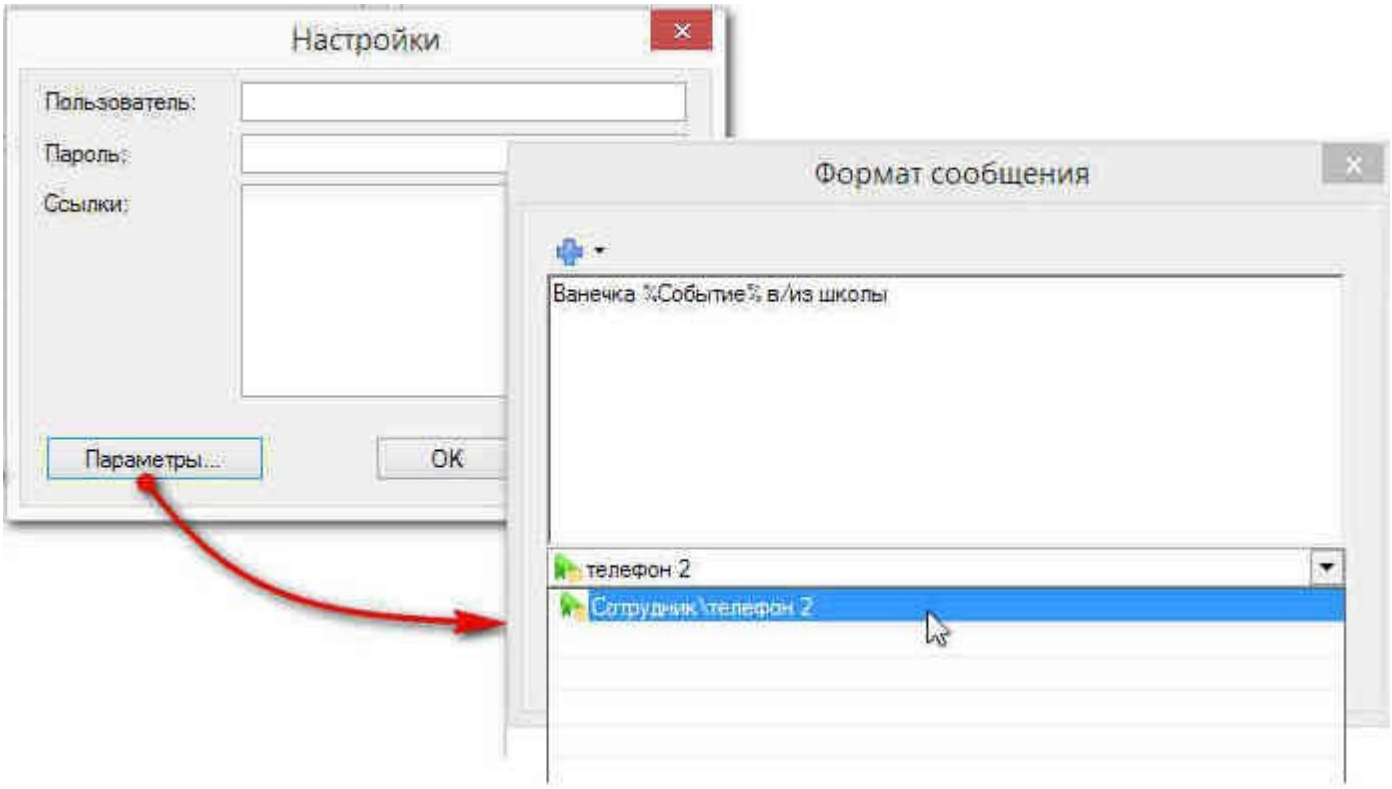
Такой выбор охватывает любой вариант прохода школьника как через дверь, так и через турникет;

- На Шаге 4 логин и пароль нужно ввести в файл скрипта SmsNotifyOnExtraFieldTelephone:



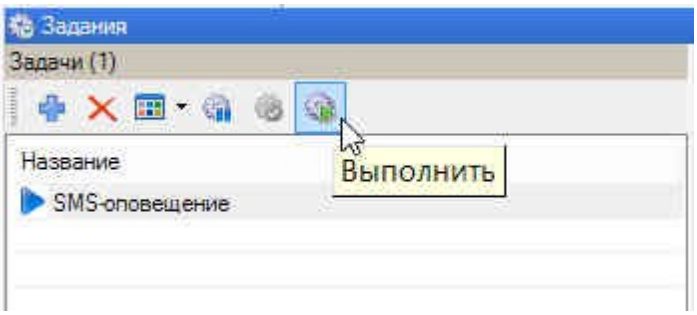
- На Шаге 5 при создании сообщения необходимо ввести логин и пароль, под которыми пользователь вошел в систему ParsecNET 3, а также указать системное дополнительное

поле[155], содержащее у каждого школьника телефон родителей, на который будет отправляться сообщение:



Системное дополнительное поле, которое будет использоваться в задании с использованием данного скрипта, должно иметь тип - "Строковый".

После создания сообщения, последовательно закройте окна, нажимая на кнопку *OK*. Задание готово. Его можно протестировать, запустив вручную с панели инструментов:



См. также:

- Мини-консоль[395]
- Настройка уведомлений[396]
- Отправка SMS через GSM-модем[398]
- Отправка сообщения в Telegram[408]
- Отправка e-mail[409]
- Печать уведомлений[411]

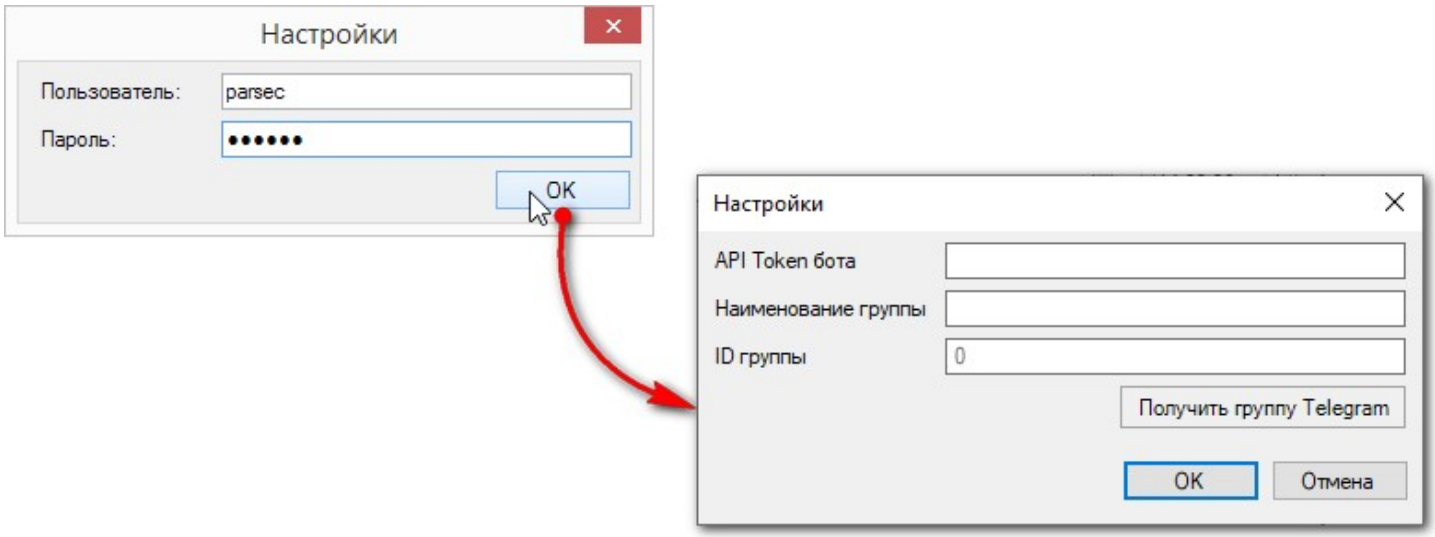
9.5 Отправка сообщения в Telegram

Система позволяет создать задачу по отправке уведомления о событии в приложение по обмену сообщениями Telegram.

Первым шагом необходимо создать Telegram-бота. Описание процесса создания находится в разделе Telegram-бот[393].

Затем выполните следующие шаги:

1. В ParsecNET 3 создайте задание[322] с типом запуска "По событию устройства", на панели *Действия* выберите команду "Выполнить код - AccessNotify_Telegram.cs";
2. Введите логин и пароль оператора, имеющего право на выполнение тех действий, которые автоматизированы данным исполняемым файлом;
3. В поле *API Token бота* окна *Параметры* введите API токен, который Вам выдал @BotFather при создании вашего бота (см. шаг 4), и нажмите на кнопку *Получить группу Telegram*. Наименование группы (в нашем примере это GroupMDOtest) и ID группы появятся в соответствующих полях окна;



4. Закройте окна, нажимая на кнопку *ОК*;
5. Теперь при прохождении выбранных в задаче субъектов через указанные в ней же точки доступа, всем участникам общего чата в Telegram будет приходить уведомления о входах и выходах в формате: "ФИО, точка прохода, событие".

См. также:

Мини-консоль[395]

Настройка уведомлений[396]

Отправка SMS через GSM-модем[398]

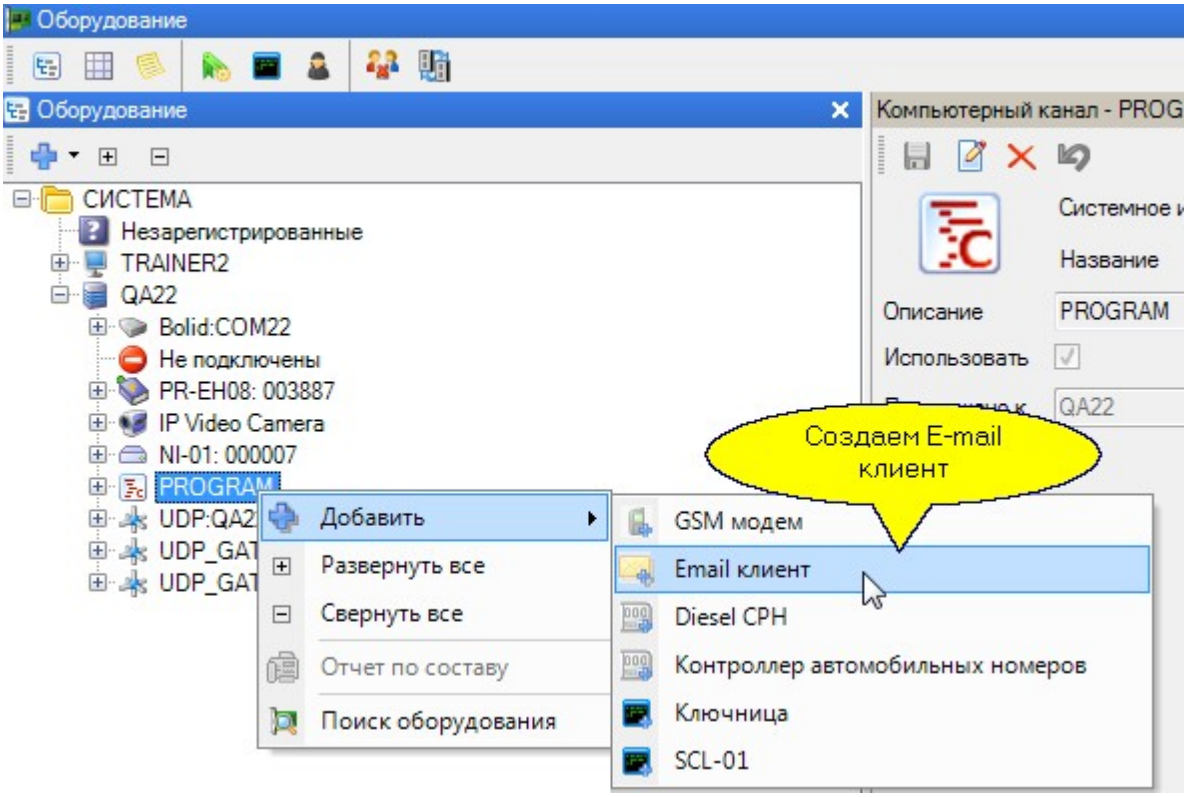
Отправка SMS через интернет-портал[402]

Отправка e-mail[409]

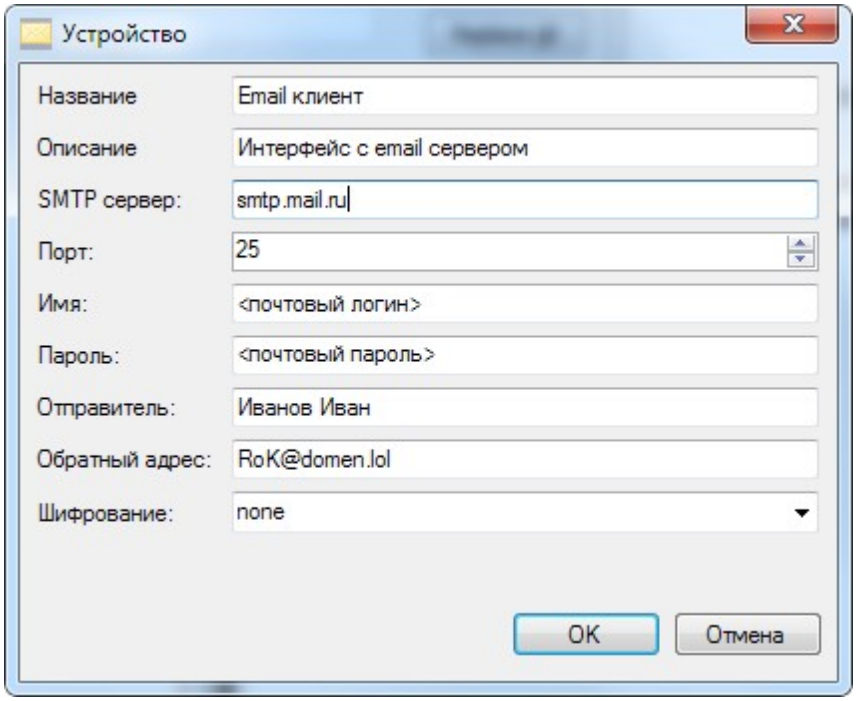
Печать уведомлений[411]

9.6 Отправка e-mail

Для отправки сообщения на заданный адрес электронной почты первым шагом необходимо на канале PROGRAM создать E-mail клиент, то есть псевдо-устройство, предназначенное для отправки электронной почты встроенными средствами Windows. Делается это из контекстного меню (по правой кнопке мышки) при выборе канала PROGRAM, как показано на рисунке ниже:



Диалог ввода параметров для e-mail клиента показан на рисунке ниже.



Если какие-то параметры вам непонятны или неизвестны - обратитесь к вашему системному администратору.

Подготовка сообщений, отправляемых по электронной почте, аналогична отправке SMS с той разницей, что в качестве устройства выбирается E-mail клиент, а вместо номера телефона вводится почтовый адрес, на который следует посылать почту.

См. также:

Мини-консоль[395]

Настройка уведомлений[396]

Отправка SMS через GSM-модем[398]

Отправка SMS через интернет-портал[402]

Отправка сообщения в Telegram[408]

Печать уведомлений[411]

9.7 Печать уведомлений

Уведомления о системном событии можно распечатать на подключенном к системе принтере. Настройка принтера описана в разделе Построчный принтер[154] .

Единственное отличие от других способов передачи уведомлений - это выбор в качестве устройства построчного принтера на шаге[321] настройки уведомления в редакторе заданий.

См. также:

Мини-консоль[395]

Настройка уведомлений[396]

Отправка SMS через GSM-модем[398]

Отправка SMS через интернет-портал[402]

Отправка сообщения в Telegram[408]

Отправка e-mail[409]

10. Настройка IP-камеры

Данный раздел не является руководством по настройке и работе с Вашей IP-камерой, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения своей камеры обратитесь к руководству по ее использованию.

Для полноценного использования функционала IP-камер, особенно с включенными функциями распознавания номеров, настоятельно рекомендуется использовать на сервере и рабочих станциях Системы процессоры с поддержкой инструкций AVX.

Подключенная к системе IP-камера позволяет получать как статические так и динамические изображения наблюдаемой территории и субъектов доступа на ней. Подсистема видеонаблюдения обладает следующими характеристиками:

- Передача изображения:
  - в формате JPEG и MJPEG по протоколу передачи данных HTTP;
  - в формате MJPEG и H.264 по протоколу передачи данных RTSP.
- Настройка частоты кадров, времени хранения и количества хранящихся кадров;
- Просмотр "живого" изображения с IP-камер в мониторе событий и в консоли видеоверификации;
- Сохранение одного или нескольких кадров;

- Распознавание автомобильных номеров.

В последующих подразделах рассмотрены вопросы подключения IP-камеры, а также ее использование в составе ParsecNET 3.

См. также:

Подключение и настройка 412

Использование камеры 414

10.1 Подключение и настройка

Чтобы интегрировать IP-видеокамеру в СКУД ParsecNET 3, первыми шагами выполните:

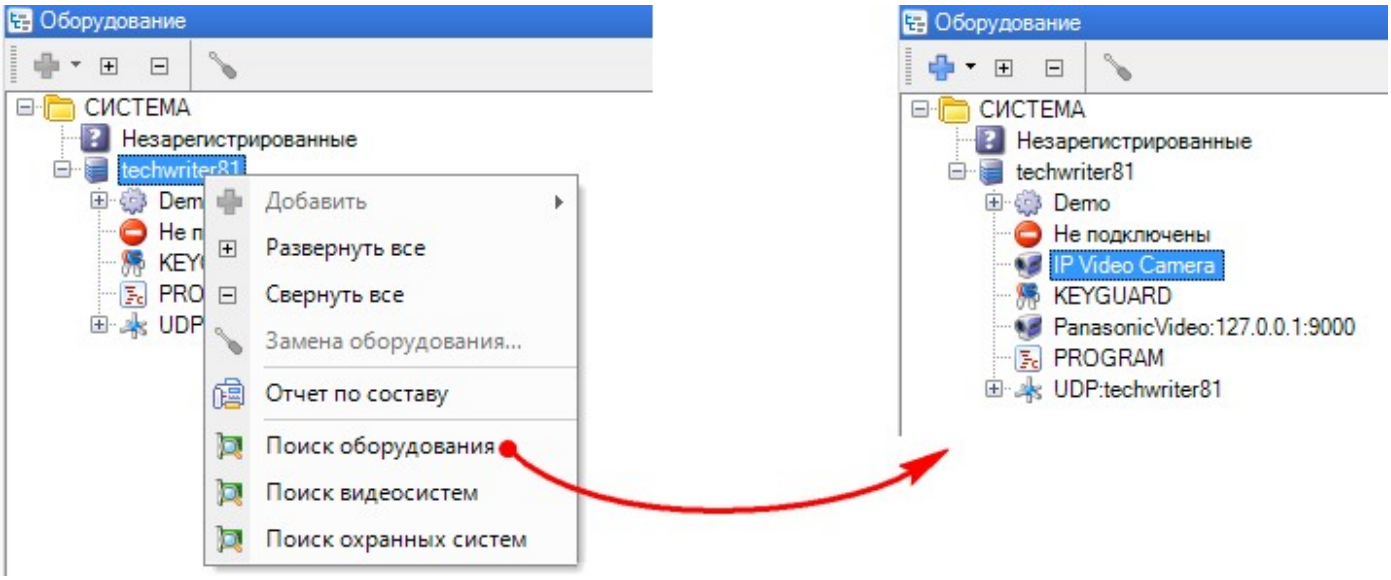
- установку и подключение камеры к рабочей станции или серверу ИСБ;
- настройку камеры в соответствии с инструкцией ее производителя.

В конечном итоге, для интеграции камеры в систему необходимо знать:

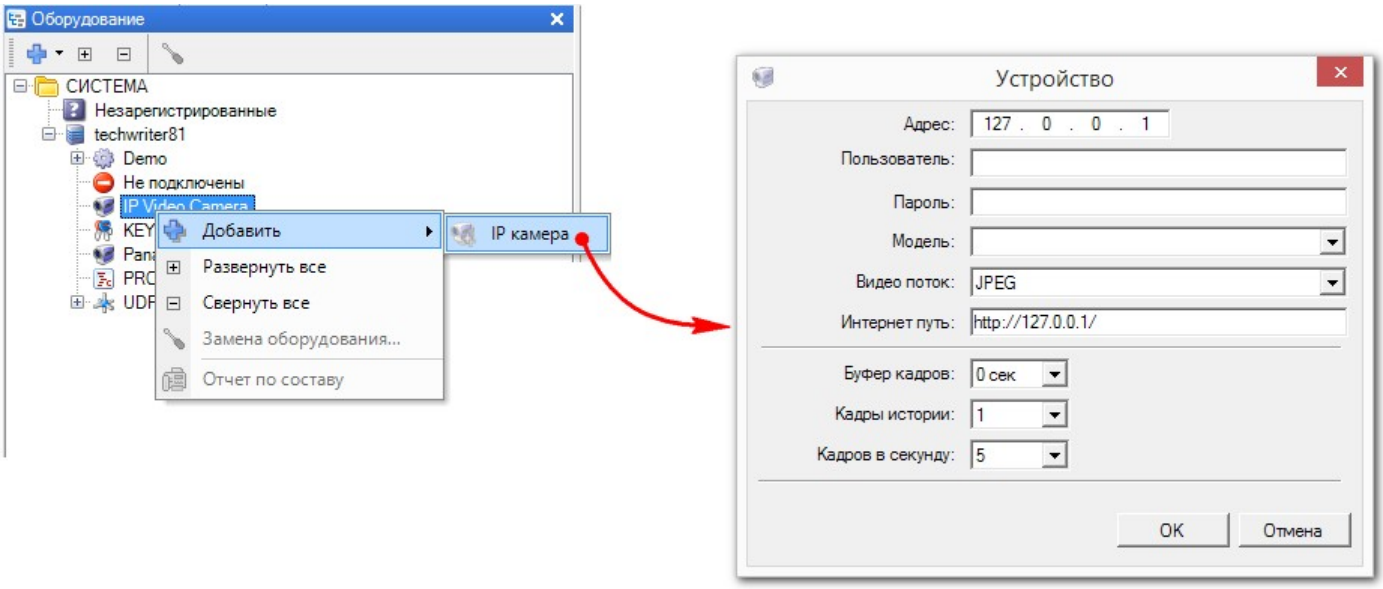
- IP-адрес камеры;
- Логин и пароль, если они заданы;
- URL для форматов JPEG/MJPEG (в зависимости от количества потоков, которые выдает камера, и поддерживаемых ею форматов).

После того, как камера настроена и установочные данные известны, выполните следующие действия:

1. Запустите консоль *Администрирование*;
2. Откройте редактор оборудования;
3. На рабочей станции, к которой подключена IP-камера, запустите поиск оборудования, выбрав одноименный пункт в контекстном меню;
4. Система обнаружит камеру и создаст для нее отдельный канал:



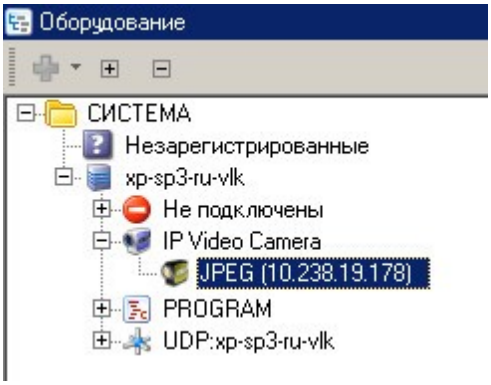
5. Откройте контекстное меню канала и выберите пункт "Добавить". Откроется окно добавления камеры на канал:



6. Заполните поля:
   - *Адрес* - IP-адрес камеры;
   - *Пользователь* - задайте логин пользователя;
   - *Пароль* - задайте пароль пользователя.
     Пара логин/пароль предназначена для доступа пользователя системы ParsecNET 3 к изображению с данной камеры;
   - *Производитель* - в раскрывающемся списке выберите производителя камеры (если есть);
   - *Модель* - в раскрывающемся списке выберите модель камеры (если есть);
   - *Интернет путь* - если выше выбраны производитель и модель, в этом списке можно будет выбрать URL для получения изображения того или иного качества, в том или ином формате. Если производитель и модель не выбраны, путь необходимо указать вручную.
     Количество URL для одной камеры определяется количеством режимов разрешения картинки, выдаваемых потоков изображения и другими характеристиками камеры;

     Если необходимо от камеры получать несколько изображений, повторите процедуру добавления камеры. При этом укажите нужный видеопоток. Также можно указать другие значения и всех остальных параметров.

   - *Буфер кадров* - период времени, по истечении которого кадр удаляется из буфера памяти. Другими словами, это "возраст" самого старого кадра в буфере;
   - *Кадры истории* - количество сохраняемых в БД кадров из буфера кадров по команде "Сохранить историю кадров". Всегда сохраняется первый и последний кадры, а также равномерно распределенные между ними кадры в количестве, заданном данным параметром;
   - *Кадров в секунду* - частота обновления изображения (fps);
   - *Включить распознавание номерных знаков* - установите флажок, если камера будет использоваться для распознавания автономеров[582]. При попадании в поле видимости камеры автомобильного номера, система распознает его и сформирует соответствующее событие.
7. Нажмите на кнопку *OK*. Окно закроется, а к каналу IP Video Camera будет подключена видеокамера:



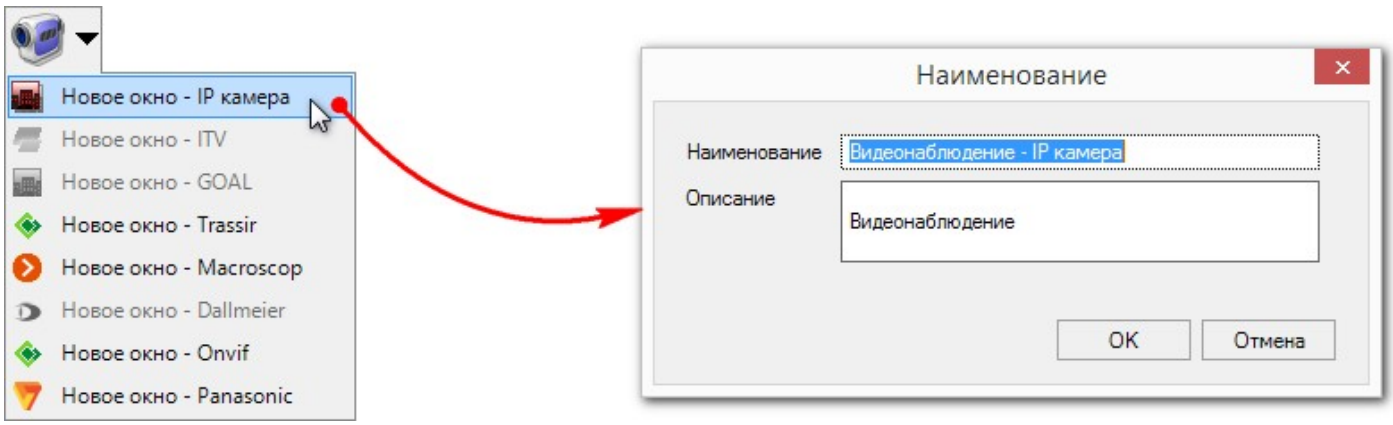
10.2 Использование камеры

Использование IP-камер

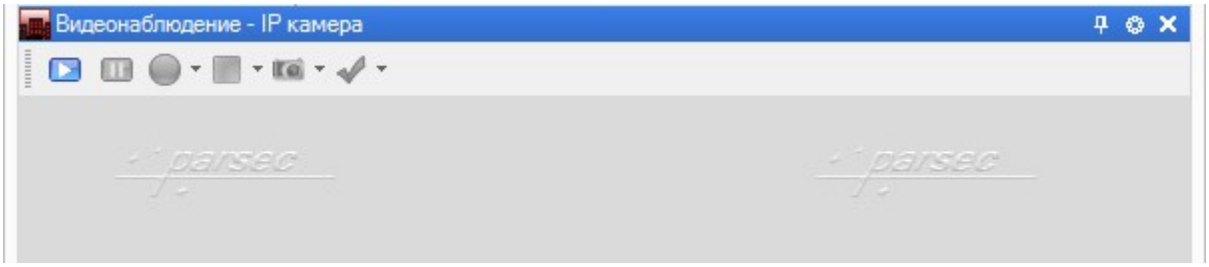
Изображение с IP-камер можно просматривать в мониторе событий и в консоли видеоверификации.

Чтобы увидеть изображение с IP-камеры, выполните следующие действия:

1. Запустите монитор событий или консоль видеоверификации;
2. В раскрывающемся списке кнопки *Видеонаблюдение* выберите пункт "Новое окно - IP камера". В открывшемся окне введите произвольное название или оставьте название по-умолчанию и нажмите на кнопку *OK*:



В консоли будет создано новое окно для отображения изображения с IP-камеры:



Элементы интерфейса этого окна:

- включение/отключение фиксированного режима, при котором не отображается панель инструментов и невозможно изменить положение и размер окна видеонаблюдения(см. раздел Блокировка внешнего вида[54]);
- открывает окно выбора камер (см. шаг 3 ниже);
- показать изображение;

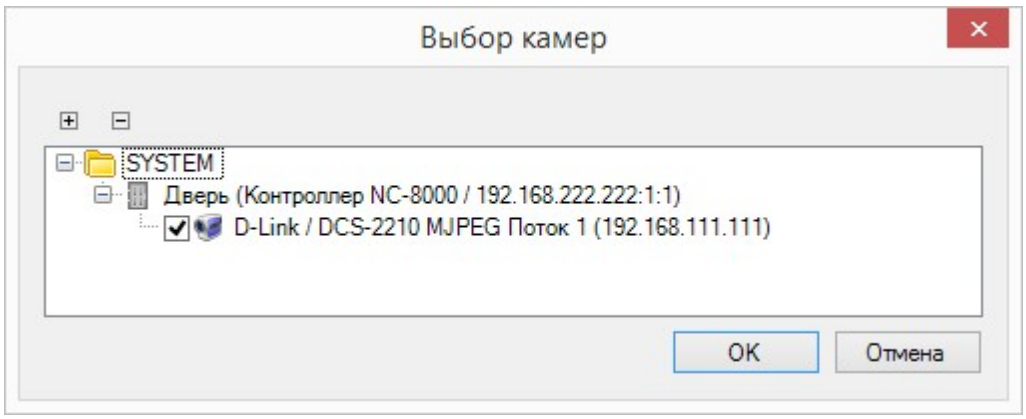
- остановить показ изображения;

- сохранить кадр;

- пометить запись. Позволяет запустить видео с момента, когда поставлена метка.

Кнопки начала и остановки записи для IP-камер не активны.

3. При первом нажатии на кнопку , система попросит выбрать нужную камеру (позднее можно будет выбрать другую камеру (которую нужно предварительно добавить), открыв это окно кнопкой):



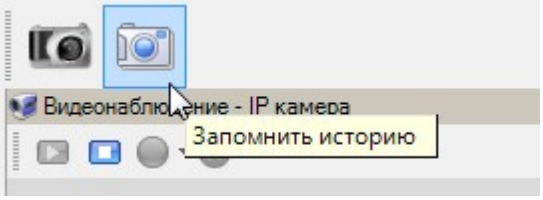
Установите флажок для той камеры или нескольких камер, изображение с которых хотите получать, и нажмите на кнопку *OK*. На рисунке выше изображена камера, включенная в группу двери посредством Редактора топологии.

Можно открыть и настроить одновременное отображение окна видеонаблюдения и окна видеоверификации, Это дает определенные удобства: можно видеть данные субъекта доступа из БД (соответствующие предъявленному идентификатору) и наблюдать в реальном времени за самим субъектом.
Подобным образом организовать окна можно как в мониторе событий, так и в консоли видеоверификации.

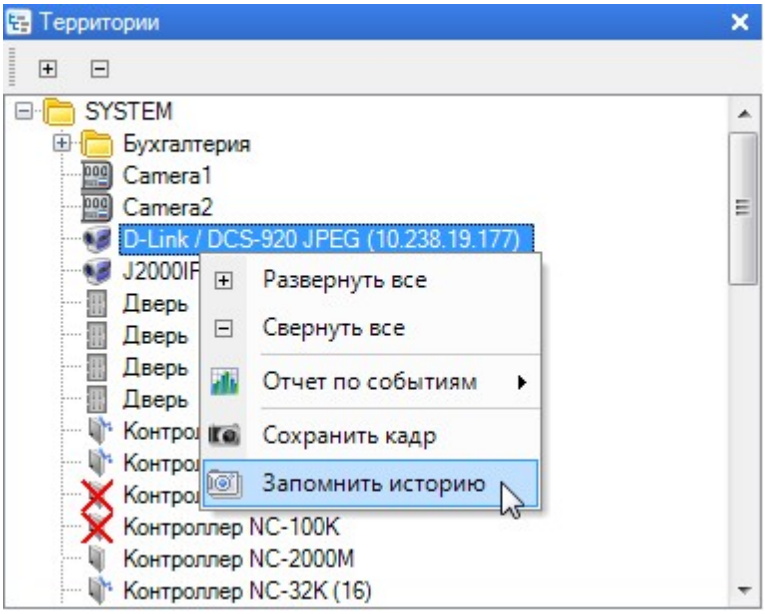
Сохранение изображений

Изображение, передаваемое IP-камерой, можно сохранить инструментами монитора событий. Сохранение производится в виде одного кадра либо группы кадров из временного диапазона, заданного при настройке (см. шаг 6 413). Видео не сохраняется.

При запуске просмотра изображения с IP-камеры на панели инструментов монитора появляются две кнопки *Сохранить кадр* и *Запомнить историю*:

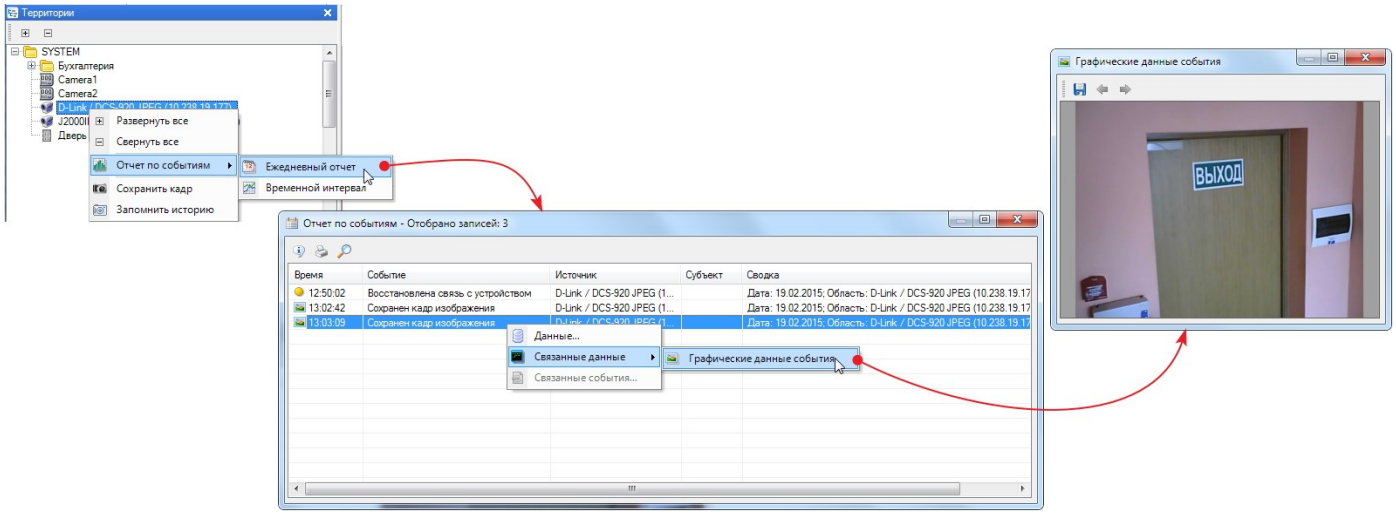


Те же функции выполняют одноименные пункты контекстного меню камеры:



При выборе сохранения одного кадра, он будет записан в БД. Чтобы просмотреть его, выполните следующие действия:

1. Составьте отчет по событиям, воспользовавшись пунктом контекстного меню или инструментами генератора отчетов по событиям[302] ;
2. Найдите нужное событие "Сохранен кадр изображения" и щелчком правой кнопки мыши откройте контекстное меню;
3. Выберите пункт "Связанные данные -> Графические данные события". Откроется сохраненный кадр:



Сохраненный кадр можно теперь сохранить в другом месте и в другом формате, нажав на кнопку .

Сохранение истории кадров производится аналогичным способом. В открывшемся окне *Графические данные события* можно будет просмотреть сохраненные кадры, переключаясь между ними при помощи кнопок и . Количество кадров и временной период, в рамках которого они делаются, задаются соответственно параметрами "Кадры истории" и "Буфер кадров" при настройке подключения камеры (см. шаг 6[413]).

11. Дополнительные модули

Общие сведения

В данном разделе описаны принципы работы дополнительных модулей системы ParsecNET 3, которые не входят в базовую версию программного обеспечения. Все эти модули требуют отдельных лицензий, прошиваемых в ключе защиты[344] системы.

К числу таких модулей относятся:

- Редактор шаблонов печати[417]. Позволяет создавать и редактировать шаблоны, используемые для печати на карточках - пропусках, а также и другие формы пропусков для сотрудников и посетителей (например, бумажные пропуска установленной на предприятии формы);
- Модуль бюро пропусков[432]. Представляет собой специализированное приложение, предназначенное для организации на предприятии пропускного режима для посетителей и гостей. Полностью интегрирован в систему, за счет чего может использовать установленное на объекте оборудование системы доступа и управлять им в соответствии с заложенной в нем логикой работы;
- Модуль учета рабочего времени[456]. На основании формируемых системой доступа данных, по введенным пользователями правилам позволяет подсчитывать отработанное сотрудниками время с формированием соответствующей отчетности. Также предоставляется возможность вводить такие поправки, как отпуска, больничные, командировки для их учета при составлении табеля учета рабочего времени;
- Модуль видеоверификации[506] позволяет организовать специализированные рабочие места для контроля за проходом субъектов доступа с выводом о них подробной информации в реальном времени. Также обеспечивает управляемый персоналом охраны проход субъектов доступа, не имеющих по какой-то причине прав прохода через конкретную точку;
- Модуль интеграции с системами видеонаблюдения[515]. Обеспечивает взаимодействие системы ParsecNET 3 со сторонней системой видеонаблюдения (например, ИСБ "Интеллект");
- Модуль интеграции с системами ОПС[603]. Обеспечивает взаимодействие системы ParsecNET 3 со сторонней системой охранного - пожарной сигнализации (например, ОПС "Стрелец");
- Модуль распознавания документов[671]. Позволяет распознавать и автоматически заносить в систему данные субъекта доступа с отсканированного документа (например, паспорта).

Необходимо еще раз обратить внимание, что данные модули требует отдельных лицензий (а модуль распознавания документов - еще и ***собственного ключа защиты***). Об условиях поставки модулей можно узнать у своих дилеров или установщиков.

11.1 Редактор шаблонов печати

Лицензируется как PNSoft-PI[344]

Назначение

Лицензируемый модуль "Редактор шаблонов печати" предназначен для разработки шаблонов, по которым в дальнейшем будут печататься пропуска сотрудников (например, на пластиковых картах доступа). Однако этим возможности редактора печати пропусков не ограничиваются - шаблон может предполагать печать данных сотрудника на стандартной бумаге формата А4,

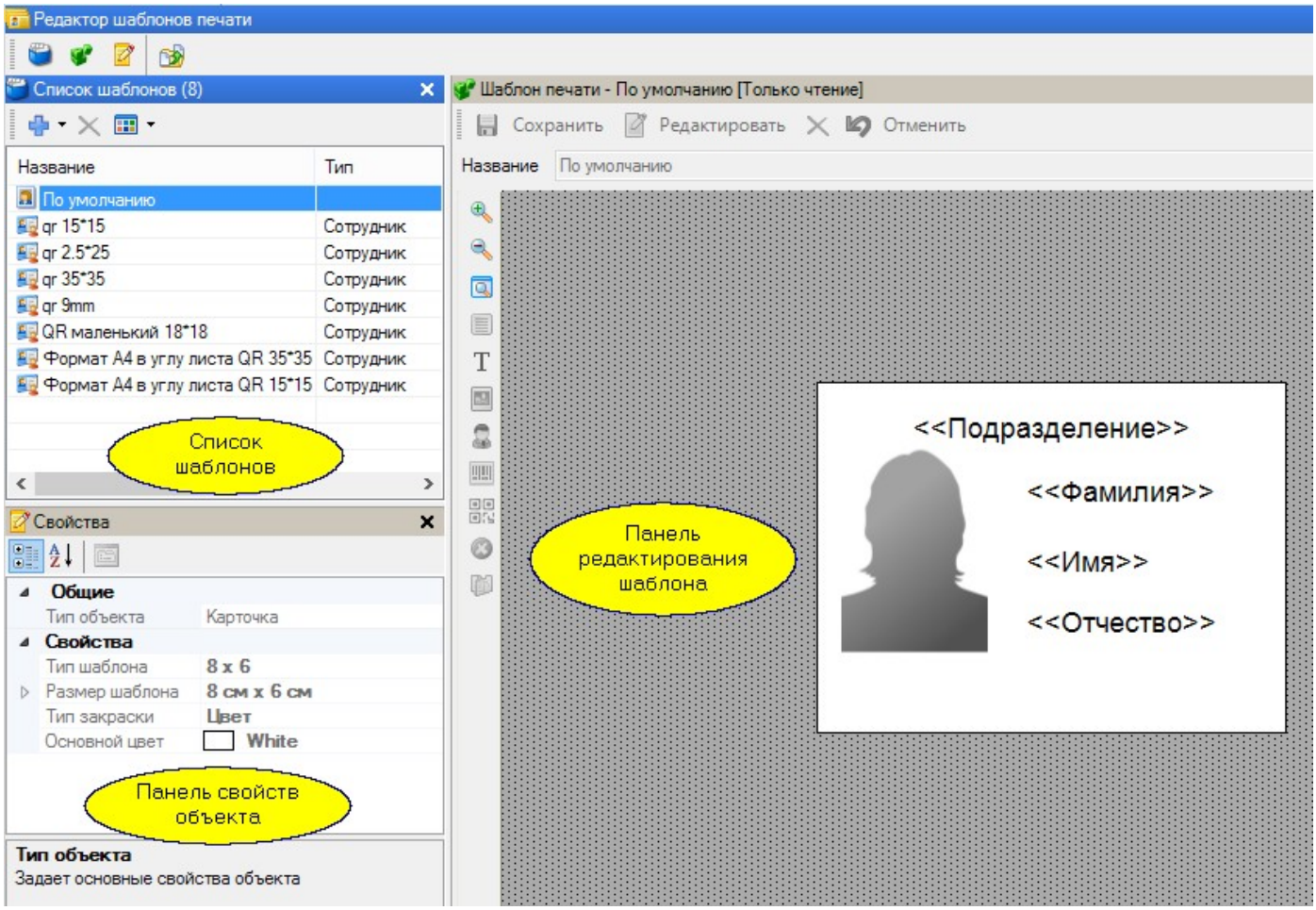
печать нескольких выбранных пропусков одновременно с раскладкой на листе большего формата и так далее.

В системе может быть неограниченное количество шаблонов печати, причем в каждой организации имеется только собственный набор - другим организациям ваши шаблоны никогда не будут доступны.

Также имеется возможность импорта шаблонов[430] печати из системы ParsecNET версии 2.5.

Панели редактора шаблонов

Редактор по-умолчанию имеет три панели: панель списка шаблонов, панель свойств редактируемого объекта шаблона и панель редактирования шаблона:



Если какая-то панель не видна, воспользуйтесь кнопками на панели инструментов редактора для восстановления панели. Также можно воспользоваться меню "Вид - по-умолчанию" из меню рабочего стола.

Создание нового шаблона печати пропусков

При поставке в системе имеется один примитивный шаблон "по-умолчанию". Вам потребуется самим создать свои шаблоны в соответствии с фирменным стилем или другими требованиями, действующими в компании. Мы для примера создадим несложный шаблон, включающий подложку, фотографию сотрудника, его фамилию, имя отчество и название подразделения.

Для создания нового шаблона в панели списка шаблонов нажмите на кнопку *(Добавить)* и в открывшемся диалоге введите название вашего шаблона.

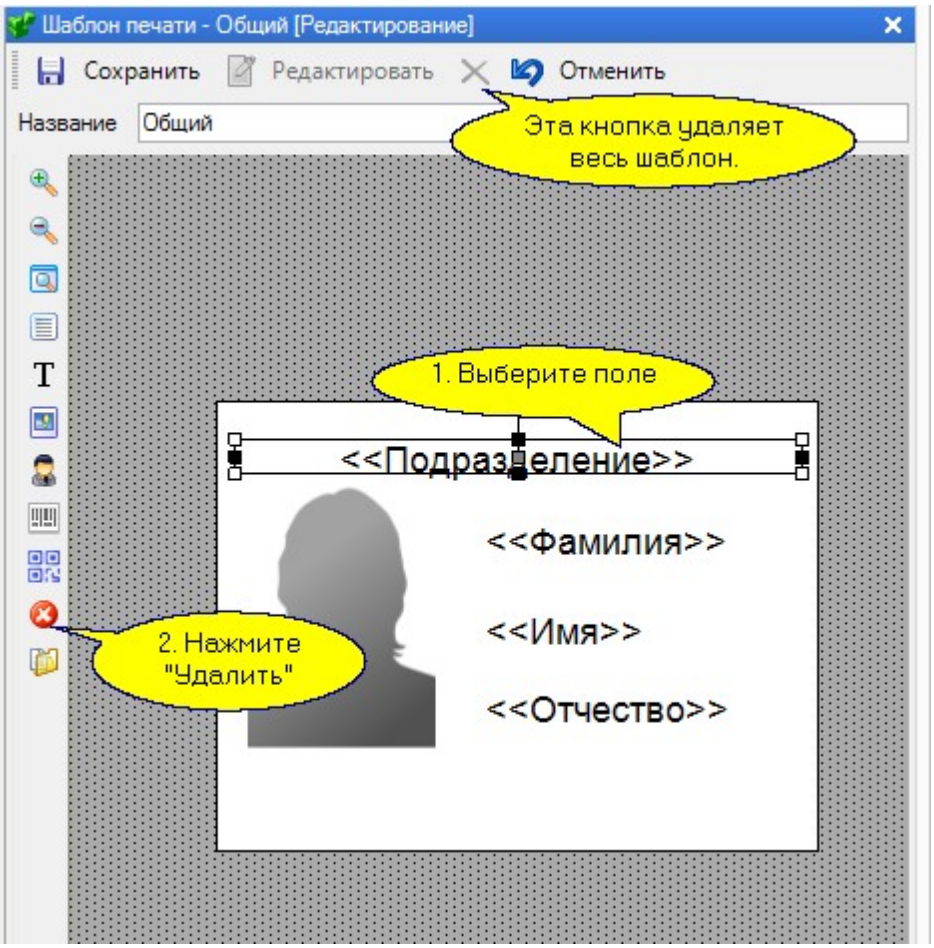
Новые шаблоны создаются на основе ранее созданных. Первый раз вам можно создать шаблон только на базе имеющегося в системе по-умолчанию, но в дальнейшем в качестве основы вы сможете выбирать и свои ранее созданные шаблоны, что может упростить процесс.

Шаблон с новым именем добавится в списке и автоматически сохранится в базе данных системы. При желании любой шаблон можно удалить из списка стандартным способом. Удаленный шаблон восстановить никаким способом будет уже невозможно.

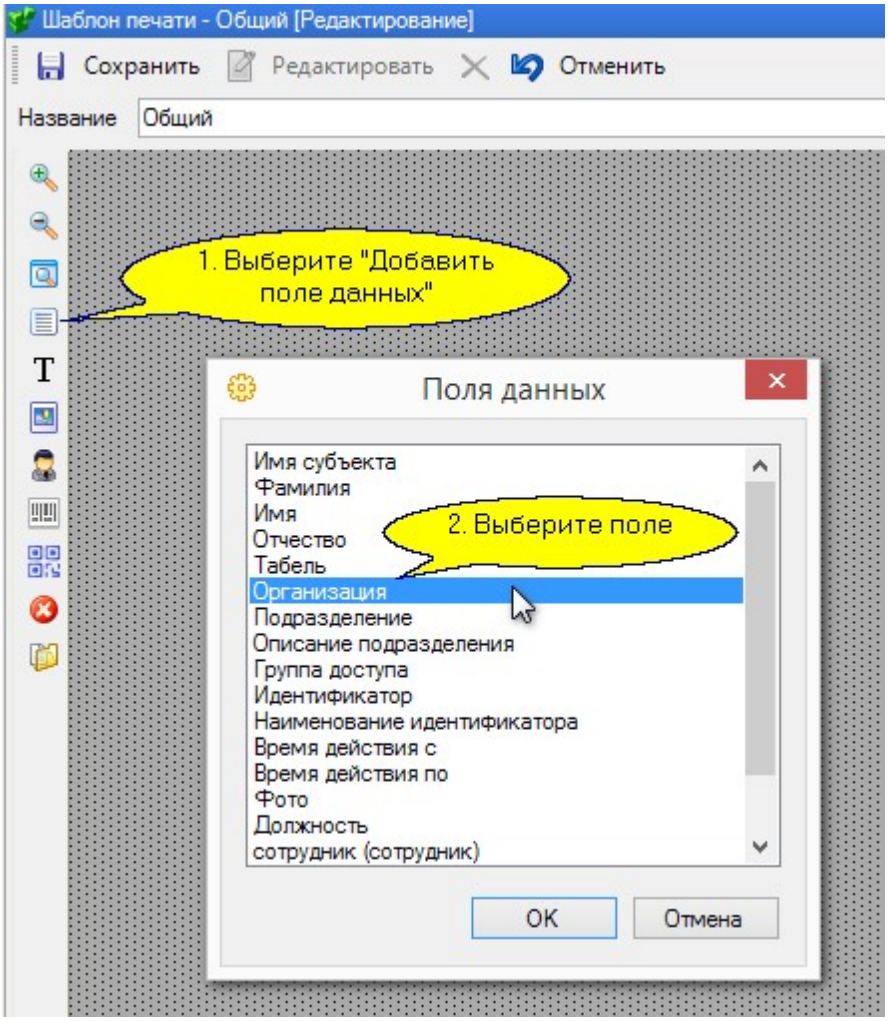
Редактирование шаблона печати пропусков

В нашем шаблоне мы унаследовали поля *Фамилия*, *Имя*, *Отчество* и *Подразделение*, а также фотографию сотрудника.

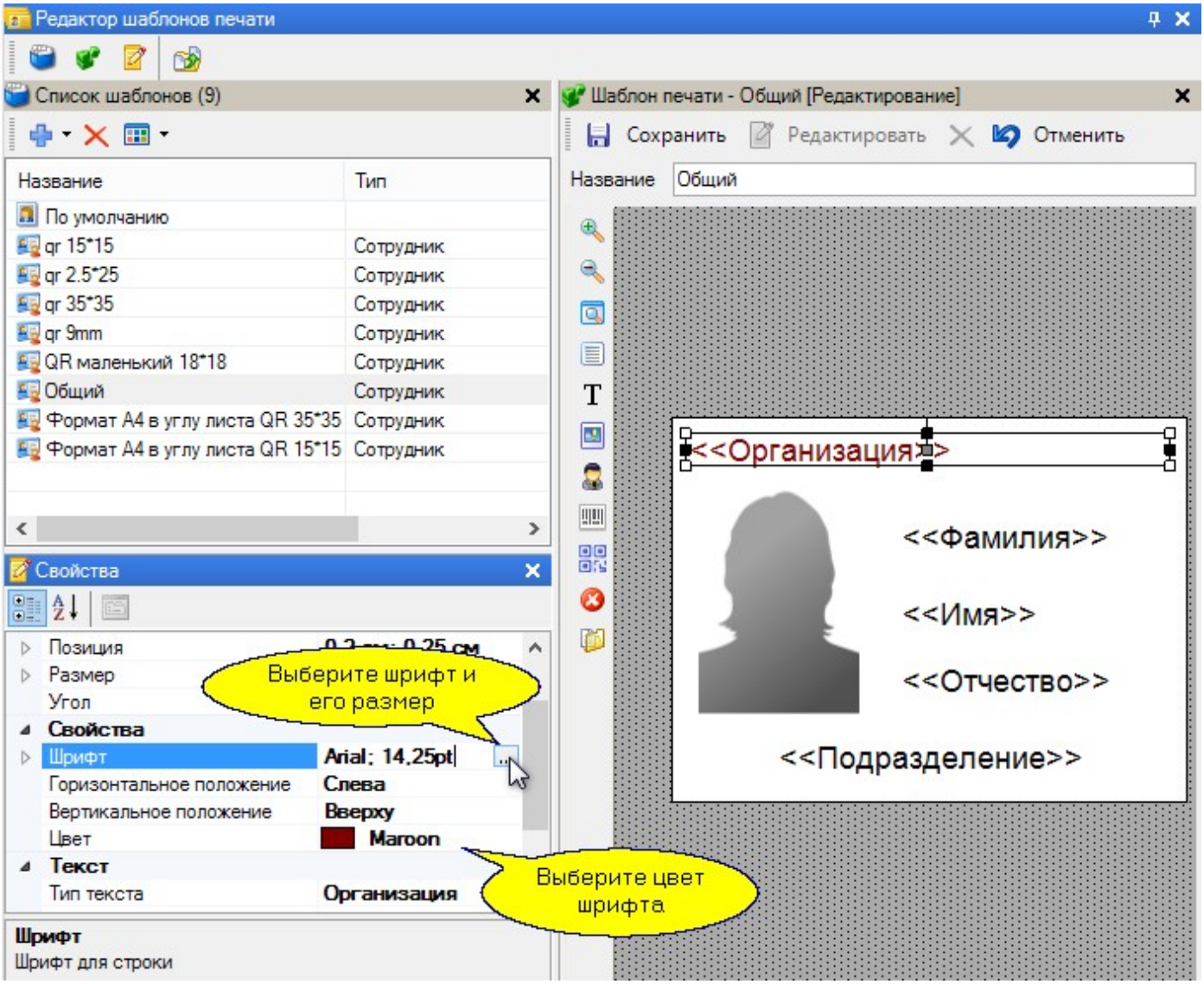
Для редактирования шаблона нужно перейти в панель редактора (правая панель) и нажать на кнопку *Изменить*, после чего нам станут доступны все инструменты редактора. Для начала удалим поле *Подразделение*:



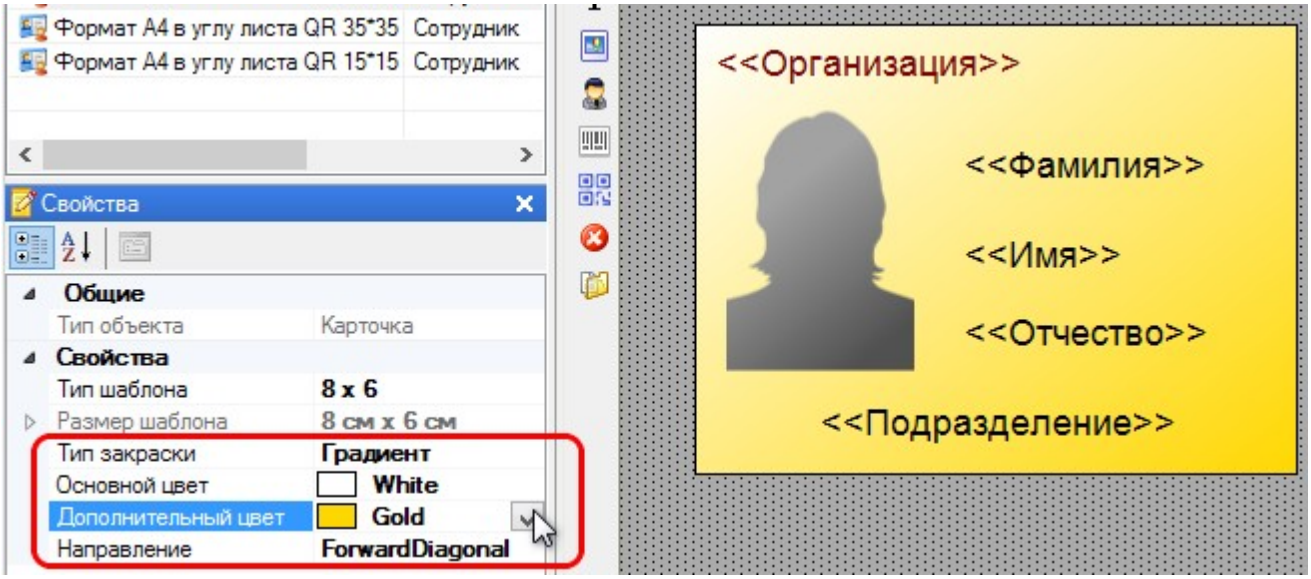
Добавим к своему шаблону название организации. Поскольку оно является полем базы данных системы, мы вводим его через опцию "Добавить поле данных". В списке полей кроме названия организации присутствуют все поля персонала, включая определенные вами дополнительные поля.



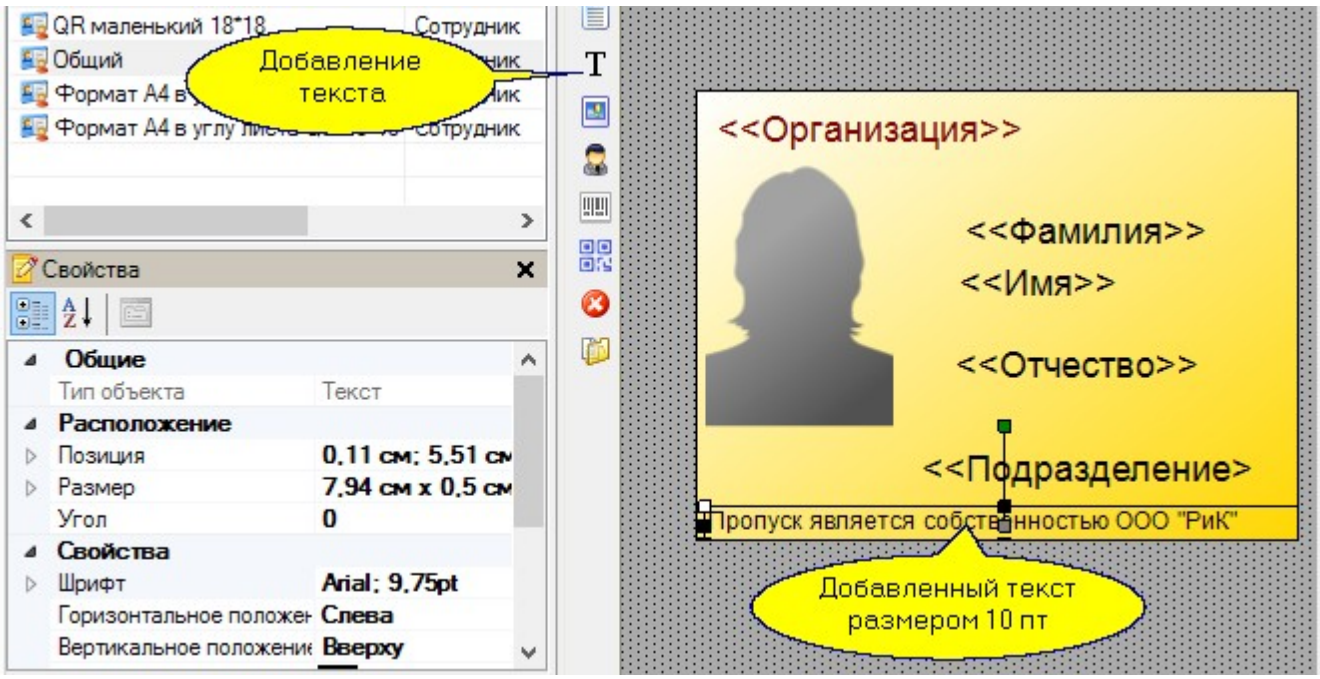
Появившееся на шаблоне поле организации расположим на шаблоне, и в панели свойств объекта поставим параметры шрифта: выбираем шрифт Arial 14 пунктов, жирный, с наклоном, а в качестве цвета выбираем Maroon:



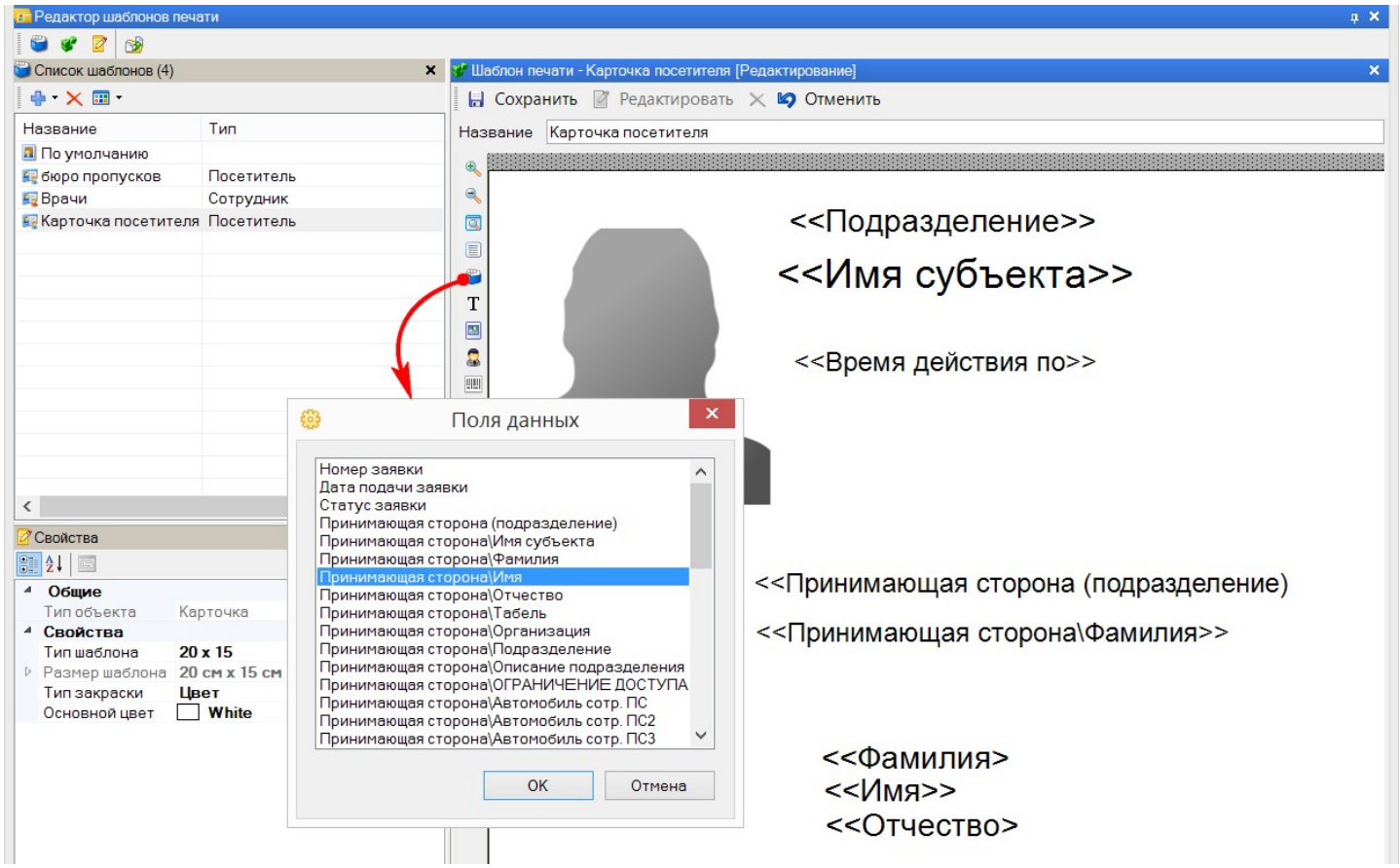
Теперь сделаем подложку, которая будет образовывать фоновое изображение для нашего пропуска. В качестве подложки может использоваться цветная заливка, либо графический файл с диска. Мы выбрали градиентную диагональную заливку с переходом от белого к желтому золотистому:



Последним штрихом добавим мелкий текст в нижней части нашего пропуска:



Шаблон пропуска посетителя имеет эксклюзивную особенность - на пропуске можно разместить сведения о текущей заявке и принимающем сотруднике:



На этом создание шаблона пропуска можно завершить. Как просмотреть изображение пропуска с реальными данными сотрудника описано в разделе ниже[427].

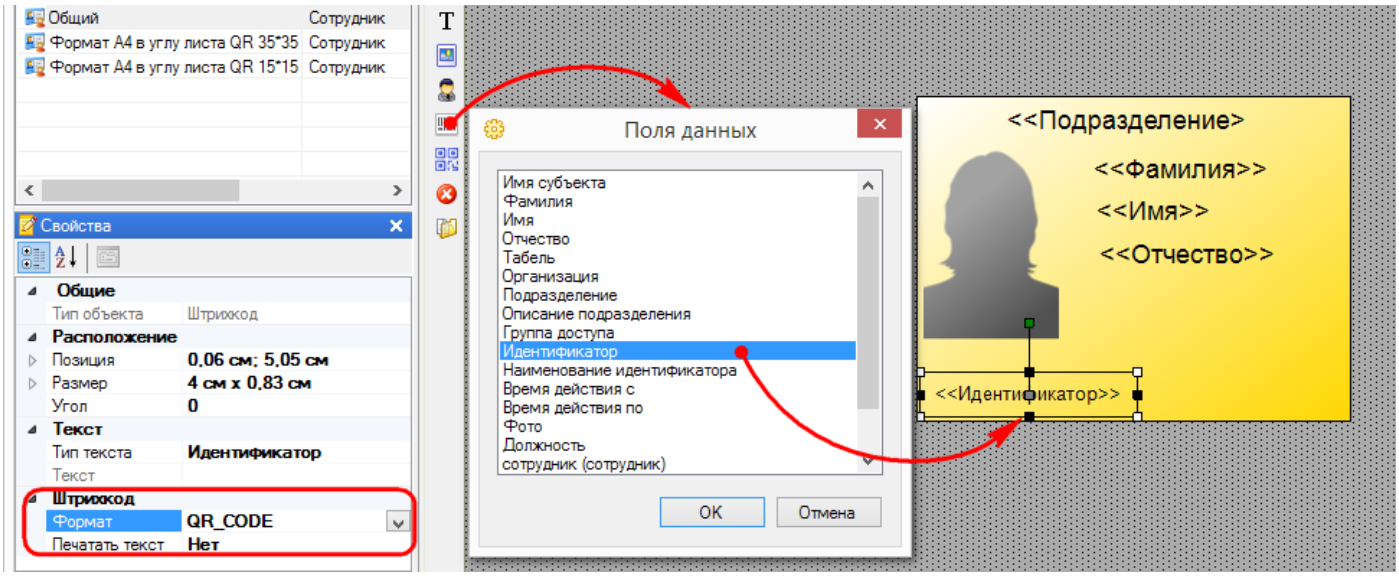
Печать штрих-кодов на пропусках

Система позволяет печатать на пропуске в виде штрих-кода любую информацию из основных или дополнительных полей карточки субъекта доступа. В этом случае на каждом пропуске штрих-код

будет свой. Либо напечатать закодированную информацию, одинаковую для каждого распечатанного пропуска.

Добавление штрих-кода на шаблон пропуска производится следующим образом:

1. Перейдите в режим редактирования, нажав на панели редактирования шаблона на соответствующую кнопку;
2. Нажмите на кнопку *Добавить штрих код*;
3. В открывшемся окне *Поля данных* выберите поле, значение из которого будет напечатано в виде штрих-кода на пропуске и нажмите на кнопку *ОК*;
4. Разместите добавленное поле штрих-кода на шаблоне пропуска и задайте его размеры;
5. Перейдите на панель свойства объекта и в разделе *Штрих код* в поле *Формат* из раскрывающегося списка выберите формат штрих-кода, который будет использоваться при кодировке сведений. (Подробнее о штрих-кодах см. в разделе Форматы штрих-кодов[431]);



Если в разделе **Текст** в поле *Тип текста* выбрать значение "Текст", то в поле штрих-кода на всех пропусках будет печататься закодированный текст, набранный ниже в поле *Текст*.

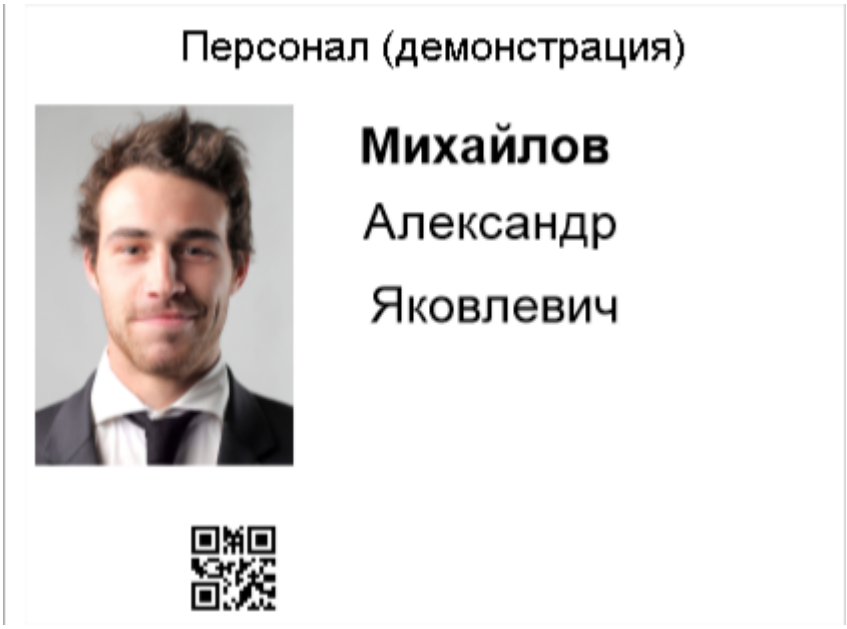
Если в разделе **Штрих код** в поле *Печатать текст* установить значение "Да", то ниже штрих-кода будет печататься то, что закодировано (при условии, что этот тип штрих-кода поддерживает такую функцию);

6. Сохраните внесенные в шаблон изменения.

Теперь пропуска будут печататься по заданному шаблону.

Обратите внимание, печать идентификаторов в виде QR-кода - это частный случай использования функции *Добавить штрих код*. Идентификатор в данном случае просто преобразовывается в QR-код без какого-либо дополнительного шифрования. Это можно применять, когда для считывания QR-кодов будут использоваться считыватели сторонних производителей.

Пропуск будет выглядеть, например, следующим образом:



Шаблон печати QR-кодов Parsec на пропусках

С введением идентификаторов "QR-код Parsec" в Редакторе шаблонов печати появилась соответствующая функция, позволяющая размещать их на печатном пропуске, а также использовать его в виде изображения на экране мобильных устройств. При этом QR-код шифруется особым ключом, который генерируется в разделе Безопасность[157]. Такие QR-коды распознаются только считывателями PNR-QX29.

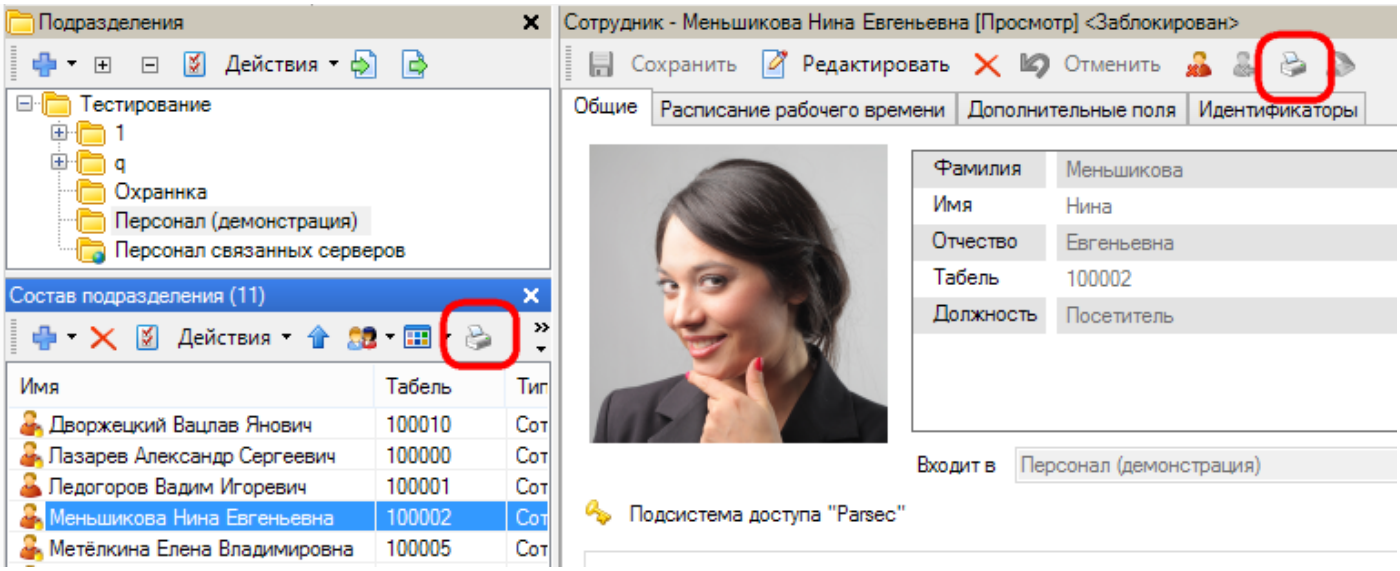
Настройка шаблона печати следующая: нажмите на кнопку *Добавить QR-код Parsec* и откорректируйте размер и положение области, в которой будет печататься QR-код, на шаблоне пропуска:



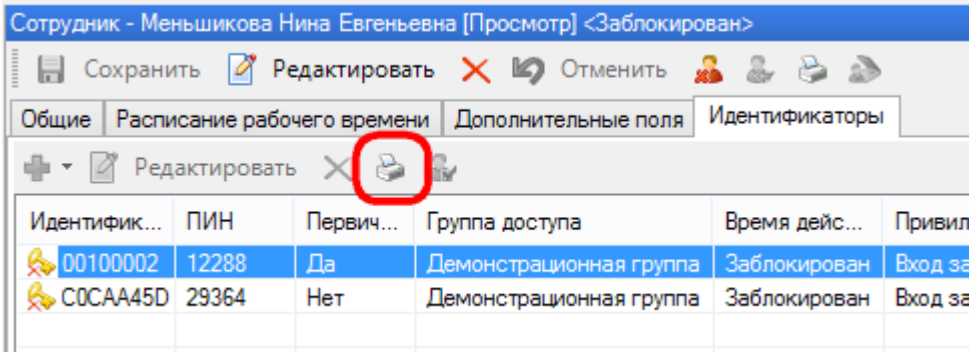
При этом следует рассмотреть 3 варианта печати:

1. Если идентификатор типа "QR-код Parsec" задан как отдельный дополнительный идентификатор субъекта, то нужно перейти на вкладку *Дополнительные идентификаторы*, выбрать этот идентификатор и инициировать печать;
2. Если идентификатор типа "QR-код Parsec" субъекту доступа не задан, то есть 2 варианта, какой идентификатор будет печататься в добавленном в шаблон пропуска поле:
   - Если печать инициируется значком на панели *Состав подразделения* или значком в карточке субъекта доступа, то в виде зашифрованного QR-кода будет печататься первичный

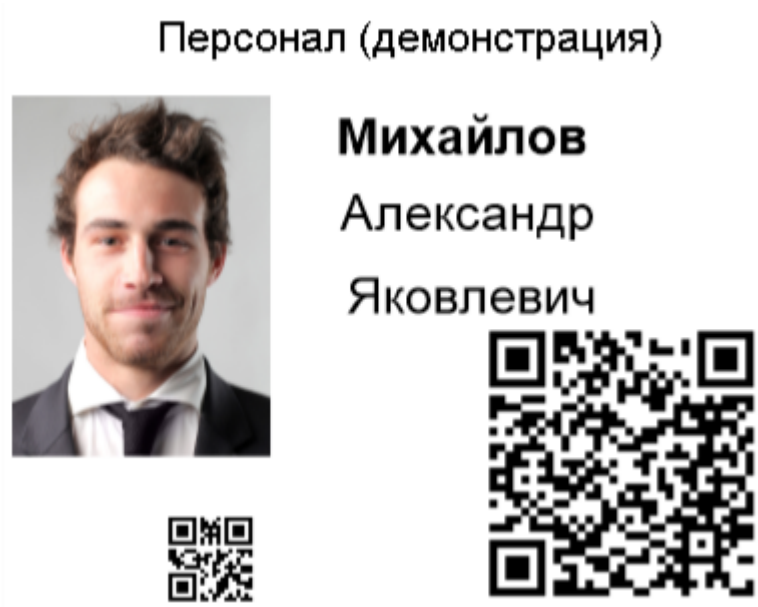
идентификатор субъекта (код, который отображается в поле *Код карты* в карточке субъекта доступа):



- Если перейти на вкладку *Дополнительные идентификаторы* и инициировать печать, то в виде QR-кода на пропуске будет напечатан выбранный дополнительный идентификатор:



Пропуск может выглядеть так:



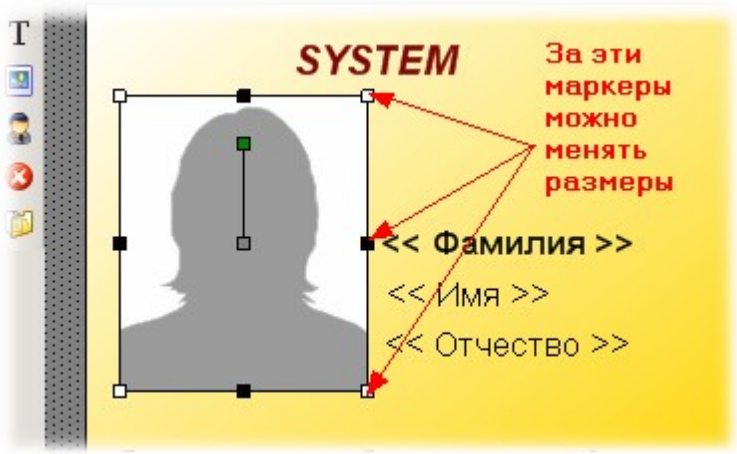
Для примера тут представлены: слева - QR-код идентификатора, напечатанный при помощи функции[422] *Добавить штрих-код*, справа - QR-код идентификатора типа "QR-код Parsec", напечатанный при помощи функции *Добавить QR-код Parsec*.

Свойства объектов шаблона печати пропусков

Шаблон печати может содержать следующие компоненты:

1. Подложка в виде цветовой заливки (непрерывной или градиентной) либо в виде изображения из файла.
2. Фотография сотрудника.
3. Набор полей из базы данных персонала организации.
4. Простой текст.
5. Графическое изображение (например, логотип компании).

Кроме подложки все остальные компоненты могут изменять свое положение и размеры для изменения размеров следует выбрать компонент в режиме редактирования и с помощью маркеров по периметру компонента изменить размер в нужную сторону:



Кроме того, компоненты можно вращать вокруг оси на любой угол. Для примера мы повернули фотографию примерно на 15 градусов:



Как видно, редактор шаблонов похож на многие графические редакторы, которыми, возможно, вы уже пользовались раньше.

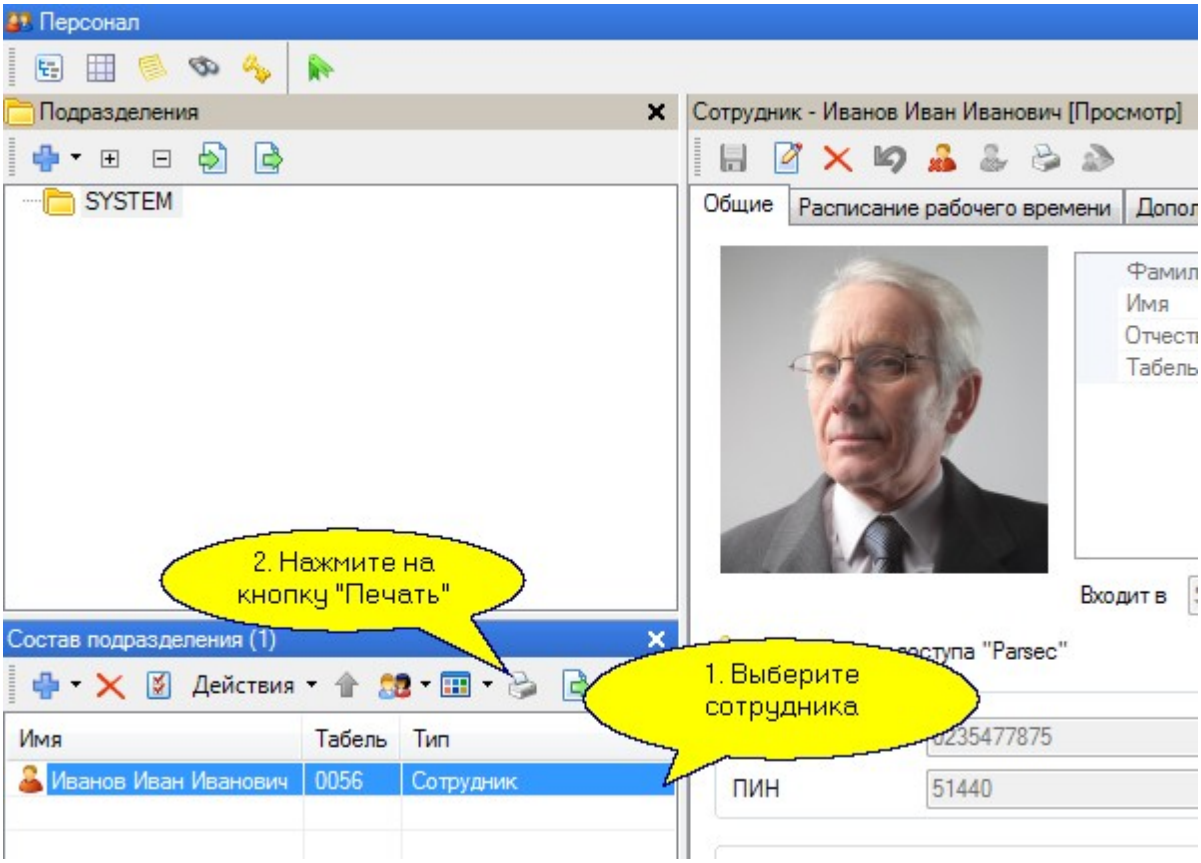
Дополнительную информацию можно найти в разделе Проверка шаблонов и печать пропусков 427

11.1.1 Проверка шаблонов и печать пропусков

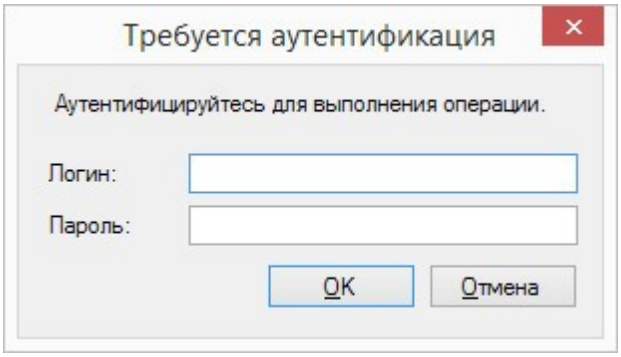
Печать пропусков осуществляется из редактора персонала. Таким же способом можно проверить шаблон на реальных данных, попытавшись напечатать одного из сотрудников. По результатам тестовой печати можно скорректировать шаблон, а затем повторить попытку.

Право оператора на печать пропусков устанавливается в редакторе операторов[194] в карточке группы операторов на вкладке *Права*. Перейдите в категорию прав "Инструменты" и в строке *Печать пропусков* выберите значение "Полный доступ".

Для просмотра печати зайдите в редактор персонала и выберите сотрудника:



После нажатия на кнопку печати, если у Вас нет прав[193] на печать пропусков, появится окно аутентификации оператора:

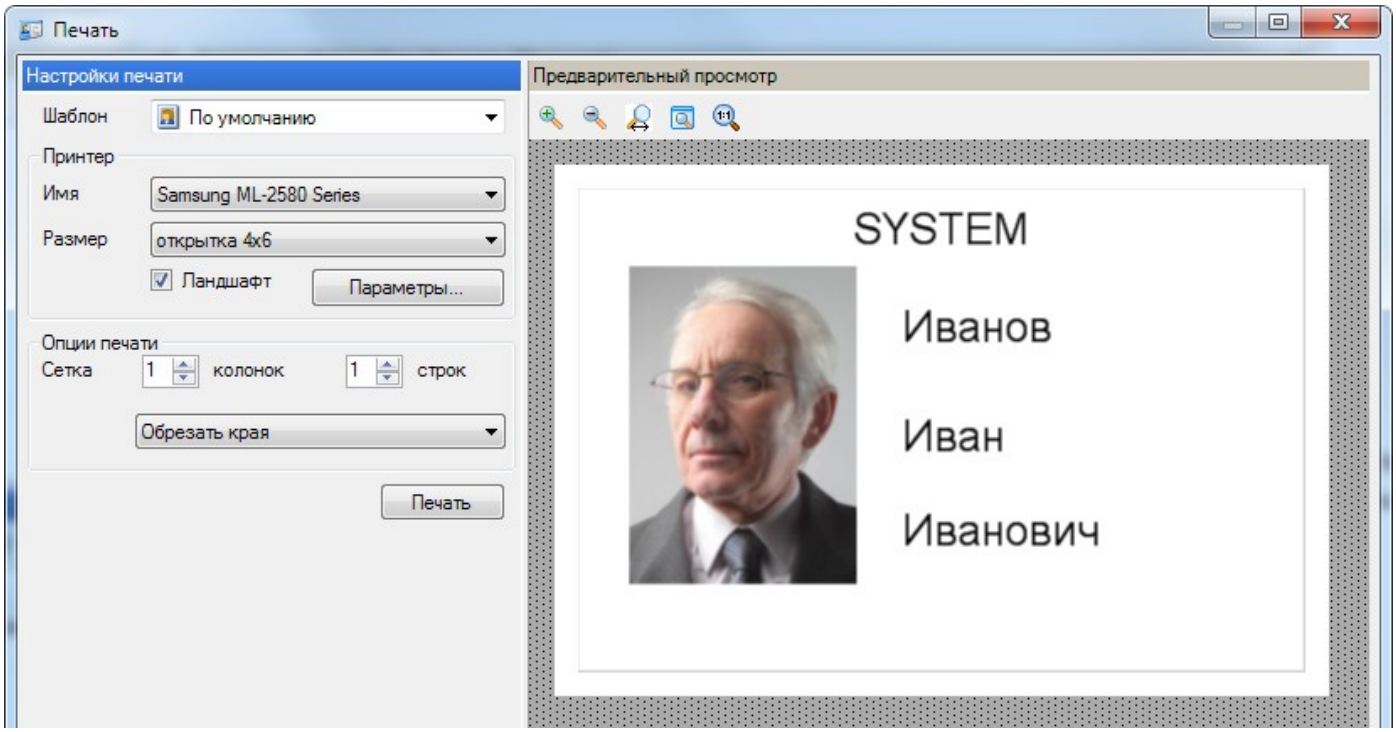


Введите логин и пароль того оператора, у которого есть право на печать, и нажмите на кнопку *ОК*. После аутентификации процедура печати может быть продолжена.

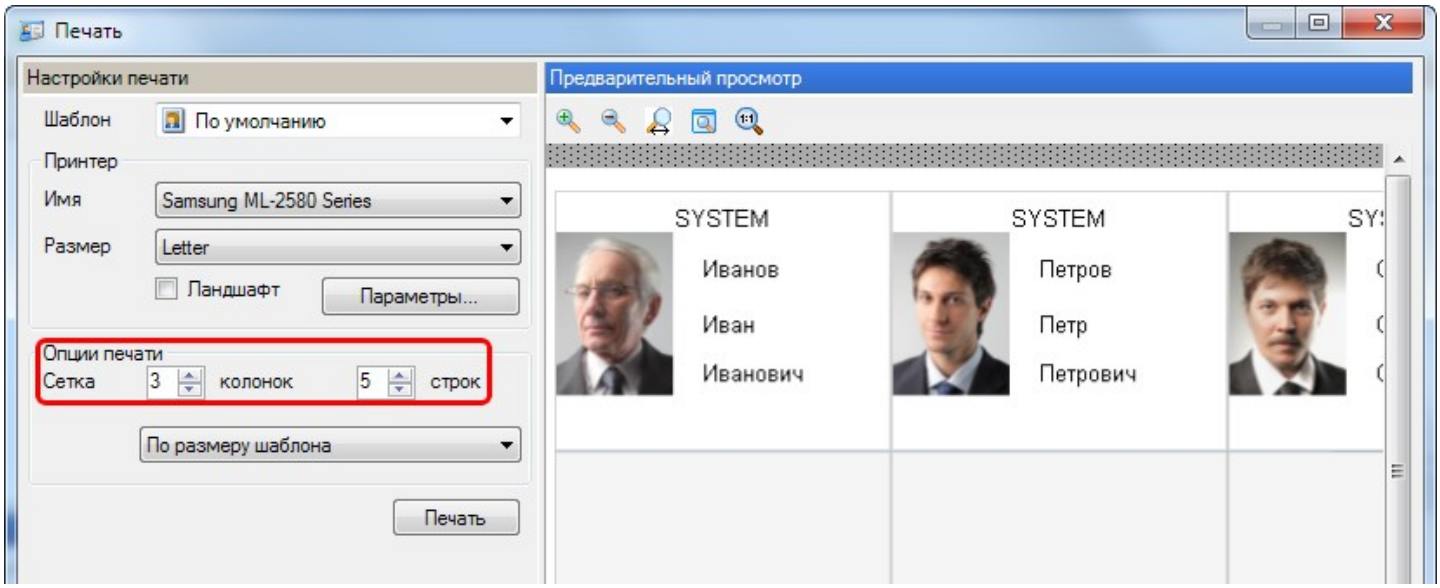
В поле *Шаблон* выберите предварительно настроенный шаблон печати. Вид пропуска будет меняться в зависимости от настроек выбираемых шаблонов.

Основная проблема, с которой придется сталкиваться - это переменная длина полей персонала, когда, например, очень длинная фамилия не помещается в отведенное для нее место.

После открытия окна предварительного просмотра перед печатью вы можете внести некоторые коррективы: выбрать конкретный принтер, выбрать размер бумаги (или карточки), определить способ помещения шаблона на лист, а также сетку печати (при печати на одном листе более одного сотрудника):

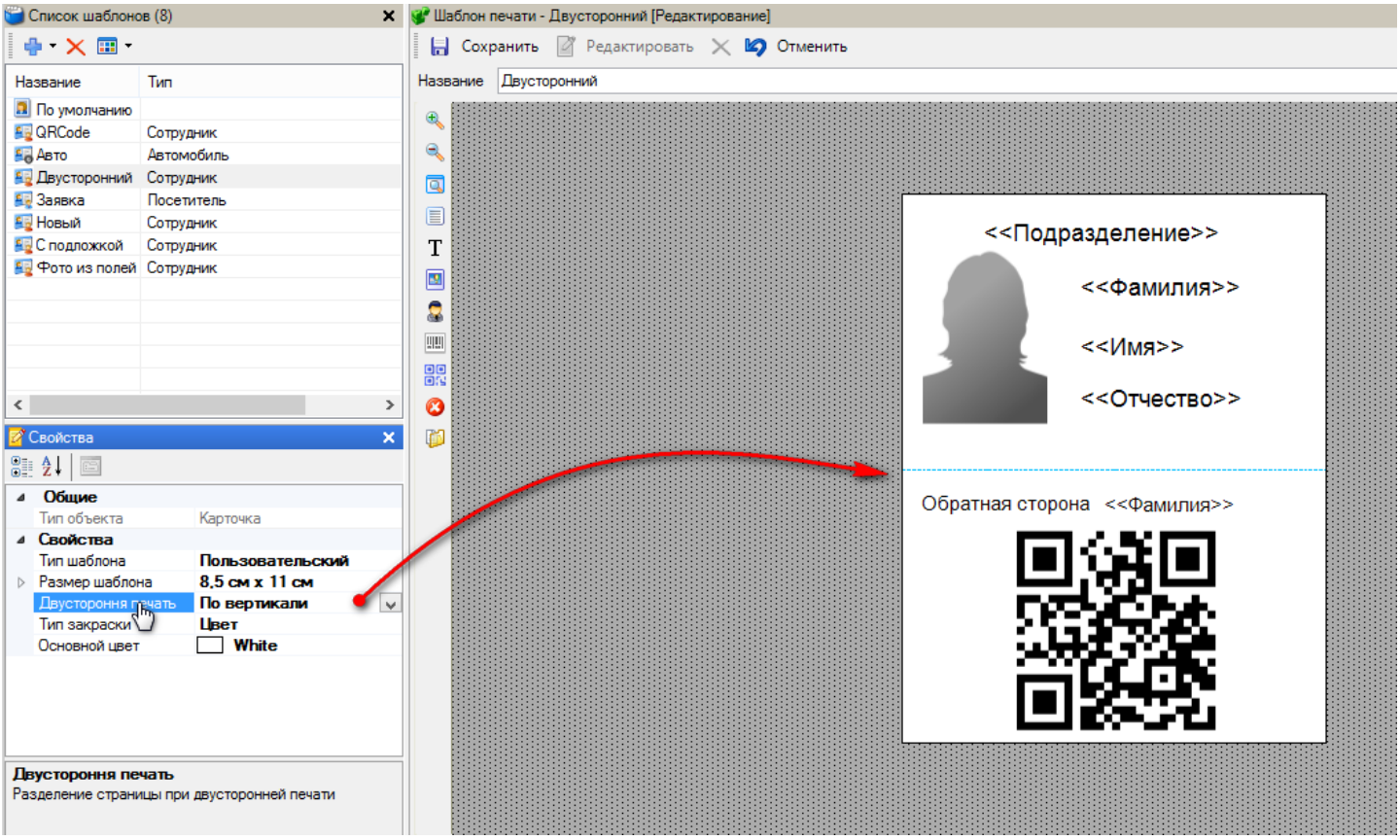


Для примера ниже показан вариант, когда на листе большого формата печатается несколько карточек сотрудников. Это возможно, например, в случаях, когда вы печатаете группу сотрудников на перфорированном листе самоклеящихся наклеек:

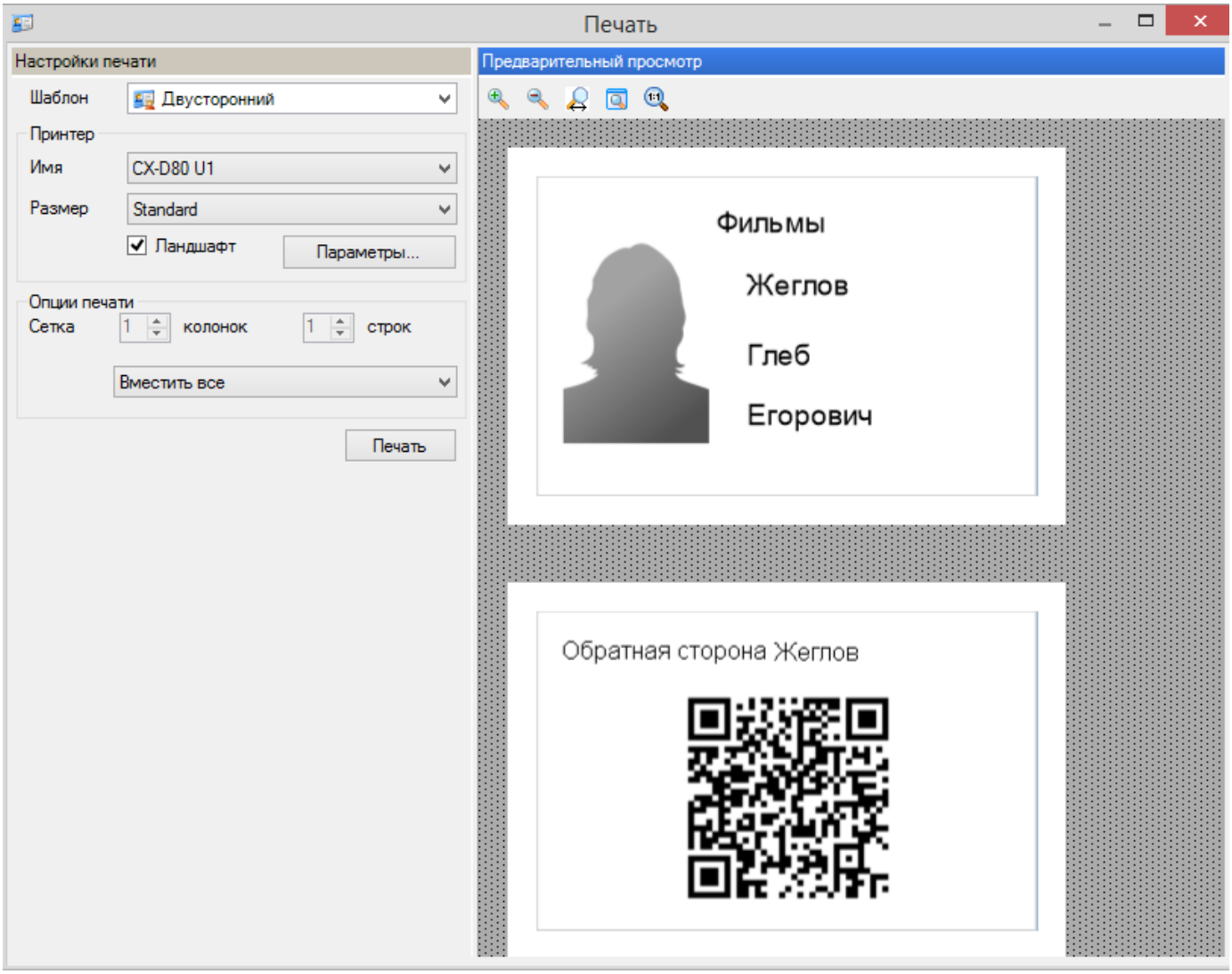


Двусторонняя печать

Если используемый принтер пропусков поддерживает двустороннюю печать, то создавать пропуска с информацией на обоих сторонах становится намного легче.
Для этого создайте шаблон и в его свойствах выберите тип шаблона *Пользовательский*.
В появившемся окне *Двусторонняя печать* выберите разделение по вертикали и отредактируйте обе стороны пропуска:

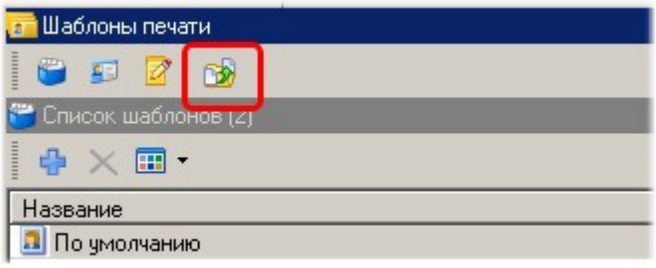


Теперь, при использовании такого шаблона и выбора принтера, поддерживающего двустороннюю печать, окно печати будет выглядеть, например, так:

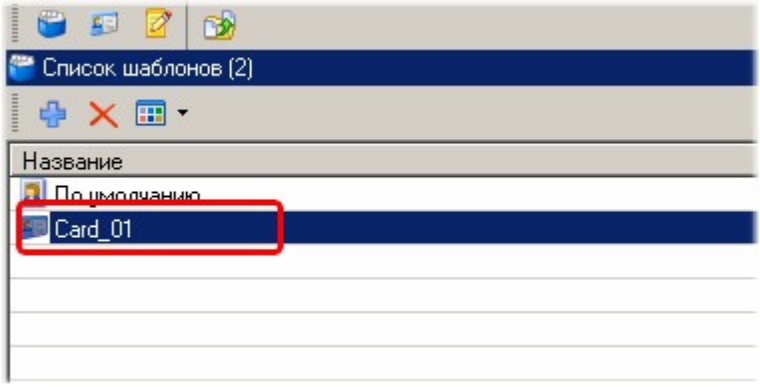


11.1.2 Импорт шаблонов из версии 2.5

Шаблоны для печати на пластиковых карточках можно импортировать из версии ParsecNET 2.5. Делается это следующим образом. В панели инструментов редактора шаблонов печати нажмите на кнопку *Импортировать из версии 2.5*:



В открывшемся окне браузера выберите файл шаблона печати пропусков версии 2.5, который необходимо импортировать, и нажмите на кнопку *Открыть*. Файлы шаблонов имеют расширение *.ap2. В результате в списке шаблонов появится новый шаблон, как показано на рисунке ниже:



При необходимости шаблон можно подредактировать, поскольку при импорте возможно некоторое изменение его внешнего вида ввиду разных принципов представления шаблонов старой и новой версий ПО.

После импорта из файла шаблон автоматически сохраняется в базе данных системы - вам не требуется предпринимать никаких дополнительных действий. При этом имя шаблона соответствует имени импортируемого файла.

11.1.3 Форматы штрих-кодов

Система позволяет печатать на пропуске в виде штрих-кода любую информацию из основных или дополнительных полей карточки субъекта доступа. Процедура добавления штрих-кодов описана в параграфе "Печать штрих-кодов на пропусках[422] "

Для печати доступен выбор следующих типов штрих-кодов (iтрих коды, в которых кодируются только цифры имеют тип данных - целочисленный. Остальные штрих коды имеют тип данных - строковый):

Линейные штрих коды:

- тип данных - целочисленный:
  - EAN-8 — кодируется 8 цифр (пример: 9031101);
  - EAN-13 — кодируется 13 цифр (пример:978020137962);
  - UPC-A — кодируется 12 цифр (пример:12121985128);
  - UPC-E — кодируется 8 цифр (пример:1234565).
- тип данных - строковый:
  - Code 128 — кодируются цифры, буквы латинского алфавита и специальные символы (пример: ABC-abc-1234);
  - Code 93 — кодируются цифры, буквы латинского алфавита и специальные символы (пример: ABC-1234-/+);
  - Code 39 — кодируются цифры (от 0 до 9), большие буквы латинского алфавита (от A до Z) и некоторые специальные символы (например, знак доллара '$'), (пример: ABC-1234);
  - Codabar — кодируются цифры, буквы латинского алфавита (A; B; C; D) (пример:A1234567890A).

Двумерные штрих коды (тип данных - строковый):

- Aztec Code — кодируются цифры, буквы латинского алфавита и специальные символы.
- Data Matrix — кодируются цифры, буквы латинского алфавита и специальные символы.
- QR — кодируются цифры, буквы латинского и кириллического алфавитов и специальные символы.

11.2 Модуль бюро пропусков

Лицензируется как PNSoft-PO [344]

Общие положения

Лицензируемый модуль "Бюро пропусков" предназначен для автоматизации процесса подачи заявок, их визирования, выдачи временных пропусков посетителям и управления проходами посетителей.

В терминах внутреннего устройства системы ParsecNET 3 модуль представляет собой ***отдельную специализированную организацию*** со своими операторами, топологией и персоналом, в качестве которого выступают посетители предприятия.

В силу специфики бюро пропусков как бизнес - процесса модуль имеет специализированную ***систему отчетов***. Кроме того, особенностью модуля является наличие ***пула карт*** (заранее подготовленных карт), являющихся пропусками для посетителей. Если в обычной организации карты закрепляются за сотрудником постоянно, то в бюро пропусков карты после использования конкретным посетителем возвращаются в пул карт и становятся вновь доступными для выдачи следующим посетителям.



Если у вас есть лицензия на бюро пропусков, то вы можете организовать в рамках системы несколько независимых бюро пропусков, например, для разных территорий.

Режимы работы и роли операторов

Для организации допуска посетителей на территорию в бюро пропусков реализованы следующие механизмы:

- ***Подача заявки на посещение предприятия***. Осуществляется с рабочих мест операторами, имеющими на это право. Такими операторами могут быть, например, секретари подразделений или отдельных компаний.
- ***Визирование (согласование) заявки*** на выдачу пропуска. может осуществляться, например, службой режима или безопасности предприятия оператором, имеющим соответствующие полномочия. Заявка на данном этапе может быть согласована или отклонена. Если заявка согласована, то она переходит в состояние ожидания выдачи пропуска.
- ***Выдача пропуска посетителю*** происходит, например, на проходной предприятия оператором, имеющим соответствующие полномочия. После выдачи пропуска заявка переходит в состояние "выдан пропуск", и код карты - пропуска загружается в соответствующие контроллеры, обеспечивая посетителю возможность прохода на территорию. Если доступ на территорию в указанное в заявке время не произошел (карта просрочена), то карта удаляется из контроллеров.
- ***Закрытие заявки*** происходит после ухода посетителя с территории. Возможно два режима закрытия заявки: вручную с рабочего места, например, охранника на проходной, либо автоматически, если на выходе установлен картоприемник, и подключенный к нему контроллер доступа формирует соответствующую транзакцию.

Таким образом, заявка на пропуск как одна из основных сущностей бюро пропусков может иметь один из следующих статусов:

- Ожидает согласования – новая заявка
- Согласована – после утверждения заявки

- Отклонена – после отказа parsec
- Выдан пропуск – после выдачи идентификатора (карты)
- Закрыта – после сдачи идентификатора (карты)

Для реализации указанных механизмов в системе прав операторов имеется специальный набор привилегий:



На приведенном рисунке определены права для группы операторов, которые могут подавать заявки на посещение. Вам необходимо создать требуемые группы операторов для всех операций с бюро пропусков в соответствии с вашим алгоритмом работы. При этом существуют следующие принципы:

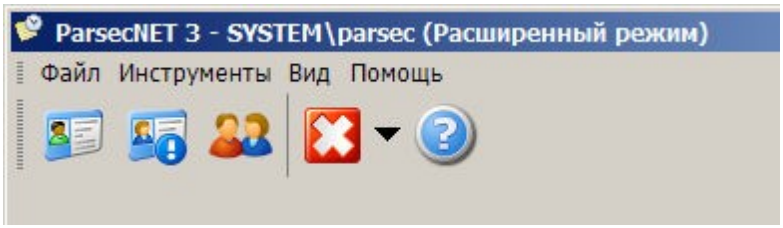
- Операторам с правом только "Выдача пропусков" запрещены редактирование заявок, редактирование посетителей, удаление заявок в статусе "Ожидает согласования";
- Операторам с правом только "Установка группы доступа"' запрещены редактирование заявок (есть возможность менять группу доступа у идентификатора), редактирование посетителей, удаление заявок в статусе "Ожидает согласования".

Административный режим

Если оператору бюро пропусков дать все права, то такой оператор сможет выполнять оформление заявки с одновременной выдачей пропуска, что характерно для небольших компаний, когда сотруднику бюро пропусков заявку подают, например, по телефону без излишних согласований. Такая операция делается буквально "в один щелчок мышкой" с единственного рабочего места бюро пропусков.

11.2.1 Инструменты бюро пропусков

Как и во всех модулях системы ParsecNET 3 консоль бюро пропусков содержит набор инструментов, обеспечивающих функционирование приложения. Ниже показана панель инструментов консоли бюро пропусков:



Слева направо находятся инструменты:


Работа с посетителями. Внесение данных посетителей в БД и выдача временных карт доступа.

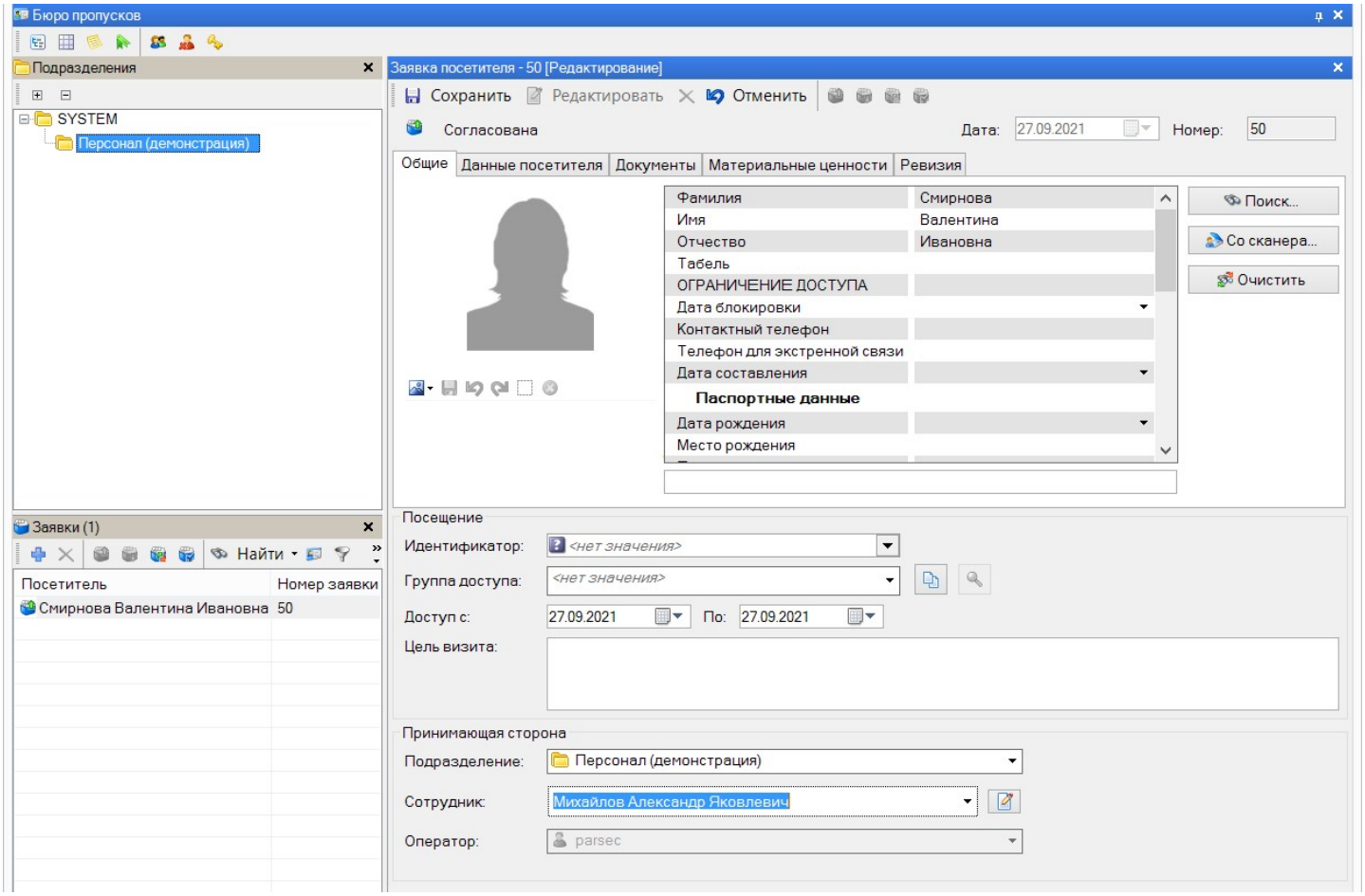

Построение отчетов по работе бюро пропусков.


Работа с персоналом организации. Внесение данных сотрудников в БД.

Завершение работы или смена оператора системы.

Вызов справки и информации о программе.

Работа с инструментами описана в разделах далее. Окно модуля в консоли *Администрирование* имеет следующий вид:



11.2.2 Инициализация бюро пропусков

Для работы бюро пропусков, как и для работы любой другой организации, необходимо произвести некоторые действия по созданию структур, требуемых для постоянной работы. Это должен сделать оператор с правами администратора бюро пропусков. Кроме того, в бюро пропусков должно быть распределено необходимое для его работы оборудование системы. Набор действий должен быть примерно следующий:

Создание групп операторов и операторов

Как и в любой организации системы, в бюро пропусков должны быть созданы свои группы операторов и операторы. Цель данного шага - распределить права между операторами, работающими в рамках бюро пропусков, например:

- Создать группу с правами только на подачу заявок. Права ограничиваются как по функциям чисто бюро пропусков, так и в части доступа к инструментам бюро пропусков.
- Создать группу для утверждения заявок.
- Создать группу для выдачи пропусков.

После создания групп в них можно ввести необходимое количество операторов. Работа с операторами и группами подробно описана с разделе Инструмент работы с операторами и группами[191].

Создание топологии

Топология нам будет необходима при создании групп доступа с тем, чтобы определять для посетителей территории, разрешенные для посещения. Например, в бизнес - центре для посетителей разных организаций - арендаторов могут быть созданы разные группы доступа, если у арендаторов имеется подсистема доступа на его территорию. Создание топологии описано в разделе Редактор топологии[203].



Для включения в топологию конкретных дверей и турникетов они предварительно должны быть распределены в бюро пропусков администратором (установщиком) системы ParsecNET 3 с помощью редактора оборудования.

Создание расписаний

Как и для постоянного персонала системы, для посетителей, скорее всего, потребуется ограничить доступ на территорию во времени, поэтому для создания соответствующих групп доступа[247] потребуется и создание расписаний с помощью редактора расписаний[213].

Создание групп доступа

После того, как будут созданы топология и расписания, необходимо создать группы доступа[247] для посетителей. Группы доступа ограничат посетителей в части перемещения как по территории, так и во времени. Например, могут быть созданы группы доступа с названиями "Посетители компании Альфа", "Посетители компании Бета" и так далее.

При создании групп доступа бюро пропусков важно включить для группы требуемый набор привилегий, так как некоторые из них влияют на правильную работу приложения. Например, только при наличии привилегии "Гостевая карта" будет обеспечена корректная работа картоприемника, если он установлен на турникете, обслуживающем выход с территории.

Подробнее о назначении привилегий можно посмотреть в документации на контроллеры, а также в разделе "Администрирование - Группы доступа - Дополнительные возможности[250] ".

Создание подразделений

Целью создания подразделений является разделение заявок и посетителей различных компаний, если они обслуживаются одним модулем бюро пропусков.

Подразделения создаются в виде иерархической структуры (дерева) аналогично тому, как это делается в редакторе персонала[255].

Создание пула идентификаторов

В бюро пропусков в постоянном обороте находится некоторое количество пропусков (идентификаторов, карт доступа), которые выдаются на время посетителю, а затем опять возвращаются в пул для последующего использования. Необходимое количество таких идентификаторов необходимо занести в бюро пропусков. Процесс описан в разделе "Создание пула идентификаторов[436] ".

Создание дополнительных полей

Для регистрации данных посетителей (например, паспортных данных) необходимо создать соответствующий набор дополнительных полей[264] для последующего использования. Делается это аналогично стандартному редактору персонала в специальной панели бюро пропусков.

Подготовка шаблонов пропусков

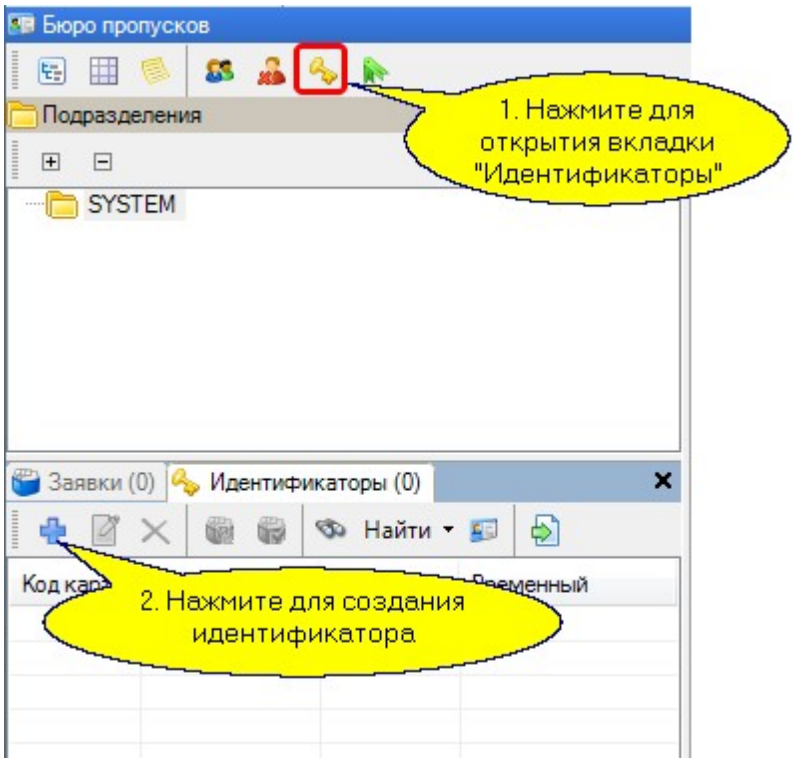
Для печати пропусков (непосредственно на картах, либо бумажных вариантов пропусков) до начала работы необходимо подготовить шаблоны пропусков. Это делается аналогично стандартному редактору шаблонов печати[417].

По завершении всех указанных подготовительных операций ваше бюро пропусков готово к работе.

11.2.3 Создание пула идентификаторов

Пул (набор) идентификаторов, которые будут выдаваться посетителям для прохода на территорию, можно создать вручную[436], а можно создать список идентификаторов в других программах, например, в Excel, сохранить его в файле формата CSV, а затем импортировать[437] этот список.

Если вкладка *Идентификаторы* в окне инструмента "Бюро пропусков" отсутствует, необходимо открыть ее, нажав на кнопку с изображением ключа на панели инструментов:

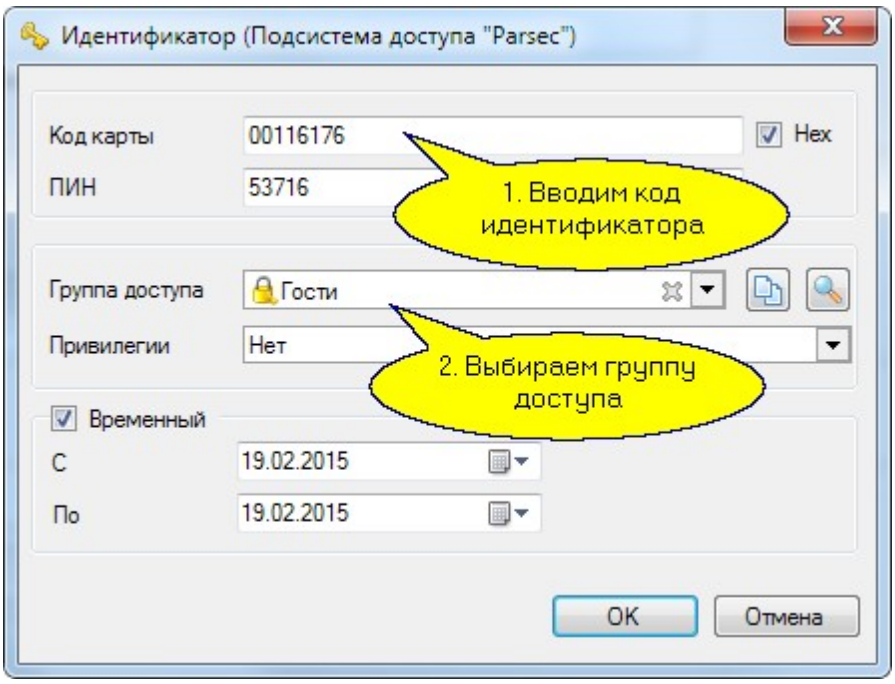


Вкладка *Идентификаторы*, в свою очередь, так же имеет панель инструментов со следующими кнопками (слева направо):

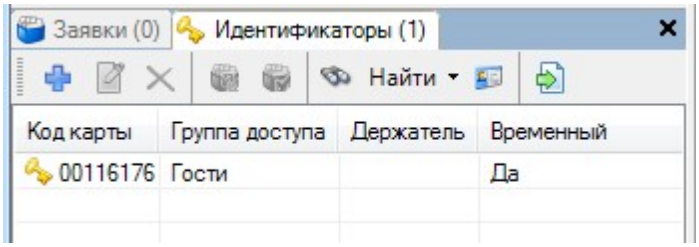
- *Создать*. Позволяет создать новый идентификатор;
- *Изменить*. Позволяет поменять идентификатору группу доступа или привилегии;
- *Удалить*. Удаляет идентификатор, выбранный на данный момент в списке;
- *Выдать идентификатор*. Присваивает идентификатор посетителю для прохода на территорию;
- *Закрыть заявку*. Закрывает заявку, по которой он был выдан посетителю, и возвращает идентификатор в пул;
- *Найти заявку или посетителя*. Позволяет найти посетителя или заявку, к которой сейчас приписан идентификатор;
- *Найти по коду*. Позволяет найти в списке идентификаторов тот, который будет поднесен к настольному считывателю.

Создание пула идентификаторов вручную

Для ввода нового идентификатора нажмите на кнопку *Создать* (синий крестик, как показано выше). Откроется диалоговое окно, в котором нужно ввести код идентификатора. Это можно сделать либо вручную, либо с помощью настольного считывателя, если он подключен к компьютеру. После ввода кода станет возможным выбрать группу доступа (в нашем случае есть только одна группа доступа):



Идентификатор занесен в пул бюро пропусков:



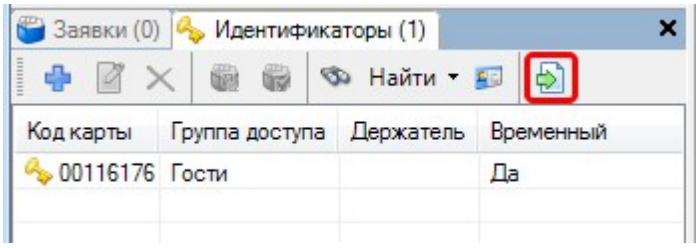
Аналогично заносим другие идентификаторы в требуемом количестве. При использовании различных групп доступа в бюро пропусков определение требуемого идентификатора при его выдаче будет происходить по названию группы доступа, к которой идентификатор приписан, поэтому постарайтесь давать группам доступа удобные осмысленные имена.

Импорт списка идентификаторов

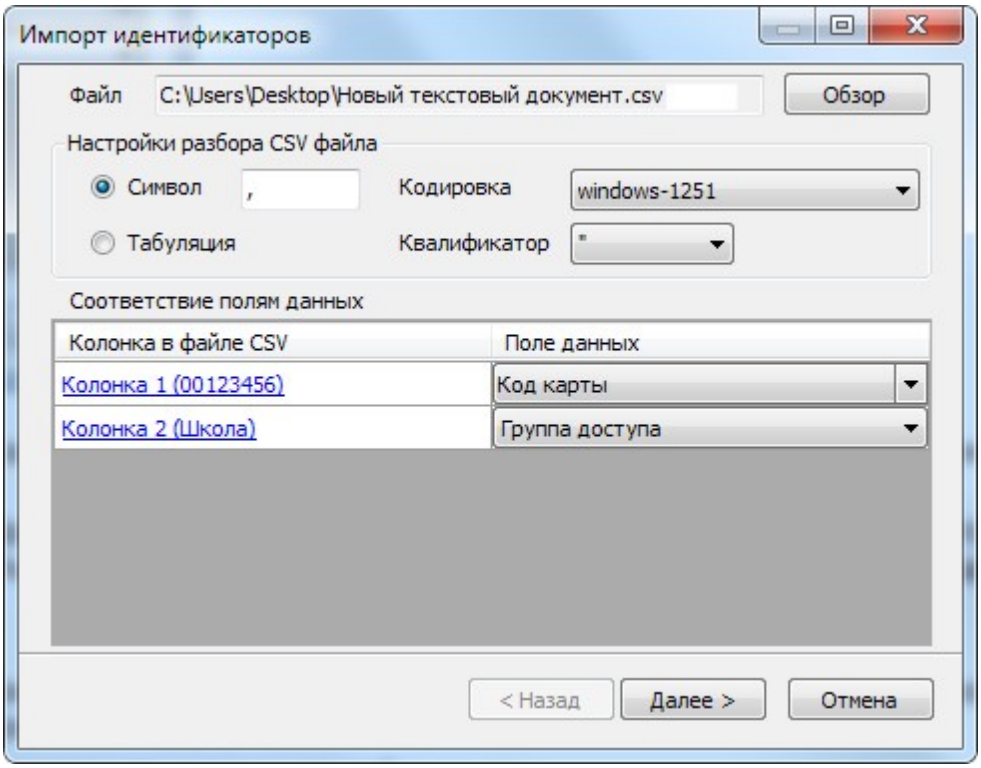
Для импорта идентификаторов используются файлы формата CSV, в котором одна запись соответствует одному идентификатору. Параметры идентификатора должны быть разделены каким-либо символом: запятыми, пробелами, точками с запятой и т.п.

Перед импортом убедитесь ,что в системе существуют группы доступа, упомянутые в CSV-файле. В противном случае система автоматически новых групп НЕ создаст и они не отобразятся рядом с импортированными кодами карт на панели идентификаторов.

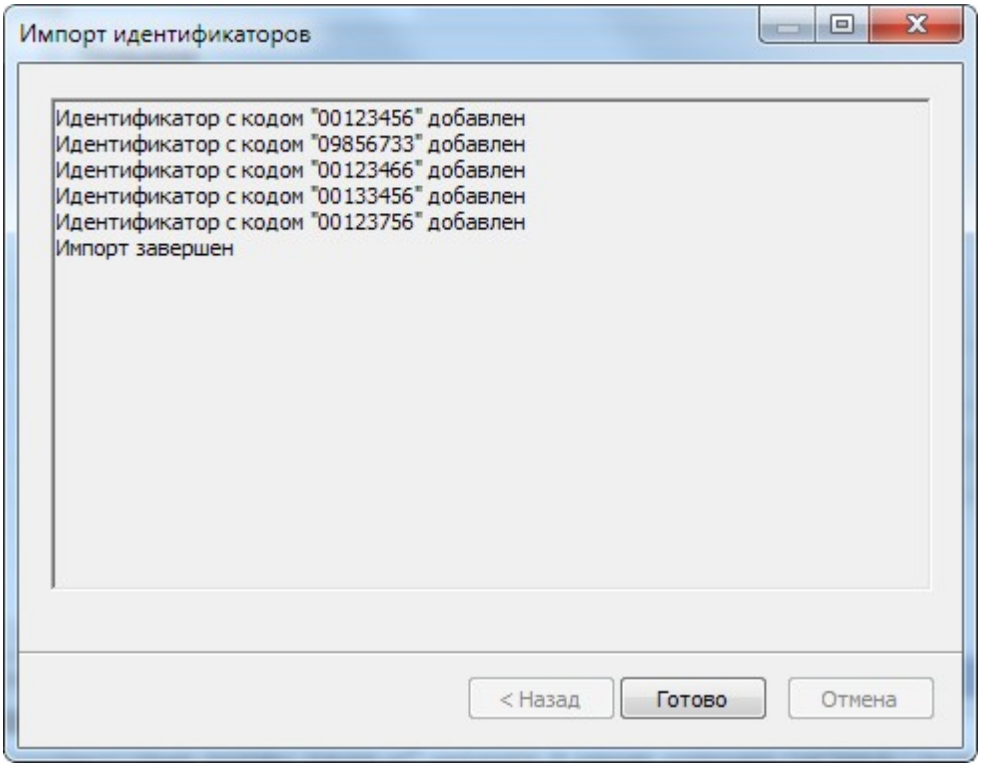
Для импорта списка идентификаторов нажмите на кнопку *Импорт…* на панели инструментов вкладки *Идентификаторы*:



В открывшемся окне установите соответствие полей в табличной части вкладки *Идентификаторы* и данных в импортируемом файле:



1. Установите переключатель в значение "Символ" или "Табуляция" в зависимости от того, как разделяются значения в файле CSV. Если нужно, введите иной символ, нежели используемая по-умолчанию запятая, например, точку с запятой;
2. Если используется квалификатор, укажите какой: двойные или одинарные кавычки. Квалификатор - это символы, обрамляющие значения импортируемых данных. Обычно применяются тогда, когда значения могут содержать знаки препинания, например, в текстовых полях. Иначе система будет воспринимать все запятые как разграничения между значениями соседствующих полей данных. по-умолчанию выбраны двойные кавычки;
3. Выберите кодировку текста в файле импорта;
4. В таблице "Соответствие полям данных" укажите в какие колонки системы должны импортироваться данные из колонок файла CSV. При этом обратите внимание, что в настоящий момент в раскрывающемся списке нужно выбирать только поля *Код карты* и *Группа доступа*. Остальные поля будут реализованы в будущем;
5. Нажмите на кнопку *Далее*. Откроется окно и запустится процедура импорта, о завершении которой сообщит появившаяся кнопка *Готово*;



В случае возникновения ошибки импорта в этом окне будет представлено описание ошибки.

Создание списка идентификаторов и сохранение его в файл CSV описано в следующем разделе[439].

Дополнительно работа с идентификаторами рассмотрена в разделе Работа с заявками[441].

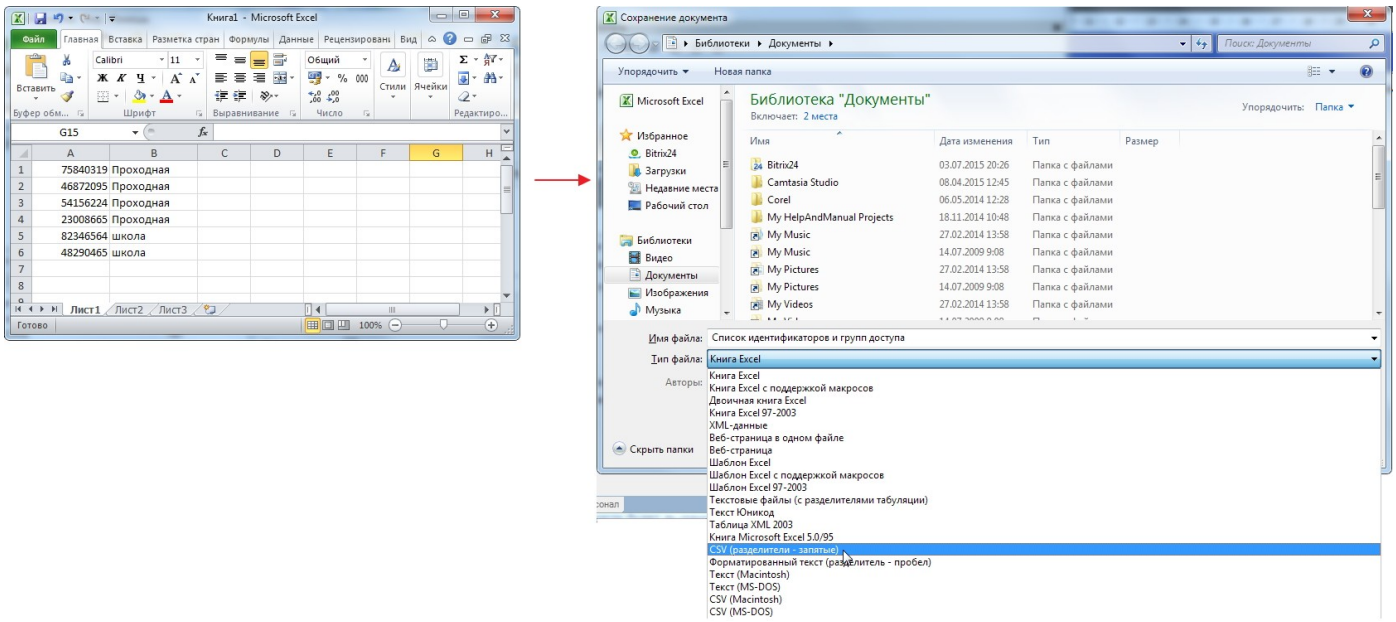
Начиная с версии 3.12.1117 появилась возможность выдавать посетителям идентификаторы в виде QR-кода без создания пула идентификаторов.

Чтобы начать использование QR-кодов в Бюро пропусков, необходимо задать настройки в Редакторе системных настроек[356].

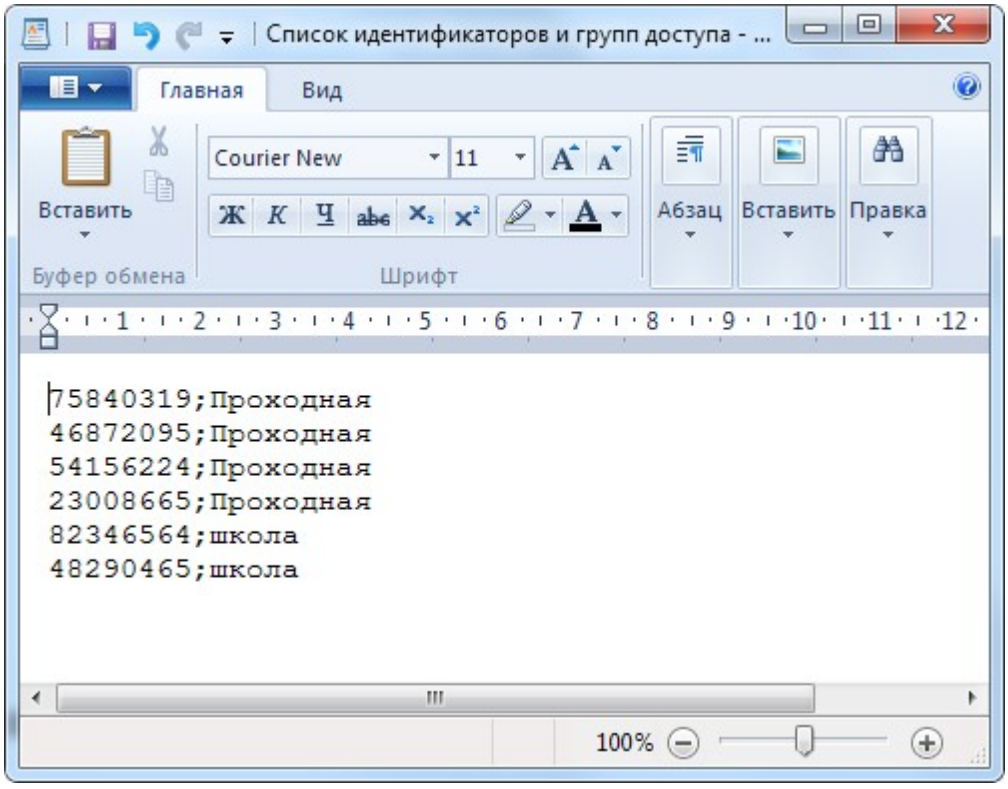
11.2.3.1 Создание списка идентификаторов во внешних программах

Файл формата CSV, содержащий список индентификаторов и групп, к которым они относятся, может быть создан вручную или выгружен из каких-либо сторонних систем контроля доступа. Создание списка идентификаторов и сохранение его в файле формата CSV в данном разделе будет рассматриваться на примере программы MS Excel.

Занесите коды карт в одну колонку, а группы доступа, которым они принадлежат, - в другую. Параметры каждого идентификатора записывайте в новой строке. После этого сохраните файл, выбрав тип файла "CSV (разделители-запятые)".



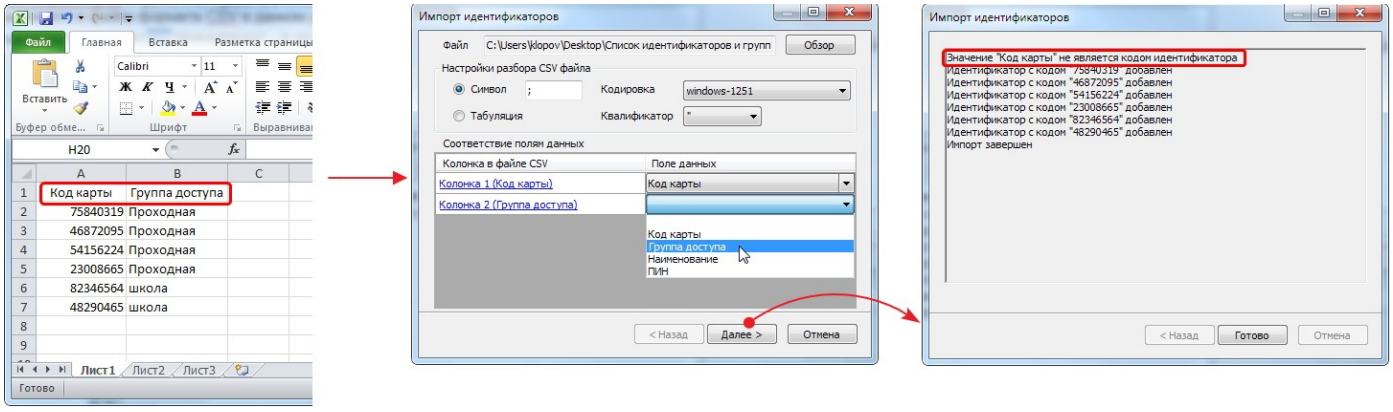
Сохраненный файл может иметь следующую структуру содержимого:



Как можно видеть на рисунке выше, CSV-файл содержит список строк, в которых перечислены коды карт и названия групп доступа, разделенные точкой с запятой. Одна строка определяет один идентификатор. Для импорта идентификаторов в систему ParsecNET 3 из CSV-файла он должен иметь подобную структуру. Допускается использование других разделителей.

Сама процедура импорта идентификаторов описана в параграфе[437] раздела "Создание пула идентификаторов".

Первую строку в CSV-файле, которая должна была бы содержать заголовки колонок, рекомендуется не создавать. Если она все-таки создана и сохранена при экспорте списка в CSV, это сделает импорт более удобным, но при импорте будет выдано сообщение, что значение первой строки не является корректным идентификатором (проигнорируйте это сообщение и продолжайте работу).



11.2.4 Работа с заявками

Здесь мы опишем основные моменты работы с бюро пропусков. Цикл работы на примере одного посетителя будет состоять из следующих шагов:

Шаг 1. Создание заявки

Предполагаем, что в дереве подразделений мы находимся в ветке своего подразделения, например, компании "Альфа". При правильном назначении областей видимости при входе в систему оператор, подающий заявку, автоматически попадает в свое подразделение.

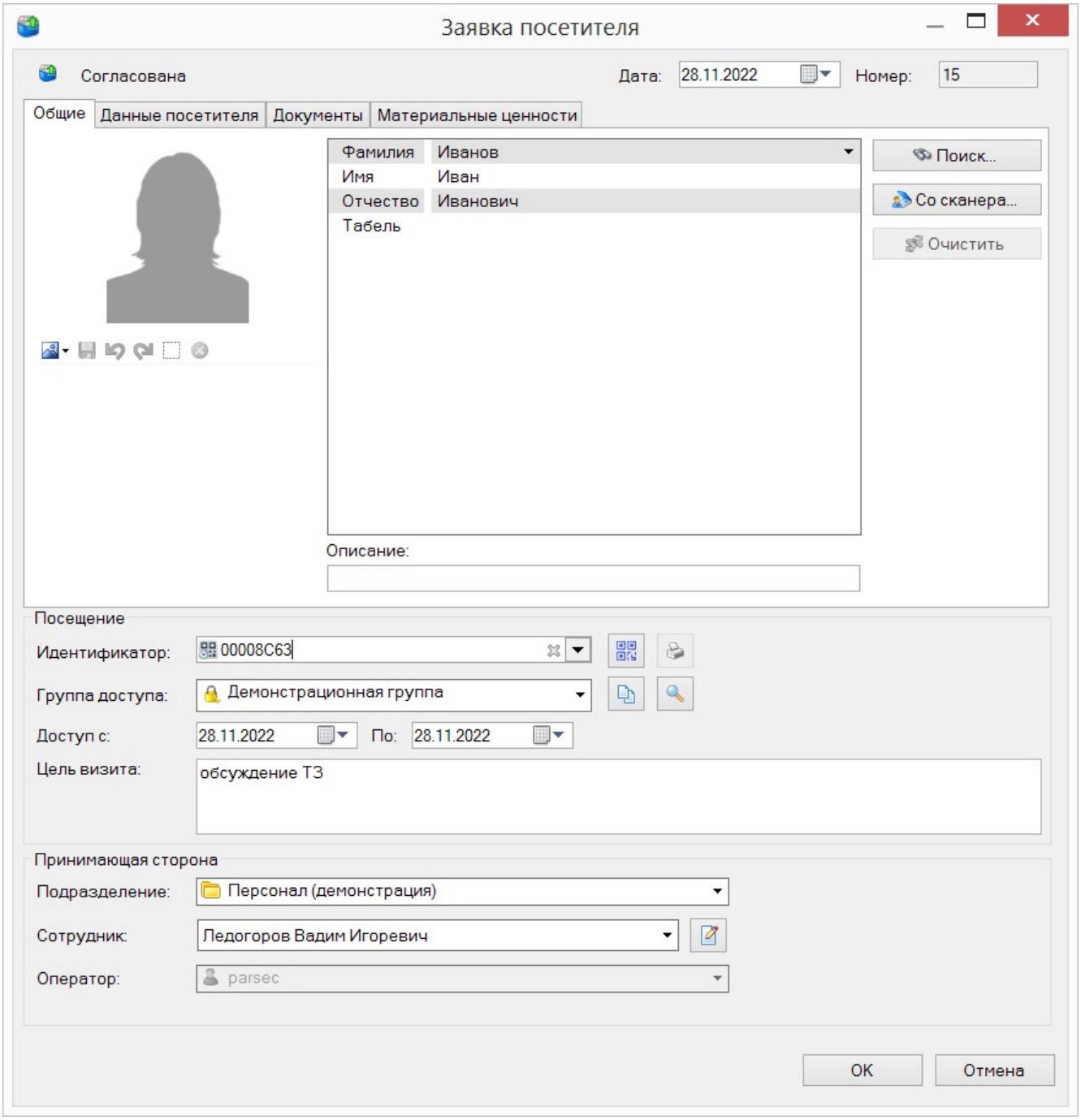
На вкладке заявок бюро пропусков нажмите на кнопку *Создать* и в открывшемся диалоговом окне введите ФИО посетителя и время посещения (в нашем примере - 1 день).

Также можно ввести необязательные данные:

- На вкладке *Данные посетителя* отображаются дополнительные поля;
- На вкладке *Документы* к заявке можно приложить любой файл, в том числе изображение со сканера, с камеры или из выбранной директории;
- На вкладке *Материальные ценности* можно записать ценные вещи, которые имеет с собой посетитель. Установкой флажков можно отметить, какие из перечисленных ценностей он имеет право вносить и какие - выносить.

Если посетитель пришел не первый раз, то можно не вводить его данные заново, а воспользоваться кнопкой *Поиск* в правой части окна. Или начните вводить символы фамилии в поле *Фамилия* и из раскрывшегося списка посетителей выберите нужного.

Заполненная заявка посетителя может выглядеть примерно так:



Если создающий заявку оператор имеет право на ее согласование, то заявка будет сразу иметь статус *Согласована*.

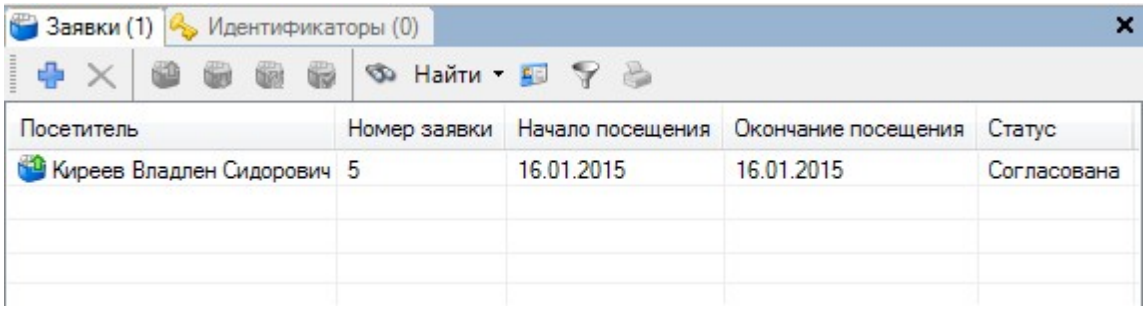
При наличии у создающего заявку оператора прав на выдачу идентификатора, будет активен раскрывающийся список *Идентификатор*, содержащий все номера из пула идентификаторов. Выбранный в этом списке идентификатор будет сразу присвоен посетителю. Если оператор, создающий заявку, не имеет прав на выдачу идентификатора, то раскрывающийся список *Идентификатор* будет неактивен.

При выборе идентификатора в поле ниже отобразится его группа доступа. Оператор (при наличии соответствующего права) может изменить группу доступа или присвоить ее, если этого не было сделано ранее при занесении идентификатора в пул.

В блоке *Принимающая сторона* можно указать конкретное подразделение, в которое пришел посетитель. Тогда заявка будет размещена в папке это подразделения в дереве подразделений в окне модуля, также принимающее подразделение будет отображаться в отчетах, например, в отчете "По посетителям".

В поле *Сотрудник* можно начать вводить фамилия принимающего сотрудника и выбрать его из раскрывшегося списка. Также можно оставить это поле пустым. Если принимающий сотрудник указан, то по нажатию на кнопку справа от этого поля откроется окно с данными этого сотрудника.

После создания заявка появляется в списке заявок и отображается в карточке заявки. В списке заявок это выглядит следующим образом:



Если оператор не имеет права согласования заявки, то ее статус - "Ожидание согласования".

Если оператор имеет право на согласование заявки, но не имеет права на выдачу идентификатора, то статус заявки будет "Согласована".

Если у оператора есть и право на согласование, и право на выдачу идентификатора, то при выдаче идентификатора статус заявки будет "Выдан пропуск", а если идентификатор не выдан, то "Согласована".

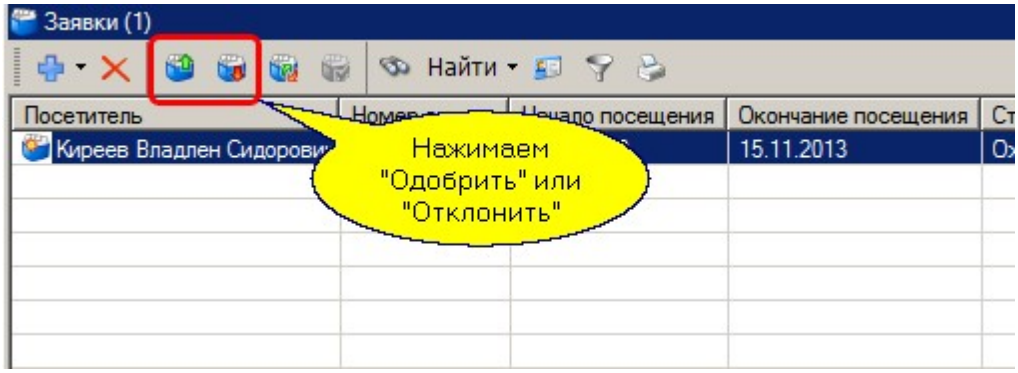
В столбце "Посетитель" можно искать заявку, вводя первые символы фамилии посетителя. В столбце будут оставаться только те фамилии, которые начинаются с введенных символов. Это стандартная функция ОС Windows.

Кнопки на панели инструментов списка заявок имеют следующее назначение (слева направо):

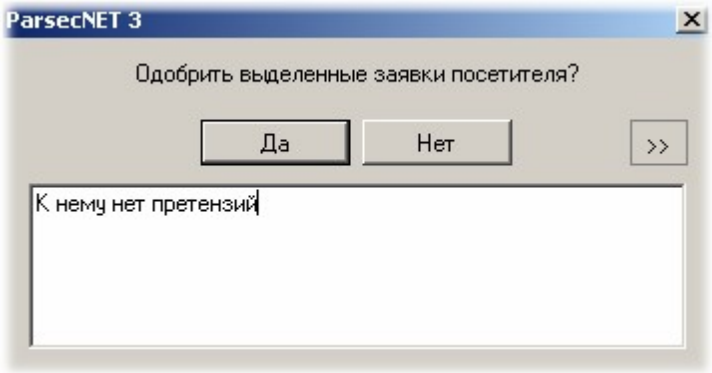
- *Создать заявку.* Создается новая пустая заявка.
- *Удалить заявку.* Удаляются только заявки со статусом "Ожидание согласования"
- *Одобрить.* Согласует заявку, разрешая выдачу пропуска.
- *Отклонить.* Запрещает посещение по заявке.
- *Выдать идентификатор.* Только для согласованных заявок. Сотрудник, имеющий право согласования заявки, может сразу воспользоваться данной функцией.
- *Закрыть заявку.* Заявка остается в архиве заявок.
- *Найти* посетителя или идентификатор, связанный с данной заявкой.
- *Найти заявку* по коду идентификатора.
- *Отфильтровать* заявки в списке по их статусу. Также можно отфильтровать только актуальные заявки, т.е. заявки, срок действия которых попадает на текущую дату.
- *Печать пропуска* по данной заявке.

Шаг 2. Согласование заявки

Согласовать (одобрить) заявку может только оператор, имеющий соответствующие права. Для одобрения заявки в списке заявок или в карточке конкретной заявки, ожидающей согласования, достаточно нажать на кнопку *Одобрить* (или *Отклонить* для отказа в посещении).



При нажатии на любую из кнопок появляется диалог с подтверждением выполнения операции, в котором можно сделать свой комментарий (например, причина отклонения заявки). В дальнейшем этот комментарий можно будет увидеть на вкладке *Ревизия* конкретной заявки. Диалог выглядит следующим образом:

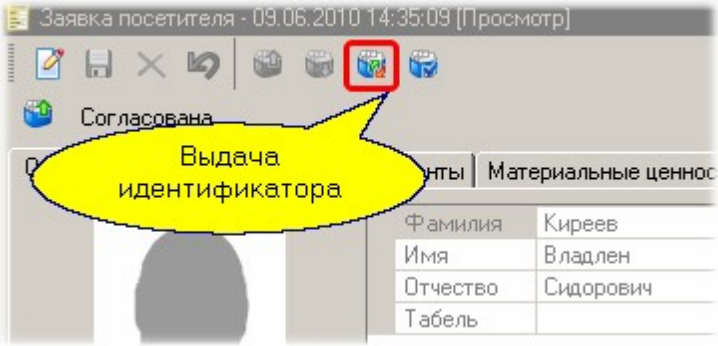


Можно одновременно одобрить несколько заявок, выделенных в списке с использованием мышки при нажатой клавише Ctrl.

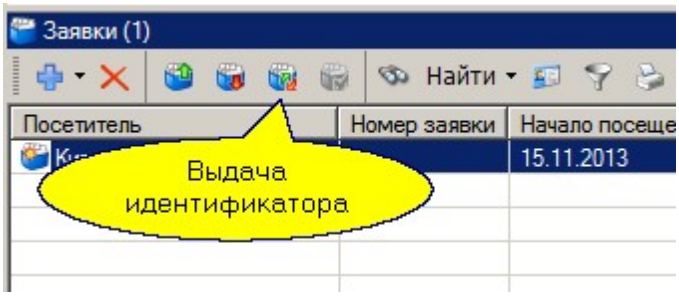
Статус заявки становится "Согласована", и теперь по ней может быть выдан пропуск.

Шаг 3. Выдача пропуска

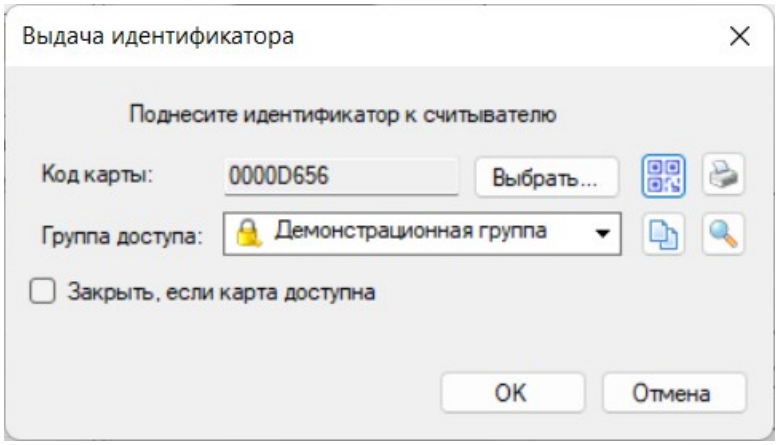
Выдача пропуска осуществляется оператором с соответствующими привилегиями. Выдать идентификатор можно как на карточке конкретной заявки:



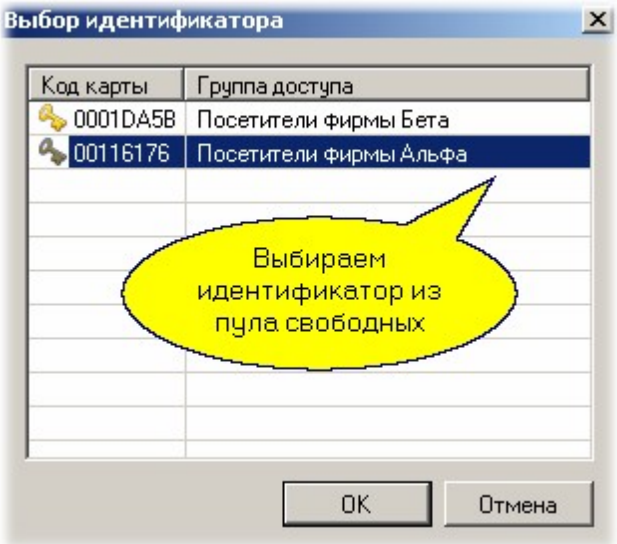
Так и через список заявок:



После выдачи идентификатора последний приписывается к посетителю, а статус заявки становится "Выдан идентификатор". Идентификатор выдается через показанный ниже диалог.

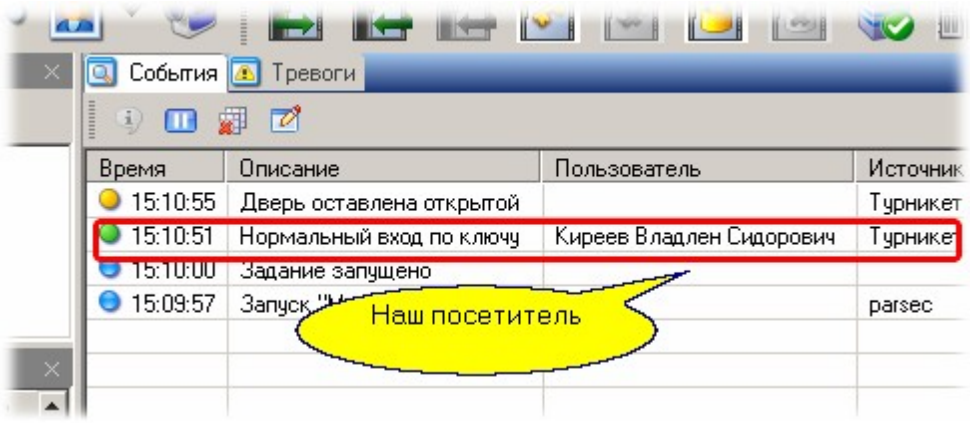


При установленном флажке *Закрыть, если карта доступна* диалоговое окно закроется автоматически после поднесения карты к настольному считывателю. Однако, если идентификатора этой карты нет в пуле, диалог останется открытым. Также можно выбрать идентификатор из пула свободных идентификаторов, нажав на кнопку *Выбрать...*

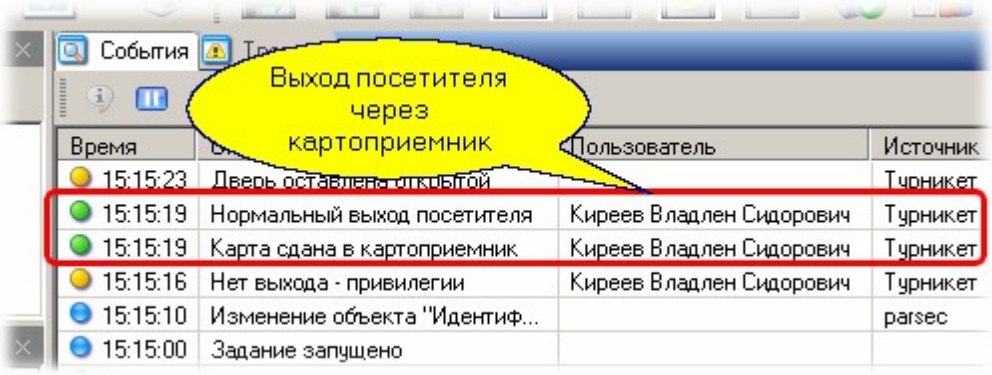


Также можно выдать посетителю в качестве идентификатора QR-код, при условии, что проведена соответствующая настройка в Редакторе системных настроек. Для этого нажмите на кнопку *Выдать QR-код* (подробнее о работе с QR кодами смотри раздел Настройки Бюро пропусков[356]).

Теперь наш посетитель может входить на территорию по точкам прохода, соответствующим его группе доступа. Если открыть монитор событий для нашего бюро пропусков, то можно будет наблюдать проходы посетителя:



Мы настроили систему на турникет с картоприемником, поэтому при выходе посетителя с территории формируются следующие транзакции:



Шаг 4. Закрытие заявки

При выходе через картоприемник с изъятием карты посетителя заявка закрывается автоматически, и сданный идентификатор возвращается в пул свободных для последующего использования.

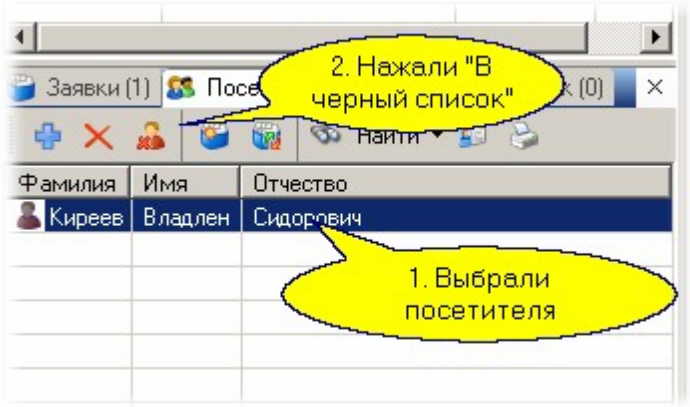
Если же картоприемника нет, то заявку после сдачи пропуска (например, вахтеру на выходе с территории) необходимо закрыть вручную с помощью нажатия на кнопку *Закрыть заявку* в карточке заявки или в списке заявок.

Помимо этого, заявка автоматически закрывается в случае занесения посетителя в черный список.

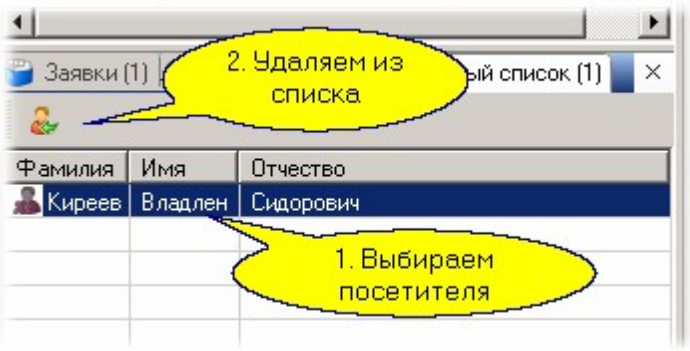
11.2.5 Черный список

Посетители бюро пропусков хранятся в базе данных на случай, если они опять посетят предприятие. Однако любого посетителя можно перенести из обычного списка в "черный список", из которого посетителя нельзя включить в заявку для очередного посещения.

Для перевода посетителя в "черный список" достаточно выбрать его в списке посетителей и нажать на кнопку *В черный список*:



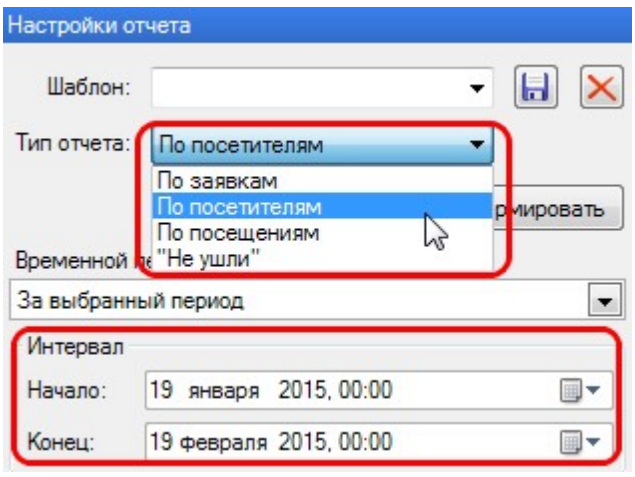
Посетитель исчезает из списка посетителей и появляется в черном списке. При необходимости его вновь можно "восстановить в правах", выделив в черном списке и нажав на кнопку *Из черного списка*:



11.2.6 Отчеты бюро пропусков

Общие положения

Бюро пропусков в силу специфики своей работы имеет и специальный набор отчетов, позволяющих анализировать работу бюро пропусков. Тип отчета выбирается из списка *Тип отчета*. Возможные варианты выбора показаны на рисунке:



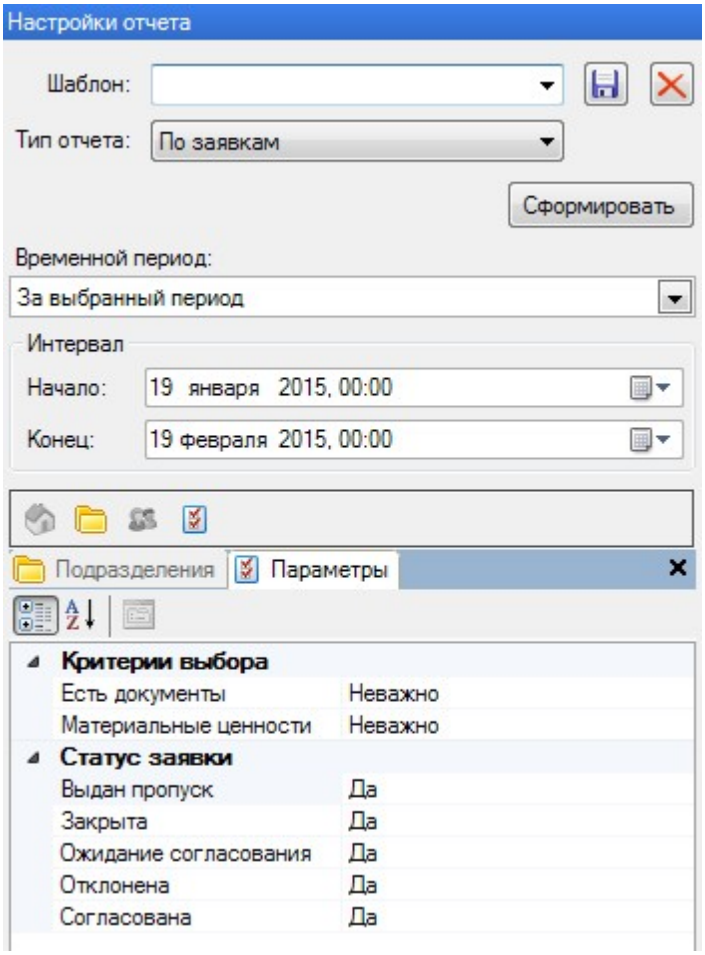
Для каждого типа отчетов существует набор критериев, по которым отбираются данные в отчет. Во всех типах отчетов (кроме "Не ушли") в качестве одного из критериев выступает диапазон времени, за который формируется отчет. Т.к. срок действия заявки указывается с точностью до суток, то в параметрах начала и конца интервала отчетов по заявкам и отчета "Не ушли"

учитывается только дата, без учёта времени. Для отчетов по посетителям и по посещениям интервал может учитываться[449] с точностью до минут.

Рассмотрим остальные критерии всех типов отчетов.

Отчет по заявкам

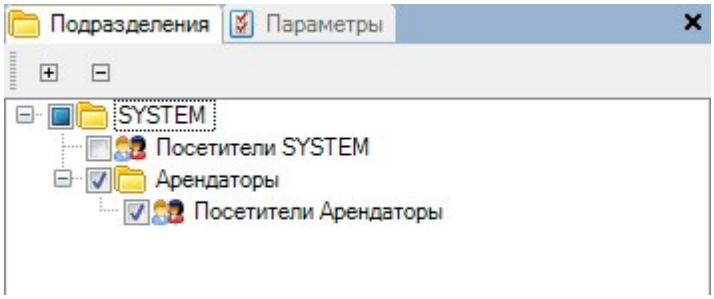
Выводит список и статус заявок бюро пропусков, время действия которых попадает в указанный интервал времени. Для данного типа отчета критерии выбираются на двух вкладках.



На вкладке *Параметры* выбираются следующие критерии:

- Наличие у посетителя документов. Варианты:
  - "Да" - в отчет отбираются заявки посетителей, к которым прикреплены документы в виде файлов, изображений и т.п.;
  - "Нет" - в отчет отбираются заявки посетителей без прикрепленных документов;
  - "Неважно" - в отчет отбираются заявки обоих предыдущих вариантов.
- Наличие у посетителя материальных ценностей. Варианты:
  - "Да" - в отчет отбираются заявки посетителей, к которым прикреплены какие-либо материальные ценности;
  - "Нет" - в отчет отбираются заявки посетителей без прикрепленных материальных ценностей;
  - "Неважно" - в отчет отбираются заявки обоих предыдущих вариантов.
- Статус заявки. Варианты:
  - "Да" - в отчете отображаются заявки, имеющие указанный статус;
  - "Нет" - такие статусы не учитываются при отборе заявок в отчет.

На вкладке *Подразделения* выбираются подразделения, заявки которых попадут в отчет. Выбор осуществляется установкой или снятием флажка. На рисунке ниже выбраны заявки только для подразделения "Арендаторы":



После нажатия на кнопку *Сформировать* строится отчет в соответствии с выбранными критериями.

Отчет по посетителям

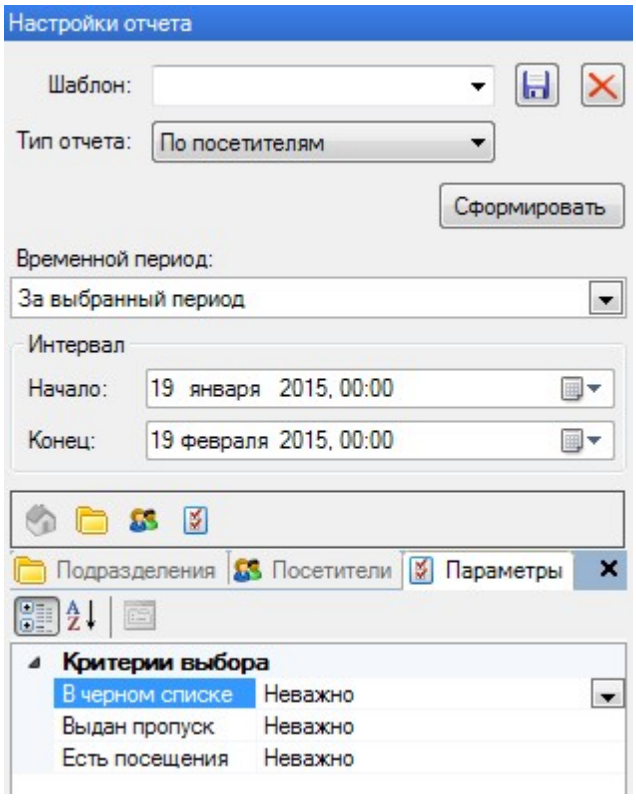
В отчет по посетителям, отбираются посетители, срок действия заявок которых попадает в указанный интервал. Для этого отчета существуют особенности отбора:

- Если в параметре “Выдан пропуск“ установлено значение “Да“, то проверяется временной интервал выдачи пропуска с учетом минут.
- Если в параметре “Есть посещения“ установлено значение “Да“, то проверяется временной интервал прохода (входа или выхода) в установленный интервал с учетом минут.

Например, на рисунке ниже указан интервал с 00 часов 00 минут 19 января по 00 часов 00 минут 19 февраля.

Если параметр "Выдан пропуск" установлен в "Да", то в отчет НЕ попадет посетитель, которому пропуск выдан 19 февраля в 15.30. Чтобы такой посетитель попал в отчет, конец интервала необходимо установить 19 февраля 23:59.

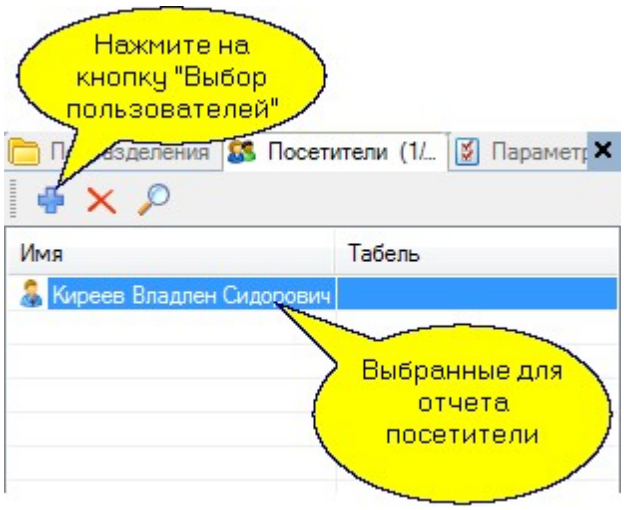
Кроме выбора интервала, также имеются вкладки для выбора параметров.



На вкладке *Параметры* выбираются следующие параметры отчета:

- Находится ли посетитель в черном списке. Варианты:
  - "Да" - в отчет попадут только те посетители, которые находятся в черном списке;
  - "Нет" - в отчет попадут только посетители, не находящиеся в черном списке;
  - "Неважно" - в отчет попадут все посетители, независимо от пребывания в черном списке.
- Выдан ли посетителю пропуск. Варианты:
  - "Да" - в отчет попадут те посетители, которым выдан пропуск в указанный интервал с учетом минут.
  - "Нет" - в отчет попадут посетители, которым не выдан пропуск;
  - "Неважно" - в отчет попадут все посетители, независимо от наличия пропуска или времени его выдачи.
- Есть ли у посетителя посещения. Варианты:
  - "Да" - в отчет попадут те посетители, у которых уже есть посещения (вход или выход) в указанный интервал с учетом минут;
  - "Нет" - в отчет попадут посетители, у которых еще нет посещений в заданный период;
  - "Неважно" - в отчет попадут все посетители, независимо от посещений.

На вкладке *Подразделения* выбираются те подразделения, посетителей которых необходимо включить в отчет. Либо на вкладке *Посетители* можно отобрать для отчета конкретных посетителей, нажав на кнопку *Выбор пользователей*:



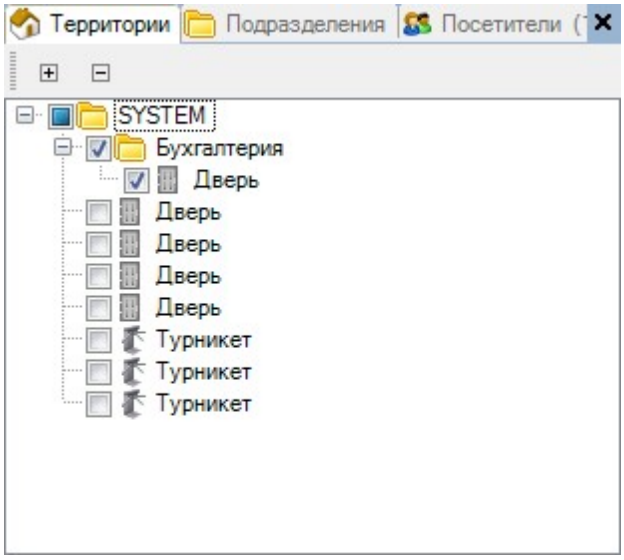
Комбинируя условия отбора, мы получим требуемые нам данные в сформированном отчете.

После нажатия на кнопку *Сформировать* строится отчет в соответствии с выбранными критериями.

Отчет по посещениям

Данный вид отчета также имеет вкладки для выбора критериев отбора фактов посещений в формируемый отчет:

- Выберите подразделения по аналогии с тем, как это было в отчете по заявкам;
- Выберите посетителей, посещения которых нас интересуют, как это было в отчете по посетителям. При этом время выдачи пропуска и время посещения отбираются в отчет с учетом минут (см. подраздел Отчет по посетителям 449);
- Выберите территории, посещения которых вас интересуют:



После нажатия на кнопку *Сформировать* формируется отчет в соответствии с выбранными критериями.

Отчет "Не ушли"

Данный отчет позволяет получить информацию о посетителях, находящихся на заданной территории в данный момент. Имеется только один критерий для формирования отчета: территория, по которой нас интересуют не покинувшие ее посетители.

Работа с шаблонами

Использование шаблонов при формирование отчетов бюро пропусков аналогично использованию его в других отчетах. Данный материал рассмотрен отдельно в разделе Работа с шаблонами в отчетах[314].

11.2.7 WEB-заявки

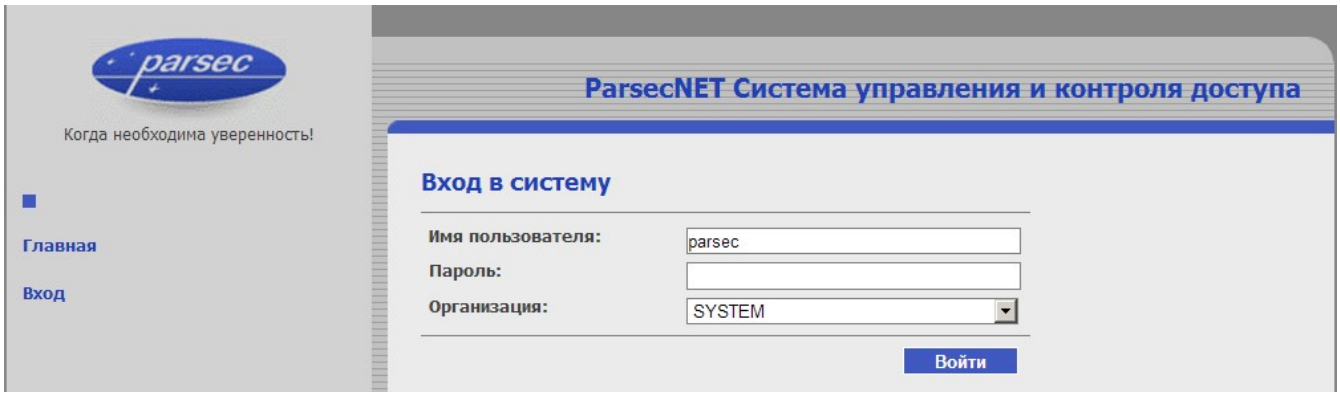
Система ParsecNET 3 позволяет сотрудникам *Бюро пропусков* создавать заявки, используя WEB-интерфейс, что позволяет обойтись без установки системы на компьютер.

Для корректной работы Системы с WEB-интерфейсом настойчиво рекомендуется убедиться, что в ОС Windows включен[33] компонент ASP.NET (Панель управления\Все элементы панели управления\Программы и компоненты\Включение и отключение компонентов Windos). Особенно актуально это для ОС Windows 10 и выше.

Чтобы войти в WEB-консоль, наберите в адресной строке своего браузера (в примере рассматривается Chrome) *http://<server_name>:10102/PassRequests,* где вместо <server_name> впишите IP-адрес или имя сервера Parsec.

Также можно перейти в сетевую папку *<server_name>\ParsecWorkstationSetup\web*, где вместо <server_name> укажите IP-адрес или имя сервера системы ParsecNET 3. В этой папке находятся ярлыки веб-форм. Скопируйте на рабочий стол или в любое удобное место ярлык "Parsec Time Corrector". Двойным щелчком по этому значку можно открывать страницу формы внесения поправок:

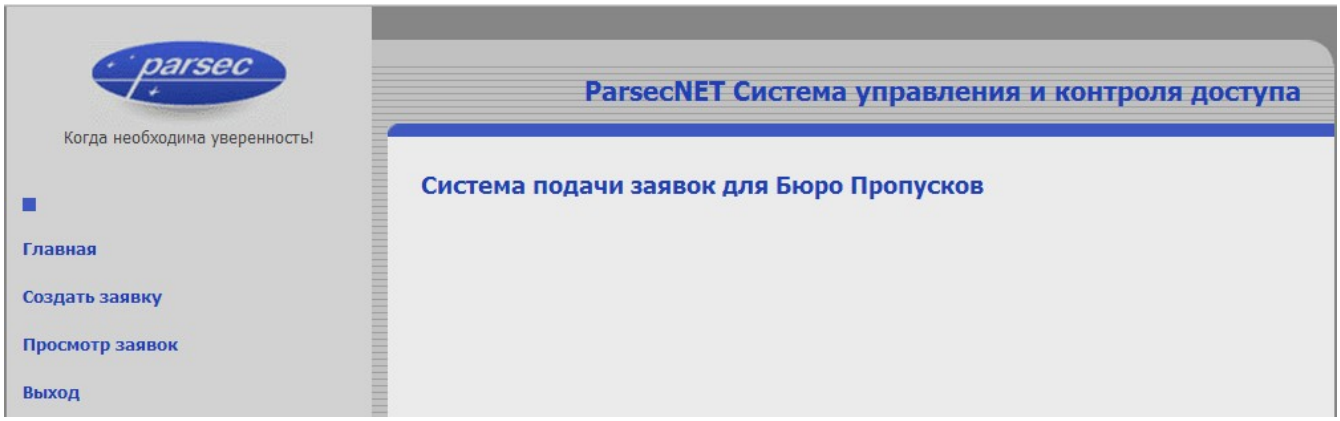
После нажатия клавиши *Enter* на странице браузера появится форма авторизации:



Введите имя пользователя и пароль, аналогичные тем, которые используются для входа в систему ParsecNET 3, а из раскрывающегося списка - свою организацию, либо корневую организацию SYSTEM.

Нажмите на клавишу *Enter* или на кнопку *Войти*. Откроется главная страница (см. рис. ниже).

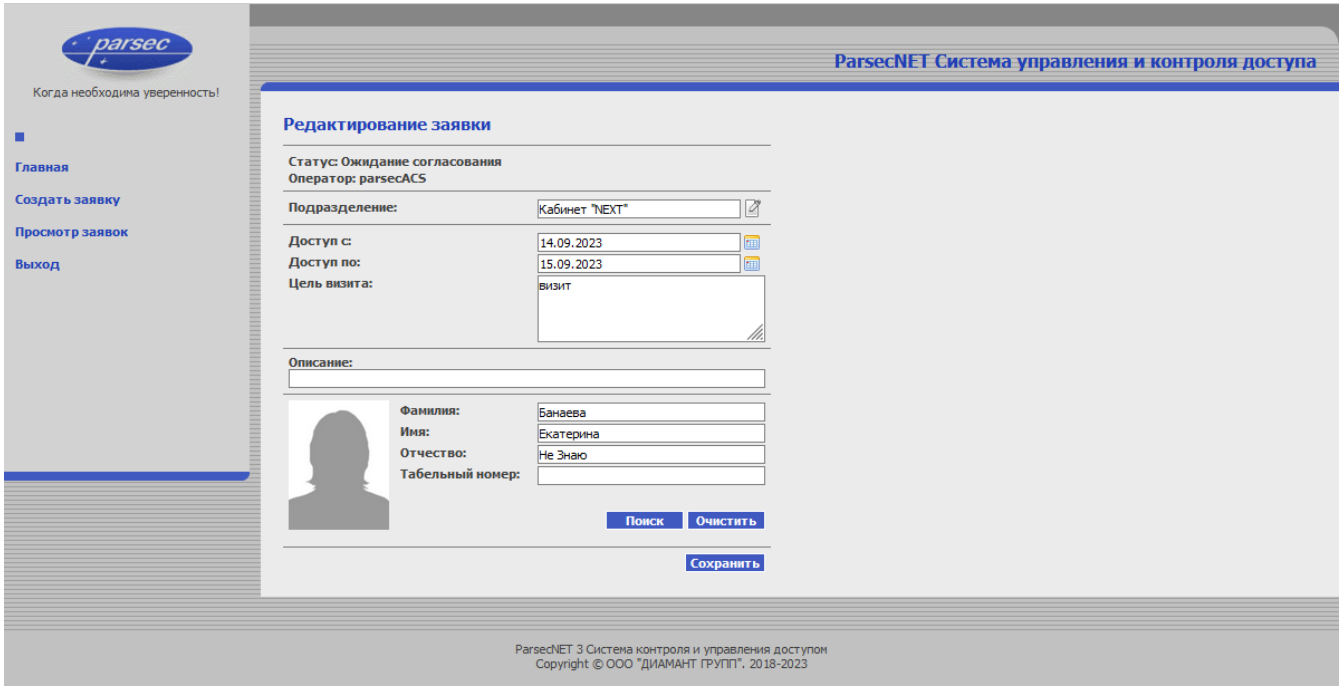
В целях повышения безопасности не рекомендуется сохранять пароли в браузере.



Создание заявки

Чтобы создать новую заявку, выполните следующие действия:

1. Нажмите на ссылку *Создать заявку* на левой панели главной страницы. Откроется окно создания заявок:

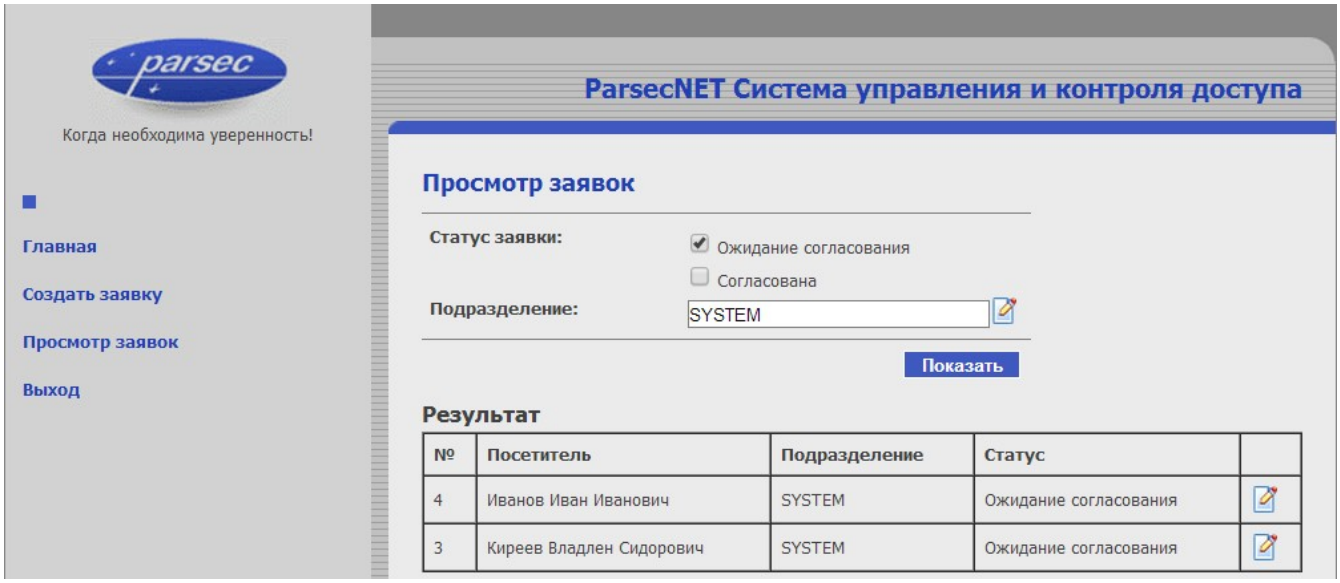


2. Выберите подразделение, в которое пришел посетитель, нажав на кнопку . (Если не выбрать подразделение, то при попытке создания заявки система сообщит об ошибке);
3. В раскрывающемся календаре *Доступ с* укажите дату, начиная с которой посетителю будет предоставлен доступ на территорию организации. По умолчанию выбрана текущая дата;
4. В раскрывающемся календаре *Доступ по* укажите дату, до которой посетителю будет предоставлен доступ на территорию организации. По умолчанию выбрана текущая дата;
5. В текстовом поле введите краткое описание цели посещения;
6. В блоке общие данные заполните поля ФИО и, при необходимости, табельного номера.

Также можно, введя первые буквы фамилии, провести поиск по БД, нажав на кнопку *Поиск*. В открывшемся окне *Посетители* выберите нужное лицо и нажмите на кнопку *Выбрать*. Все данные о нем будут отображены в соответствующих полях.

Просмотр заявок

Для просмотра заявок перейдите на соответствующую страницу, нажав на ссылку *Просмотр заявок*.



При установке флага *Ожидание согласование* в таблицу будут отобраны заявки, для которых ожидается одобрение ответственных лиц. А при установке флага *Согласована* - уже одобренные ими.

Нажав на кнопку справа от поля *Подразделение* можно открыть список и выбрать конкретное подразделение, заявки на посещение которого будут отображены в таблице.

После нажатия на кнопку *Показать* в таблицу будут отобраны заявки, удовлетворяющие заданным условиям.

Нажатие на кнопку справа от строки посетителя открывает страницу соответствующей заявки.

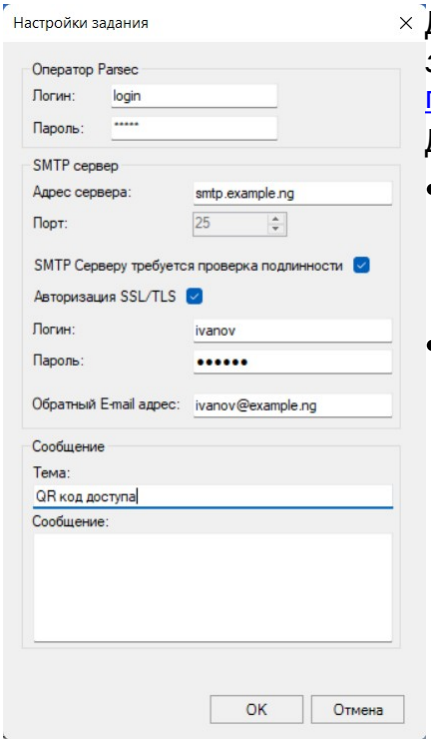
11.2.8 Отправка QR-кода посетителям

Система позволяет отправить назначенный посетителю идентификатор в виде QR-кода доступа двумя способами:

- посредством задания на указанный e-mail;
- на мобильное устройство посетителя по запросу к заранее созданному Telegram-боту[393] . Если идентификатор в заявке уже назначен, бот пришлет его QR-код в ответ на любое сообщение в личном чате.
  Если идентификатор еще не назначен, но заявка согласована и в настройках Бюро пропусков[356] установлен флажок *Выдавать идентификатор посетителю по команде Telegram бота*, то Telegram-бот самостоятельно выдаст "QR-код Parsec" в системе ParsecNET и передаст его в чат.

Описание настроек для обоих способов приведено ниже.

Отправка QR-кода по e-mail



Данное окно открывается при нажатии на кнопку *Настройка задания по отправке QR-кода* в разделе "Настройки Бюро пропусков[356] " редактора системных настроек.

Для настройки задания выполните следующие шаги:

- В блоке *Оператор Parsec* введите имя и пароль пользователя, от имени которого будет запускаться задание (это не обязательно должен быть оператор, создающий данное задание);
- В блоке *SMTP сервер* заполните поля:
  - *Адрес сервера* - введите адрес своего почтового сервера;
  - *Порт* - введите номер порта для подключения к SMTP серверу;
  - *SMTP серверу требуется проверка подлинности* - при установке флажка станут доступными поля:
    - *Авторизация SSL/TLS* - при установленном флажке авторизация будет производиться по клиентским TLS/SSL сертификатам. При установке флажка порт SMTP сервера выбирается автоматически, значение в поле *Порт* не учитывается;
    - *Логин* - имя пользователя для SMTP сервера;
    - *Пароль* - пароль для SMTP сервера;
    - *Обратный E-mail адрес* - укажите адрес электронной почты для получения системных сообщений и т.п.

- В блоке *Сообщение* заполните поля *Тема* и *Сообщение* (при необходимости). Посетитель будет получать на почту, указанную в дополнительном поле своей карточки, сообщение с заданной темой и сообщением и с прикрепленным QR кодом доступа;
- Нажмите на кнопку *ОК*. Задание сохранится и его можно будет просмотреть в Редакторе заданий.

Если в Редакторе заданий на вкладке *События* в разделе *Аудит изменений* снять флажки у событий "Создание объекта "Заявка посетителя" и "Создание объекта "Заявка посетителя", то сообщения посетителям можно будет отправлять только вручную по нажатию кнопки[454] *Отправить QR код на E-mail*. Кнопка появляется после генерации QR кода для посетителя.

Отправка QR-кода посредством Telegram

Для правильного взаимодействия СКУД Parsec и мессенджера Telegram выполните следующие действия:

0. Создайте Telegram-бота[393];
1. В редакторе персонала создайте для посетителей дополнительное поле[264], в котором будут отображаться их мобильные номера. С названием, например, "Мобильный телефон" (тип "строковый");
2. Скачайте файл *TelegramQRBot_publish.zip* - https://disk.yandex.ru/d/jqBa_pEellyVdA;
3. Распакуйте содержимое в папку *C:\Program Files\MDO\ParsecNET 3*. Папка распаковки может быть любая, но рекомендуется указанная ранее;
4. В Системе откройте Редактор системных настроек и перейдите в раздел Настройка бюро пропусков[356];
5. Включите режим редактирования и установите флажок *Разрешить использование идентификаторов типа "QR-код "Parsec" в заявках Бюро пропусков*;
6. Выберите группу доступа тех посетителей, которые будут получать QR-коды через Telegram. Кончено, группу необходимо создать заранее. Например, группу доступа "Посетители центрального офиса";
7. Установите флажок *Мобильный телефон* и выберите дополнительное поле, созданное на шаге 1;
8. Установите флажок *Выдавать идентификатор посетителю по команде Telegram бота*. Тогда, если идентификатор доступа еще не назначен, но заявка согласована, то Telegram-бот самостоятельно выдаст "QR-код Parsec" в системе ParsecNET и передаст его в чат;
9. Нажмите на кнопку *Настройки Telegram бота* и сохраните файл *appsettings.json* в папке, в которую был распакован архив *TelegramQRBot_publish.zip* на шаге 3 (по умолчанию *C:\Program Files\MDO\ParsecNET 3*);
10. Откройте любым текстовым редактором файл *appsettings.json* (например, Блокнотом) и вставьте в следующие строки нужные значения:
    - *ParsecLogin* - логин оператора для входа в ПО PasrecNET3;
    - *PasrecPassword* - пароль оператора для входа в ПО PasrecNET3;

    Логин и пароль необходимо вводить того оператора, в соответствии с правами которого бот будет генерировать QR-коды Parsec. Это значит, что доступ посетителей будет ограничен теми подразделениями и территориями, которые входят в область видимости[194] данного оператора. А минимальный набор прав должен включать:

- для работы бота без установки флажка *Выдавать идентификатор посетителю по команде Telegram бота*:
  - Редактор персонала - Просмотр;
  - Запуск бюро пропусков;
  - Редактор групп доступа - Просмотр;
  - Запуск Монитора событий.
- для работы бота с возможностью выдачи идентификатора по его команде дополнительно необходимы права:
  - Редактор персонала - Полный доступ;
  - Бюро пропусков - Подача заявок;
  - Бюро пропусков - Выдача пропусков.

- *TelegramBotToken* - API-ключ созданного ранее бота.
  Если у вас его нет, в Telegram перейдите в раздел *Контакты* и в строке поиска наберите *@BotFather*. Наберите команду */mybots* и в появившемся списке кнопок выберите *API Token*.
  Не рекомендуется использовать команду */token*, так как при этом API бота пересоздается заново;

11. Сохраните изменения в файле *appsettings.json*;
12. Запустите приложение *TelegramQRBot.exe* в той папке, куда был распакован архив на шаге 3. Для корректной работы функции отправки QR-кодов через Telegram это приложение должно быть запущено.

На этом настройка ПО ParsecNET 3 закончена.

Теперь можно создавать посетителей и указывать в дополнительном поле *Мобильный телефон* номера их мобильных устройств.

Посетитель, найдя в Telegram созданного бота, отправляет ему любое сообщение (даже одну букву) и в ответ получает идентификатор доступа в виде QR-кода (при условии, что его заявка согласована).

11.3 Модуль учета рабочего времени

Лицензируется как PNSoft-AR[344]

Лицензируемый модуль учета рабочего времени (**УРВ**) анализирует данные, связанные с персоналом предприятия: количество отработанных часов, приход, опоздание и прочее, позволяя создавать так называемые "бизнес-отчеты". В данной версии формы отчетности максимально приближены к существующим в России стандартам и рекомендациям, в первую очередь это относится к табелю учета рабочего времени за месяц, который формируется в формате формы Т-13.

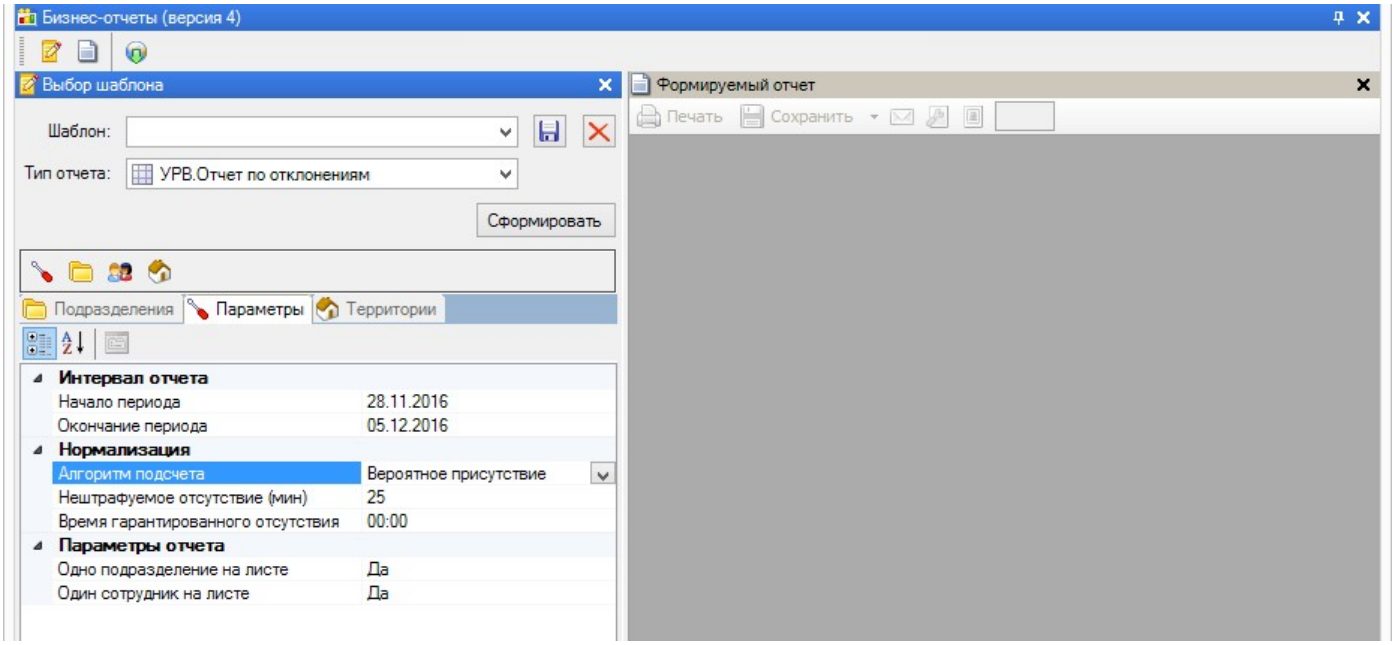


Прежде, чем пытаться получить отчет УРВ, обязательно познакомьтесь с разделом "Особенности учета рабочего времени [461]***", чтобы полученный результат Вас удовлетворил.***



В настоящее время в системе присутствуют две версии модуля УРВ. Настоятельно рекомендуется использовать для формирования отчетов УРВ версию 4. Старая версия более не поддерживается.

Консоль редактора бизнес-отчетов запускается командой "Пуск -> Все программы -> Parsec 3 -> Отчеты".



Панели генератора отчетов УРВ

Модуль УРВ (версия 4) в стандартной конфигурации состоит из следующих элементов:

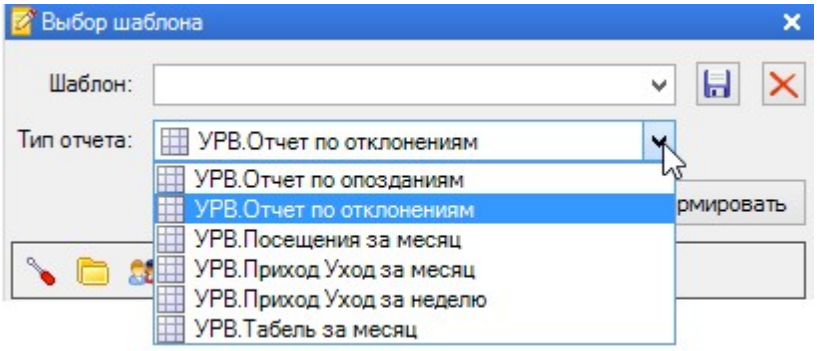
- Панель инструментов (вверху);
- Панель выбора шаблона и типа отчета (слева вверху);
- Панель выбора параметров отчета (слева внизу);
- Панель формируемого отчета (справа).

В свою очередь, панель выбора параметров отчета имеет вкладки для выбора параметров отчета:

- Подразделения - выбор подразделений, по сотрудникам которых будет составлен отчет;
- Пользователи - выбор конкретных пользователей, по которым будет составлен отчет;
- Параметры - настройка временных и иных параметров отчета;
- Территории - выбор территорий, события на которых будут учитываться при составлении отчета.

Типы отчетов

Модуль учета рабочего времени может формировать следующие отчеты, выбираемые в раскрывающемся списке *Тип отчета*:



- "Отчет по автомобилям"[474]. Время въезда и выезда автомобилей;
- "Отчет по опозданиям"[476]. Опозданием система считает приход на работу позже начала периода обязательного рабочего времени. При составлении отчета можно задать период "разрешенного опоздания", приход в рамках которого не будет отражаться в отчете;
- "Отчет по отклонениям"[477] позволяет получить информацию по таким нарушениям и отклонениям, как опоздания, прогулы, нарушение режима регистрации (типа "нет входа", "нет выхода" и так далее). Формируется за неделю;
- "Посещения за месяц"[478] отображает посещение сотрудником своего рабочего места в каждое число месяца;
- "Приход/уход за месяц"[480] показывает время прихода, время ухода и отработанное время для выбранных сотрудников в каждый день месяца;
- "Приход/уход за неделю"[480] показывает время прихода, время ухода и отработанное время для выбранных сотрудников в каждый день недели;
- "Табель за месяц"[482] представляет собой хорошо всем знакомый табель учета рабочего времени по форме Т-13;

В старой версии модуля УРВ доступны также следующие типы отчетов:

- *"Уход раньше времени"[493] отображает случаи, когда сотрудник ушел раньше, чем закончился период его обязательного рабочего времени в данный день;*
- *"Табель за неделю"[503] - модификация месячного табеля с привязкой к неделе и несколько измененной по отношению к Т-13 формой самого отчета.*
- *"Отчет по посещениям"[489] отражает прогулы сотрудников. Прогулом, с т.з. системы, является отсутствие сотрудника на работе в период обязательного рабочего времени. При этом на данный день не должна быть введена поправка к рабочему времени;*
- *"Дифференциальный отчет"[491] позволяет оценить отношение общего времени нахождения на территории предприятия ко времени, проведенному непосредственно на рабочем месте. Требуется наличие системы доступа как на входе на предприятие, так и на входе на рабочее место (в цех, комнату и так далее). Формируется за неделю;*

Работа с отдельными отчетами рассмотрена в соответствующих подразделах.

В отчетах УРВ можно использовать шаблоны для быстрого выбора типа отчета и определения его параметров, которые могут быть разными для

разных подразделений. Работа с шаблонами[314] описана в отдельном разделе руководства.

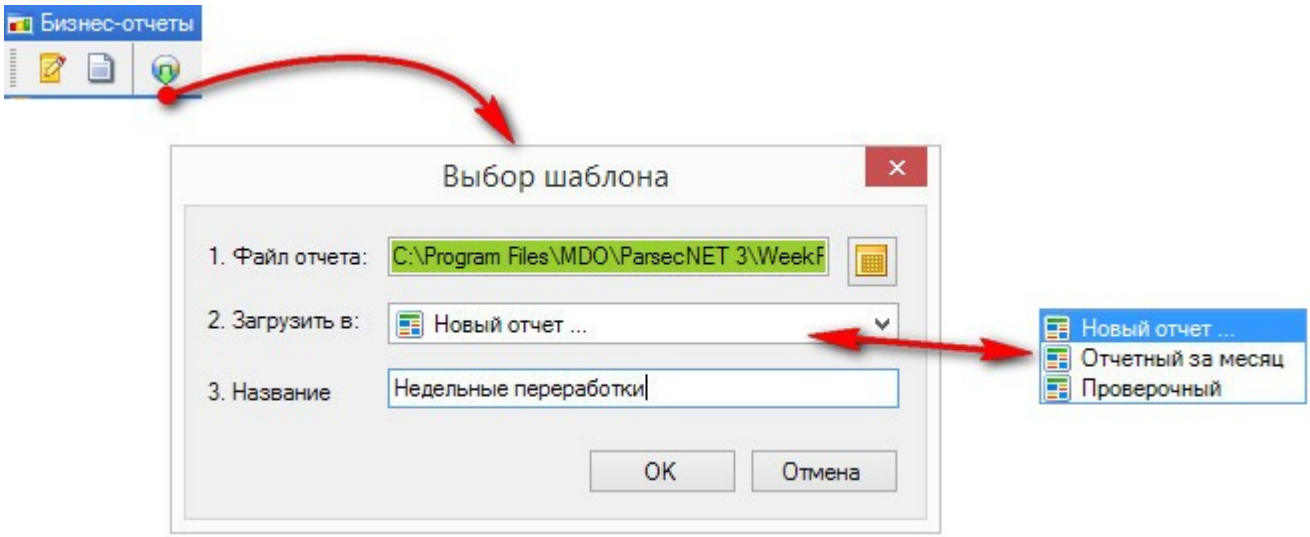
Модуль УРВ позволяет при формировании отчетов использовать корректирующие поправки, такие, как отпуска, командировки, больничные и другие. Поправки вводятся с помощью отдельного инструмента - редактора поправок к рабочему времени.[462]

Импорт отчетов УРВ

По-умолчанию файлы предустановленных в систему отчетов хранятся в папке "C:\Program Files\MDO\ParsecNET 3", это файлы с расширением .frx (Fast Reports). Опытные пользователи могут самостоятельно изменять эти отчеты. При этом рекомендуется сохранить измененный отчет под другим именем и провести импорт этого отчета в систему. Естественно, импортировать можно и другие файлы отчетов с расширением .frx.

Для импорта нового отчета выполните следующие действия:

1. Нажмите на кнопку *Загрузить отчет* на панели инструментов модуля УРВ. Откроется окно выбора:

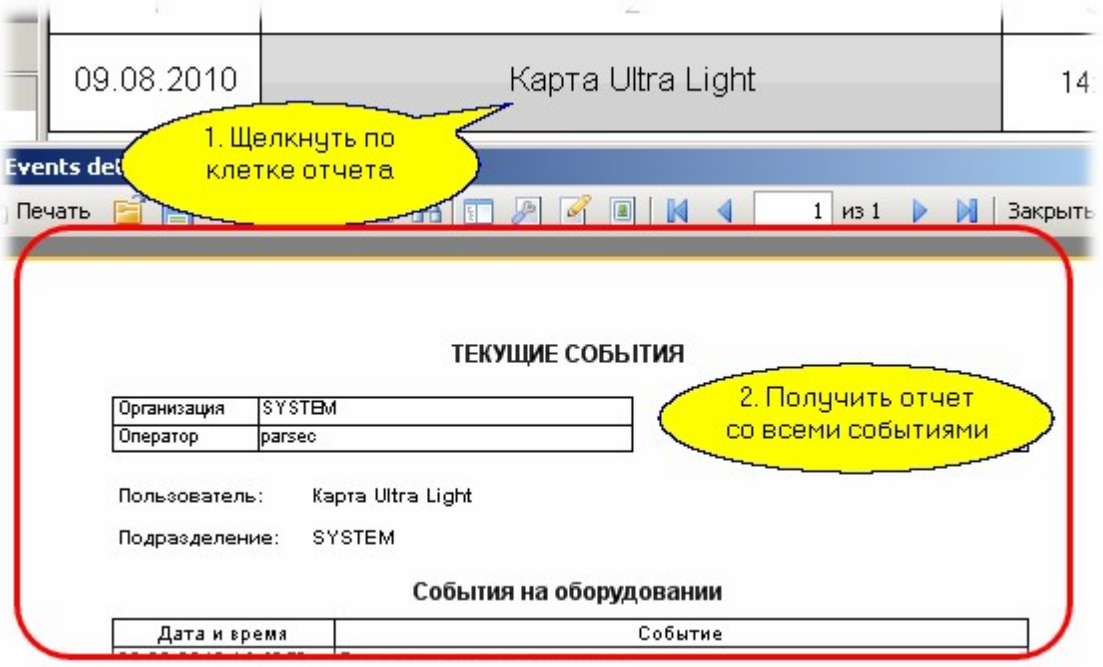


2. Укажите путь к файлу отчета;
3. Выберите как сохранить отчет в системе. Можно создать в системе новый отчет, а можно сохранить файл как уже существующий отчет, выбрав его название в раскрывающемся списке, например, "Отчетный за месяц";
4. Введите название нового отчета. При выборе в шаге 3 существующего отчета поле будет неактивным;
5. Нажмите на кнопку *OK*.

Файл отчета будет импортирован в систему под выбранным именем. После этого он будет отображаться в раскрывающемся списке поля *Тип отчета* и с ним можно осуществлять те же действия, что и с предустановленными отчетами.

Контекстный отчет по событиям

Во всех отчетах модуля имеется возможность оперативно посмотреть информацию о событиях для заданного человека в заданный день, что позволяет понять, как человеку начислялось рабочее время или определялись его отклонения, как показано ниже:



См. также:

[Особенности учета рабочего времени](#)[461]

[Отчеты УРВ (версия 4)](#)[469]

11.3.1 Особенности учёта рабочего времени

Введение

В последние годы все чаще СКУД используется не только как система безопасности, но и как источник информации для работы систем организации бизнес-процессов. Наиболее распространено использование собранной СКУД информации для учёта рабочего времени и контроля дисциплины сотрудников.

Модуль УРВ (версия 4) предназначен как раз для решения данной задачи без привлечения сторонних программных средств. Основные функции данного модуля – формирование месячного табеля учёта рабочего времени с выводом информации в стандартную форму Т-13, формирование недельных табелей учёта рабочего времени, а также формирование отчётов по разного рода отклонениям (опоздания, уход раньше времени, прогулы и так далее).

При учёте рабочего времени модуль также предоставляет уникальную возможность посчитать отдельно время нахождения сотрудника на территории предприятия вообще и на рабочем месте в частности.

Вместе с модулем внесения поправок в отработанное время (который позволяет вносить в систему отпуска, больничные, командировки и другие поправки) модуль УРВ (версия 4) предоставляет достаточно объективную информацию по использованию сотрудниками своего рабочего времени.

Учёт рабочего времени с учётом и подсчётом всех нюансов – достаточно сложная задача, особенно при недостатке объективных данных. Кроме того, в каждой организации действуют свои принципы учёта: у кого-то более либеральные, у кого-то более жёсткие. Разными являются и рабочие графики – их разнообразие не перечислить на одной странице.

В общем случае, для работы по учёту рабочего времени необходимо выполнить следующие действия:

- Создать расписания рабочего времени с назначением праздничных и исключительных дней;
- Присвоить расписание подразделению или отдельному сотруднику;
- Задать поправки рабочего времени (больничные, отпуска и так далее);
- Создать отчёты по учёту рабочего времени – определит правила подсчёта отработанного времени.

Чтобы все алгоритмы работали так, как вы этого ожидаете, важно выполнять условия, которые определяют корректность счёта. Основных условий два: достоверность данных и настройка исходных данных.

Достоверность данных

Подсчёт отработанного времени основывается на зафиксированных системой фактах прохода пользователей. Если какая-то часть информации опущена, то системе приходится "додумывать" за пользователя, а это не всегда приводит к наилучшему результату. Например, у пользователя не зафиксирован вход в начале дня, но есть выход в конце рабочего дня. Спрашивается: как это трактовать? Не засчитывать рабочий день, либо подставить искусственно вход в начале рабочего дня? А если пользователь пришёл не утром, а в обед, не зафиксировав проход?

Аналогичная ситуация неоднозначности возникает, например, если утром есть два последовательных входа без промежуточного выхода - какой из входов считать началом присутствия?

Из приведённых примеров видно, что корректность подсчёта в системе учёта рабочего времени зависит от достоверности объективных данных по проходам пользователей.

Если у вас на входе стоит турникет, то достоверность будет достаточно высокой в силу особенностей работы турникета. А если у вас обычная дверь, через которую, сговорившись, могут по одной карте пройти двое или трое? Здесь поможет только дисциплина сотрудников.



Обеспечьте максимальную дисциплину проходов через точки доступа, по которым ведётся учёт рабочего времени (техническими средствами или административными мерами) – это позволит Вам получать максимально достоверные результаты.

Настройка исходных данных

Для получения отчёта по учёту рабочего времени используется много исходных данных, часть из которых может настраиваться оперативно при создании отчёта (правила подсчёта и некоторые другие), а часть задаётся, практически, один раз после установки системы. К однократно настраиваемым параметрам относятся расписания рабочего времени[221], создаваемые в редакторе расписаний.

Весь учёт отработанного времени, а также различные отклонения, рассчитываются на основе расписаний, и от корректности их задания зависит корректность подсчётов.

Важно понимать следующие моменты при составлении расписания:

- На отчётный период (периоды) необходимо заранее составить расписание, соответствующее графику работы подразделения. Если это стандартное недельное расписание, то оно может быть единственным и действовать достаточно долго без изменений. Если это сменное расписание, то в какие-то моменты времени его, возможно, потребуется скорректировать;
- Не забудьте в редакторе расписаний занести праздники, а, также, исключительные дни (перенос рабочих дней в канун праздника или после него), и указать на использование праздников в конкретном расписании;
- Обязательно укажите нормы отработки за день и за неделю для корректного обсчёта отработанного времени и анализа различных отклонений;
- Имейте в виду, что рабочее время есть простое, когда присутствие человека засчитывается в отработанное время, и обязательное, относительно которого рассчитываются отклонения и нарушения.

См. также:

Модуль учета рабочего времени[456]

Отчеты УРВ (версия 4)[469]

11.3.1.1 Поправки к рабочему времени

Модуль учета рабочего времени позволяет получить достоверную информацию для табеля учета рабочего времени в том случае, если сотрудник находится в рабочее время на территории

предприятия. Если же он находится в командировке, на больничном и так далее, то результаты, выводимые модулем учета рабочего времени в месячный табель, будут отличаться от истины и малопригодны, например, для начисления заработной платы.

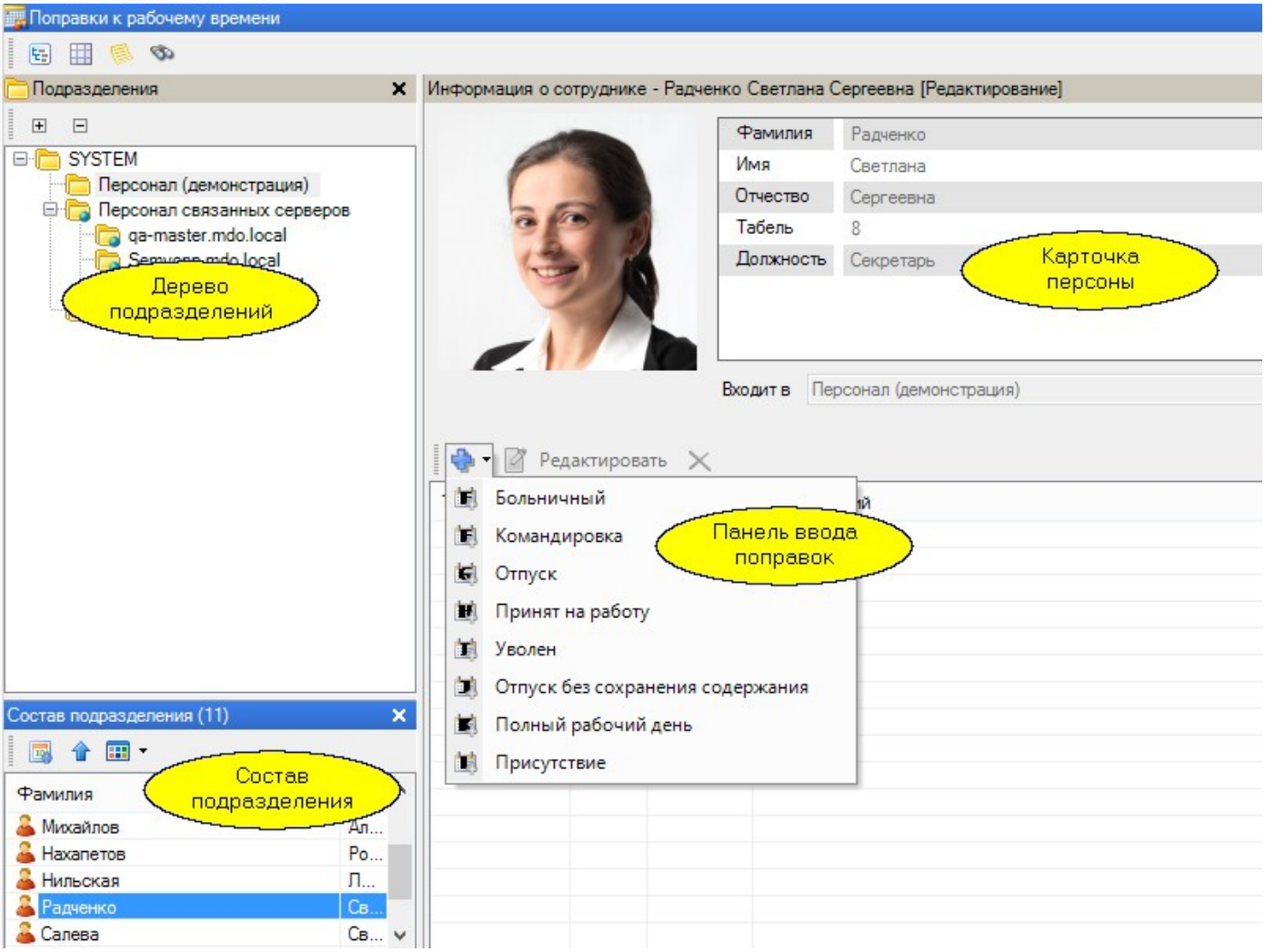
Модуль поправок к рабочему времени позволяет исправить данную ситуацию - он предназначен для ручного ввода различных отклонений, которые затем учитываются системой при формировании табеля учета рабочего времени. Поправки можно вводить как в консоли ParsecNET 3, так и в веб-форме[466] .

Модуль запускается кнопкой  и позволяет вводить следующие поправки:

- ***Больничный***. Вводятся даты начала и окончания отсутствия сотрудника по болезни.
- ***Командировка***. Вводится интервал дат, в которые сотрудник находился в командировке.
- ***Отпуск***. Вводятся данные об оплачиваемом отпуске сотрудника.
- ***Принят на работу***. Применяется для того, чтобы правильно оформлять табель на сотрудника, принятого на работе в середине месяца.
- ***Уволен***. Применяется для того, чтобы правильно оформлять табель на сотрудника, уволенного в середине месяца.
- ***Отпуск без сохранения содержания***. Для учета отгулов и других отсутствий без оплаты этого времени.
- ***Полный рабочий день***. Для введения данных об отработанном дне, если в системе сотрудник по какой-то причине не отмечен (например, забыл дома свою карточку и был запущен на территорию вручную).
- ***Присутствовал***. Для введения данных о присутствии на территории с уточнением по дате и времени начала и окончания периода (с точностью до минут).

Панели редактора поправок

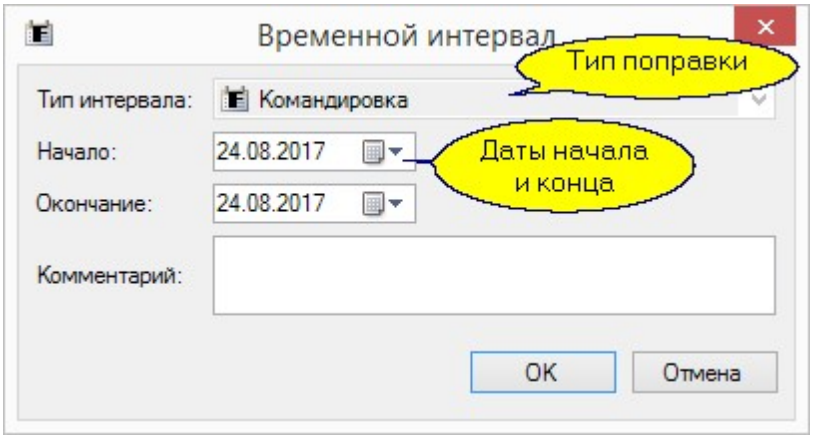
Редактор поправок к рабочему времени в конфигурации по-умолчанию напоминает редактор персонала: имеет панель с деревом подразделений, список элементов подразделения и карточку персоны. Дополнительно имеется панель поправок, расположенная под карточкой персоны:



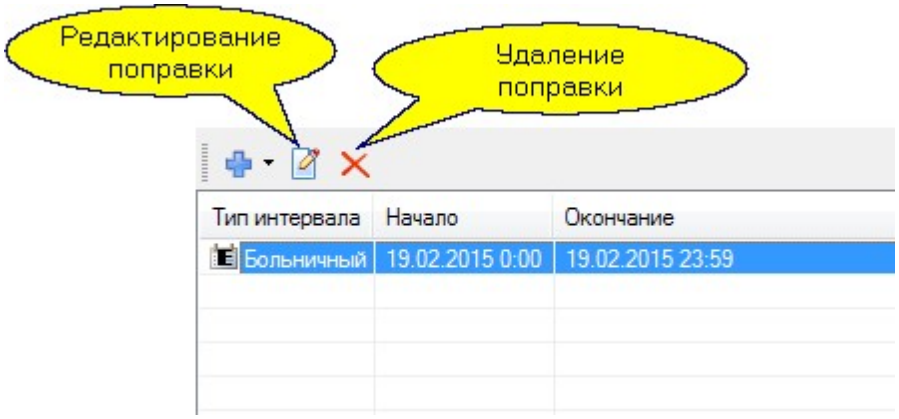
Для ввода поправки:

1. Выберите сотрудника из состава подразделения (внизу слева на предыдущем рисунке);
2. На панели ввода поправок нажмите на кнопку *Добавить* и выберите тип поправки из раскрывающегося списка;
3. В открывшемся окне введите даты начала и конца поправки. Если поправка на один день, то даты начала и конца совпадают;
4. При необходимости добавьте комментарий;
5. Нажмите на кнопку *OK*.

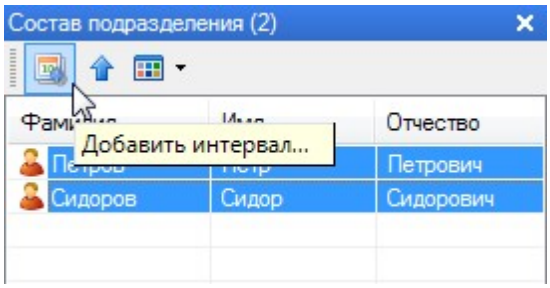
На рисунке ниже показано окно ввода поправки "Командировка" сроком на 3 дня с 4 мая по 6 мая включительно:



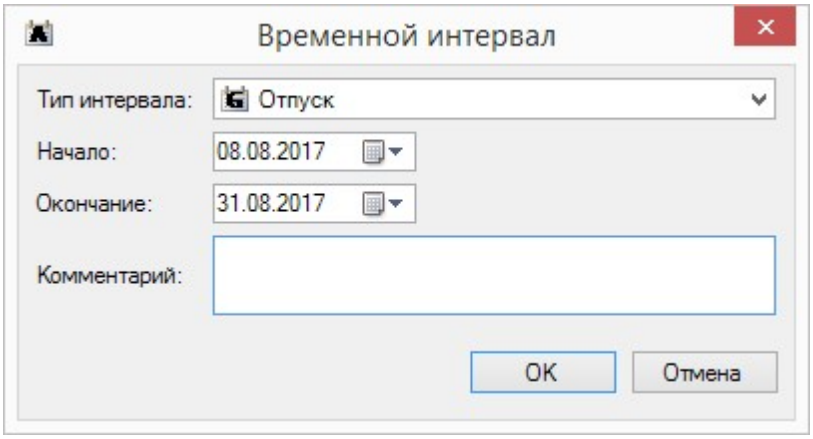
Поправки можно редактировать или удалять, если это потребуется (естественно, до формирования отчетного документа). На рисунке показаны используемые для этого средства:



Для внесения поправки группе сотрудников выделите в панели списка несколько человек (щелкая мышкой при нажатой и удерживаемой клавише Ctrl), а затем нажмите на кнопку *Добавить интервал*, как показано на рисунке:

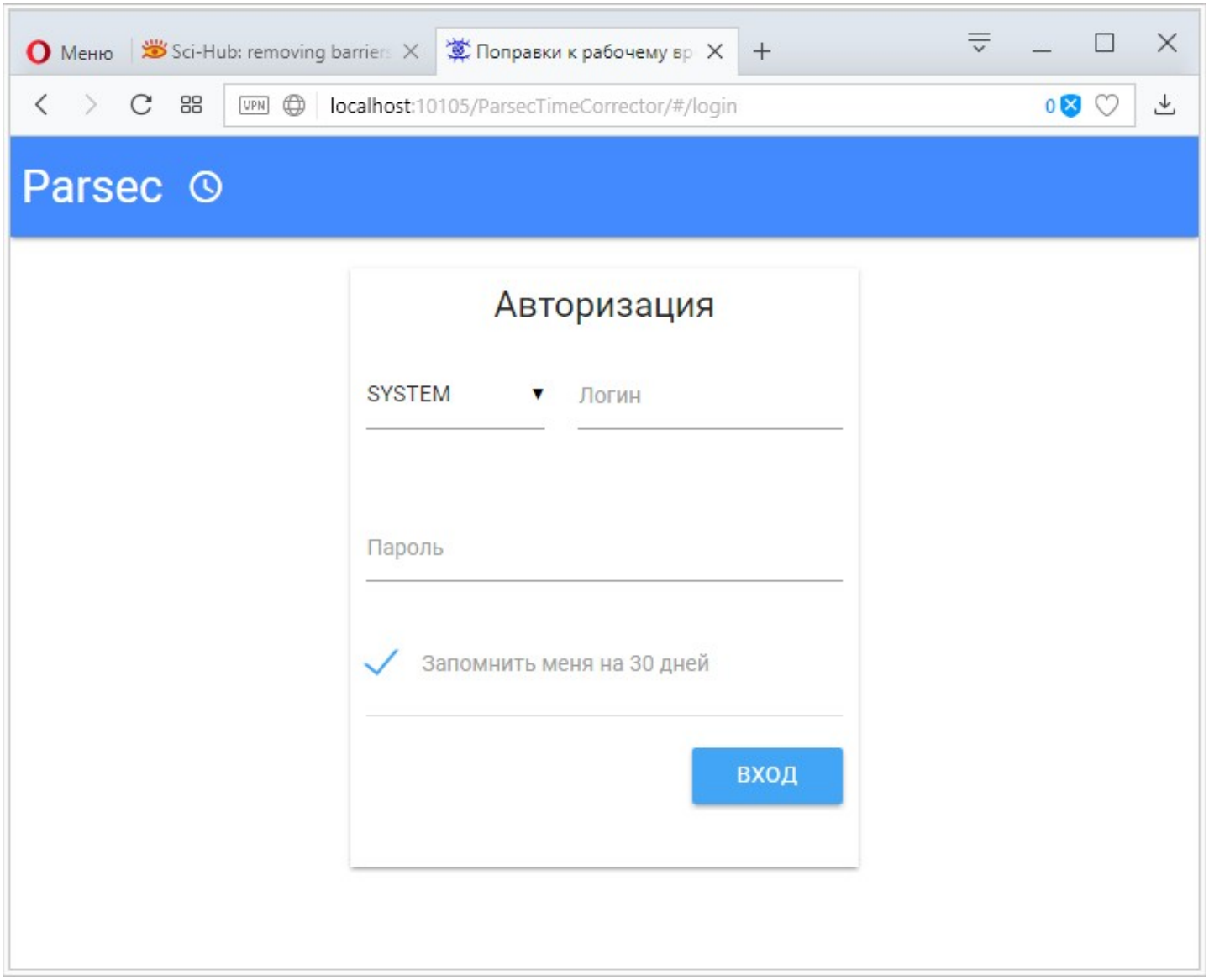


Введите интервал сразу для всех выбранных сотрудников в открывшемся отдельном окне:



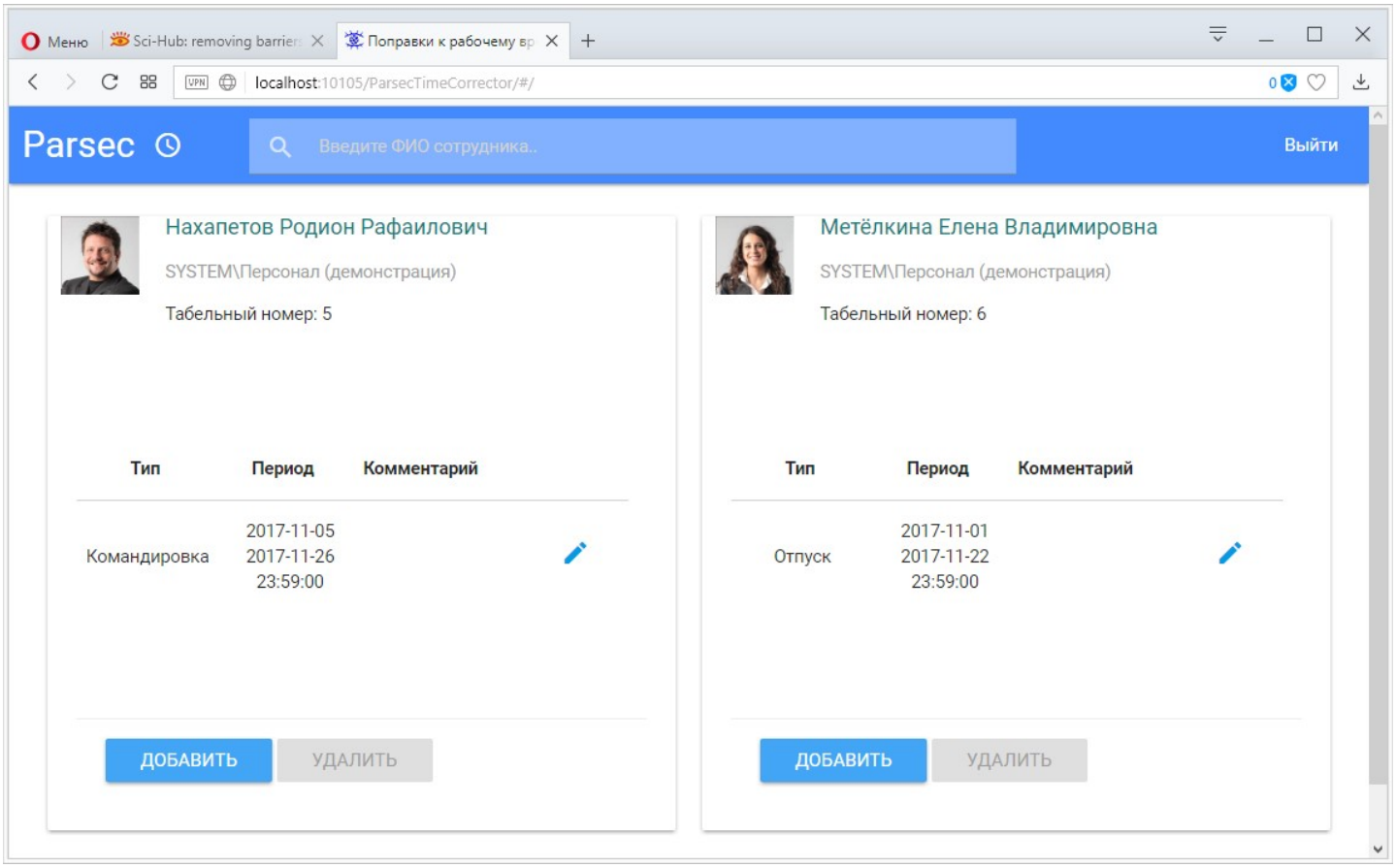
Web-форма для введения поправок к рабочему времени

Ввести поправки к рабочему времени можно через веб-форму, которая откроется в браузере, используемом по умолчанию. Чтобы открыть форму, скопируйте в адресную строку своего браузера *http://<server_name>:10105/ParsecTimeCorrector/*, где вместо <server_name> укажите IP-адрес или имя сервера. Форма откроется в новой вкладке браузера.
Также можно перейти в сетевую папку *<server_name>**ParsecWorkstationSetup**web*, в которой находятся ярлыки веб-форм. Скопируйте на рабочий стол или в любое удобное место ярлык "Parsec Time Corrector". Двойным щелчком по этому значку можно открывать страницу формы внесения поправок:



Если нужно, выберите организацию и введите логин и пароль сотрудника, имеющего право доступа к модулю поправок к рабочему времени.

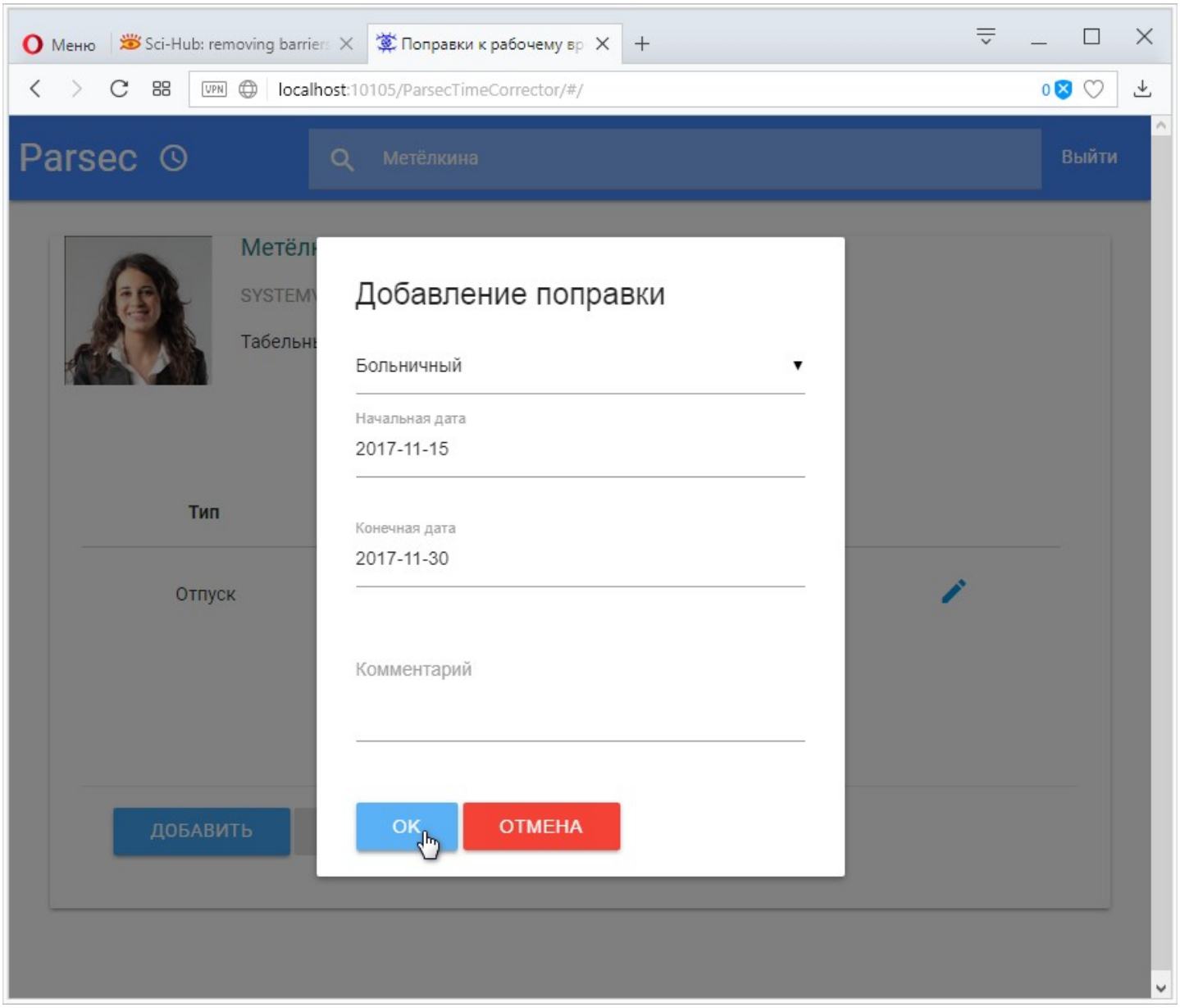
При установленном флажке *Запомнить меня на 30 дней* данные для входа запоминаются на сервере. И если сервер не перезапускался, то в следующий раз система откроет сразу рабочее окно, в котором отображаются карточки всех сотрудников, которые имеют оправки к рабочему времени:



Если ни у кого из сотрудников нет поправок к рабочему времени, окно будет пустым.

Введите фамилию нужного сотрудника в поле поиска и нажмите на клавишу *Enter*.

Для добавления поправки, нажмите на кнопку *ДОБАВИТЬ* и заполните открывшуюся форму, после чего нажмите на кнопку *ОК*:



См. также:

Модуль учета рабочего времени[456]

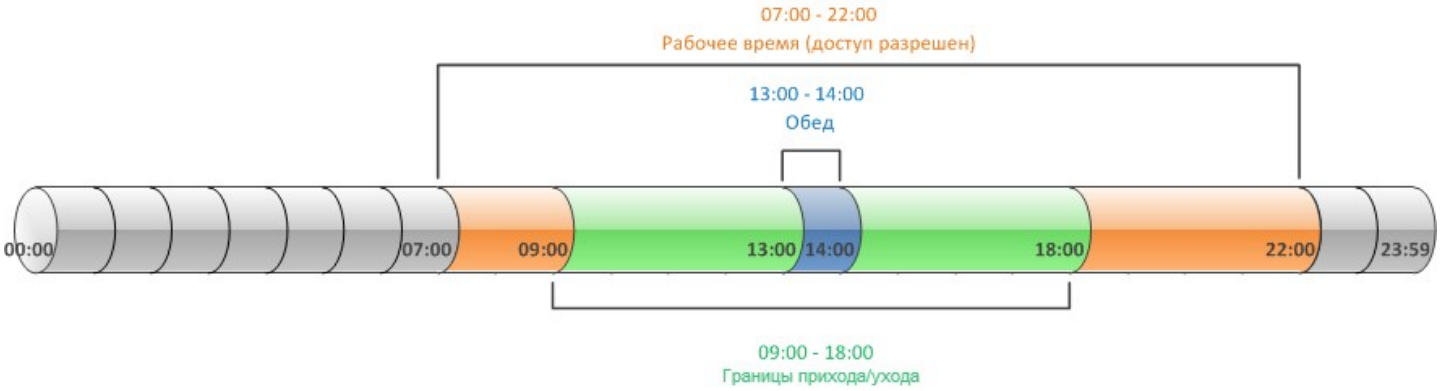
11.3.2 Отчеты УРВ (версия 4)

Поскольку задача модуля Бизнес-отчеты (версия 4) – посчитать отработанное сотрудниками время за выбранный период и сравнить его с плановым, то алгоритм расчёта рабочего времени для отчётов был унифицирован: для решения поставленной задачи разработаны алгоритмы нормализации интервалов присутствия, которые влияют на результат расчёта.

При подсчете УРВ в качестве максимальной величины отработанного сотрудником времени принимается сумма всех периодов рабочего времени. Обед не является рабочим временем и его присутствие в рабочем времени, с точки зрения системы, аналогично двум непересекающимся периодам рабочего времени.

Дополнительно оператор может указать границы прихода/ухода (время самого позднего прихода и самого раннего ухода). Это делается добавлением интервала в расписании рабочего времени[238]. Этот параметр не влияет на подсчет отработанного времени, но влияет на фиксацию нарушений: опозданий и уходов раньше времени.

Общая схема структуры рабочего времени:



Данные о событиях входов и выходов сотрудников обрабатываются прежде, чем используются в расчетах. На основании данных о событиях строится набор интервалов присутствия человека. При этом делаются следующие предположения:

• В интервале между событиями Вход-Выход человек находится внутри;

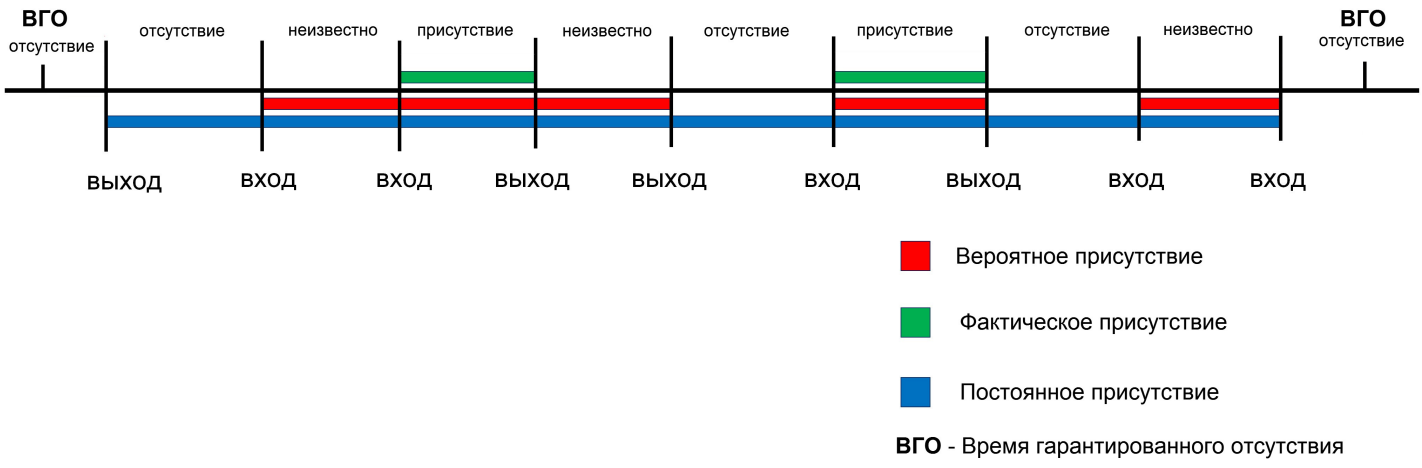
• В интервале между событиями Выход-Вход человек находится снаружи;

• В остальные интервалы (Выход-Выход и Вход-Вход) - местоположение сотрудника неизвестно.

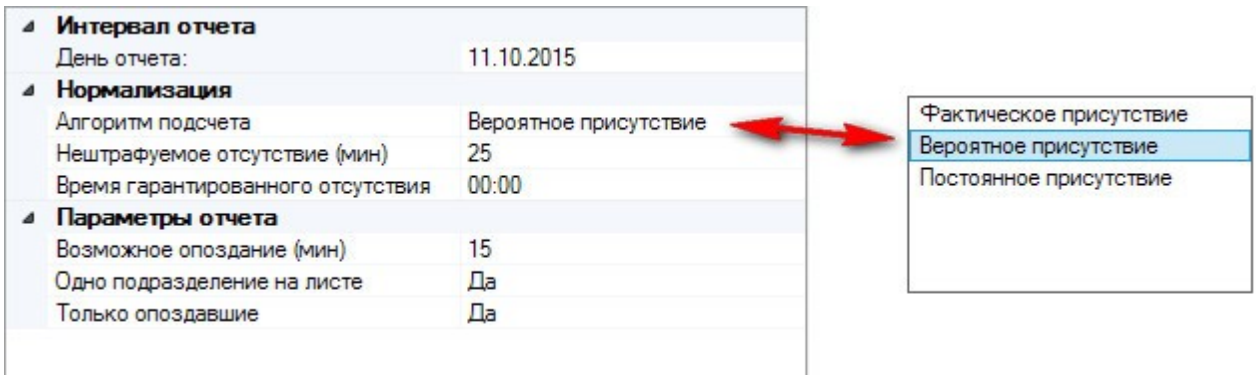
При построении отчета за некоторый период времени (строится с точностью до дня) события анализируются за указанный период плюс события за сутки до этого. События за эти сутки нужны для того, чтобы определить местоположение сотрудника - снаружи или внутри. Если точно определить местоположение сотрудника не удается - нет данных или получен период неизвестности - он считается находящимся снаружи.

Исходя из предположений выше, интервалы обозначаются как интервалы присутствия, отсутствия и неизвестности.

На схеме ниже изображены учитываемые периоды рабочего времени в зависимости от выбранного алгоритма подсчета:



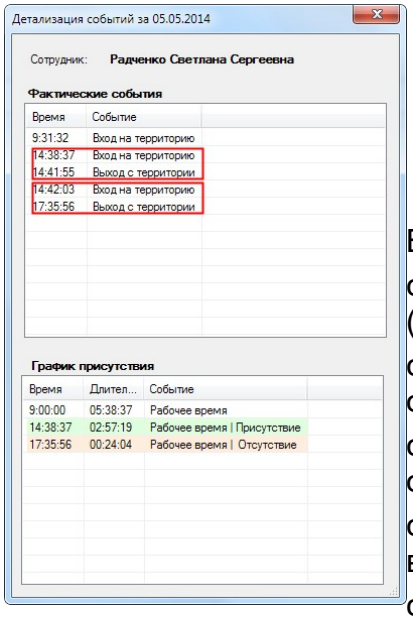
Пользователь имеет возможность указать один из способов подсчета времени.



Ниже показано, как разные алгоритмы считают время одного дня сотрудника:

- **Фактическое присутствие** - суммируются только интервалы присутствия за период рабочего времени. Интервалы неизвестности считаются отсутствием сотрудника на рабочем месте и проверяются на соответствие требованию параметра *Нештрафуемое отсутствие*. Можно

назвать этот способ "жесткий счет". На рисунке выше учитываемые при этом способе подсчета интервалы обозначены зеленым цветом. В окне детализации событий это выглядит следующим образом:



В отработанное время входят только периоды присутствия:

с 9:00:00 (начало рабочего времени) до 9:31:32 - период отсутствия (не входит в отработанное время);

с 9:31: 32 по 14:38:37 - период неизвестности (не входит в отработанное время);

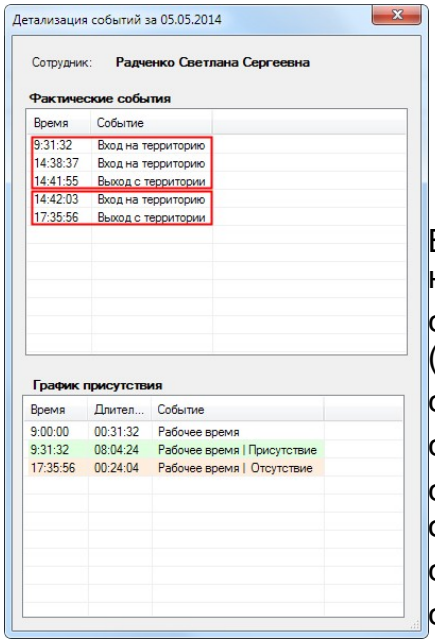
с 14:38:37 по 14:41:55 - период присутствия (засчитывается в отработанное время);

с 14:41:55 по 14:42:03 - период отсутствия (не входит в отработанное время);

с 14:42:03 по 17:35:56 - период присутствия (засчитывается в отработанное время);

с 17:35:56 до 18:00:00 (конец рабочего времени) - период отсутствия (не входит в отработанное время).

- **Вероятное присутствие** - суммируются интервалы присутствия и интервалы неизвестности, попадающие в период рабочего времени. Можно назвать это "мягкий счет" (отрезки красного цвета на рисунке выше). В окне детализации событий это выглядит как на рисунке ниже:



В отработанное время входят и периоды присутствия, и периоды неизвестности:

с 9:00:00 (начало рабочего времени) до 9:31:32 - период отсутствия (не входит в отработанное время);

с 9:31: 32 по 14:38:37 - период неизвестности

с 14:38:37 по 14:41:55 - период присутствия

с 14:41:55 по 14:42:03 - период отсутствия (не входит в отработанное время);

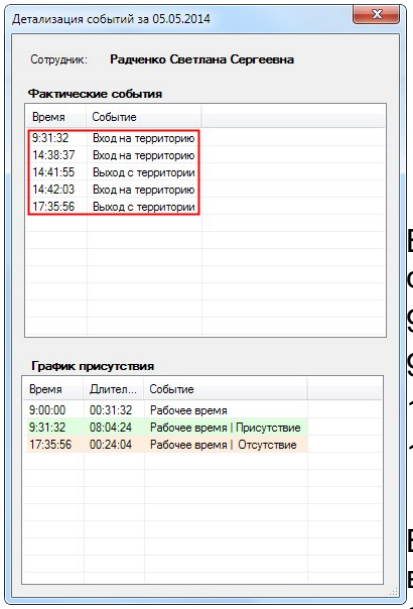
с 14:42:03 по 17:35:56 - период присутствия

с 17:35:56 до 18:00:00 (конец рабочего времени) - период отсутствия (не входит в отработанное время).

- **Постоянное присутствие**. Это способ подсчета для одного считывателя. Рекомендуется для использования при неориентированных точках прохода. В этом режиме все события считаются проходами без направления. При этом делаются следующие допущения:
  - Первое событие в сутки - Вход;
  - Последнее событие в сутки - Выход;

○ Остальные события игнорируются.

Затем система сравнивает начало и конец полученного периода присутствия (синий отрезок на схеме выше) с началом и концом заданного рабочего времени, вычисляя отработанное время и определяя, было ли опоздание, недоработка и т.п. Параметр *Время гарантированного отсутствия* при этом режиме влияния на подсчет отработанного времени не оказывает.



В отработанное время входит период от первого до последнего события в рамках рабочего времени:

9:00:00 - начало рабочего времени;

9:31:32 - первое событие;

17:35:56 - последнее событие;

18:00:00 - конец рабочего времени.

В том случае, когда первое событие произошло до начала рабочего времени, а последнее - после конца рабочего времени, то количество отработанного времени будет равно установленному в расписании рабочему времени.

Параметр нормализации *Нештрафуемое отсутствие (мин)* задает максимальную длительность интервала отсутствия на рабочем месте в рабочее время, который в процессе подсчета отработанного времени будет считаться интервалом присутствия. Например, периоды перекуров, когда они делаются за пределами территории (что актуально в соответствии с принятым законодательством). Если этот параметр поставить в 0, то фактически будет считаться чистое время, так как все, даже короткие, интервалы отсутствия будут вычитаться из отработанного времени.

Отсутствие в рабочее время (РВ) – ситуация, когда сотрудник в рабочее время отсутствовал на территории дольше, чем указано в параметре *Нештрафуемое отсутствие*, но меньше 4 часов. В последнем случае в месячном табеле будет указан прогул.

Время гарантированного отсутствия. Для корректной работы модуля УРВ версии 4 система считает, что в указанный момент времени на территории сотрудников нет. Интервал присутствия или неопределенности, содержащий в себе момент времени гарантированного отсутствия, система считает интервалом отсутствия.

Рекомендуется устанавливать время гарантированного отсутствия в ночной период.

В случае ночной смены, время до момента гарантированного отсутствия отсчитывается не от начала суток, а от окончания смены.

Параметр настройки *Разрешенное отсутствие в день (мин)* есть только в отчетах "Приход/уход за месяц" и "Приход/уход за неделю". Это максимальное количество минут, которое может быть учтено как отработанное, из суммарного штрафуемого времени отсутствия сотрудника. Т.е. суммируются все интервалы отсутствия за день, величина которых превышает значение параметра *Нештрафуемое отсутствие (мин)*. Из этой суммы вычитается разрешенное время отсутствия. Если получено положительное значение, то это и есть время некомпенсируемого работодателем отсутствия сотрудника на рабочем месте. Например, разрешенное время отсутствия может использоваться для предоставления сотрудникам времени на обед в том случае, когда обеденное время учитывается как рабочее.

Возможное опоздание (мин). Не учитываемое системой время опоздания; считается от границы прихода. Используется только в отчете по опозданиям.

Система ищет интервал присутствия сотрудника с момента начала рабочего времени до границы прихода. Если такой интервал есть, то система не будет учитывать опоздание. Например, доступ на территорию для сотрудника открыт с 8.00, а граница прихода - 9.00. Величина возможного опоздания задана в 10 минут. Сотрудник пришел в 8.30, а в 8.59 вышел покурить на 15 минут. В этом случае опоздание не будет засчитано.

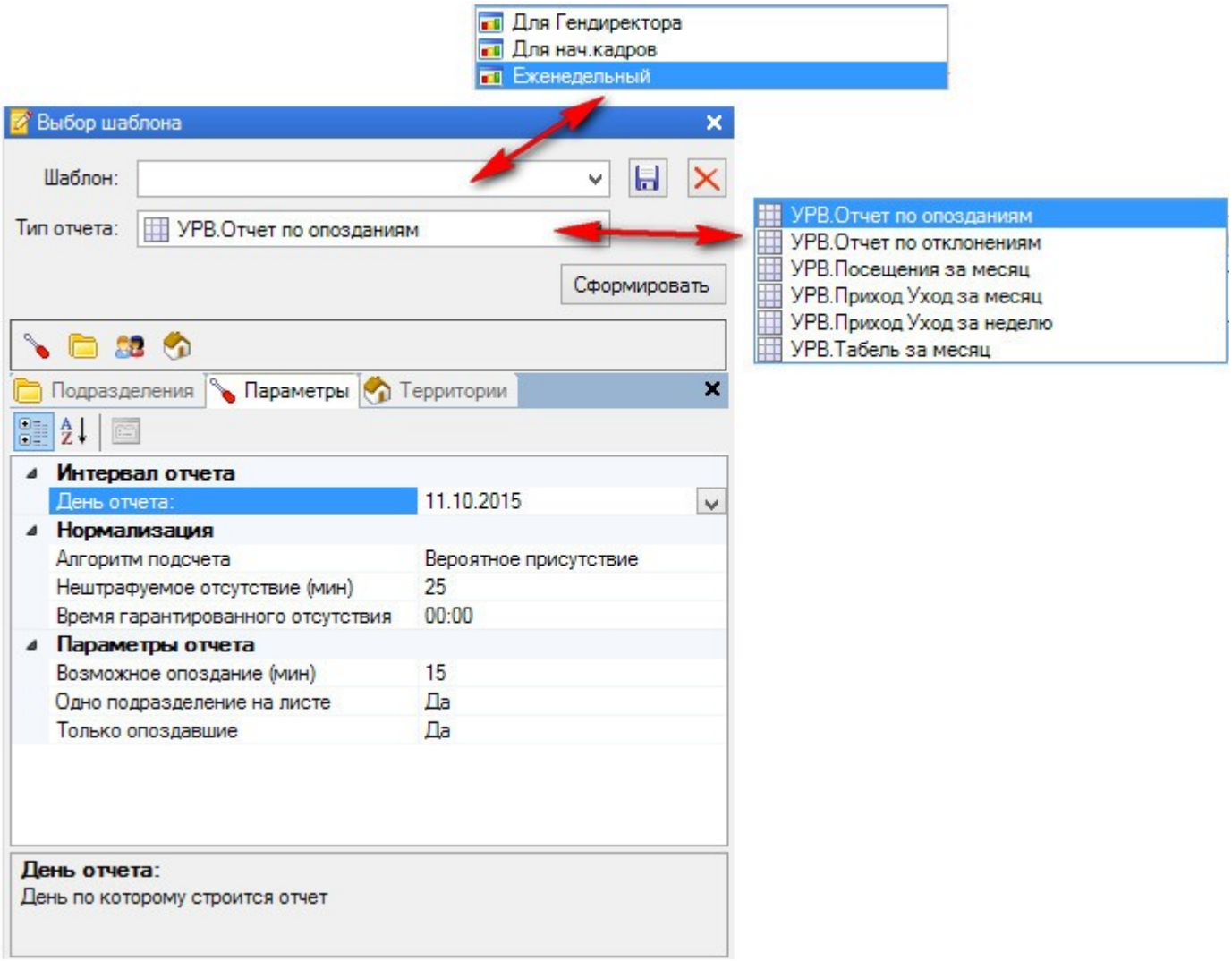
11.3.2.1 Построение отчётов УРВ

Убедитесь, что подразделению или сотруднику(-ам), по которым необходимо получить отчет, задано расписание рабочего времени[221] .

Для получения отчета по автомобилям расписание рабочего времени задается подразделениям, в которые входят владельцы интересующих вас автомобилей.

Чтобы сформировать отчет, выполните следующие действия:

1. Откройте инструмент Бизнес-отчеты;
2. В раскрывающемся списке *Шаблон* выберите шаблон отчета (если он сохранен ранее) и нажмите на кнопку *Построить отчет*. Система создаст отчет с параметрами, сохраненными в шаблоне.
   Если готового шаблона нет, перейдите к следующему шагу;
3. Выберите тип отчета из одноименного раскрывающегося списка;
4. Установите атрибуты и параметры отчета;
   При необходимости используйте фильтр, чтобы ограничить сведения конкретными точками прохода и/или сотрудниками. При необходимости выбора нескольких территорий или сотрудников используйте клавиши Shift и Ctrl;
5. Если такой отчет нужно составлять периодически, сохраните его в качестве шаблона, нажав на кнопку (*Сохранить)* и введя наименование шаблона;
6. Нажмите на кнопку *Сформировать*. Готовый отчет отобразится на панели *Формируемый отчет*.



Если в полученном отчете строки сотрудников залиты розовым цветом, это значит, что для таких сотрудников не назначено расписание рабочего времени. Это справедливо для всех типов отчетов. Для отчета "Посещения за месяц" такая заливка также может появиться, если в расписании рабочего времени не назначены границы прихода/ухода.

В случае отсутствия у сотрудника расписания, все дни для него будут считаться выходными. А дни, когда он присутствовал на рабочем месте, будут помечаться как работа в выходной:



Отчет по посещениям за Июнь 2014 г.

Подразделение: Арендодатели

№ п/п	Фамилия, Имя, Отчество	Отметки о посещениях по числам месяца																													
		1 Вс	2 Пн	3 Вт	4 Ср	5 Чт	6 Пт	7 Сб	8 Вс	9 Пн	10 Вт	11 Ср	12 Чт	13 Пт	14 Сб	15 Вс	16 Пн	17 Вт	18 Ср	19 Чт	20 Пт	21 Сб	22 Вс	23 Пн	24 Вт	25 Ср	26 Чт	27 Пт	28 Сб	29 Вс	30 Пн	
1	Охрана Эталон	В	В	В	В	В	В	В	РВ	РВ	РВ	РВ	В	В	В	РВ	РВ	РВ	РВ	РВ	РВ	В	РВ	РВ	РВ	РВ	РВ	РВ	В	РВ	РВ	

11.3.2.1.1 Отчет по автомобилям

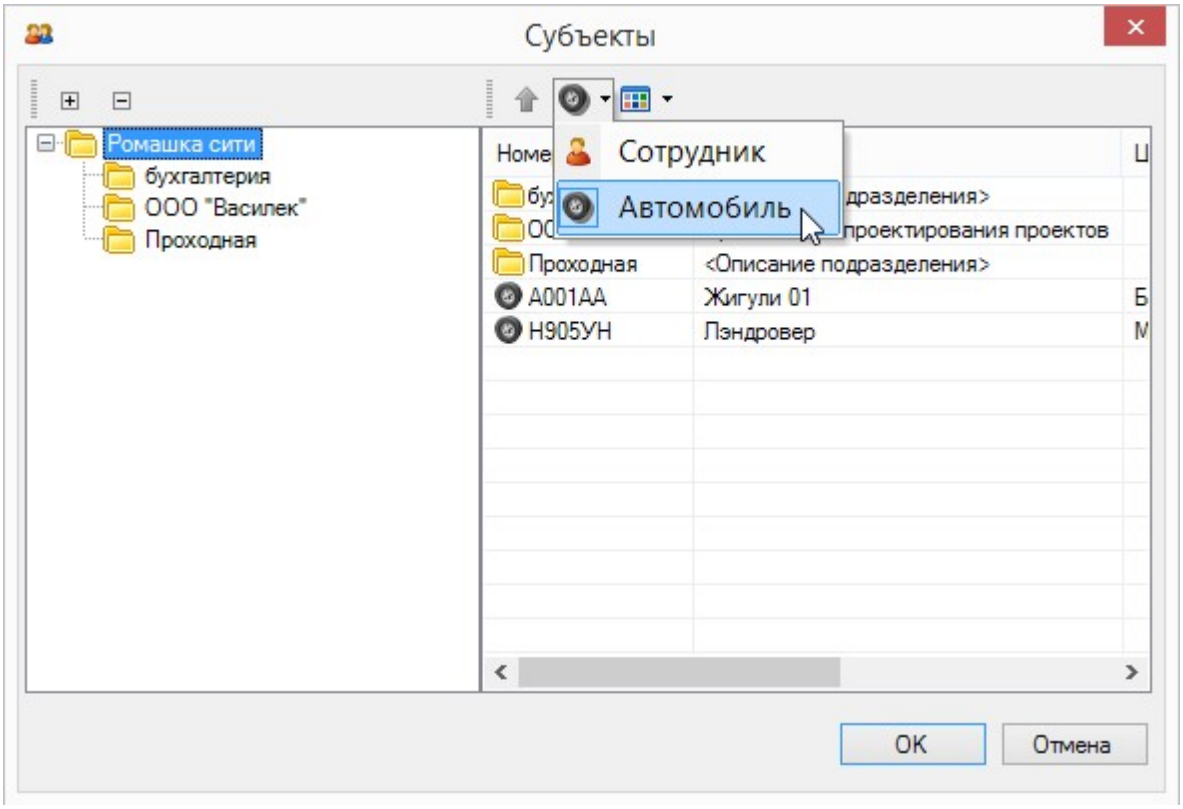
Чтобы сформировать отчет, выполните следующие действия:

1. Убедитесь, что подразделениям, в которые входят владельцы интересующих Вас автомобилей, заданы расписания рабочего времени. Автомобилю нельзя задать персональное расписание рабочего времени, в отличие от Сотрудника;
2. Откройте инструмент Бизнес-отчеты;

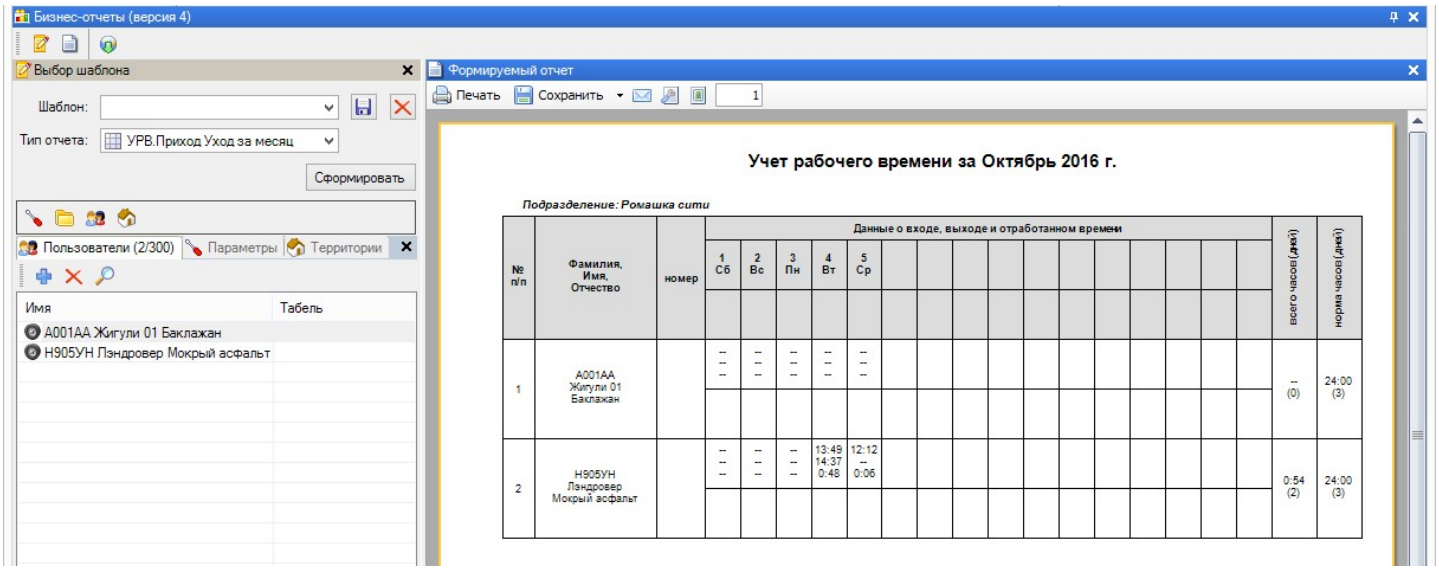
3. В раскрывающемся списке *Шаблон* выберите шаблон отчета (если он сохранен ранее) и нажмите на кнопку *Построить отчет*. Система создаст отчет с параметрами, сохраненными в шаблоне.
   Если готового шаблона нет, перейдите к следующему шагу;
4. Выберите тип отчета из одноименного раскрывающегося списка;
5. Установите атрибуты и параметры отчета.

   При необходимости используйте фильтр, чтобы ограничить сведения конкретными точками прохода и/или сотрудниками. При необходимости выбора нескольких территорий или автомобилей используйте клавиши Shift и Ctrl;

6. На вкладке *Пользователи* нажмите на кнопку выбора субъектов доступа . В открывшемся окне *Субъекты*, нажмите на кнопку фильтра и выберите субъект "Автомобиль":



7. Выделите интересующие Вас автомобили и нажмите на кнопку *ОК*. Выбранные автомобили будут добавлены на вкладку *Пользователи* инструмента Бизнес-отчеты (версия 4) (см. рис. ниже);
8. Если такой отчет нужно составлять периодически, сохраните его в качестве шаблона, нажав на кнопку (*Сохранить)* и введя наименование шаблона;
9. Нажмите на кнопку *Сформировать*. Готовый отчет отобразится на панели *Формируемый отчет*.



11.3.2.2 Отчёт по опозданиям

На рисунке представлен отчет по опозданиям.



Отчет по опозданиям за 22.01.2015 г.

Подразделение: Сотрудники

№ п/п	Фамилия, Имя, Отчество	Номер	Отметки об опоздании			Границы прихода / ухода (макс. опоздание)
			Время прихода / ухода	Опоздание	На месте	
1	Дворжецкий Вацлав Янович	03	11:05 / 18:01	1:05		10:00 / 18:00 (15)

Отчет позволяет получить данные по опозданиям, зафиксированным системой, с учетом заданных правил учета рабочего времени (расписаний, допустимых отклонений, норм отработки). Отчет может формироваться только за один день. Кроме этого, отчет может быть выведен по одному сотруднику или по всему выбранному подразделению.

Для формирования отчета по опозданиям, по аналогии с остальными отчетами, необходимо проделать стандартные шаги[473].

Как и для других бизнес-отчетов, настроенный отчет по опозданиям можно сохранить в виде шаблона.

Примеры

Для сотрудника установлен период рабочего времени (когда доступ разрешен) с 9.30 до 18.30, а границы прихода/ухода - с 10.00 до 18.00.

Установим период возможного опоздания 15 мин.

1. Сотрудник пришел на работу в 11.05. Система посчитает его опоздание - 1 час 5 минут (см. рис. выше).
2. Сотрудник пришел на работу в 9.30. В 9.55 ушел (покинул территорию). Вернулся в 10.20. Система "не заметит" его отсутствия с 9.55 по 10.20 и посчитает, что он начал работу с 9.30.

Система ищет интервал присутствия сотрудника с момента начала рабочего времени до границы прихода. Если такой интервал есть, то система не будет учитывать опоздание.
Параметр* Возможное опоздание *не используется в "Отчете по отклонениям". Это может привести к противоречию: например, возможное опоздание - 10 мин. Сотрудник пришел в 9.07. "Отчет по отклонениям" покажет опоздание, а "Отчет по опозданиям" - нет.

11.3.2.3 Отчёт по отклонениям

Отчет по отклонениям позволяет получить данные по всем нарушениям, зафиксированным системой, с учетом заданных правил учета рабочего времени (расписаний, допустимых отклонений, норм отработки). В отчет попадают все выбранные сотрудники, а не только те, у которых имелись отклонения на заданном интервале времени.

ОТЧЕТ ПО ОТКЛОНЕНИЯМ

Дата составления	Отчетный период	
	с	по
29.07.2014	22.07.2014	30.07.2014

Подразделение Сотрудники

Дворжецкий Вацлав Янович

Дата	Приход	Уход	Всего	Опоздание	НВХ	НВЫ	ОПЗ	УРВ	ПЕР	ОТС	ОРД
22.07.2014	13:39	18:39	5:00	3:39			X				X
23.07.2014	14:38	21:19	6:41	4:38		X	X				X
24.07.2014	18:46	18:47	0:00	--	X						X
25.07.2014	14:22	20:34	6:12	4:22			X				X
26.07.2014	--	--	--	--	X					X	X
27.07.2014	--	--	--	--	X					X	X
28.07.2014	14:49	23:59	9:09	4:49		X	X				X
29.07.2014	--	--	--	--	X					X	X

Условные обозначения:
НВХ — нет входа, НВЫ — нет выхода, ОПЗ — опоздание, УРВ — уход раньше времени
ПЕР — переработка, ОТС — отсутствие, ОРД — отлучка в течение рабочего дня

В отчете для каждого сотрудника указываются (в часах и минутах):

- Время прихода;
- Время ухода;
- Сумма отработанного за день времени;
- Величина опоздания.

Кроме этого, в отчет включаются следующие отклонения:

- НВХ - нет входа. Отмечается в случае, если первым событием дня у сотрудника является выход;
- НВЫ - нет выхода. Отмечается в случае, если последним событием дня у сотрудника является вход;
- ОПЗ - опоздание. Отмечается, если в период с начала рабочего времени до границы прихода отсутствует начальная точка интервала присутствия;

Система ищет интервал присутствия сотрудника с момента начала рабочего времени до границы прихода. Если такой интервал есть, то система не будет учитывать опоздание. Например, доступ на территорию для сотрудника открыт с 8.00, а граница прихода - 9.00. Сотрудник пришел в 8.30, а в 8.59 вышел покурить на 15 минут. Опоздание не будет засчитано.
Параметр* Возможное опоздание *в данном отчете не используется. Это может привести к противоречию между "Отчетом по опозданиям" и "Отчетом по отклонениям". Например, возможное опоздание - 10 мин. Сотрудник пришел в 9.07. "Отчет по отклонениям" покажет опоздание, а "Отчет по опозданиям" - нет.

- УРВ - уход раньше времени. Отмечается при уходе сотрудника с рабочего места раньше границы ухода;
- ПЕР - переработка. Отмечается в случае, если в конкретный день сотрудник переработал установленную при настройке системы (в расписании) дневную норму;
- ОТС - отсутствие. Отклонение фиксируется, если нет ни одного интервала присутствия сотрудника в период рабочего времени;
- ОРД - отлучка в течение рабочего дня. Нарушение фиксируется, если сотрудник покидал территорию на время большее, чем указано в параметре «Нештрафуемое отсутствие».

Примеры

При проверке на уход раньше времени система ищет интервал присутствия сотрудника от границы ухода до момента конца рабочего времени. Если такой интервал есть, то система не считает уход раньше времени.

Для сотрудника установлен период рабочего времени (когда доступ разрешен) с 8.30 до 18.30, а границы прихода/ухода - с 9.00 до 18.00.

1. Сотрудник покинул рабочее место в 17.59. Система зафиксирует уход раньше времени;
2. Сотрудник вышел с территории в 17.50 и вновь вошел в 18.20. Окончательно ушел в этот день в 18.27. Система не будет считать уход раньше времени.

11.3.2.4 Посещения за месяц

Отчет по посещениям отображает посещение сотрудником своего рабочего места в каждое число месяца.

Состояния, обозначенные в отчете условными символами, вычисляются программой на основе транзакций, формируемых контроллерами доступа.

Отчет по посещениям за Май 2014 г.

Подразделение: Сотрудники

№ п/п	Фамилия, Имя, Отчество	Отметки о посещениях по числам месяца																														
		1 Чт	2 Пт	3 Сб	4 Вс	5 Пн	6 Вт	7 Ср	8 Чт	9 Пт	10 Сб	11 Вс	12 Пн	13 Вт	14 Ср	15 Чт	16 Пт	17 Сб	18 Вс	19 Пн	20 Вт	21 Ср	22 Чт	23 Пт	24 Сб	25 Вс	26 Пн	27 Вт	28 Ср	29 Чт	30 Пт	31 Сб
1	Дворжецкий Вацлав Янович	В	В	В	В	О	О	О/У	О	В	В	В	В	В	О	О	О	В	В	О	О	О	О	К	В	В	О	О	О	О	О	В
2	Лазарев Александр Сергеевич	В	В	В	В	О	О	О	О	В	В	В	В	В	О	О	О	В	В	О	О	О	О	О	В	В	О	О	О	О	О	В
3	Ледогоров Вадим Игоревич	В	В	В	В	О	О	О	ОТ	В	В	В	В	В	ОТ	О	О	В	В	О	О	О	ПР	К	В	В	О	О	О	О	О	В
4	Меньшикова Нина Евгеньевна	В	В	В	В	О	У	ПР	О/У	В	В	В	В	В	О	У		В	В	О	У	У	О		В	В	О	У		О	О	В
5	Метёлкина Елена Владимировна	В	В	В	В	О	О	О	К	В	В	В	В	В	О	О		В	В	Б	О	О	О/У		В	В	О	О/У	О	О		В
6	Михайлов Александр Яковлевич	В	В	В	В	ОТ	ОТ	ОТ	ОТ	В	В	В	В	В	О	О	О	В	В	О	О	О	О	О	В	В	О	О	О	О	О	В
7	Нахапетов Родион Рафаилович	В	В	В	В	О	О	О	О	В	В	В	В	В	О	О		В	В	О	О	О	О		В	В	О	О	О	О		В
8	Нильская Людмила Валерьяновна	?	В	В	В	?	?	?	?	В	В	В	В	В	?	?	?	В	В	?	?	?	?	?	В	В	?	?	?	?	?	В
9	Радченко Светлана Сергеевна	В	В	В	В	О/У	О/У	У	О/У	В	В	В	В	В	О/У	У	ОТ	В	В	О/У	О/У	У	У		В	В	О	У	У	Б	Б	В
10	Семенцова Надежда Мефодьевна	В	В	В	В	О	О	О	О/У	В	В	В	В	В	О	О	О	В	В	О	О	О	О	О	В	В	О	О	О	О	О	В
11	Тимофеев Николай Дмитриевич	В	В	В	В	О	О	О	О	В	В	В	В	В	О	О	О	В	В	О	О	О	О	О	В	В	Б	О	О	О	О	В

Условные обозначения:
О — опоздание, У — уход раньше времени, Х — отсутствие, ХР — прогул с фактом присутствия, Б — больничный, К — командировка, В - выходной, ОТ — отпуск, ПР — полный рабочий день, РВ — Работа в выходной, ? — не принят на работу, $ — отпуск без сохранения содержания

ОФИС/parsec 23.09.2014 16:56:47 1/1

Подробности события можно увидеть, щелкнув по нужной ячейке любой клавишей мыши.

Условные обозначения, используемые в отчете:

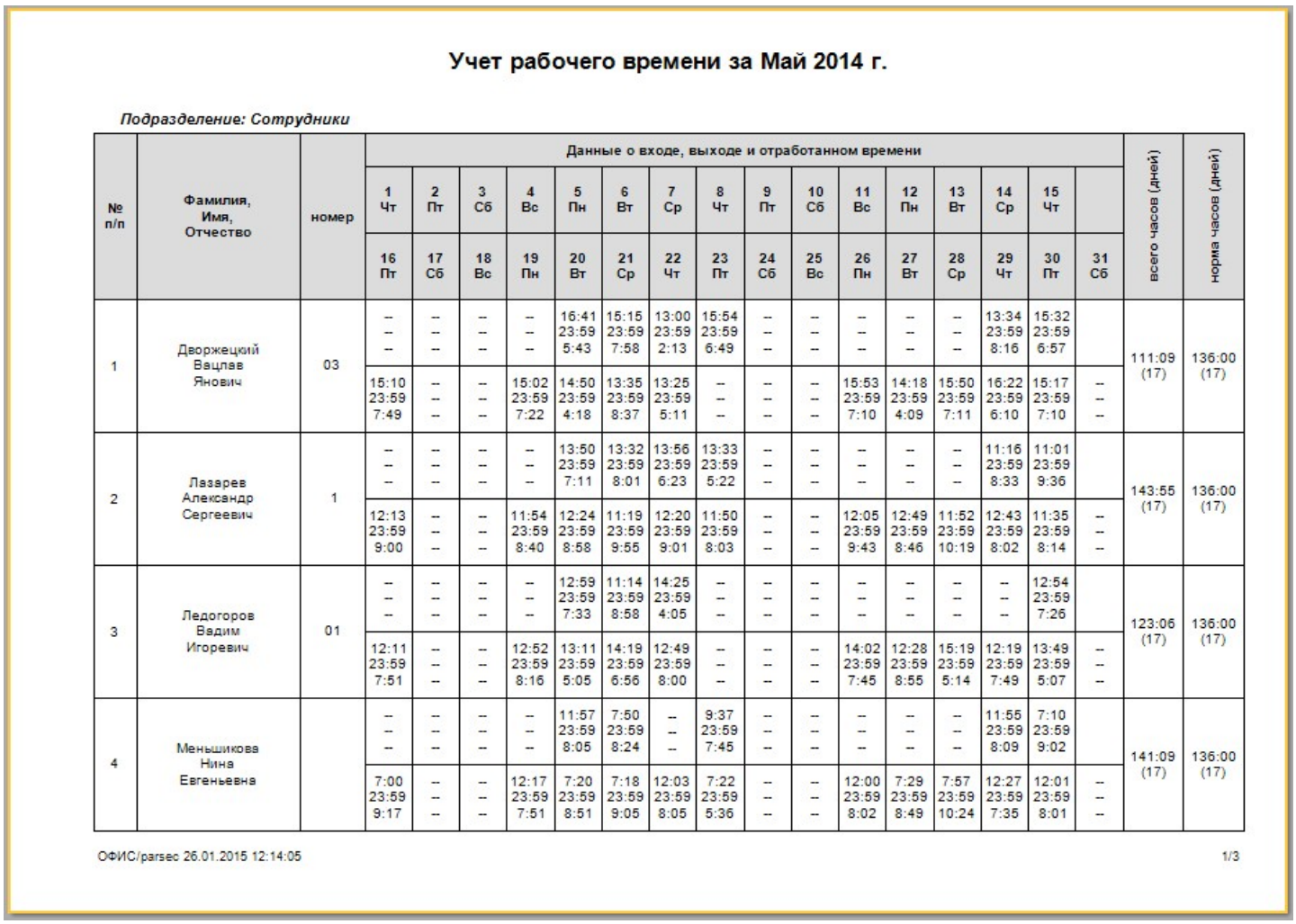
- О - опоздание. Отмечается, если в период с начала рабочего времени до границы прихода отсутствует начальная точка интервала присутствия;
- У - уход раньше времени. Отмечается при уходе сотрудника с рабочего места раньше границы ухода;
- Х - отсутствие. Отмечается, если нет интервала присутствия в период рабочего времени;
- ХР - прогул с фактом присутствия. Отмечается, если у сотрудника в период рабочего времени есть разовый интервал отсутствия величиной 4 часа и более;
- Б - больничный. Установлена соответствующая поправка рабочего времени;
- К - командировка. Установлена соответствующая поправка рабочего времени;
- В - выходной. Во временном профиле данного дня не установлены границы прихода/ухода и сотрудник отсутствовал в этот день;
- ОТ - отпуск. Установлена соответствующая поправка рабочего времени;
- ПР - присутствие без проходов. Сотруднику установлена поправка[462] рабочего времени *Полный рабочий день*;
- РВ - работа в выходной. Во временном профиле данного дня не установлены границы прихода/ухода, но сотрудник присутствовал в этот день;
- ? - не принят на работу. Отметка устанавливается в дни, предшествующие дате принятия на работу, в которые по карте сотрудника зафиксированы проходы. Либо в дни после даты его увольнения. Например, сотрудник принят на работу 5 числа, уволен 25, но раньше и позже этого периода в текущий месяц, по его карте зафиксированы проходы:

№ п/п	Фамилия, Имя, Отчество	Отметки о посещениях по числам месяца																														
		1 Вс	2 Пн	3 Вт	4 Ср	5 Чт	6 Пт	7 Сб	8 Вс	9 Пн	10 Вт	11 Ср	12 Чт	13 Пт	14 Сб	15 Вс	16 Пн	17 Вт	18 Ср	19 Чт	20 Пт	21 Сб	22 Вс	23 Пн	24 Вт	25 Ср	26 Чт	27 Пт	28 Сб	29 Вс	30 Пн	
1	Нильская Людмила Валерьяновна	В	?	?	?	?		В	В				В	Х	В	В						В	В			?	?	?	В	В	?	

- $ - отпуск "за свой счет".

11.3.2.5 Приход/уход за месяц

Отчет "Приход/уход за месяц" показывает время прихода, время ухода и отработанное время для выбранных сотрудников в каждый день месяца.



Учет рабочего времени за Май 2014 г.

Подразделение: Сотрудники

№ п/п	Фамилия, Имя, Отчество	номер	Данные о входе, выходе и отработанном времени																всего часов (дней)	норма часов (дней)
			1 Чт	2 Пт	3 Сб	4 Вс	5 Пн	6 Вт	7 Ср	8 Чт	9 Пт	10 Сб	11 Вс	12 Пн	13 Вт	14 Ср	15 Чт			
			16 Пт	17 Сб	18 Вс	19 Пн	20 Вт	21 Ср	22 Чт	23 Пт	24 Сб	25 Вс	26 Пн	27 Вт	28 Ср	29 Чт	30 Пт	31 Сб		
1	Дворжецкий Вацлав Янович	03	-- -- --	-- -- --	-- -- --	-- -- --	16:41 23:59 5:43	15:15 23:59 7:58	13:00 23:59 2:13	15:54 23:59 6:49	-- -- --	-- -- --	-- -- --	-- -- --	-- -- --	13:34 23:59 8:16	15:32 23:59 6:57		111:09 (17)	136:00 (17)
			15:10 23:59 7:49	-- -- --	-- -- --	15:02 23:59 7:22	14:50 23:59 4:18	13:35 23:59 8:37	13:25 23:59 5:11	-- -- --	-- -- --	-- -- --	15:53 23:59 7:10	14:18 23:59 4:09	15:50 23:59 7:11	16:22 23:59 6:10	15:17 23:59 7:10	-- -- --		
2	Лазарев Александр Сергеевич	1	-- -- --	-- -- --	-- -- --	-- -- --	13:50 23:59 7:11	13:32 23:59 8:01	13:56 23:59 6:23	13:33 23:59 5:22	-- -- --	-- -- --	-- -- --	-- -- --	-- -- --	11:16 23:59 8:33	11:01 23:59 9:36		143:55 (17)	136:00 (17)
			12:13 23:59 9:00	-- -- --	-- -- --	11:54 23:59 8:40	12:24 23:59 8:58	11:19 23:59 9:55	12:20 23:59 9:01	11:50 23:59 8:03	-- -- --	-- -- --	12:05 23:59 9:43	12:49 23:59 8:46	11:52 23:59 10:19	12:43 23:59 8:02	11:35 23:59 8:14	-- -- --		
3	Ледогоров Вадим Игоревич	01	-- -- --	-- -- --	-- -- --	-- -- --	12:59 23:59 7:33	11:14 23:59 8:58	14:25 23:59 4:05	-- -- --	-- -- --	-- -- --	-- -- --	-- -- --	-- -- --	-- -- --	12:54 23:59 7:26		123:06 (17)	136:00 (17)
			12:11 23:59 7:51	-- -- --	-- -- --	12:52 23:59 8:16	13:11 23:59 5:05	14:19 23:59 6:56	12:49 23:59 8:00	-- -- --	-- -- --	-- -- --	14:02 23:59 7:45	12:28 23:59 8:55	15:19 23:59 5:14	12:19 23:59 7:49	13:49 23:59 5:07	-- -- --		
4	Меньшикова Нина Евгеньевна		-- -- --	-- -- --	-- -- --	-- -- --	11:57 23:59 8:05	7:50 23:59 8:24	-- -- --	9:37 23:59 7:45	-- -- --	-- -- --	-- -- --	-- -- --	-- -- --	11:55 23:59 8:09	7:10 23:59 9:02		141:09 (17)	136:00 (17)
			7:00 23:59 9:17	-- -- --	-- -- --	12:17 23:59 7:51	7:20 23:59 8:51	7:18 23:59 9:05	12:03 23:59 8:05	7:22 23:59 5:36	-- -- --	-- -- --	12:00 23:59 8:02	7:29 23:59 8:49	7:57 23:59 10:24	12:27 23:59 7:35	12:01 23:59 8:01	-- -- --		

ОФИС/parsec 26.01.2015 12:14:05 1/3

Щелкнув по ячейке отчета, можно получить полную детализацию событий, сгенерированных сотрудником в этот день.

11.3.2.6 Приход/уход за неделю

Отчет "Приход/уход за неделю" показывает время прихода, время ухода и отработанное время для выбранных сотрудников в каждый день рабочей недели.

Учет рабочего времени за неделю с 16.06.2014 по 23.06.2014

Подразделение: Сотрудники

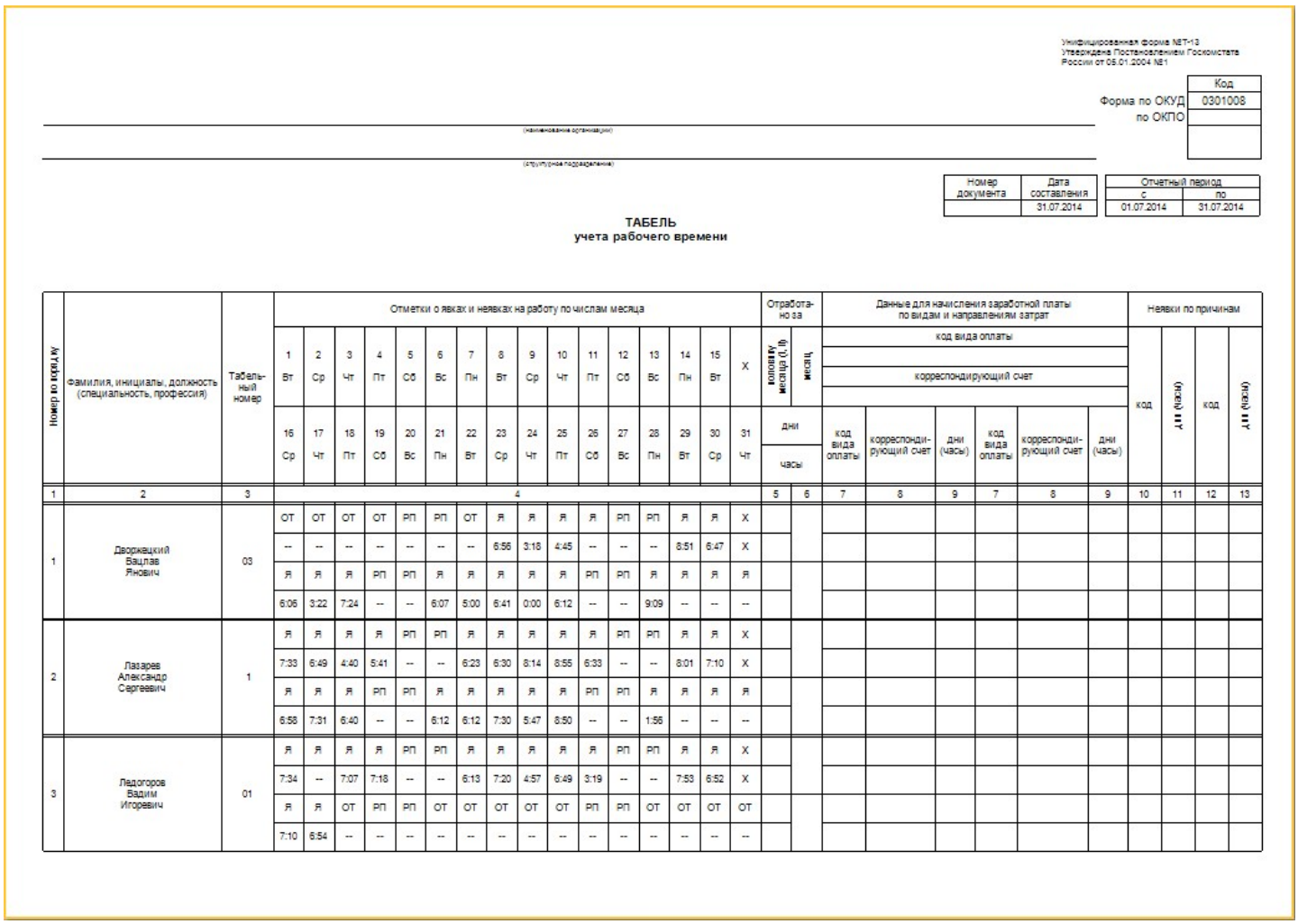
№ п/п	Фамилия, Имя, Отчество	номер	Данные о входе, выходе и отработанном времени							Всего часов (дней)	Норма часов (дней)
			16 Пн	17 Вт	18 Ср	19 Чт	20 Пт	21 Сб	22 Вс		
1	Дворжецкий Вацлав Янович	03	14:06 23:01 8:54	13:06 18:40 5:33	9:46 22:45 12:59	14:53 18:20 3:26				30:53 (4)	40:00 (5)
2	Лазарев Александр Сергеевич	1	11:35 20:56 9:21	12:55 21:12 8:17	12:47 21:06 8:19	12:54 20:35 7:41	12:59 21:25 8:26			42:05 (5)	40:00 (5)
3	Ледогоров Вадим Игоревич	01	12:54 22:36 9:41	12:08 20:06 7:58	13:21 19:55 6:33	14:42 20:15 5:32	15:27 19:02 3:34			33:20 (5)	40:00 (5)
4	Меньшикова Нина Евгеньевна		-- -- 8:00	-- -- 8:00	-- -- 8:00	-- -- 8:00	-- -- 8:00			40:00 (5)	40:00 (5)
5	Метёлкина Елена Владимировна	26	9:16 18:00 8:43	10:31 18:23 7:52	10:49 18:52 8:02	12:27 18:01 8:00	10:10 15:46 5:35			38:14 (5)	40:00 (5)
6	Михайлов Александр Яковлевич	05	13:19 18:52 5:33	13:40 20:41 7:00	14:30 20:58 6:28	13:22 20:18 6:56	13:28 21:33 8:05			34:04 (5)	40:00 (5)
7	Нахапетов Родион Рафаилович	28	11:54 20:07 8:12	7:55 16:16 8:20	-- -- 8:00	-- -- 8:00	14:38 19:30 8:00			40:33 (5)	40:00 (5)
8	Нильская Людмила Валерьяновна	15	8:59 18:00 9:00	8:51 17:36 8:44	8:40 17:38 8:58	8:39 18:01 9:22	8:24 12:56 4:31			40:36 (5)	40:00 (5)

ОФИС/parsec 18.08.2014 12:52:43 1/1

Щелкнув по ячейке отчета, можно получить полную детализацию событий, сгенерированных сотрудником в этот день.

11.3.2.7 Табель за месяц

На рисунке ниже представлен месячный табель учета рабочего времени по форме Т-13.



Унифицированная форма №Т-13
Утверждена Постановлением Госкомстата России от 05.01.2004 №1

	Код
Форма по ОКУД	0301008
по ОКПО	

(наименование организации)

(структурное подразделение)

Номер документа	Дата составления	Отчетный период с	Отчетный период по
	31.07.2014	01.07.2014	31.07.2014

ТАБЕЛЬ
учета рабочего времени

Номер по порядку	Фамилия, инициалы, должность (специальность, профессия)	Табельный номер	Отметки о явках и неявках на работу по числам месяца																Отработано за		Данные для начисления заработной платы по видам и направлениям затрат						Неявки по причинам			
			1 Вт	2 Ср	3 Чт	4 Пт	5 Сб	6 Вс	7 Пн	8 Вт	9 Ср	10 Чт	11 Пт	12 Сб	13 Вс	14 Пн	15 Вт	X	половину месяца (I, II)	месяц	код вида оплаты						код	(дни)	код	(дни)
			16 Ср	17 Чт	18 Пт	19 Сб	20 Вс	21 Пн	22 Вт	23 Ср	24 Чт	25 Пт	26 Сб	27 Вс	28 Пн	29 Вт	30 Ср	31 Чт	дни	часы	код вида оплаты	корреспондирующий счет	дни (часы)	код вида оплаты	корреспондирующий счет	дни (часы)				
1	2	3	4																5	6	7	8	9	7	8	9	10	11	12	13
1	Дворжецкий Вацлав Янович	03	ОТ	ОТ	ОТ	ОТ	РП	РП	ОТ	Я	Я	Я	Я	РП	РП	Я	Я	X												
			--	--	--	--	--	--	--	6:56	3:18	4:45	--	--	--	8:51	6:47	X												
			Я	Я	Я	РП	РП	Я	Я	Я	Я	Я	РП	РП	Я	Я	Я	Я												
			6:06	3:22	7:24	--	--	6:07	5:00	6:41	0:00	6:12	--	--	9:09	--	--	--												
2	Лазарев Александр Сергеевич	1	Я	Я	Я	Я	РП	РП	Я	Я	Я	Я	Я	РП	РП	Я	Я	X												
			7:33	6:49	4:40	5:41	--	--	6:23	6:30	8:14	8:55	6:33	--	--	8:01	7:10	X												
			Я	Я	Я	РП	РП	Я	Я	Я	Я	Я	РП	РП	Я	Я	Я	Я												
			6:58	7:31	6:40	--	--	6:12	6:12	7:30	5:47	8:50	--	--	1:56	--	--	--												
3	Ледогоров Вадим Игоревич	01	Я	Я	Я	Я	РП	РП	Я	Я	Я	Я	Я	РП	РП	Я	Я	X												
			7:34	--	7:07	7:18	--	--	6:13	7:20	4:57	6:49	3:19	--	--	7:53	6:52	X												
			Я	Я	ОТ	РП	РП	ОТ	ОТ	ОТ	ОТ	ОТ	РП	РП	ОТ	ОТ	ОТ	ОТ												
			7:10	6:54	--	--	--	--	--	--	--	--	--	--	--	--	--	--												

Щелкнув по ячейке отчета, можно получить полную детализацию событий, сгенерированных сотрудником в этот день.

Расшифровка кодов интервалов рабочего времени формы Т-13 приведена в таблице:

Таблица 1. Коды и наименования интервалов учёта рабочего времени.

Наименование интервала учёта рабочего времени	Код буквенный	Код цифровой
Часы (дни) работы по факту присутствия дневные	**Я**	**01**
Ночные часы работы	**Н**	**02**
Работа в выходные и праздничные дни	**РП**	**03**
Сверхурочные часы работы	**С**	**04**
Служебные командировки	**К**	**06**
Ежегодный отпуск (оплачиваемый)	**ОТ**	**09**
Отпуск без сохранения содержания (не оплачиваемый)	**ДО**	**16**
Временная нетрудоспособность (оплачиваемый больничный)	**Б**	**19**
Прогулы	**ПР**	**24**

Выходные и праздничные дни	**В**	**26**
Опоздания	**ОП**	**-**
Преждевременный уход с работы	**УХ**	**-**
Неустроен на работу	**Х**	**-**
Присутствие без проходов (если сотрудник забыл свой пропуск)	**БПР**	**43**

Правила расчёта рабочего времени в системе

Неявка на работу без уважительной причины или отсутствие на работе без уважительной причины более 4 часов (непрерывно) в течение расчётного дня приводят табеле Т-13 к формированию прогула за анализируемый день.

При формировании табеля за месяц учитываются поправки рабочего времени, т.е. учитывается время, указанное в нормах отработки (см. п. Настройка расписания рабочего времени[238]).

Что засчитывается в рабочее время:

- Фактически отработанное время с кодом 01;
- Сверхурочные часы (переработка) за отчетный период. Рассчитывается как превышение нормы, код 05;
- Служебная командировка, с временем по дневной норме (например, 8 часов) с кодом 10;
- Работа в выходные и праздничные дни. Заносится с кодом 03.

Что засчитывается в отсутствие:

- Оплачиваемый отпуск с кодом 14. Время из нормы за день;
- Больничный с кодом 25. Время берётся из нормы за день;
- Прогулы с кодом 31. Прогул – это отсутствие более 4 часов в день или полное отсутствие на территории;

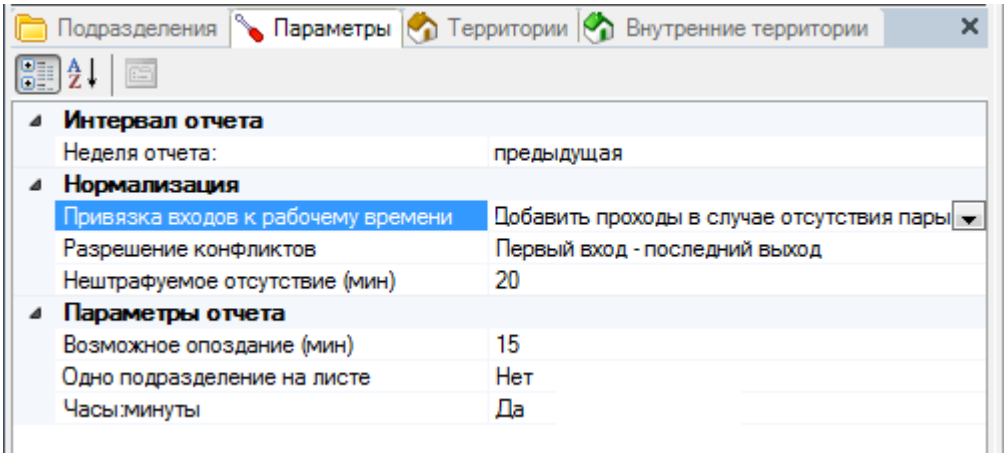
Если сотрудник отсутствует в границах прихода/ухода, но присутствовал в рабочее время (доступ разрешён), то это будет считаться прогулом.

- Преждевременный уход с работы с кодом 36. Как уход раньше границы ухода;
- Отпуск без сохранения содержания (неоплачиваемый).

11.3.3 Отчёты по учёту рабочего времени

Данная версия модуля составления отчетов УРВ устарела и более не поддерживается. Настоятельно рекомендуется использовать для формирования отчетов инструмент "Бизнес-отчеты (версия 4)[469] "

Поскольку задача модуля УРВ – посчитать отработанное сотрудниками время за выбранный период и сравнить его с плановым, то алгоритм расчёта рабочего времени для отчётов был унифицирован: для решения поставленной задачи разработан список параметров нормализации интервалов присутствия, которые влияют на результат расчёта.



В системе применяются следующие методы нормализации интервалов присутствия сотрудников на указанных территориях:

1. Данные обрабатываются за конечный интервал времени (например, с 1 по 30 числа месяца), а между интервалами рабочего времени могут быть разные несостыковки, поэтому введены две настройки нормализации – «Привязка входов к рабочему времени»:

- «Изъять проходы в случае отсутствия пары» – при отсутствии у входа или выхода пары до начала следующего рабочего времени данное событие аннулируется.
- «Добавить проходы в случае отсутствия пары» – при наличии входа без выхода, окончанием интервала считается окончание ближайшего интервала рабочего времени (справа). При наличии выхода без входа, началом интервала считается начало ближайшего интервала рабочего времени (слева).

Первая настройка трактует события не в пользу работника, вторая – в его пользу.

2. Для разрешения проблемы отсутствия строго парных событий "вход-выход", можно выбрать следующие методы нормализации – «Разрешение конфликтов»:

- «Первый вход – последний выход» – при последовательности нескольких входов подряд или нескольких выходов подряд, для входов берётся первый, для выходов – последний из ближайшей последовательности выходов, то есть события трактуются в пользу сотрудника.
- «Последний вход – первый выход» – по аналогии с предыдущим пунктом, из последовательных входов берётся последний, из ближайшей последовательности выходов – первый. События трактуются не в пользу сотрудника.
- «Один считыватель» – считается только интервал времени между первым и последним прикладыванием карты (идентификатора) к считывателю.
- «Последний вход – последний выход» – при последовательности нескольких входов подряд или нескольких выходов подряд, для входов берётся последний и для выходов – последний.

При создании отчётов по учёту рабочего времени для сотрудников с разрешённой ночной сменой НЕ РЕКОМЕНДУЕТСЯ использование правила «Первый вход – последний выход».

3. Параметр нормализации «Нештрафуемое отсутствие (мин)»:
Это максимальная длительность отсутствия на рабочем месте, которая игнорируется при учёте отработанного времени. Например, при перекурах за пределами территории (что реально в жизни). Если этот параметр поставить в 0, то мы и будем фактически считать чистое время, так как все, даже короткие отсутствия, будут вычитаться из отработанного времени.

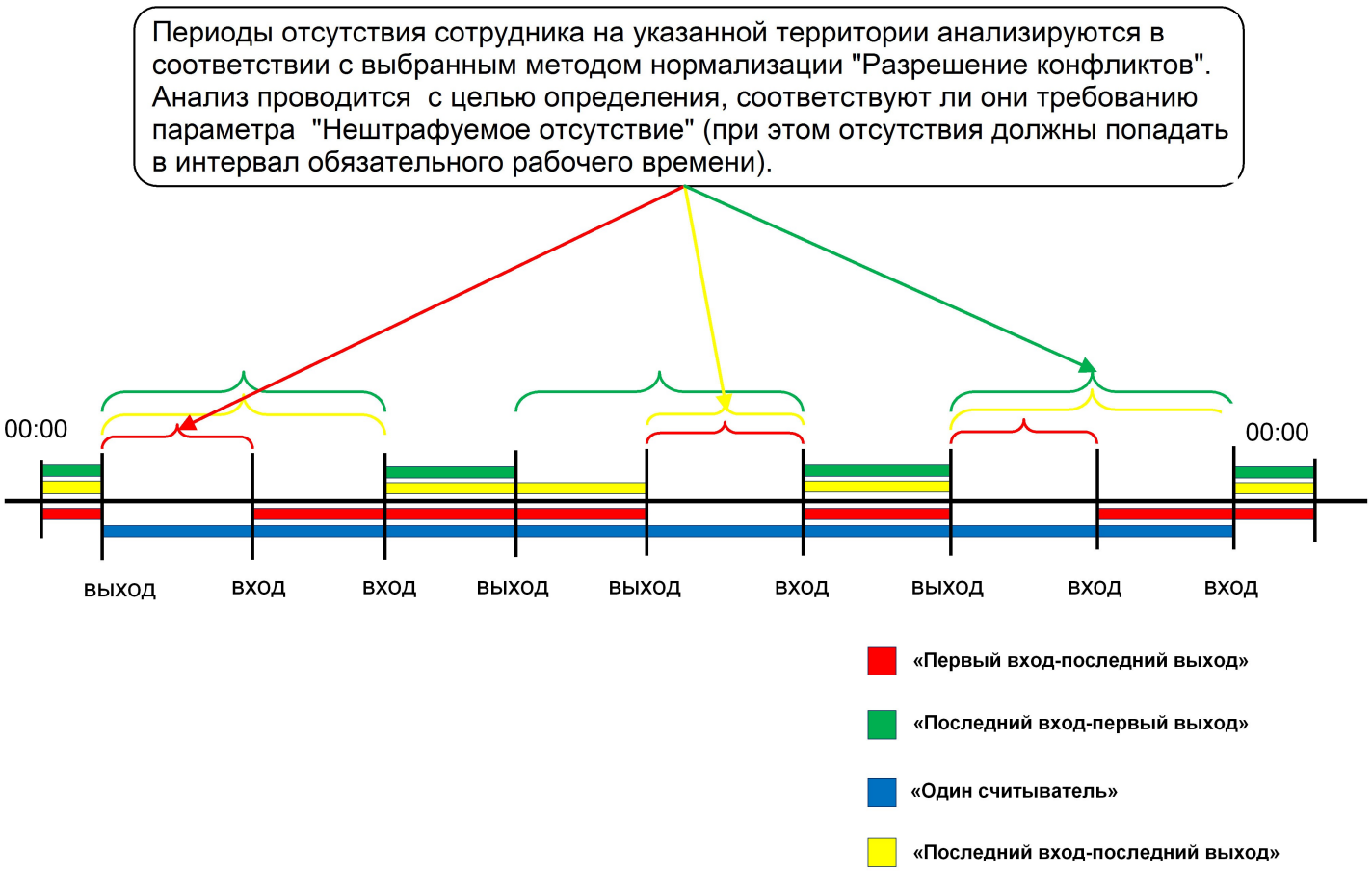
К неочевидным параметрам отчетов можно отнести следующий:

- "Отображать всех сотрудников" - параметр имеет значение "Да" и "Нет". При выборе значения "Нет" те сотрудники, у которых нет данных для отображения, не будут отображаться в отчете. Например, в отчете "Уход раньше времени" отобразятся только те, у которых за отчетный период такие уходы были.

Общий подход к подсчёту параметров для отчёта

На нижеследующем графике приведен пример всех входов и выходов одного сотрудника в течение рабочего дня. Красным цветом обозначены интервалы времени, которые засчитываются при использовании правила «Первый вход – последний выход». Зелёным цветом обозначены те интервалы времени, которые будут суммироваться по правилу «Последний вход – первый выход». Синим цветом выделен интервал времени, который определяется по правилу «Один считыватель». Жёлтым цветом обозначены интервалы времени, которые будут суммироваться по правилу «Последний вход – последний выход».

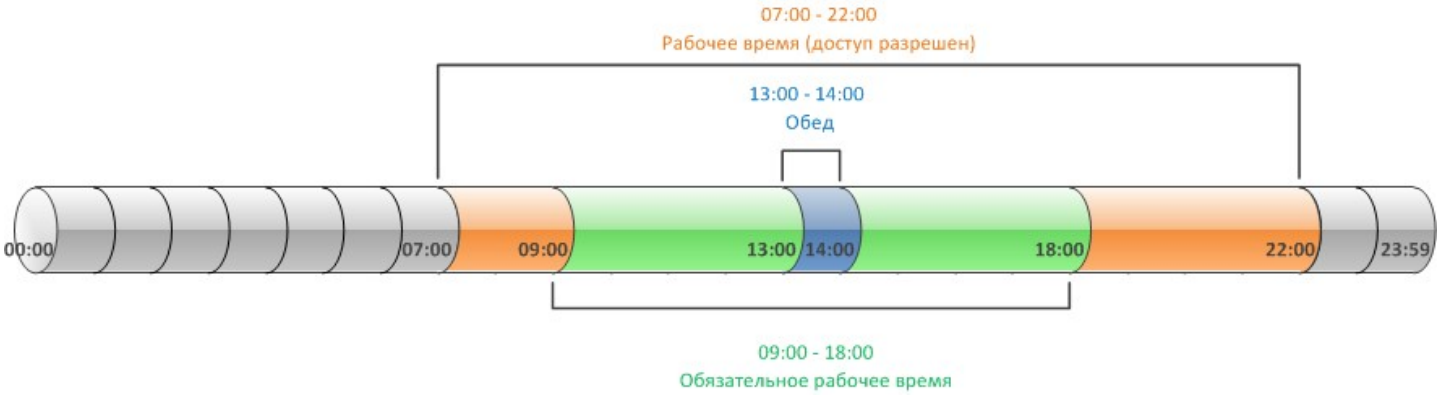
Предполагается включение в параметрах отчётов настройки нормализации «Привязка входов к рабочему времени» – «Добавить проходы в случае отсутствии пары».



Примечание: Отсутствие в рабочее время (РВ) – ситуация, когда сотрудник в обязательное рабочее время сотрудник отсутствовал на территории дольше, чем указано в параметре"Нештрафуемое отсутствие", но меньше 4 часов. В последнем случае в месячном табеле будет указано отсутствие на работе.

Важно: Для корректной работы модуля, после окончания рабочего дня, даже если не было выхода, считаем работника фактически вышедшим за пределы контролируемой территории (независимо от настройки нормализации «Добавить проходы в случае отсутствия пары»).

После проведения выбранных процедур нормализации интервалов присутствия сотрудника на указанной территории получаем следующее представление графика рабочего времени для недельного расписания УРВ:



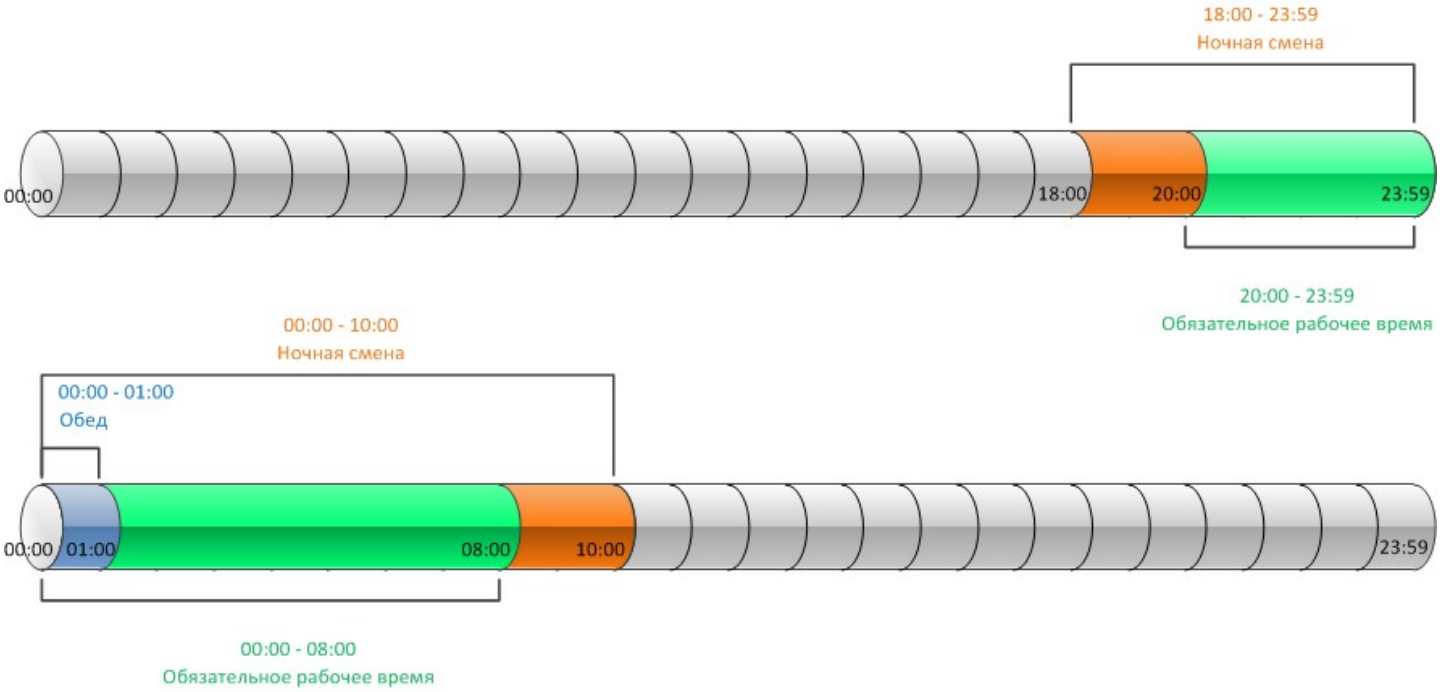
Присутствие сотрудника в пределах интервала "Рабочее время (доступ разрешен)" засчитывается в суммарное рабочее время.

Нарушения фиксируются относительно обязательного рабочего времени.

Обеденный перерыв вычитается из рабочего времени.

Для сменного графика логика примерно такая же с той разницей, что нет обеденного перерыва, а смена переходит через полночь, чего не бывает в обычном недельном расписании.

На следующем рисунке отображен пример графика рабочего времени для случая ночной смены:



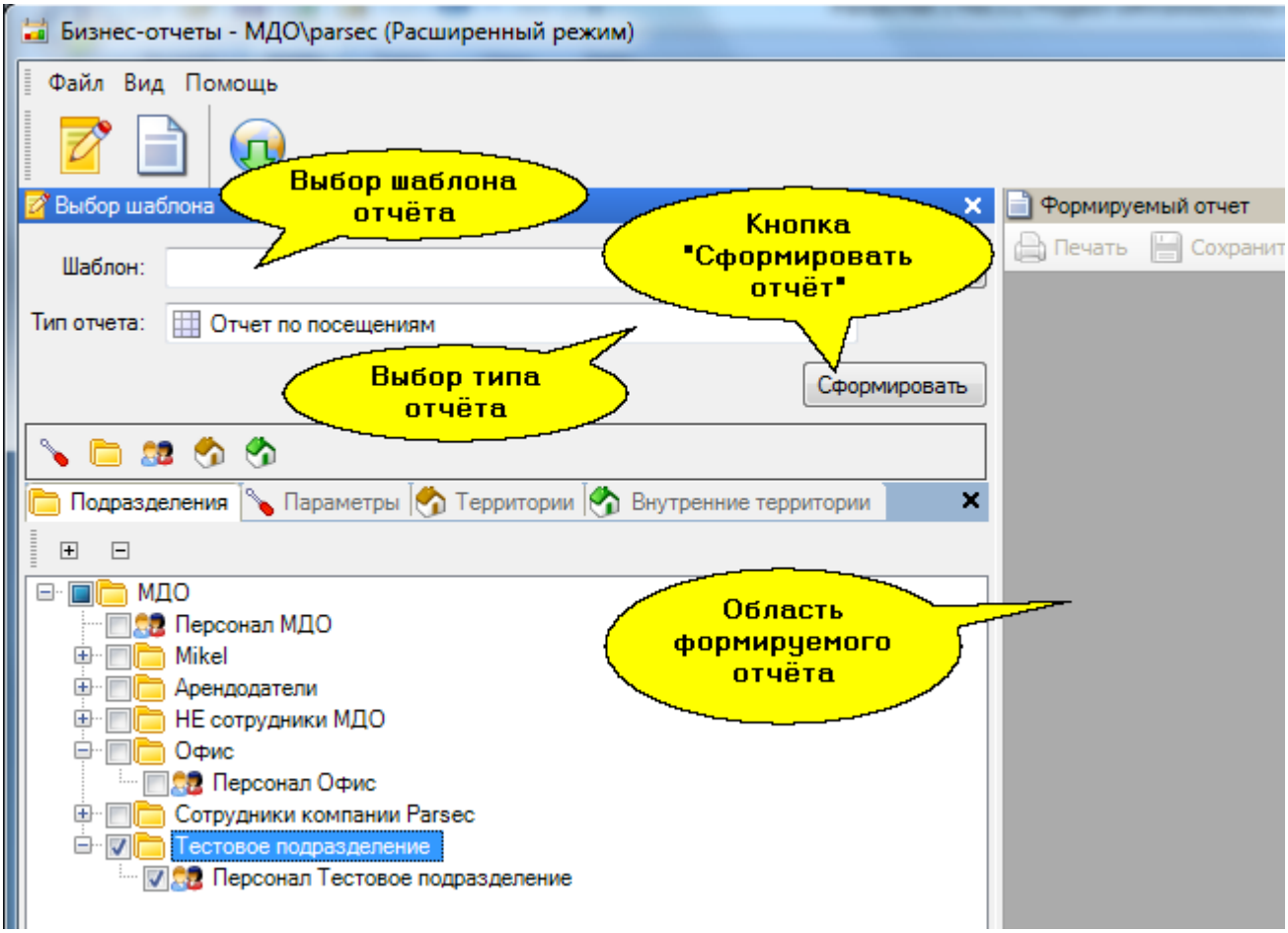
Примечание: Если часть смены или вся смена имеет еще и атрибут ночной смены (он может накладываться на смену), то внутри этого интервала отдельно подсчитывается ночное время, выводимое в табель формы Т13.

11.3.3.1 Построение отчётов

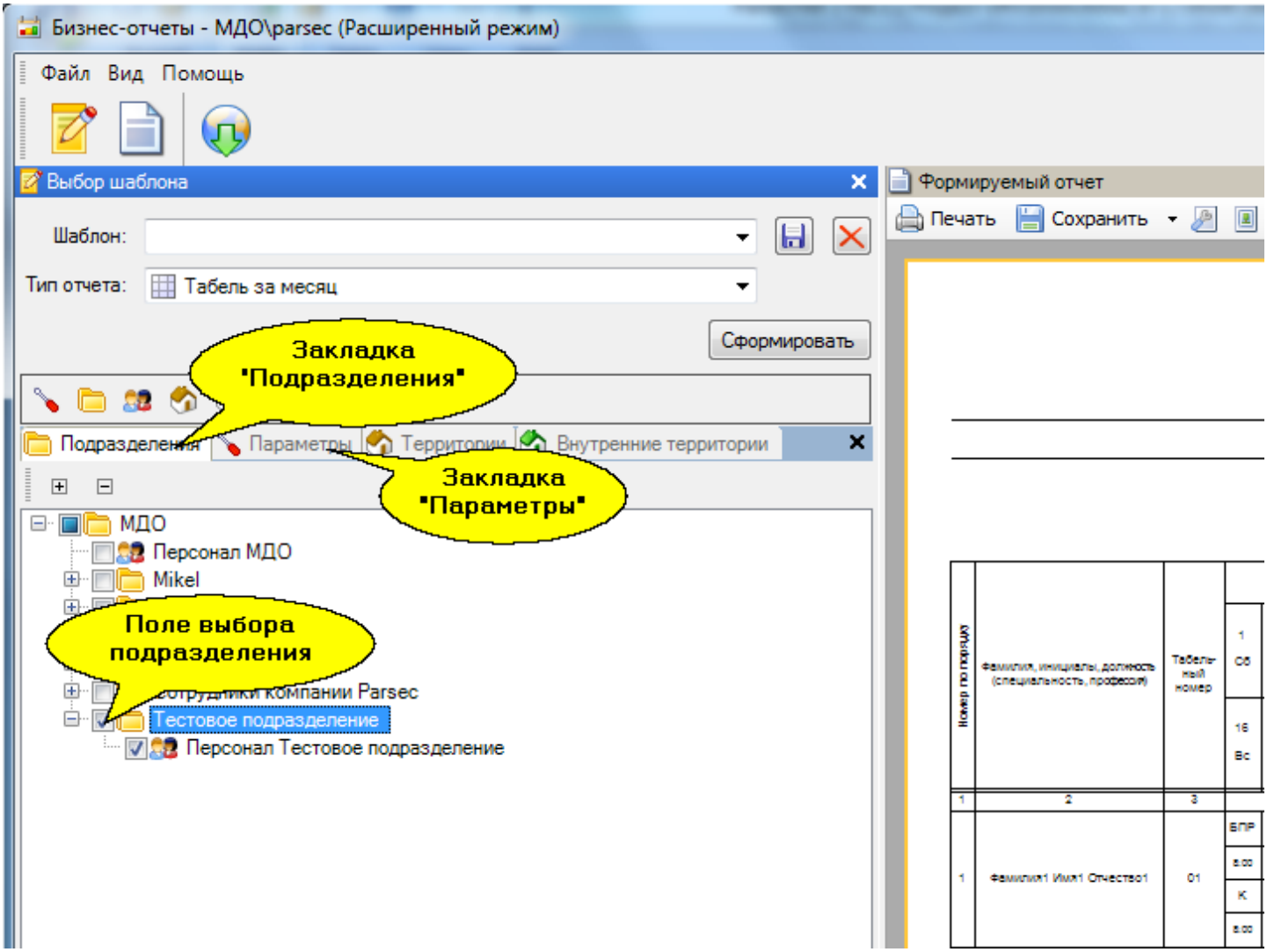
Убедитесь, что подразделению или сотруднику(-ам), по которым необходимо получить отчет, задано расписание рабочего времени[221] .

Откройте редактор Бизнес-отчёты, выполнив команду "Пуск -> Все программы -> Parsec 3 -> Отчеты".

Укажите шаблон отчета (если он сохранен или загружен ранее).



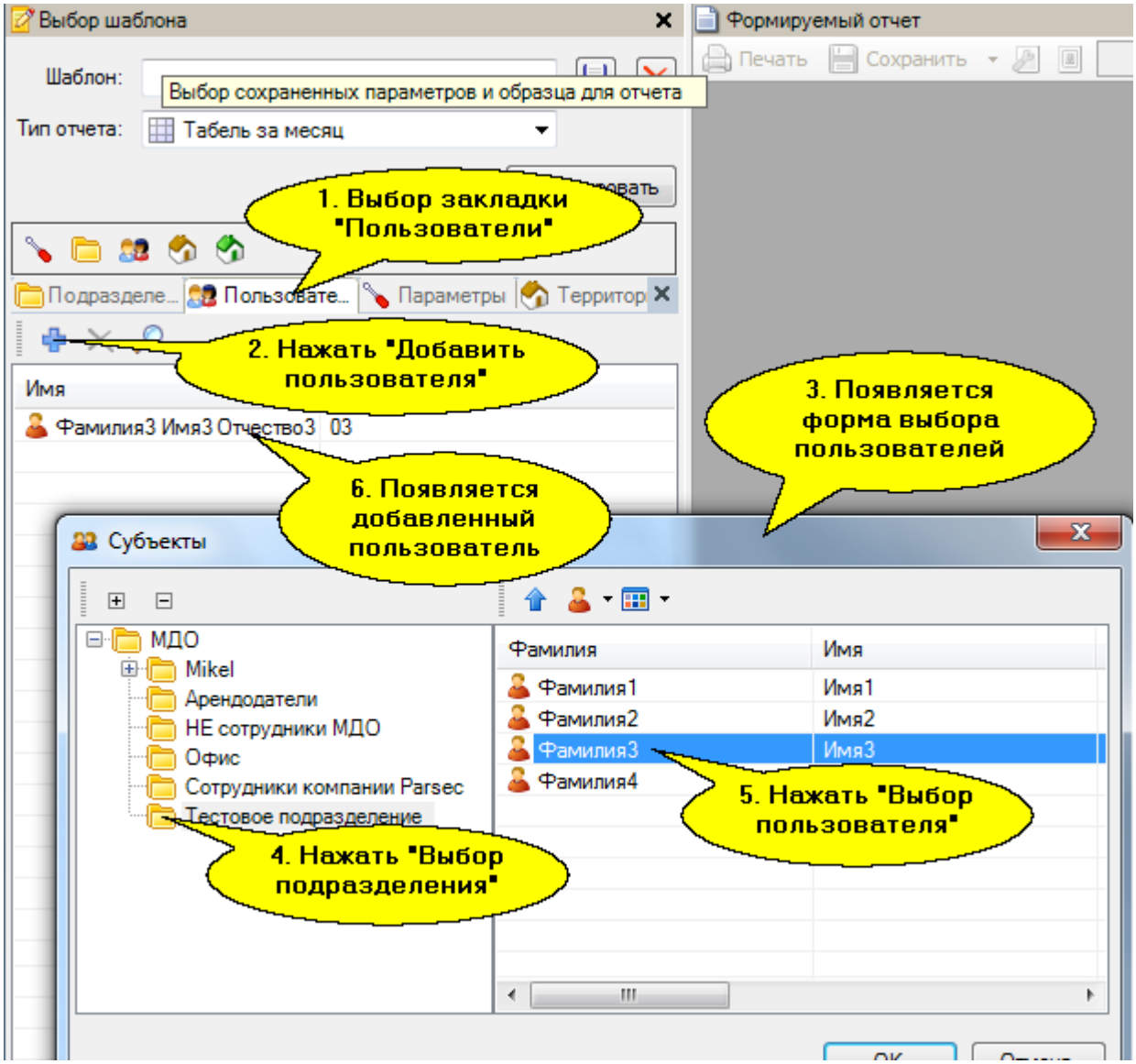
1. Выберите *Тип отчёта*. (При необходимости можно заказать специализированный шаблон отчета у производителя системы, который также будет отображаться в этом списке).
1. Затем перейдите на вкладку *Подразделения* и нажмите на кнопку +, чтобы развернуть дерево подразделений. Установите флажок выбора слева от интересующих Вас подразделений.
1. Задайте нужные параметры отчёта на вкладке *Параметры*, затем нажмите на кнопку *Сформировать*.



Отчёт сформируется справа в области «Формируемый отчёт».

Можно построить отчёт по отдельному пользователю. Для этого выберите закладку «Пользователи» и нажмите на пиктограмму ✚ «Добавить пользователя». Откроется форма выбора пользователей «Субъекты». В этой форме нажмите на значок подразделения, а затем в списке сотрудников - на пользователя (см. рисунок ниже).

Важно: Для построения отчёта для одного пользователя необходимо на вкладке «Подразделения» снять все флажки, так как при их наличии для построения отчёта выбираются все пользователи указанных подразделений .



11.3.3.2 Отчёт по посещениям

На скриншоте ниже представлен отчёт по посещениям.



ОТЧЕТ ПО ПОСЕЩЕНИЯМ

Организация	МДО
Подразделение	

Дата составления	Отчетный период	
	с	по
27.10.2011	01.09.2011	01.10.2011

Номер по порядку	Фамилия, инициалы, должность (специальность, профессия)	Отметки о неявках на работу по числам месяца																												
		1 Чт	2 Пт	3 Сб	4 Вс	5 Пн	6 Вт	7 Ср	8 Чт	9 Пт	10 Сб	11 Вс	12 Пн	13 Вт	14 Ср	15 Чт	16 Пт	17 Сб	18 Вс	19 Пн	20 Вт	21 Ср	22 Чт	23 Пт	24 Сб	25 Вс	26 Пн	27 Вт	28 Ср	29 Чт	30 Пт	-
1	Фамилия1 Имя1 Отчество1			-	-		X				-	-						-	-						-	-					
2	Фамилия2 Имя2 Отчество2			-	-						-	-						-	-						-	-					
3	Фамилия3 Имя3 Отчество3			-	-						-	-			X			-	-						-	-					
4	Фамилия4 Имя4 Отчество4			-	-						-	-							-		-				-	-					

Ответственное лицо _____ (должность) _____ (личная подпись) _____ (расшифровка подписи) «__» _____ 20__ г.

Страница 1 из 1 90%

Отчёт по посещениям позволяет получить данные по всем нарушениям, зафиксированным системой, с учётом заданных правил учёта рабочего времени (расписаний, допустимых отклонений, норм отработки). Отчёт может формироваться за месяц. Кроме того, отчёт может быть выведен как по одному сотруднику, так и по всему выбранному подразделению.

В отчёте используются следующие условные обозначения:

- «-» – выходной;
- «X» – отсутствие;
- Пустая ячейка означает нормально отработанный день.

Для формирования отчёта по посещениям, по аналогии с остальными отчётами, необходимо проделать стандартные шаги:

1. Выбрать тип отчёта;
2. Указать территорию, по которой формируется отчёт;
3. Указать, для какого подразделения (или сотрудника) будем формировать отчёт;
4. Назначить параметры отчёта.

1. После этих шагов можно нажать на кнопку *Сформировать* и получить требуемый отчёт, который можно распечатать или сохранить в файл.

Как и для других отчётов модуля учёта рабочего времени, любой настроенный отчёт можно сохранить в виде шаблона.

Примеры

Для сотрудника установлен период рабочего времени (когда доступ разрешен) с 8.30 до 18.30, а обязательного рабочего времени - с 9.00 до 18.00.

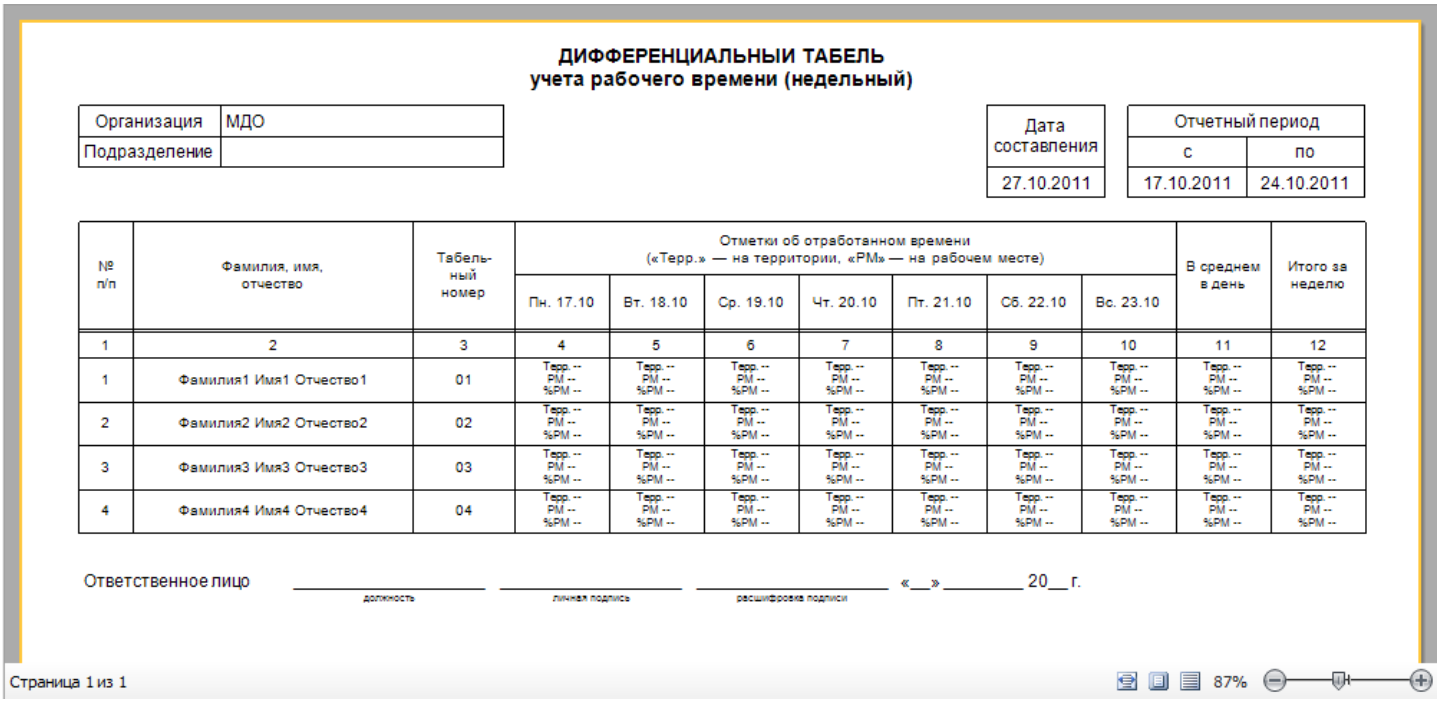
1. Установим в параметрах отчета возможность ухода раньше времени 15 мин.

Сотрудник ушел с работы в 17.40. Система посчитает уход раньше времени на 20 минут.

Если сотрудник ушел с работы в 17.48, то система не будет считать это уходом раньше времени.

11.3.3.3 Дифференциальный отчет

На скриншоте ниже представлен дифференциальный отчёт:



ДИФФЕРЕНЦИАЛЬНЫЙ ТАБЕЛЬ
учета рабочего времени (недельный)

Организация	МДО
Подразделение	

Дата составления
27.10.2011

Отчетный период	
с	по
17.10.2011	24.10.2011

№ п/п	Фамилия, имя, отчество	Табельный номер	Отметки об отработанном времени («Терр.» — на территории, «РМ» — на рабочем месте)							В среднем в день	Итого за неделю
			Пн. 17.10	Вт. 18.10	Ср. 19.10	Чт. 20.10	Пт. 21.10	Сб. 22.10	Вс. 23.10		
1	2	3	4	5	6	7	8	9	10	11	12
1	Фамилия1 Имя1 Отчество1	01	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --
2	Фамилия2 Имя2 Отчество2	02	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --
3	Фамилия3 Имя3 Отчество3	03	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --
4	Фамилия4 Имя4 Отчество4	04	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --	Терр. -- РМ -- %РМ --

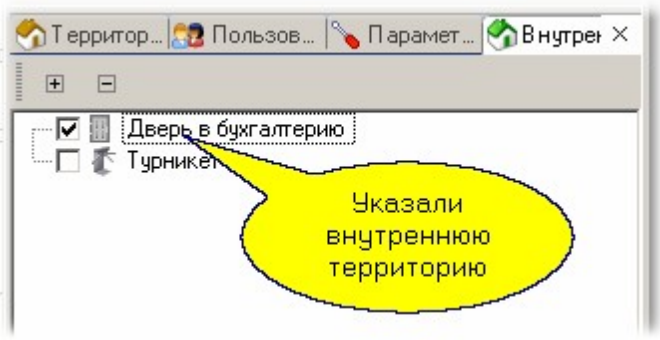
Ответственное лицо _____ должность _____ личная подпись _____ расшифровка подписи «__» _____ 20__ г.

Страница 1 из 1 87%

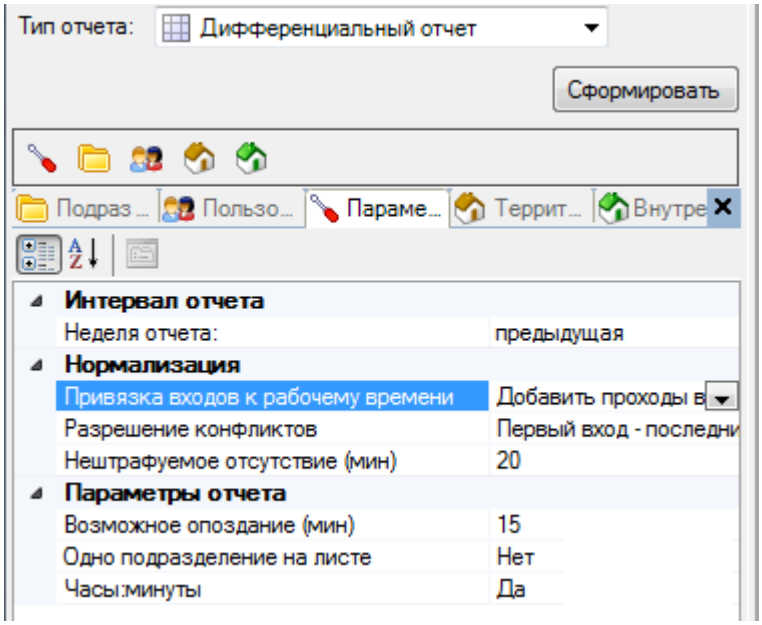
Дифференциальный отчет представляет собой разновидность недельного табеля с одной важной особенностью: он позволяет оценить эффективность использования рабочего времени сотрудника путем определения, какую часть этого времени сотрудник провел на территории предприятия вообще и какую часть времени - непосредственно на рабочем месте.

Для получения дифференциального отчета требуется, чтобы двухсторонними точками прохода были оборудованы как вход на предприятие, так и вход в зону, которая считается рабочим местом сотрудника (цех, кабинет и так далее)

Подготовка исходных данных для отчета полностью аналогична подготовке данных для недельного табеля[503], но дополнительно на последней вкладке *Внутренние территории* необходимо указать точки прохода, ограничивающие рабочее место сотрудника (сотрудников):



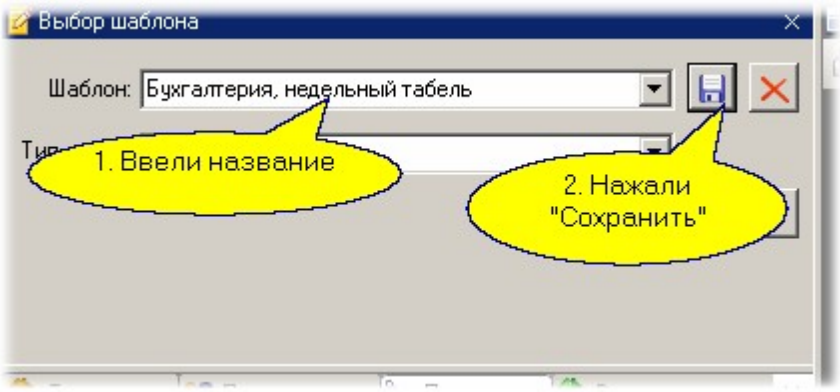
Смысловое значение параметров следующее.



- "Привязка входов к рабочему времени". Если у человека есть вход и нет выхода или есть выход, но нет входа, имеем возможность поступит двояко: либо изъять непарный проход (фактически засчитать прогул), либо добавить парный проход (простить пользователя за то, что он не отметился).
- "Разрешение конфликтов". Относится к двойным (и более) входам или выходам, то есть когда есть два или более входов подряд без соответствующих выходов и наоборот. Засчитывать можно: «первый вход – последний выход» — при последовательности нескольких входов подряд или нескольких выходов подряд, для входов берётся первый, для выходов – последний, то есть события трактуются в пользу сотрудника; «последний вход – первый выход» — по аналогии с предыдущим пунктом, из последовательных входов берётся последний, из последовательности выходов – первый, события трактуются в пользу руководства; «один считыватель» — считается только интервал времени между первым и последним прикладыванием карты (идентификатора) к считывателю; «последний вход – последний выход» — при последовательности нескольких входов подряд или нескольких выходов подряд, для входов берётся последний и для выходов – последний.
- "Нештрафуемое отсутствие". Если сотрудник отсутствовал на территории (рабочем месте) не более указанного интервала времени (за один раз), то этот интервал из рабочего времени не вычитается. Применяется, например, если на перекуры надо выходить за территорию предприятия.
- "Возможное опоздание". Опоздание относительно начала рабочего дня, за которое сотрудник ещё не попадает в нарушители.
- "Одно подразделение на листе". Если мы выбираем эту опцию, то при формировании отчёта по нескольким подразделениям за один раз отчёт для каждого подразделения будет начинаться с новой страницы.
- "Часы:минуты". Формат вывода результатов расчёта. При установке «Нет» время будет выводиться в виде десятичной дроби, например, 16,8 часа.

Как видно на рисунке вверху, в параметрах мы выбрали «Предыдущая». Расчёт недельного табеля за текущую (не закончившуюся) неделю будет некорректным.

1. Если вам такой отчёт придётся в дальнейшем формировать регулярно, то следует настроенные параметры сохранить в виде шаблона. Для этого введите в поле *Шаблон* его название, например, «Бухгалтерия, недельный табель» и нажмите *Сохранить*:

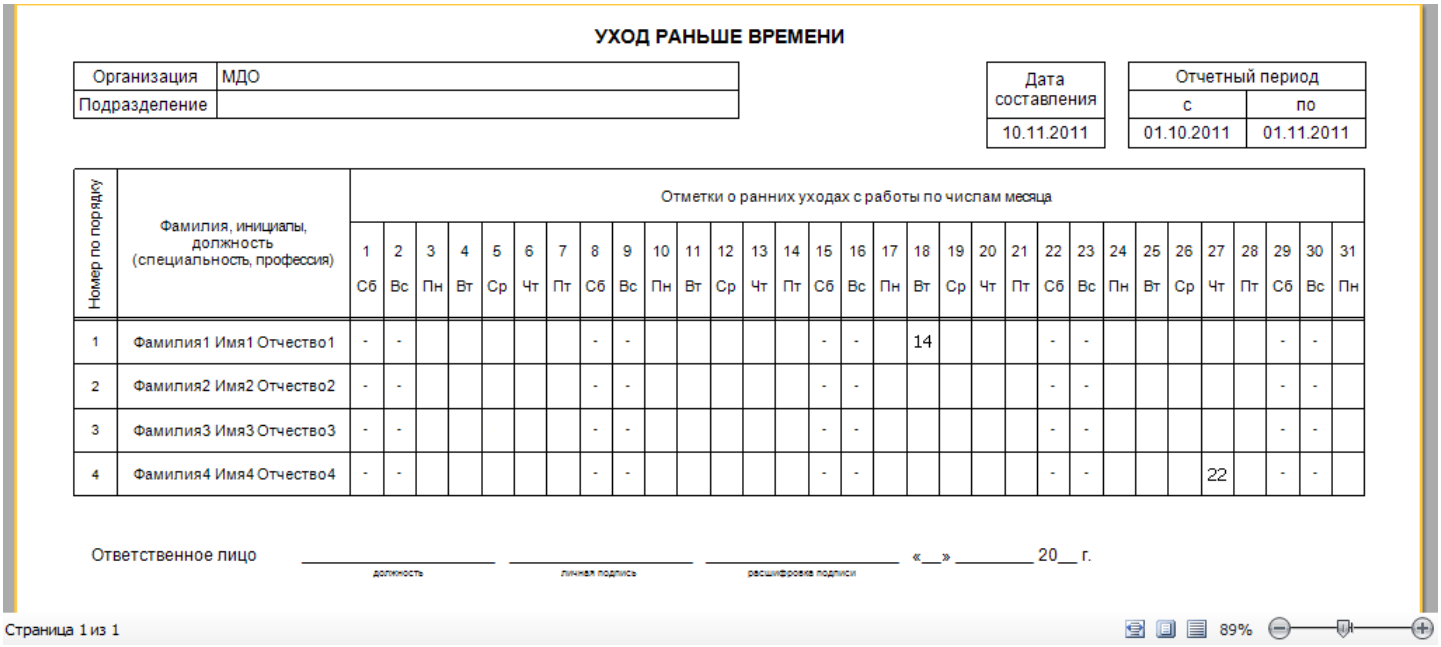


Как и для других отчетов модуля УРВ, любой настроенный дифференциальный отчет можно сохранить в виде шаблона. Работа с шаблонами в инструментах отчётов описана в дополнительном подразделе[314].

1. После выбора всех параметров необходимо нажать на кнопку *Сформировать*, и результирующий отчёт появится в правой панели рабочего окна. Вы можете отправить его сразу на печать на любой доступный принтер, либо сохранить в одном из возможных форматов в файл на диске.

11.3.3.4 Уход раньше времени

На скриншоте ниже представлен отчёт по уходу раньше времени (рис. 50).



УХОД РАНЬШЕ ВРЕМЕНИ

Организация	МДО
Подразделение	

Дата составления	Отчетный период	
	с	по
10.11.2011	01.10.2011	01.11.2011

Номер по порядку	Фамилия, инициалы, должность (специальность, профессия)	Отметки о ранних уходах с работы по числам месяца																													
		1 Сб	2 Вс	3 Пн	4 Вт	5 Ср	6 Чт	7 Пт	8 Сб	9 Вс	10 Пн	11 Вт	12 Ср	13 Чт	14 Пт	15 Сб	16 Вс	17 Пн	18 Вт	19 Ср	20 Чт	21 Пт	22 Сб	23 Вс	24 Пн	25 Вт	26 Ср	27 Чт	28 Пт	29 Сб	30 Вс	31 Пн
1	Фамилия1 Имя1 Отчество1	-	-						-	-						-	-		14				-	-						-	-	
2	Фамилия2 Имя2 Отчество2	-	-						-	-						-	-						-	-						-	-	
3	Фамилия3 Имя3 Отчество3	-	-						-	-						-	-						-	-						-	-	
4	Фамилия4 Имя4 Отчество4	-	-						-	-						-	-						-	-			22			-	-	

Ответственное лицо _____ должность _____ личная подпись _____ расшифровка подписи «__» _____ 20__ г.

Страница 1 из 1 89%

Отчёт по уходу раньше времени позволяет получить данные по уходам раньше времени с работы сотрудниками, которые зафиксированы системой, с учётом заданных правил учёта рабочего времени (расписаний, допустимых отклонений, норм отработки). Отчёт может формироваться за месяц. Кроме того, отчёт может быть выведен как по одному сотруднику, так и по всему выбранному подразделению.

В отчёте используются следующие условные обозначения:

- «-» – выходной;

- «14», «22» – минуты. Система зарегистрировала последний выход сотрудника с территории на указанное количество минут раньше, чем завершился период обязательного рабочего времени данного сотрудника;
- Пустая ячейка означает нормально отработанный день.

Для формирования отчёта по опозданиям, по аналогии с остальными отчётами, необходимо проделать стандартные шаги:

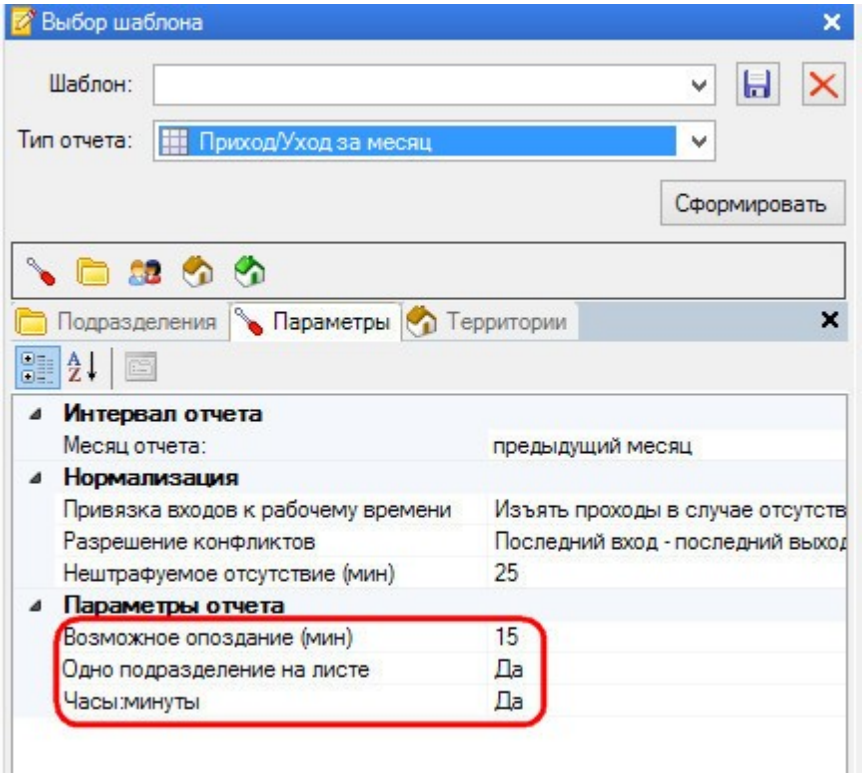
1. Выбрать тип отчёта;
2. Указать территорию, по которой формируется отчёт;
3. Указать, для какого подразделения (или сотрудника) будем формировать отчёт;
4. Назначить параметры отчёта.

1. После этих шагов можно нажать на кнопку *Сформировать* и получить требуемый отчёт, который можно распечатать или сохранить в файл.

Как и для других отчётов модуля учёта рабочего времени, любой настроенный отчёт можно сохранить в виде шаблона.

11.3.3.5 Приход/уход за месяц

Отчет "Приход/уход за месяц" отличается от отчета "Табель за месяц[496] " параметрами, по которым строится отчет. В остальном отчеты аналогичны.



11.3.3.6 Кто ушел последним

Данный отчет позволяет определить, кто из сотрудников покинул территорию последним.

Данный отчет может быть сформирован только для сотрудников, работающих НЕ в ночную смену.

КТО УШЕЛ ПОСЛЕДНИМ

Организация	SYSTEM

Дата составления	Отчетный период	
	с	по
12.10.2015	01.10.2015	12.10.2015

SYSTEM

Дата	Время ухода	Точка прохода	Фамилия Имя Отчество
06.10.2015 Вт	16:40	Проходная	Исаев Максим Юрьевич
07.10.2015 Ср	23:59	авто-выход	Кудюрова Александра Валерьевна
12.10.2015 Пн	12:21	Проходная	Кудюрова Александра Валерьевна

Страница 1

11.3.3.7 Отчёт по опозданиям

На скриншоте ниже представлен отчёт по опозданиям .

ОТЧЕТ ПО ОПОЗДАНИЯМ

Организация	МДО
Подразделение	

Дата составления	Отчетный период	
	с	по
10.11.2011	01.10.2011	01.11.2011

Номер по порядку	Фамилия, инициалы, должность (специальность, профессия)	Отметки об опозданиях на работу по числам месяца																													
		1 Сб	2 Вс	3 Пн	4 Вт	5 Ср	6 Чт	7 Пт	8 Сб	9 Вс	10 Пн	11 Вт	12 Ср	13 Чт	14 Пт	15 Сб	16 Вс	17 Пн	18 Вт	19 Ср	20 Чт	21 Пт	22 Сб	23 Вс	24 Пн	25 Вт	26 Ср	27 Чт	28 Пт	29 Сб	30 Вс	31 Пн
1	Фамилия1 Имя1 Отчество1	-	-						-	-						-	-						-	-						-	-	
2	Фамилия2 Имя2 Отчество2	-	-			6			-	-						-	-						-	-						-	-	
3	Фамилия3 Имя3 Отчество3	-	-						-	-						-	-						-	-						-	-	
4	Фамилия4 Имя4 Отчество4	-	-						-	-						-	-						-	-						-	-	

Ответственное лицо _____ (должность) _____ (личная подпись) _____ (расшифровка подписи) «__» _____ 20__ г.

Страница 1 из 1 89%

Отчёт по опозданиям позволяет получить данные по опозданиям, зафиксированным системой, с учётом заданных правил учёта рабочего времени (расписаний, допустимых отклонений, норм отработки). Отчёт может формироваться за месяц. Кроме того, отчёт может быть выведен как по одному сотруднику, так и по всему выбранному подразделению.

В отчёте используются следующие условные обозначения:

- «-» – выходной;
- «6» – минуты. Система зарегистрировала вход сотрудника на территорию на указанное количество минут позже начала периода обязательного рабочего времени данного сотрудника. ;
- Пустая ячейка означает нормально отработанный день.

Для формирования отчёта по опозданиям, по аналогии с остальными отчётами, необходимо проделать стандартные шаги:

1. Выбрать тип отчёта;
2. Указать территорию, по которой формируется отчёт;

3. Указать, для какого подразделения (или сотрудника) будем формировать отчёт;
4. Назначить параметры отчёта.

1. После этих шагов можно нажать на кнопку *Сформировать* и получить требуемый отчёт, который можно распечатать или сохранить в файл.

Как и для других отчётов модуля учёта рабочего времени, любой настроенный отчёт можно сохранить в виде шаблона.

Примеры

Для сотрудника установлен период рабочего времени (когда доступ разрешен) с 8.30 до 18.30, а обязательного рабочего времени - с 9.00 до 18.00.

1. Установим в параметрах отчета период нештрафуемого отсутствия 30 мин.

В этом случае может возникнуть следующая ситуация: сотрудник пришел на работу в 8.30. В 8.55 ушел (покинул территорию). Вернулся в 9.20. Система "не заметит" его выхода в 8.55 и посчитает, что он начал работу с 8.30.



Алгоритм реализован таким образом, что опоздание считается от момента начала обязательного рабочего времени, что иногда может приводить к коллизиям фактов. Например, доступ на территорию для сотрудника открыт с 8.00, а обязательное рабочее время начинается с 9.00. Величина возможного опоздания задана в 10 минут. Сотрудник пришел в 8.30, а в 8.59 вышел покурить на 15 минут. В этом случае система засчитает ему опоздание.

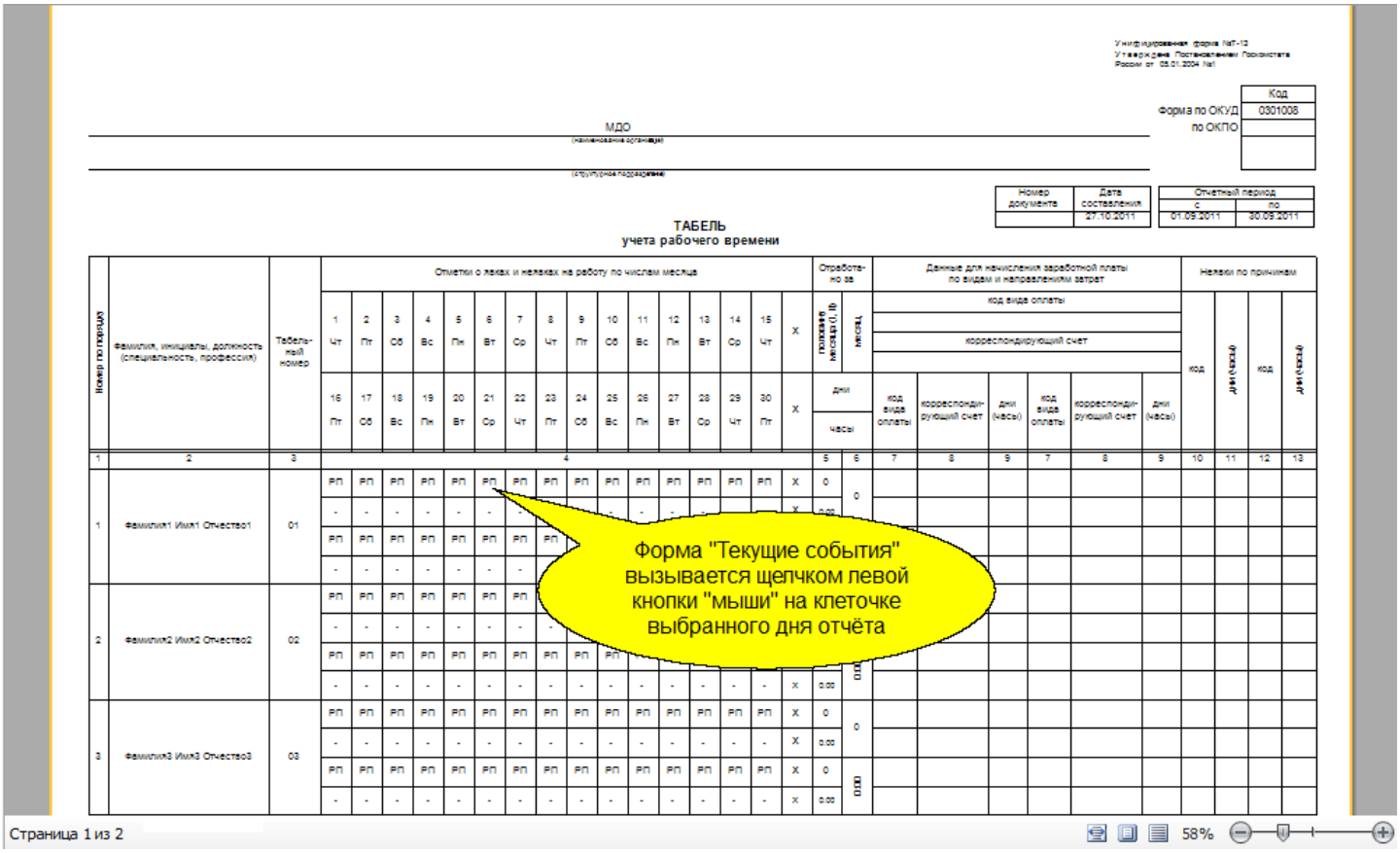
Чтобы избежать подобных ошибочных записей можно задавать большее время разрешенного опоздания.

2. Установим период возможного опоздания 15 мин.

Сотрудник пришел на работу в 9.18. Система посчитает его опоздание - 18 минут.

11.3.3.8 Табель за месяц

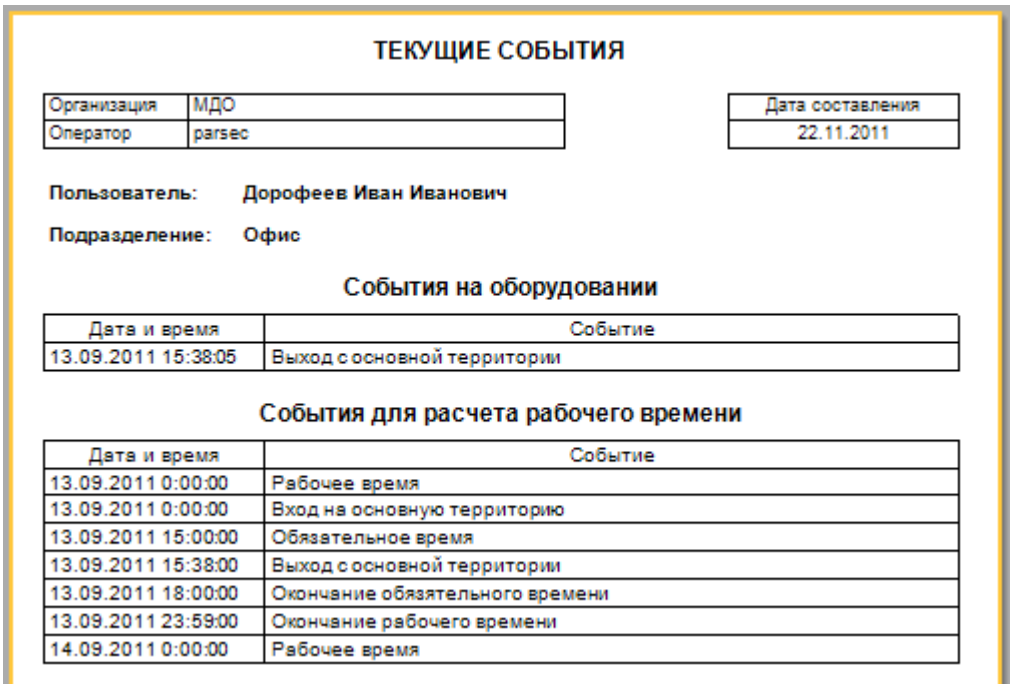
На скриншоте ниже представлен месячный табель учёта рабочего времени по форме Т-13.



Расшифровка кодов интервалов рабочего времени (РП, СП, ОСЧ, К, Б и т.д.) формы Т-13 приведена в табл. 1 ниже по тексту.

Для развёрнутой детализации событий каждого дня отчётного периода применяется отдельная экранная форма *Текущие события*, которая вызывается щелчком левой клавишей мышки по ячейке выбранного дня отчёта.

Такая возможность детализации событий доступна как в «Табеле за месяц», так и в любом другом типе отчёта, кроме «Дифференциального отчёта».



ТЕКУЩИЕ СОБЫТИЯ

Организация	МДО
Оператор	parsec

Дата составления
22.11.2011

Пользователь: **Дорофеев Иван Иванович**

Подразделение: **Офис**

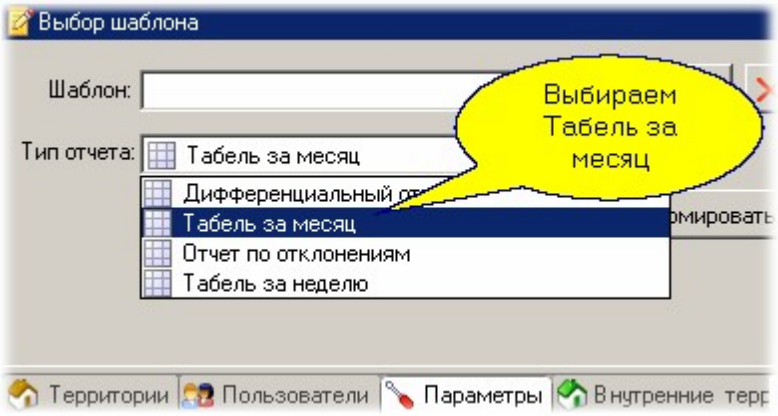
События на оборудовании

Дата и время	Событие
13.09.2011 15:38:05	Выход с основной территории

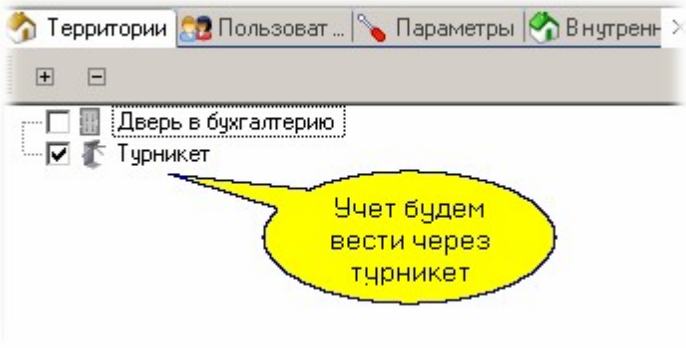
События для расчета рабочего времени

Дата и время	Событие
13.09.2011 0:00:00	Рабочее время
13.09.2011 0:00:00	Вход на основную территорию
13.09.2011 15:00:00	Обязательное время
13.09.2011 15:38:00	Выход с основной территории
13.09.2011 18:00:00	Окончание обязятельного времени
13.09.2011 23:59:00	Окончание рабочего времени
14.09.2011 0:00:00	Рабочее время

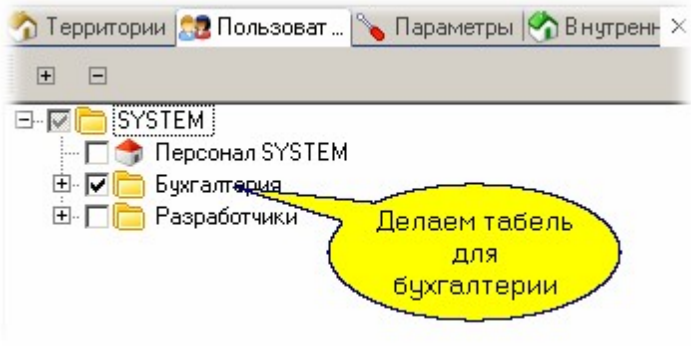
Для формирования месячного табеля учета рабочего времени с выводом результатов по форме Т-13 необходимо в модуле УРВ выбрать из раскрывающегося списка данный тип отчета:



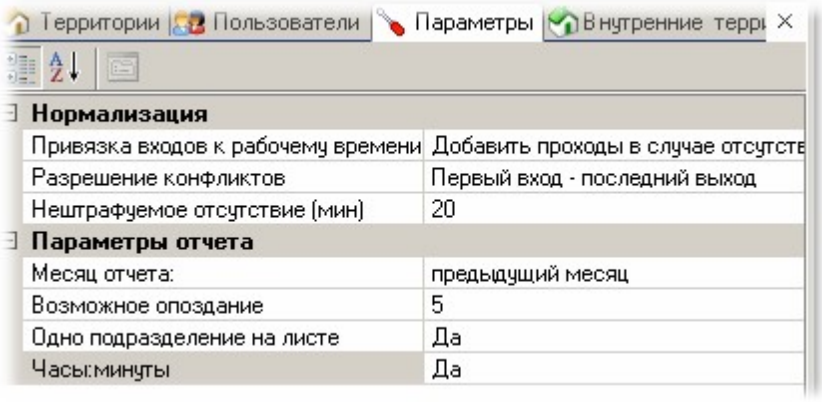
Далее на закладке территорий выбираем точки прохода, по которым ведется учет нахождения сотрудника на рабочем месте (на территории предприятия):



Следующим шагом выбираем подразделение, для которого будет сформирован месячный табель:



На вкладке параметров настраиваем параметры подсчета рабочего времени:

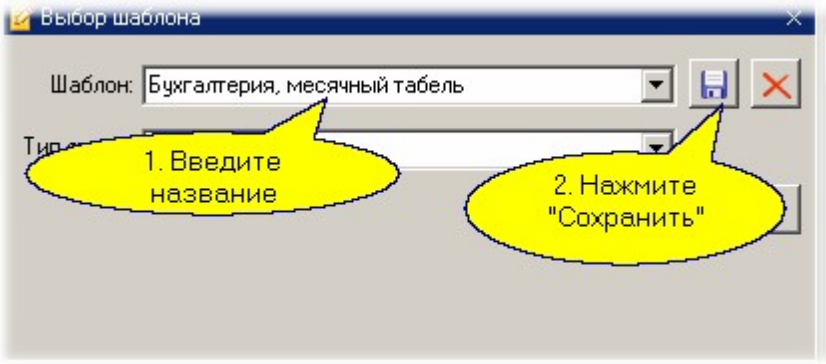


Смысловое значение параметров следующее:

- "Привязка входов к рабочему времени". Если у человека есть вход и нет выхода или есть выход но нет входа, имеем возможность поступит двояко: либо изъять непарный проход (фактически засчитать прогул), либо добавить парный проход (простить сотрудника за то, что он не отметился).
- "Разрешение конфликтов". Относится к двойным (и более) входам или выходам, то есть когда есть два или более входов подряд без соответствующих выходов и наоборот. Засчитывать можно первый из входов и последний из выходов (демократичный вариант), либо последний из входов (первый из выходов) - жесткий вариант подсчета.
- "Нештрафуемое отсутствие". Если сотрудник отсутствовал на территории (рабочем месте) не более указанного интервала времени (за один раз), то этот интервал из рабочего времени не вычитается. Применяется, например, если на перекуры надо выходить за территорию предприятия.
- "Возможное опоздание". Опоздание относительно начала рабочего дня, за которое сотрудник еще не попадает в нарушители.
- "Одно подразделение на листе". Если мы выбираем эту опцию, то при формировании отчета по нескольким подразделениям за один раз отчет для каждого подразделения будет начинаться с новой страницы.
- "Часы:минуты". Формат вывода результатов расчета. При установке "Нет" время будет выводиться в виде десятичной дроби, например, 16,8 часа.

Как видно на рисунке вверху, в параметрах мы выбрали "Предыдущий месяц". Расчет месячного табеля за текущий (не закончившийся) месяц будет некорректным.

Если вам такой отчет придется в дальнейшем формировать регулярно, то следует настроенные параметры сохранить в виде шаблона. Для этого введите в поле *Шаблон* его название, например, "Бухгалтерия, месячный табель" и нажмите *Сохранить*:



Работа с шаблонами в инструментах отчетов описана в дополнительном разделе[314] .

1. После выбора всех параметров необходимо нажать на кнопку *Сформировать*, и результирующий отчет появится в правой панели рабочего окна. Вы можете отправить его сразу на печать на любой доступный принтер, либо сохранить в одним из возможных форматов в файл на диске.

Другие типы отчетов рассмотрены в разделах "Табель за неделю"[503] , "Отчет по отклонениям"[501] и "Дифференциальный отчет"[491]

Правила расчёта рабочего времени в системе

Таблица 1. Коды и наименования интервалов учёта рабочего времени.

Наименование интервала учёта рабочего времени	Код буквенный	Код цифровой
Часы (дни) работы по факту присутствия дневные	**Я**	**01**
Ночные часы работы	**Н**	**02**
Работа в выходные и праздничные дни	**РП**	**03**
Сверхурочные часы работы	**С**	**04**
Служебные командировки	**К**	**06**
Ежегодный отпуск (оплачиваемый)	**ОТ**	**09**
Отпуск без сохранения содержания (не оплачиваемый)	**ДО**	**16**
Временная нетрудоспособность (оплачиваемый больничный)	**Б**	**19**
Прогулы	**ПР**	**24**
Выходные и праздничные дни	**В**	**26**
Опоздания	**ОП**	**-**
Преждевременный уход с работы	**УХ**	**-**
Неустроен на работу	**Х**	**-**
Присутствие без проходов (если сотрудник забыл свой пропуск)	**БПР**	**43**

Неявка на работу без уважительной причины или отсутствие на работе без уважительной причины более 4 часов (непрерывно) в течение расчётного дня приводят к формированию прогула за анализируемый день.

Что засчитывается в рабочее время:

- Фактически отработанное время с кодом 01;
- Фактически отработанное время в ночные часы (если указанно в расписании) с кодом 02;
- Сверхурочные часы (переработка) за отчётный период. Рассчитывается относительно нормы, как её превышение, код 05;
- Служебная командировка, с временем по дневной норме (пример, 8 часов) с кодом 10;
- Работа в выходные и праздничные дни. Заносится с кодом 03, но только для недельного расписания. Если использовать сменное расписание, то работа в выходные и праздники отдельно не обсчитывается.

Что засчитывается в отсутствие:

- Оплачиваемый отпуск с кодом 14. Время из нормы за день;
- Больничный с кодом 25. Время берётся из нормы за день;
- Прогулы заносятся с кодом 31. Прогул – это отсутствие более 4 часов в день или полное отсутствие на территории.

Если сотрудник отсутствует в обязательное рабочее время, но присутствовал в рабочее время (доступ разрешён), то это будет считаться прогулом.

- Преждевременный уход с работы заносятся с кодом 36. Как уход с рабочего времени раньше окончания обязательного рабочего времени;
- Отпуск без сохранения содержания (неоплачиваемый).

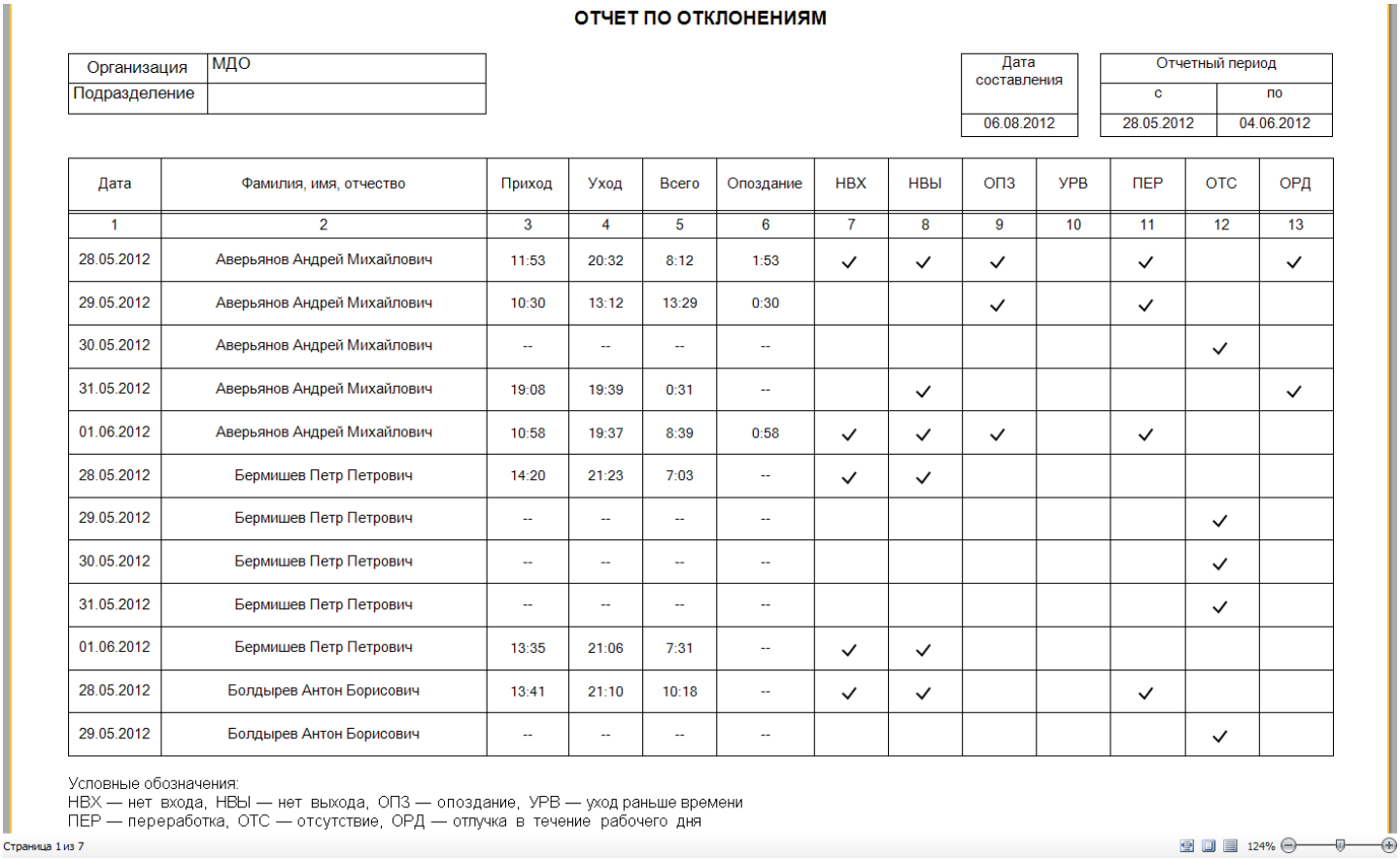
Пояснения к форме Т13:

При формировании табеля за месяц учитываются поправки рабочего времени, т.е. учитывается время, указанное в «нормах отработки»[223].

«Ночная смена» – если интервал указан как ночная смена, то при подсчёте отработанного времени данное время суммируется и заносится с кодом Н (02).

11.3.3.9 Отчёт по отклонениям

На скриншоте ниже представлен отчёт по отклонениям.



ОТЧЕТ ПО ОТКЛОНЕНИЯМ

Организация	МДО
Подразделение	

Дата составления	Отчетный период	
	с	по
06.08.2012	28.05.2012	04.06.2012

Дата	Фамилия, имя, отчество	Приход	Уход	Всего	Опоздание	НВХ	НВЫ	ОПЗ	УРВ	ПЕР	ОТС	ОРД
1	2	3	4	5	6	7	8	9	10	11	12	13
28.05.2012	Аверьянов Андрей Михайлович	11:53	20:32	8:12	1:53	✓	✓	✓		✓		✓
29.05.2012	Аверьянов Андрей Михайлович	10:30	13:12	13:29	0:30			✓		✓		
30.05.2012	Аверьянов Андрей Михайлович	--	--	--	--						✓	
31.05.2012	Аверьянов Андрей Михайлович	19:08	19:39	0:31	--		✓					✓
01.06.2012	Аверьянов Андрей Михайлович	10:58	19:37	8:39	0:58	✓	✓	✓		✓		
28.05.2012	Бермишев Петр Петрович	14:20	21:23	7:03	--	✓	✓					
29.05.2012	Бермишев Петр Петрович	--	--	--	--						✓	
30.05.2012	Бермишев Петр Петрович	--	--	--	--						✓	
31.05.2012	Бермишев Петр Петрович	--	--	--	--						✓	
01.06.2012	Бермишев Петр Петрович	13:35	21:06	7:31	--	✓	✓					
28.05.2012	Болдырев Антон Борисович	13:41	21:10	10:18	--	✓	✓			✓		
29.05.2012	Болдырев Антон Борисович	--	--	--	--						✓	

Условные обозначения:
НВХ — нет входа, НВЫ — нет выхода, ОПЗ — опоздание, УРВ — уход раньше времени
ПЕР — переработка, ОТС — отсутствие, ОРД — отлучка в течение рабочего дня

Страница 1 из 7 124%

Отчёт по отклонениям позволяет получить данные по всем нарушениям, зафиксированным системой, с учётом заданных правил учёта рабочего времени (расписаний, допустимых отклонений, норм отработки). Отчёт может формироваться за день, неделю или месяц. Кроме того, в параметрах можно установить «Показывать всех сотрудников» – в этом случае в отчёт попадут все сотрудники, а не только те, у которых имелись отклонения на заданном интервале времени.

В отчёте для каждого сотрудника указываются (в часах и минутах):

- Время его первого прихода;
- Время последнего ухода;
- Сумма отработанного за день времени;
- Величина опоздания.

Кроме того, в отчёт включаются следующие отклонения:

- ***Нет входа*** *(сокращение НВХ).* Формируется в случае, если у сотрудника был выход с территории, но соответствующий ему вход не зафиксирован;
- ***Нет выхода*** *(сокращение НВЫ).* Формируется в случае, если у сотрудника был вход на территорию, но соответствующий ему выход не зафиксирован;
- ***Опоздание*** *(ОПЗ).* Формируется в случае, если зафиксирован приход сотрудника позже начала рабочего дня на величину более допустимого опоздания. Например, возможное опоздание установлено на 5 минут, начало рабочего дня в 9:00, а сотрудник пришёл в 9:08 - в этой ситуации опоздание будет зафиксировано;
- ***Уход раньше времени*** *(сокращение УРВ).* Фиксируется при уходе сотрудника с рабочего места раньше окончания рабочего дня;
- ***Переработка*** *(сокращение ПЕР).* Формируется в случае, если в конкретный день сотрудник переработал установленную при настройке системы (в расписании) дневную норму;

- ***Отсутствие*** *(сокращение ОТС).* Отклонение фиксируется, если присутствие сотрудника на рабочем месте в данный день не зафиксировано. В отличие от месячного табеля, требуется полное отсутствие. В месячном табеле прогул засчитывается при отсутствии на рабочем месте в течение 4 и более часов;
- ***Отлучка в течение рабочего дня*** *(ОРД).* Нарушение фиксируется, если сотрудник покидал территорию на время большее, чем указано в параметре «Нештрафуемое отсутствие».

Для формирования отчёта по отклонениям, по аналогии с остальными отчётами, необходимо проделать стандартные шаги:

1. Выбрать тип отчёта;
2. Указать территорию, по которой формируется отчёт;
3. Указать, для какого подразделения (или сотрудника) будем формировать отчёт;
4. Назначить параметры отчёта.

1. После этих шагов можно нажать на кнопку *Сформировать* и получить требуемый отчёт, который можно распечатать или сохранить в файл.

Как и для других отчётов модуля учёта рабочего времени, любой настроенный отчёт можно сохранить в виде шаблона.

11.3.3.10 Посещения за месяц

Отчет "Посещения за месяц" отображает посещение сотрудником своего рабочего места в каждое число месяца.

Состояния, обозначенные условными символами, вычисляются модулем УРВ на основе транзакций, формируемых контроллерами доступа.

ТАБЕЛЬ УЧЕТА ПОСЕЩЕНИЙ

Организация	МДО
Подразделение	

Дата составления
05.07.2013

Отчетный период	
с	по
01.07.2013	05.07.2013

Номер по порядку	Фамилия, инициалы, должность (специальность, профессия)	Отметки о посещениях по числам месяца																													
		1 Пн	2 Вт	3 Ср	4 Чт	5 Пт	6 Сб	7 Вс	8 Пн	9 Вт	10 Ср	11 Чт	12 Пт	13 Сб	14 Вс	15 Пн	16 Вт	17 Ср	18 Чт	19 Пт	20 Сб	21 Вс	22 Пн	23 Вт	24 Ср	25 Чт	26 Пт	27 Сб	28 Вс	29 Пн	30 Вт	31 Ср
1	Бурков Дмитрий Владимирович	О	У	О	У	О																										
2	Виноградов Юрий Валентинович	У	О	О	У																											
3	Исаева Александра Валерьевна	У	Б	Б																												

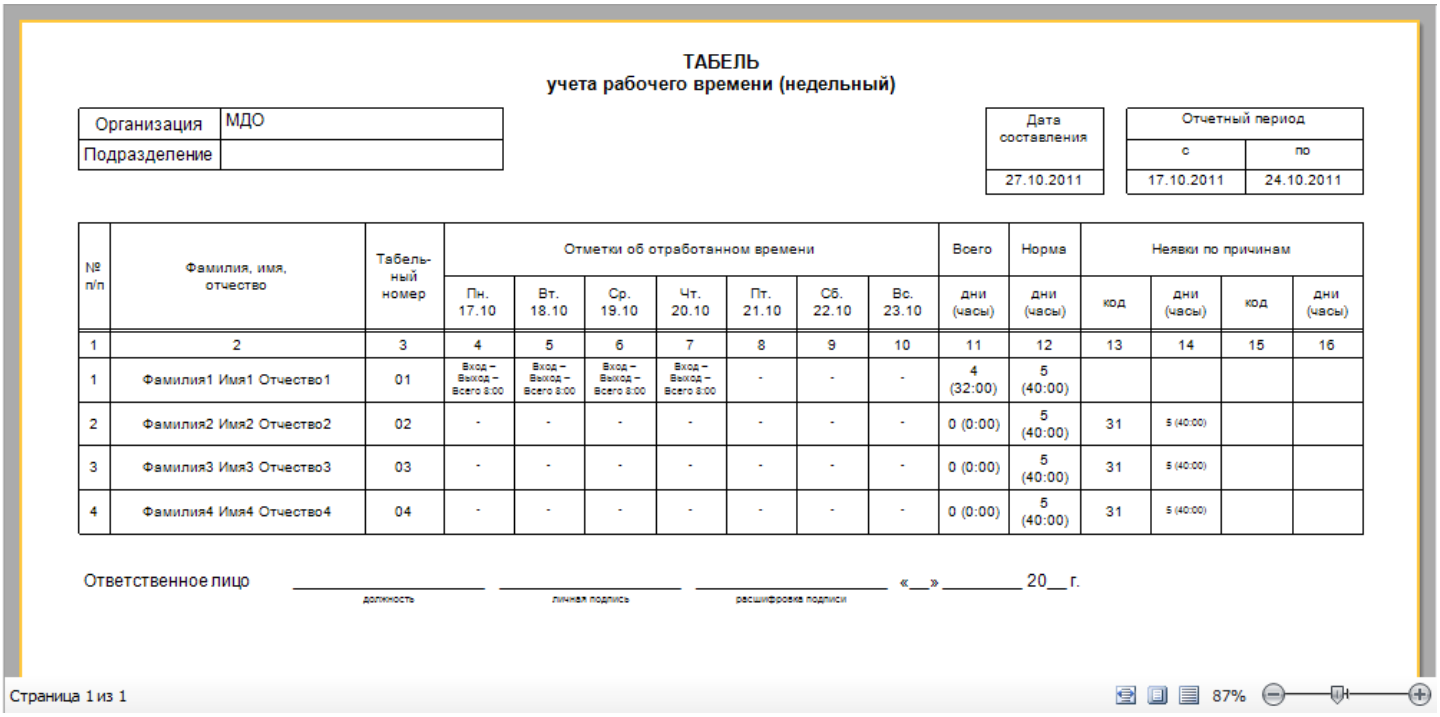
Ответственное лицо _____ _____ _____ «__» _____ 20__ г.
должность личная подпись расшифровка подписи

Условные обозначения:
О — опоздание, У — уход раньше времени, Х — отсутствие, ХР — прогул с фактом присутствия, Б — больничный, К — командировка, В - выходной, ОТ — отпуск, ПР — присутствие без проходов, РВ — Работа в выходной, ? — не принят на работу

Страница 1

11.3.3.11 Табель за неделю

На скриншоте ниже представлен недельный табель учёта рабочего времени.



ТАБЕЛЬ
учета рабочего времени (недельный)

Организация	МДО
Подразделение	

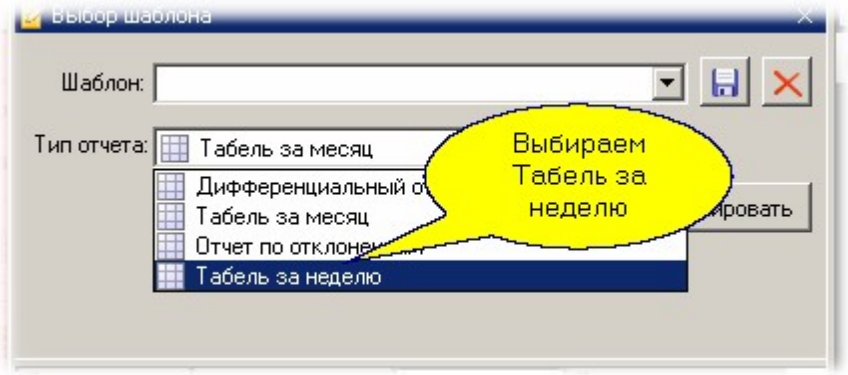
Дата составления	Отчетный период	
	с	по
27.10.2011	17.10.2011	24.10.2011

№ п/п	Фамилия, имя, отчество	Табельный номер	Отметки об отработанном времени							Всего	Норма	Неявки по причинам			
			Пн. 17.10	Вт. 18.10	Ср. 19.10	Чт. 20.10	Пт. 21.10	Сб. 22.10	Вс. 23.10	дни (часы)	дни (часы)	код	дни (часы)	код	дни (часы)
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Фамилия1 Имя1 Отчество1	01	Вход – Выход – Всего 8:00	Вход – Выход – Всего 8:00	Вход – Выход – Всего 8:00	Вход – Выход – Всего 8:00	-	-	-	4 (32:00)	5 (40:00)				
2	Фамилия2 Имя2 Отчество2	02	-	-	-	-	-	-	-	0 (0:00)	5 (40:00)	31	5 (40:00)		
3	Фамилия3 Имя3 Отчество3	03	-	-	-	-	-	-	-	0 (0:00)	5 (40:00)	31	5 (40:00)		
4	Фамилия4 Имя4 Отчество4	04	-	-	-	-	-	-	-	0 (0:00)	5 (40:00)	31	5 (40:00)		

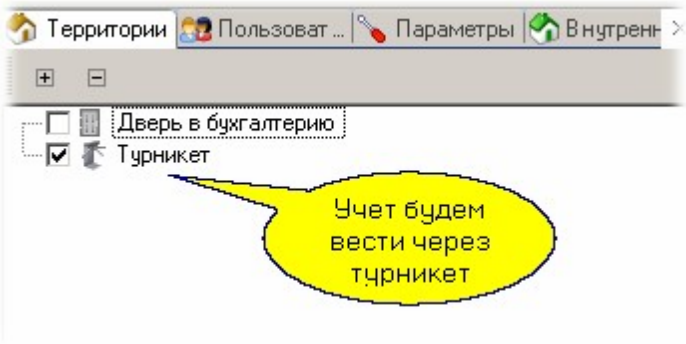
Ответственное лицо _____ (должность) _____ (личная подпись) _____ (расшифровка подписи) «__» _____ 20__ г.

Страница 1 из 1 87%

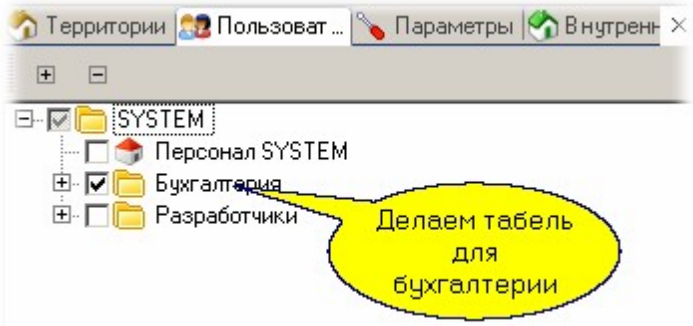
Формирование недельного табеля учета рабочего времени подобно формированию месячного табеля. Для формирования табеля учета рабочего времени за неделю необходимо в модуле УРВ выбрать из раскрывающегося списка данный тип отчета:



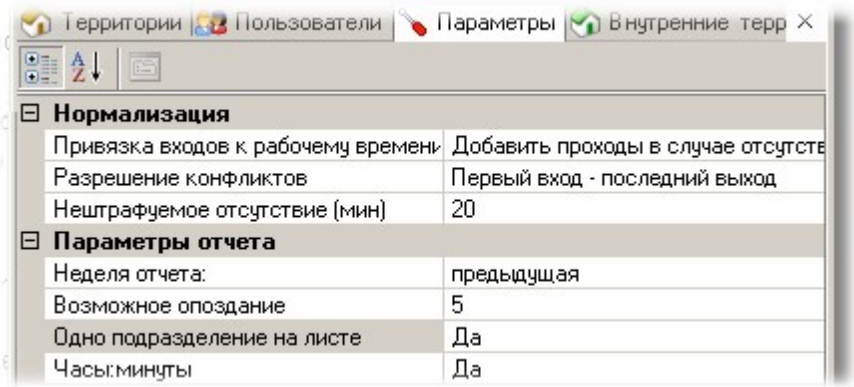
Далее на закладке территорий выбираем точки прохода, по которым ведется учет нахождения сотрудника на рабочем месте (на территории предприятия):



Следующим шагом выбираем подразделение, для которого будет сформирован табель за неделю:



На вкладке параметров настраиваем параметры подсчета рабочего времени:

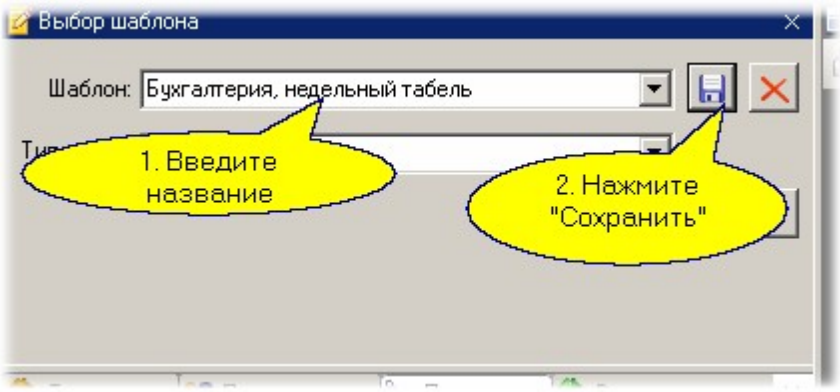


Смысловое значение параметров следующее:

- "Привязка входов к рабочему времени". Если у человека есть вход и нет выхода или есть выход, но нет входа, имеем возможность поступит двояко: либо изъять непарный проход (фактически засчитать прогул), либо добавить парный проход (простить сотрудника за то, что он не отметился).
- "Разрешение конфликтов". Относится к двойным (и более) входам или выходам, то есть когда есть два или более входов подряд без соответствующих выходов и наоборот. Засчитывать можно первый из входов и последний из выходов (демократичный вариант), либо последний из входов (первый из выходов) - жесткий вариант подсчета.
- "Нештрафуемое отсутствие". Если сотрудник отсутствовал на территории (рабочем месте) не более указанного интервала времени (за один раз), то этот интервал их рабочего времени не вычитается. Применяется, например, если на перекуры надо выходить за территорию предприятия.
- "Возможное опоздание". Опоздание относительно начала рабочего дня, за которое сотрудник еще не попадает в нарушители.
- "Одно подразделение на листе". Если мы выбираем эту опцию, то при формировании отчета по нескольким подразделениям за один раз отчет для каждого подразделения будет начинаться с новой страницы.
- "Часы:минуты." Формат вывода результатов расчета. При установке "Нет" время будет выводиться в виде десятичной дроби, например, 16,8 часа.

Как видно на рисунке вверху, в параметрах мы выбрали "Предыдущая". Расчет недельного табеля за текущую (не закончившуюся) неделю будет некорректным.

Если вам такой отчет придется в дальнейшем формировать регулярно, то следует настроенные параметры сохранить в виде шаблона. Для этого введите в поле *Шаблон* его название, например, "Бухгалтерия, недельный табель" и нажмите *Сохранить*:



Работа с шаблонами в инструментах отчетов описана в дополнительном разделе[314].

1. После выбора всех параметров необходимо нажать на кнопку *Сформировать*, и результирующий отчет появится в правой панели рабочего окна. Вы можете отправить его сразу на печать на любой доступный принтер, либо сохранить в одним из возможных форматов в файл на диске.

Таблица 1. Коды и наименования интервалов учёта рабочего времени.

Наименование интервала учёта рабочего времени	Код цифровой
Ежегодный отпуск (оплачиваемый)	**09**
Отпуск без сохранения содержания (не оплачиваемый)	**16**
Временная нетрудоспособность (оплачиваемый больничный)	**19**
Прогулы	**24**

Неявка на работу без уважительной причины или отсутствие на работе без уважительной причины более 4 часов (непрерывно) в течение расчётного дня приводят к формированию прогула за анализируемый день.

11.4 Модуль видеоверификации

Лицензируется как PNSoft-VV[344]

Назначение и состав

Модуль видеоверификации позволяет организовать специализированное рабочее место сотрудника службы безопасности. При этом оператор за монитором имеет возможность управлять одной точкой прохода, получая дополнительную информацию из различных источников, настраиваемых администратором системы. Например, можно сравнить фотографию из базы данных с личностью проходящего субъекта доступа, выводить изображение с одной или более телекамер. Таким образом, видеоверификация позволяет организовывать дополнительный контроль проходящих сотрудников или транспорта, а также организовывать интерактивные точки прохода с обязательной реакцией оператора.

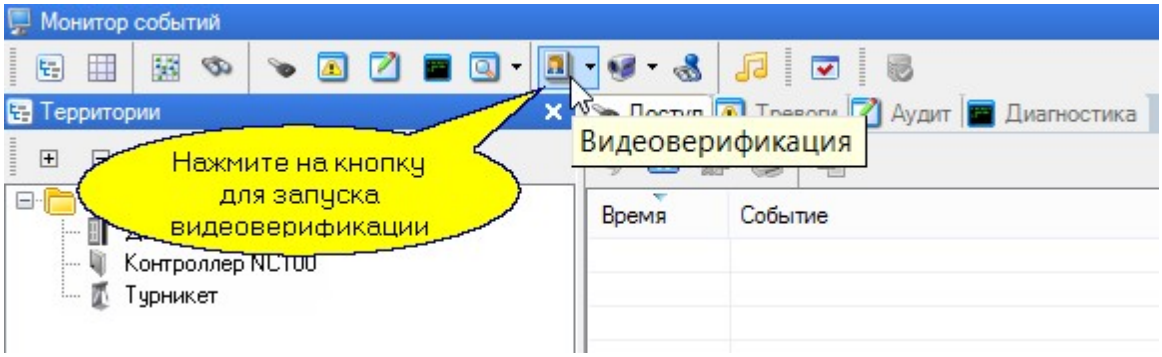
Дополнительную гибкость при использовании видеоверификации обеспечивает программный контроллер, позволяя, например, использовать подсистему распознавания автомобильных номеров.

Модуль видеоверификации может работать как дополнительная панель монитора событий, либо как самостоятельный инструмент системы ParsecNET 3. При работе в качестве самостоятельного инструмента модуль может работать в полноэкранном режиме, занимая всю площадь монитора компьютера.

Количество одновременно работающих окон (или панелей) видеоверификации на одном ПК не ограничено.

Запуск видеоверификации

В данном примере рассмотрим работу модуля видеоверификации как панели монитора событий. Чтобы открыть панель видеоверификации, нажмите на соответствующую кнопку на панели инструментов Монитора:



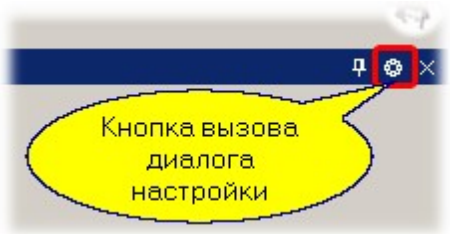
В появившемся диалоге введите название для данной панели видеоверификации и нажмите на кнопку *ОК*. В результате появится новая панель. Расположите[45] ее как вам удобно в рамках окна монитора.

Видеоверификация может работать как в **режиме наблюдения**, так и в **режиме управления** (когда оператор определяет возможность прохода или проезда субъекта доступа).

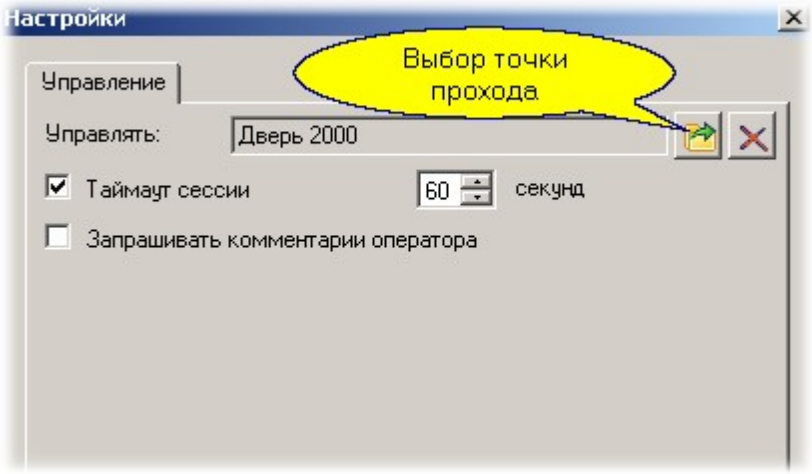
Организуйте панель видеоверификации для реализации режима управления (режим наблюдения организуется так же, но без указания точек прохода для управления).

Шаг 1. Настройка управления

Вызовите диалог настройки панели видеоверификации с помощью кнопки в правом верхнем углу панели:



В появившемся диалоговом окне выберите точку прохода, которой будете управлять:



Дополнительно настраиваются следующие параметры:

- **Таймаут сессии**. Установите, если требуется реакция оператора. При установленном таймауте, если реакция оператора не последует в течение заданного времени, будет создана транзакция отсутствия реакции оператора.
- **Запрашивать комментарий оператора**. Если флажок установлен, то при выдаче оператором разрешения на проход появится диалог, в котором необходимо будет написать объяснение причины своего действия. Оно сохранится вместе с его реакцией.

После установки требуемых параметров нажмите на кнопку *ОК*, заканчивая настройки режима управления.

Если точка прохода для управления не назначена, видеоверификация будет работать только в режиме наблюдения, без вмешательства оператора.

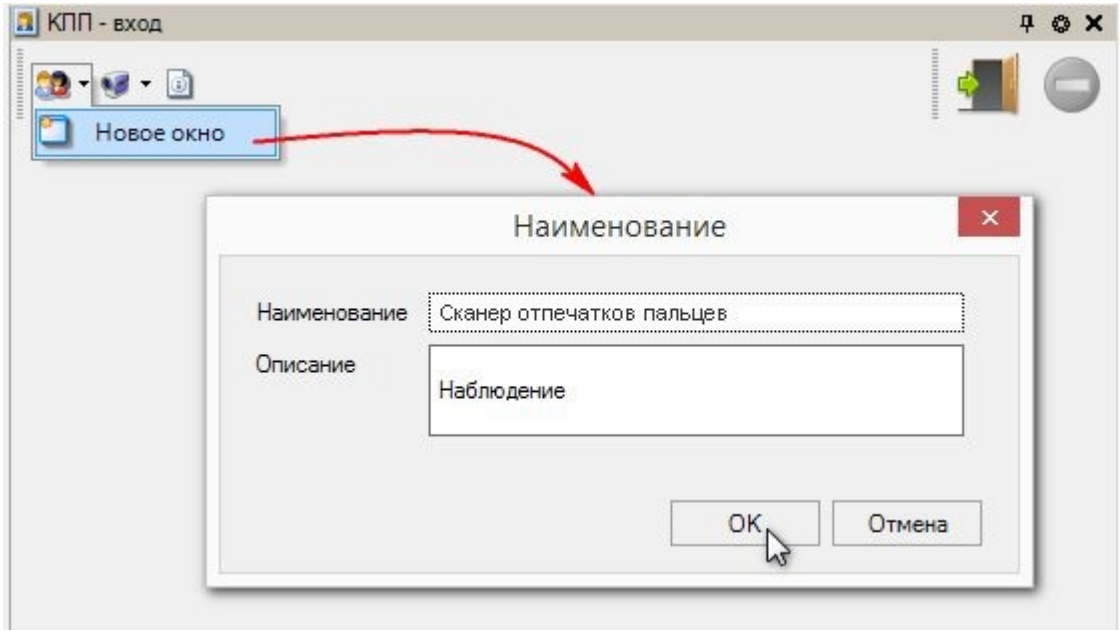
Сразу после определения точки прохода для управления появится панель инструментов с двумя кнопками: *Впустить* и *Отказать*. Ее можно разместить с любой стороны панели (или окна) видеоверификации. На рисунке ниже она размещена в правом нижнем углу:



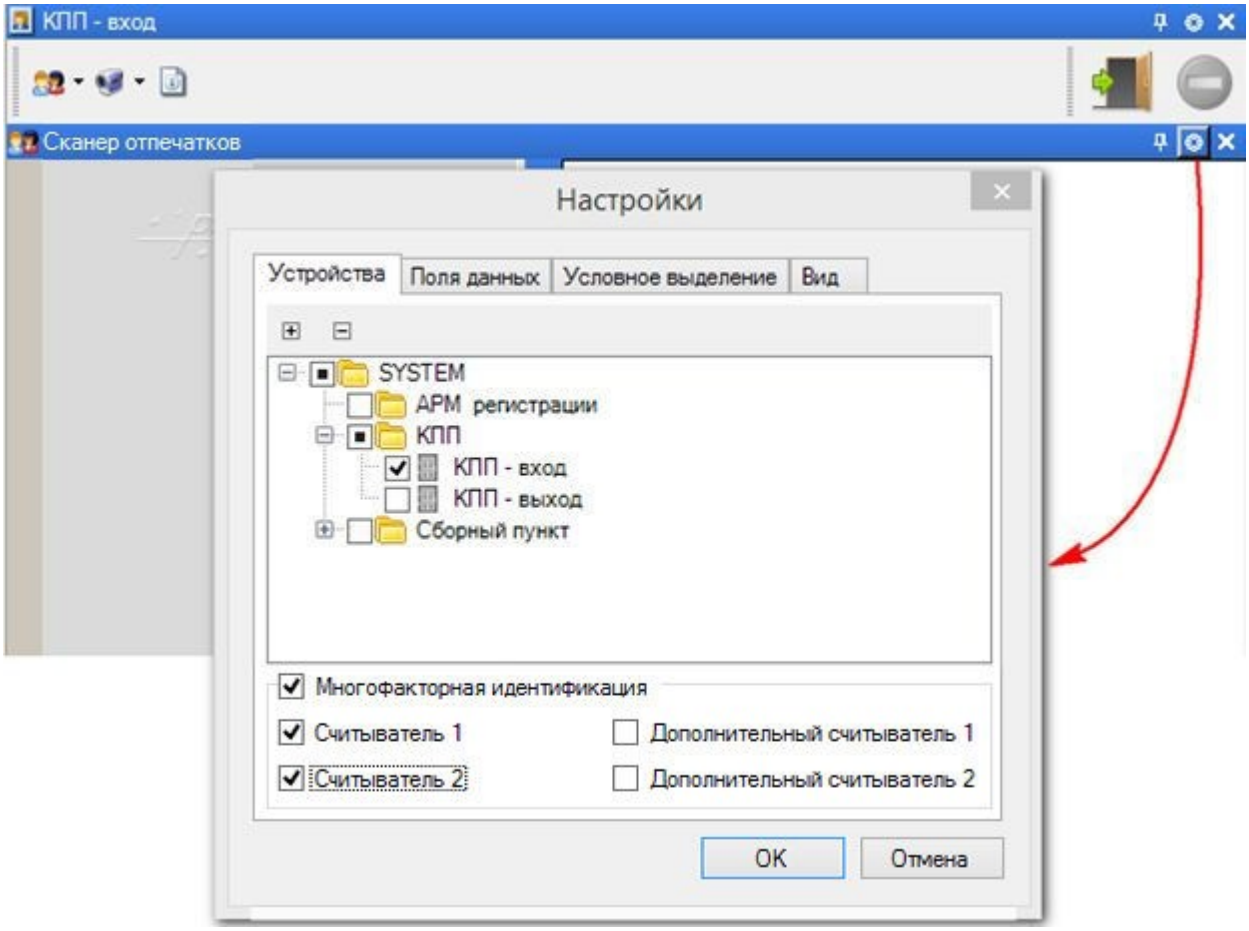
Кнопки перетаскиваются мышкой за вертикальную черту, показанную на рисунке выше.

Шаг 2. Наблюдение точек доступа

Создайте новое окно наблюдения с использованием панели инструментов (на примере сканера отпечатков пальцев):



В результате появится новое окно наблюдения. В нем на вкладке *Устройства* необходимо указать точку прохода, информацию с которой мы хотим наблюдать.



Многофакторная идентификация

Система позволяет настроить двухфакторную идентификацию на точках прохода - идентификацию по нескольким параметрам. Это возможно только при использовании контроллеров доступа NC-8000[76] и NC-60K/NC-60K.M[85], имеющих возможность подключения 4 устройств идентификации, например: считыватель, сканер радужной оболочки глаза, сканер отпечатков пальцев и т.п. Данный функционал позволяет повысить безопасность, предоставляя доступ при совпадении нескольких идентификаторов у одного

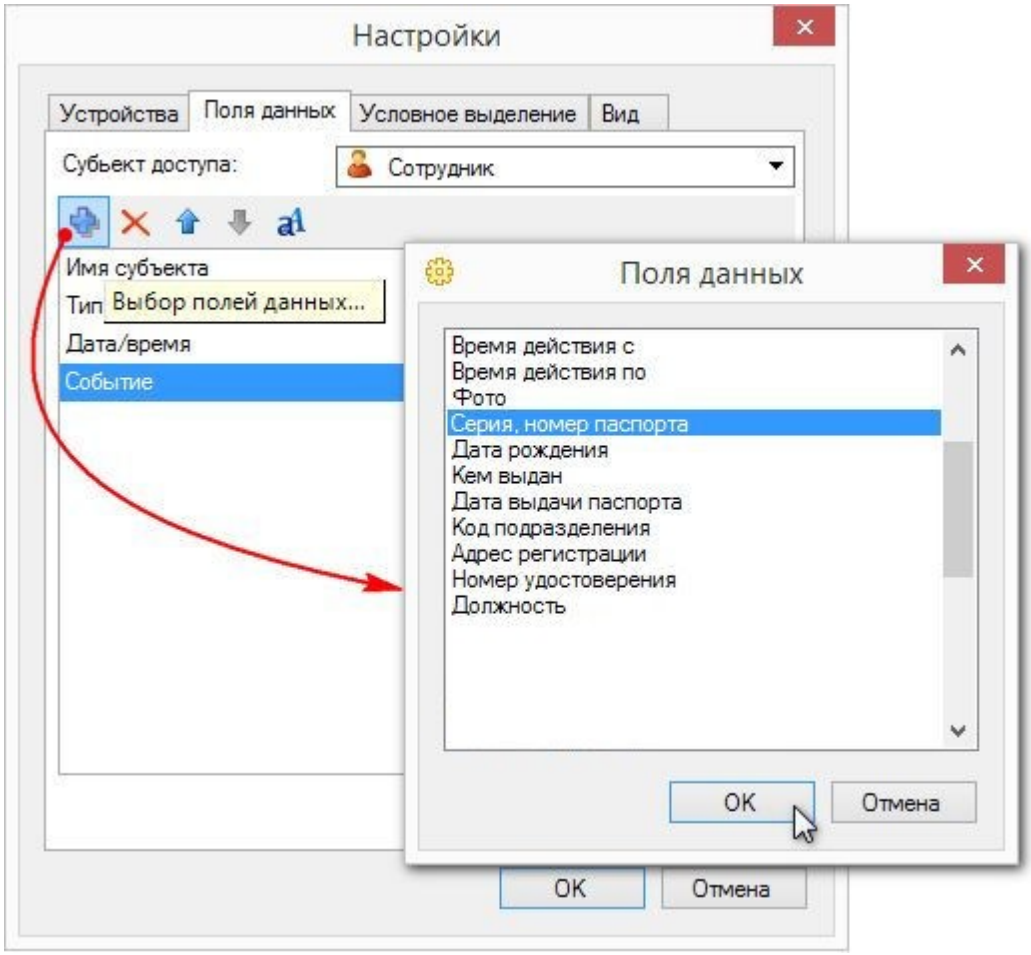
субъекта доступа, например: код карты + отпечаток пальца, или скан радужной оболочки глаз и отпечаток пальца и т.д.

Чтобы отслеживать только события, сгенерированные устройствами идентификации, выберите точку прохода и установите флажок *Многофакторная идентификация* (рисунок выше).

Затем выберите, какие каналы контроллера будут задействованы на этой точке прохода (на рисунке выше показан этап настройки точки прохода "КПП". Два устройства идентификации (*Считыватель 1* и *Считыватель 2*) являются внешними и предназначены для контроля входа. Каналы *Считыватель 3* и *Считыватель 4* заняты устройствами идентификации, контролирующими выход).

Использование двухфакторной идентификации возможно только при наличии контроллера доступа NC-8000 со специальной прошивкой. Для полной информации обратитесь в Отдел сопровождения проектов https://www.parsec.ru/support/inspection/ .

На вкладке *Поля данных* настройте вывод текстовых сообщений. Для каждой категории субъектов доступа (посетитель, сотрудник, или автомобиль) набор выводимых полей, их порядок, а также шрифтовое оформление настраиваются отдельно.



На вкладке *Условное выделение* можно настроить панель видеоверификации для отображения строк данных на цветном фоне. Для этого выполните шаги:

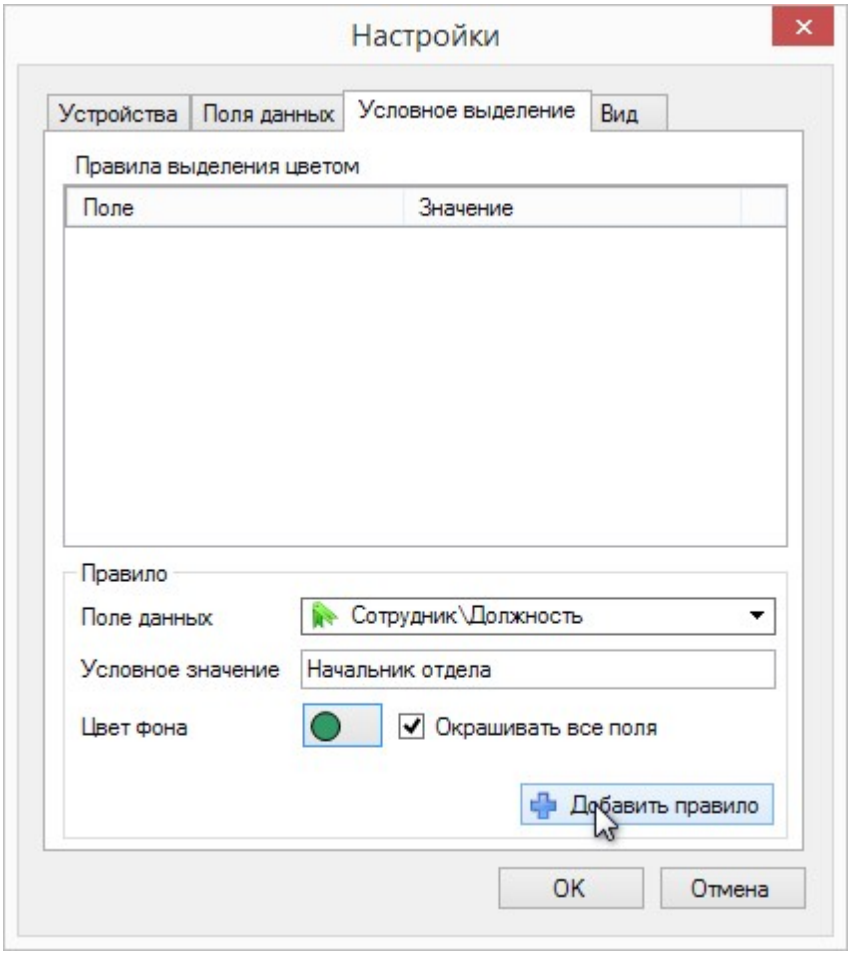
- В поле *Поле данных* из раскрывающегося списка выберите дополнительное поле[264], созданное заранее. Например, создайте общее дополнительное поле "Должность", в котором каждому субъекту доступа будет указываться наименование должности (для сокращения вариантов отображения, сгруппируйте

должности по группам): у всех начальников отделов будет записано "Начальник отдела", у всех менеджеров по продажам, мерчандайзеров и т.п. - "Менеджер", у всех водителей - "Водитель". Также может быть и единственная должность, например, "Генеральный директор";

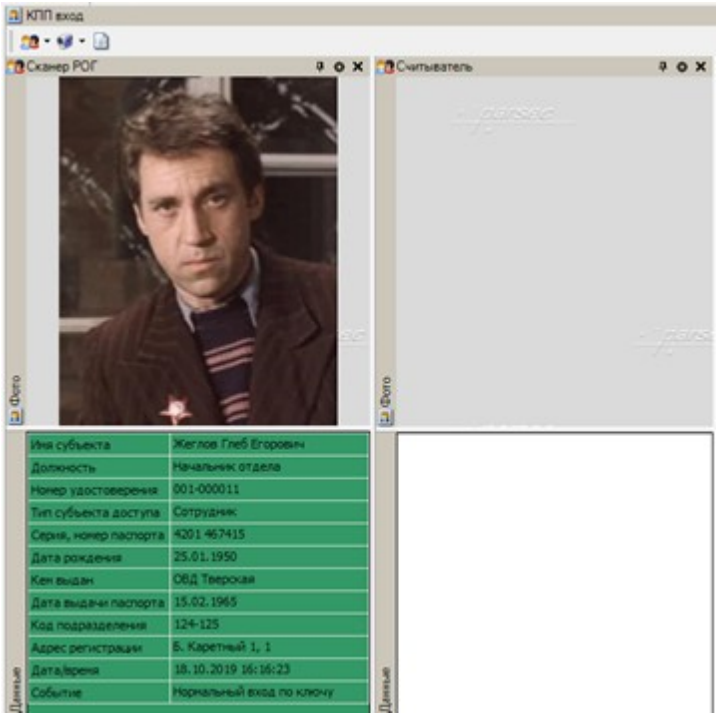
- В поле *Условное значение* введите значение дополнительного поля, выбранного на предыдущем шаге (без кавычек). При совпадении заданного значения со значением выбранного дополнительного поля у идентифицируемого субъекта доступа, выбранное поле будет отображаться на цветном фоне. Например, для Начальника транспортного отдела введите "Начальник отдела";
- В поле *Цвет фона* выберите желаемый цвет;



- Установите флажок *Окрашивать все поля*, если хотите, чтобы все поля данных были окрашены в этот цвет. В противном случае в выбранный цвет будет окрашиваться только поле данных, выбранное в настройках правила;
- Нажмите на кнопку *Добавить правило*:

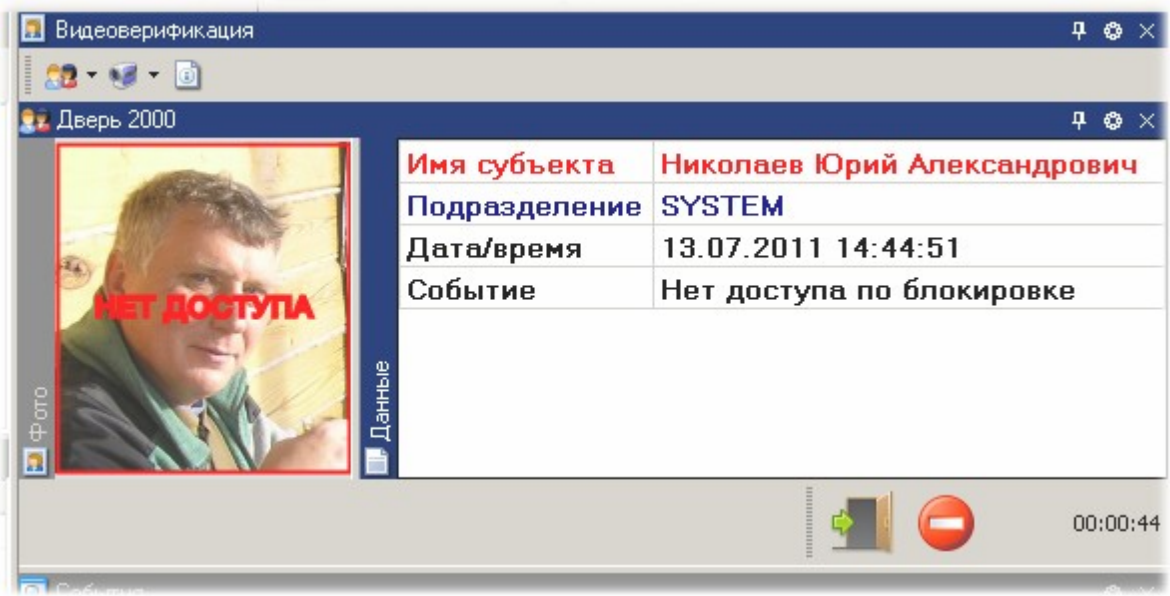


- Сохраните созданное правило, нажав на кнопку *ОК*. Теперь, когда какой-то из начальников отделов приложит свою карту к считывателю, поля данных на панели видеоверификации будут отображаться на зеленом фоне:



- Повторите настройку условного выделения для остальных групп должностей, например:
  - Водитель;
  - Генеральный директор.

На вкладке *Вид* настройте, какие из элементов окна наблюдения будут показываться в панели видеоверификации, и после нажатия на кнопку *ОК* настройка окна будет закончена. Можно уже проверить работу системы: предъявите, например, на контролируемой точке прохода карту, не имеющую в данный момент доступа. Результат показан на рисунке:

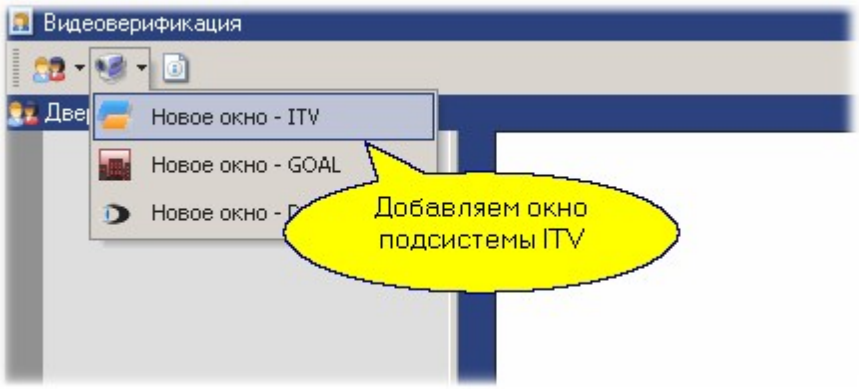


Если отказать в доступе, панель очистится с формированием транзакции отказа оператора. Если же разрешить вход, то откроется диалог, в котором необходимо ввести причину, почему оператор пропустил данного субъекта (появлением диалога управляет флажок *Запрашивать комментарий* оператора, см. Шаг 1) .

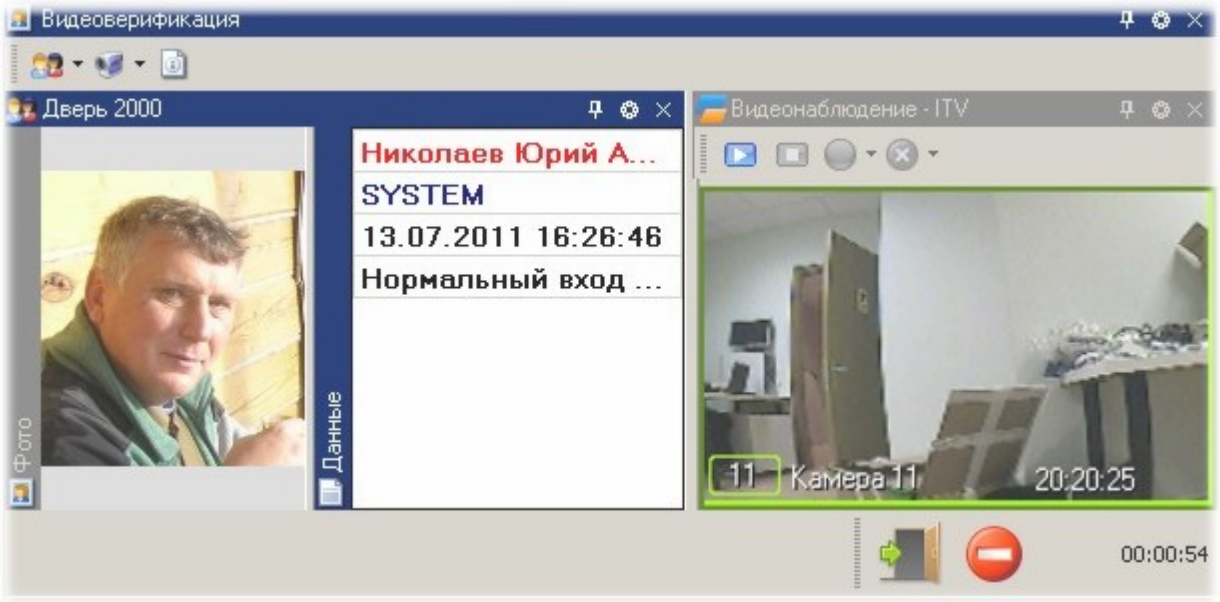
Обратите внимание, что рядом с кнопками управления можно видеть обратный отсчет времени до окончания сессии (мы настраивали сессию на 60 секунд).

Шаг 3. Добавление видеонаблюдения

Можно добавить к панели видеоверификации окна наблюдения (любое количество) для дистанционного контроля происходящего на точке прохода или в ее окрестностях. При этом можно добавить несколько окон от разных видеоподсистем, если они присутствуют в вашей системе:



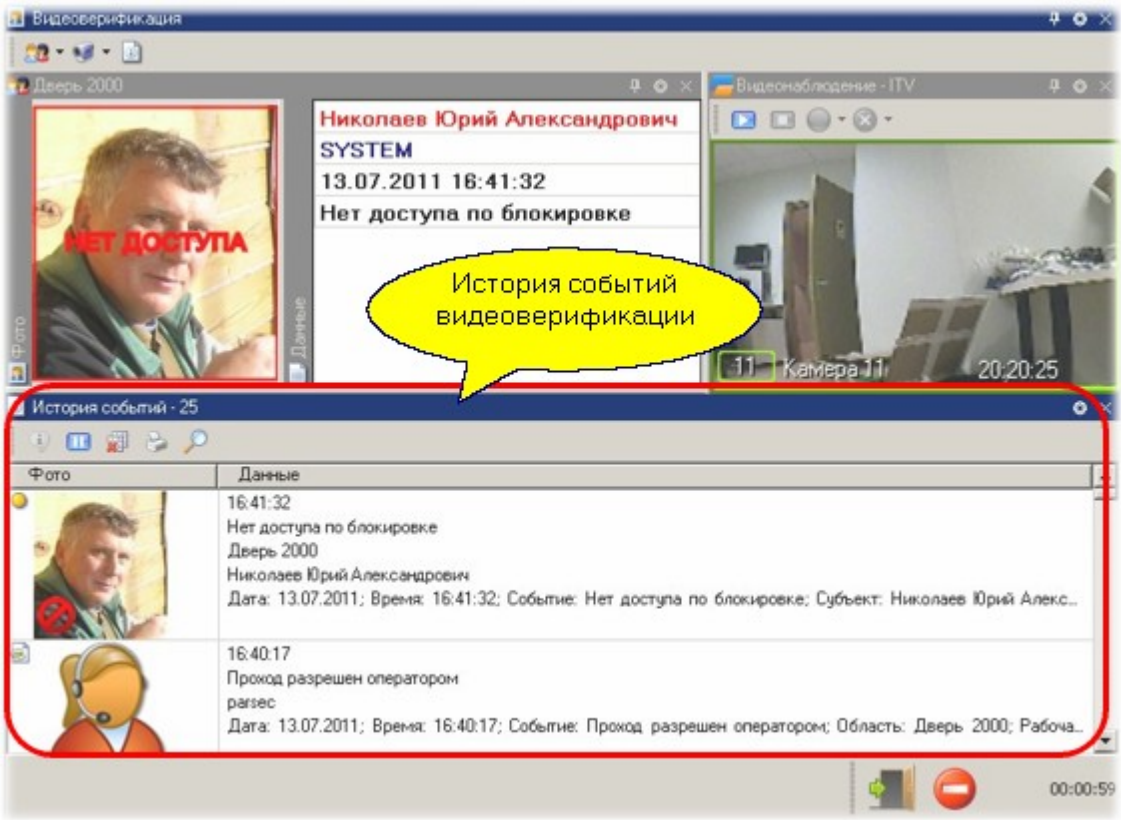
Теперь, помимо данных субъекта и данных события в окне наблюдения, можно визуально контролировать происходящее:



Шаг 4. Добавление истории событий

История событий окончательно превращает панель видеоверификации в законченный инструмент сотрудника охраны, поскольку позволяет не только видеть текущую ситуацию на точке прохода, но и историю событий.

Панель истории событий может быть настроена для отображения событий аналогично тому, как это делается в Мониторе, либо с показом фотографий. Последнее иллюстрируется следующим рисунком:



По истории событий можно производить поиск, распечатывать ее как отчет по событиям, а также получать полную информацию по любому событию, как это делается в Мониторе.

См. также:

Монитор событий[287]

11.4.1 Дополнительные возможности

Отдельный инструмент

Видеоверификация может работать как отдельный инструмент в полноэкранном режиме. В этом случае она запускается как отдельное приложение из папки программ системы ParsecNET 3. Однако, после первого запуска вы получаете оконный (не полноэкранный) режим. Если вам необходимо ограничить возможности оператора за дисплеем, например, чтобы охраннику ничего не мешало на экране, то соответствующий режим придется настроить самостоятельно:

1. Оператору, для которого настраивается этот режим, временно поднимите права на изменение и сохранение вида приложения, на выход из программы;
2. От имени этого оператора запустите приложение "Видеоверификация" из папки с набором приложений ParsecNET 3 в меню *Пуск*;
3. Раскройте окно инструмента на весь экран двойным щелчком по заголовку окна или кнопкой на правой стороне заголовка окна;
4. Настройте все параметры: события, на которые будем реагировать, размер и цвет шрифта и фона[515] в панели персональных данных и т.д.;
5. В меню *Вид* отметьте автосохранение вида приложения;
6. Через меню *Вид* выключите панель инструментов данного окна. Настройка параметров теперь недоступна;
7. Настройте размер и положение панелей *Фото*, *Персональные данные* и *Действия*. Ненужные панели закройте;
8. С помощью меню *Вид* переключитесь в полноэкранный режим;
9. С помощью меню *Вид* переключитесь в фиксированный режим. После этого панели перемещать уже будет невозможно;
10. Последним шагом через меню *Вид* выключите отображение главного меню.

Теперь окно видеоверификации занимает всю площадь экрана и не содержит органов управления, позволяющих изменить его вид. Поскольку мы включили автосохранение вида, можно выйти по комбинации клавиш Alt-F4.

Теперь самое время лишить оператора прав на изменение внешнего вида и выход из программы. Если после этого опять запустить видеоверификацию от имени этого оператора, то последний практически ничего не сможет сделать с экраном компьютера.

Выход из полноэкранного режима осуществляется по клавише F11, но ввиду отсутствия у оператора прав на изменение внешнего вида будет выведен диалог с просьбой ввести имя и пароль оператора, у которого есть права на указанные действия.

11.5 Интеграция с системами видеонаблюдения

Лицензируется как PNSoft-VI[344]

Основные возможности

Интеграция с системами видеонаблюдения позволяет реализовать в системе ParsecNET 3 следующий функционал:

- Просмотр "живого" видео с камер системы видеонаблюдения в мониторе событий системы;
- Ручное управление записью через монитор событий системы;
- Управление записью с камер видеонаблюдения по событиям системы;
- Управление записью с камер видеонаблюдения с использованием менеджера заданий;

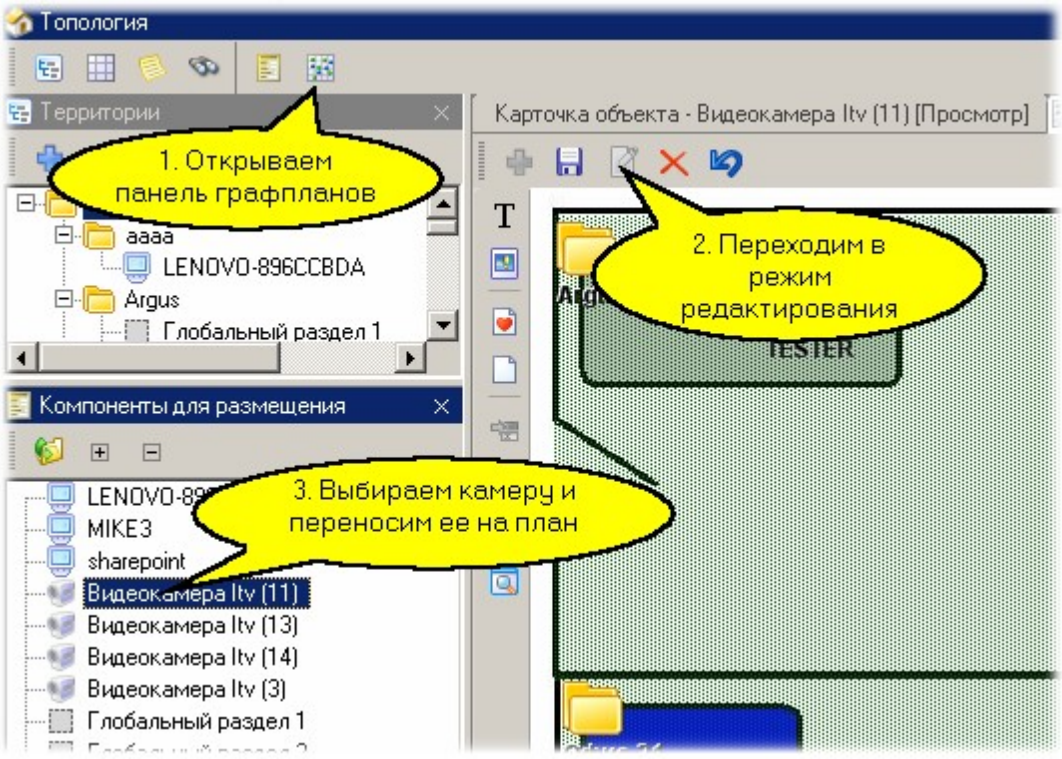
- Ретроспективный анализ событий с просмотром не только данных о событии, но и связанных с событиями видеозаписей;
- Включение и выключение режима охраны в видеоподсистеме (детектор движения или активности);
- Получение видеопотока как аналоговых, так и с IP-камер.

Конфигурирование и настройка внешних систем видеонаблюдения должны производится штатными средствами внешней системы. Со стороны ParsecNET 3 может поддерживаться только настройка оперативных параметров, таких, как яркость, контрастность, раскладка камер в окне монитора (при условии, что интеграционные механизмы внешней системы предоставляют такие возможности).

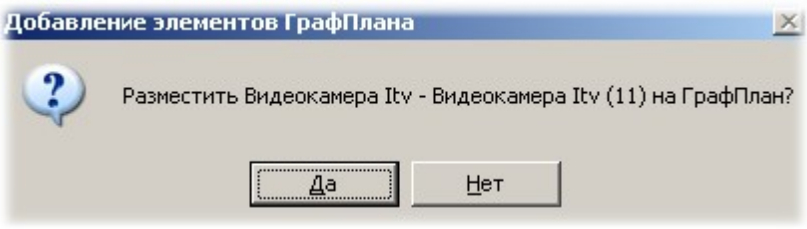
Использование графпланов

Как и другие компоненты системы безопасности, видеокамеры могут размещаться на интерактивных графических планах, если они используются в системе ParsecNET 3.

Графические планы создаются в редакторе топологии[203] . Вкратце покажем, как размещать видеокамеры на графическом плане и использовать их в мониторе событий. Основные шаги показаны на рисунке ниже:



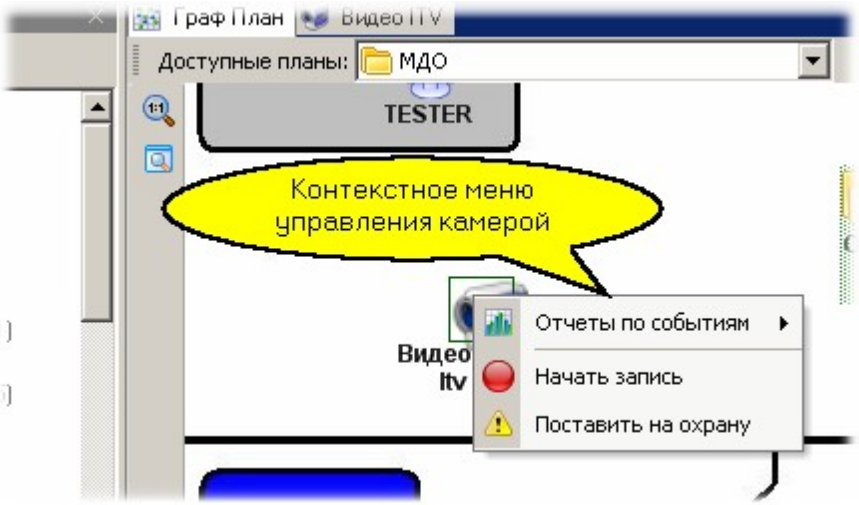
Подтверждаем размещение камеры на плане:



После этого помещаем камеру на плане в требуемом месте и сохраняем графический план.

Теперь в мониторе событий мы можем на графическом плане (он доступен только в расширенном режиме - в режиме "новичок" графпланы недоступны) наблюдать за статусом камеры и управлять ей в рамках возможностей, предоставляемых конкретной видеосистемой. В частности, можно включать и выключать запись с камеры.

Ниже в качестве примера показано контекстное меню управления камерой. Данное меню вызывается щелчком правой кнопки мышки по изображению камеры.



Элементы управления в окнах видоесистем

- показать изображение;
- остановить показ изображения;
- начать видеозапись;
- завершить запись видео;
- сохранить кадр;
- пометить запись. Позволяет запустить видео с момента, когда поставлена метка.

См. также:

Система ИСБ "Интеллект" 518

Система GOALCity 527

Система TRASSIR 531

Системы Macroscop и LTV-Gorizont 539

Система Panasonic 559

Система SecurOS 566

Создание графических планов 208

11.5.1 Система ИСБ "Интеллект"

Данный раздел не является руководством по использованию системы ИСБ "Интеллект" производства компании ITV | AxxonSoft, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы ИСБ "Интеллект" обратитесь к оригинальному руководству.

Видеосистема ИСБ "Интеллект" предоставляет поддержку следующих функциональных возможностей:

- Просмотр "живого" видео с камер системы видеонаблюдения (без возможности самостоятельно создавать "раскладки" камер в окне видеонаблюдения);
- Ручное управление записью через монитор событий системы;
- Управление записью с камер по событиям системы или с использованием менеджера заданий;
- Просмотр связанных с событиями системы видеозаписей;
- Включение и выключение режима охраны (детектор движения или активности видеокамеры);
- Получение событий от видеосистемы и сохранение их в архиве событий ParsecNET 3;
- Использование системы для распознавания номеров[593] транспортных средств.

В последующих подразделах рассмотрены вопросы подключения видеосистемы ИСБ "Интеллект", а также ее использование в составе ParsecNET 3 при мониторинге.

Детальное рассмотрение работы с окном видеонаблюдения данный документ не содержит, поскольку данное окно является компонентом видеосистемы ИСБ "Интеллект" и полностью повторяет работу окна видеонаблюдения этой системы. Для ознакомления с его работой обратитесь к документации ИСБ "Интеллект".

Для использования любой из видеокамер подсистемы ИСБ "Интеллект" для распознавания номерных знаков автомобилей данная функция должна быть предварительно настроена собственными средствами ИСБ "Интеллект". Если такая настройка произведена, можно с использованием контроллера автомобильных номеров и редактора заданий системы ParsecNET 3 организовать автомобильную проходную[588].

См. также:

Подключение и настройка[518]

Использование системы[522]

11.5.1.1 Подключение и настройка

Особенности установки на 64-разрядные станции

При установке ИСБ "Интеллект" на 32-разрядные станции дополнительных действий не требуется.

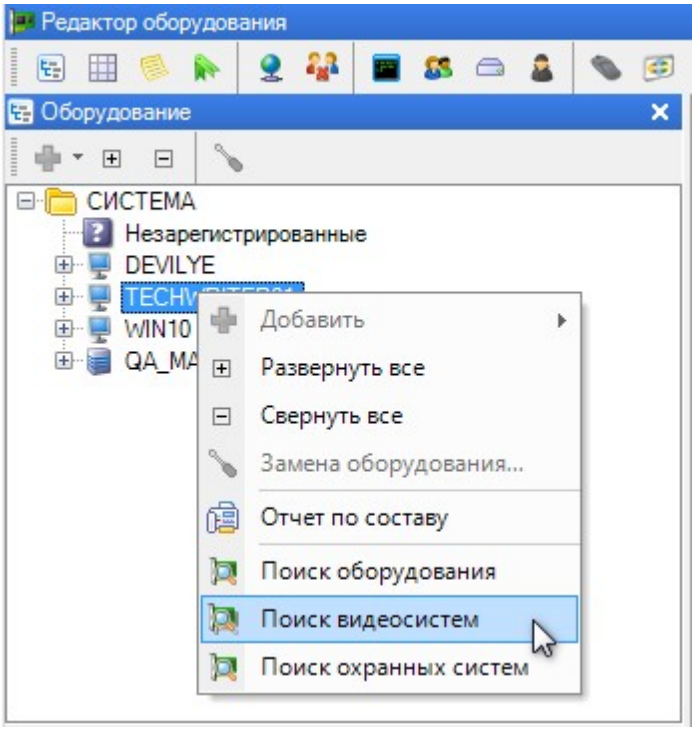
При установке ИСБ "Интеллект" на 64-разрядные станции необходимо после обычной установки запустить приложение "ParsecNET 3 - 32 bit converter.exe" из папки с установочными файлами ParsecNET 3. Приложение запускается на тех компьютерах, на которых установлен ИСБ "Интеллект". Также это приложение требуется запускать каждый раз после обновления системы ParsecNET 3.

Чтобы интеграция заработала, нужно обновить библиотеки. Для этого:
- ***остановите службу ParsecNET 3 Video;***

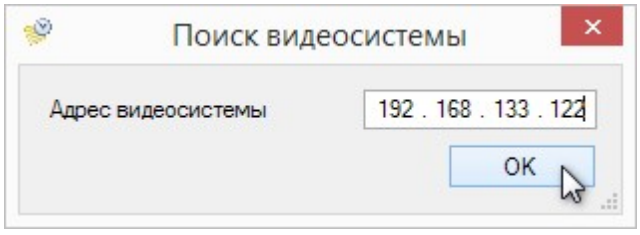
- ***(для ПО Интеллект всех версий) скопируйте библиотеку "iidk.dll" по-умолчанию из папки "C:\Program Files (x86)\Интеллект\Modules" и вставьте с заменой в папку "C:\Program Files\MDO\ParsecNET 3";***
- ***(для ПО Интеллект версий 4.10.2 и выше) скопируйте библиотеку "boost_thread-vc100-mt-1_47.dll" по-умолчанию из папки "C:\Program Files (x86)\Интеллект\Modules" и вставьте в папку "C:\Program Files\MDO\ParsecNET 3"***
- ***запустите службу ParsecNET 3 Video.***

Подключение ИСБ "Интеллект"

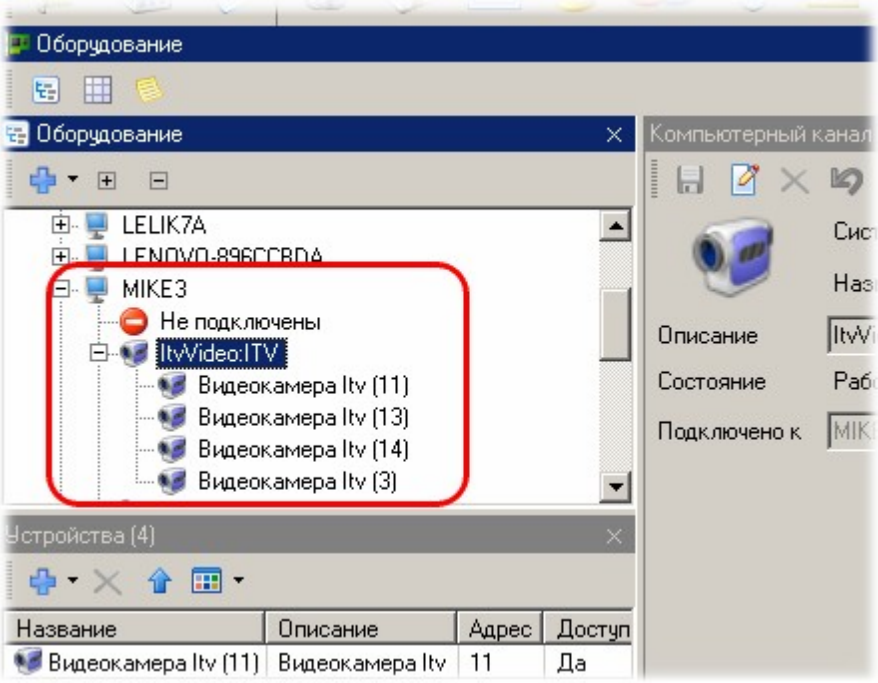
Для подключения ИСБ "Интеллект" запустите консоль "Администрирование" ParsecNET 3 и в контекстном меню рабочей станции Parsec (сервера или локального ПК) выберите "Поиск видеосистем":



В открывшемся окне введите IP-адрес ПК, на котором установлен сервер видеосистемы (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования") и нажмите на кнопку *ОК*:



Система произведет поиск и отобразит видеосистему ИСБ "Интеллект" в дереве оборудования:



Для использования видеокамер достаточно штатными средствами ИСБ "Интеллект"установить рабочее место видеонаблюдения на те компьютеры, на которых будут рабочие станции ParsecNET 3 с возможностью использования видеонаблюдения.

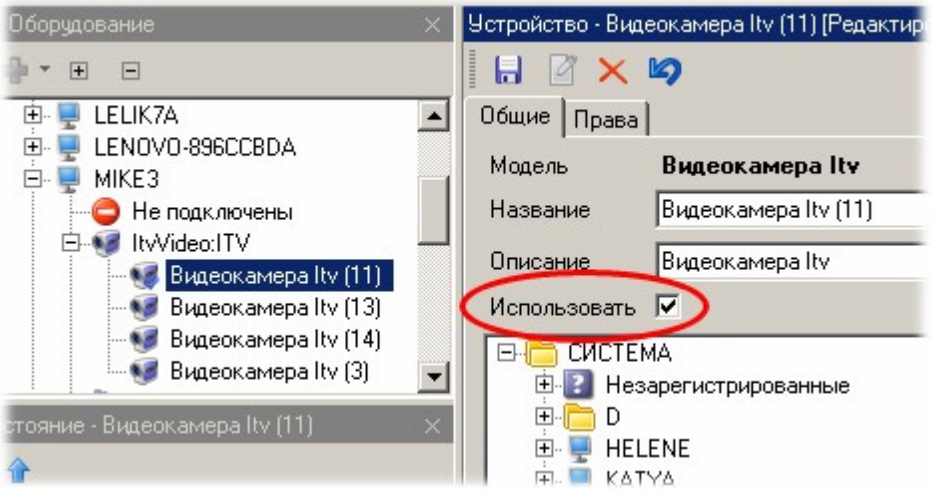
В приведенном выше примере в системе зарегистрировали рабочую станцию "MIKE3". Поскольку на ней установлен сервер ИСБ "Интеллект" и на нем зарегистрированы четыре видеокамеры, под рабочей станцией "MIKE3" автоматически появился компьютерный канал "ItvVideo:ITV" с подключенными к нему камерами.

Канал и камеры ИСБ "Интеллект" будут видны на любой рабочей станции ParsecNET 3, но использование камер будет возможно только на тех станциях, на которых установлена ИСБ "Интеллект" (как минимум - рабочее место).

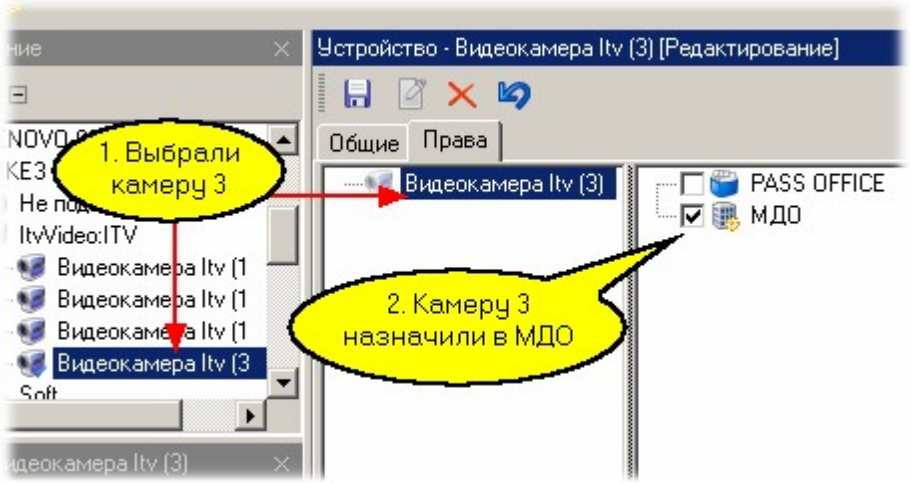
Настройка использования камер

В панели свойств редактора оборудования для каждой из видеокамер можно снять или установить флажок *Использовать* (см. рисунок ниже). Для ИСБ "Интеллект" это не отразится на показе изображения, так как механизм отключения камеры интеграционным сервисом данной системы не предоставляется.

Вместе с тем, работа с камерой в части управления записью или детектором движения, а также контроль состояния камеры (ее статус) из системы ParsecNET 3 соответственно разрешается или запрещается.

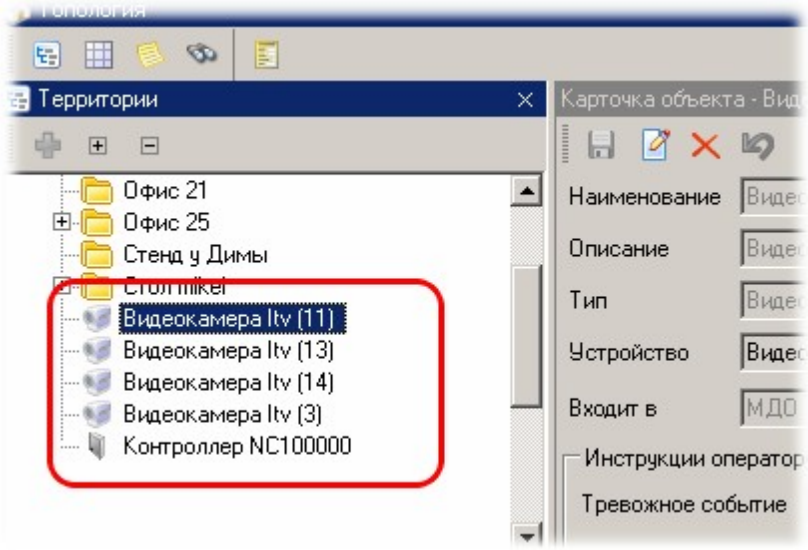


Аналогично оборудованию доступа, камеры ИСБ "Интеллект" необходимо распределить для пользования между организациями ParsecNET 3 с помощью редактора оборудования, для чего на вкладке *Права* панели свойств необходимо для выбранной камеры проставить флажки в требуемых организациях, как показано на рисунке ниже:

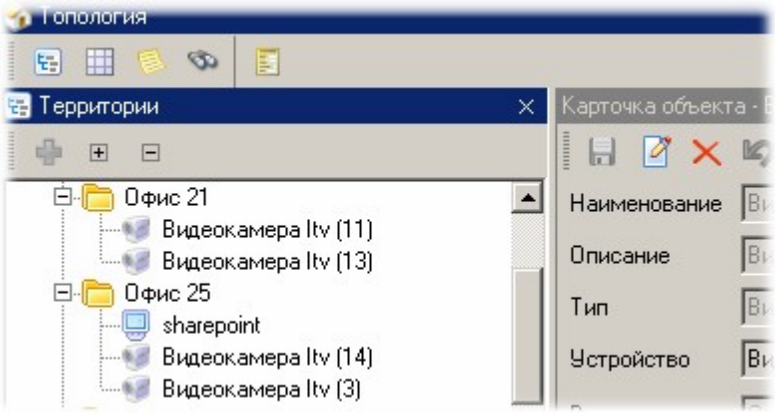


Распределение камер по топологии

Если у вас не компактная система, то необходимо распределить камеры по топологии с помощью редактора топологии[203]. На рисунке ниже видно, что после авторазмещения все камеры попали в корень топологии организации:



Стандартными средствами редактора топологии распределим камеры по две в Офис 21 и в Офис 25. Результат иллюстрируется следующим рисунком:

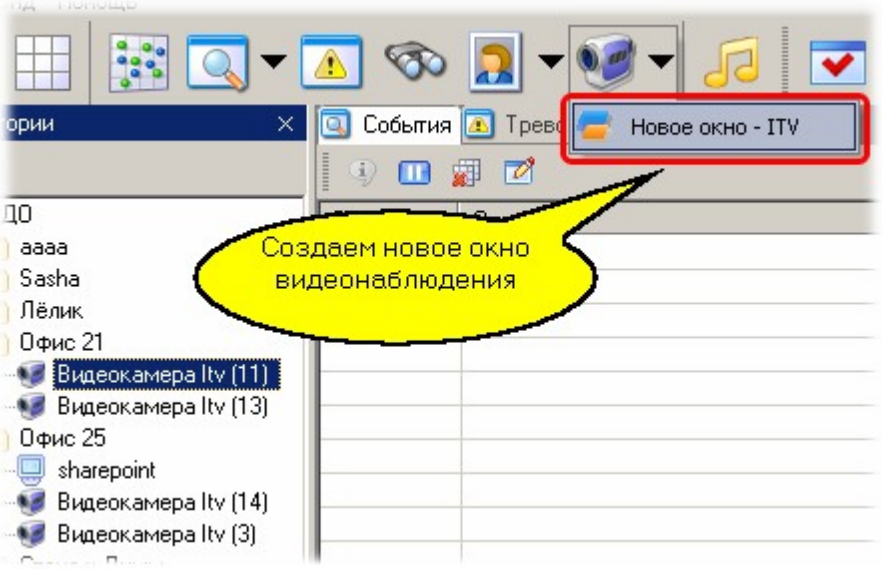


Теперь можно использовать видеокамеры в мониторе событий.

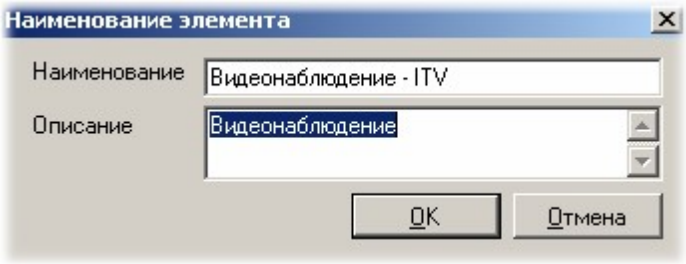
11.5.1.2 Использование системы

Использование камер в мониторе событий

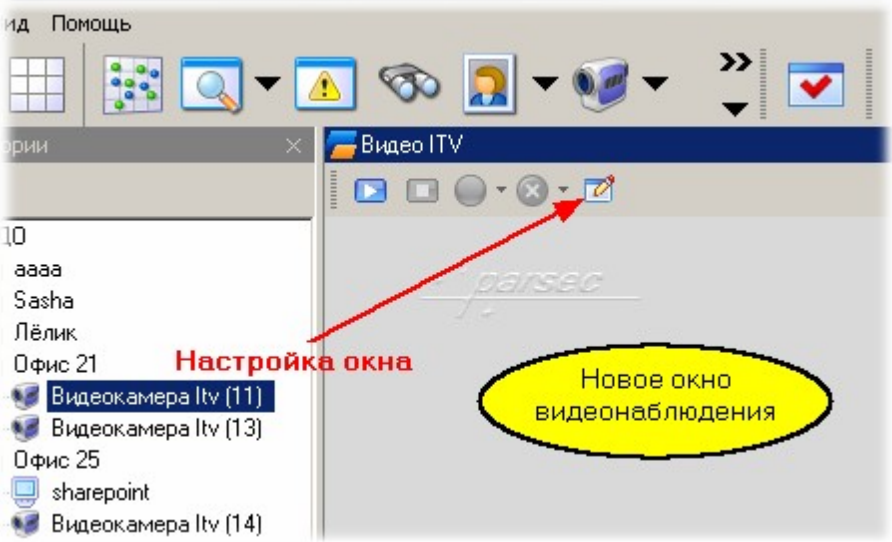
Первым шагом необходимо создать в мониторе событий окно видеонаблюдения. Для этого выбираем в панели инструментов "Видеонаблюдение - Новое окно ITV":



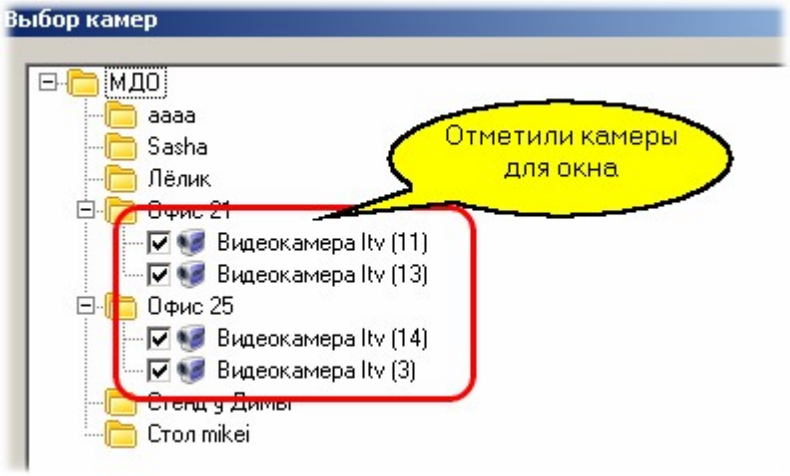
В появившемся диалоговом окне корректируем при необходимости название и описание нового окна:



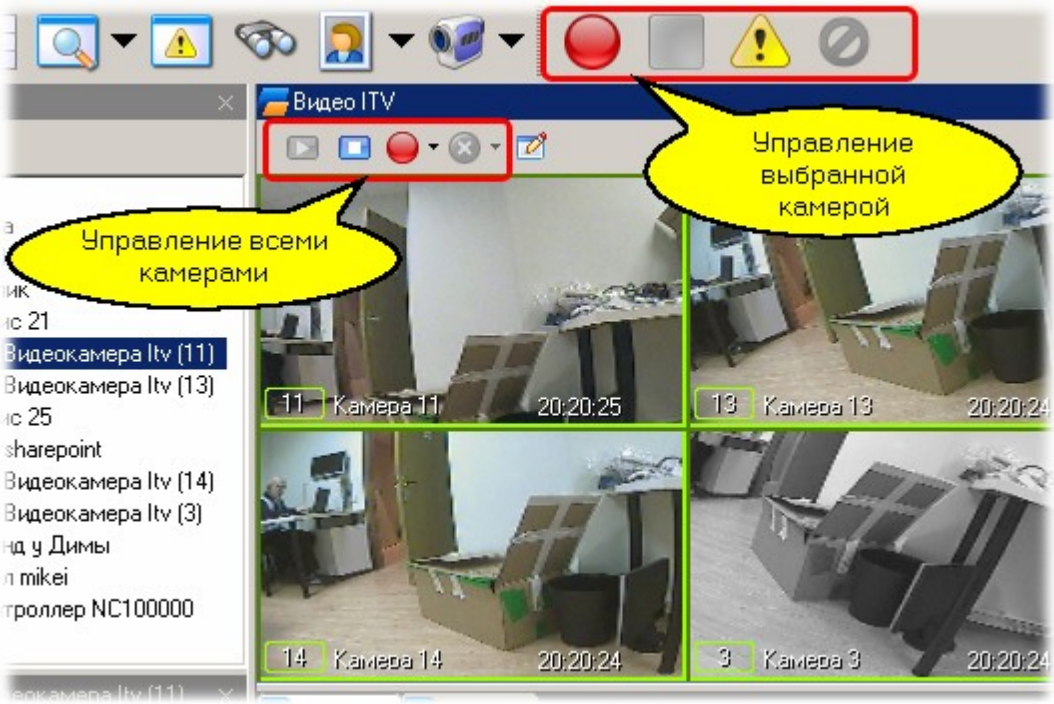
а затем размещаем новое окно в мониторе событий удобным для нас образом и в панели инструментов окна нажимаем кнопку настройки:



В появившемся диалоге отмечаем камеры, которые будем выводить в окне видеонаблюдения. В нашем случае мы выводим все четыре камеры:



Полученный результат показан на рисунке ниже.



Теперь для любой из камер вы можете включить или выключить запись, а также включить или выключить детектор движения камеры (поставить или снять с охраны зону видеонаблюдения).

Замечание: Вы можете создавать любое количество окон видеонаблюдения, распределяя по ним предоставленные в организацию камеры, если вам это необходимо.

См. также:

- Редактор топологии[203]
- Монитор событий[287]
- Редактор заданий[321]

11.5.1.3 Автоматизация работы ИСБ "Интеллект"

Система ParsecNET 3 предоставляет возможность автоматизировать некоторые аспекты работы ИСБ "Интеллект".

Ниже приведен пример такой автоматизации.

Имеются следующие исходные условия:

- Система "Интеллект" настроена. В системе задействованы камеры с номерами 5 и 7;
- Интерфейс IIDK имеет номер 119;
- На камерах настроенные пресеты;
- В системе ParsecNET 3 присутствует охранный контроллер с настроенными областями.

Необходимо обеспечить:

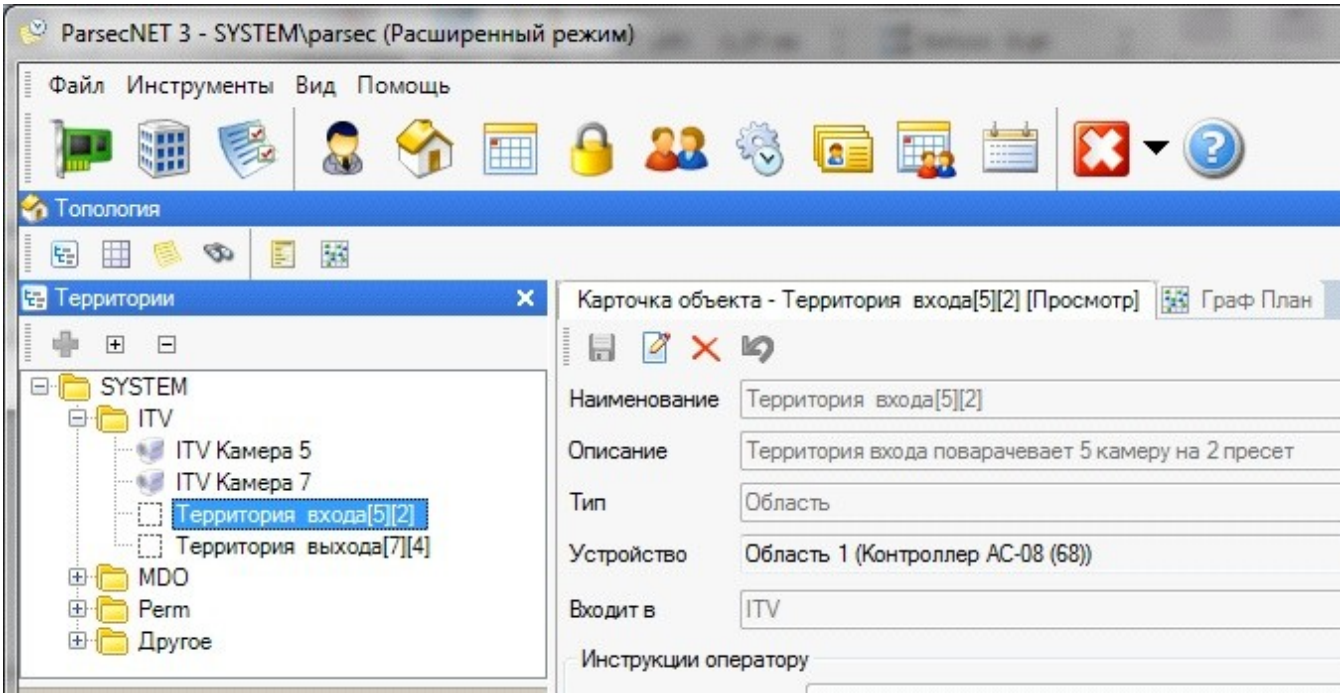
По получении тревоги с охранных областей активировать соответствующие пресеты камер:

- Для тревоги с "Территория входа" 5 камера должна повернуться в положение 2-го пресета;
- Для тревоги с "Территория выхода" 7 камера должна повернуться в положение 4-го пресета.

(Задача выполняется без использования макросов ИСБ "Интеллект")

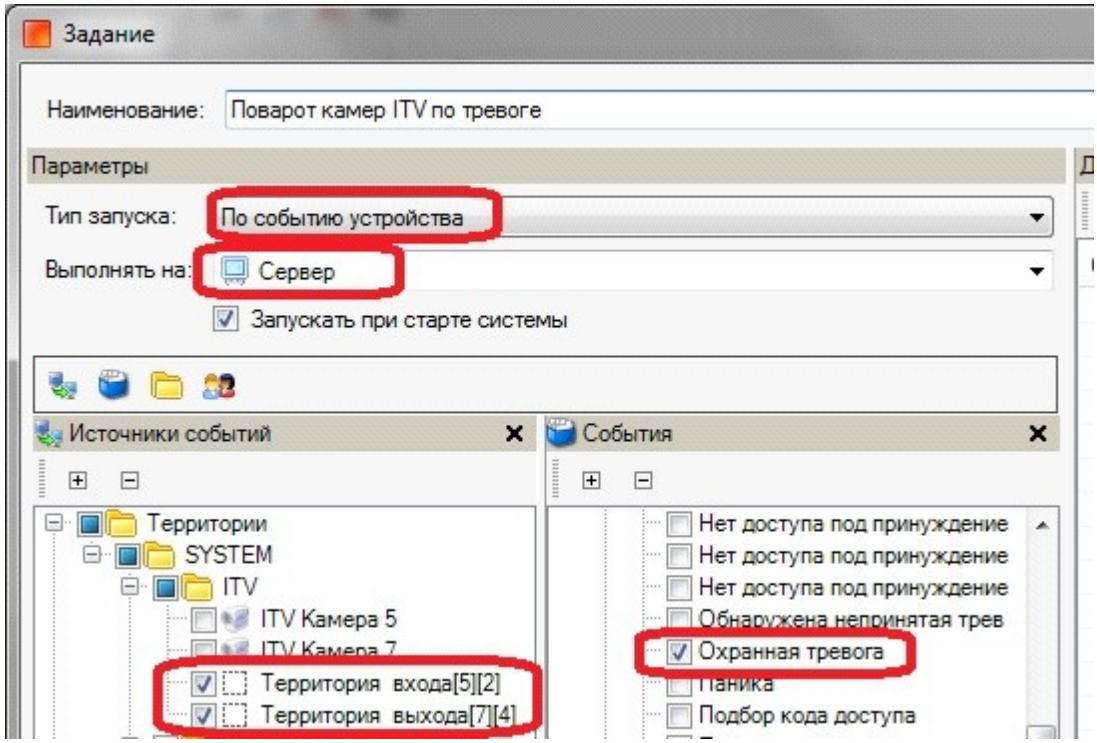
Для реализации данной задачи необходимо выполнить следующие действия:

1. В редакторе топологии назовите территории в соответствии с маской <название территории>[номер поворотного устройства][номер пресета]:



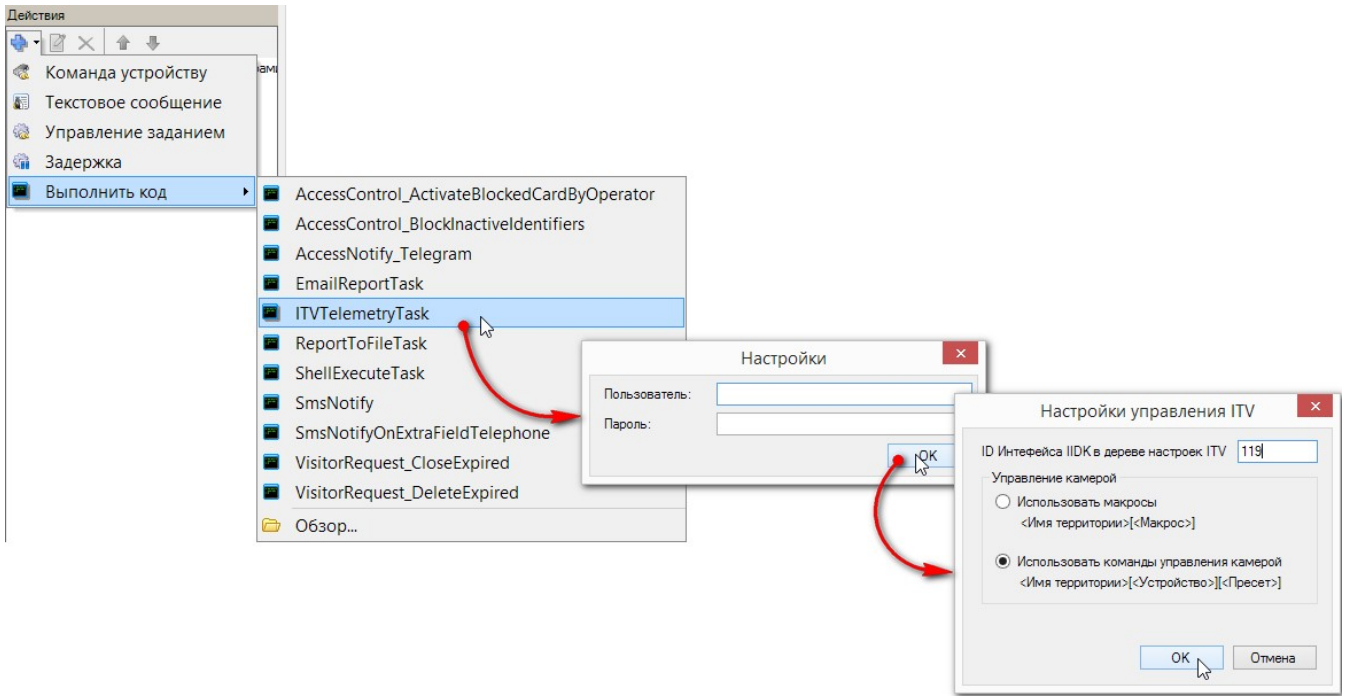
2. Создаем задание и указываем необходимые параметры:

   - Тип запуска: *По событию устройства*;
   - Выполнять на: *Сервер* (компьютер, на котором установлена ИСБ "Интеллект");
   - На вкладке *Источники событий* выберите территории охранного контроллера;
   - На вкладке *События* выберите событие "Охранная тревога":



3. Добавьте действие «Выполнить код». Выберите файл скрипта ITVTelemetryTask и укажите правильные параметры:

- Логин и пароль к системе ParsecNET 3 того оператора, который имеет доступ к просмотру задействованных территорий (см. шаг 1 и 2);
- Номер интерфейса IIDK из ИСБ "Интеллект" (см. Руководство по эксплуатации ИСБ "Интеллект");
- Выберите тип управления камерами. В нашем примере макросы не используются:



4. Сохраните созданную задачу.

Теперь, при получении от охранного контроллера тревоги на территории "Территория входа" поворотное устройство 5 повернет камеру в положение, заданное во 2-м пресете. А в случае тревоги на "Территории выхода" - 7 камера придет в положение, заданное в 4-м пресете.

11.5.2 Система GOALCity

Основные возможности

ParsecNET 3 поддерживает работу только с системой GOALCity версии Cassandra.



Данный раздел не является руководством по использованию системы GOALCity, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы GOALCity обратитесь к оригинальному руководству.

Видеосистема GOALCity предоставляет поддержку следующих функциональных возможностей:

- Просмотр "живого" видео с камер системы видеонаблюдения (без возможности самостоятельно создавать "раскладки" камер в окне видеонаблюдения);
- Сохранение меток видеоархива по событиям в системе ParsecNET 3;
- Просмотр связанных с событиями системы видеозаписей при наличии меток;
- Включение и выключение режима охраны (детектор движения или активности видеокамеры).
- Использование подсистемы распознавания номеров для идентификации автомобилей;
- Получение событий от видеосистемы и сохранение их в архиве событий ParsecNET 3.

В последующих подразделах рассмотрены вопросы подключения системы GOALCity.

Детальное рассмотрение работы с окном видеонаблюдения данный документ не содержит, поскольку данное окно является компонентом системы GOALCity и полностью повторяет работу окна видеонаблюдения этой системы. Для ознакомления с его работой обратитесь к документации GOALCity.

Для использования любой из видеокамер подсистемы GOALCity для распознавания номерных знаков автомобилей данная функция должна быть предварительно настроена собственными средствами GOALCity. Если такая настройка произведена, можно с использованием программного контроллера и редактора заданий системы ParsecNET 3 организовать автомобильную проходную[584].



Для работы подсистемы GOALCity требуется установка на рабочую станцию Parsec клиента GOALCity, а также наличие в подсистеме видеонаблюдения архивного сервера GOALCity.

См. также:

Подключение и настройка[527]

Использование системы[531]

11.5.2.1 Подключение и настройка

Особенности установки на 64-разрядные станции

При установке системы GOALCity на 32-разрядные станции дополнительных действий не требуется.

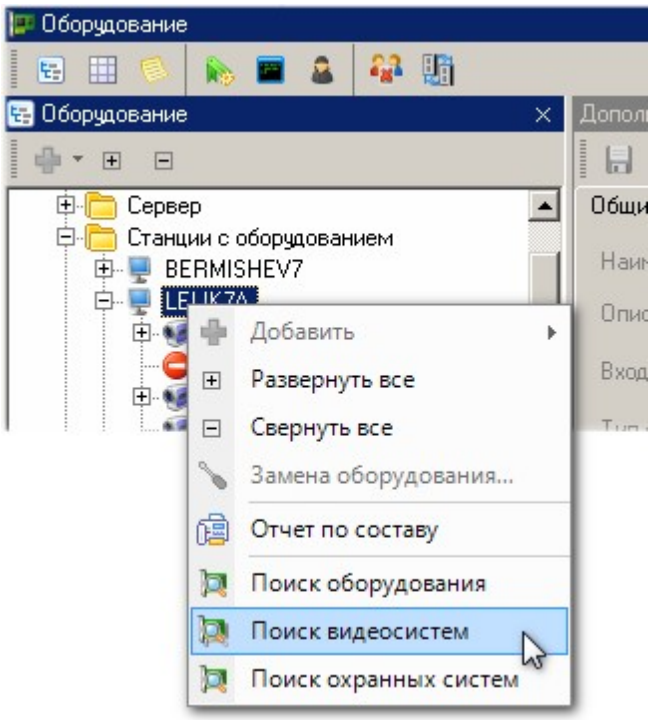
При установке GOALCity на 64-разрядних станции необходимо после обычной установки запустить приложение "ParsecNET 3 - 32 bit converter.exe" из папки с установочными файлами

ParsecNET 3. Приложение запускается на тех компьютерах, на которых установлен GOALCity. Также это приложение требуется запускать каждый раз после обновления системы ParsecNET 3.

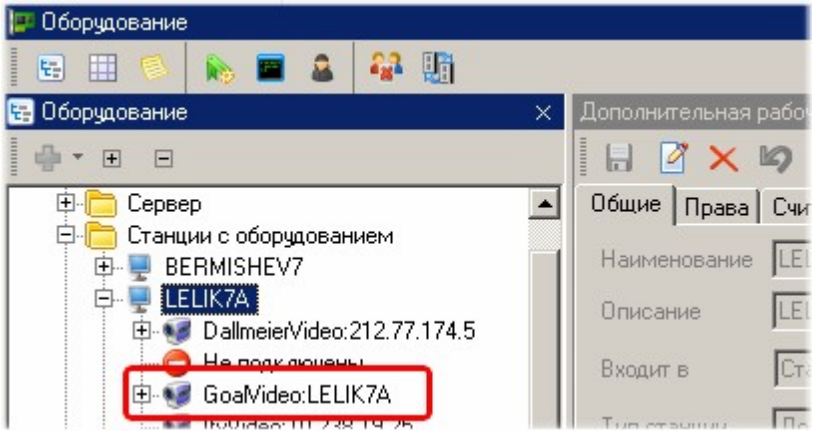
Подключение системы GOALCity

Со стороны системы ParsecNET 3 подключение системы GOALCity производится в режиме plug-and-play, запускаемой вручную. Однако для этого видеосистема должна быть предварительно установлена на тех компьютерах, на которых должны располагаться сервера GOALCity и рабочие станции ParsecNET 3 с возможностью использования видеонаблюдения. При этом на рабочих станциях ParsecNET 3 достаточно установить рабочее место видеонаблюдения штатными средствами GOALCity. Непременным условием для просмотра видеоархивов является установка архивного сервера GOALCity.

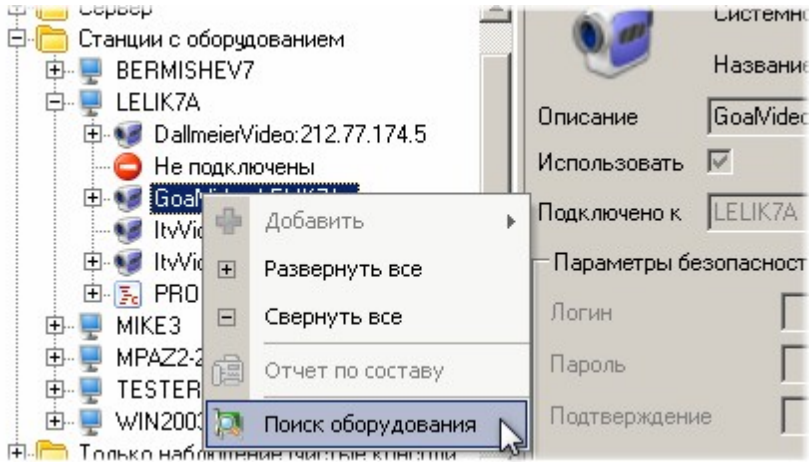
В приводимом ниже примере в системе зарегистрирована рабочая станцию "LELIK7A". Запустите на данной рабочей станции поиск видеосистем:



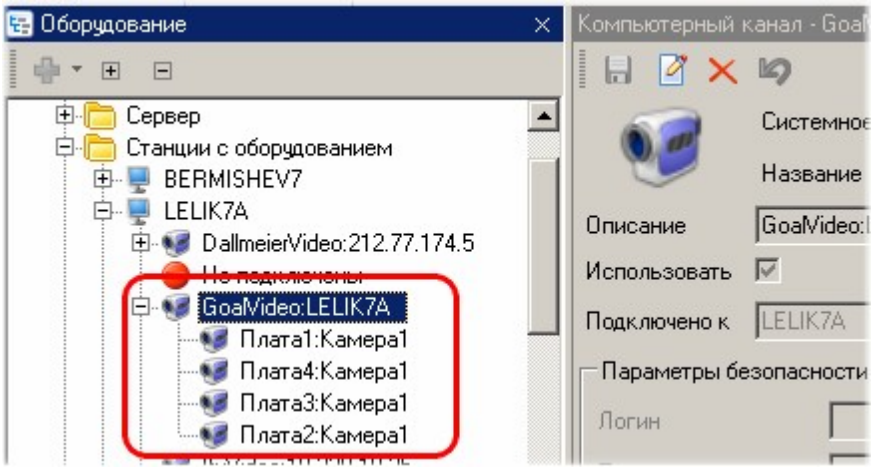
IP-адрес ПК, на котором установлен сервер видеосистемы (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования"). В результате появится канал с названием "GoalVideo:LELIK7A":



Далее на этом канале запустите поиск оборудования для обнаружения видеокамер:



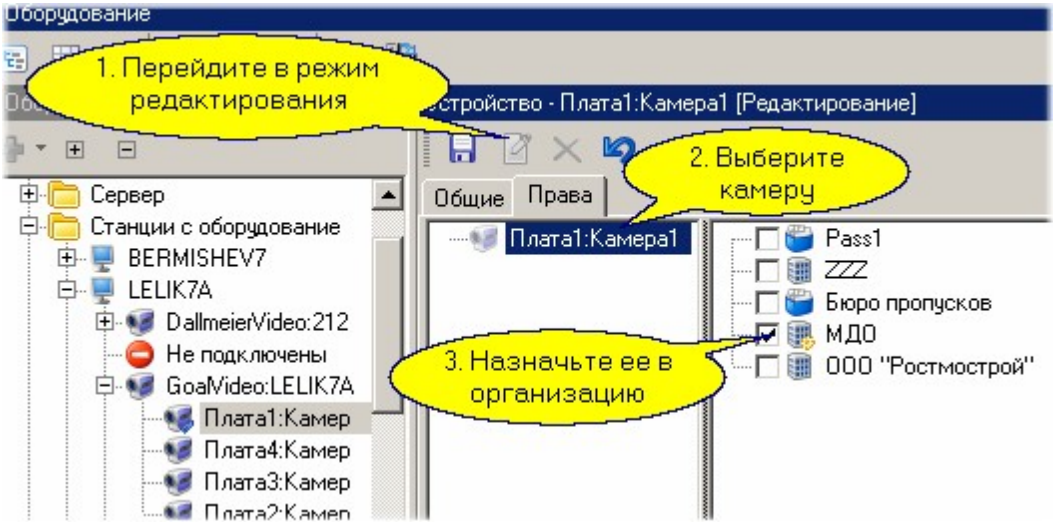
В результате на этом канале должны появиться подключенные к видеосерверу камеры:



Канал и камеры будут видны на любой рабочей станции ParsecNET 3, но использование камер будет возможно только на тех станциях, на которых установлен клиент системы GOALCity.

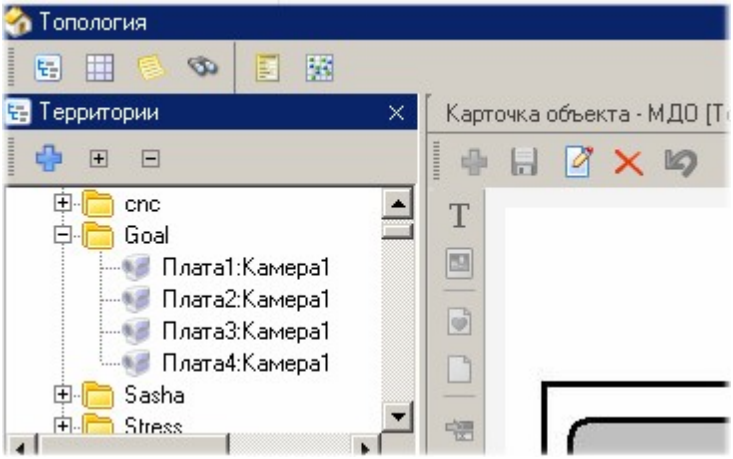
Настройка использования камер

В панели свойств редактора оборудования каждую из видеокамер можно назначить для использования в одной или более организации системы ParsecNET 3, как показано на рисунке ниже:

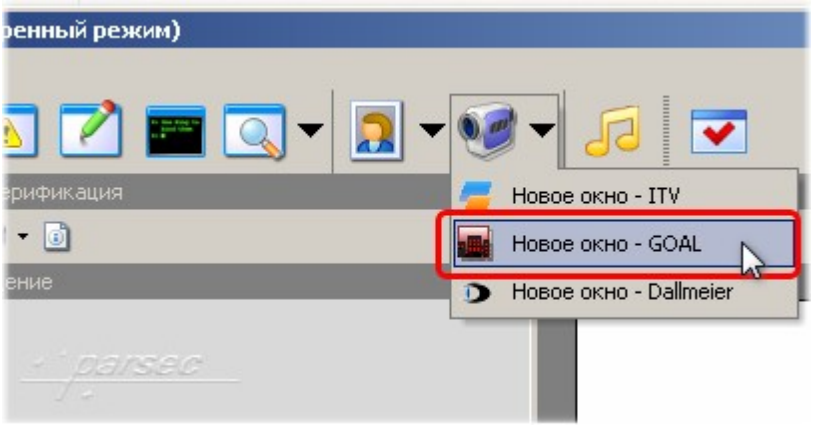


Распределение камер по топологии

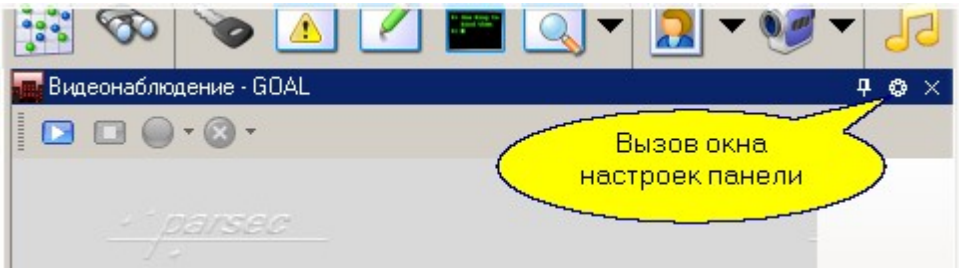
Теперь с использованием редактора топологии размещаем камеры как нам удобно в топологии системы:



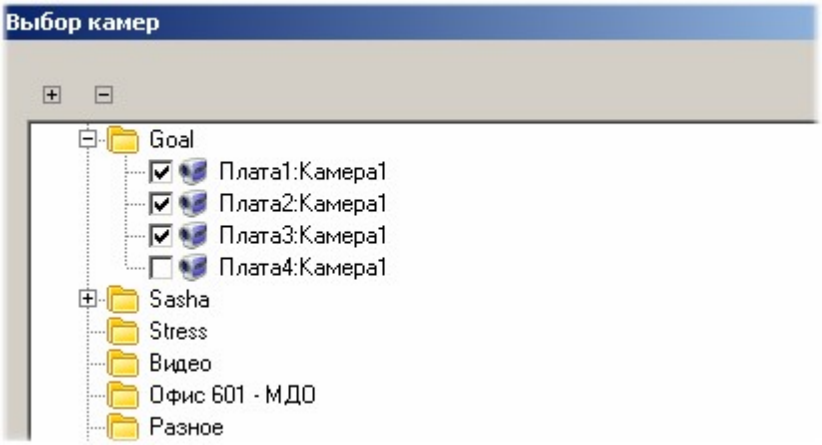
В мониторе событий можно создать одну или более панелей видеонаблюдения:



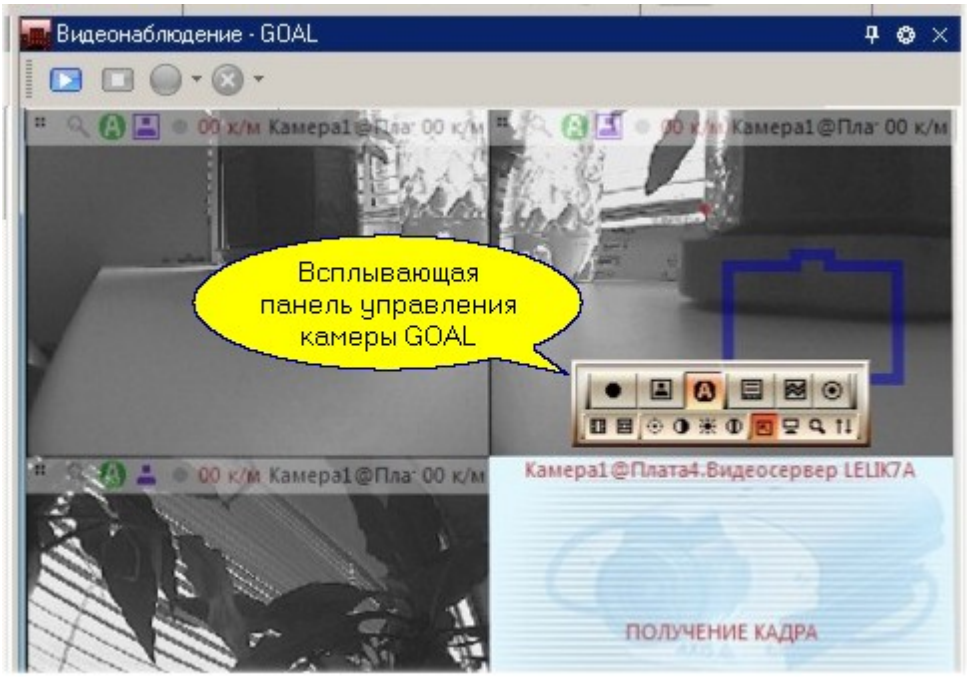
На созданной панели откройте окно настроек:



В окне настроек укажите, какие камеры включить в эту панель:



Результатом будет сформированная панель видеонаблюдения:



См. также:

Система GOALCity[527]

Использование системы[531]

11.5.2.2 Использование системы

Совместная работа GOALCity и Parsec

Совместная работа Parsec с системой видеонаблюдения GOALCity аналогична[522] работе с ИСБ "Интеллект". Дополнительный функционал, обеспечиваемый системой видеонаблюдения GOALCity, позволяет использовать видеокамеры в качестве источника идентификационной информации автомобилей. При этом предварительно камера GOALCity должна быть настроена для работы в режиме распознавания автомобильных номеров.

См. также:

Система GOALCity[527]

Подключение и настройка[527]

Автопроходная на основе программного контроллера[584]

11.5.3 Система TRASSIR

Данный раздел не является руководством по использованию системы TRASSIR компании DSSL, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы TRASSIR обратитесь к оригинальному руководству.

Видеосистема TRASSIR предоставляет поддержку следующих функциональных возможностей:

- Просмотр "живого" видео с камер системы видеонаблюдения (без возможности самостоятельно создавать "раскладки" камер в окне видеонаблюдения);
- Ручное управление записью через монитор событий системы;
- Управление записью с камер по событиям системы или с использованием менеджера заданий;
- Просмотр связанных с событиями системы видеозаписей;
- Включение и выключение режима охраны (детектор движения или активности видеокамеры);
- Использование модуля AutoTrassir для распознавания автомобильных номеров;
- Получение событий от видеосистемы и сохранение их в архиве событий ParsecNET 3.

В последующих подразделах рассмотрены вопросы подключения системы TRASSIR, а также ее использование в составе ParsecNET 3 при мониторинге.

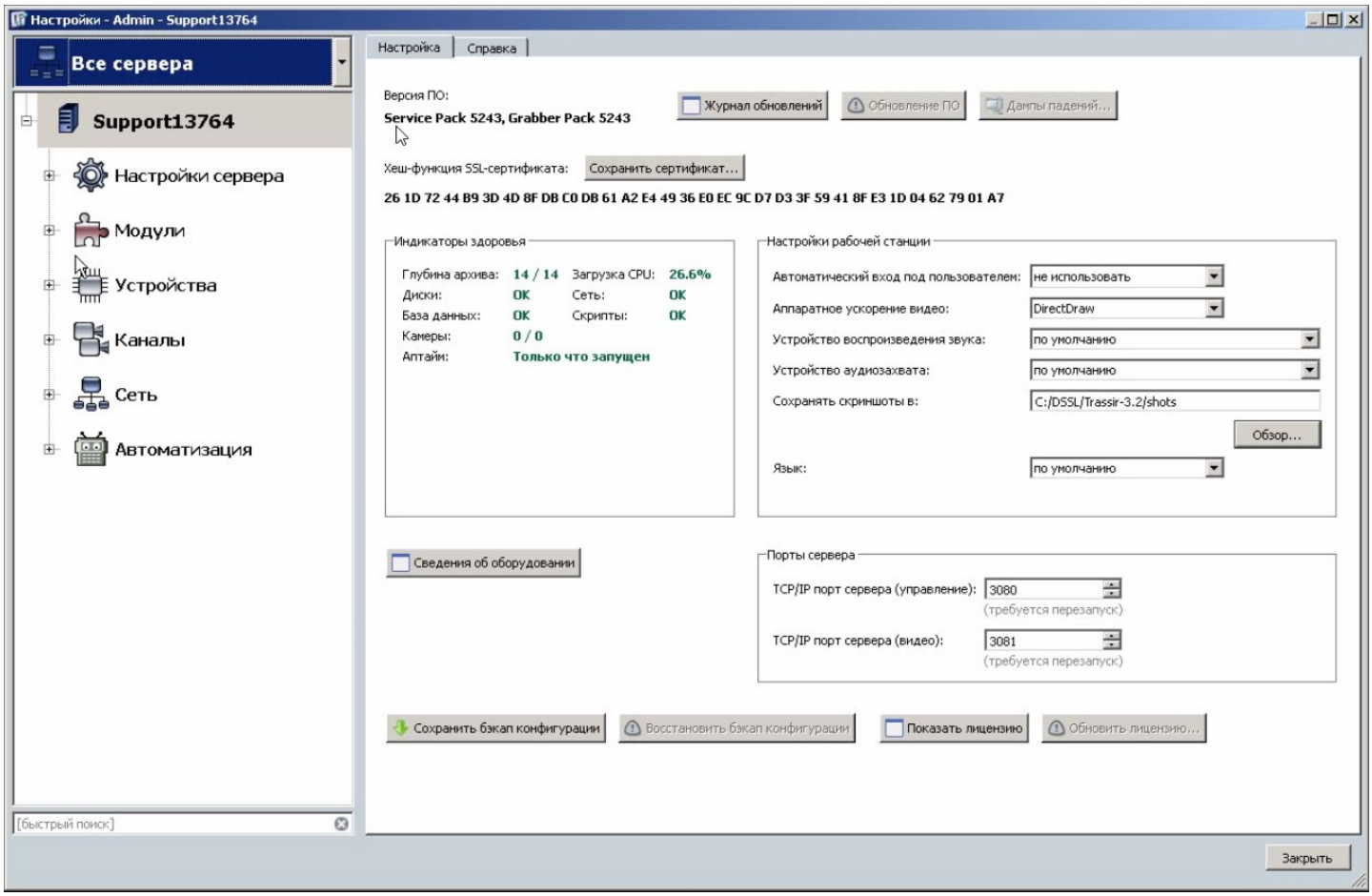
Детальное рассмотрение работы с окном видеонаблюдения данный документ не содержит, поскольку данное окно является компонентом системы TRASSIR и полностью повторяет работу окна видеонаблюдения этой системы. Для ознакомления с его работой обратитесь к документации TRASSIR.

Для использования любой из видеокамер подсистемы TRASSIR для распознавания номерных знаков автомобилей данная функция должна быть предварительно настроена собственными средствами TRASSIR. Если такая настройка произведена, можно с использованием программного контроллера и редактора заданий системы ParsecNET 3 организовать автомобильную проходную[584].

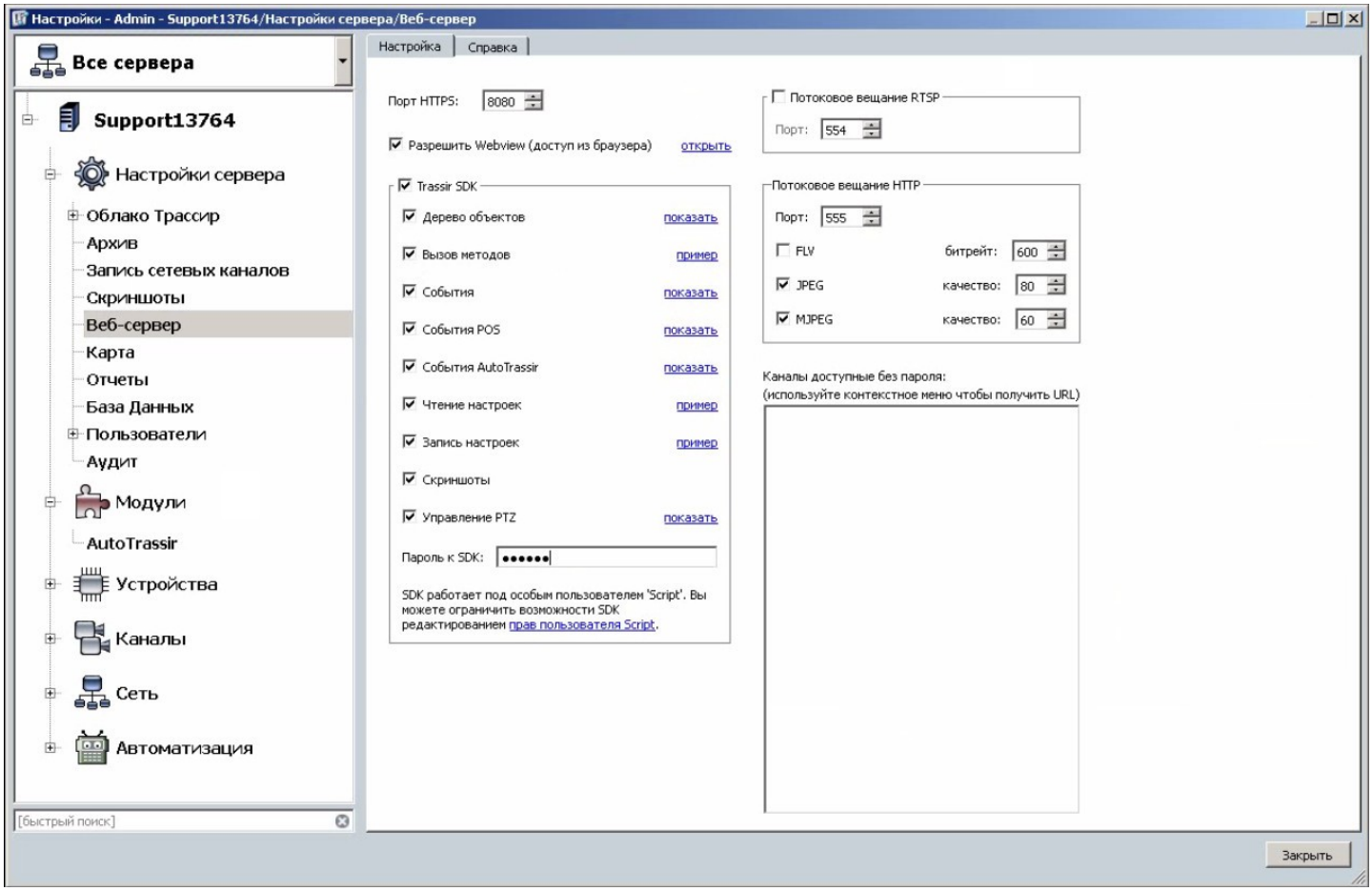
11.5.3.1 Настройка

Скачайте установочный пакет системы TRASSIR с сайта производителя.

Установите сервер системы TRASSIR. Запустите программу и откройте окно настроек:



Перейдите в раздел "Настройки сервера" - "Веб-сервер". На правой панели установите флажок *Разрешить Webview (доступ из браузера)*. Затем задайте пароль SDK:



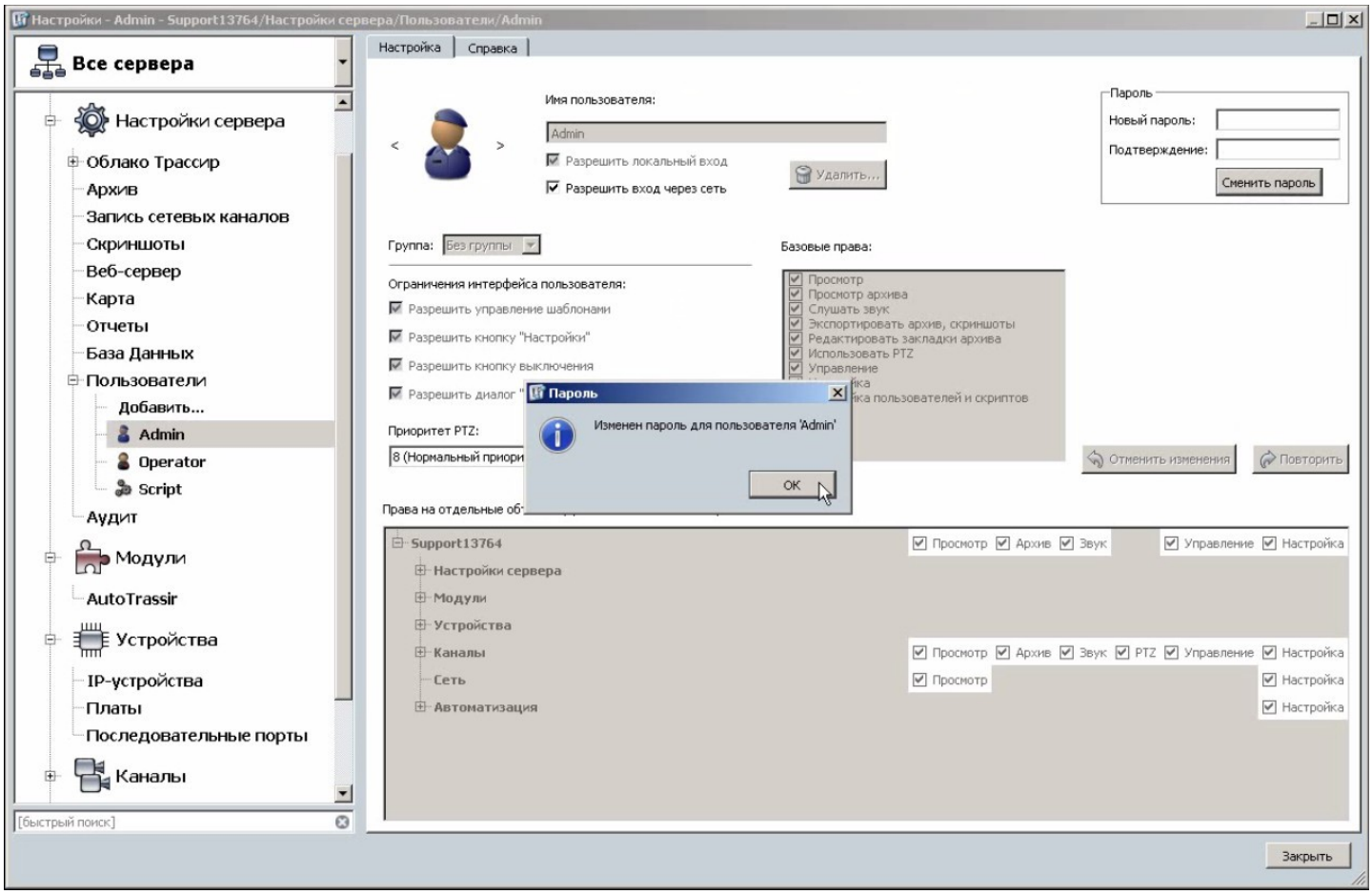
Для настройки доступа пользователя с административными правами перейдите в раздел "Настройки сервера" - "Пользователи" - "Админ".

В правой панели установите флажок *Разрешить вход через сеть*.

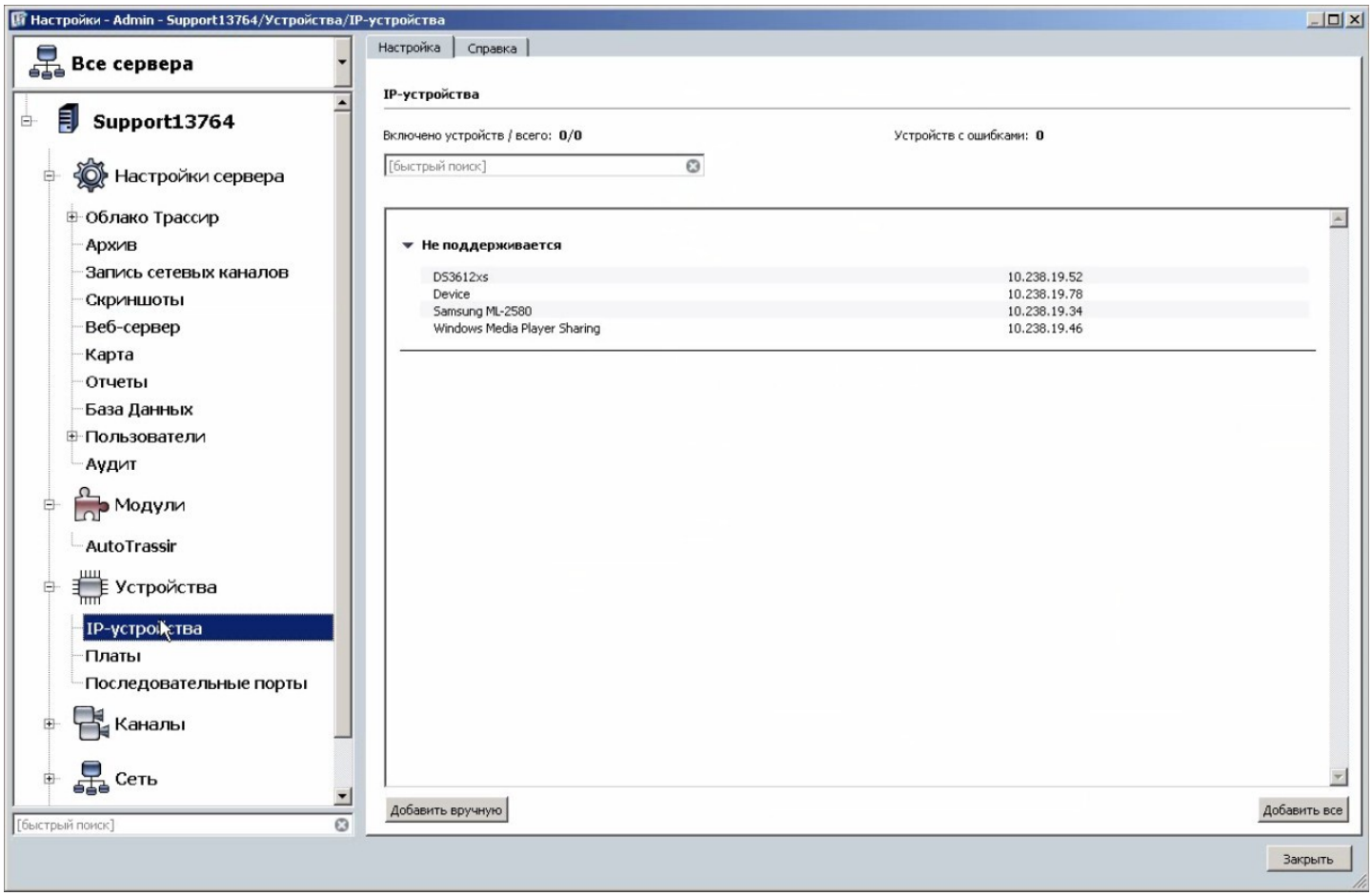
В информационном блоке *Пароль* задайте новый пароль администратора и подтвердите его, после чего нажмите на кнопку *Сменить пароль*.

Пароль к SDK и пароль администратора должны быть одинаковыми.

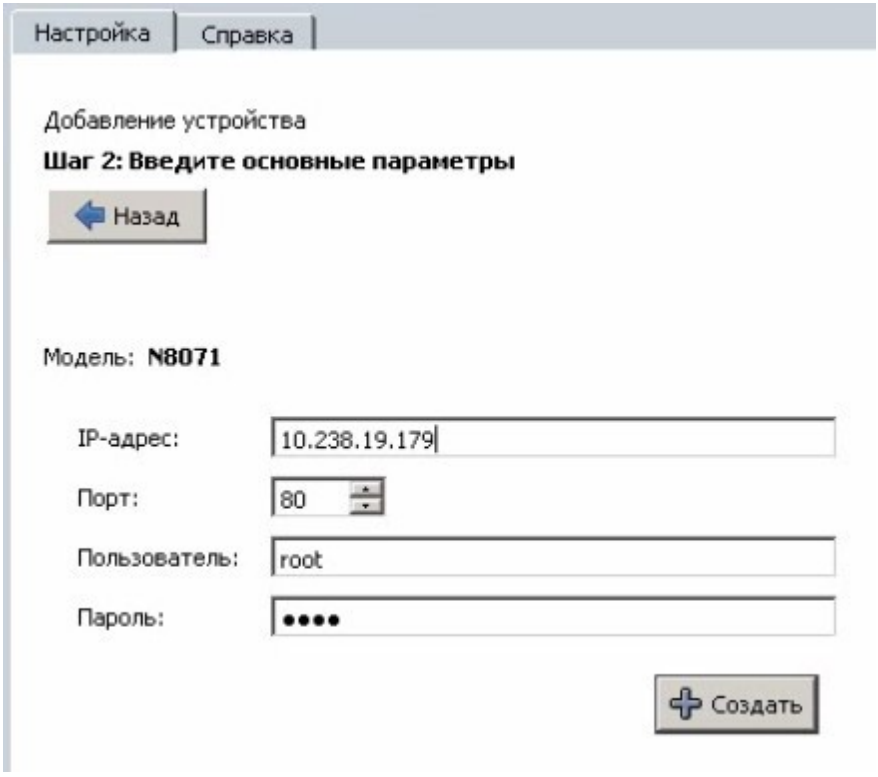
Подтвердите смену пароля, нажав на кнопку *ОК* в окне сообщения:



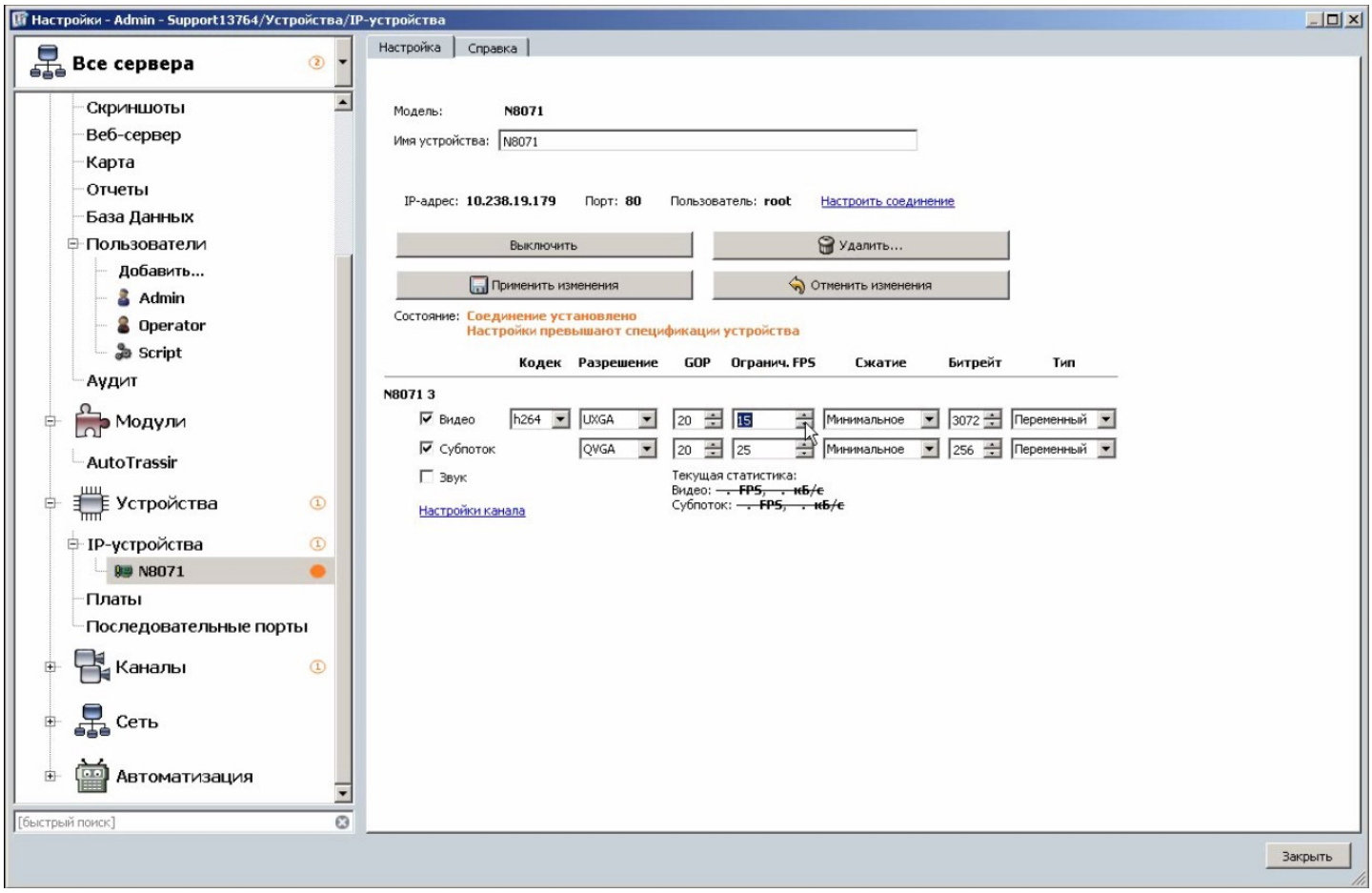
Если в мастере первого запуска системы TRASSIR был указан правильный IP-адрес камеры, то она должна подключиться автоматически. Если по каким-либо причинам этого не произошло, подключите камеру(-ы) вручную. Для этого перейдите в раздел "Устройства" - "IP-устройства":



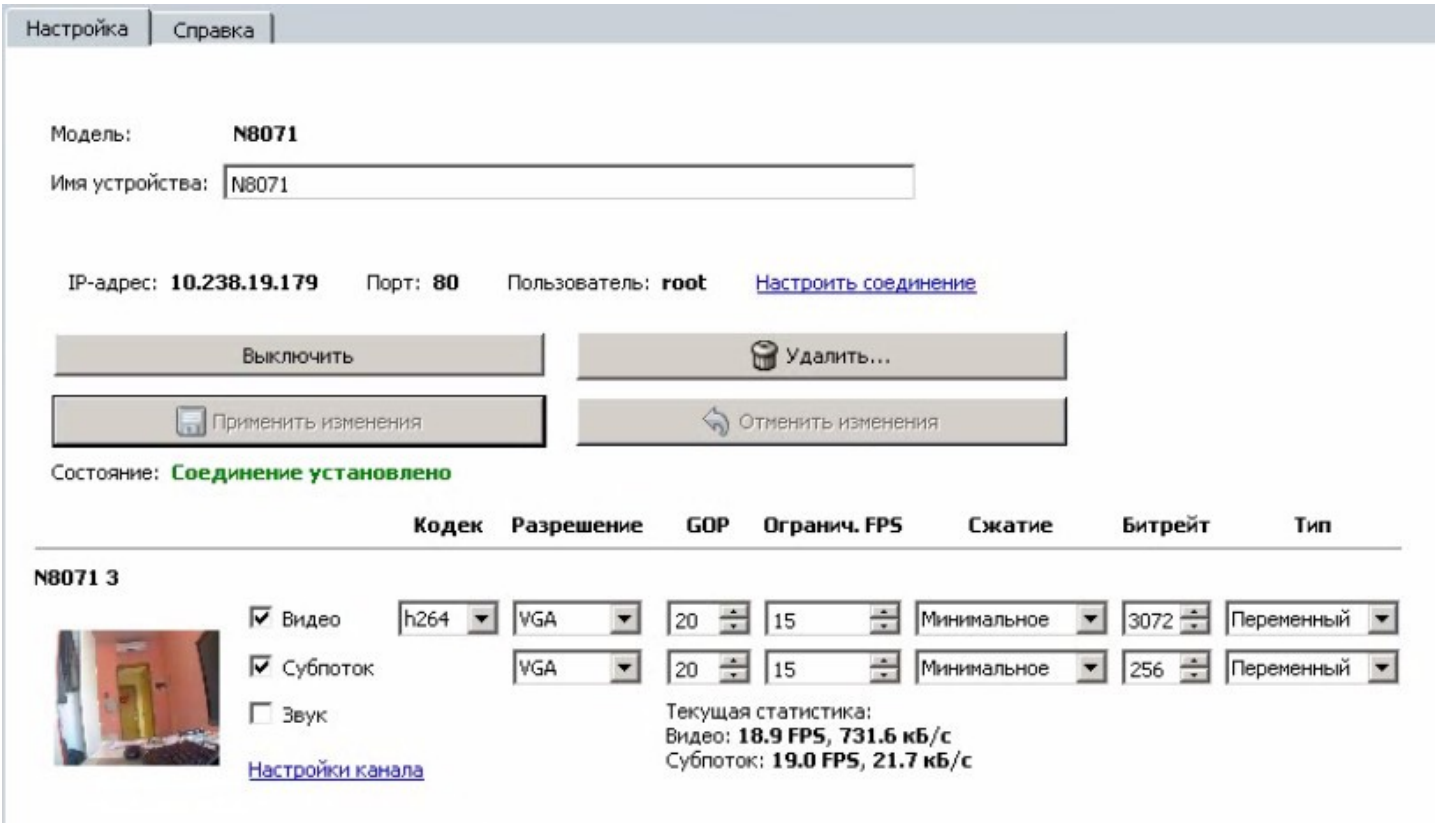
На правой панели нажмите на кнопку *Добавить вручную* и в последовательно раскрывающихся списках выберите производителя и модель своей IP-камеры. Откроется окно добавления устройства:



Введите IP-адрес камеры, выберите порт, и задайте имя пользователя и пароль для доступа к ней, после чего нажмите на кнопку *Создать*. Откроется окно параметров камеры:

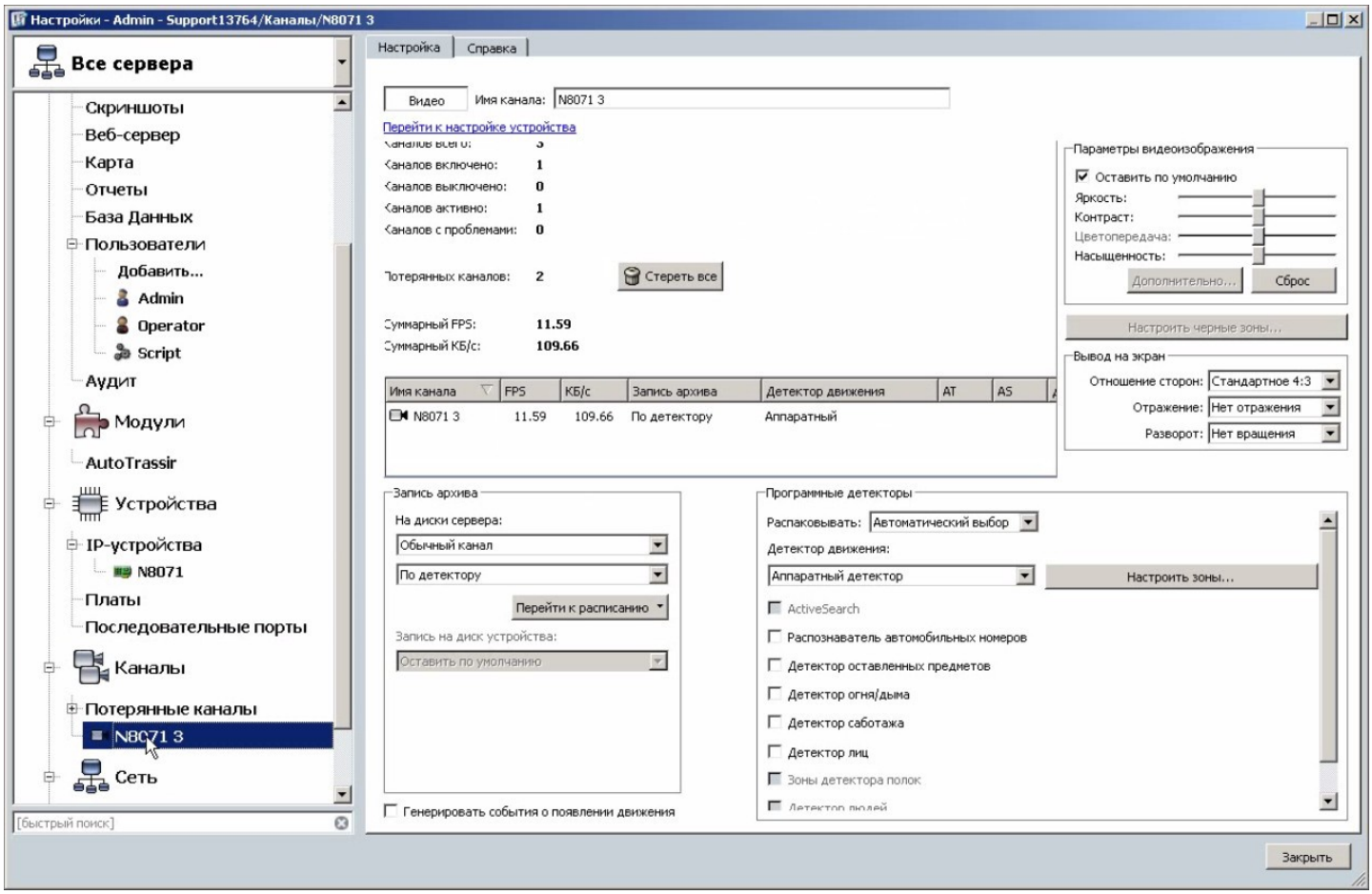


Настройте ограничение FPS, разрешение и другие параметры в соответствии со спецификациями камеры, после чего нажмите на кнопку *Применить изменения*. При правильных настройках панель должна выглядеть, например, так:



На этом основные настройки завершены.

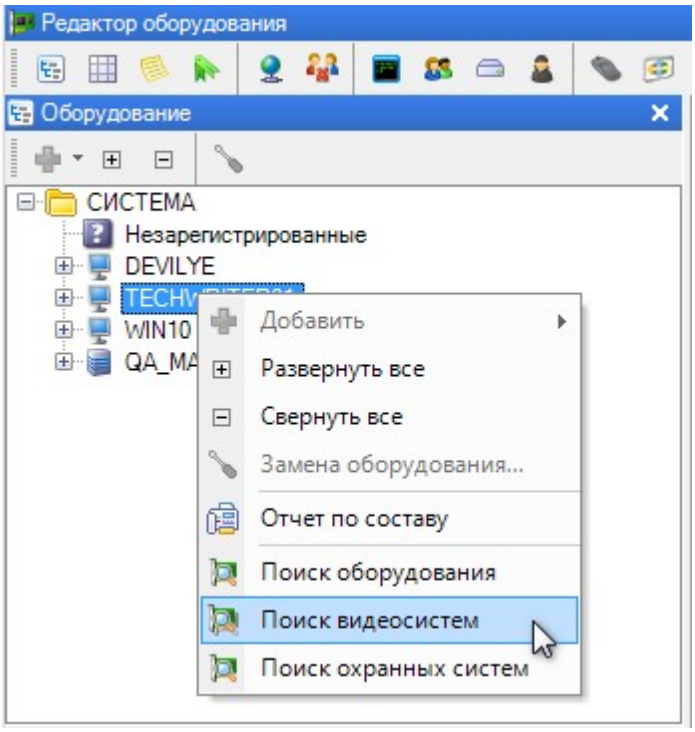
Параметры изображения, архивации и т.п. можно настроить в разделе "Каналы" - "<модель камеры> <номер канала>":



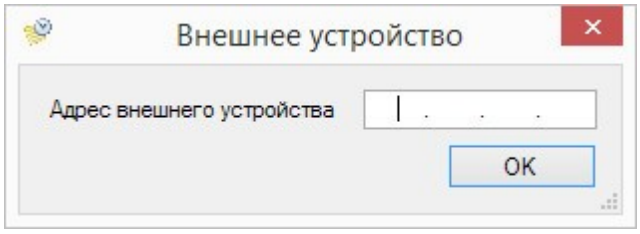
11.5.3.2 Подключение и использование системы

Рекомендуется проводить подключение системы TRASSIR на сервере ParsecNET 3, это позволит работать с ней всем рабочим станциям независимо друг от друга.

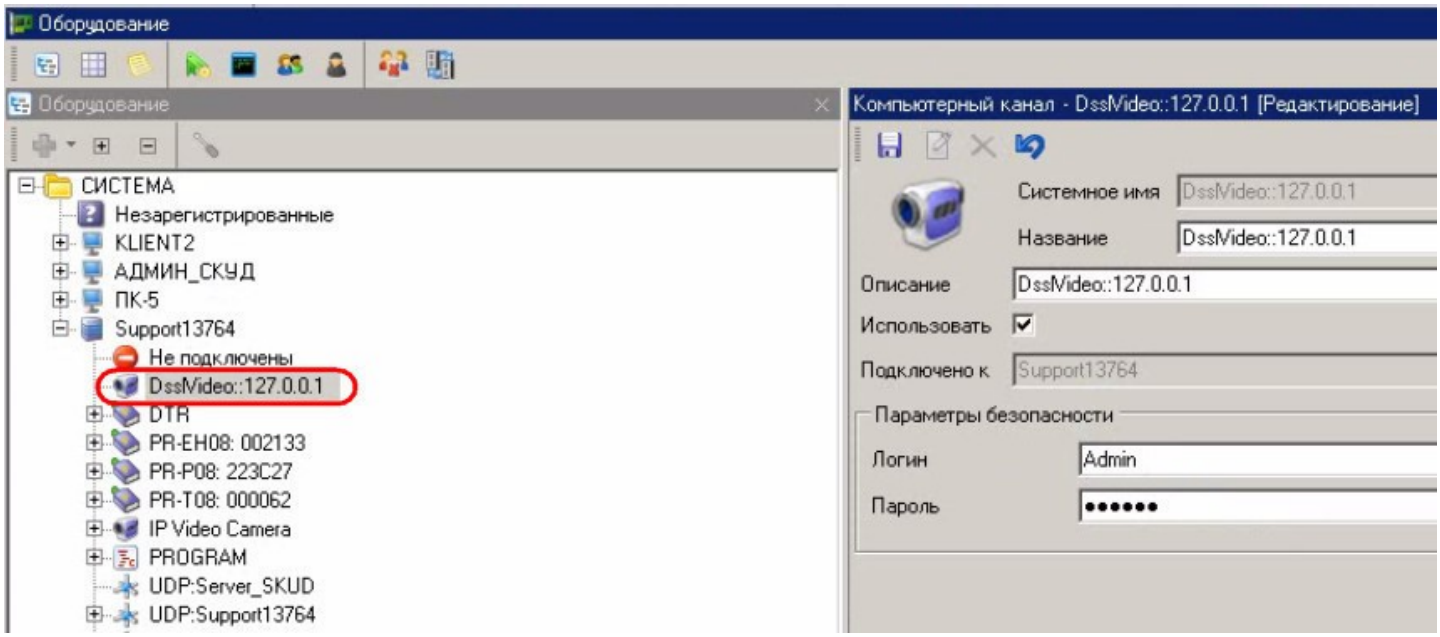
Запустите систему ParsecNET 3 и проведите поиск видеосистемы. Для этого в контекстном меню контекстном меню рабочей станции Parsec (сервера или локального ПК) выберите "Поиск видеосистем":



В открывшемся окне введите IP-адрес ПК, на котором установлено ПО TRASSIR (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования"):

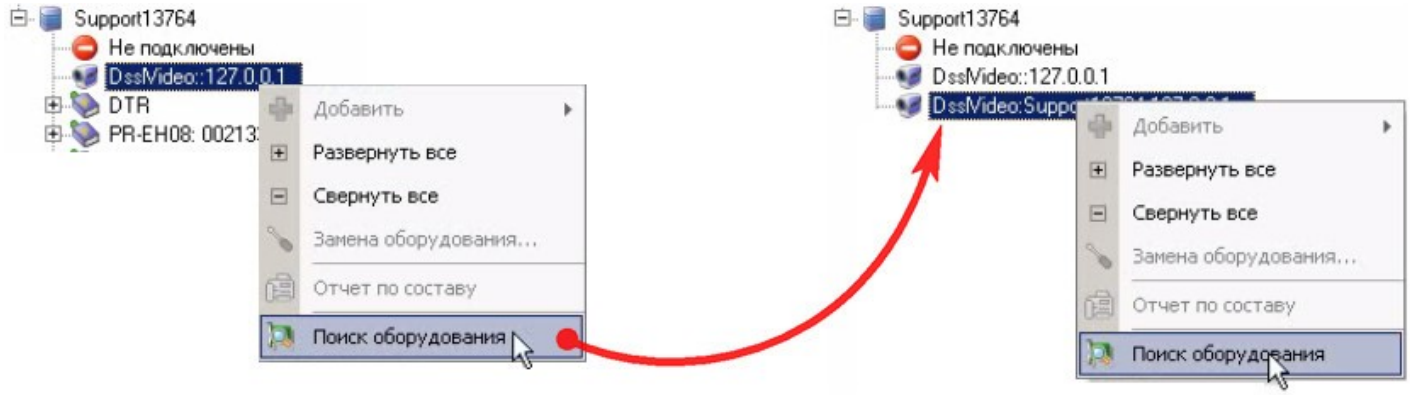


В списке оборудования должно появиться новый видеоканал с адресом сервера TRASSIR, на рисунке ниже это "DSSLVideo: 127.0.0.1":



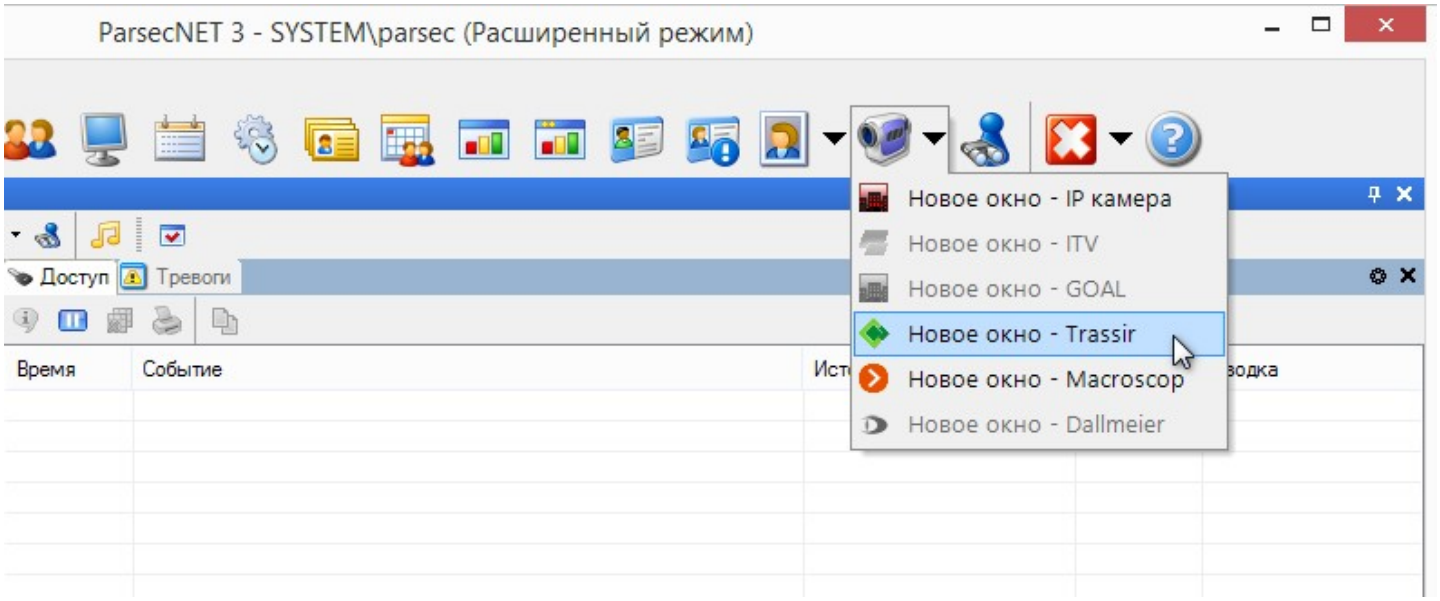
Перейдите в режим редактирования и введите логин и пароль для доступа, заданные на этапе настройки[534]. Сохраните изменения.

Проведите поиск оборудования на этом видеоканале. Будет обнаружен второй видеоканал (в нашем примере это "DssVideo:Support13764"), на котором, в свою очередь, нужно провести поиск оборудования:

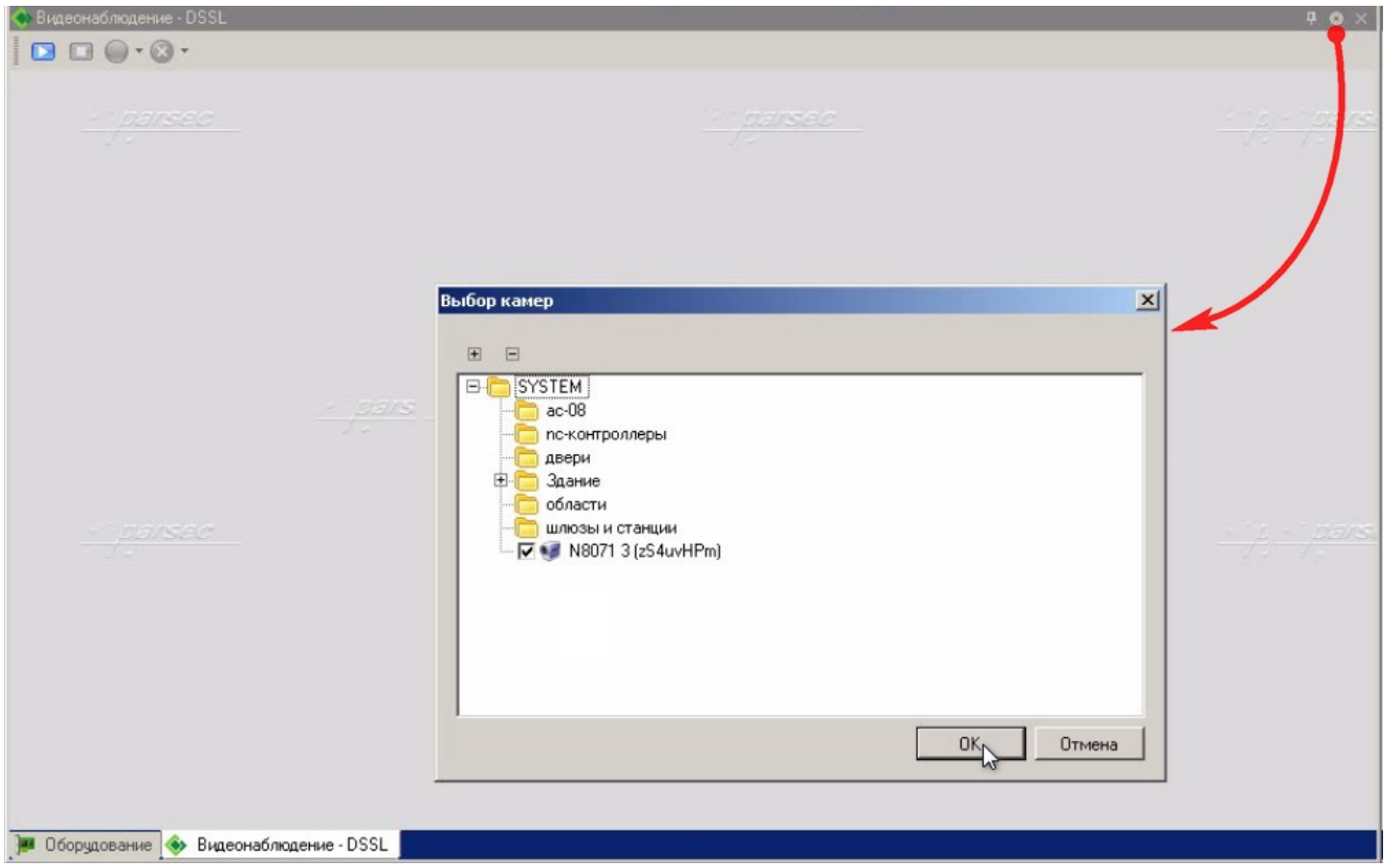


На втором видеоканале должна обнаружиться предварительно подключенная к системе TRASSIR и настроенная IP-камера.

Добавьте новое окно видеонаблюдения TRASSIR:



В окне видеонаблюдения выберите камеру системы TRASSIR и нажмите на кнопку *OK*:



Теперь в этом окне будет отображаться видео с выбранной камеры, которое можно использовать для видеоидентификации, сохранять в архив и т.п.

11.5.4 Системы Macroscop и LTV-Gorizont

В этом разделе описываются возможности видеосистемы Macroscop и настройки ParsecNET 3 для работы с ней.

Видеосистема LTV-Gorizont отличается от Macroscop следующим:

- работает только с видеокамерами марки LTV;
- не имеет возможности распознавания автомобильных номеров.

Установка и настройки ParsecNET 3 для работы с LTV-Gorizont точно такие же, как и для Macroscop.



Данный раздел не является руководством по использованию системы Macroscop (LTV-Gorizont), а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы Macroscop (LTV-Gorizont) обратитесь к оригинальному руководству.

Основные возможности

Видеосистема *Macroscop* предоставляет поддержку следующих функциональных возможностей:

- Просмотр "живого" видео с камер системы видеонаблюдения (без возможности самостоятельно создавать "раскладки" камер в окне видеонаблюдения);
- Ручное управление записью через монитор событий системы;
- Управление записью с камер по событиям системы или с использованием менеджера заданий;
- Просмотр связанных с событиями системы видеозаписей;
- Распознавания автомобильных номеров;
- Получение событий от видеосистемы и сохранение их в архиве событий ParsecNET 3*:*
  - Автоматическое определение появления человеческого лица в поле камеры;
  - Автоматическое информирование о предметах, оставленных в заданной области поля зрения камеры;
  - Автоматическое информирование о движении в заданной области поля зрения камеры.

В последующих подразделах рассмотрены вопросы использования системы в составе ParsecNET 3 при мониторинге.

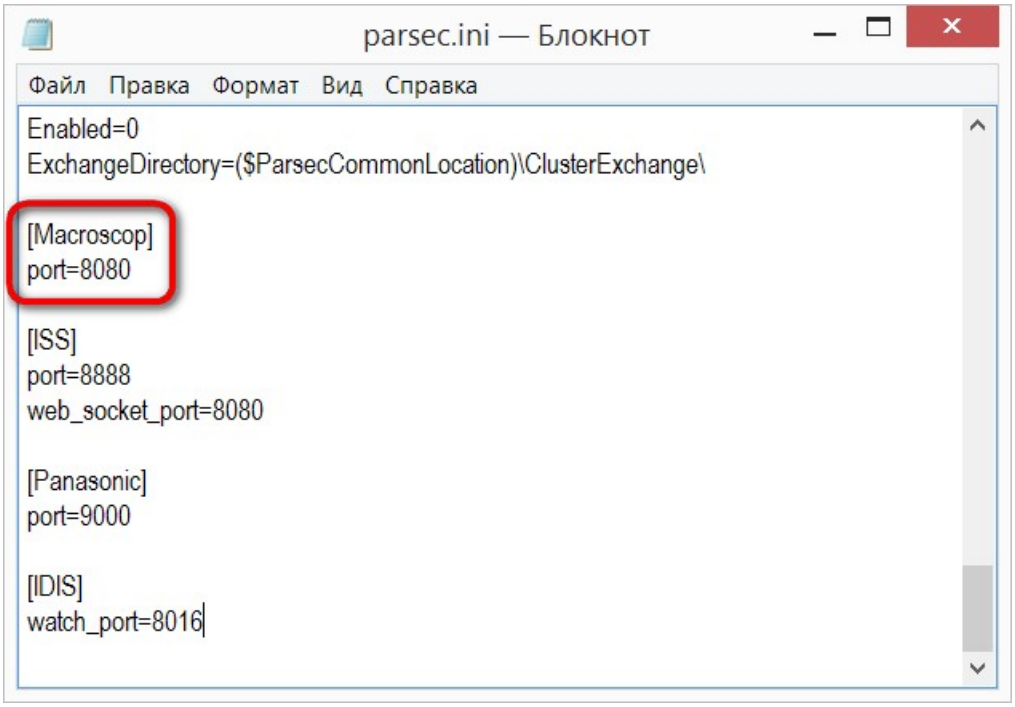
Детальное рассмотрение работы с окном видеонаблюдения данный документ не содержит, поскольку данное окно является компонентом системы Macroscop и полностью повторяет работу окна видеонаблюдения этой системы. Для ознакомления с его работой обратитесь к документации Macroscop.

Для использования любой из видеокамер подсистемы Macroscop для распознавания номерных знаков автомобилей данная функция должна быть предварительно настроена собственными средствами Macroscop. Если такая настройка произведена, можно с использованием программного контроллера и редактора заданий системы ParsecNET 3 организовать автомобильную проходную[584].

11.5.4.1 Подключение и настройка

Установите систему Macroscop с дистрибутивного носителя, следуя подсказкам мастера установки.

Если при настройке был изменен порт по умолчанию, то его необходимо обязательно изменить и в файле настройки ParsecNET *parsec.ini*, находящемся по умолчанию по адресу *C:\ProgramData\MDO\ParsecNET 3*:



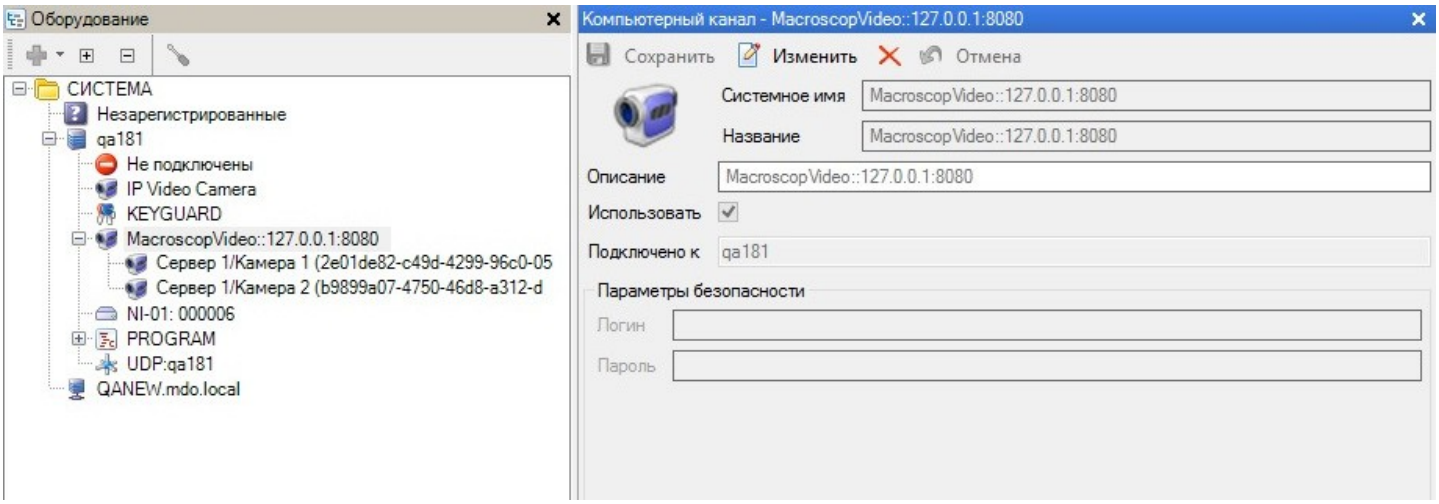
После установки запустите систему и смените логин и пароль доступа. Они понадобятся для интеграции с системой ParsecNET 3.

11.5.4.2 Использование системы

Запустите систему ParsecNET 3 на ПК, на котором установлена система Macroscop, и проведите поиск новой видеосистемы. Для этого в контекстном меню рабочей станции Parsec (сервера или локального ПК) выберите команду "Поиск видеосистем".

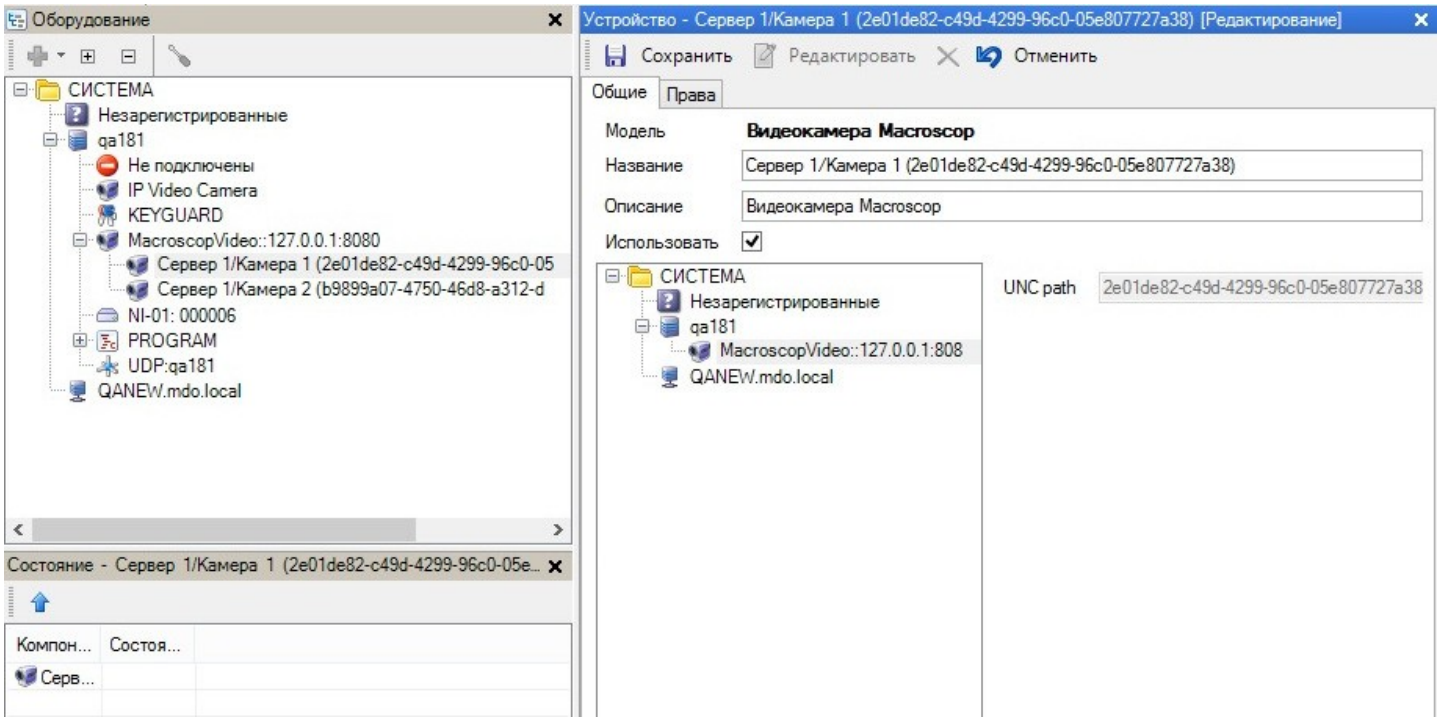
В открывшемся окне введите IP-адрес ПК, на котором установлено ПО Macroscop (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования"), и нажмите на кнопку *ОК*.

В списке оборудования должен появиться новый видеоканал, в нашем примере это "MacroscopVideo::127.0.0.1:8080":

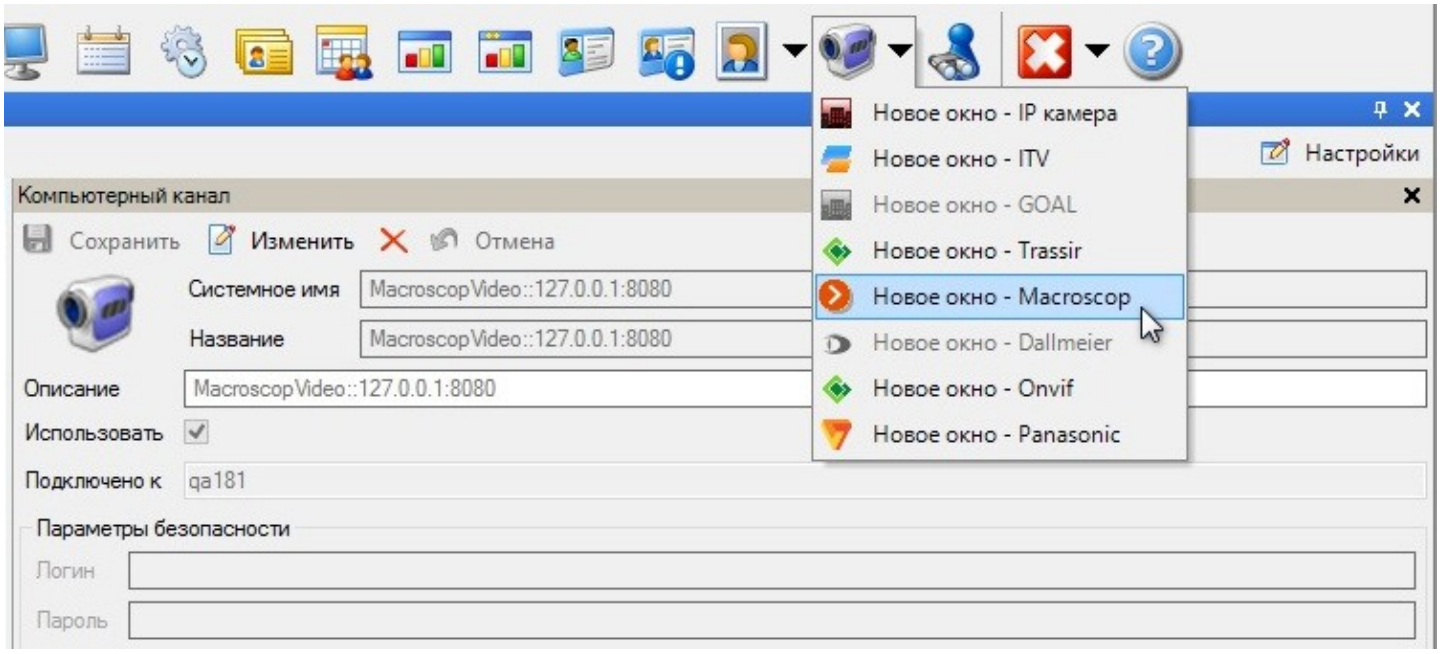


Перейдите в режим редактирования и введите логин и пароль для доступа, заданные в системе Macrosop. Сохраните изменения.

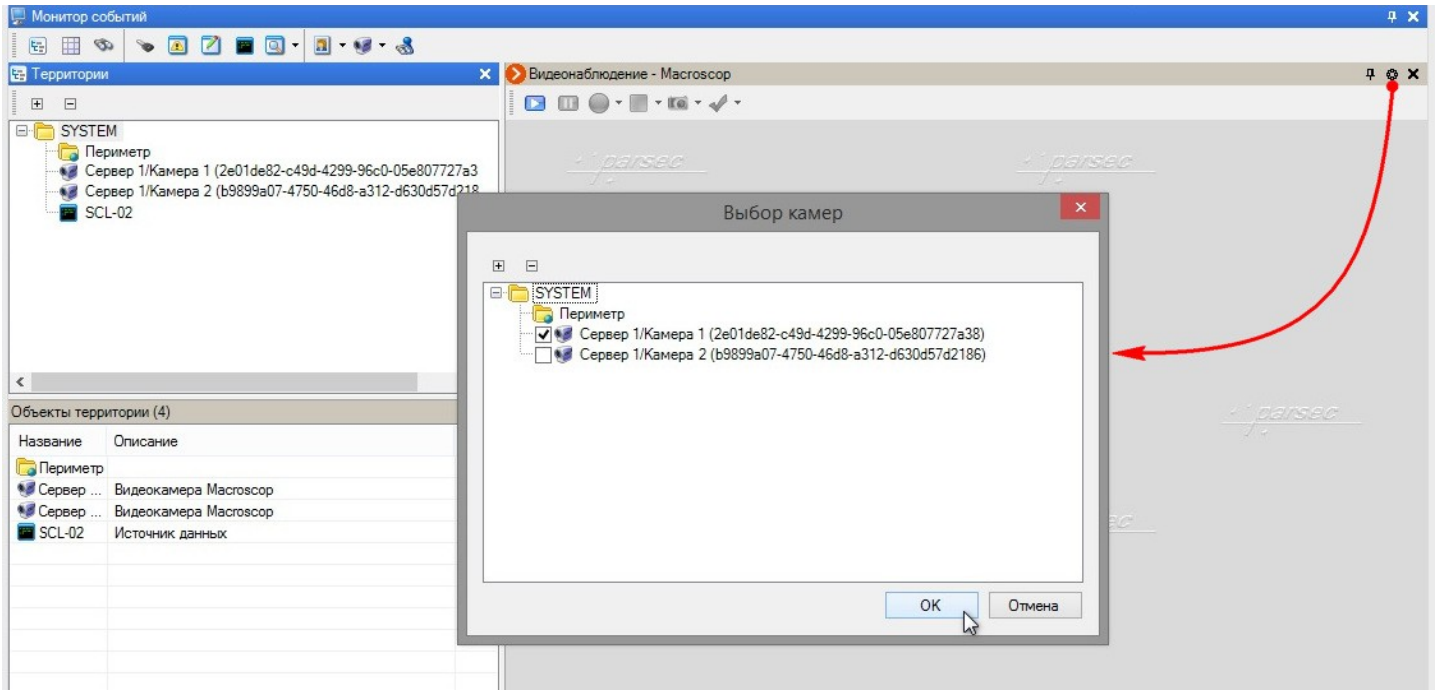
Теперь проведите поиск нового оборудования на этом видеоканале. Должны обнаружиться видеокамеры, подключенные и настроенные при установке системы Macroscop (на рис. ниже это "Сервер 1/Камера 1" и "Сервер 1/Камера 2"):



Добавьте новое окно видеонаблюдения Macroscop:



В окне видеонаблюдения выберите камеру системы Macroscop и нажмите на кнопку *ОК*:



Теперь в этом окне будет отображаться видео с выбранной камеры, которое можно использовать для видеоидентификации, сохранять в архив и т.п.

11.5.5 Система Milestone

В этом разделе описывается взаимодействие видеосистемы Milestone и ParsecNET 3.

Данный раздел не является руководством по использованию системы Milestone, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы Milestone обратитесь к оригинальному руководству.

Интеграция с ПО Milestone XProtect в системе ParsecNET 3 реализована с использованием ПО Milestone ONVIF Bridge, которое является частью открытой платформы Milestone и имеет интерфейс, поддерживающий стандарт ONVIF для извлечения живого и архивного видео из видео-менеджера Milestone XProtect.

ONVIF-это открытый глобальный консорциум, который работает над созданием стандартного и безопасного способа коммуникации между системами IP-видеонаблюдения. Цель состоит в упрощении обмена видеоданными. Для достижения этой цели Milestone Systems и разработала Milestone ONVIF Bridge.

Для установки и управления медиа-сеансами между двумя или более конечными клиентами используется протокол потоковой передачи данных в реальном времени (RTSP).

Мост Milestone ONVIF Bridge использует профиль ONVIF Profile S и RTSP для обработки запросов на видео от клиентов ONVIF, а также для потоковой передачи видео клиентам ONVIF от установленного видео-менеджера XProtect.

Ссылка на видеоинструкцию по установке и настройке Milestone ONVIF Bridge:
https://www.youtube.com/watch?v=bQXYxlFZgsE

Модуль интеграции Parsec с ONVIF - это ONVIF клиент, позволяющий получить в ПО ParsecNET 3 следующий функционал:

- получение списка видеокамер, подключенных к ONVIF Bridge (камеры не обязательно должны поддерживать стандарт ONVIF);
- получение списка видеокамер, поддерживающих стандарт ONVIF (данная функция не связана с модулем ONVIF Bridge, реализована через поддержку стандарта ONVIF Discovery);
- просмотр "живого" видеопотока с камер системы видеонаблюдения Milestone XProtect (поток получается через ONVIF Bridge по протоколу RTSP);
- просмотр "живого" видеопотока с камер, поддерживающих стандарт ONVIF (поток получается напрямую с камеры по протоколу RTSP);
- установка временных меток для видеокамер подсистемы Milistone, по которым можно через ПО ParsecNET просмотреть видеозаписи, сохраненные в архиве Milestone XProtect VMS.

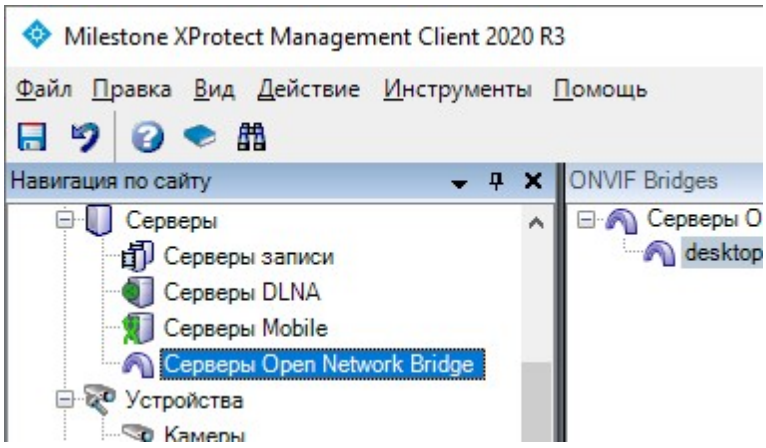
В последующих подразделах рассмотрены вопросы интеграции СКУД ParsecNET 3 с системой видеонаблюдения Milestone.

11.5.5.1 Подключение и настройка

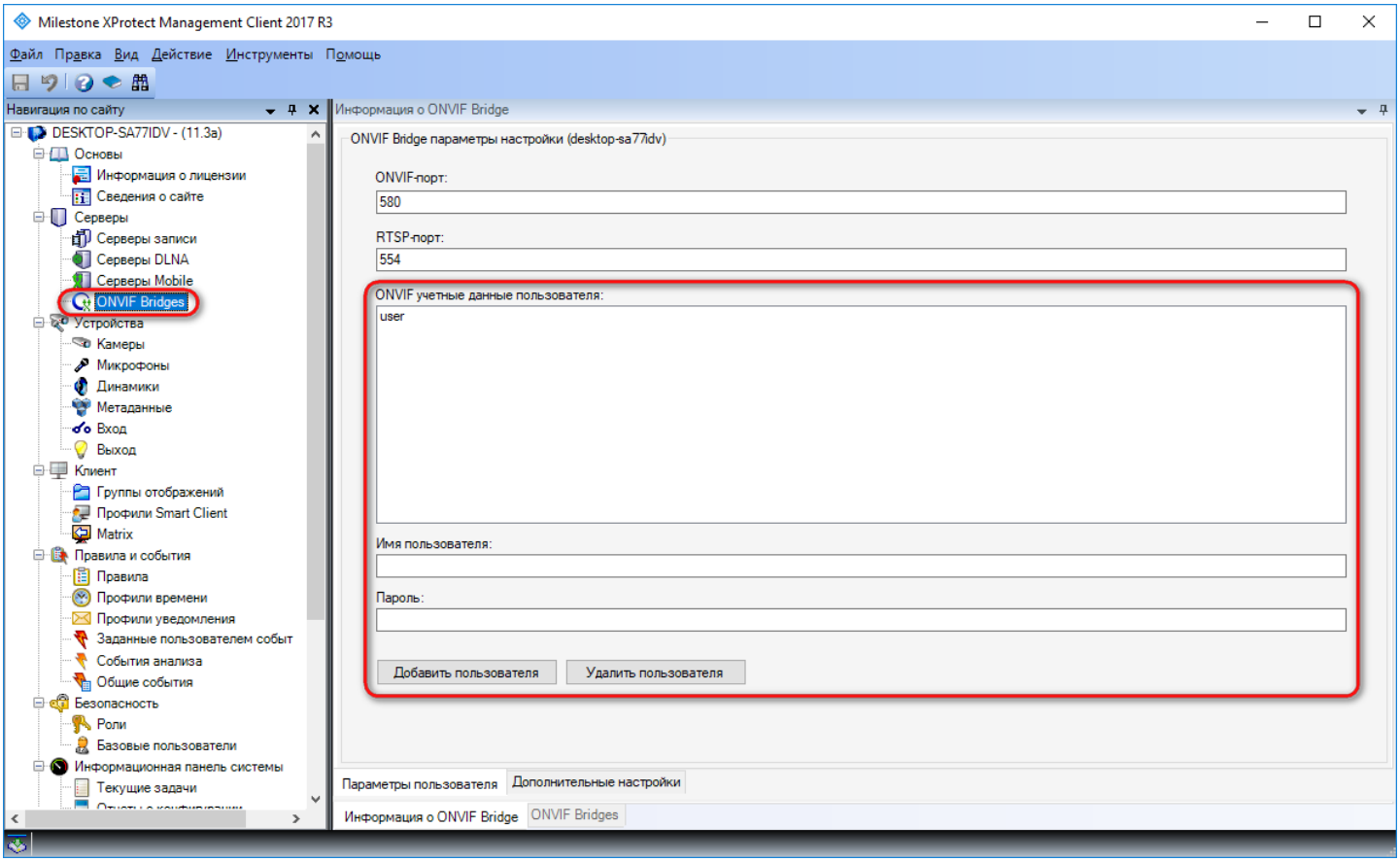
Установите необходимое ПО системы Milestone с дистрибутивного носителя, следуя подсказкам мастера установки (при необходимости обратитесь к документации Milestone).

Модуль интеграции был успешно протестирован с использованием Milestone Xpotect Professional +2017 R3 (11.3a), +2019 R3 (13.2a), +2020 R3 и Milestone Onvif Bridge 11.3.1.

1. После установки запустите программу XProtect Management Client. Дальнейшие действия зависят от используемой версии.
   - Если вы используете версию Milestone Xpotect Professional +2020 R3, то:
     - Перейдите в раздел "Безопасность" - "Роли" - "Администраторы" и добавьте базового пользователя, задав логин и пароль;
     - Перейдите в раздел в разделе "OpenNetworkBridge" и продублируйте создание пользователя с теми же логином и паролем.



   - Если вы используете версию Milestone Xpotect Professional +2017 R3 (11.3a) или +2019 R3 (13.2a), то перейдите в раздел ONVIF Bridge и создайте пользователя, задав логин и пароль для авторизации ONVIF-клиента (см. рис. ниже).

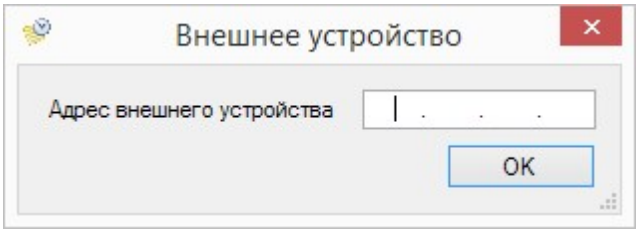


Логин и пароль понадобится указать в ПО системы ParsecNET 3.

11.5.5.2 Использование системы

Запустите консоль "Администрирование» системы ParsecNET 3 на ПК, и проведите поиск видеосистемы:

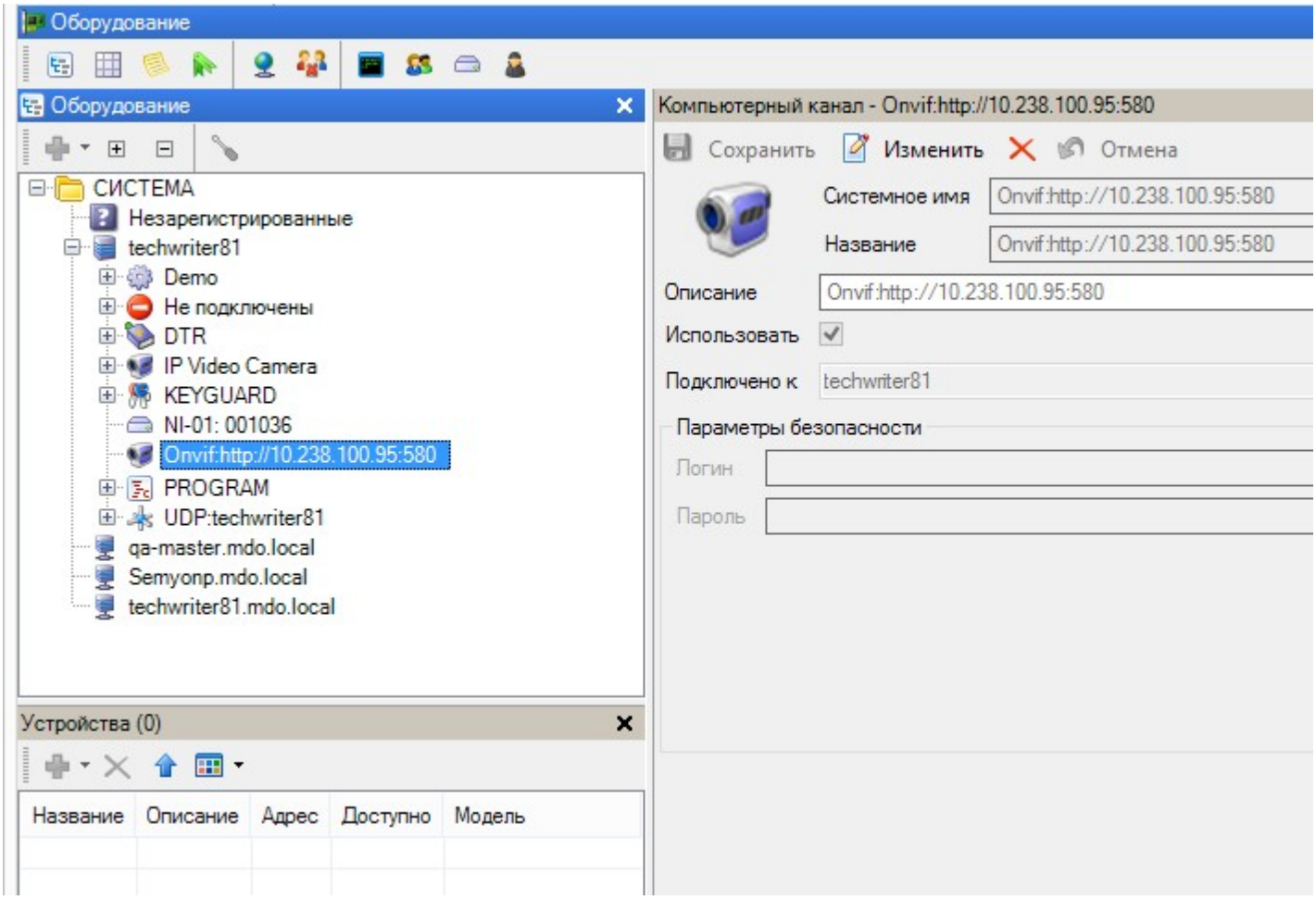
1. в контекстном меню рабочей станции Parsec (сервера или локального ПК) выберите команду "Поиск видеосистем";
2. в открывшемся окне введите IP-адрес ПК, на котором установлено ПО Milestone ONVIF Bridge (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования");



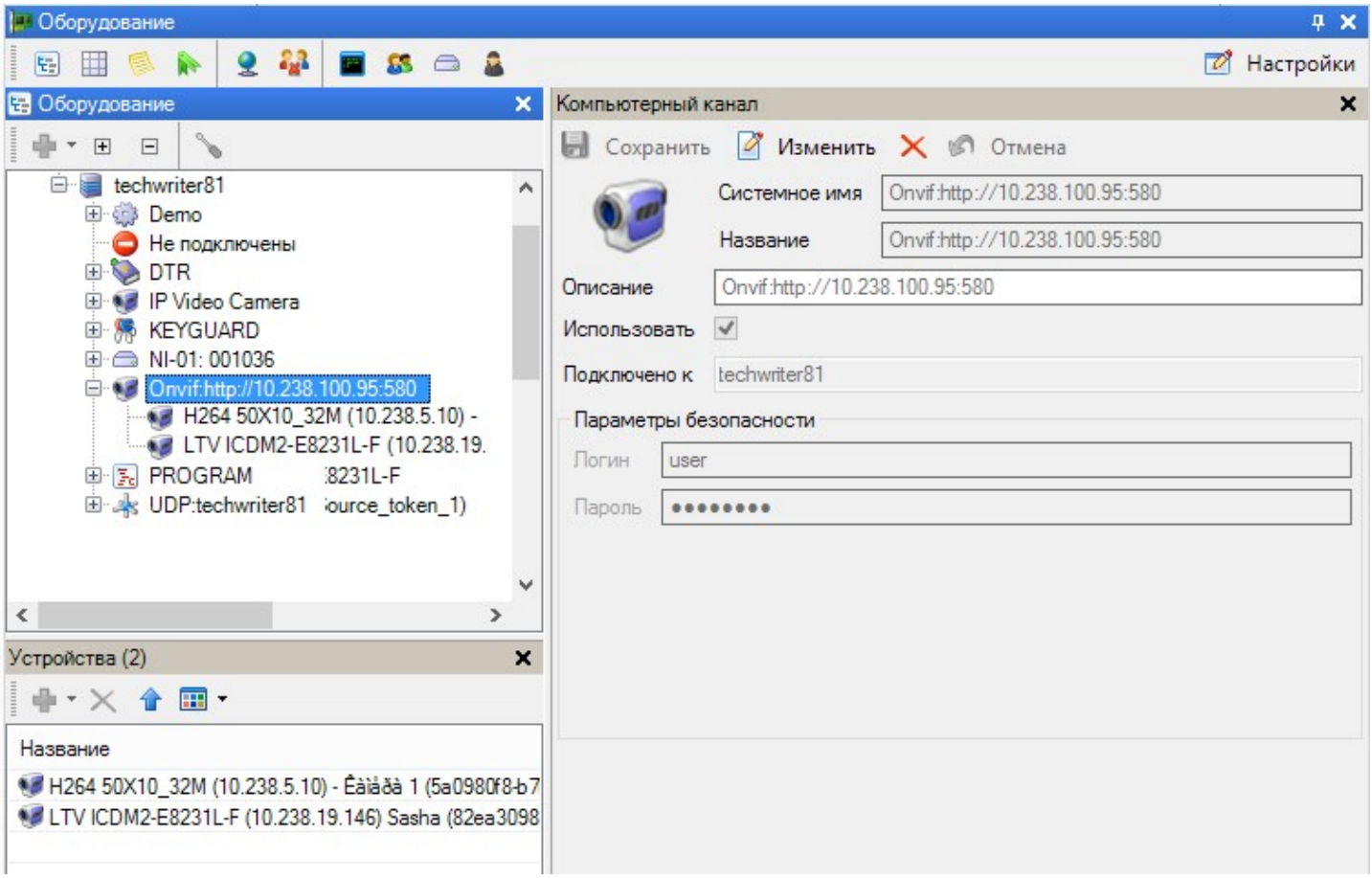
Если в системе не установлен сервер Milestone и, соответственно, нет ПО Milestone ONVIF Bridge, обнаружение ONVIF видеокамер и просмотр видеопотока с них все еще возможен в ПО системы ParsecNET 3. Для этого в окне поиска внешних устройств введите маску подсети 255.255.255.255. ParsecNET обнаружит все ONVIF видеокамеры в вашей подсети и отобразит их отдельными каналами на панели "Оборудование".

3. Нажмите на кнопку *ОК*.

   В списке оборудования должен появиться канал устройства, работающего по стандарту ONVIF. На рисунке ниже это канал сервера Milestone ONVIF Bridge "Onvif:http://10.238.100.95:580":



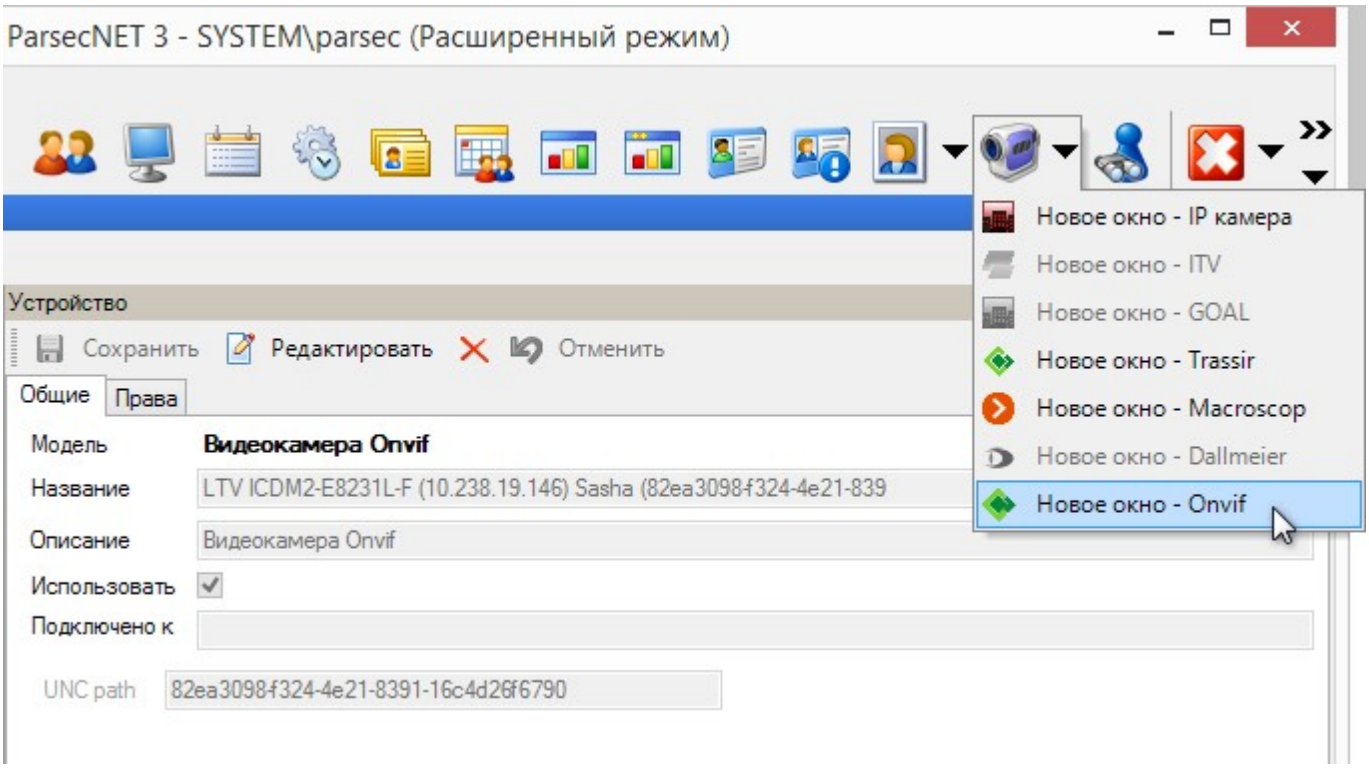
4. Выделите канал сервера, перейдите в режим редактирования и в блоке *Параметры безопасности* введите логин и пароль, [заданные](#)[544] в системе Milestone. Сохраните изменения.
5. Теперь проведите поиск оборудования на ONVIF-канале. Должны обнаружиться все камеры, подключенные к серверу Milestone ONVIF Bridge (в нашем примере это H264 и LTV):



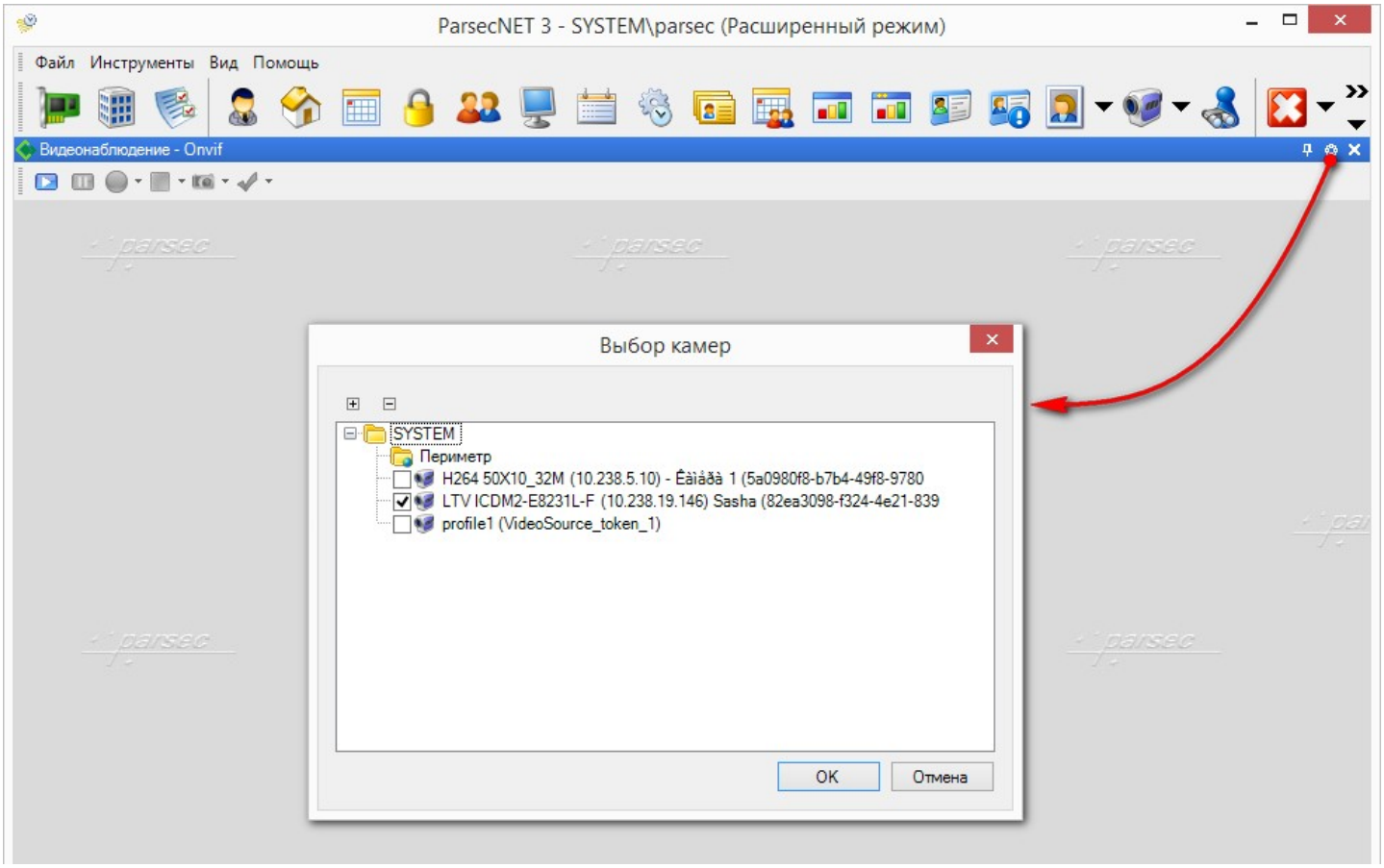
При использовании функции интеграции с Milestone, если в Milestone XProtect включена запись видеоархива, то её можно будет получить с сервера ONVIF Bridge и воспроизвести средствами ПО PNSoft (для камеры в Parsec будет доступна команда установки временной метки).

Если видеопоток от камеры ПО системы ParsecNET 3 получает напрямую, то возможности работы с видеозаписью данной камеры не будет.

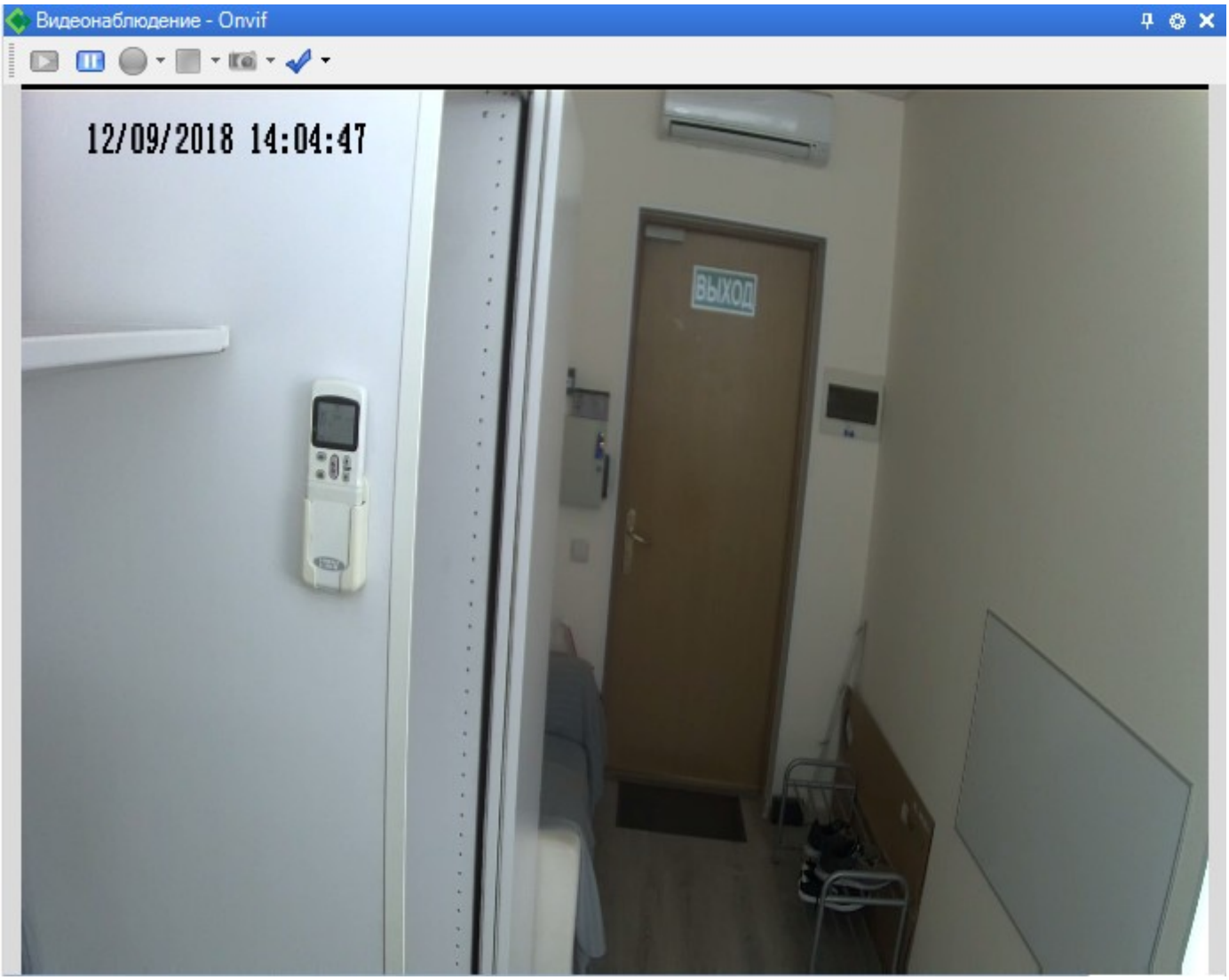
6. Добавьте новое окно видеонаблюдения Milestone:



7. В окне видеонаблюдения выберите камеру и нажмите на кнопку *OK*:



Теперь в этом окне будет отображаться видео с выбранной камеры, которое можно использовать для видеоидентификации, помечать кадр для последующего поиска в видеоархиве и т.п.:



Элементы интерфейса этого окна:

- включение/отключение фиксированного режима, при котором не отображается панель инструментов и невозможно изменить положение и размер окна видеонаблюдения(см. раздел Блокировка внешнего вида[54]);
- открывает окно выбора камер;
- показать изображение;
- остановить показ изображения;
- начать запись;
- остановить запись;
- сохранить кадр;
- установка временной метки на кадр.

Также такое окно можно открыть в Мониторе событий[287].

11.5.5.3 Плагин Access Control

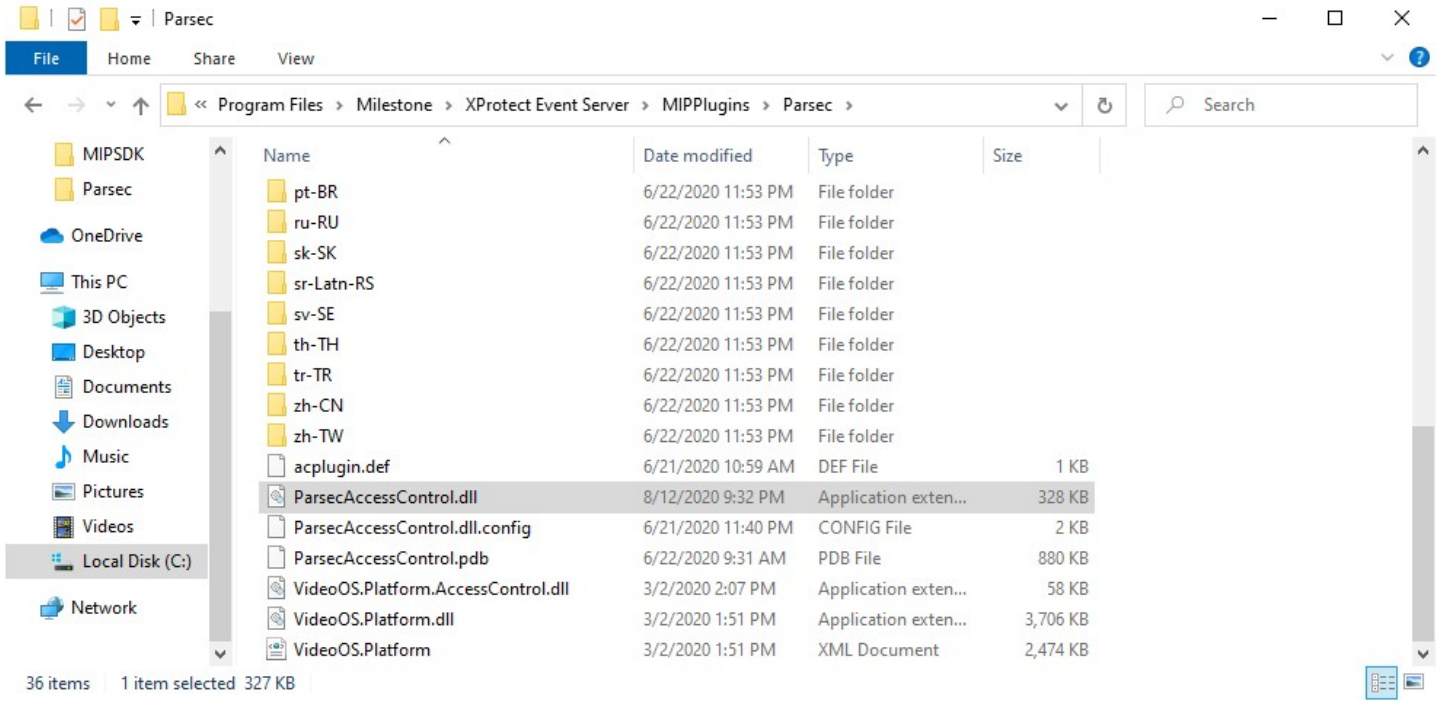
Этот раздел содержит инструкции по настройке взаимодействия ПО ParsecNET 3 и системы Milestone с помощью плагина Access Control.
Созданный разработчиками Parsec плагин Access Control для системы Milestone позволяет работать со СКУД ParsecNET 3 из приложения XProtect Smart Client, позволяет в реальном времени отслеживать события и вести наблюдение за точками прохода из пользовательского интерфейса системы Milestone.

Для корректного взаимодействия плагина и ПО Milestone необходимы:

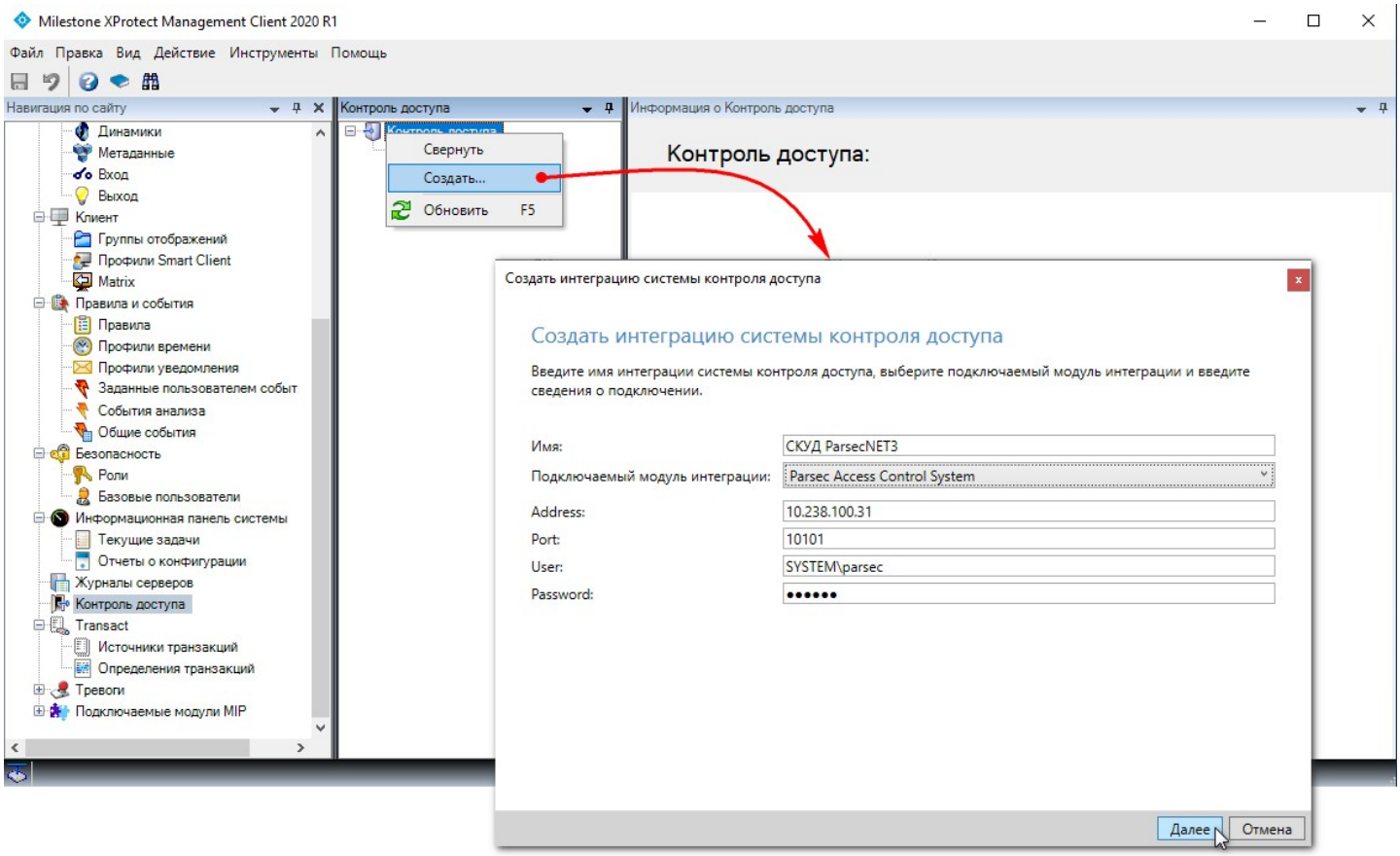
- установленное ПО ParsecNET 3 версии 3.10.325.23 или выше;
- лицензия для наблюдения за точками прохода, приобретенная у Milestone;
- установленное ПО Milestone XProtect - Management Client и Smart Client.

Для настройки взаимодействия выполните следующие шаги:

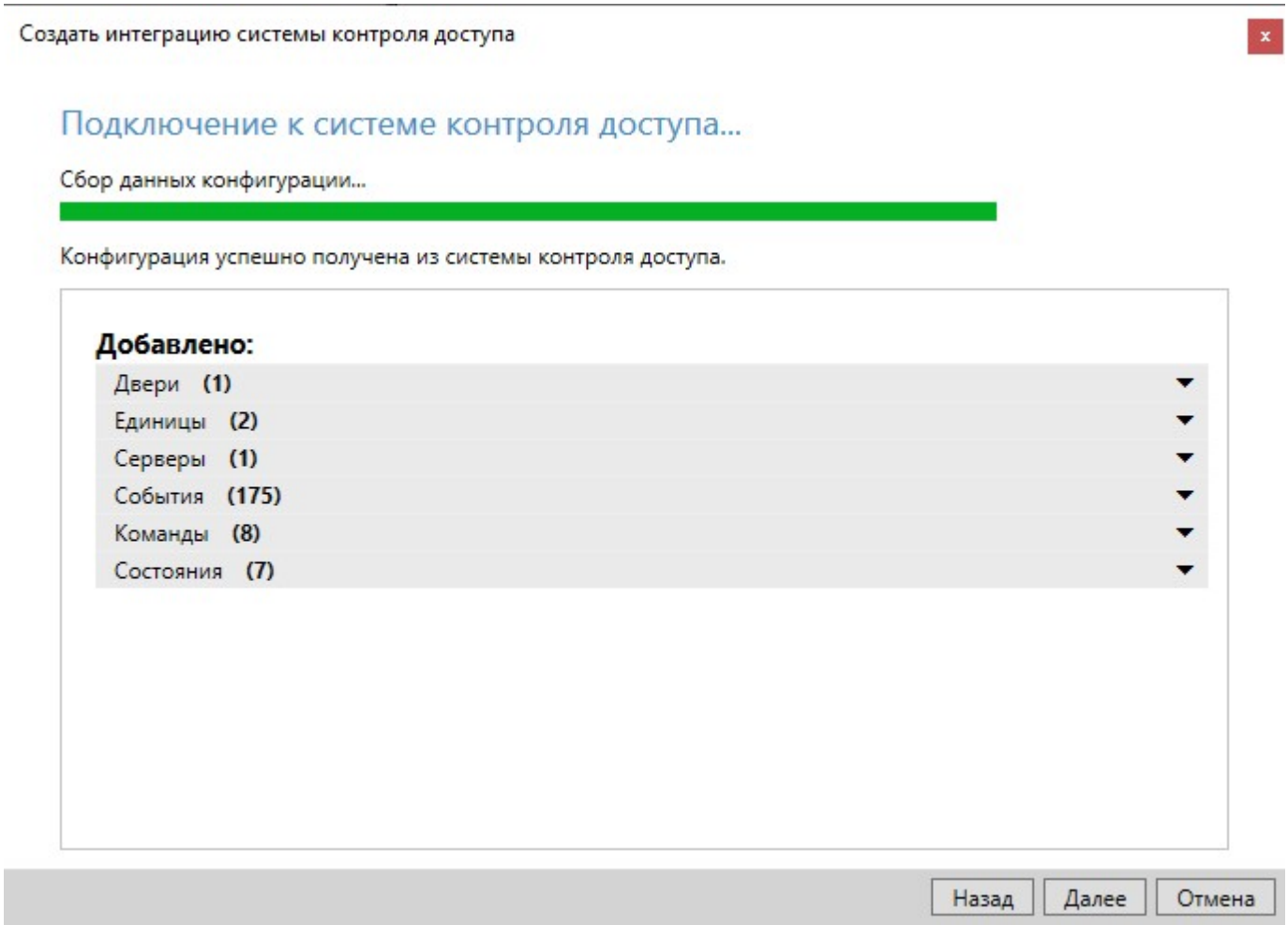
1. Скачайте архив с плагином для Milestone на сайте Parsec;
2. На ПК, где установлен сервер событий Xprotect Event Server, найдите папку для размещения плагинов от сторонних разработчиков (по умолчанию она находится по адресу C:\Program Files\Milestone\XProtect Event Server\MIPPlugins) и создайте в ней директорию Parsec;
3. Поместите содержимое полученного архива в созданную директорию:



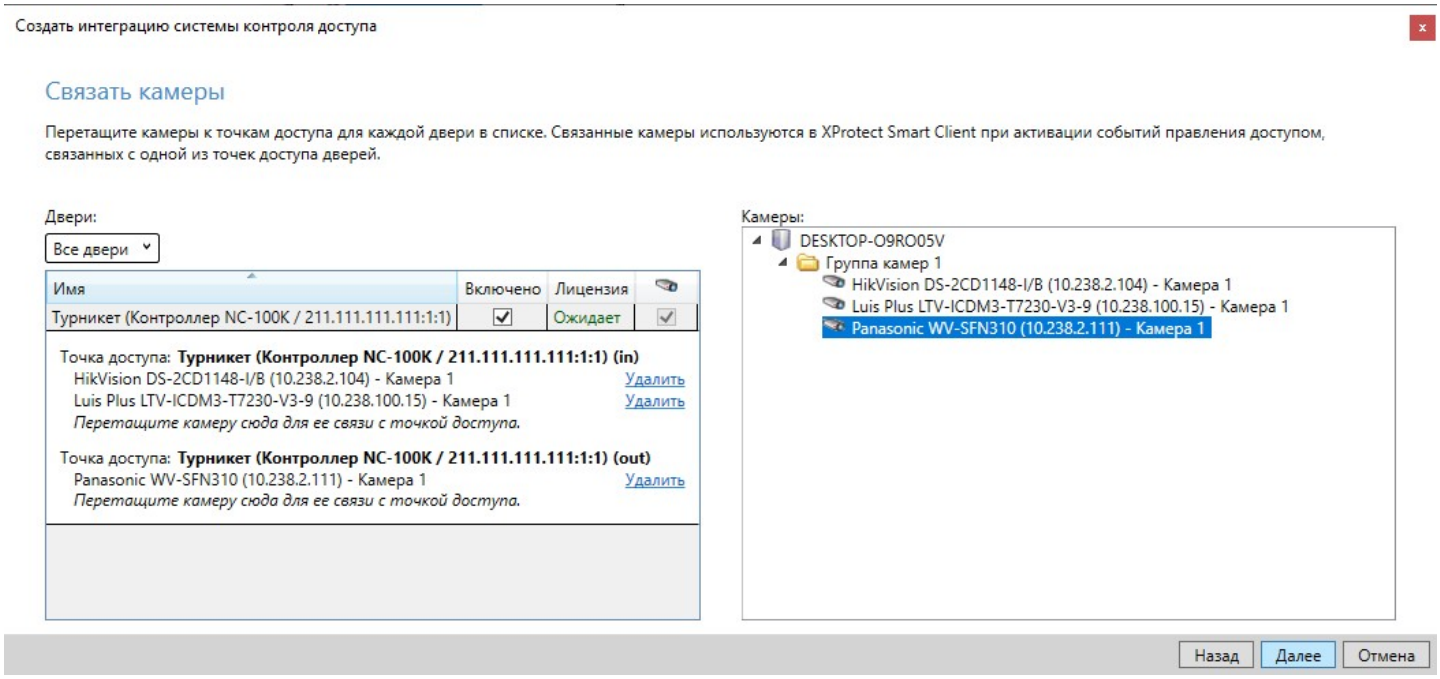
4. Перезапустите службы Milestone - XProtect Management Server и XProtect Event Server или перезагрузите свой ПК;
5. Запустите приложение XProtect Management Client и на левой панели *Навигация по сайту* выберите раздел *Контроль доступа*;
6. В контекстом меню раздела выберите команду "Создать...";
7. В открывшемся окне введите название для СКУД ParsecNET 3 (может быть произвольным);
8. Из раскрывающегося списка *Подключаемый модуль интеграции* выберите плагин "Parsec Access Control System";
9. В поле *Address* укажите адрес сервера Parsec;
10. Значение в поле *Port* оставьте по умолчанию (здесь указывается номер TCP-порта действующего сервера СКУД ParsecNET 3, по которому работает сервис интеграции Parsec);
11. Введите логин и пароль пользователя ParsecNET 3, имеющего права на просмотр территорий и точек прохода, которые необходимо отслеживать посредством данного плагина:



12. Нажмите на кнопку *Далее* . Система Milestone соберет сведения о конфигурации СКУД ParsecNET 3 и выведет их в окне:

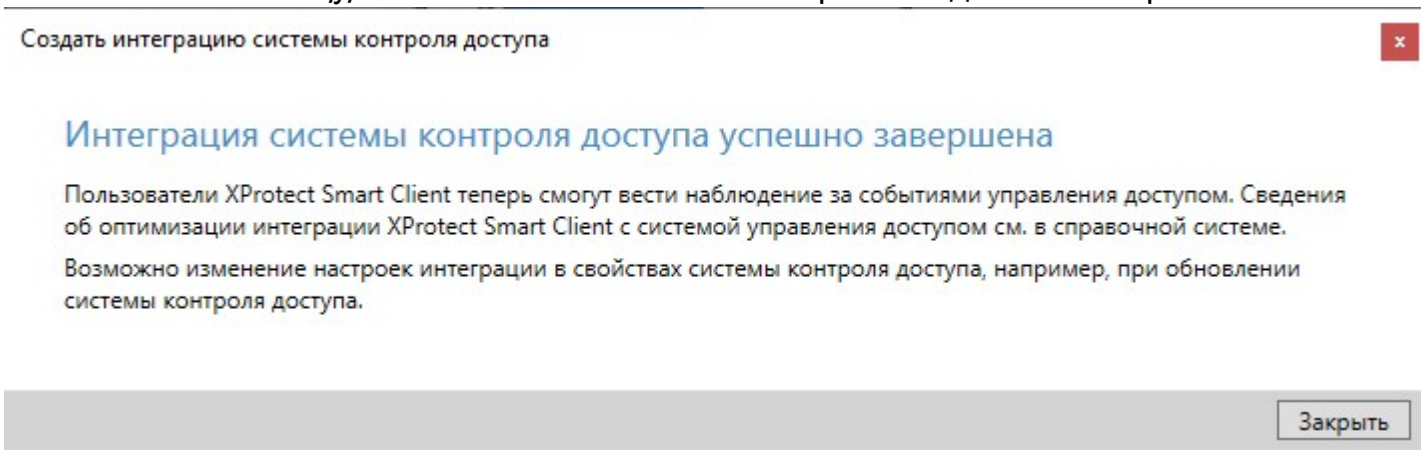


13. Нажмите на кнопку *Далее* . Откроется окно для связи камер с точками прохода:



Перетащите камеру из списка камер на точку прохода так, чтобы направление обзора камеры соответствовало желаемому направлению прохода.
На примере выше видно, что камеры HikVision и Lois Plus LTV направлены на вход через турникет. А камера Panasonic направлена на выход через этот турникет;

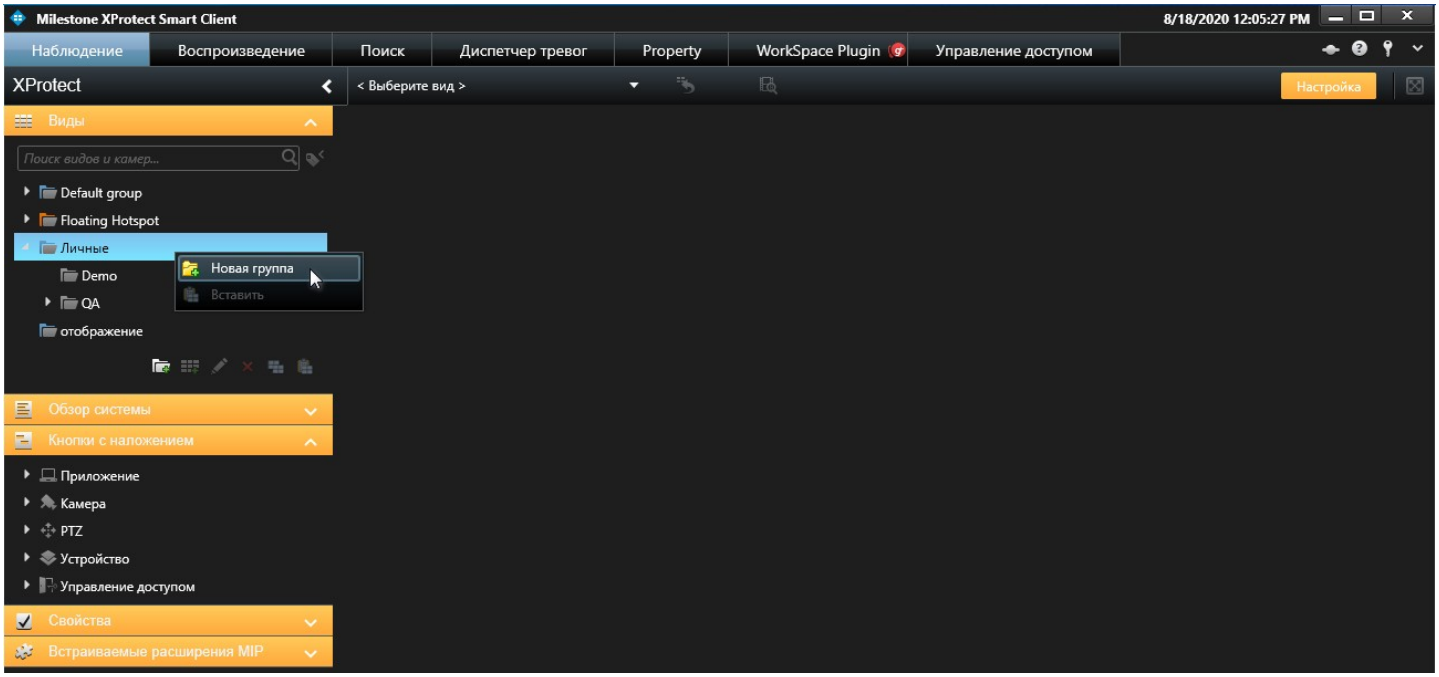
14. Нажмите на кнопку *Далее* . Система Milestone сохранит заданные настройки:



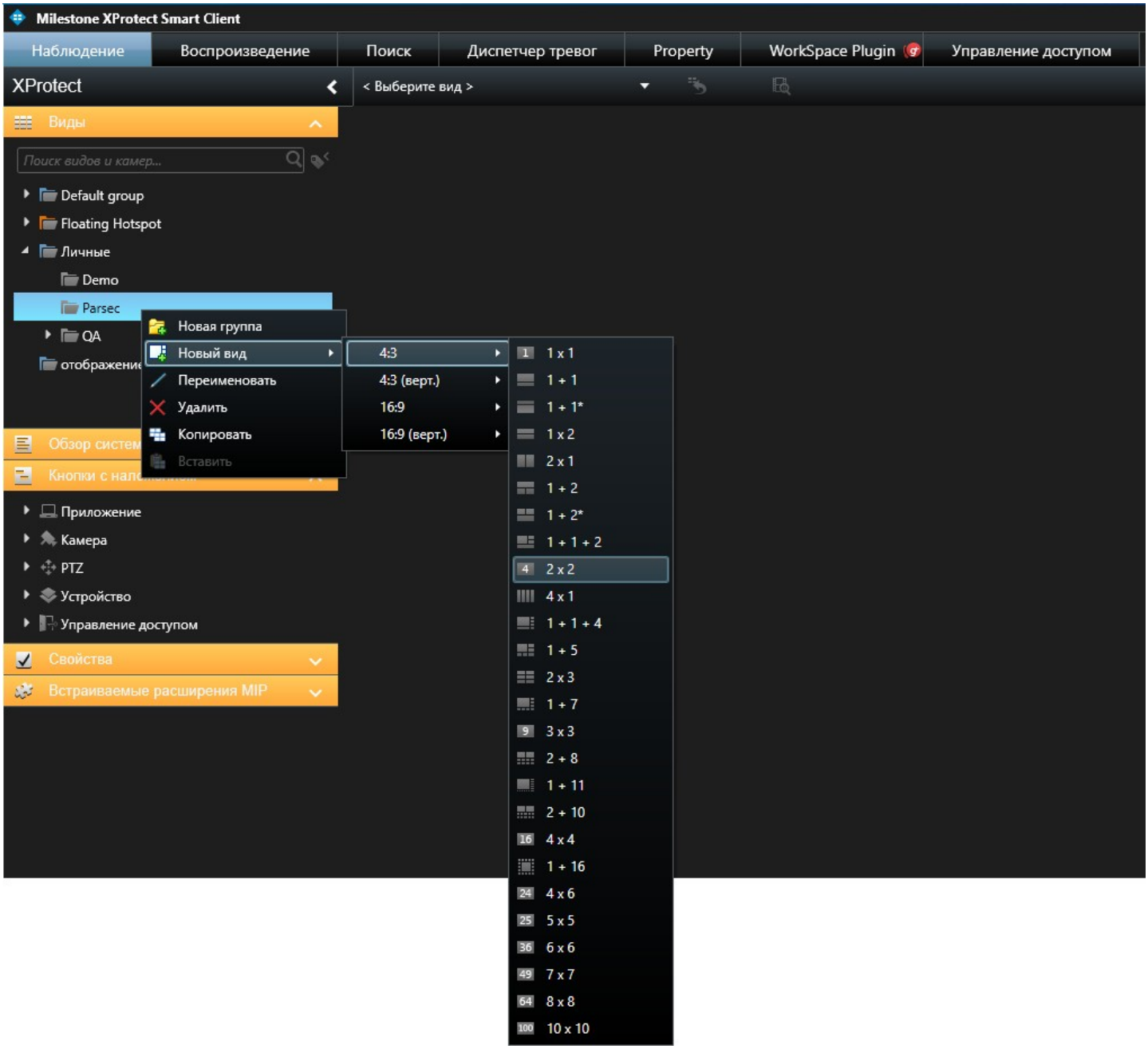
На этом настройка плагина завершена.

Дальнейшая работа с плагином производится в программе XProtect Smart Client. Подробности работы с программой описаны в ее Руководстве по эксплуатации (справке). Ниже приведено краткое описание основных шагов по настройке и работе со СКУД Parsec при помощи XProtect Smart Client.

Запустите программу и перейдите в режим настроек, нажав на кнопку *Наст ройки* . Желтым цветом подсветятся доступные для изменений параметры.
В контекстном меню группы Личные выберите команду *Новая группа* и создайте группу для СКУД ParsecNET 3:

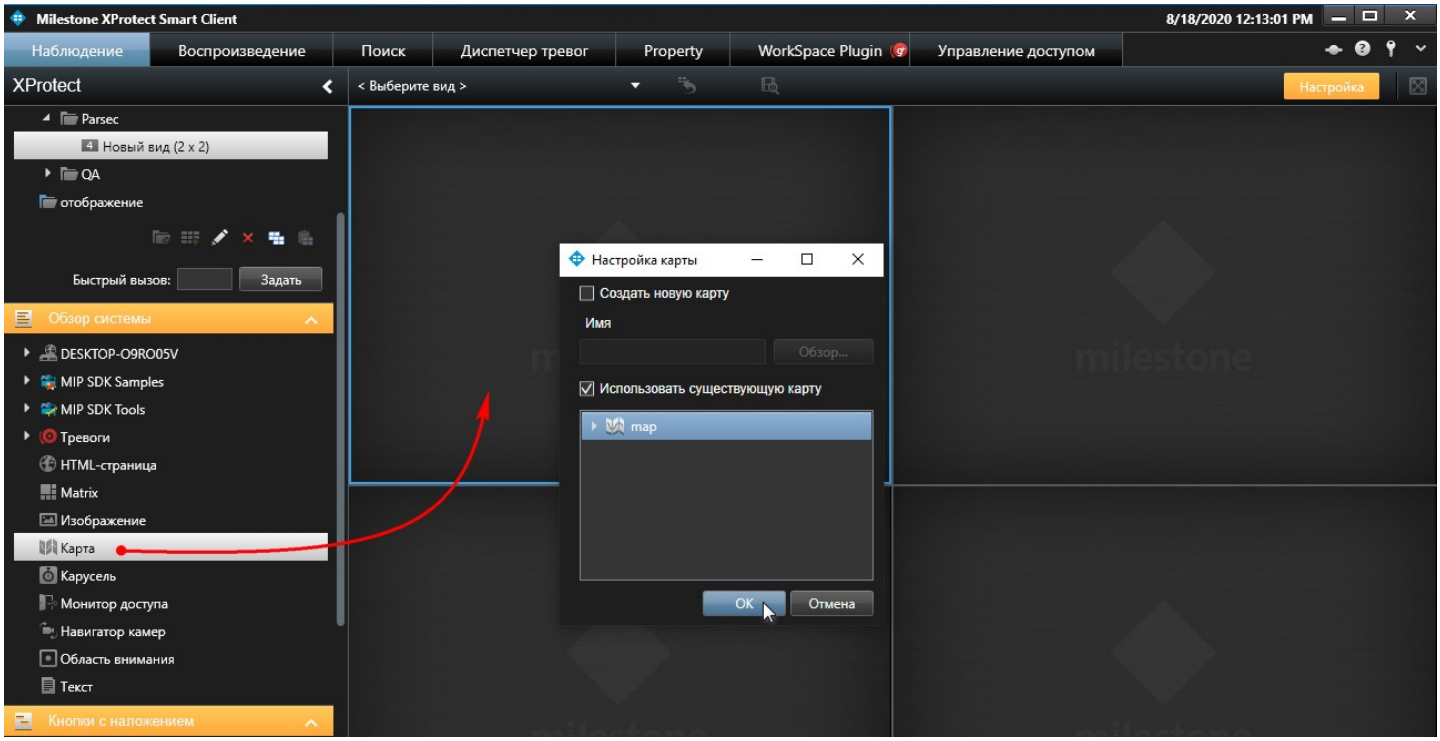


В контекстном меню созданной группы *Parsec* выделите команду *Новый вид* и выберите количество строк и колонок для отображения:

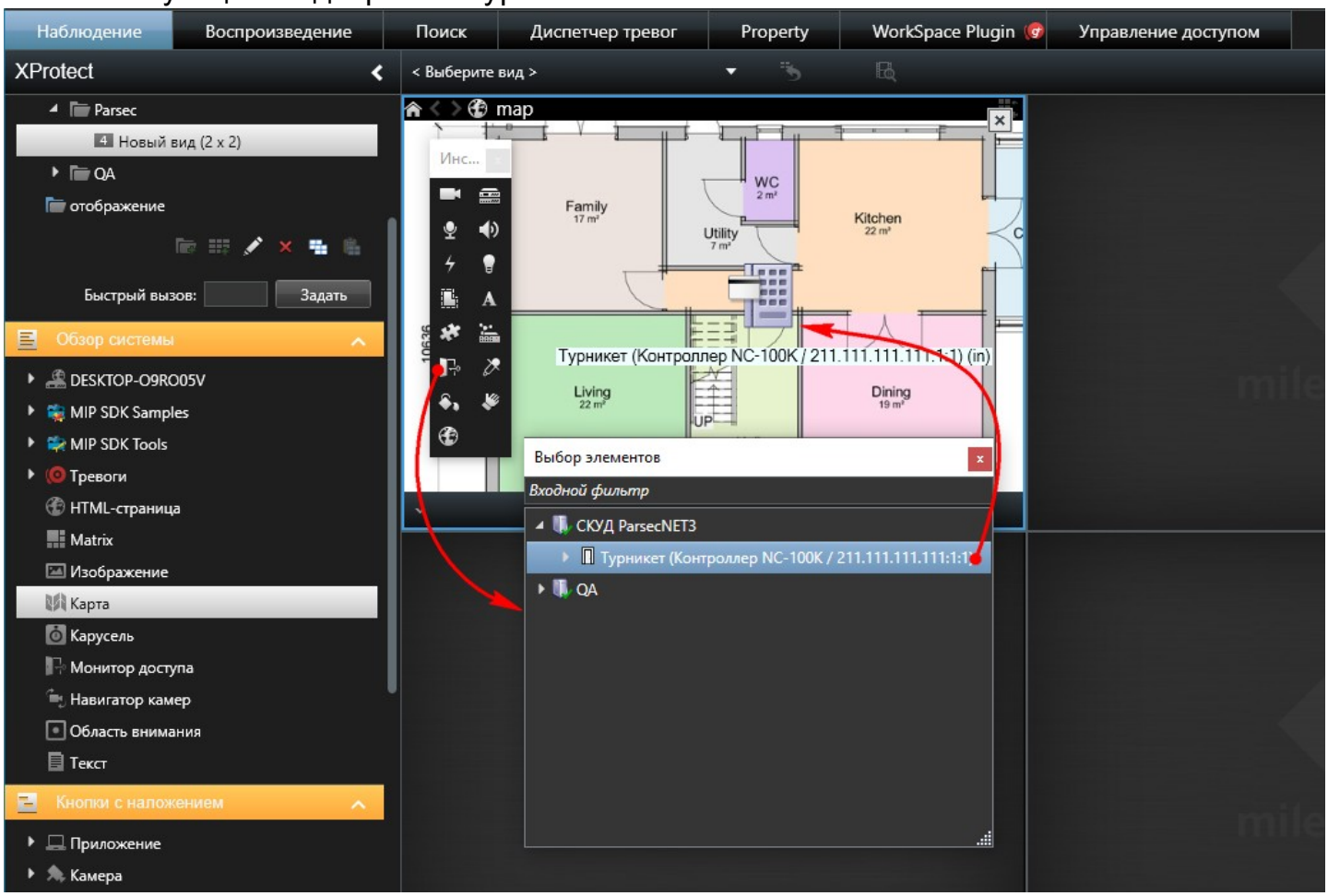


В окнах вида можно отображать план территории или помещения, либо изображение с камеры.

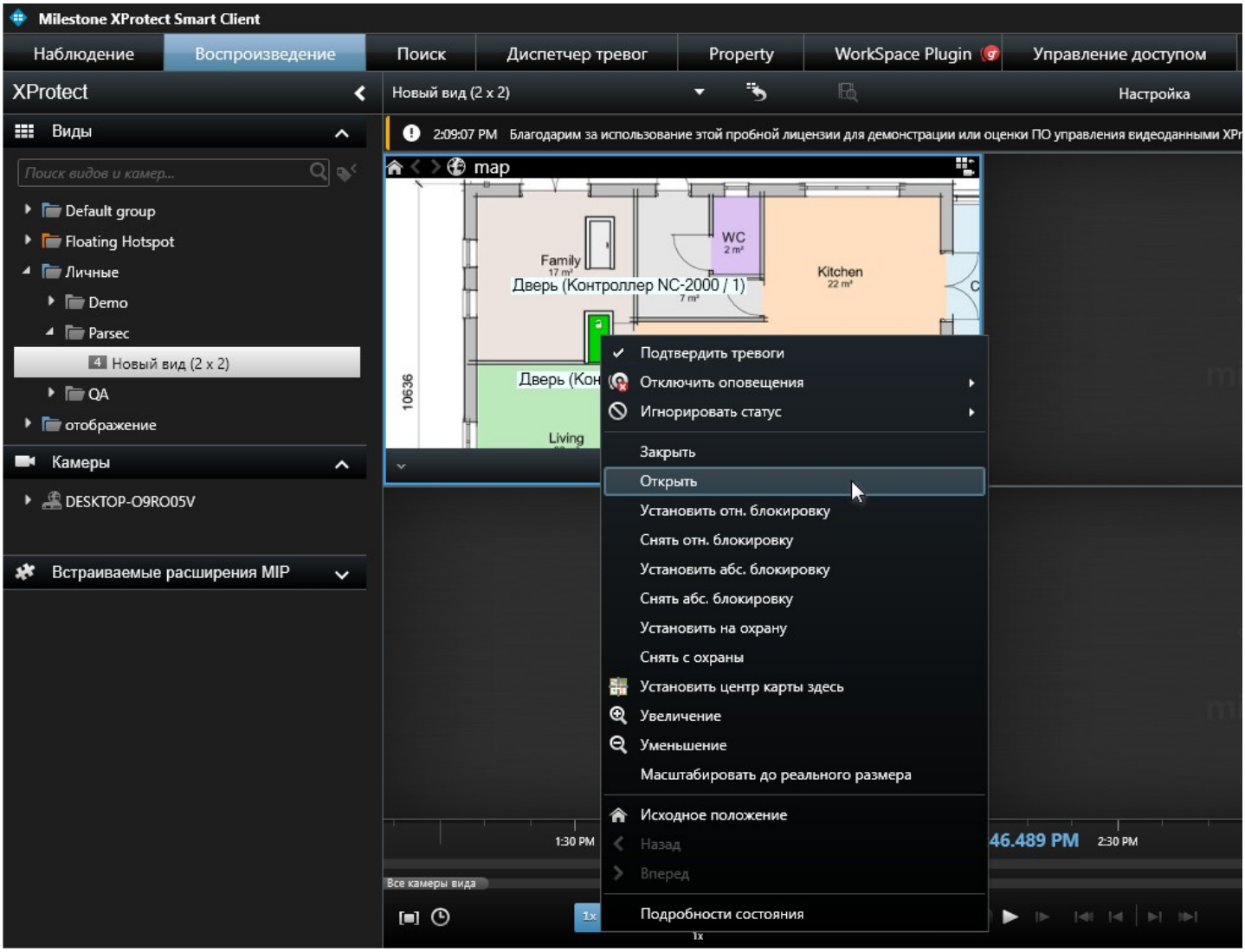
Из раздела *Обзор системы* перетащите строку *Карта* в одно из окон. В открывшемся окне выделите файл существующей карты или укажите путь к файлу карты. Файл, конечно же, должен быть подготовлен заранее. После нажатия на кнопку *OK* в окне появится топология выбранной Вами территории.



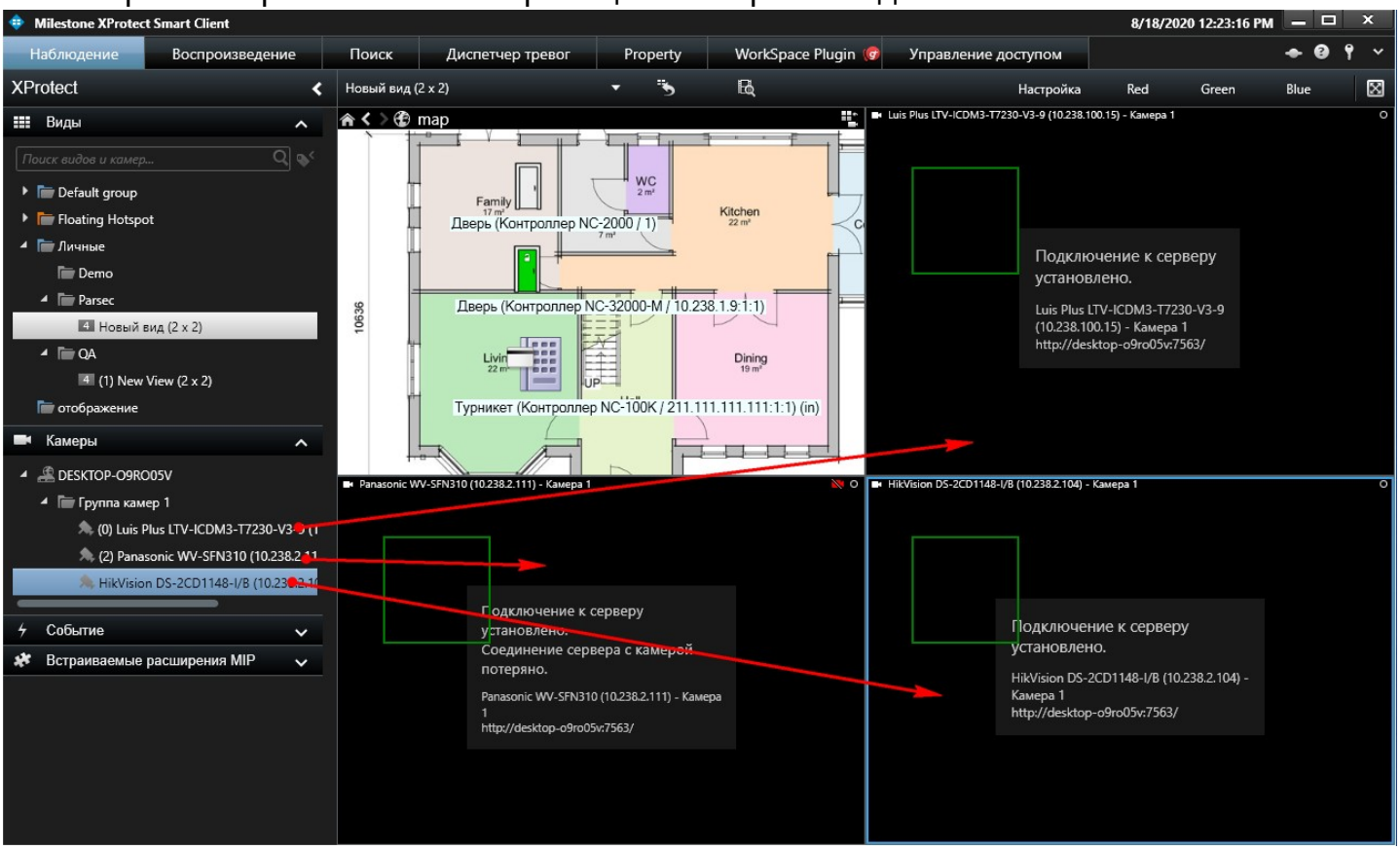
В режиме настройки на карте отображается панель инструментов. Нажмите на кнопку Управление доступом, выберите группу своей СКУД и перетяните на план территории, соответствующие ей двери или турникеты:



Выйдите из режима настройки, еще раз нажав на кнопку *Настройки*. Желтая подсветка пропадет. В этом режиме можно напрямую управлять дверьми и турникетами:



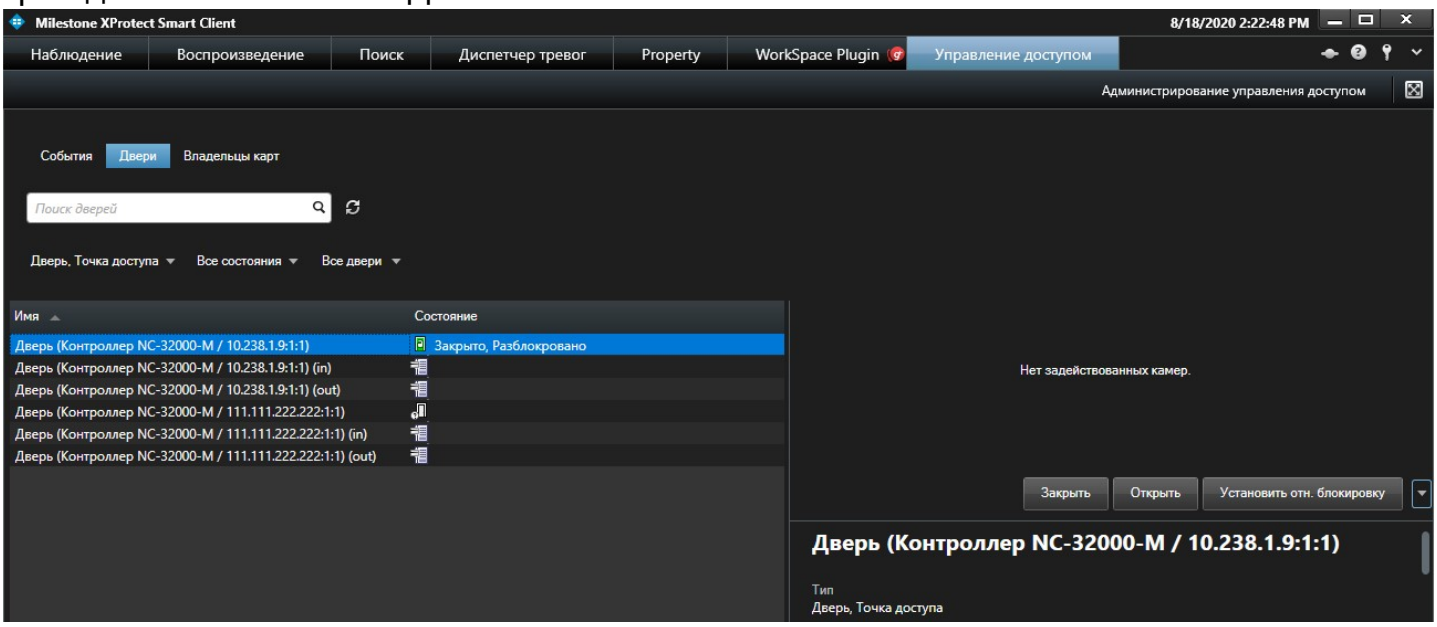
Также в рабочем режиме можно перетащить камеры по отдельным окнам:



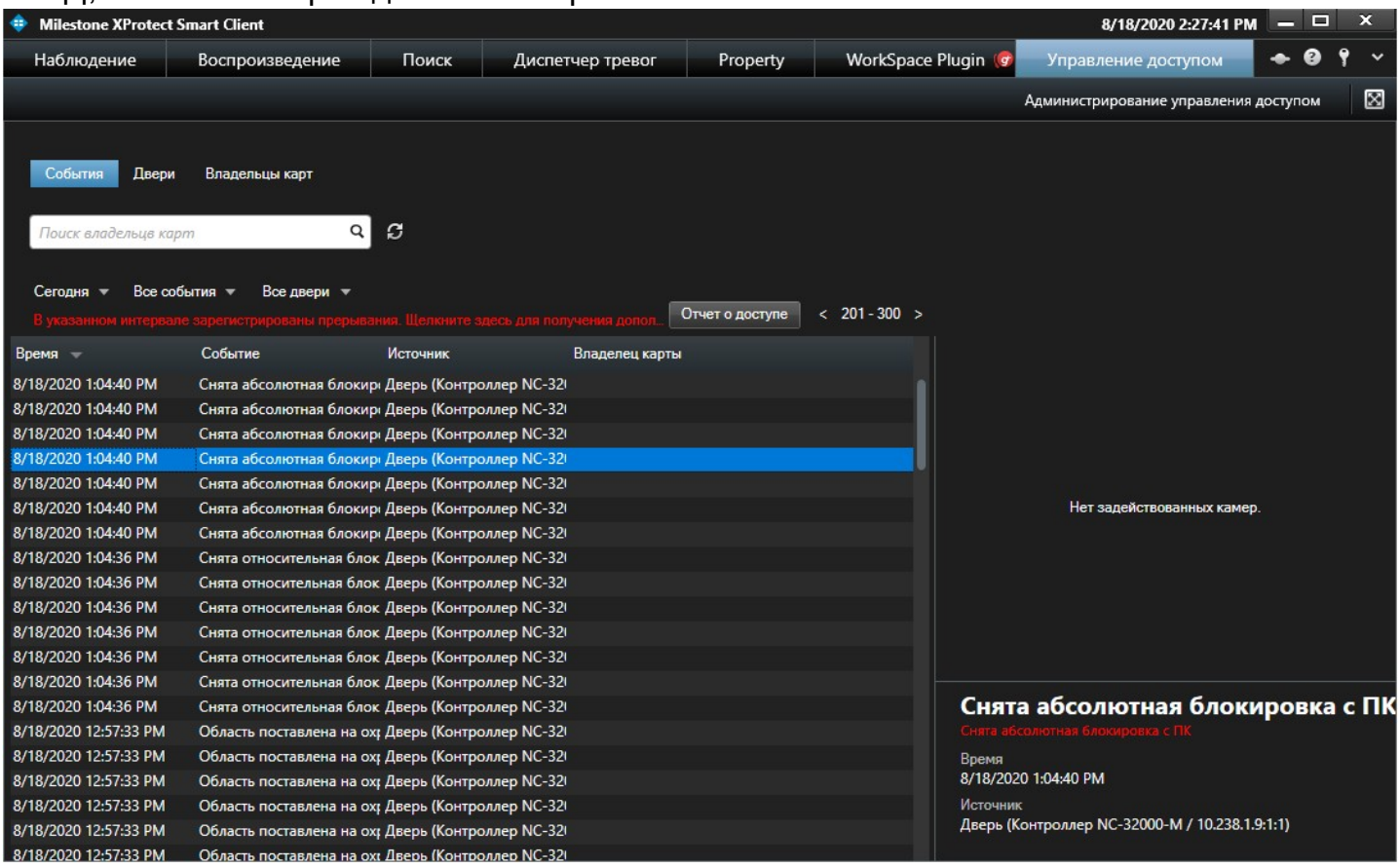
Вкладка "Управление доступом"

На вкладке *Управление доступом* отображаются компоненты точек прохода, события и держатели карт.

В разделе *Двери* из раскрывающихся списков можно выбрать компоненты для отображения, конкретизировать, какие состояния будут отображаться и элементы точек прохода тех или иных СКУД:



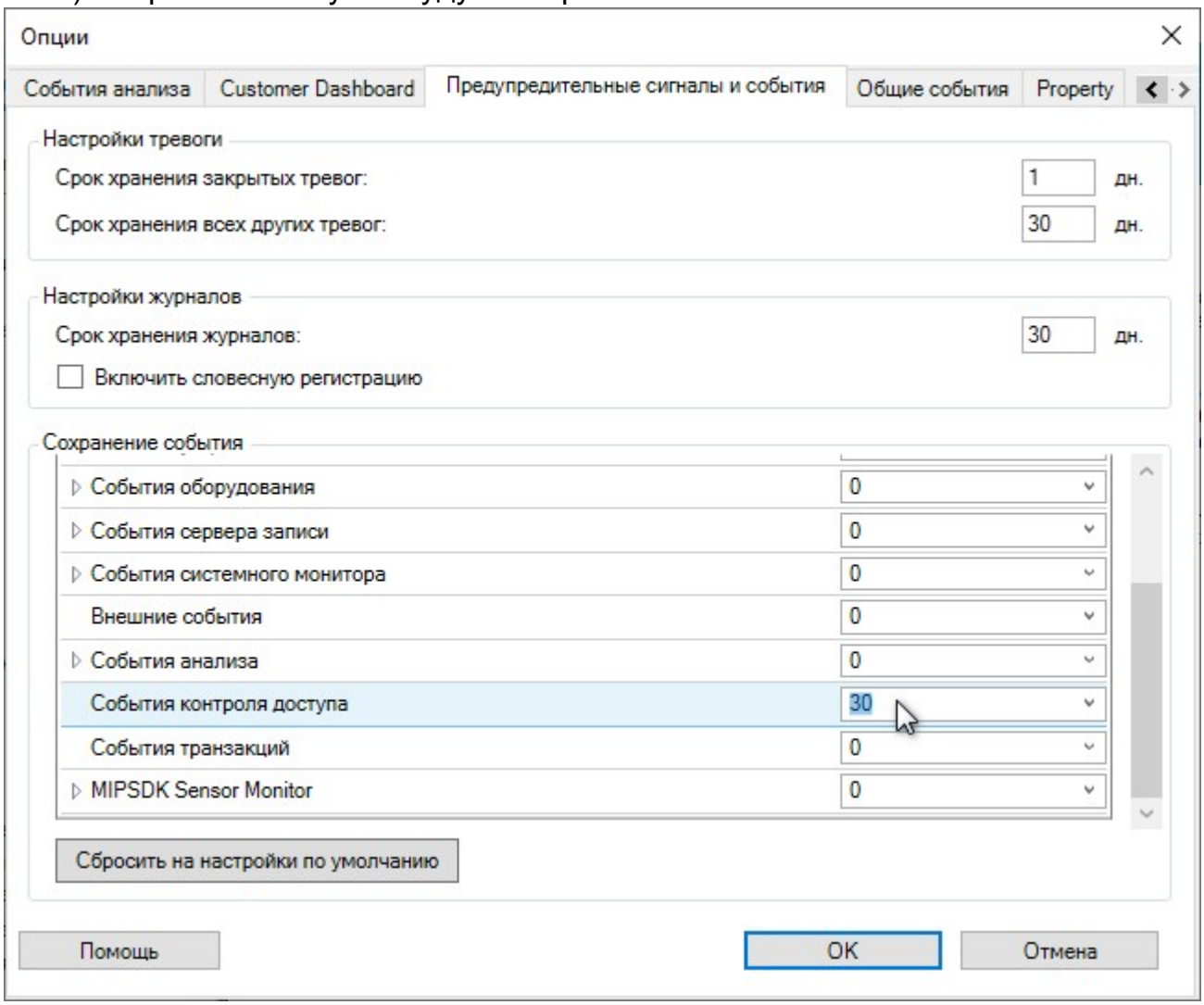
В разделе *События* можно настроить временной период, категорию события и компоненты СКУД, события которых должны отображаться.



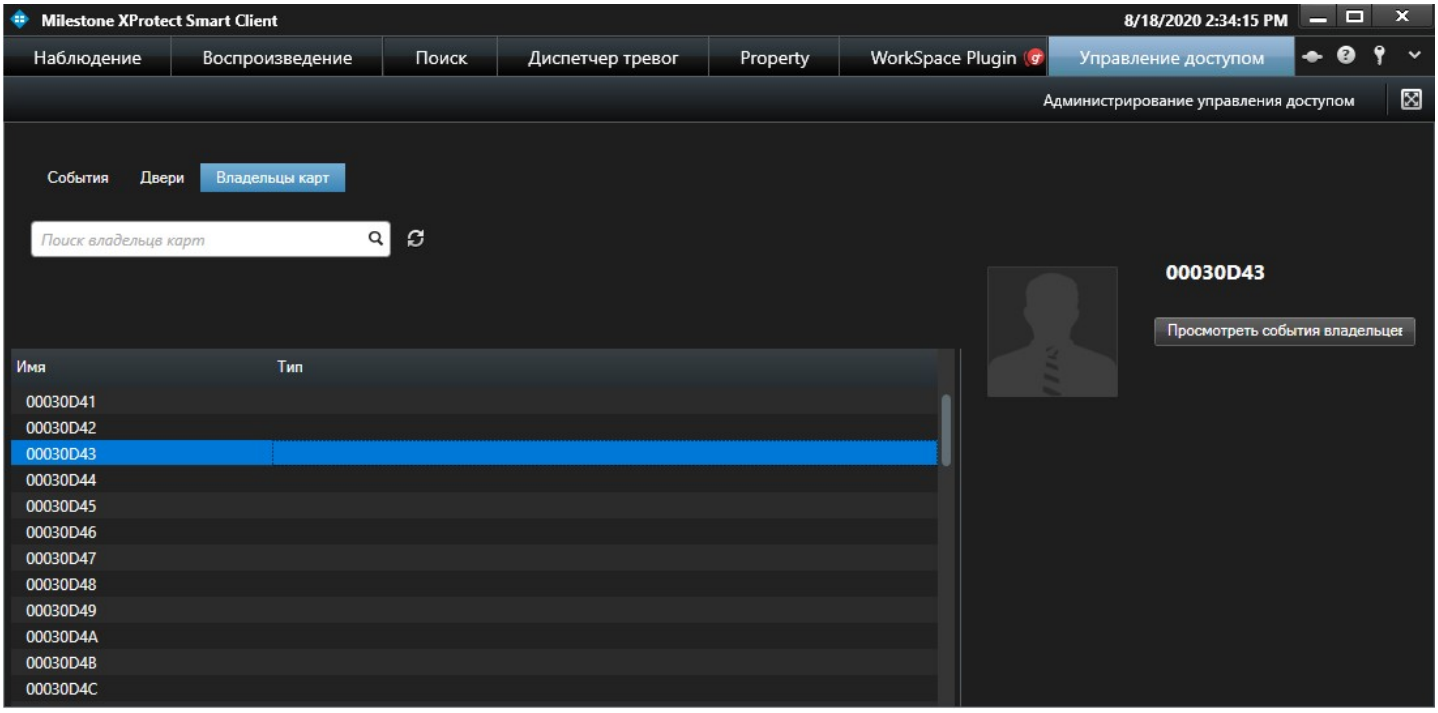
В случае, когда интервал отображения событий выбран иной, нежели *Автоматическое обновление*, необходимо указать срок, который события будут храниться в БД Milestone.

Для этого запустите XProtect Management Client, перейдите в раздел *Инструменты - Опции* *Предупредительные сигналы и события*. В списке настроек *Сохранение*

событ ия установите для параметра *Событ ия конт роля дост упа* значение, отличное от установленного по умолчанию 0. Например, если в Smart Client установлен пользовательский интервал отображение событий в 30 дней, то в опциях Management Client срок хранения события контроля доступа также не должен быть меньше 30 дней (рисунок ниже). В противном случае будут отображаться не все события.



В разделе *Владельцы карт* можно просмотреть полный список пользователей СКУД, найти конкретного пользователя и просмотреть связанные с ним события.



11.5.6 Система Panasonic Video Insight

В этом разделе описывается взаимодействие видеосистемы Video Insight производства Panasonic и СКУД ParsecNET 3.

На текущий момент СКУД была протестирована и показала надежную работу с ПО Video Insight версий 7.3.0.127 и 7.4.2.32

Данный раздел не является руководством по использованию системы Video Insight, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы Video Insight обратитесь к оригинальному руководству.

Работа с видеосистемой состоит из следующих принципиальных шагов:

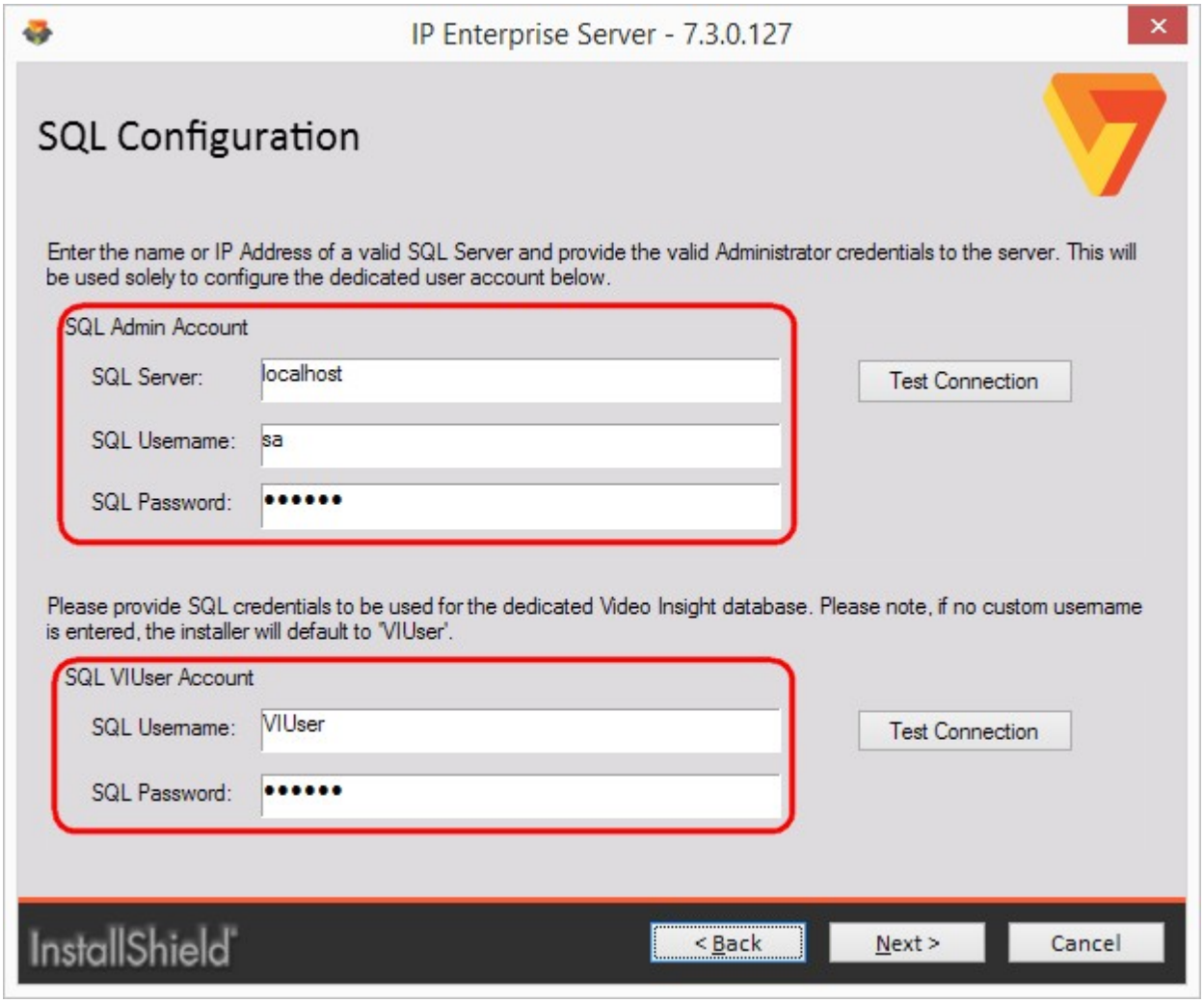
1. Установка сервера системы[559] Video Insight и добавление в нее видеокамер;
2. Установка приложения API на том же ПК, где установлен сервер системы Video Insight;
3. Поиск сервера видеосистемы[562] средствами ParsecNET;
4. Поиск камер, подключенных к серверу видеосистемы;
5. Настройка окна (окон) видеонаблюдения для системы Video Insight.

11.5.6.1 Подключение и настройка

1. Установите необходимое ПО системы Video Insight с дистрибутивного носителя, следуя подсказкам мастера установки (при необходимости обратитесь к документации Video Insight).

   Настоятельно рекомендуется ставить сервер системы Video Insight на отдельный ПК с достаточным объемом памяти для хранения видеозаписей.

   При установке потребуется задать параметры для учетных записей Администратора SQL (SQL Admin Account) и Пользователя SQL (SQL VIUser Account), запомните их, они потребуются позднее:



Проведите тесты соединений, при необходимости устраните ошибки.

После установки на ПК появится приложение VI Monitor Plus;

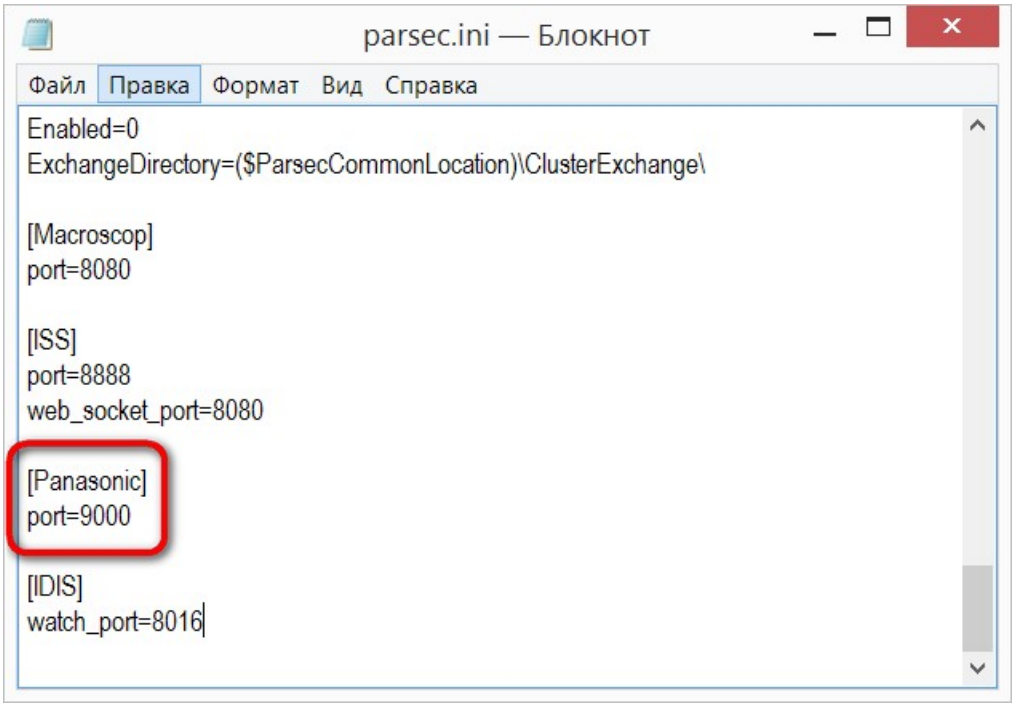
2. После установки сервера видеосистемы установите приложение InsightAPI v.1.0.25.1 (с другими версиями интеграция не тестировалась). Получить приложение можно по запросу на сайте https://security.panasonic.ru/, нажмите на кнопку *Скачать* и выберите *Программное обеспечение Video Insight*. Для корректной установки приложения потребуются учетные данные SQL Admin Account.
3. Запустите приложение VI Monitor Plus:



В этом приложении добавьте и настройте камеры.

Для входа по умолчанию используется имя пользователя Administrator, пароль - пустое поле. Их можно изменить в настройках Administration - Servers - Setup and Configuration. Эти же имя пользователя и пароль будет необходимо ввести в ПО ParsecNET 3.

Если при настройке был изменен порт по умолчанию, то его необходимо обязательно изменить и в файле настройки ParsecNET *parsec.ini*, находящемся по умолчанию по адресу *C:\ProgramData\MDO\ParsecNET 3*:

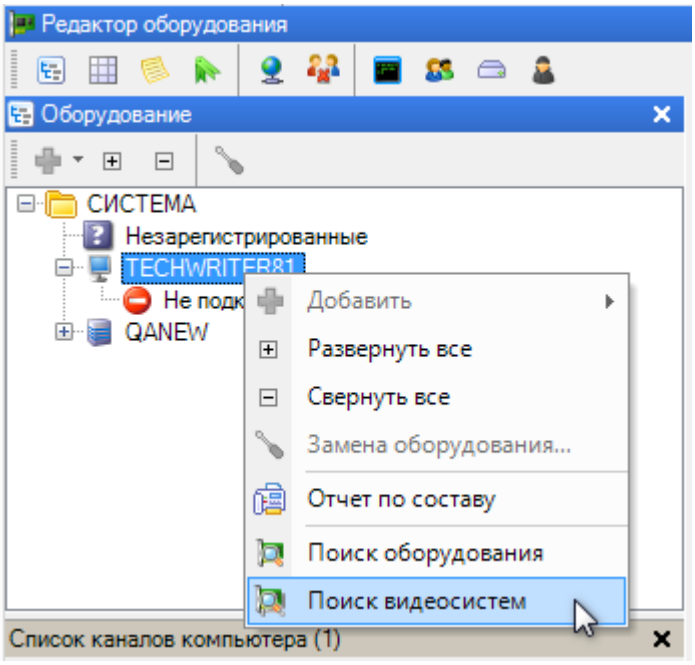


Теперь СКУД ParsecNET 3 готов работать с системой Video Insight.

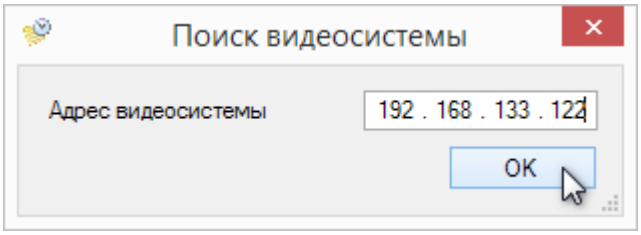
11.5.6.2 Использование системы

После того как система Video Insight и приложение InsightAPI установлены, к видеосистеме добавлены и настроены камеры, ее можно использовать в рамках СКУД ParsecNET 3. Для этого выполните следующие шаги:

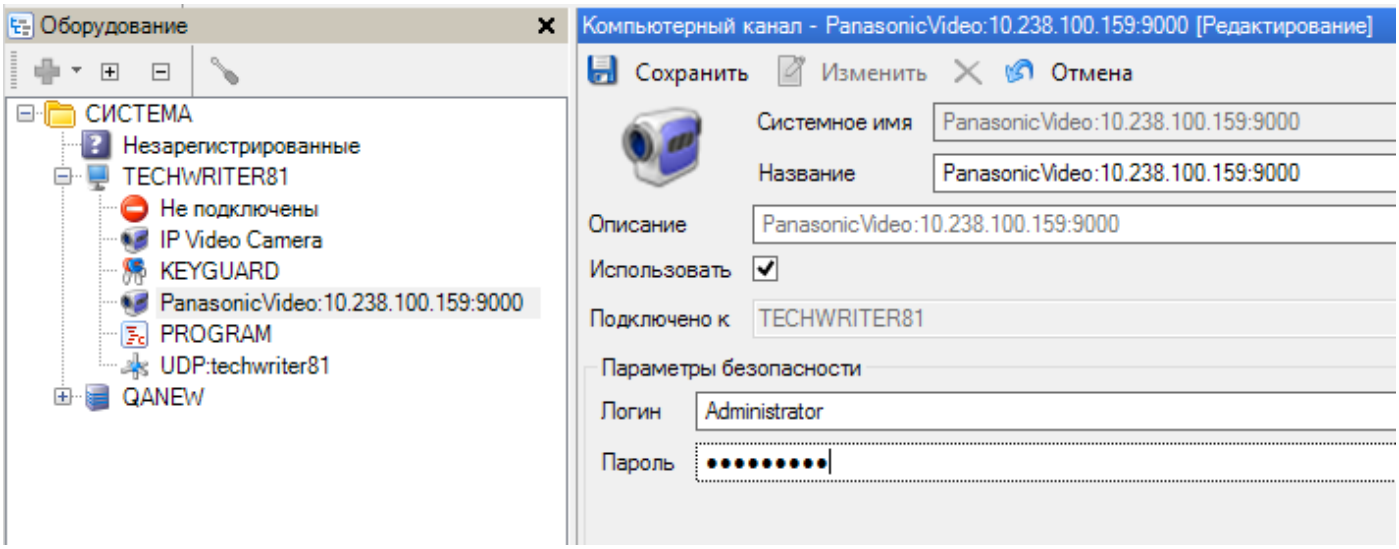
1. Запустите консоль "Администрирование" ParsecNET 3 на ПК и в контекстном меню рабочей станции Parsec (сервера или локального ПК) выберите "Поиск видеосистем":



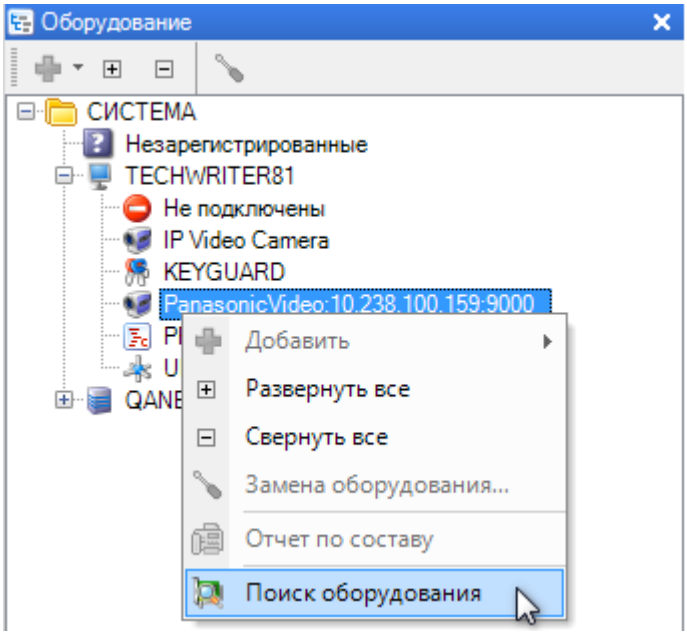
2. В открывшемся окне введите IP-адрес ПК, на котором установлен сервер видеосистемы (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования") и нажмите на кнопку *ОК*:



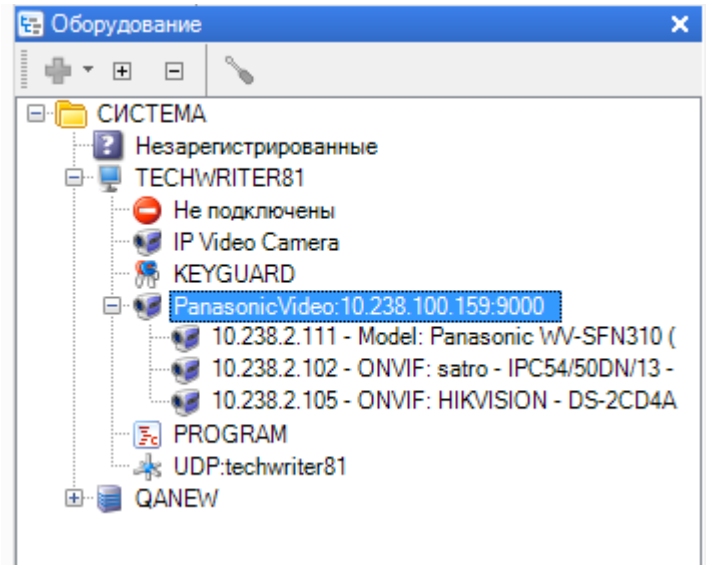
3. После того, как канал сервера системы Video Insight будет обнаружен, необходимо обнаружить подключенные к серверу видеосистемы камеры. Но для этого сначала необходимо ввести логин и пароль для доступа к VI Monitor Plus[559] :



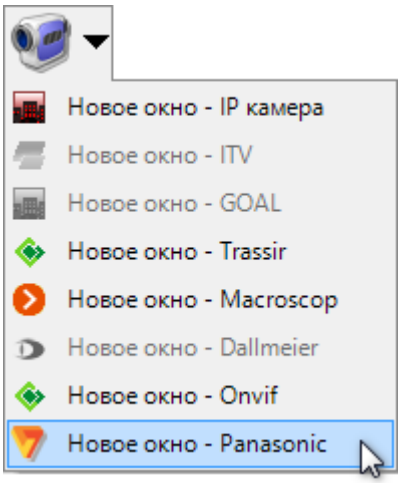
4. Проведите на канале видеосистемы поиск оборудования:



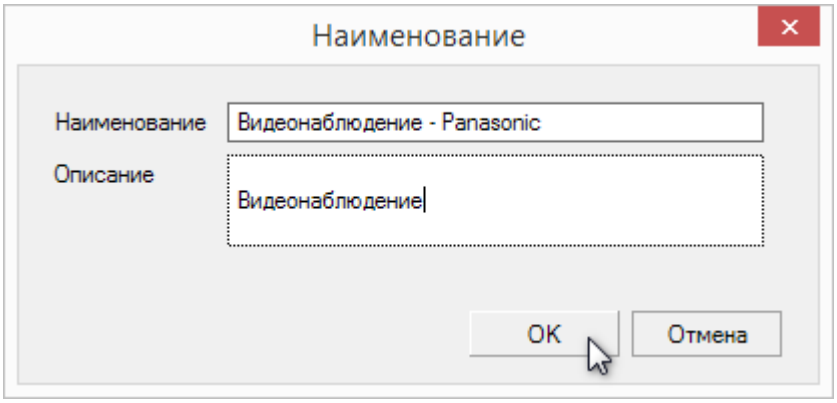
Подключенные к серверу видеосистемы камеры отобразятся в Редакторе оборудования:



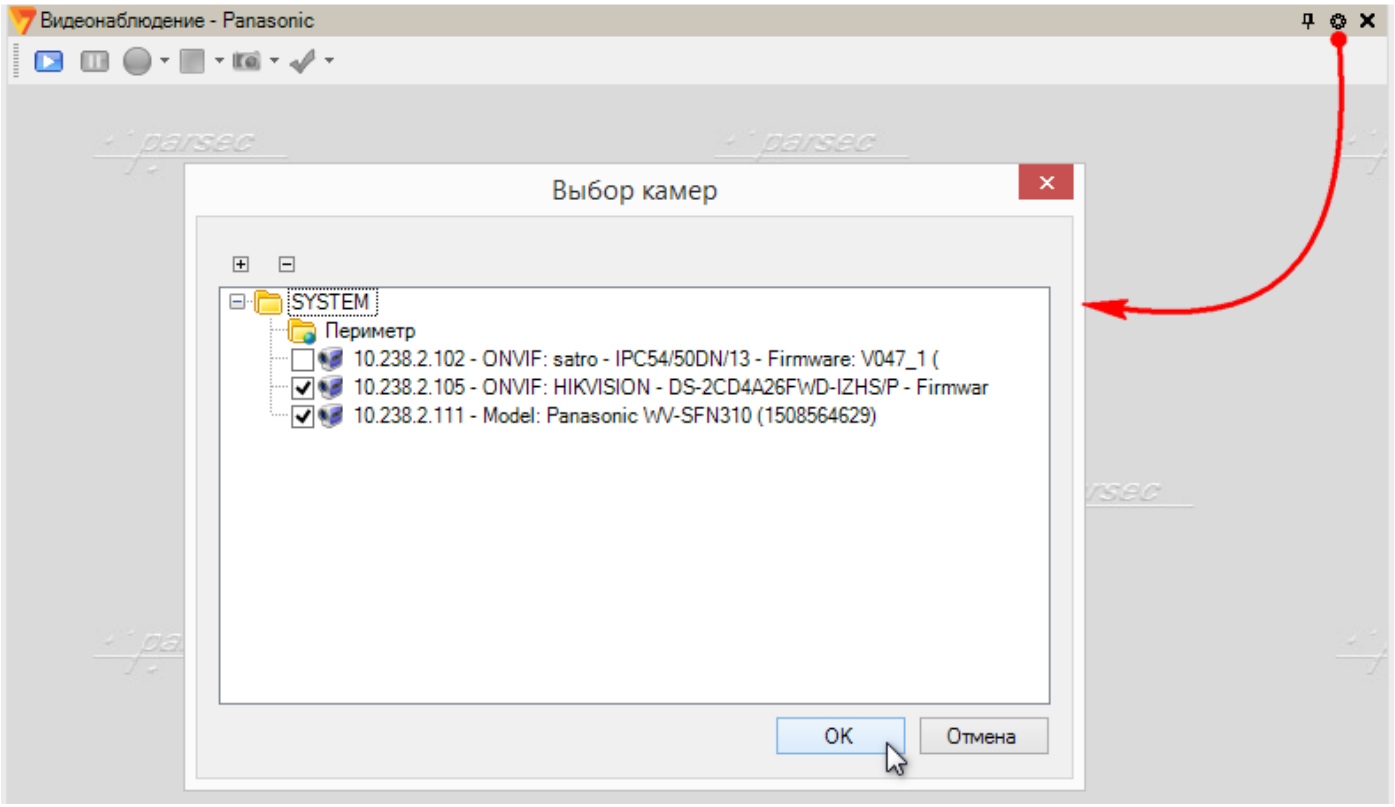
5. В раскрывающемся списке *Видеонаблюдение* выберите команду "Новое окно - Panasonic":



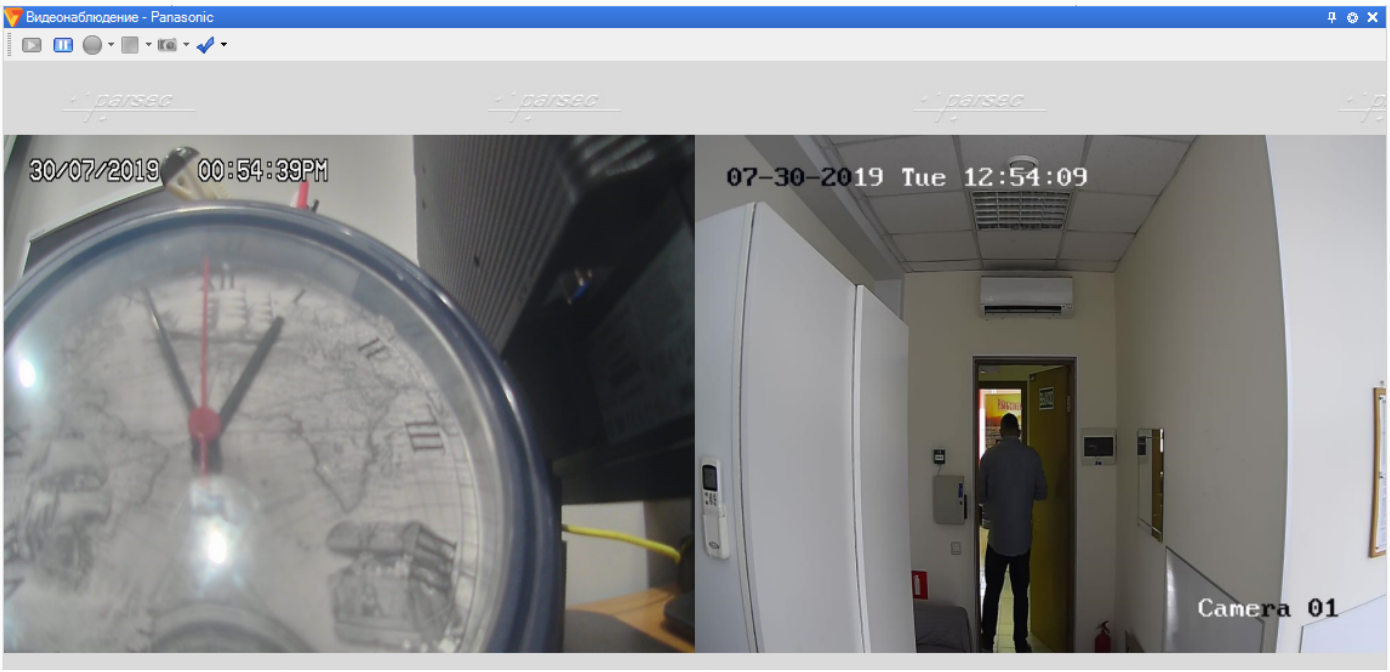
6. В открывшемся окне введите его название и, если необходимо, описание. После чего нажмите на кнопку *ОК*:



7. В правом верхнем углу созданного окна нажмите на кнопку *Настройки* и выберите камеры, изображение с которых будет отображаться в данном окне видеонаблюдения:



8. Изображение с выбранных камер будет выведено в окно. Система позволяет как вывести изображение с нескольких камер в одно окно, так и создать для каждой камеры свое окно видеонаблюдения:



Элементы интерфейса окна видеонаблюдения:

- включение/отключение фиксированного режима, при котором не отображается панель инструментов и невозможно изменить положение и размер окна видеонаблюдения(см. раздел Блокировка внешнего вида[54]);
- открывает окно выбора камер;
- показать изображение;
- остановить показ изображения;
- начать запись (функция недоступна для этой видеосистемы);

- остановить запись (функция недоступна для этой видеосистемы);
- сохранить кадр (функция недоступна для этой видеосистемы);
- установка временной метки на кадр.

11.5.7 Система SecurOS (ISS)

В этом разделе описывается взаимодействие видеосистемы SecurOS производства компании ISS и СКУД ParsecNET 3.
На текущий момент СКУД была протестирована и показала надежную работу с ПО SecurOS 10.5, 10.6, 11.2 и 11.5_R1.
При обновлении ПО ParsecNET 3 до версии 3.10.325.19 или выше и наличии работающей интеграции с ПО SecurOS версии 10.5 необходимо также обновить модуль ActiveMedia Kit до версии 10.6 для возобновления работы интеграционных механизмов.



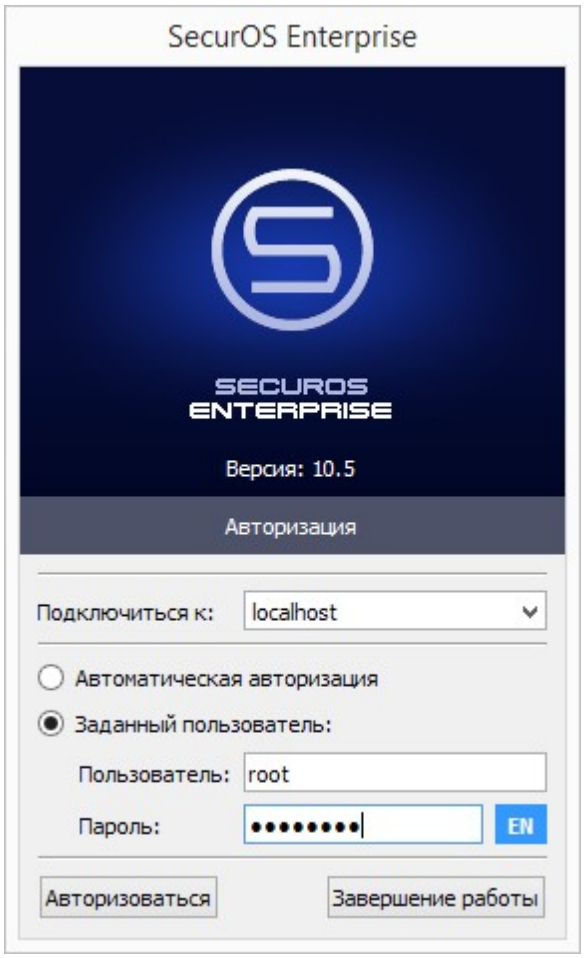
Данный раздел не является руководством по использованию системы SecurOS, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы SecurOS обратитесь к оригинальному руководству.

Работа с видеосистемой состоит из следующих принципиальных шагов:
1. Установка сервера системы[566] SecurOS;
2. Установка приложения MediaKit той же версии, что и ПО SecurOS. RestIP
   Установка производится на ПК, где установлен сервер системы SecurOS, а так же на том ПК, где будет использоваться система SecurOS;
3. Запуск и настройка приложения SecurOS, добавление видеокамер;
4. Поиск сервера видеосистемы[568] средствами ParsecNET;
5. Поиск камер, подключенных к серверу видеосистемы;
6. Настройка окна (окон) видеонаблюдения для системы SecurOS;
7. При необходимости, настройка модуля распознавания лиц FaceX[572].

Также в видеосистеме SecurOS имеется модуль распознавания лиц FaceX, интеграция с которым описана в разделе.

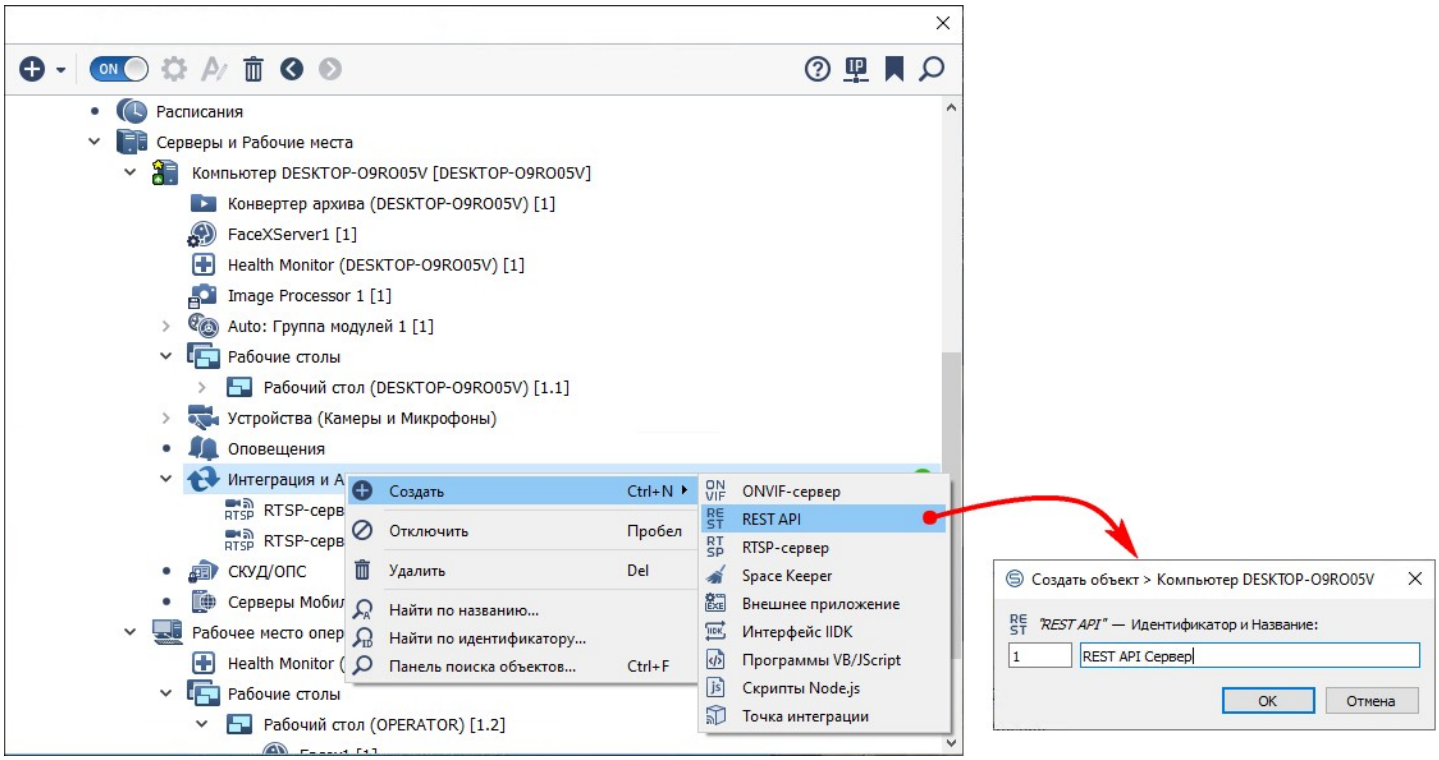
11.5.7.1 Подключение и настройка

1. Установите необходимое ПО системы SecurOS с дистрибутивного носителя, следуя подсказкам мастера установки (при необходимости обратитесь к документации SecurOS).
   Настоятельно рекомендуется ставить сервер системы SecurOS на отдельный ПК с достаточным объемом памяти для хранения видеозаписей.
   При установке сервера выберите последовательно:
   - Установка с расширенными настройками;
   - Видеосервер;
   - Сервер конфигурации;
   - Устанавливать ISS Integrated Devices Pack.
2. После установки сервера видеосистемы установите приложение MediaKit (с другими версиями интеграция не тестировалась).
3. Запустите приложение SecurOS:



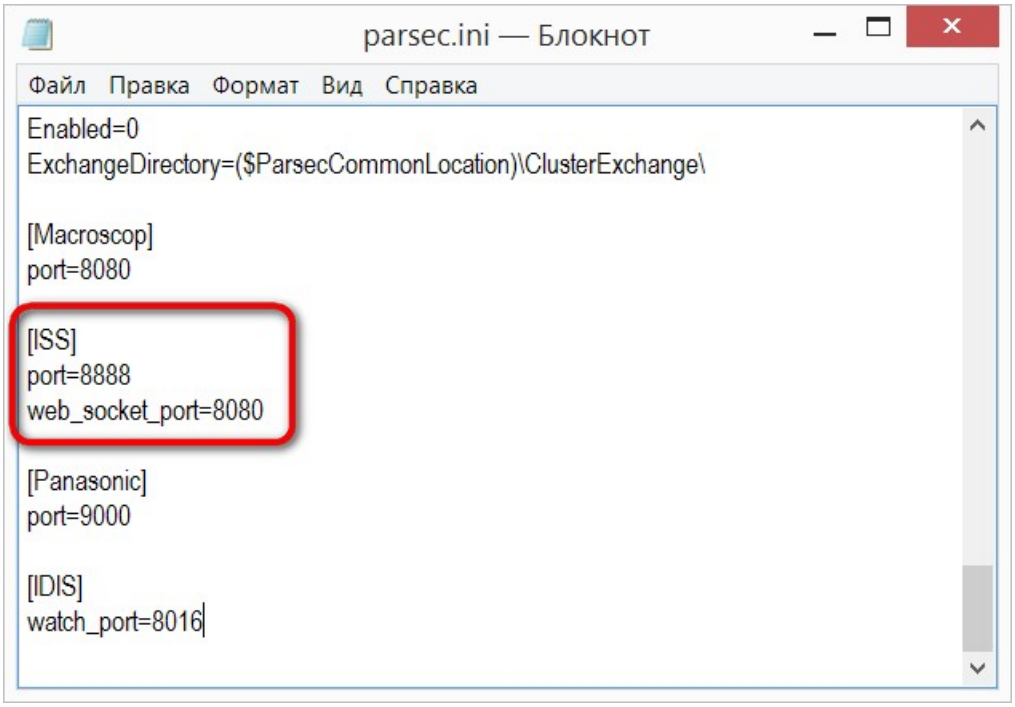
Для входа по умолчанию используется имя пользователя root, пароль - securos.

В запущенной программе SecurOS Enterprise откройте окно настроек и в разделе *Интеграция и Автоматизация* добавьте объект REST API:



Затем добавьте камеры в разделе *Устройства (Камеры и Микрофоны)*, руководствуясь инструкцией по эксплуатации системы SecurOS.

Если при настройке был изменен порт по умолчанию, то его необходимо обязательно изменить и в файле настройки ParsecNET *parsec.ini*, находящемся по умолчанию по адресу *C:\ProgramData\MDO\ParsecNET 3*:

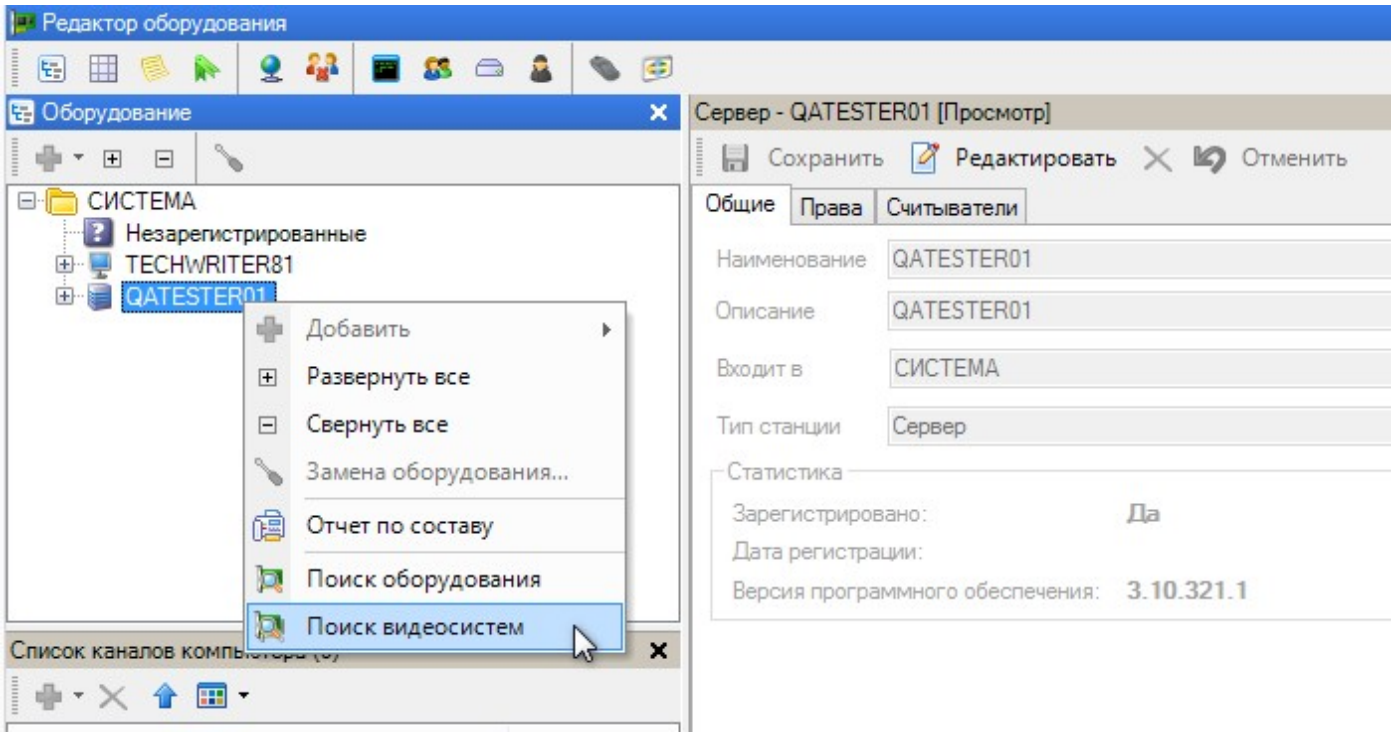


После этого СКУД ParsecNET 3 готов работать с системой SecurOS.

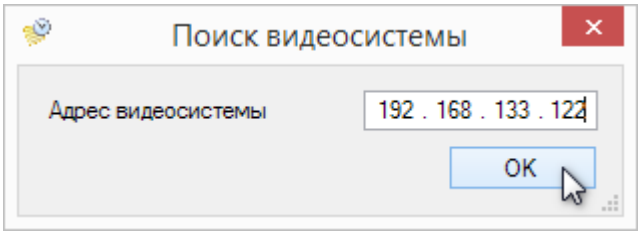
11.5.7.2 Использование системы

После того как система SecurOS и приложение MediaKit установлены, к видеосистеме добавлены и настроены камеры, ее можно использовать в рамках СКУД ParsecNET 3. Для этого выполните следующие шаги:

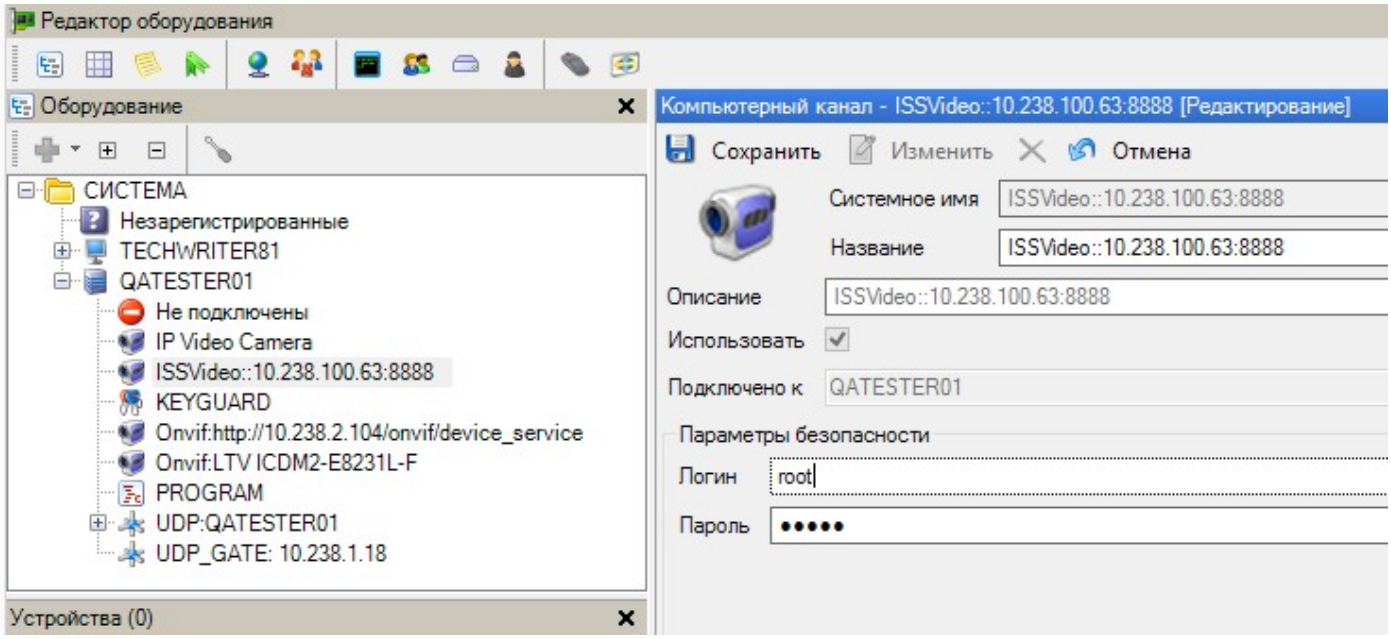
1. Запустите консоль "Администрирование" ParsecNET 3 на ПК и в контекстном меню рабочей станции Parsec (сервера или локального ПК) выберите "Поиск видеосистем":



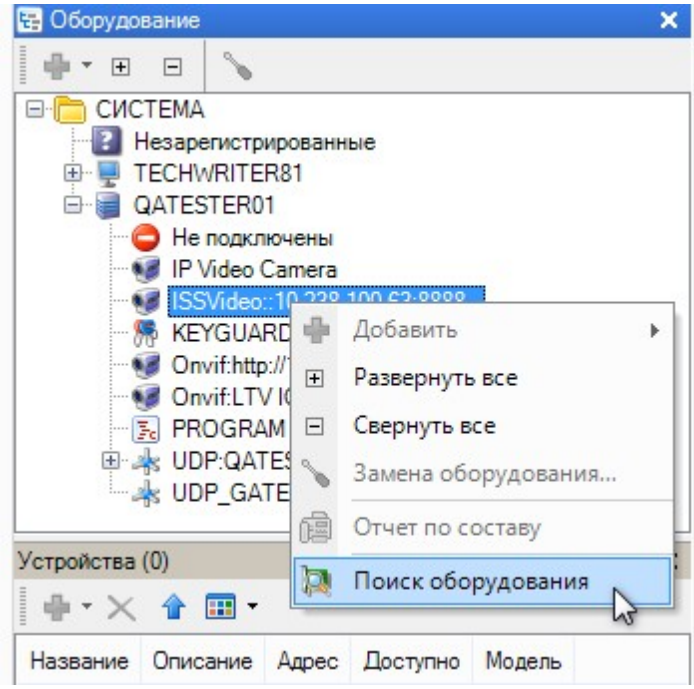
2. В открывшемся окне введите IP-адрес ПК, на котором установлен видеосервер (если оставить поле адреса пустым, то поиск будет осуществляться на локальной машине, что аналогично функции "Поиск оборудования") и нажмите на кнопку *ОК*:



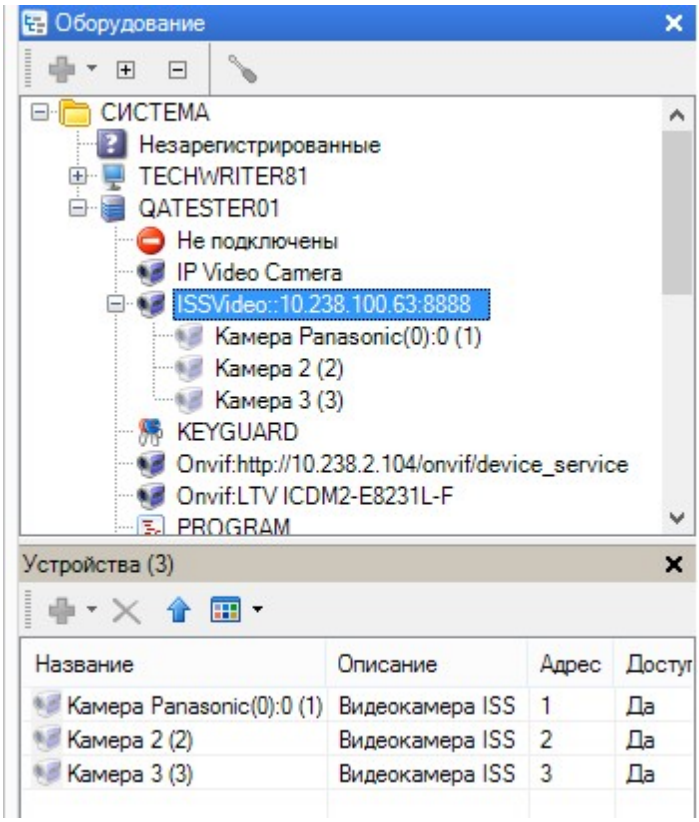
3. После того, как канал сервера видеосистемы SecurOS будет найден, необходимо обнаружить подключенные к нему камеры. Но для этого сначала необходимо ввести логин и пароль для доступа к SecurOS[566]:



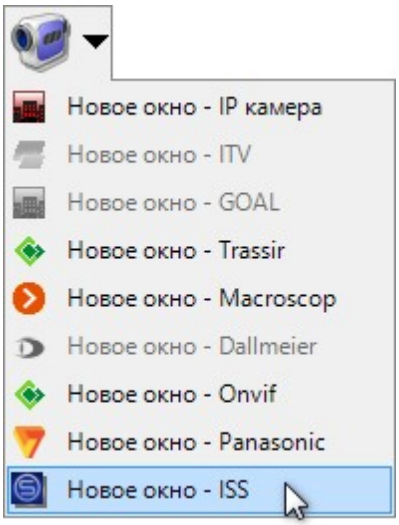
4. Проведите на канале видеосистемы поиск оборудования:



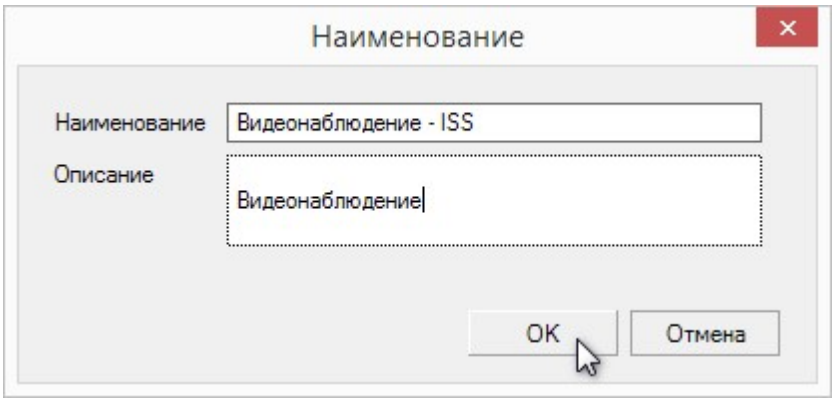
Подключенные к серверу видеосистемы камеры отобразятся в Редакторе оборудования:



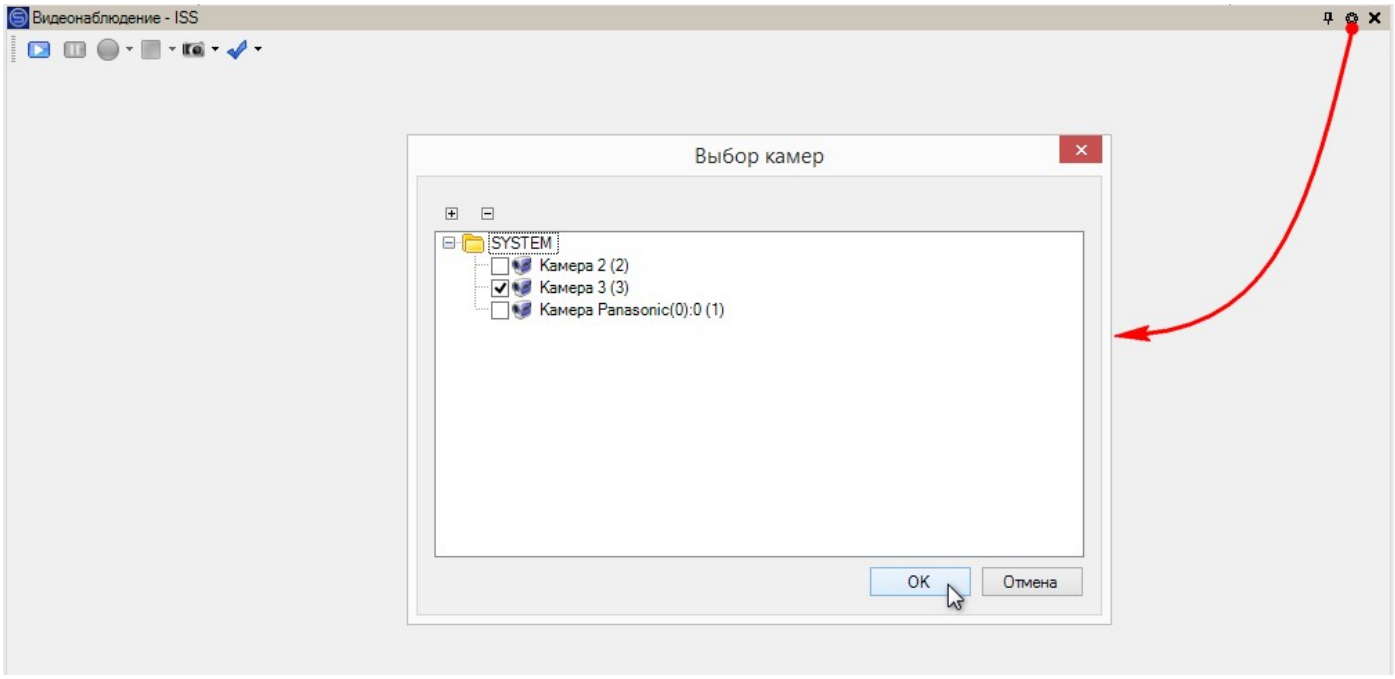
5. В раскрывающемся списке *Видеонаблюдение* выберите команду "Новое окно - ISS":



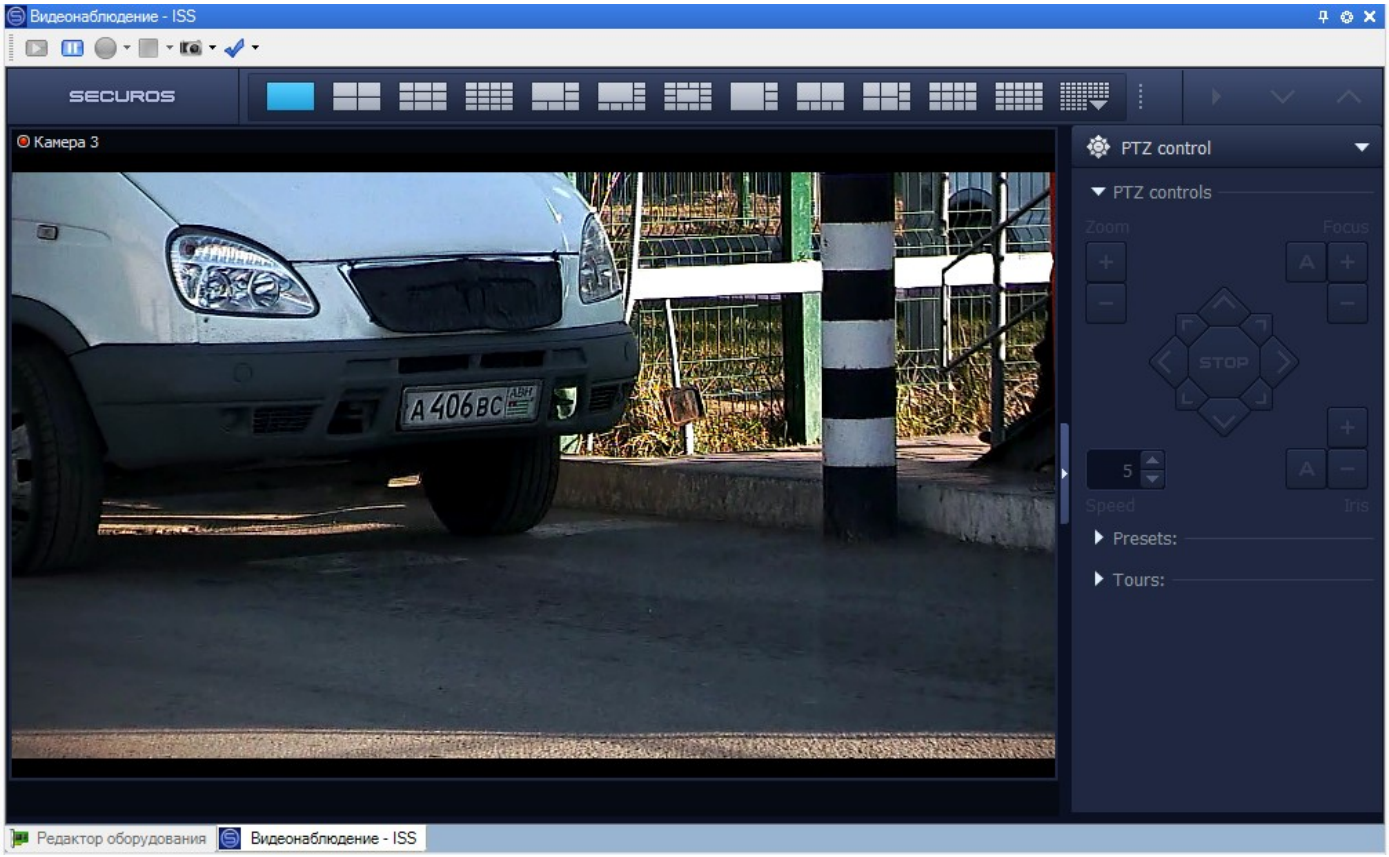
6. В открывшемся окне введите его название и, если необходимо, описание. После чего нажмите на кнопку *OK*:



7. В правом верхнем углу созданного окна нажмите на кнопку *Настройки* и выберите камеры, изображение с которых будет отображаться в данном окне видеонаблюдения:



8. Изображение с выбранных камер будет выведено в окно. Система позволяет как вывести изображение с нескольких камер в одно окно, так и создать для каждой камеры свое окно видеонаблюдения:



Элементы интерфейса окна видеонаблюдения:

- включение/отключение фиксированного режима, при котором не отображается панель инструментов и невозможно изменить положение и размер окна видеонаблюдения(см. раздел Блокировка внешнего вида[54]);

- открывает окно выбора камер;

- показать изображение;
- остановить показ изображения;
- начать запись (функция недоступна для этой видеосистемы);
- остановить запись (функция недоступна для этой видеосистемы);
- сохранить кадр;
- установка временной метки на кадр.

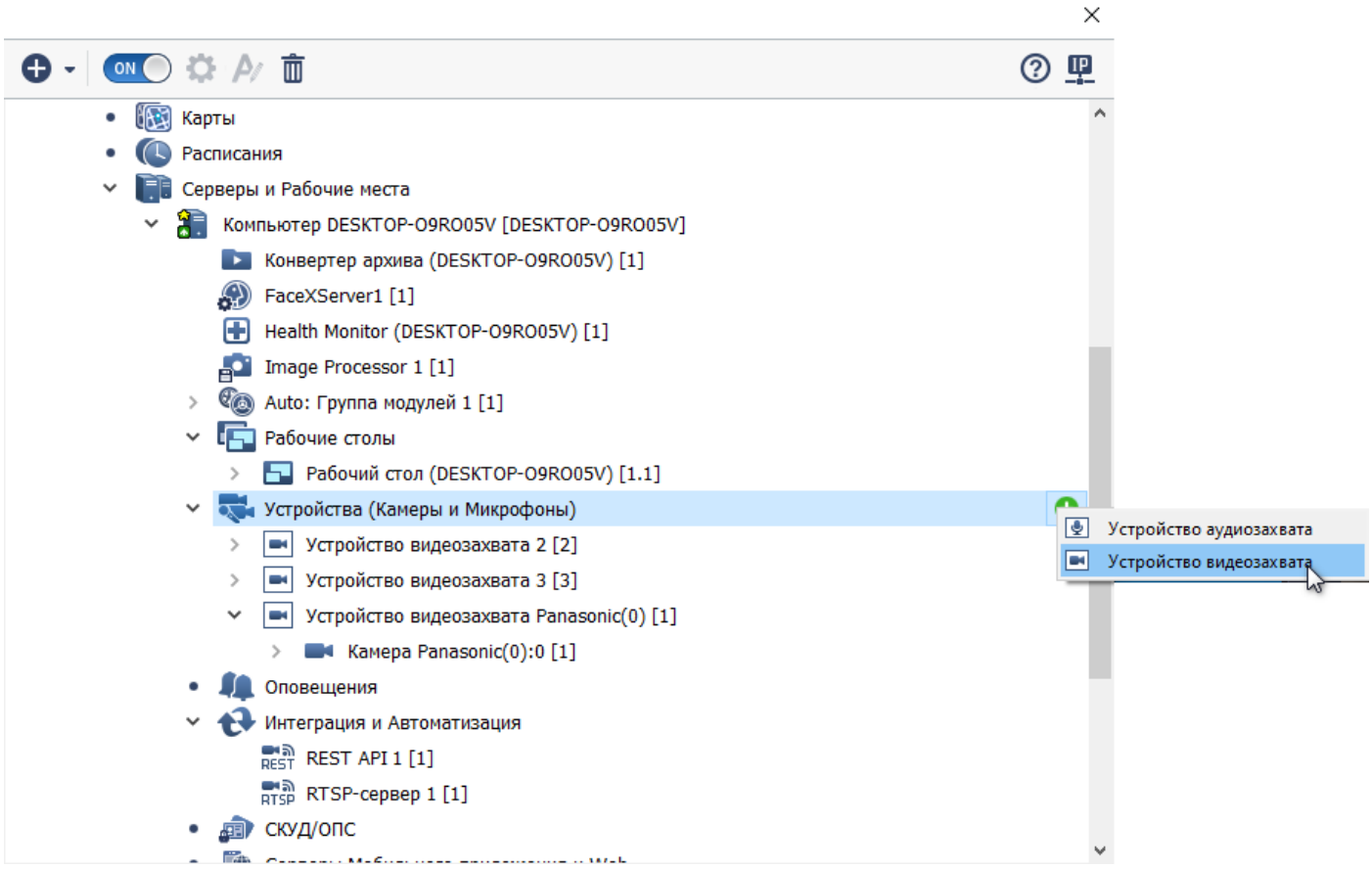
11.5.7.3 Модуль распознавания лиц FaceX

SecurOS FaceX - видеоаналитическая система распознавания лиц компании ISS на базе сверточных нейронных сетей, обеспечивающая следующие возможности:

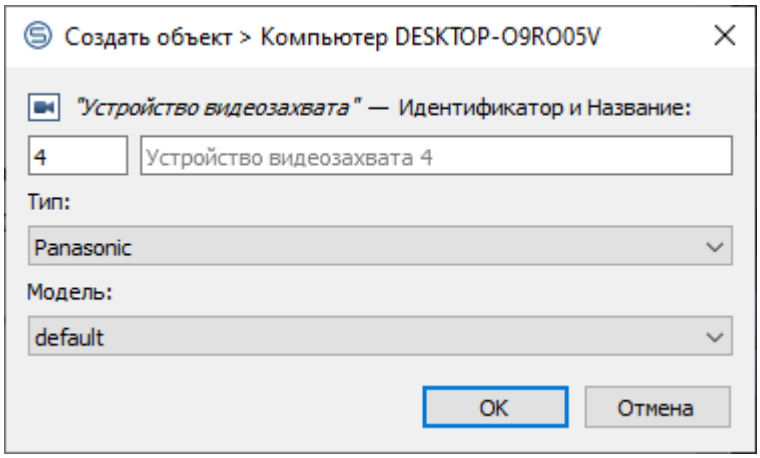
- Автоматическая детекция и распознавание лиц в режиме реального времени с отображением зафиксированных результатов в интерфейсе оператора SecurOS FaceX.
- Протоколирование информации обо всех задетектированных лицах и фактах распознавания с сохранением данных о месте и времени, ссылки на видеофрагмент в видеоархиве.
- Защита от подмены лиц.
- Автоматический захват лиц всех людей, находящихся в зоне детекции камеры.
- Высокое качество распознавания в широком диапазоне внешних условий (ракурс, изменяющаяся и недостаточная освещенность, осадки).

Организация взаимодействия СКУД ParsecNET 3 и модуля распознавания лиц FaceX состоит в выполнении следующих шагов:

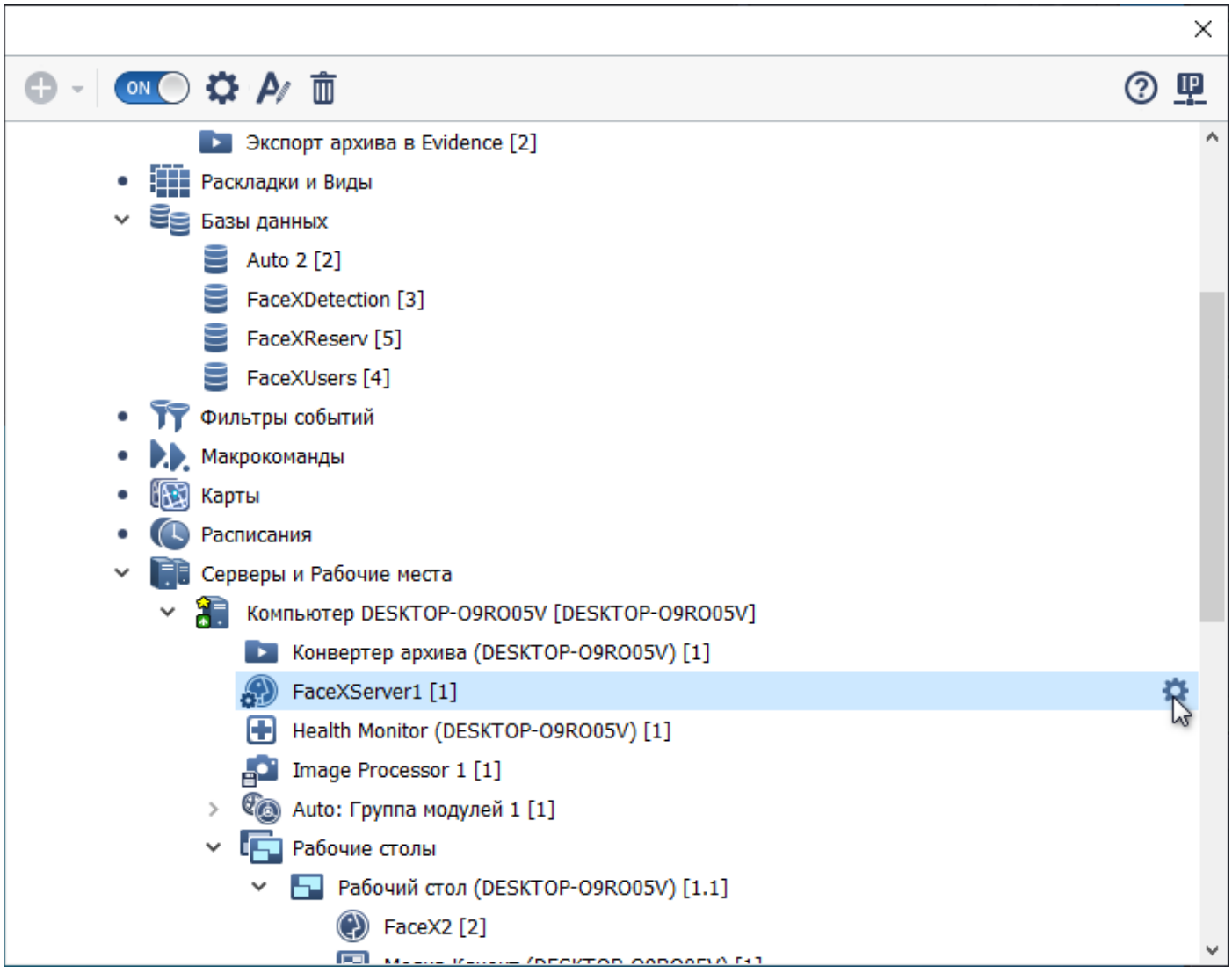
1. Установите и настройте систему видеонаблюдения SecurOS, следуя руководству по ее эксплуатации;
2. Настройте модуль FaceX в рамках видеосистемы SecurOS:
   - Запустите программу SecurOS Enterprise;
   - Перейдите в раздел *Устройства (Камеры и Микрофоны)*, нажмите на кнопку *Создать* справа и выберите команду *Устройства видеозахвата*:



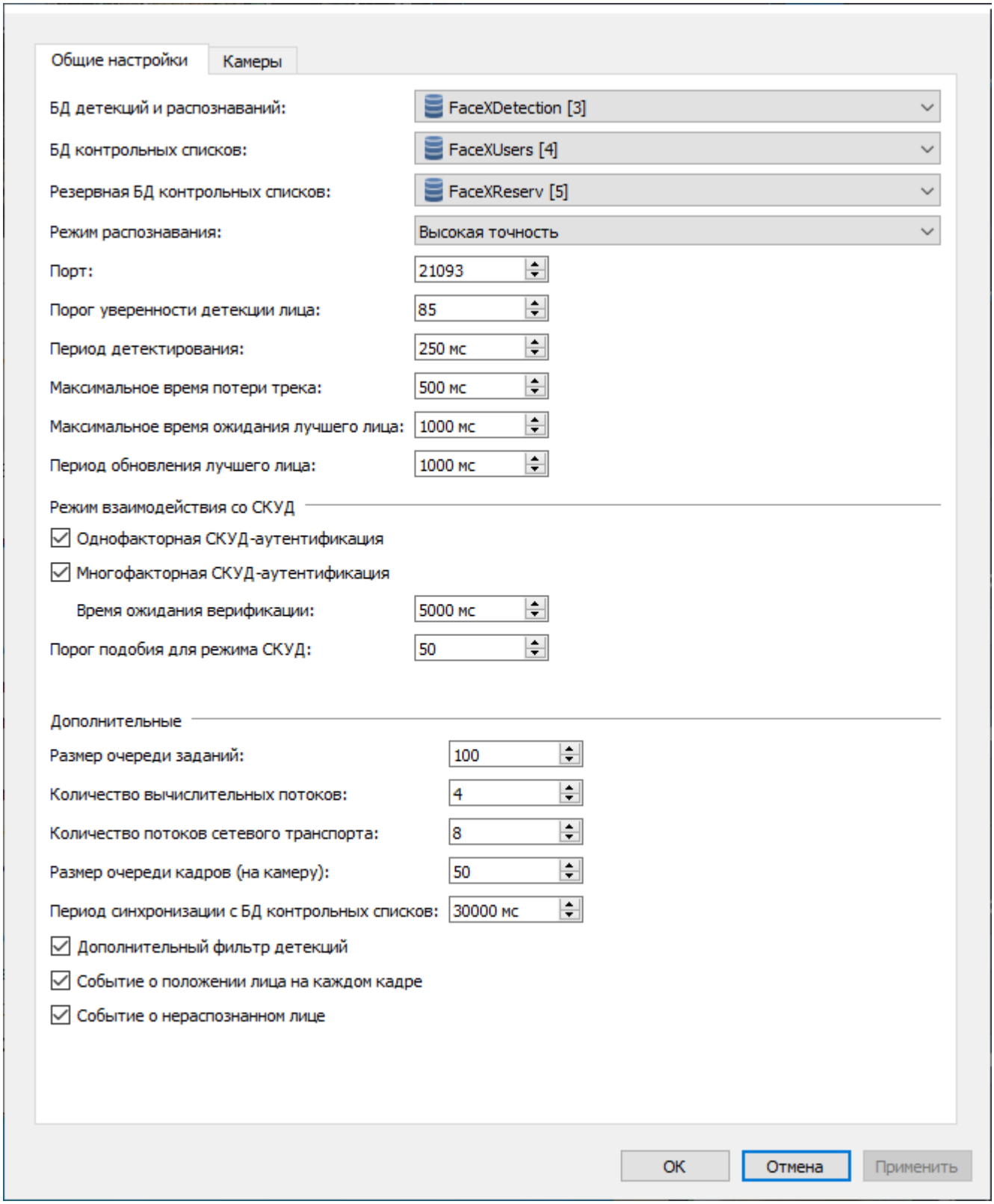
- В открывшемся окне выберите модель камеры и нажмите на кнопку *OK*:



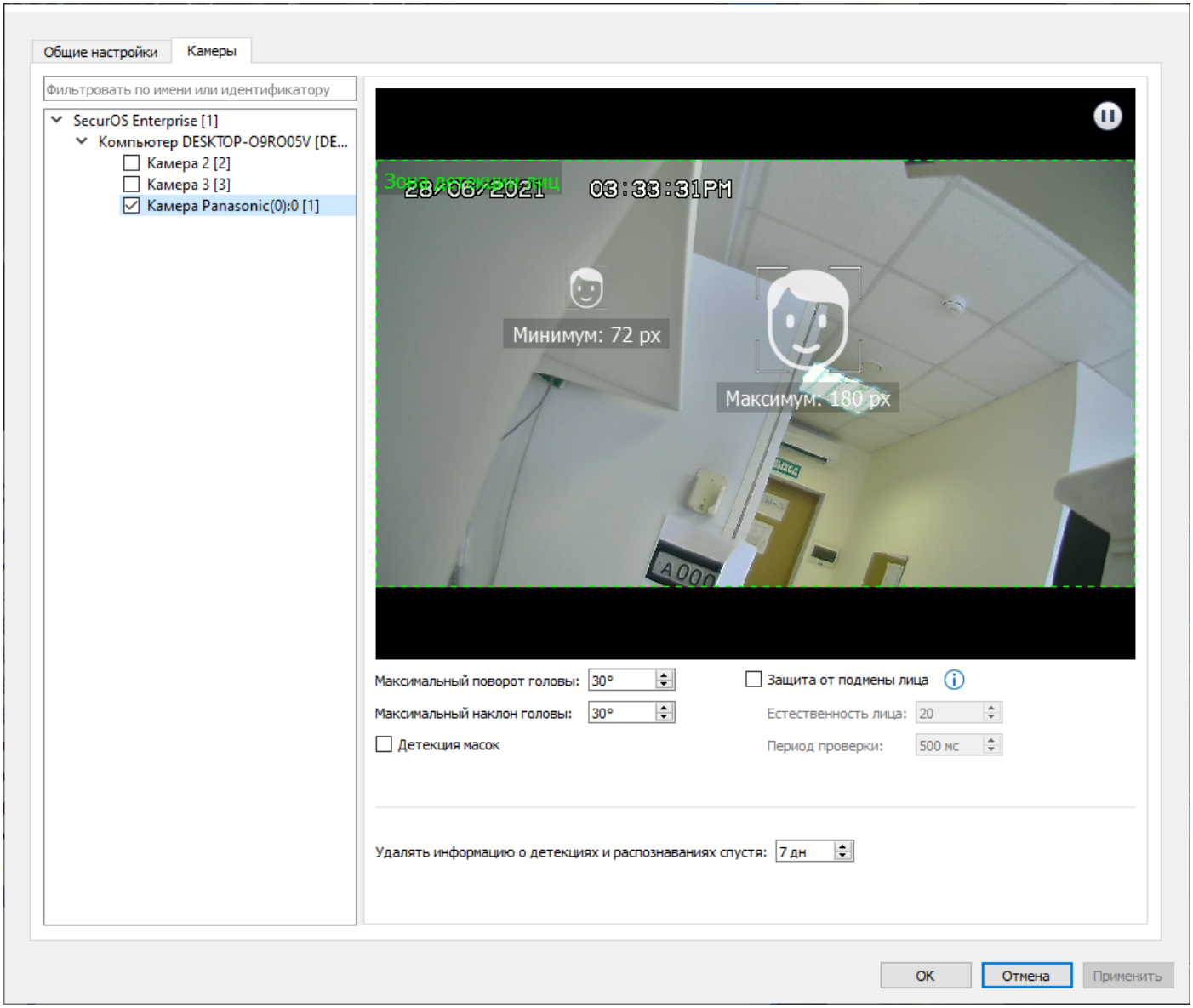
- Перейдите в раздел сервера FaceXServer и нажмите на значок настройки:



- В открывшемся окне на вкладке *Общие настройки* задайте значения параметров соответствии с руководством по эксплуатации (Securos FaceX User Guide):

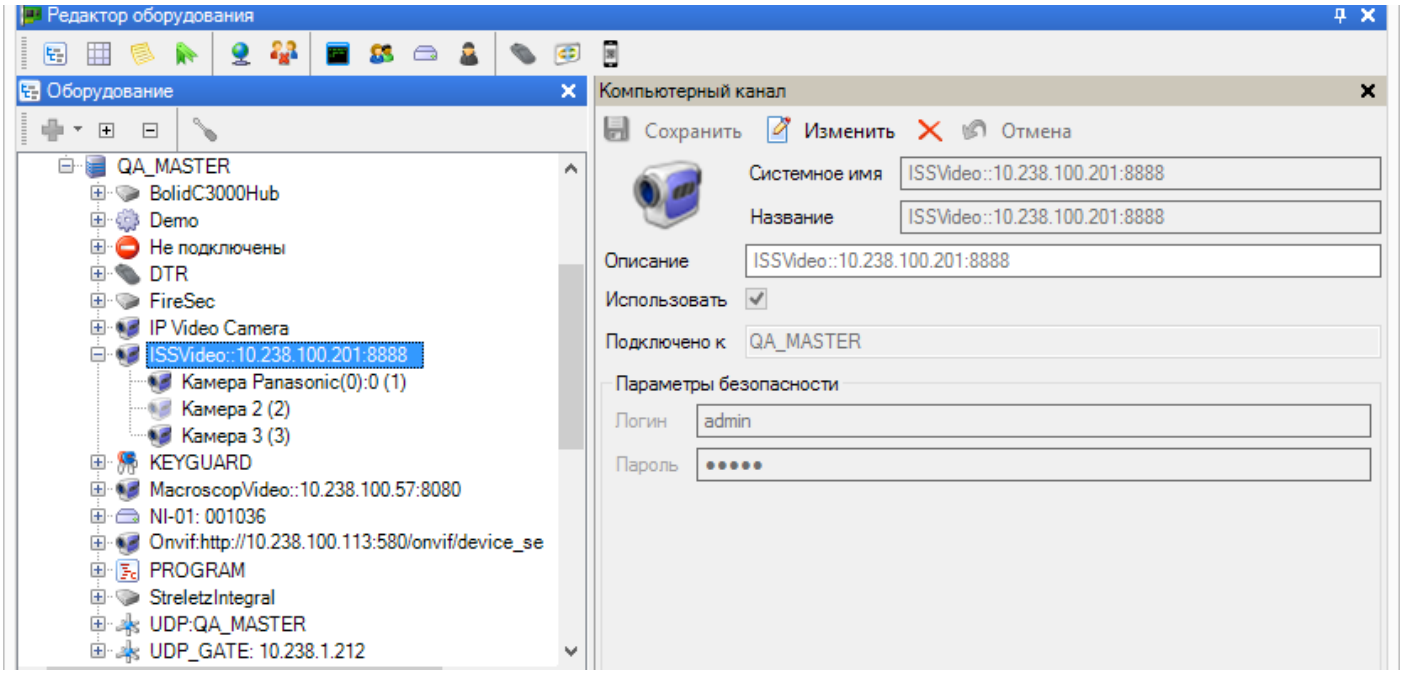


- Перейдите на вкладку *Камеры*, выберите одну из подключенных камер;
- Задайте необходимые параметры и сохраните настройки:

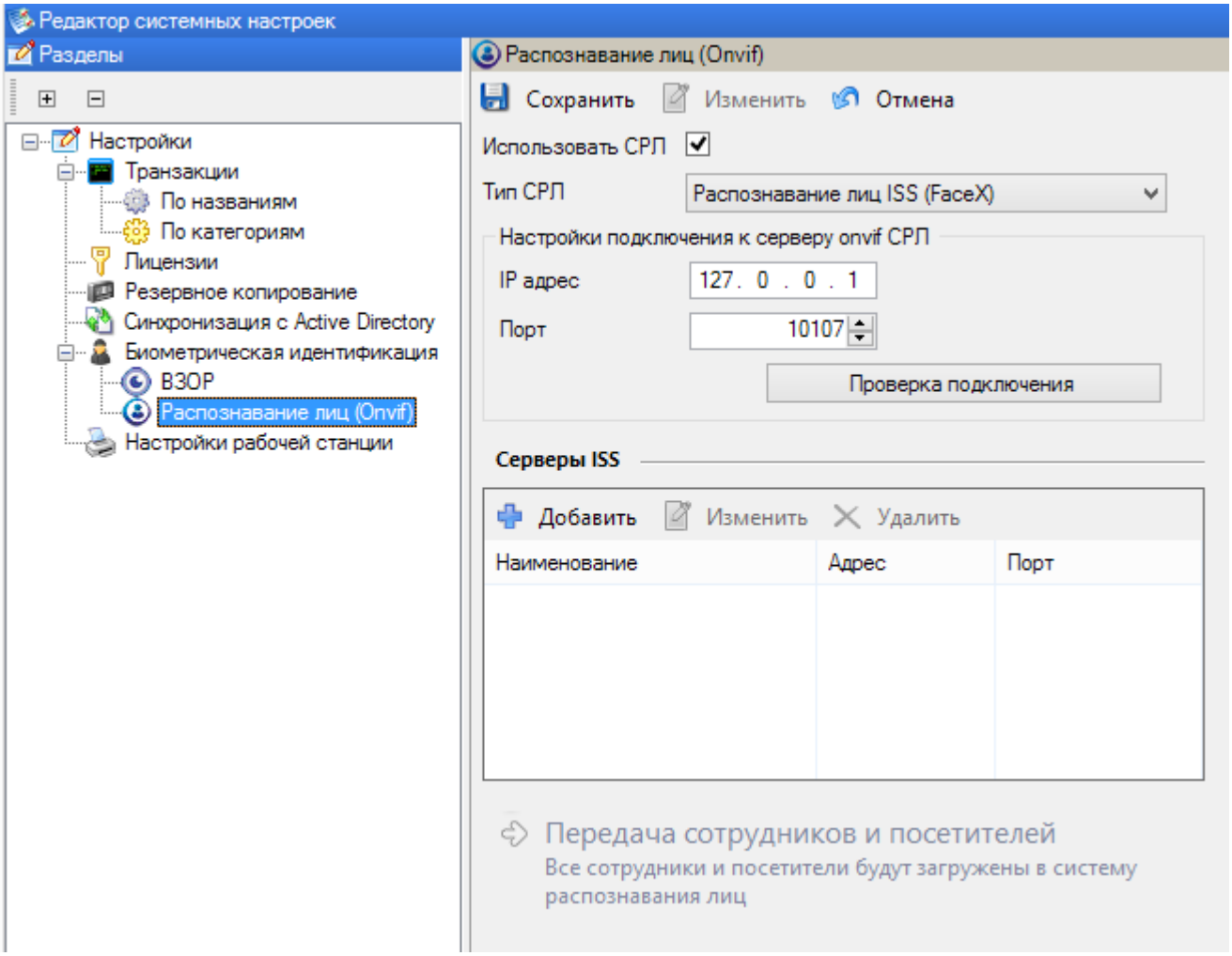


Проведите настройку всех камер и сохраните результат;

3. Запустите консоль *Администрирование* ПО ParsecNET 3 и перейдите в Редактор оборудования;
4. Проведите поиск видеосистем[64], введя в окне поиска IP-адрес сервера SecurOS. В дереве оборудования должен появиться канал ISSVideo;
5. Перейдите в режим редактирования. Введите логин и пароль для доступа к серверу и сохраните изменения;
6. Проведите поиск оборудования на найденном канале. Должны появиться все камеры, подключенные к серверу SecurOS:

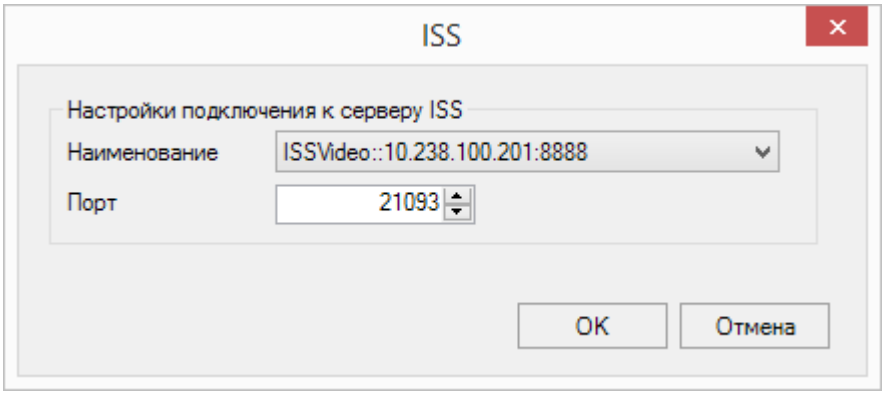


7. Перейдите в Редактор системных настроек СКУД ParsecNET3 и откройте раздел *Биометрическая идентификация - Распознавание лиц (Onvif)*;
8. Перейдите в режим редактирования и установите флажок *Использовать СРЛ*;
9. Из раскрывающегося списка *Тип СРЛ* выберите *Система распознавания лиц ISS*. (Настройка интеграционного модуля распознавания лиц на основе Onvif описана в другом разделе[353]);
10. В блоке *Настройки подключения к серверу Onvif СРЛ* отображаются параметры сервера onvif, устанавливаемого по-умолчанию при установке ПО ParsecNET 3. В случае, если параметры сервера onvif были изменены, необходимо внести соответствующие изменения и в этот блок.



Для проверки связи с сервером Onvif нажмите на кнопку *Проверка подключения*. Результаты проверки отобразятся в отдельном окне: "Подключение к серверу onvif прошло успешно" или "Сервер onvif не найден";

11. В блоке *Серверы ISS* нажмите на кнопку *Добавить*;
12. В открывшемся окне из раскрывающегося списка выберите один из найденных на шаге 4 серверов SecurOS:



Заполните остальные поля:

- *Порт* - порт сервера SecurOS;
- *Логин* и *Пароль* - соответственно, логин и пароль для доступа к серверу SecurOS.

13. Нажмите на кнопку *OK* и сохраните изменения. Редактор системных настроек выйдет из режима редактирования;
14. Выберите нужный сервер ISS и нажмите на ставшую активной кнопку *Передача сотрудников и посетителей*. Сведения будут переданы на сервер SecurOS. Впоследствии все изменения

в БД СКУД автоматически передаются в БД SecurOS.
Лицо претендента на проход будет обнаруживается камерой и сравнивается с БД лиц пользователей на сервере SecurOS. Полученные результаты передаются на сервер СКУД ParsecNET 3, который и определяет право на проход.

11.5.8 Система IDIS

В этом разделе описываются возможности видеосистемы IDIS и настройки ParsecNET 3 для работы с ней.

Данный раздел не является руководством по использованию системы IDIS, а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы IDIS обратитесь к оригинальному руководству.

Основные возможности

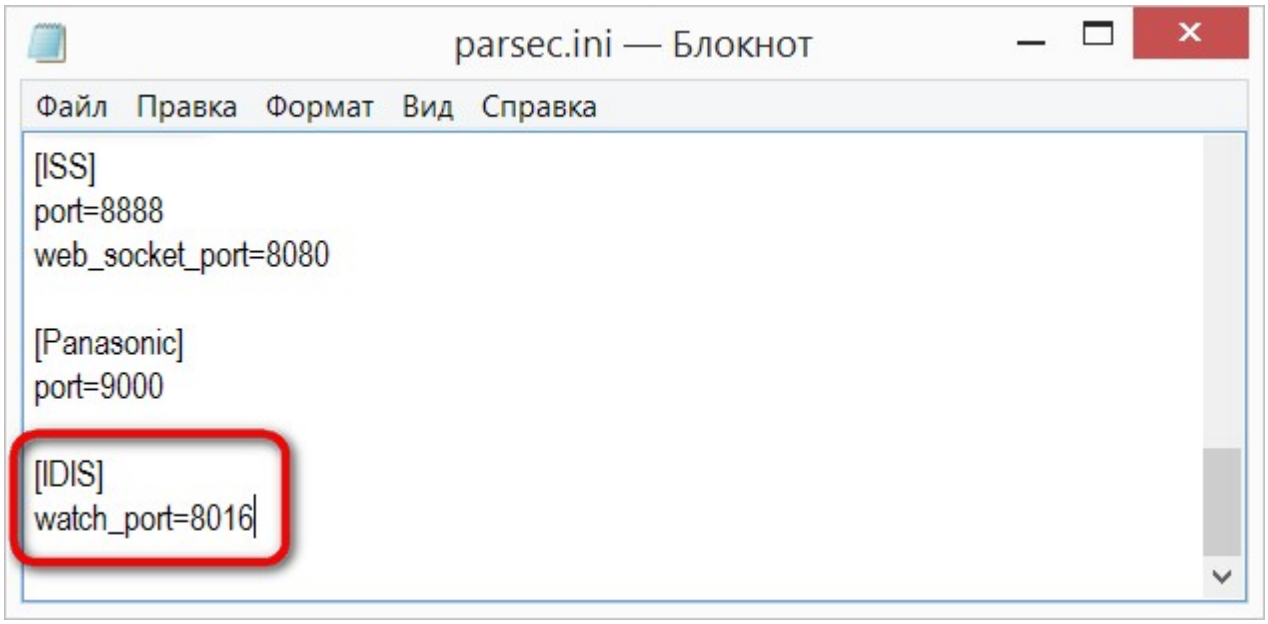
Видеосистема IDIS предоставляет поддержку следующих функциональных возможностей:

- Добавление на сервер / рабочую станцию ParsecNET через редактор оборудования канала интеграции с видеорегистратором IDIS;
- Получение из ПО видеорегистратора IDIS списка камер, подключенных в систему с созданием объектов типа "Камера" в ПО ParsecNET 3 на канале IDIS в Редакторе оборудования;
- Воспроизведение живого видеопотока с камер системы IDIS в Мониторе событий и инструменте "Видеоверификация";
- Воспроизведение архивного видеопотока с камер системы IDIS в ПО ParsecNET 3 (в модуле журнала событий системы);
- Возможность привязать камеры видеосистемы IDIS к точке прохода ParsecNET 3 в Редакторе топологии для отображения живого видеопотока с камер по тревожным событиям от точек прохода и архивного видеопотока с камер.

11.5.8.1 Подключение и настройка

Установите и настройте видеорегистратор IDIS, следуя указаниям мастера установки и руководству по эксплуатации. Подключите камеры к видеорегистратору.

Если при настройке был изменен порт по умолчанию, то его необходимо обязательно изменить и в файле настройки ParsecNET *parsec.ini*, находящемся по умолчанию по адресу *C:\ProgramData\MDO\ParsecNET 3*:

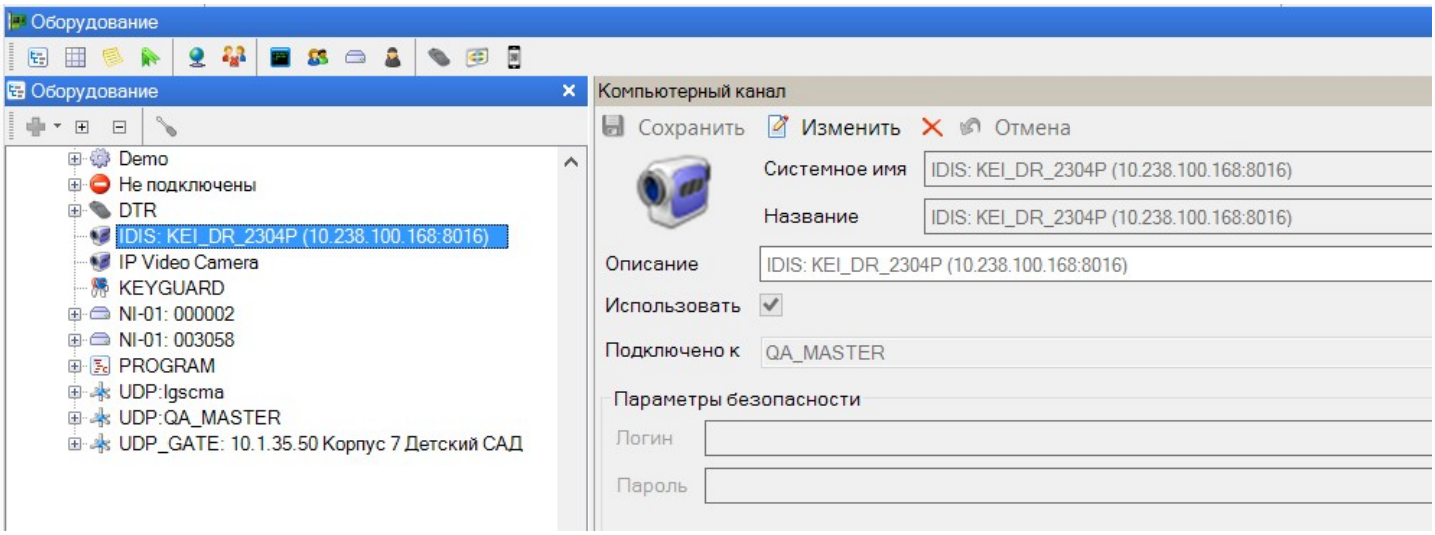


11.5.8.2 Использование системы

Запустите систему ParsecNET 3 на ПК, который будет работать с видеорегистратором IDIS, и проведите поиск новой видеосистемы. Для этого в контекстном меню рабочей станции ParsecNET (сервера или локального ПК) выберите команду "Поиск видеосистем".

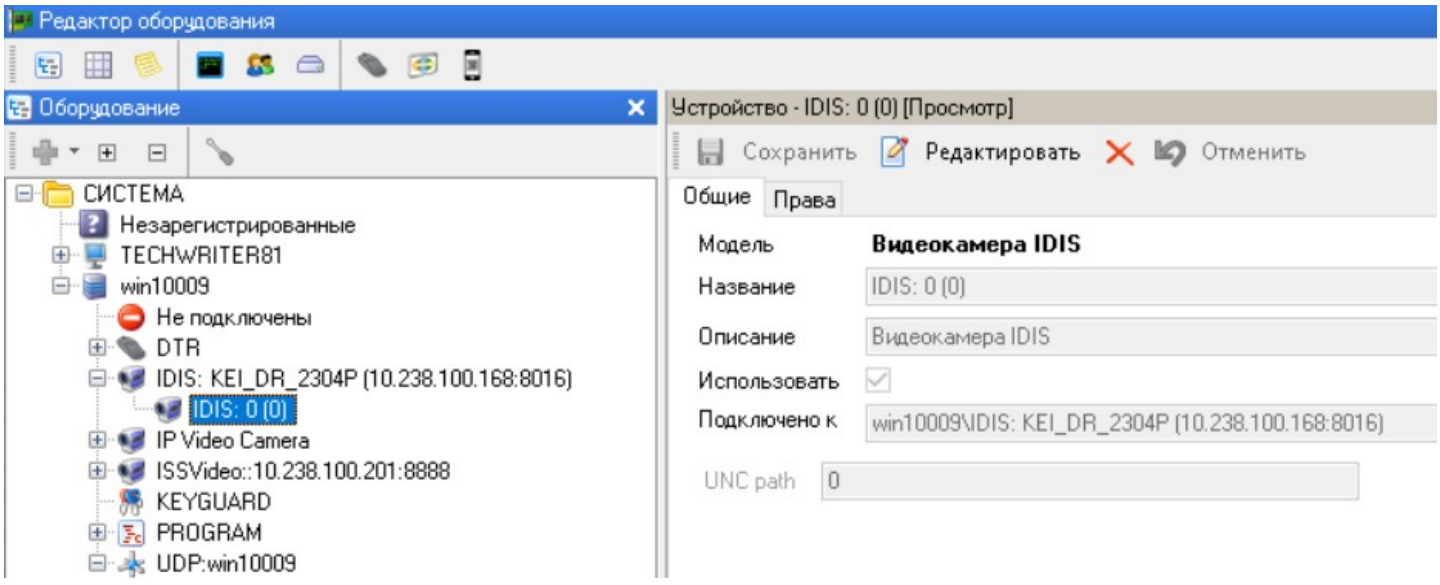
В открывшемся окне введите IP-адрес видеорегистратора IDIS (если оставить поле адреса пустым, IDIS обнаружен не будет) и нажмите на кнопку *OK*.

В списке оборудования должен появиться новый видеоканал, в нашем примере это "IDIS: KEI_DR_2304P (10.238.100.168:8016)":

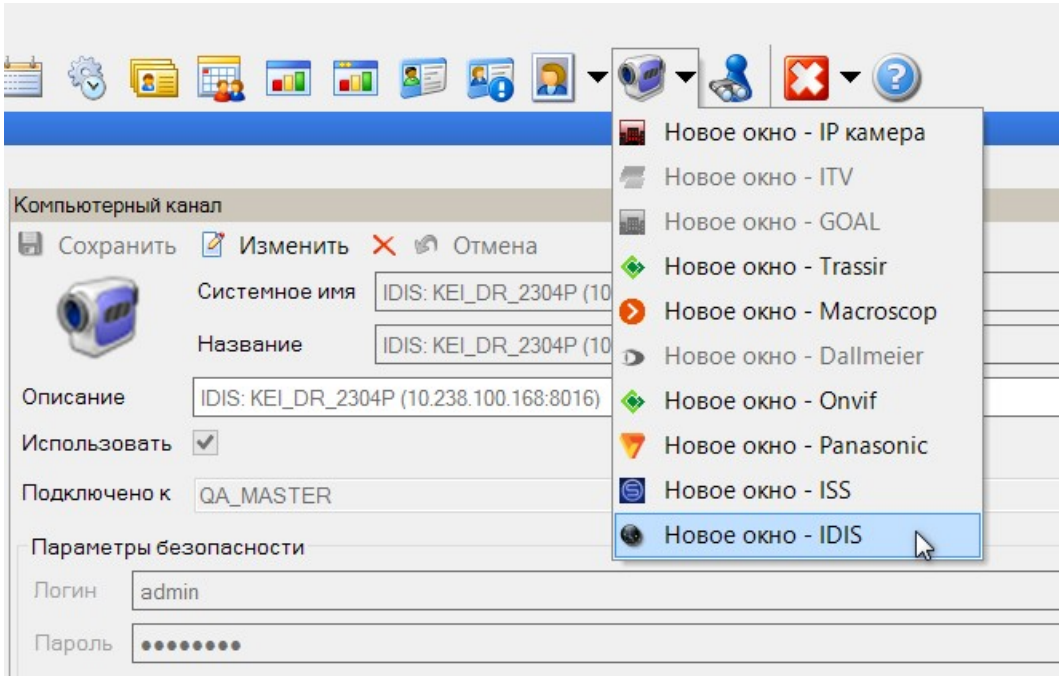


Перейдите в режим редактирования и введите логин и пароль для доступа, заданные при настройке видеорегистратора IDIS. Сохраните изменения.

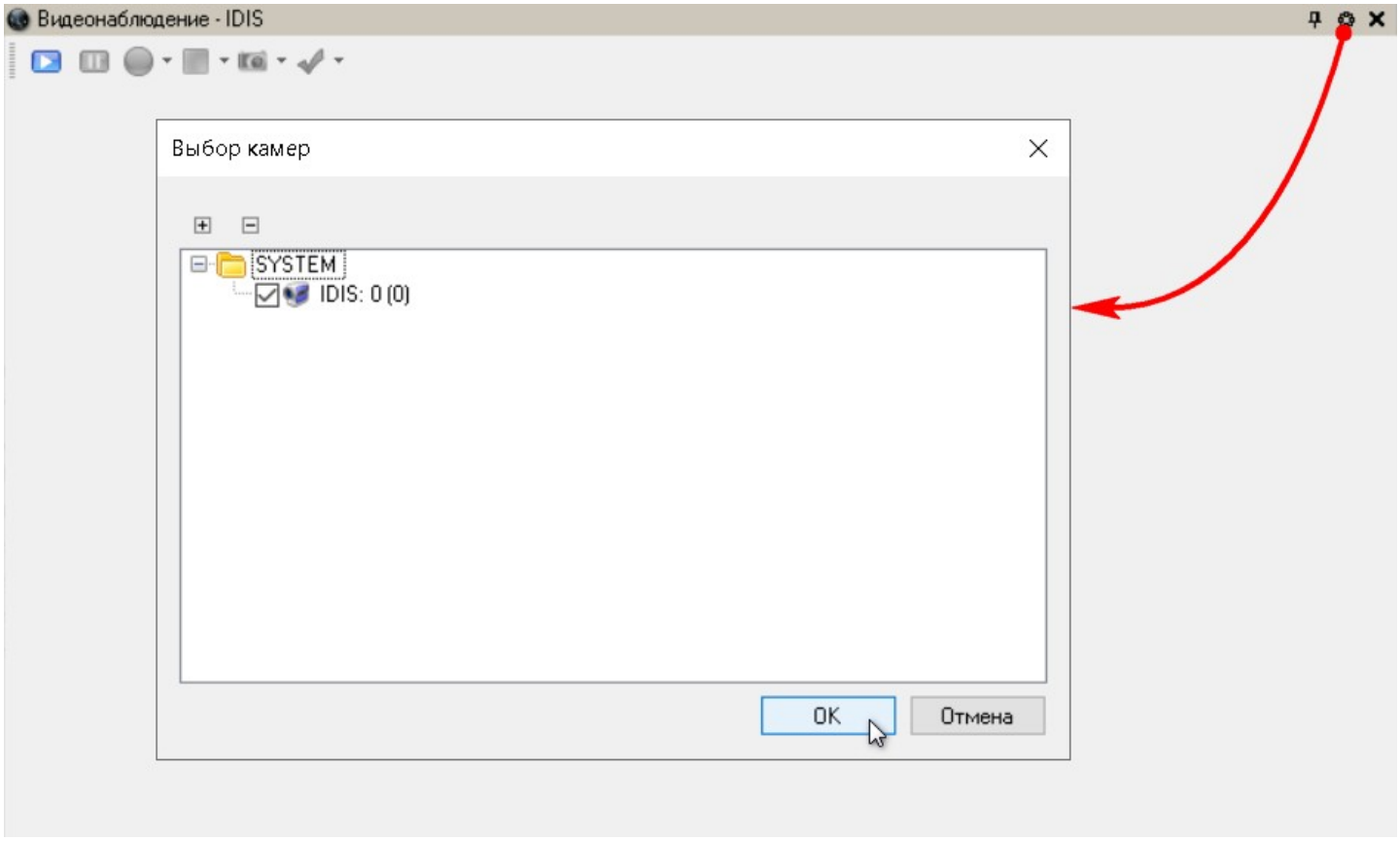
Теперь проведите поиск нового оборудования на этом видеоканале. Должны обнаружиться видеокамеры, подключенные и настроенные при установке видеорегистратора (на рис. ниже это "IDIS: 0 (0)"):



Добавьте новое окно видеонаблюдения IDIS:



В окне видеонаблюдения выберите камеру, подключенную к видеорегистратору IDIS и нажмите на кнопку *OK*:



Теперь в этом окне будет отображаться видео с выбранной камеры, которое можно использовать для видеоидентификации, сохранять в архив и т.п. Также камеры можно привязать[211] к конкретным точкам прохода.

11.6 Распознавание автомобильных номеров

Пользователи ParsecNET 3 имеют возможность распознавать автомобильные номера при помощи:

- собственного модуля[582] СКУД ParsecNET 3;

- внешней системы распознавания автономеров NumberOK[591];
- встроенного в IP-камеры Hikvision Smart-IP[594] ПО;
- камер Mobotix[598] с функцией распознавания автономеров;
- систем видеонаблюдения[515] GOALCity, TRASSIR, Macroscop или ИСБ "Интеллект", имеющих в своем составе функцию распознавания номеров.

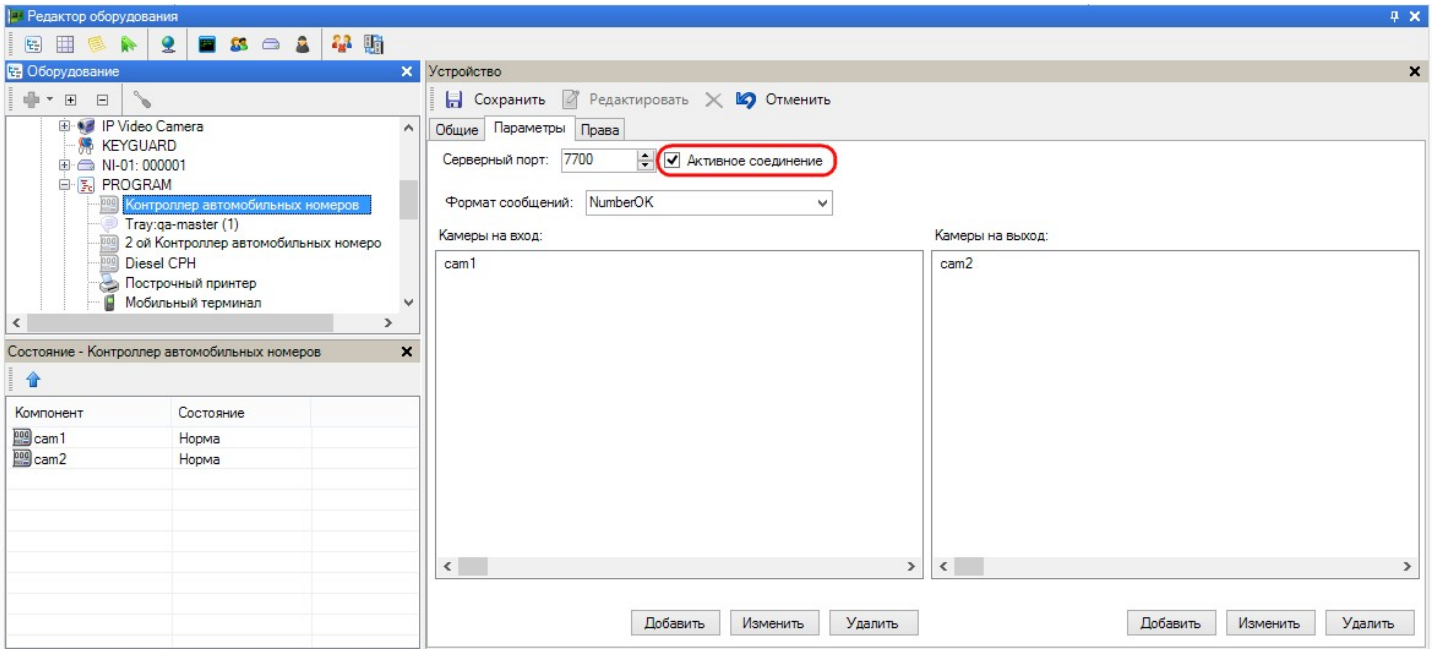
Если используются собственный модуль распознавания Parsec, системы видеонаблюдения GOALCity, TRASSIR, Macroscop или камеры Hikvision Smart-IP, то для организации автомобильной проходной[584] необходимо использовать программный контроллер[187] SCL-02.

При использовании для распознавания автономеров систем NumberOK[591], ИСБ "Интеллект"[593] или камер Mobotix[598] для создания автопроходной необходимо использовать контроллер автомобильных номеров[588]. Этот контроллер обеспечивает взаимодействие с любыми системами распознавания автономеров, при условии, что выходные данные будут представлены данной системой в xml-файле[591] заданной структуры.

Поскольку при использовании этих систем используется протокол TCP/IP, необходимо указать, какое соединение будет использоваться контроллером: пассивное или активное. Для этого предназначен флажок *Активное соединение* на вкладке *Параметры* в карточке контроллера автомобильных номеров.

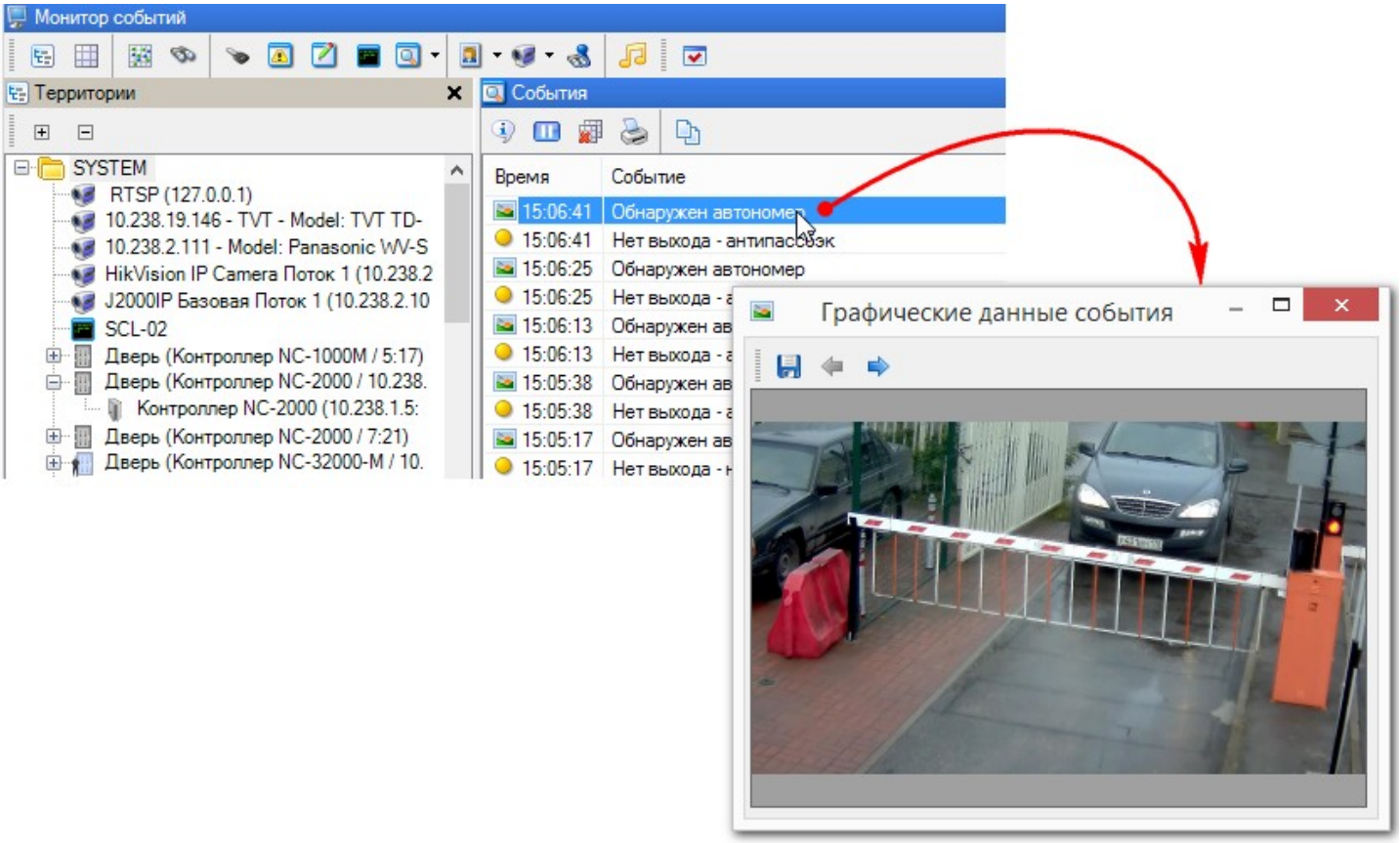
Если флажок *Активное соединение* стоит, то модуль будет сам пытаться установить соединение по указанному в настойках порту на локальном хосте (127.0.0.1).

Если флажок снят, то модуль ожидает соединения по выбранном порту.

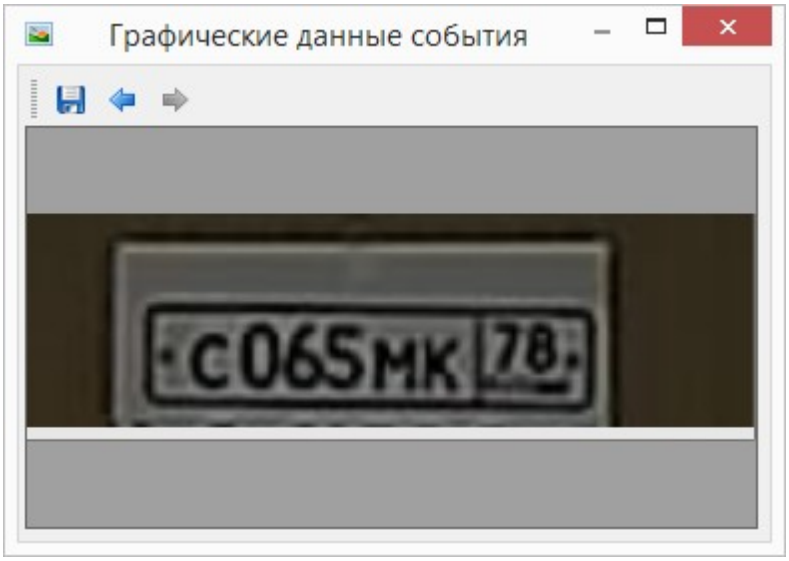


При использовании для распознавания автономеров ИСБ "Интеллект" или ПО NumberOK флажок "Активное соединение" должен быть установлен.

Когда автомобильный номер обнаруживается в поле зрения видеокамеры, в Мониторе событий генерируется транзакция *Обнаружен автономер*. Двойной щелчок по записи открывает окно просмотра:



Если используются камеры **Hikvision**, то нажатие на активную стрелку вправо приведет к отображению распознанного номера крупным планом. Вернуться к общему виду можно, нажав на стрелку влево.



11.6.1 Модуль распознавания автомобильных номеров Parsec

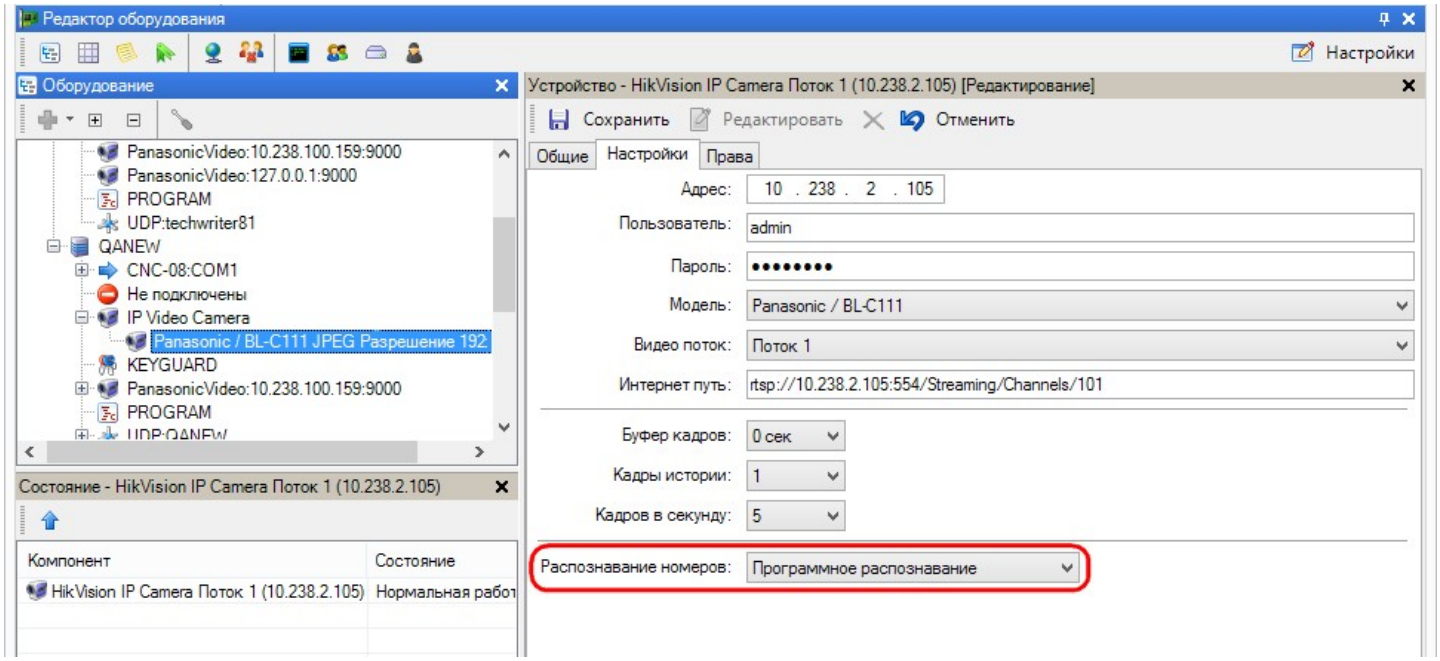
Модуль задействует встроенные в ПО средства видеоанализа для распознавания автомобильных номеров на изображениях, полученных с подключенных в систему IP-камер.

Для работы необходимо, чтобы ПК, к которому подключена IP-камера, работал на процессоре с архитектурой x64 и наличие 64-разрядной версии ОС Windows.

Данный функционал выпущен в тестовом режиме и впоследствии будет лицензирован.

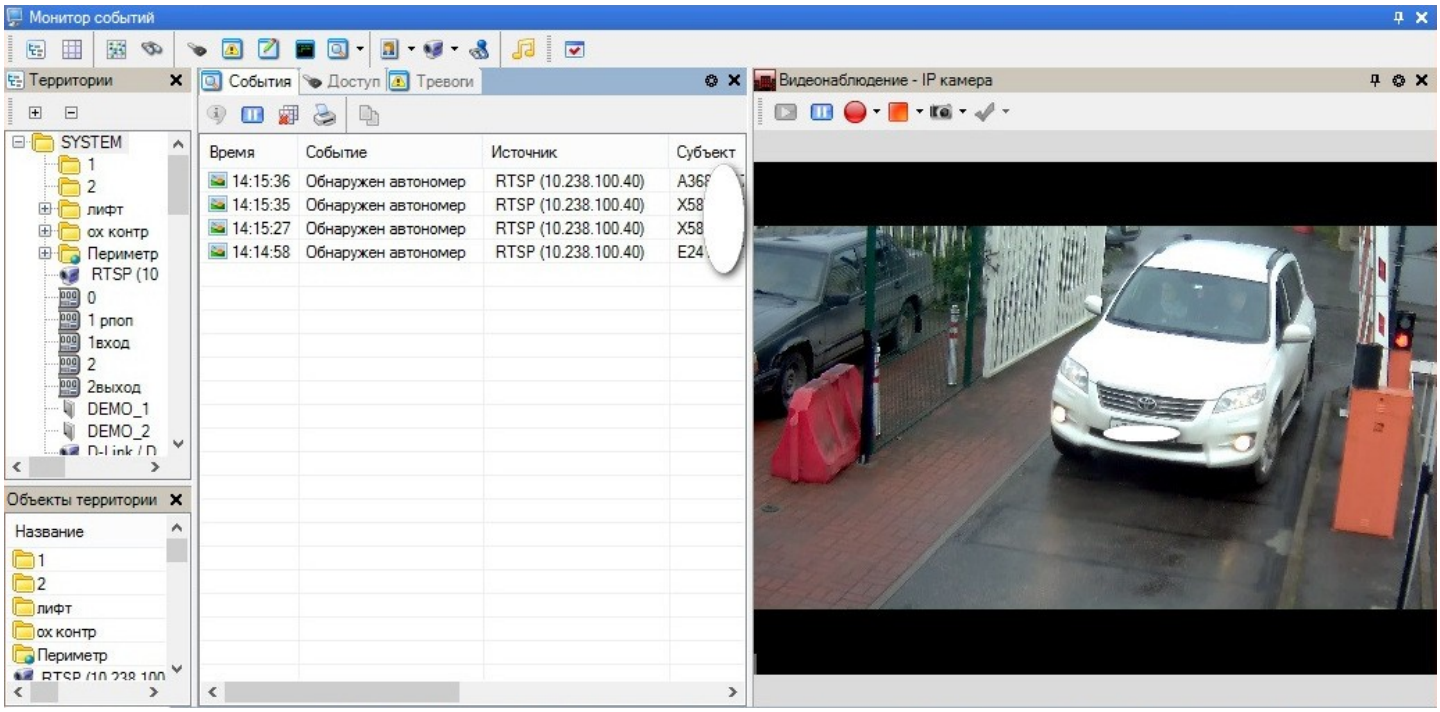
В тестовом режиме поддерживается работа максимум на 2 камерах.

Для работы модуля необходимо в карточке видеокамеры на вкладке *Настройки*, из раскрывающегося списка *Распознавание номеров* выбрать *Программное распознавание*:



Модуль распознает только стандартные российские номера.

Теперь, при попадании автомобильного номера в поле видимости камеры, в монитор событий поступает сообщение о событии "Обнаружен автономер":



Используя данный модуль, можно [создать автопроходную](#)[584] .

11.6.2 Система Dallmeier

В данном разделе описан не поддерживаемый в настоящее время модуль интеграции со снятым с производства продуктом Dallmeier - DI-NPR.

Для использования подсистемы распознавания номерных знаков автомобилей Dallmeier она должна быть предварительно настроена собственными средствами.

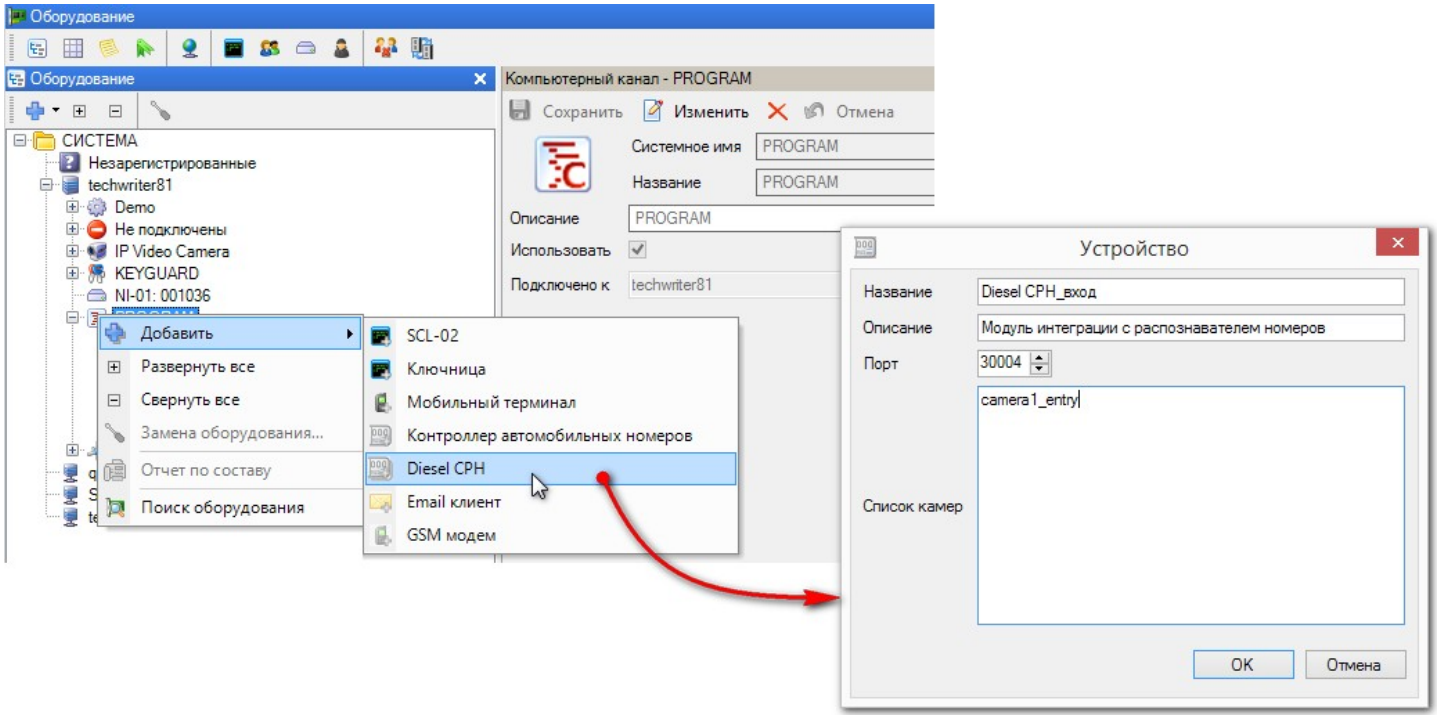
Если такая настройка произведена, можно с использованием программного контроллера и редактора заданий системы ParsecNET 3 организовать автомобильную проходную.

Создание и настройка устройства Diesel CPH

Компонент Diesel CPH (Система Распознавания Номеров) предназначен для получения информации о распознанном автомобильном номере от подсистемы Dallmeier.

На программном канале создайте устройство, внеся название, описание, указав номер порта, который будет "слушать" устройство, и заполнив список камер. Список должен состоять из записанных с новой строки идентификаторов камер, которые использует подсистема Dallmeier.

Если организуется автомобильная проходная с отдельными камерами на вход и на выход, необходимо создать два устройства Diesel CPH - на вход и на выход:



11.6.3 Автопроходная на основе программного контроллера

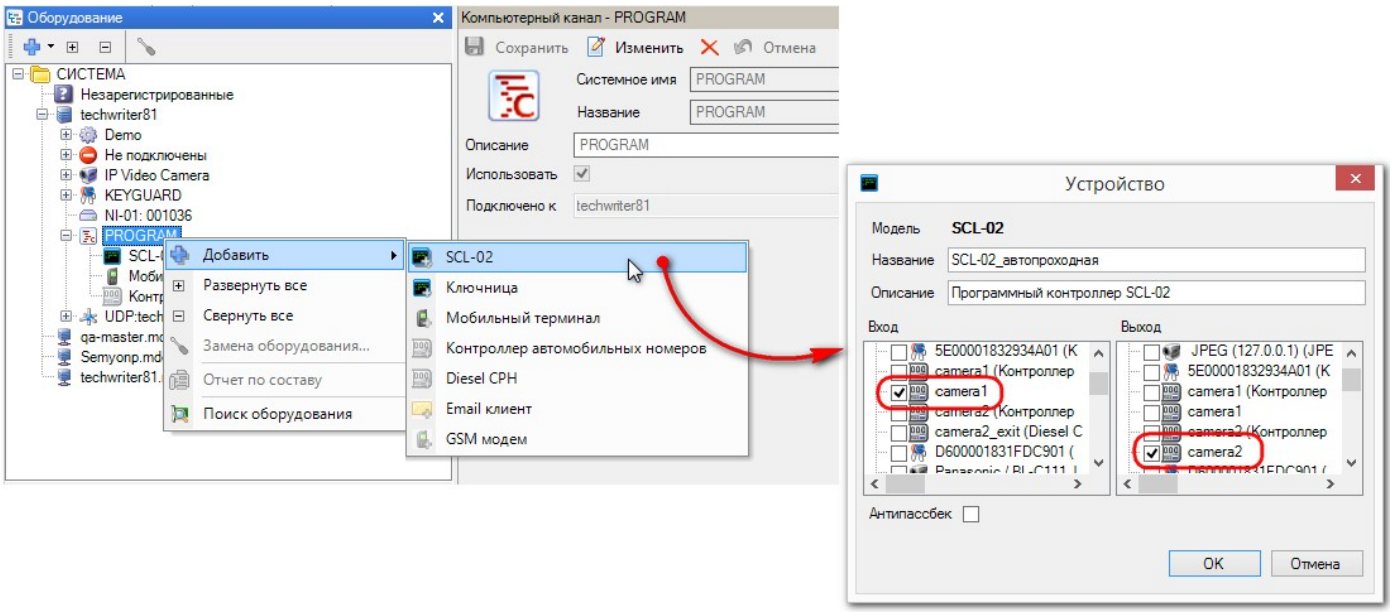
Если для распознавания автономеров используются собственный модуль **Parsec** либо системы видеонаблюдения **GOALCity, TRASSIR, Macroscop** или **Hikvision**, общий алгоритм создания автоматизированной автопроходной будет следующим:

1. Создайте программный контроллер и назначьте ему в качестве источника идентификационных данных видеокамеры на въезд и/или на выезд;
2. Создайте группу доступа, которая будет назначаться всем автомобилям, имеющим разрешение на въезд и/или выезд с охраняемой территории;
3. Добавьте в эту группу доступа созданный на первом шаге программный контроллер. Теперь при распознавании номерного знака автомобиля (событие "Обнаружен автономер") программный контроллер будет формировать в системе событие "Нормальный вход по ключу" или "Нормальный выход по ключу", если этот номер входит в группу доступа, созданную на втором шаге;
4. При помощи редактора заданий организуйте открытие шлагбаума при возникновении событий "Нормальный вход по ключу" или "Нормальный выход по ключу". Источником данных событий при этом служит программный контроллер.

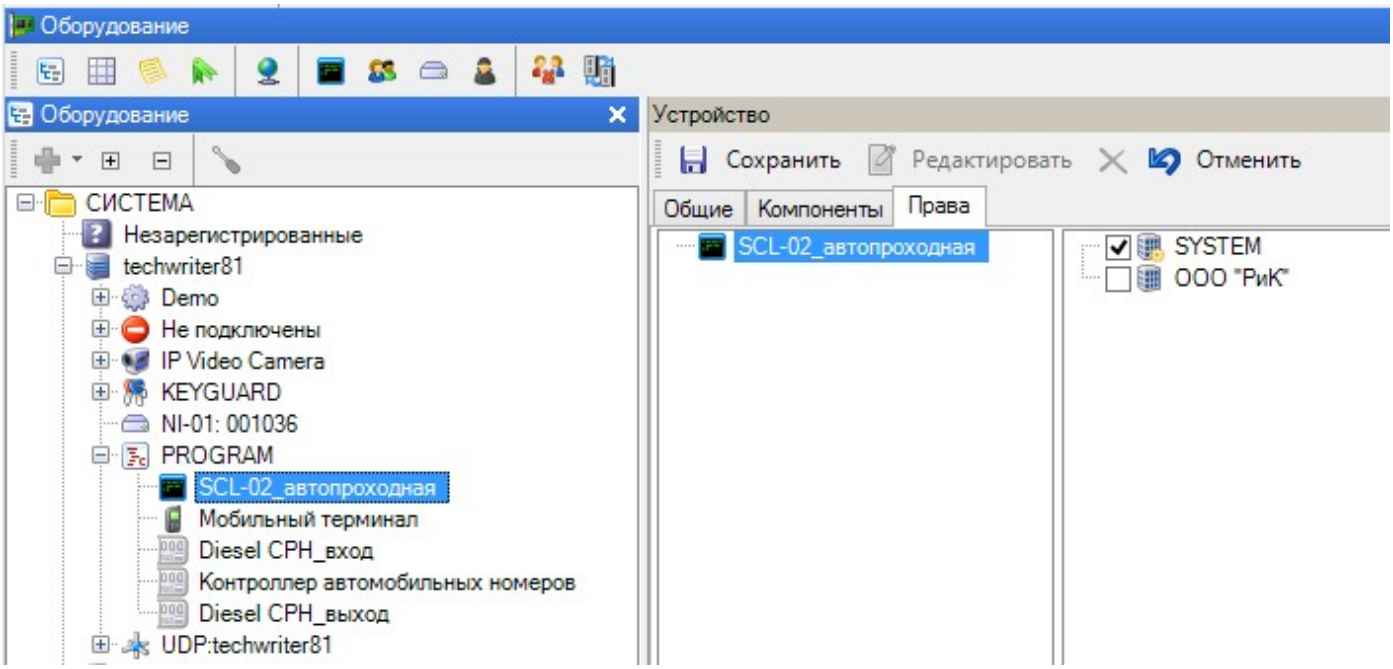
Создание и настройка контроллера

Программный контроллер по выполняемым функциям аналогичен стандартному контроллеру системы доступа с той разницей, что он работает на ПК, используя поступающую извне идентификационную информацию.

Созданному программному контроллеру, который будет обрабатывать сигналы от устройств распознавания номеров, назначьте в качестве источника сигнала видеокамеры на вход и на выход:



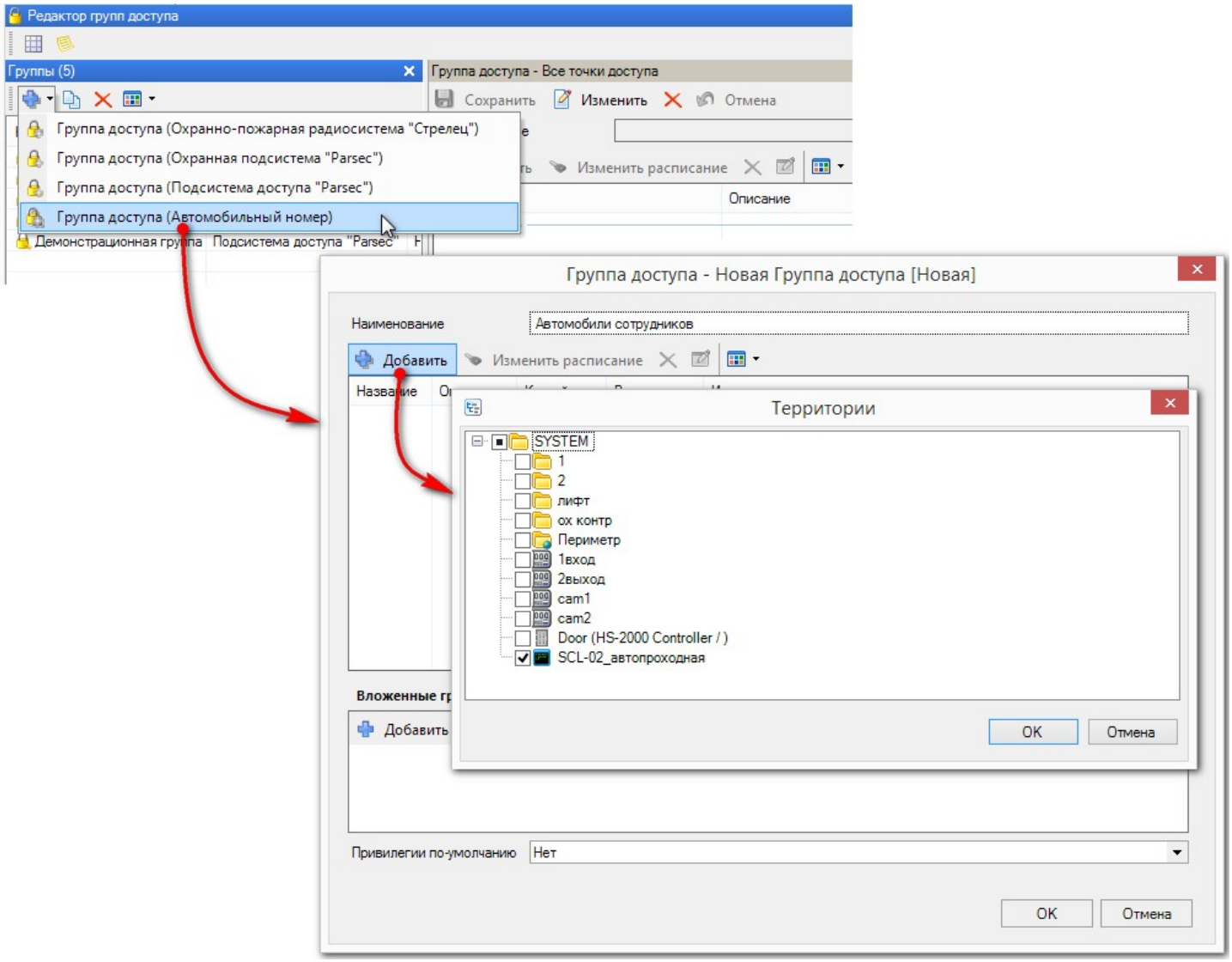
Распределите созданный контроллер в организацию - в нашем примере в базовую организацию "SYSTEM":



Теперь включите программный контроллер в группу доступа и назначьте эту группу автомобилям, которые имеют право ездить через созданную автопроходную.

Создание группы доступа

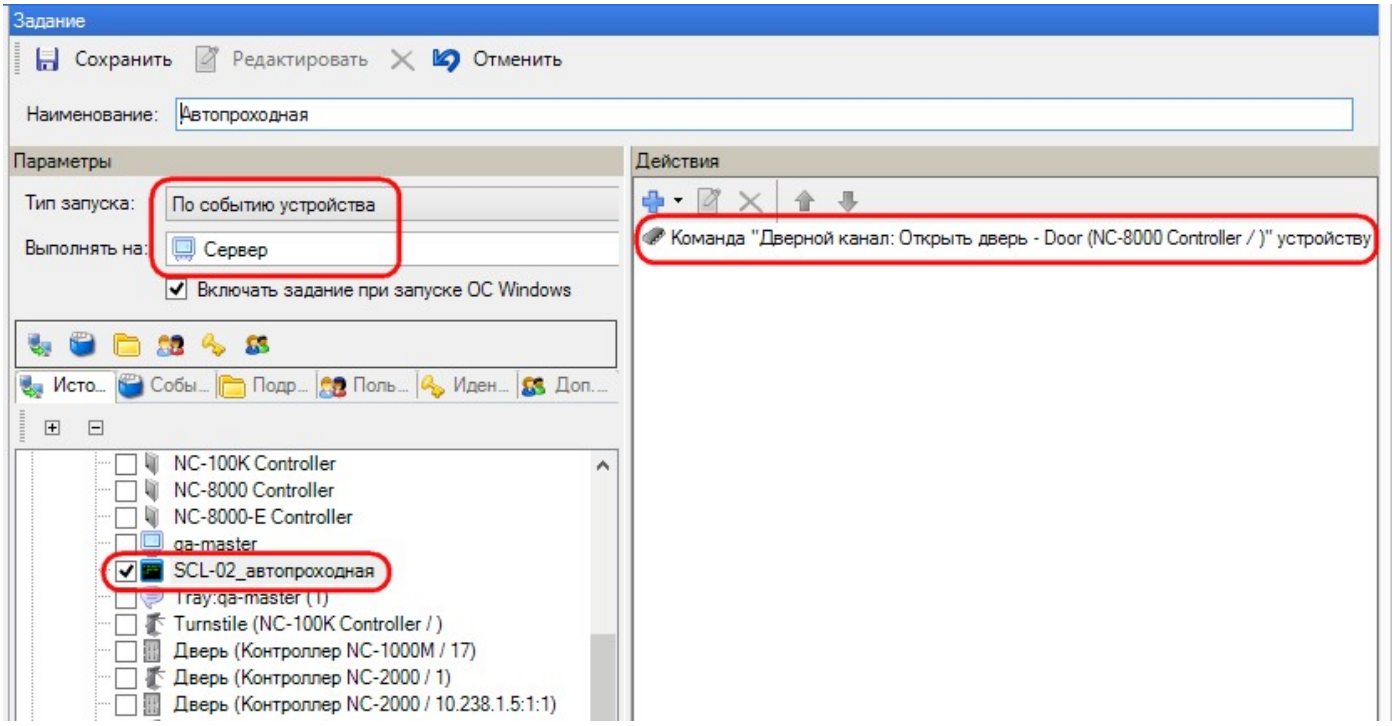
Для транспортных средств в качестве субъектов доступа существует специальный тип группы доступа:



При создании в редакторе персонала нового субъекта доступа типа "автомобиль" назначить ему можно будет только группу типа "Группа доступа (Автомобильный номер)".

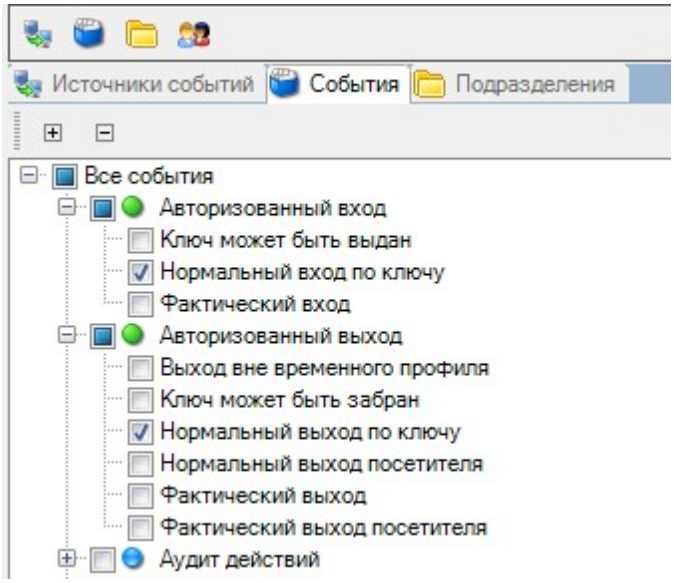
Создание задания

В редакторе заданий создайте задачу, которая работает по событиям от программного контроллера и посылает команду другому устройству:

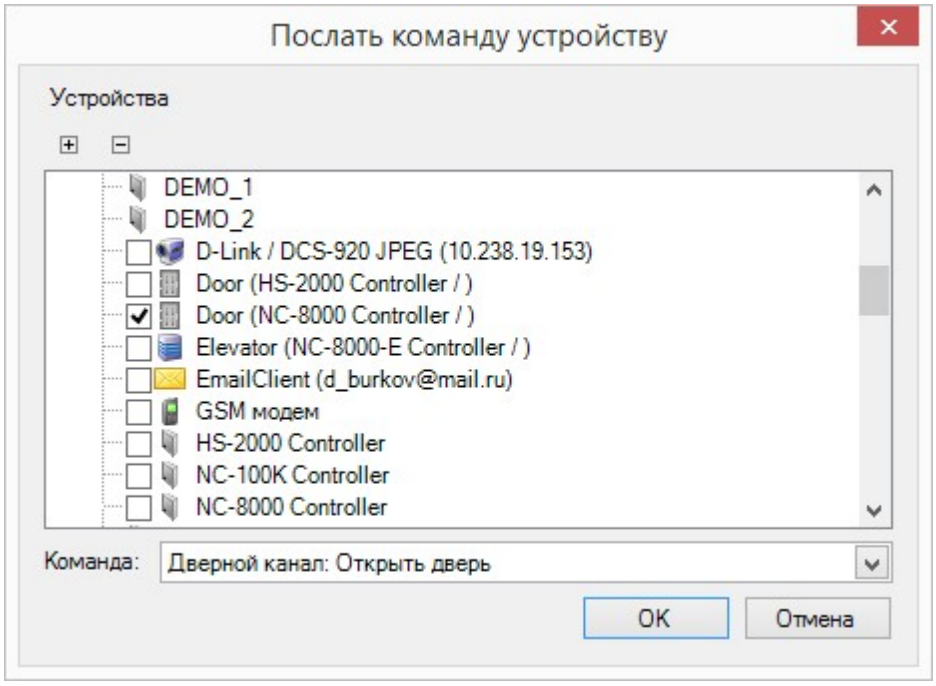


Обратите внимание, что источник данных доступен для выбора только тем организациям, операторам которых (при создании источника) предоставлено право работы с ним.

В качестве входных событий выбираем событие "Нормальный вход по ключу" и "Нормальный выход по ключу", которые будет генерировать программный контроллер при факте распознания автомобильного номера, соответственно, при въезде и выезде:



На выходе будем управлять реле контроллера, к которому, например, можно подключить привод ворот:



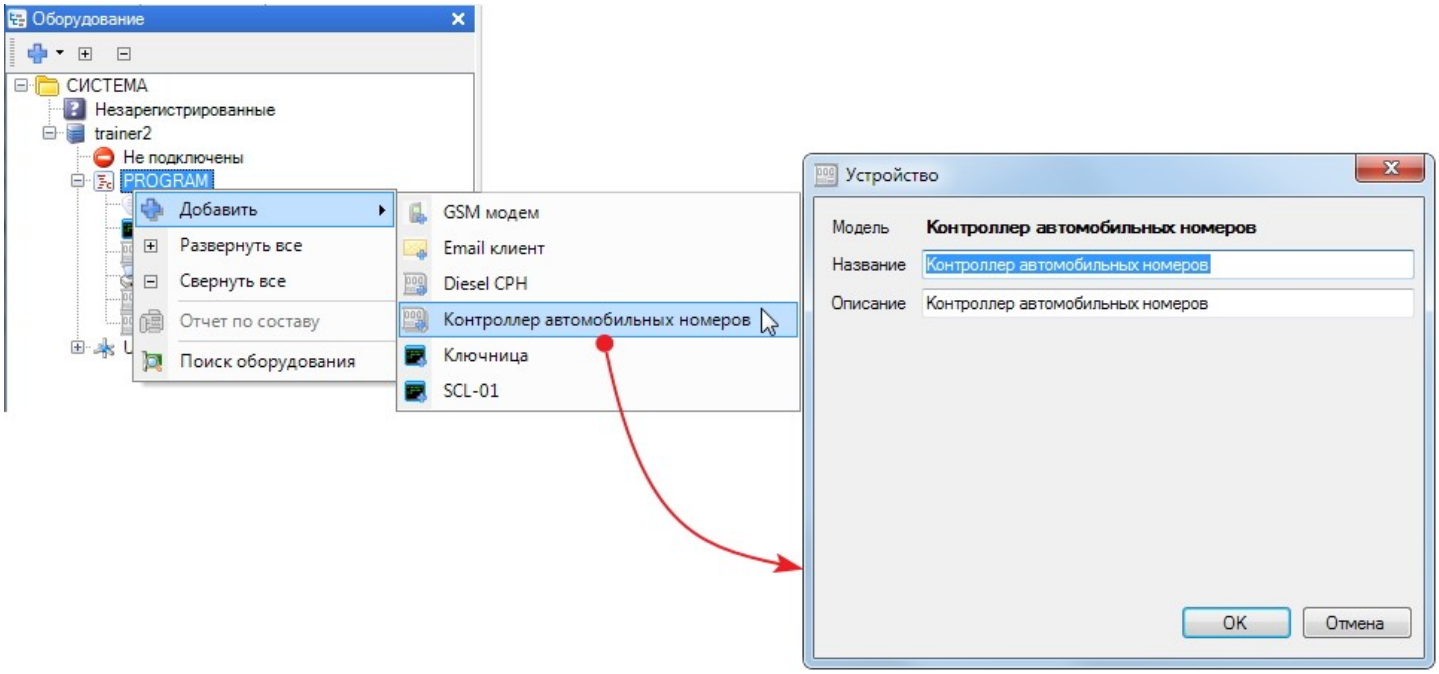
11.6.4 Контроллер автомобильных номеров

Контроллер автомобильных номеров предназначен для обеспечения взаимодействия с системой распознавания автономеров NumerOK, системой видеонаблюдения ИСБ "Интеллект" и камерами Mobotix, а также для интеграции с ParsecNET 3 любых иных систем видеонаблюдения, обладающих собственными средствами для распознавания номерных знаков транспортных средств. Для использования такой системы распознавания номерных знаков автомобилей она должна быть предварительно настроена своими средствами и на выходе предоставлять сведения о распознанном автомобильном номере в xml-файле[591] с заданной структурой.

Если такая настройка произведена, можно с использованием программного контроллера и менеджера заданий системы ParsecNET 3 организовать автомобильную проходную.

Создание и настройка контроллера автомобильных номеров

На программном канале создайте контроллер, введя название и, при необходимости, описание:



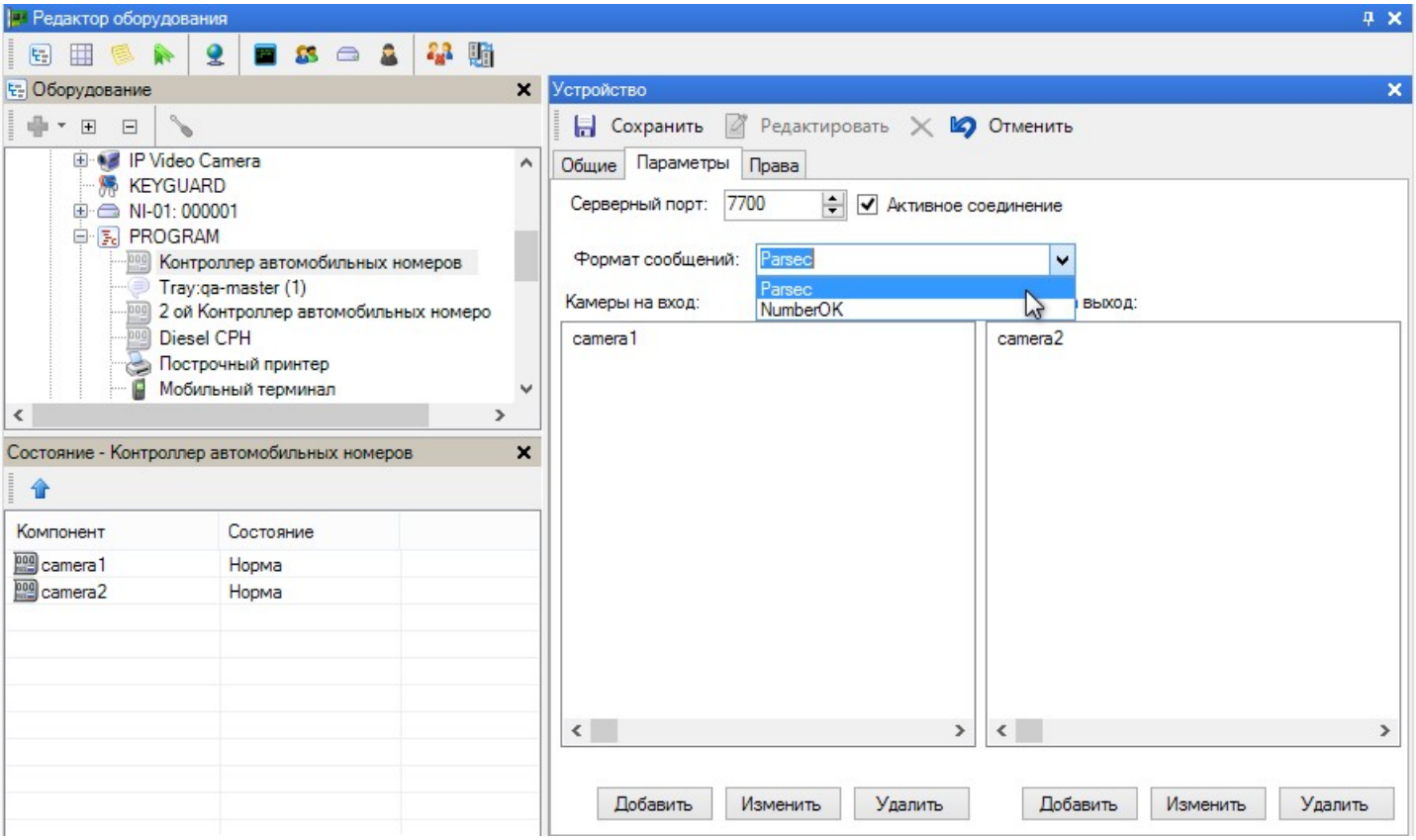
В настройках контроллера укажите номер порта, по которому будет производиться обмен.

А также укажите, какое соединение TCP/IP будет использоваться контроллером: пассивное или активное. Для этого предназначен флажок *Активное соединение.*

Если флажок *Активное соединение* стоит, то модуль будет сам пытаться установить соединение по указанному в настойках порту на локальном хосте (127.0.0.1).

Если флажок снят, то модуль ожидает соединения по выбранном порту.

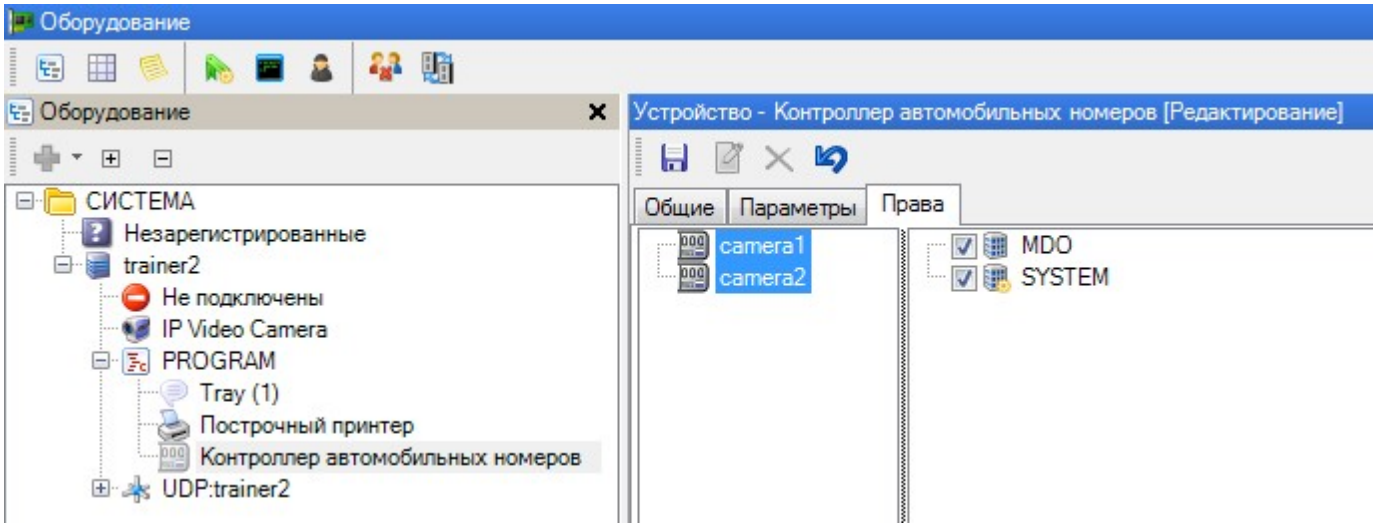
При использовании для распознавания автономеров ИСБ "Интеллект" или ПО NumberOK флажок "Активное соединение" должен быть установлен.



В поле *Формат сообщений* выберите, как будет работать контроллер:

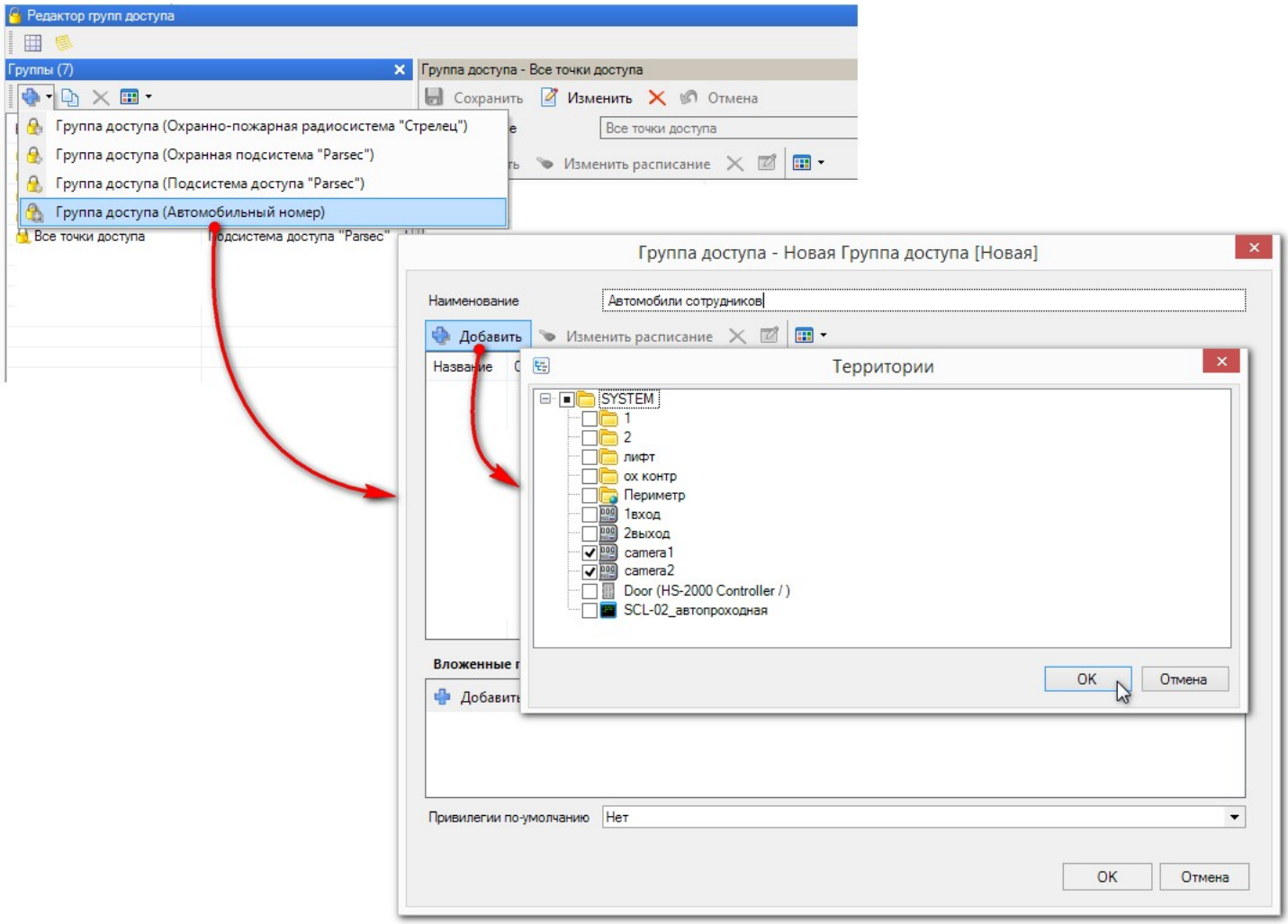
- "Parsec" - для работы[503] с ИСБ "Интеллект" и другими внешними системами распознавания автономеров. На панели *Камеры на вход* и *Камеры на выход* добавьте значения параметра cam-id[591] соответственно для камер на вход и на выход;
- "NumberOK" - для работы ПО NumberOK[591]. Если выбрана работа с ПО NumberOK[591], то на панель *Камеры на вход* добавьте номер видеопотока, настроенного на направление "въезд", а на панель *Камеры на выход*, соответственно, - номер видеопотока на выезд;
- "Mobotix" - для работы с камерами Mobotix[598], имеющими функцию распознавания автономеров. На панель *Камеры на вход* добавляются уникальные идентификаторы камер, направленных "въезд", а на панель *Камеры на выход*, соответственно, - идентификаторы камер на выезд

На вкладке *Права* распределите камеры созданного контроллера в организацию - в данном примере в организации "MDO" и "SYSTEM":



Теперь включите камеры контроллера автомобильных номеров в группу доступа и назначьте эту группу автомобилям, которые имеют право доступа на охраняемую территорию.

Для транспортных средств в качестве субъектов доступа существует специальный тип группы доступа:



При создании в редакторе персонала нового субъекта доступа типа "автомобиль" назначить ему можно будет только группу типа "Группа доступа (Автомобильный номер)".

Далее можно создать задачу[601] "открыть шлагбаум если у автомобиля с распознанным номером есть право доступа".

11.6.4.1 Структура XML-документа

Подраздел предназначен для специалистов, производящих интеграцию системы распознавания автомобильных номеров и СКУД ParsecNET 3.

Сведения об автомобильном номере от внешней системы распознавания должны передаваться в СКУД ParsecNET 3 в xml-документе со следующей структурой:

<?xml version="1.0" encoding="UTF-8"?>

<CAR_PLATE version="1.0" direction = "in" cam-id = "camera1" time = "2002-05-30T09:00:00" plate = "x456tt198" plate_mask = "RUS">

<!-- base64jpg -->

</CAR_PLATE>

Атрибуты элемента CAR_PLATE:

- version (обязательный): внутренний параметр, версия протокола, должен быть = "1.0";
- direction (обязательный): in - направление движения "к камере". Любые другие значения приводят к тому, что файл игнорируется системой;
- cam-id (обязательный): идентификатор камеры;
- time (обязательный): дата/время события в формате Internet time;
- plate (обязательный): распознанный номер, латинские буквы и цифры;
- plate_mask (необязательный): маска замены символов в распознанном номере. В текущий момент используется маска "??????*", где
  - ? - означает, что символ надо оставить как есть;
  - * - этот символ и все символы после него - игнорируются.

Если содержимое элемента CAR_PLATE не пустое, то ожидается, что оно представляет собой картинку или фрагмент картинки с камеры в формате base64.

11.6.5 Распознавание автономеров NumberOK

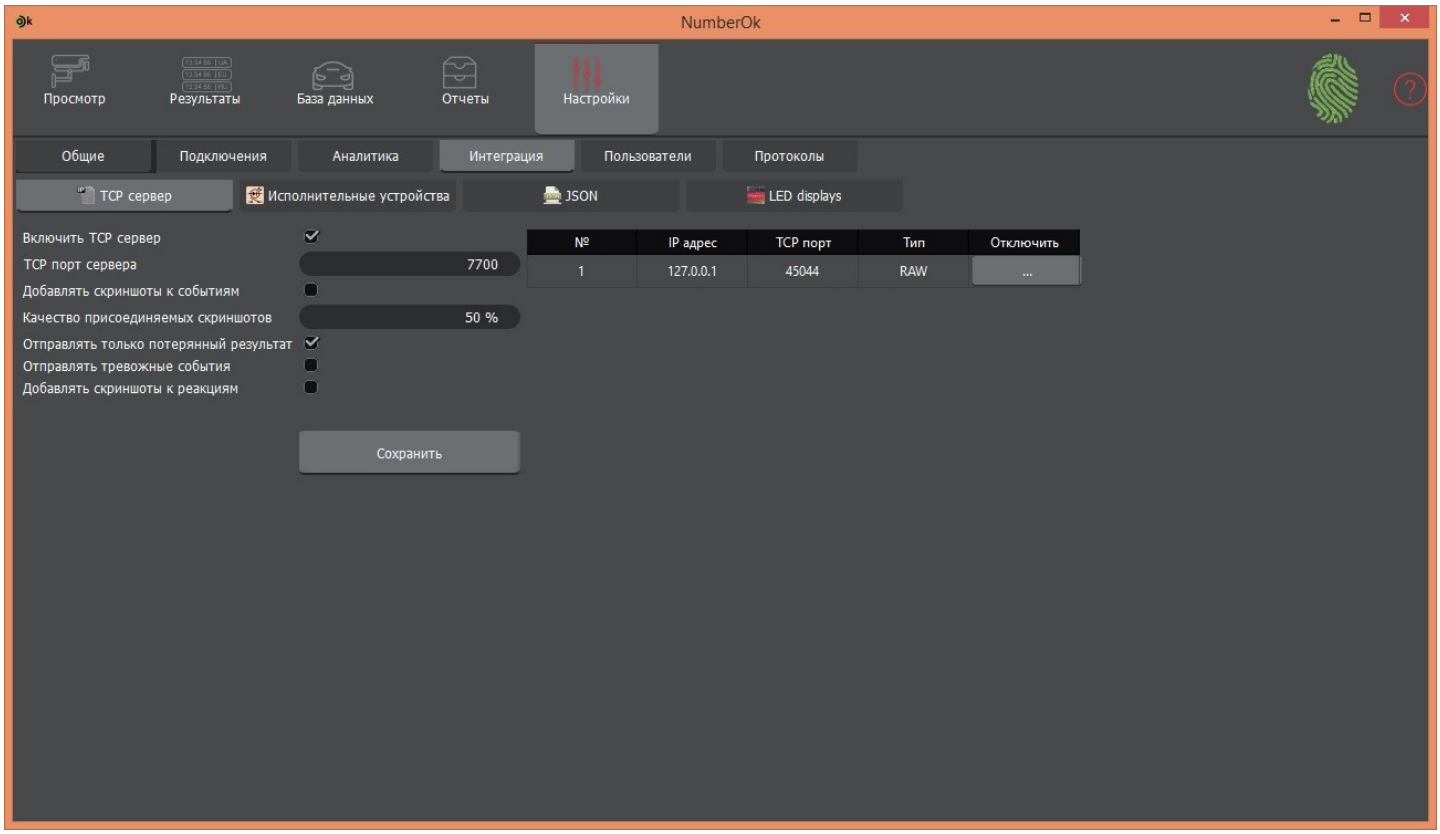
Для использования ПО распознавания номерных знаков автомобилей **NumberOK** необходимо предварительно установить и настроить его собственными средствами.

После этого, можно с использованием программного контроллера и менеджера заданий системы ParsecNET 3 организовать автомобильную проходную.

Нюансы настройки NumberOK

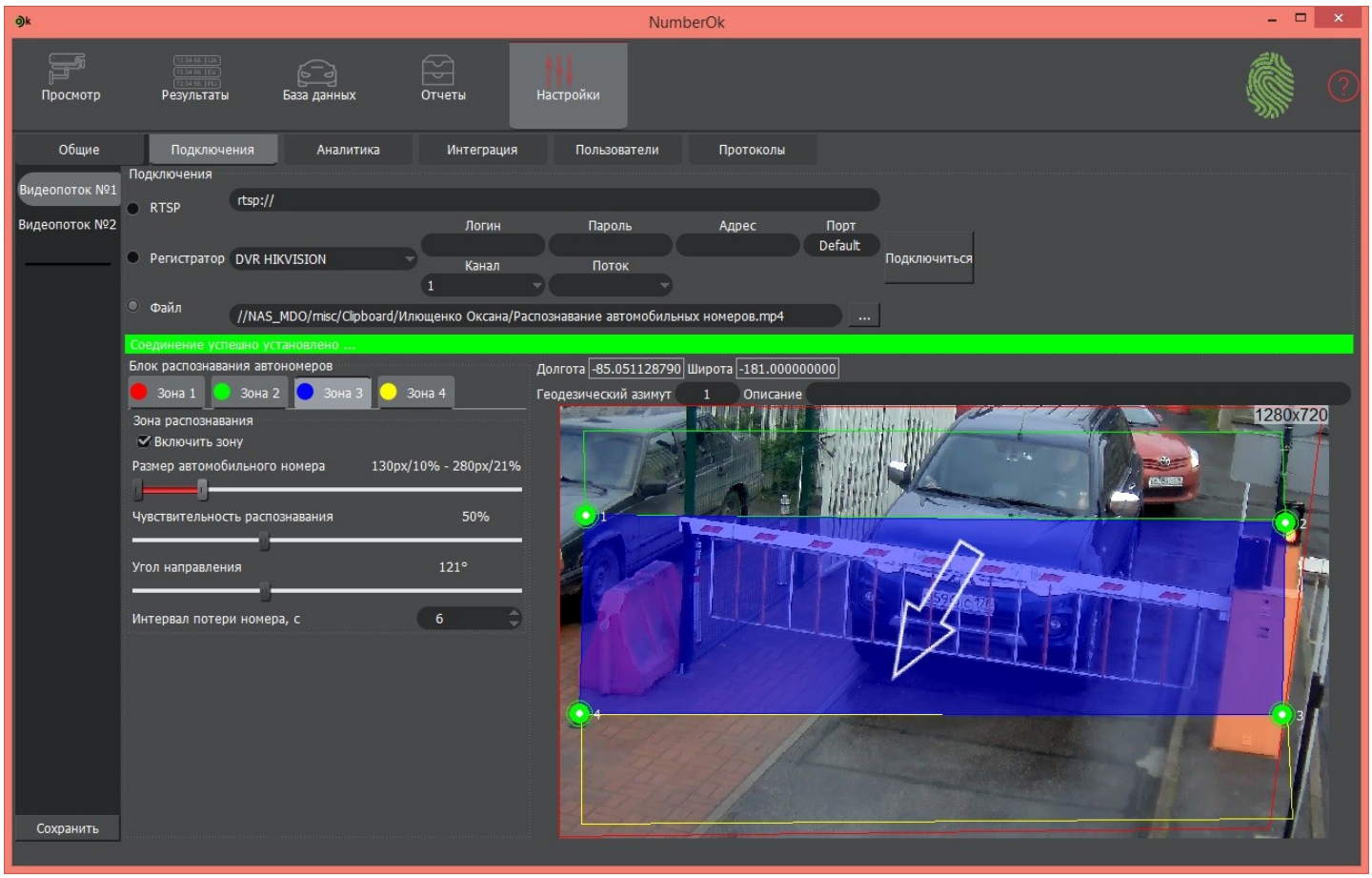
Чтобы корректно организовать взаимодействие ПО NumberOK с ПО ParsecNET, необходимо учесть следующие важные моменты:

1. В ПО NumberOK разделе *Настройки - Интеграция* необходимо установить флажок *Включить TCP сервер* и указать *TCP порт сервера* (если необходимо, обратитесь к системному администратору), после чего сохранить внесенные изменения:



Запомните TCP порт сервера, он понадобится для настройки ПО ParsecNET.

2. ПО NumberOK позволяет определить направление проезда транспортного средства. В целях обеспечения безопасности доступа нас интересует направление на въезд и на выезд. На рисунке ниже показана настройка камеры (*Видеопоток №1*) на въезд. Номера видеопотоков, настроенных на въезд и на выезд, необходимо указать в [настройках контроллера автомобильных номеров](#)[589].



Настройка ПО ParsecNET

1. Создайте контроллер автомобильных номеров[588];
   - В настройках контроллера на вкладке *Параметры* укажите номер TCP порта сервера, использованный при настройке ПО NumberOK;
   - Установите флажок *Активное соединение* (обязательно);
   - В поле *Формат сообщений* выберите значение *NumberOK*;
   - На панели *Камеры на вход* добавьте номер видеопотока, настроенного на направление "въезд";
   - На панели *Камеры на выход* добавьте номер видеопотока, настроенного на направление "выезд";
   - На вкладке *Права* распределите камеры созданного контроллера в организацию, которая должна иметь к ним доступ;
   - Сохраните сделанные изменения.
2. Включите камеры контроллера автономеров в группу доступа и назначьте эту группу автомобилям, которые имеют право доступа на охраняемую территорию. (Обратите внимание на особенности[585] создания группы доступа);
3. Создайте задание[601] на открытие шлагбаума автопроходной.

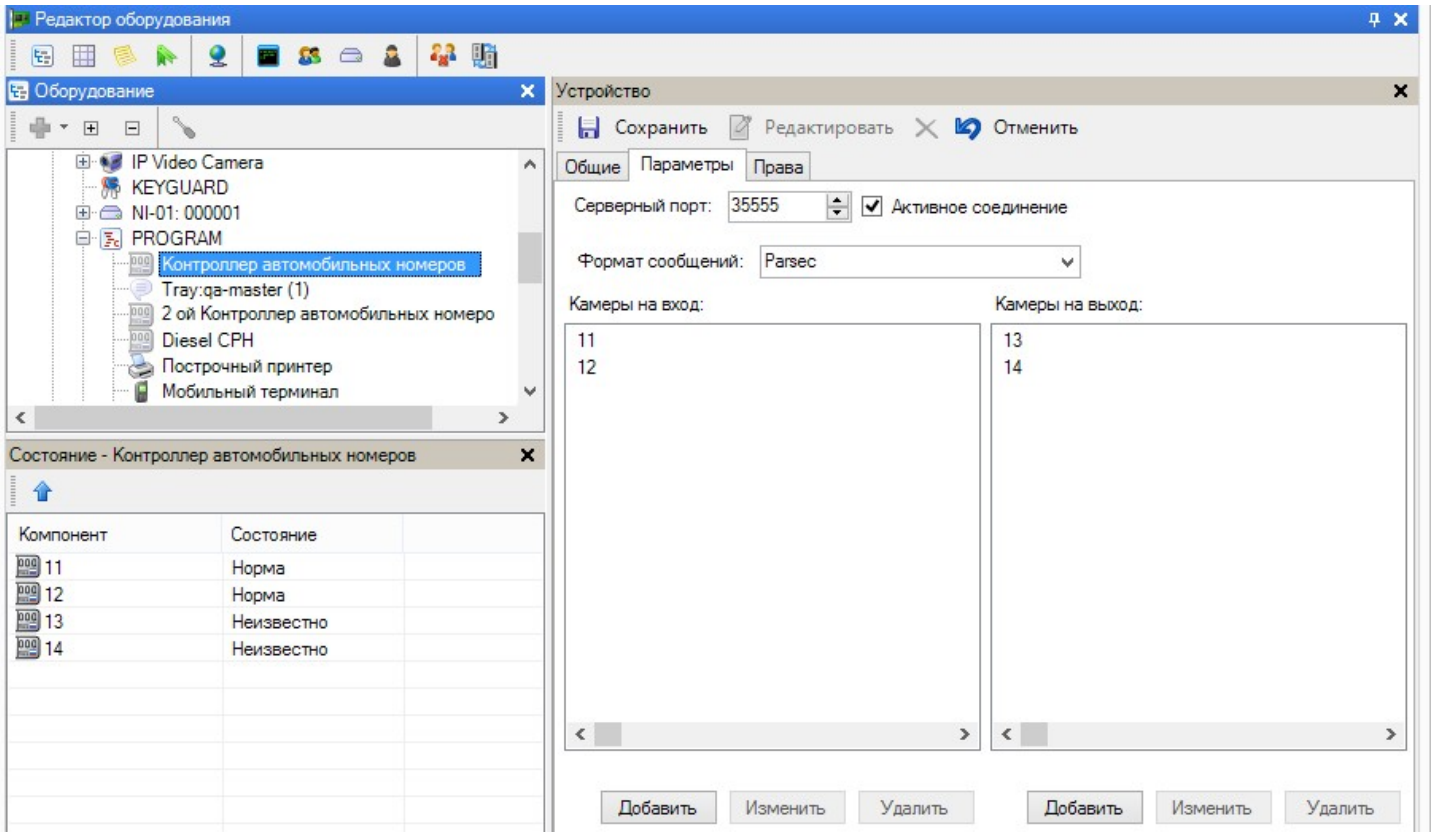
По завершении всех действий, шлагбаум будет автоматически открываться, когда имеющий допуск автомобиль въедет в зону распознавания автономера в разрешенное ему время.

11.6.6 Распознавание автономеров ИСБ "Интеллект"

Для взаимодействия со СКУД ParsecNET 3 при распознавании автомобильных номеров необходимо использовать базовое ПО ИСБ "Интеллект" версии не ниже 4.10.3 и модуль Авто-Интеллект версии не ниже 5.4.0.1571.

Использование ИСБ "Интеллект" для распознавания номеров транспортных средств имеет свои особенности:

1. В то время, как сервер ИСБ "Интеллект" может быть установлен[518] на любой машине СКУД Parsec, компонент "Сервер распознавания автомобильных номеров" ИСБ "Инетллект" и контроллер автомобильных номеров на канале PROGRAM должны быть установлены на одном ПК, предназначенном для распознавания номеров;
2. В контроллере автомобильных номеров на вкладке *Параметры* необходимо установить следующие настройки:
   - указать серверный порт 35555;
   - установить флажок *Активное соединение*;
   - выбрать формат сообщения "Parsec";
   - на панелях *Камеры на вход/выход* указать ID камер (отображаются в ПО "Интеллект"), настроенных, соответственно, на вход и на выход:



- На вкладке *Права* распределите камеры созданного контроллера в организацию, которая должна иметь к ним доступ;
- Сохраните сделанные изменения.

3. Включите камеры контроллера автономеров в группу доступа и назначьте эту группу автомобилям, которые имеют право доступа на охраняемую территорию.(Обратите внимание на особенности[585] создания группы доступа);
4. Создайте задание[601] на открытие шлагбаума автопроходной.

По завершении всех действий, шлагбаум будет автоматически открываться, когда имеющий допуск автомобиль въедет в зону распознавания автономера в разрешенное ему время.

11.6.7 Распознавание автономеров Hikvision

Для распознавания номерных знаков автомобилей видеокамеры **Hikvision** специальной серии Smart IP снабжены встроенным аналитическим модулем. Камеры, имеющие встроенную функцию распознавания номеров перечислены тут.

Для использования этих камер в рамках СКУД ParsecNET необходимо предварительно установить и настроить камеры собственными средствами Hikvision. Кроме этого для корректной работы модуля интеграции с камерами Hikvision Smart IP с функцией распознавания автомобильных номеров рекомендуется в Web интерфейсе камеры произвести следующие настройки:

- В главном меню нажмите на кнопку Configuration, на левой панели выберите System -> Security, в открывшемся окне перейдите в раздел Security Service и снимите флажок *Enable Illegal Login Lock*;
- На левой панели выберите раздел Road Traffic, в раскрывающемся списке *Region* обязательно выберите "CIS" (номера стран СНГ) или "CIS and Europe". Там же в раскрывающемся списке *Select Mode* выберите "City Street".

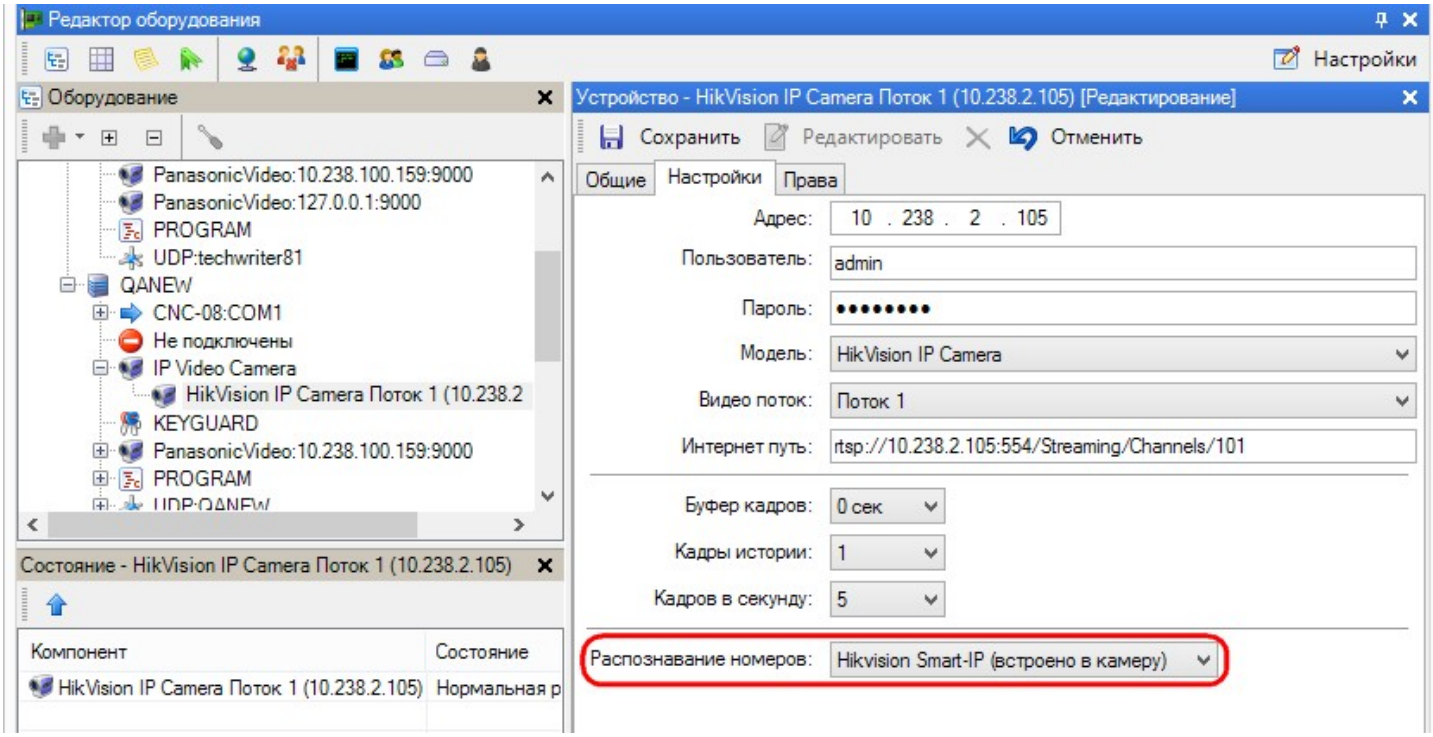
Настройка области распознавания номеров (Area Settings) возможна только через компонент ActiveX, который работает только в браузере Internet Explorer (и

только в нем отображается живое видео Live view). Настройка области распознавания производится также в разделе Road Traffic.

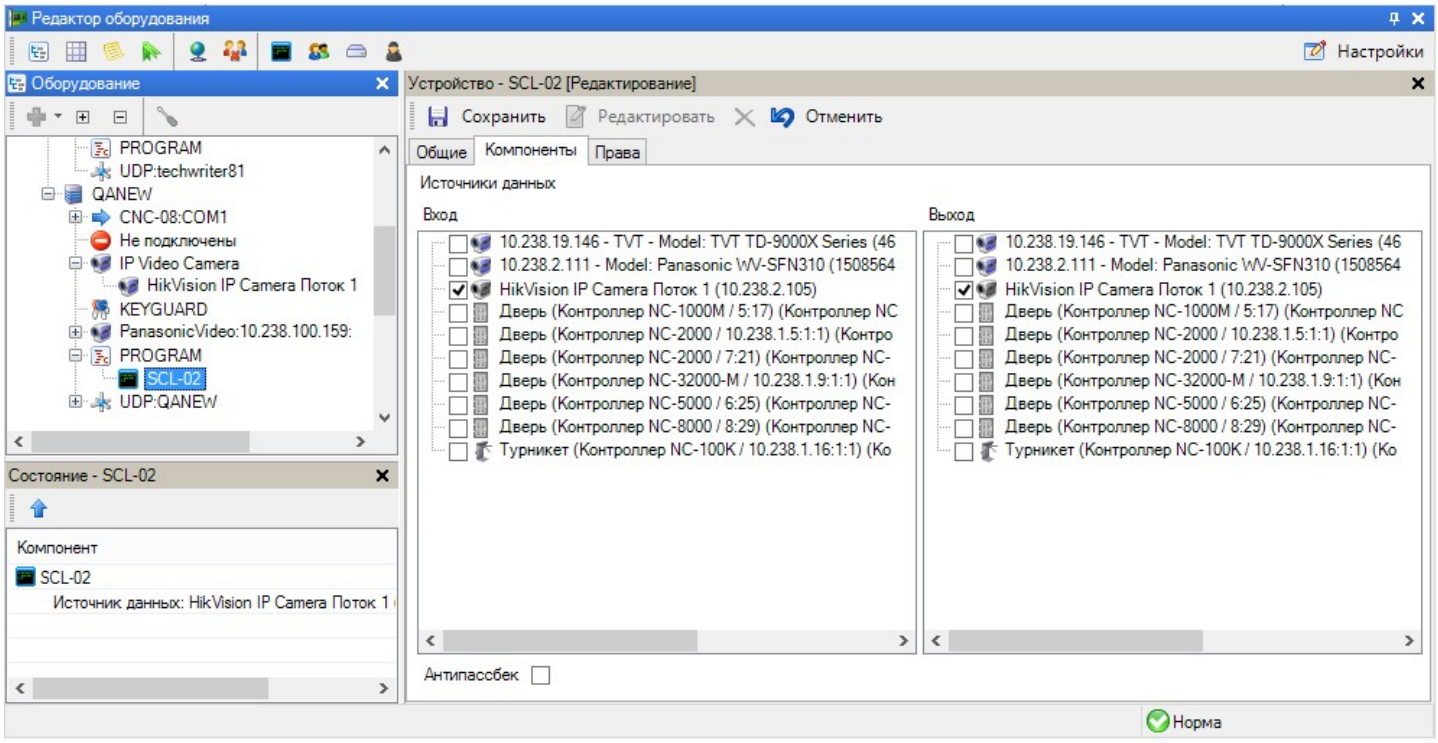
По итогам установки, для интеграции камеры в Систему необходимо знать:

- IP-адрес камеры;
- Логин и пароль, если они заданы;
- URL для форматов JPEG/MJPEG (в зависимости от количества потоков, которые выдает камера, и поддерживаемых ею форматов).

Добавление камеры в Систему производится так же, как и любой другой IP-камеры[412]. При этом в карточке устройства на вкладке *Настройки*, из раскрывающегося списка *Распознавание номеров* необходимо выбрать значение "Hikvision Smart-IP (встроено в камеру)":

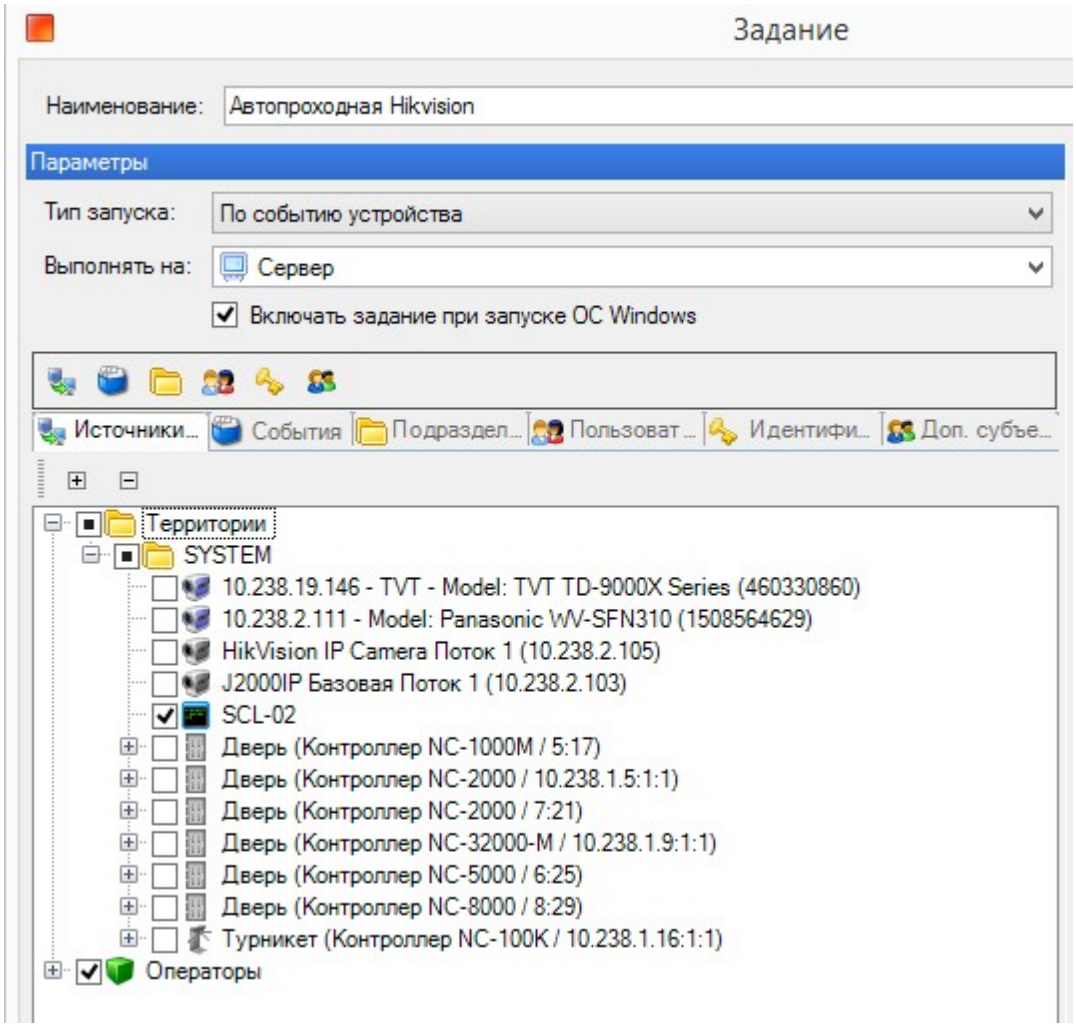


Следующим шагом необходимо создать программный контроллер[187] SCL-2. При этом источником выберите камеры Hikvision направленные соответственно на вход и на выход. Также может быть реализована точка прохода с одной камерой (как на примере ниже):

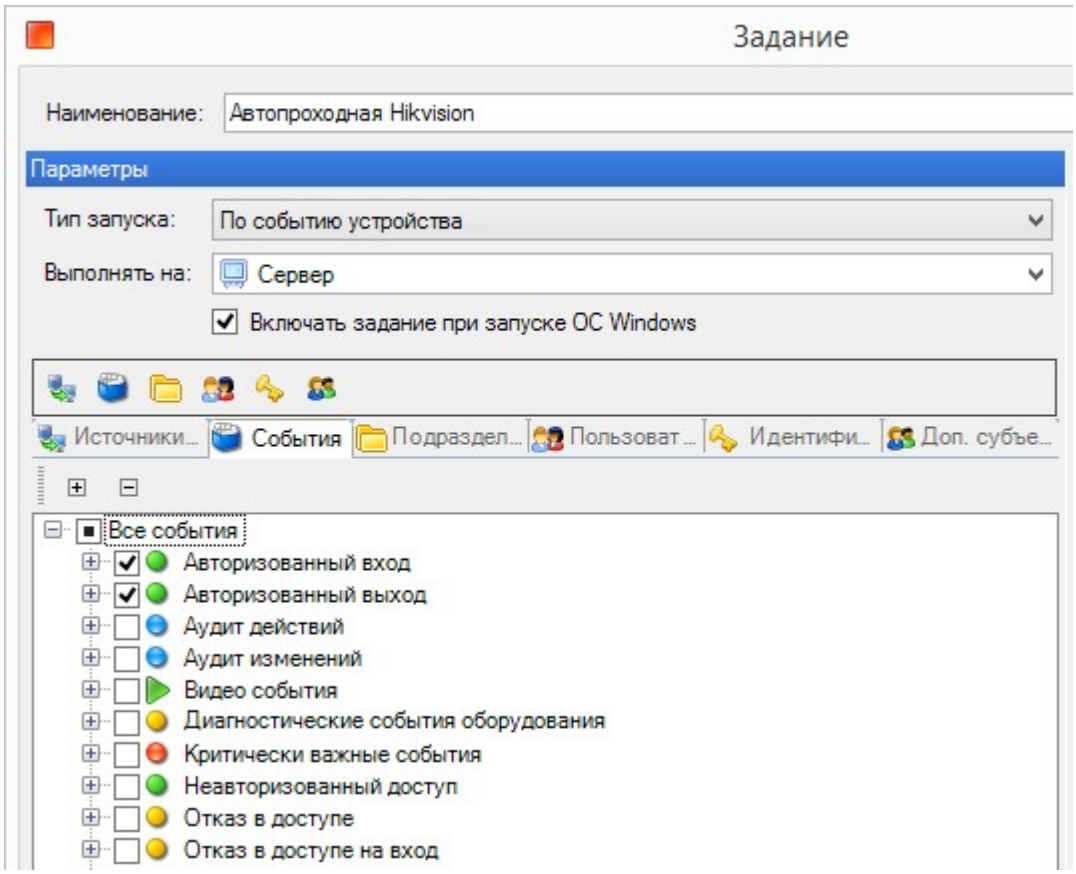


Добавьте созданный программный контроллер (источник данных) в группу доступа (либо создайте для него отдельную группу доступа) (шаг 2[189]).

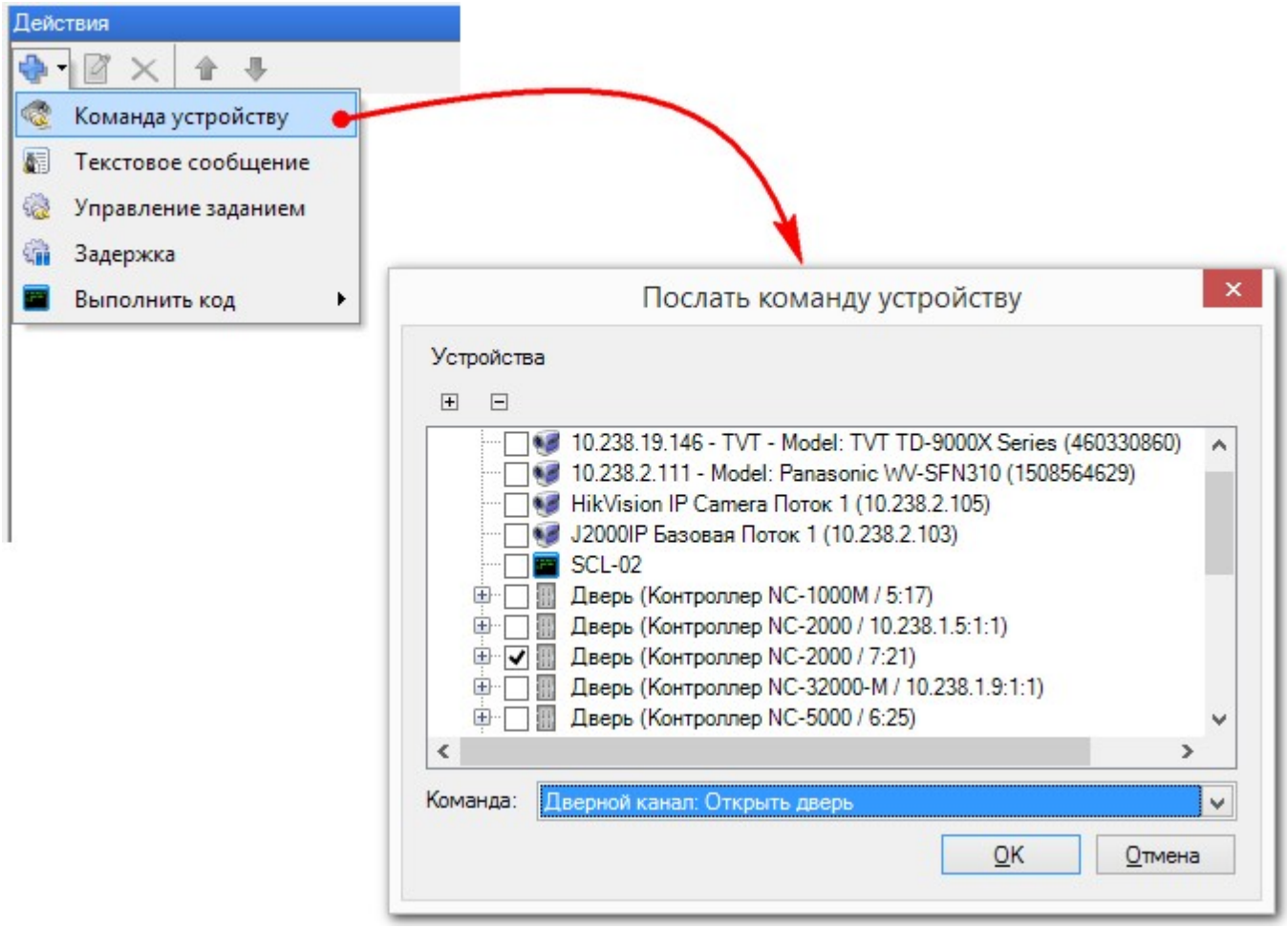
Теперь при распознании номера транспортного средства, имеющего право доступа, программный контроллер сформирует транзакцию входа. Далее на основании этой транзакции с помощью Редактора заданий[321] можно сформировать команду управления любому исполнительному устройству, например, команду шлагбауму на открытие. Другими словами, можно организовать автопроходную на основе программного контроллера[584]. При этом в качестве источников выберите созданный программный контроллер:



В качестве событий - авторизованные вход и выход:



А в качестве действия - команду контроллеру шлагбаума (или иному исполнительному устройству) на открытие:



По завершении всех действий, шлагбаум будет автоматически открываться, когда имеющий допуск автомобиль въедет в зону распознавания автономера в разрешенное ему время.

11.6.8 Распознавание автономеров Mobotix

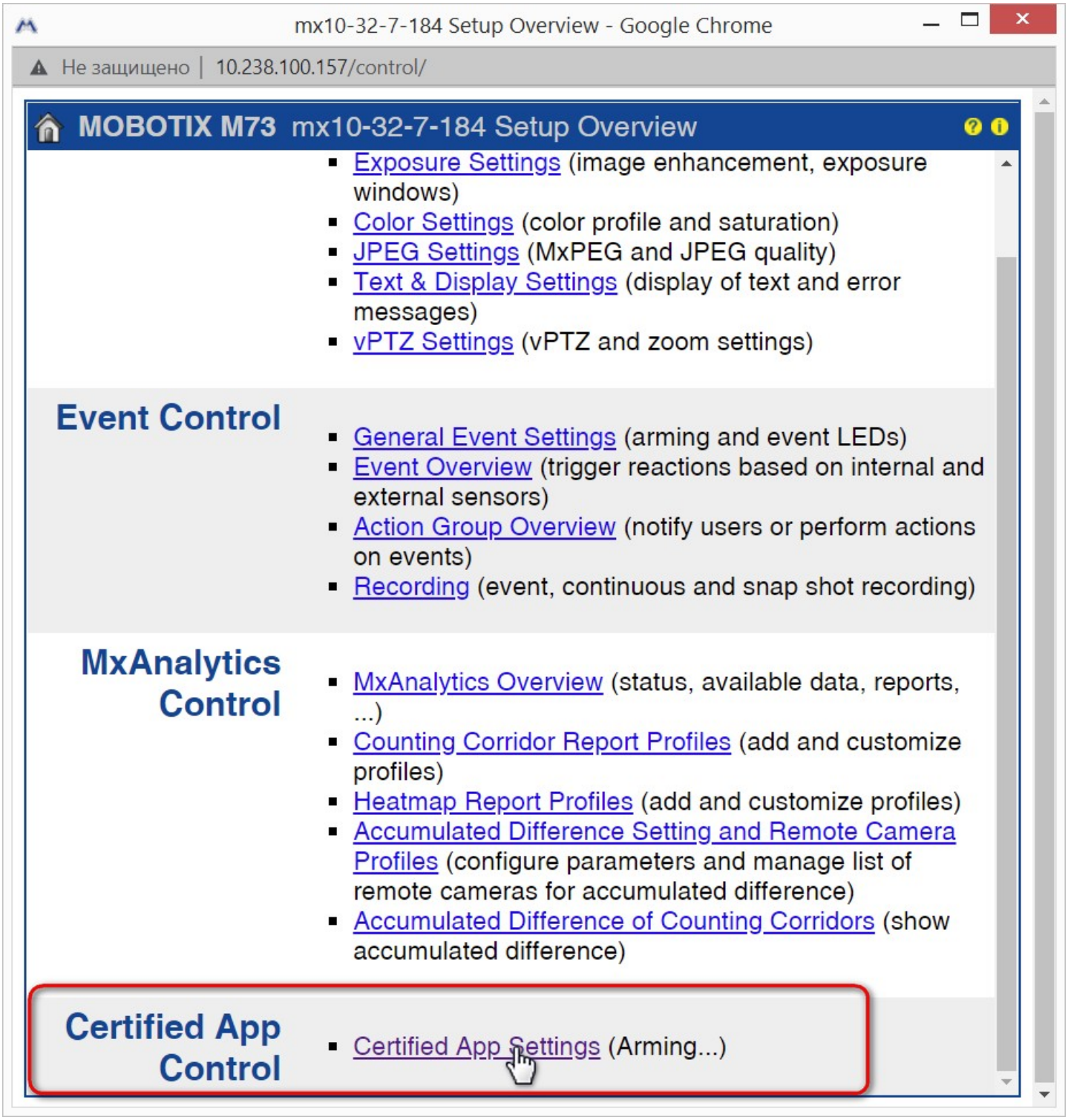
В СКУД ParsecNET 3 может использоваться функция распознавания номеров камеры Mobotix M73 High Performance IoT Camera.

Для использования функции распознавания номеров камеры Mobotix необходимо предварительно установить и настроить ее собственными средствами, при этом задав обязательные параметры, описанные в шагах ниже:

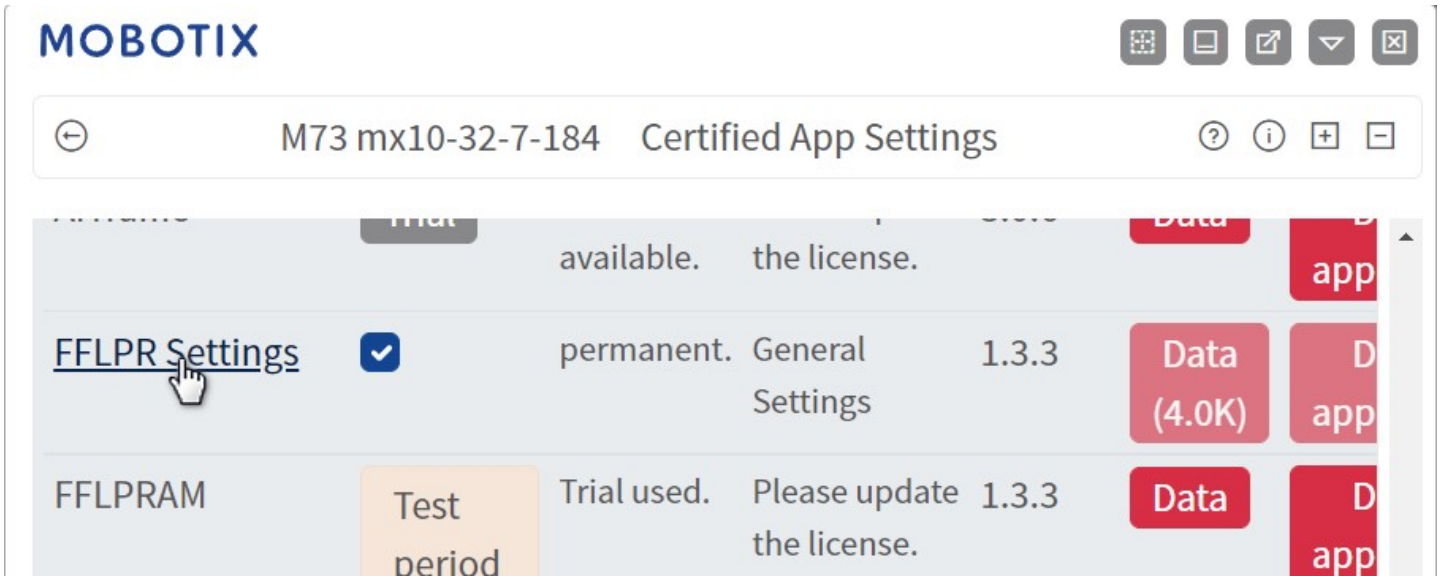
1. Введите IP-адрес камеры в поисковую строку браузера и нажмите клавишу Enter. Откроется web-интерфейс камеры;
2. Нажмите на кнопку Setup Menu:



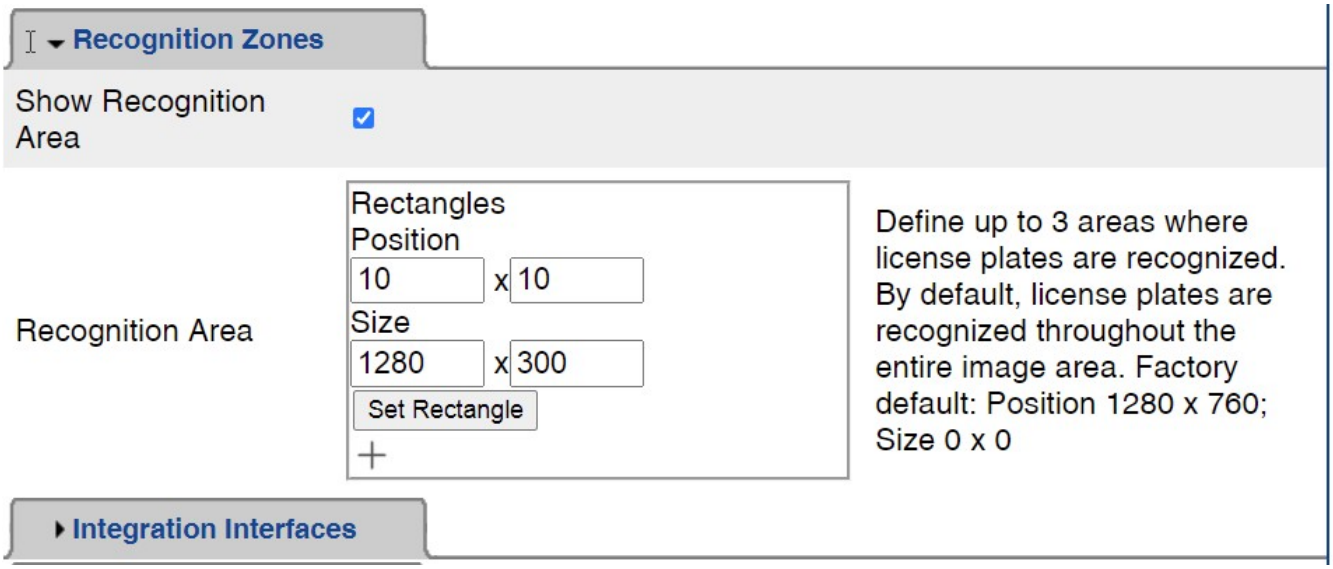
3. В появившемся окне авторизации введите логин и пароль доступа к камере;
4. Выберите раздел Certified App Settings:



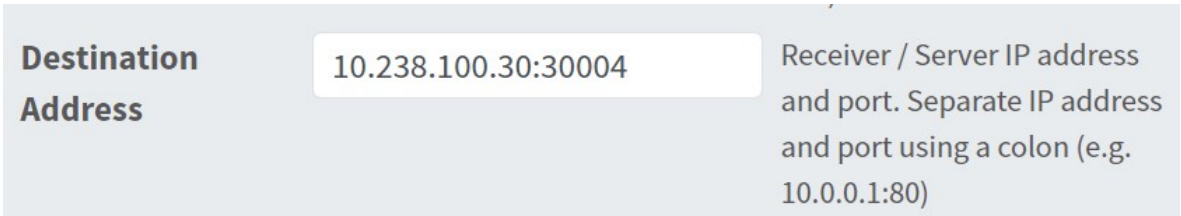
5. Прокрутите список настроек вниз, до раздела FFLPR Settings и щелкните по ссылке. Флажок должен быть установлен:



6. В разделе настроек FFLPR установите следующие значения параметров:
   - Для параметра **Region** выберите значение EU + CIS;
   - В подразделе *Recognition Zones* установите флажок **Show Recognition Area**;
   - Определите до 3 областей, в которых распознаются автомобильные номера. По умолчанию автомобильные номера распознаются по всей области изображения. Заводские настройки: положение 1280 x 760; Размер 0 x 0:



   - В подразделе Integration Interfaces установите значения параметров:
     - Флажок **Enable** - установлен;
     - **Destination Address** - укажите IP-адрес и порт того ПК, на котором будет работать контроллер автомобильных номеров Parsec. Порты в этом поле и в карточке настройки контроллера автомобильных номеров в ПО Parsec должны совпадать;



     - Для параметра **Transfer Protocol** выберите значение TCP;

- В поле **Device ID** задайте уникальный идентификатор камеры. В дальнейшем он понадобится для настройки взаимодействия с контроллером автомобильных номеров;
- Установите флажок **Event Type: New**.

7. После завершения всех настроек нажмите на кнопку *Set* (*Задать*) (для сохранения изменений) и *Close* (*Закрыть*) внизу окна;
8. Подтвердите желание сохранить изменения, нажав на кнопку ОК в появившемся окне запроса. Меню камеры закроется.

На этом настройка камеры завершена.

Далее необходимо создать и настроить контроллер автомобильных номеров.

Настройка ПО ParsecNET

1. Создайте контроллер автомобильных номеров[588]:
   - В настройках контроллера на вкладке *Параметры* укажите номер порта, использованный при настройке камеры Mobotix;
   - Флажок *Активное соединение* должен быть снят (обязательно);
   - В поле *Формат сообщений* выберите значение Mobotix;
   - На панели *Камеры на вход* добавьте уникальный идентификатор (значение поля Device ID) камеры, направленной на "въезд";
   - На панели *Камеры на выход* добавьте уникальный идентификатор (значение поля Device ID) камеры, направленной на "выезд";
   - На вкладке *Права* распределите камеры созданного контроллера в организацию, которая должна иметь к ним доступ;
   - Сохраните сделанные изменения.

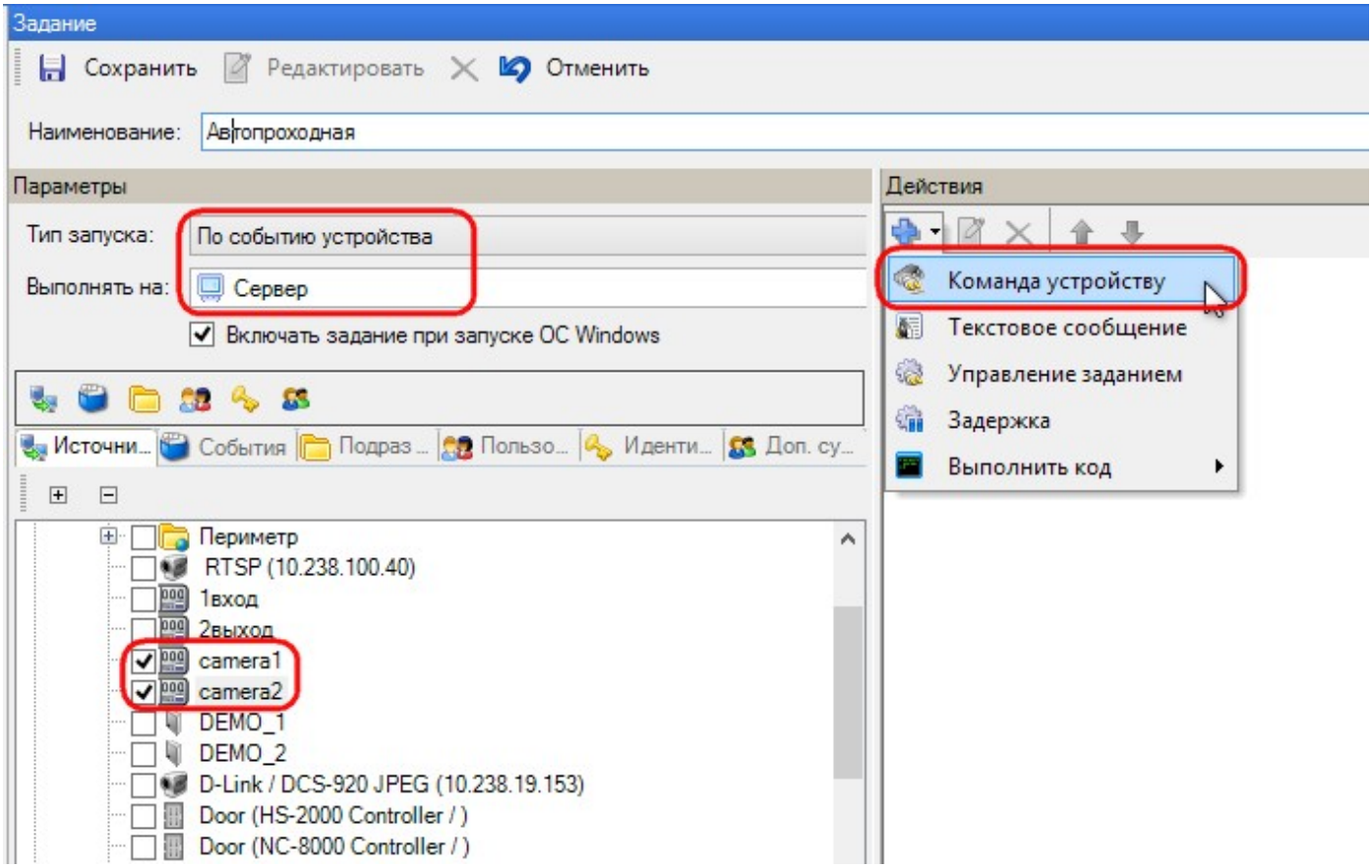
   Если есть необходимость создать автопроходную, выполните оставшиеся 2 шага.
2. Включите камеры контроллера автономеров в группу доступа и назначьте эту группу автомобилям, которые имеют право доступа на охраняемую территорию. (Обратите внимание на особенности[585] создания группы доступа);
3. Создайте задание[601] на открытие шлагбаума автопроходной.

По завершении всех 3 шагов, шлагбаум будет автоматически открываться, когда имеющий допуск автомобиль въедет в зону распознавания автономера в разрешенное ему время.

11.6.9 Автопроходная на основе контроллера автономеров

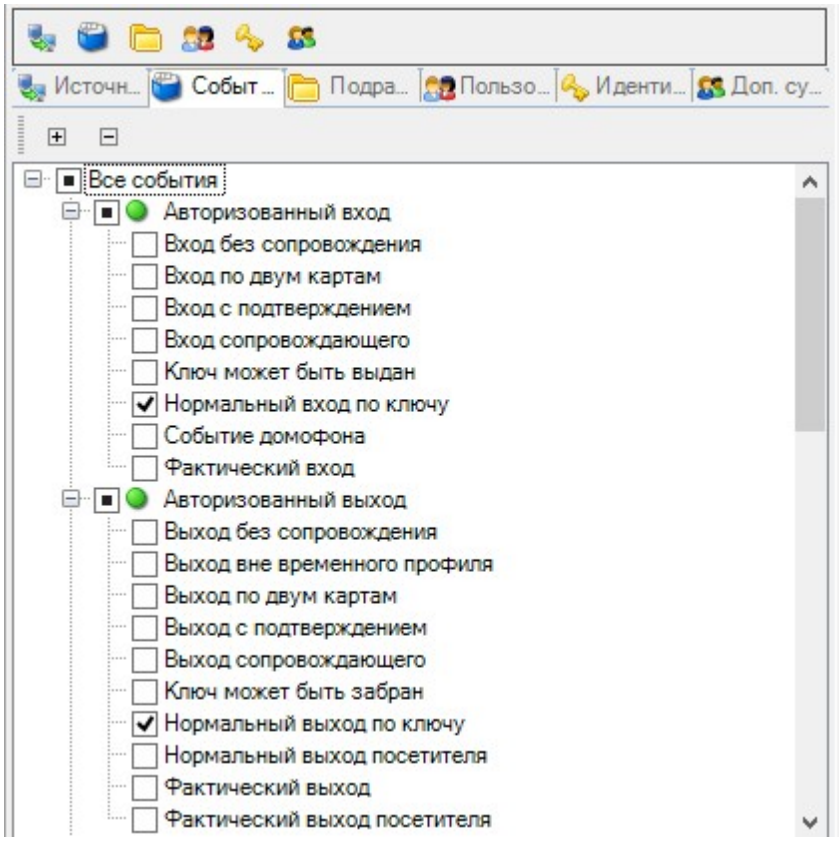
В данном разделе описывается создание автопроходной для случая, когда для распознавания автономеров используется система распознавания NumerOK[591], ИСБ "Интеллект"[593], камеры Mobotix[598] или внешние системы, передающие данные в заданном xml-формате[591].

Например, нам нужно организовать контроль въезда и выезда автотранспорта с территории. В редакторе заданий[321] создаем задачу, которая работает по событиям от контроллера автономеров и посылает команду другому устройству:

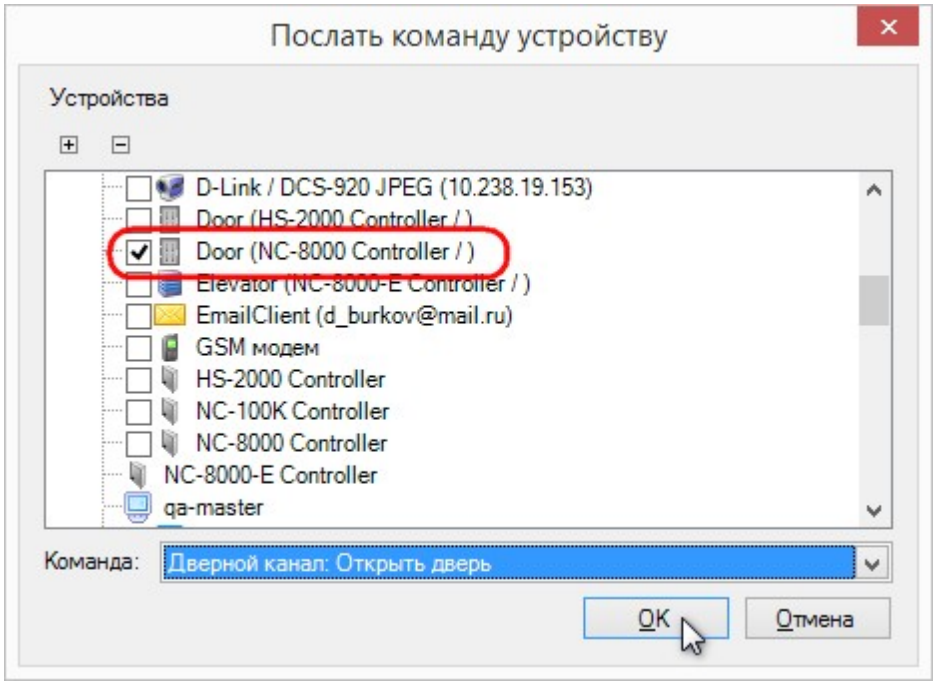


Обратите внимание, что контроллер, как источник данных, доступен для выбора только тем организациям, операторам которых (при создании контроллера автономеров) предоставлено право работы с ним.

В качестве инициирующих событий выбираем события "Нормальный вход по ключу" и "Нормальный выход по ключу", которые будет генерировать контроллер при факте распознания автомобильного номера на въезд и выезд соответственно:



На выходе будем управлять реле контроллера, к которому, например, можно подключить привод шлагбаума:



Теперь при распознании номера транспортного средства, имеющего право доступа, система откроет шлагбаум (при условии, что данный субъект пытается получить доступ в рамках своего временного профиля) и пропустит автомобиль на территорию. Аналогично для выезда.

11.7 Интеграция с системами ОПС

Лицензируется как PNSoft-AI [344]

Общие положения

Интеграция с системами охранно-пожарной сигнализации (ОПС) позволяет обеспечить комплексный подход к обеспечению безопасности объекта и расширить функциональные возможности системы ParsecNET 3 не только на величину возможностей интегрируемой ОПС, а значительно выше за счет организации взаимодействия интегрируемых подсистем. Например, при авторизованном проходе сотрудника через дверь можно автоматически снять помещение с охраны, а при возникновении пожара в конкретной области автоматически открыть защищаемые системой доступа двери для эвакуации персонала.



Конфигурирование и настройка систем ОПС должно производится штатными средствами интегрируемой системы. Со стороны ParsecNET 3 может поддерживаться только настройка некоторых оперативных параметров (при условии, что интеграционные механизмы системы ОПС предоставляют такие возможности).

Использование графпланов

Как и другие компоненты системы безопасности, компоненты проинтегрированных систем ОПС могут размещаться на интерактивных графических планах, если они используются в СКУД ParsecNET 3.

Графические планы создаются в редакторе топологии[203] .

См. также:

- Система "Стрелец"[605]
- Система "Стрелец-Интеграл"[616]
- Система "Мурена"[624]
- Система "Болид"[629]
- Создание графических планов[208]

11.7.1 Система "Стрелец"

Общие положения



Данный раздел не является руководством по использованию системы "Стрелец", а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы "Стрелец" обратитесь к оригинальному руководству.

Радиоканальная система охранно-пожарной сигнализации "Стрелец" позволяет оборудовать системой ОПС как небольшие, так и достаточно крупные объекты.

Неоспоримым преимуществом системы является простота ее монтажа (не требуется прокладка коммуникаций), а также более высокая (по сравнению с проводными системами) надежность при пожаре.

ПО ParsecNET 3 поддерживает полностью или частично следующее оборудование системы "Стрелец":

- Радиоканальные расширители типов РРОП, АСБ-РС, РРП-240, РРОП-И;
- Охранные извещатели типов Икар-5Р, Аргус-Р, Икар-4Р;
- Пожарные извещатели типов Аврора-Р, Аврора-ДТР, Аврора-ТР, ИПДЛ-Р;
- Входные модули с одним шлейфом сигнализации РИГ, ДПВ-Р, ТД-Р;
- Радиобрелок управления РБУ;
- Ручной пожарный извещатель ИПР-Р;
- Исполнительное устройство ИБ-Р;
- Поверхностные акустические извещатели Арфа-Р, Арфа-Р, Арфа-2Р;
- Системные устройства управления типов ПУ-Р, БПИ RS-RF, ПУП-Р;
- Локальный беспроводной пульт управления ПУЛ-Р;
- Локальный пульт управления ПУЛ;
- Исполнительные устройства ИБ-Р и.2, Сирена-Р, "Маячок";
- Коммуникационные устройства УОО-АВ исп.1, УОО-Аргон, УОО-GSM-С1, УОО-Атлас-20;
- Исполнительные устройства Орфей-Р, Орфей-РТР;
- Блоки управления и контроля типов ШС БУК-Р, ШС1 БУК-Р, ШС2 БУК-Р, ШС3 БУК-Р, ШС4 БУК-Р.



Если конфигурирование системы "Стрелец" в целом делается ее штатными средствами, то занесение субъектов доступа настоятельно рекомендуется делать средствами системы ParsecNET 3, что обеспечит однозначную идентификацию пользователей "Стрельца" вне зависимости от того, в каком радиорасширителе эти пользователи присутствуют.

См. также:

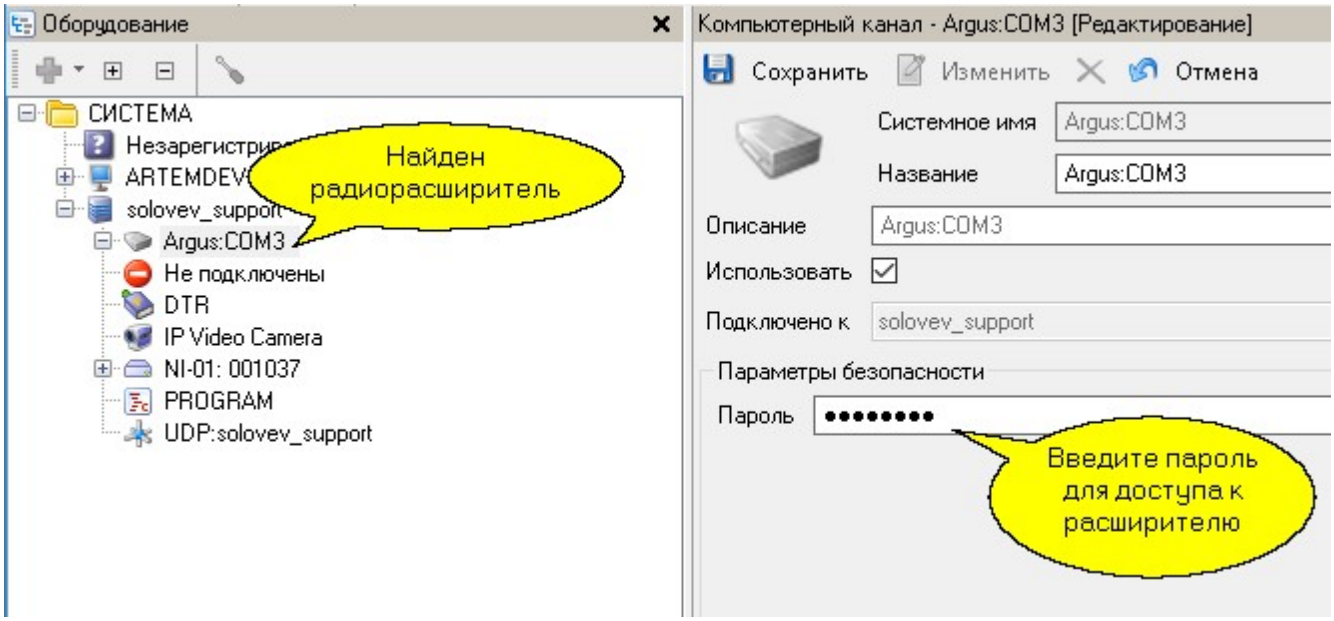
Подключение и настройка[606]

Использование системы[612]

11.7.1.1 Подключение и настройка

Подключение оборудования

Если у вас имеется система "Стрелец", предварительно сконфигурированная своими штатными средствами, можно подключать ее к системе ParsecNET 3. Для этого подключите нулевой радиорасширитель "Стрелец" к COM-порту сервера или зарегистрированной рабочей станции Parsec. Примерно в течение полутора минут в редакторе оборудования под компьютером, к которому подключен "Стрелец" появится соответствующий канал, как показано на рисунке ниже.

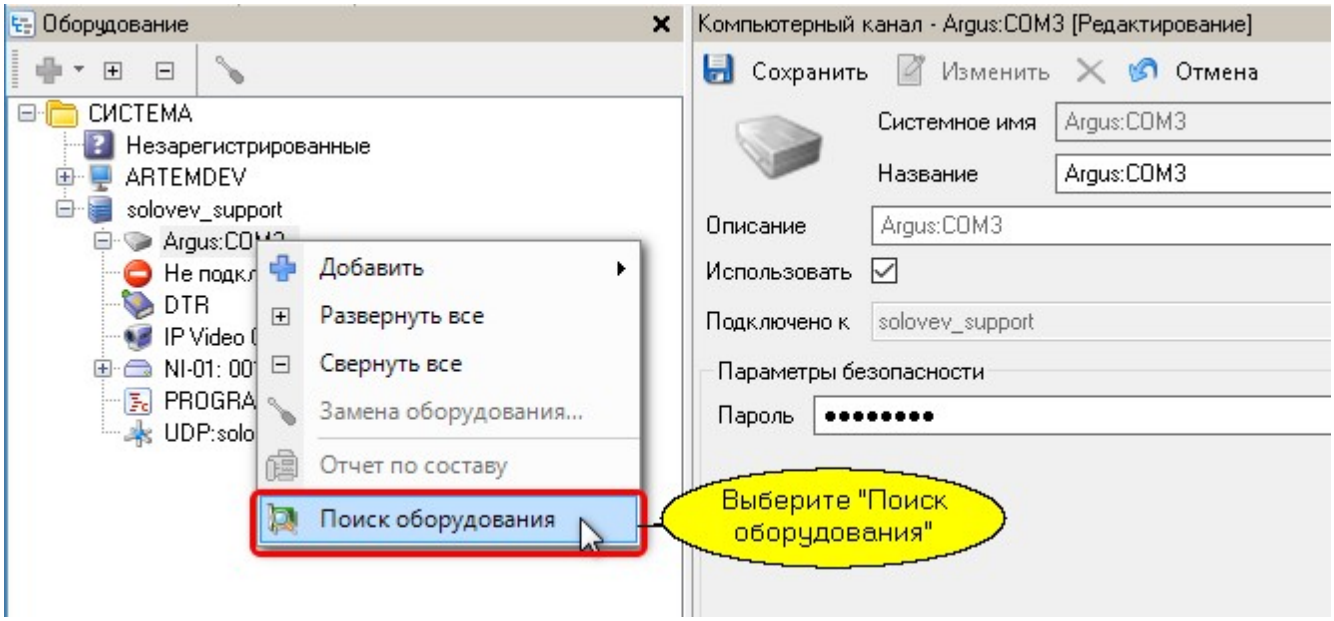


Для конфигурирования системы "Стрелец" с помощью ее собственных утилит следует подключать ее к компьютеру, на котором не установлена система ParsecNET 3, так как ParsecNET 3 захватит COM-порт "Стрельца" и не позволит использовать его другим программам, в том числе утилитам настройки.

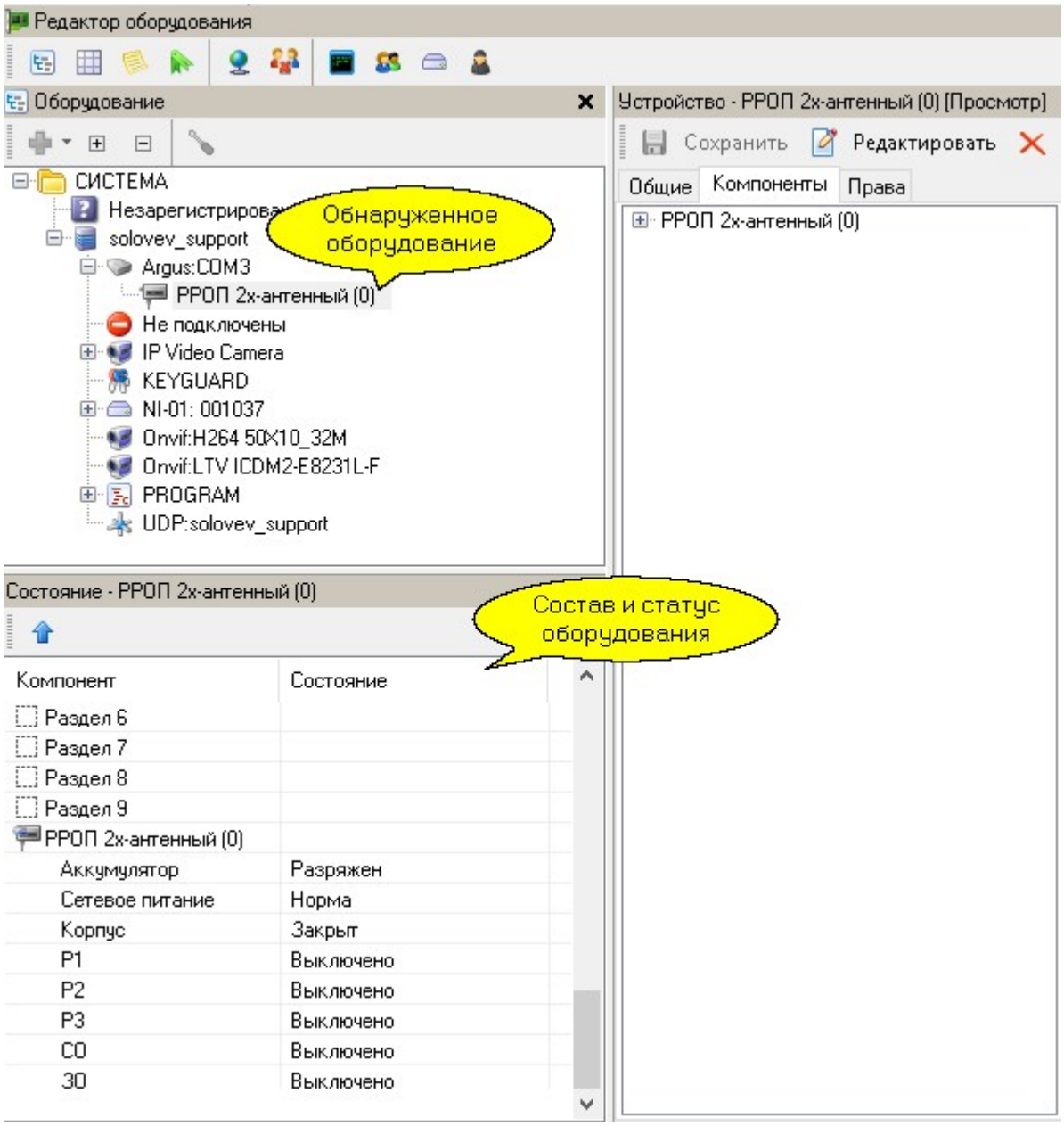
Выбрав канал "Argus:COMx" в дереве оборудования, переходим в панель свойств, включаем режим редактирования и вводим пароль для доступа к "Стрельцу".

Для системы "Стрелец" пароль по-умолчанию - 11112222 (четыре единицы и четыре двойки).

Теперь можно перейти к получению конфигурации системы "Стрелец", для чего необходимо на канале из контекстного меню выбрать "Поиск оборудования":



Через некоторое время (от одной до нескольких минут, в зависимости от масштабов системы ОПС) ParsecNET 3 обнаружит все подключенное оборудование и разместит его в дереве оборудования. Пример показан на следующем рисунке:

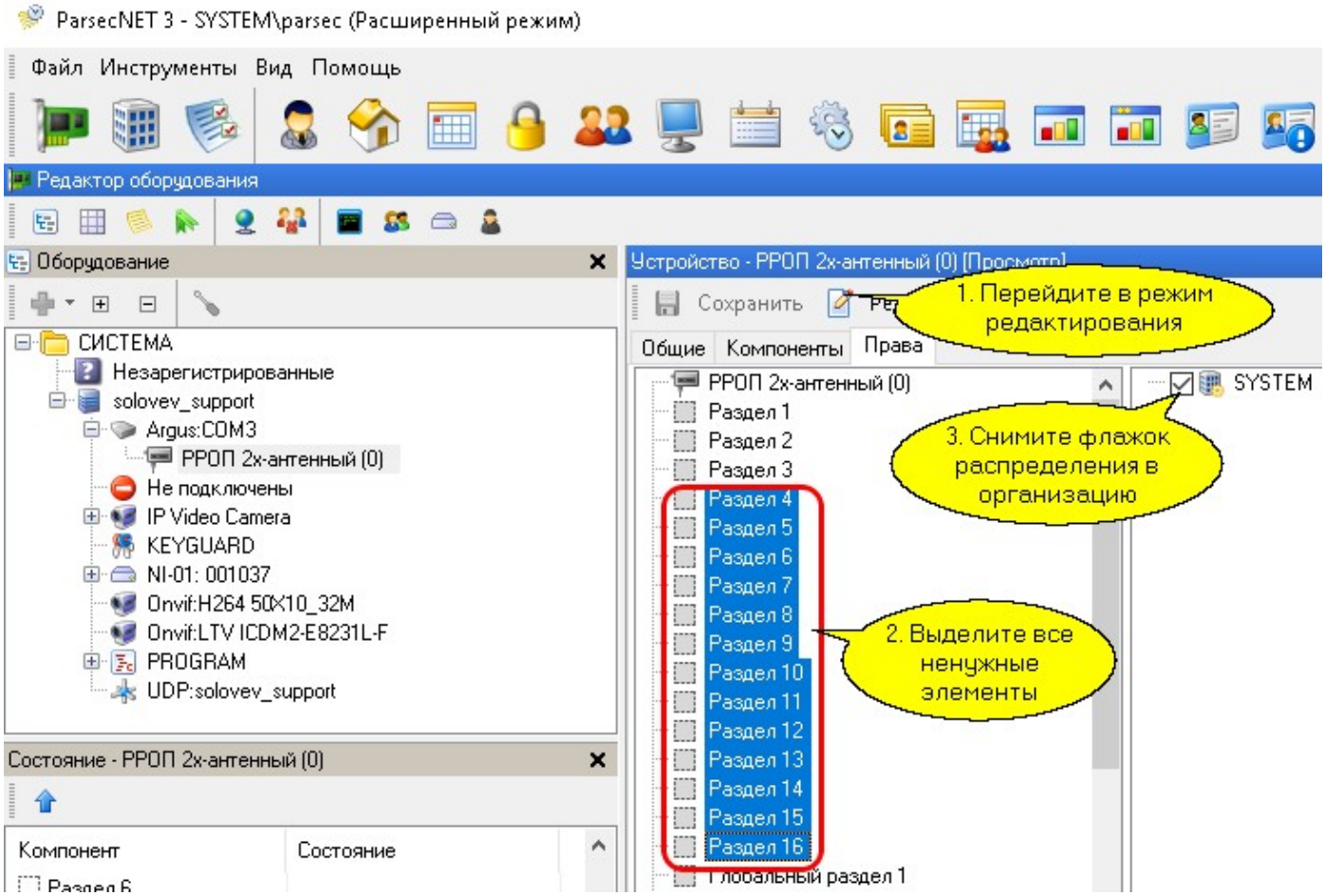


В дереве появятся все радиорасширители, подключенные к конкретному компьютеру, а при выборе в дереве конкретного расширителя в списке ниже появится статус расширителя и перечень оборудования (например, датчик), которое подключено к данному расширителю. Кроме того, в списке будут показаны все поддерживаемые расширителем разделы - как локальные, так и глобальные.

Более того, все обнаруженное оборудование системы "Стрелец" будет автоматически распределено в корень главной организации (СИСТЕМА или SYSTEM). Вам останется в дальнейшем в редакторе топологии распределить разделы и оборудование по элементам топологии, если вам это необходимо.

Убираем лишнее оборудование

Если вам не требуется использовать все разделы или оборудование, что достаточно часто встречается на практике, то вы можете на кладке "Права" панели свойств редактора оборудования изъять из обращения ненужные элементы. Например, на рисунке ниже мы исключаем разделы с пятого по шестнадцатый:

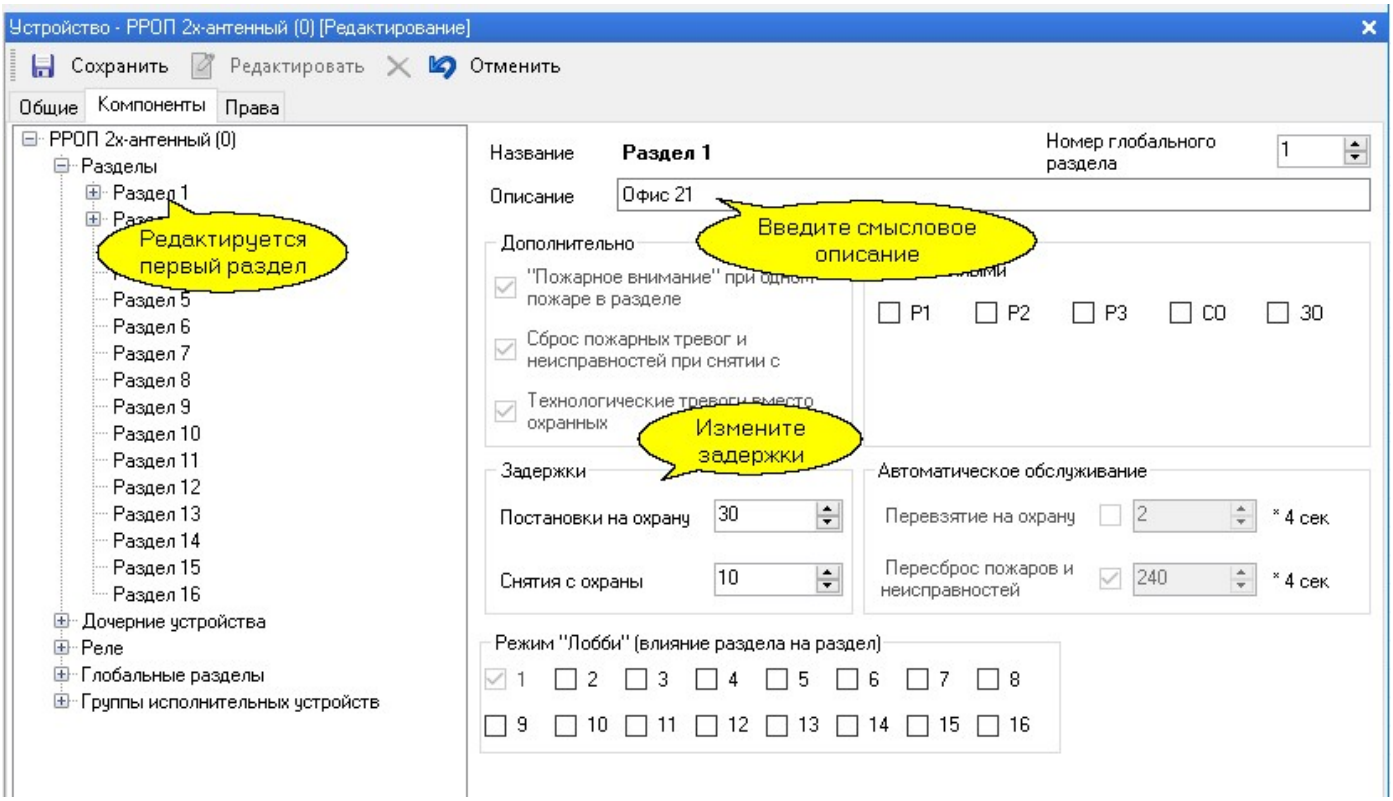


После того, как неиспользуемое (как минимум в данной организации) оборудование и разделы отредактированы, можно настроить некоторые параметры работы компонентов системы "Стрелец".

Конфигурирование оборудования

Основная конфигурация системы "Стрелец" производится ее собственными средствами, в системе можно откорректировать некоторые параметры, необходимые в ежедневной работе, а также поименовать сущности осмысленными именами.

Например, для раздела можно указать, помимо его смыслового описания, время задержки постановки на охрану и снятия с охраны, как показано на следующем рисунке:

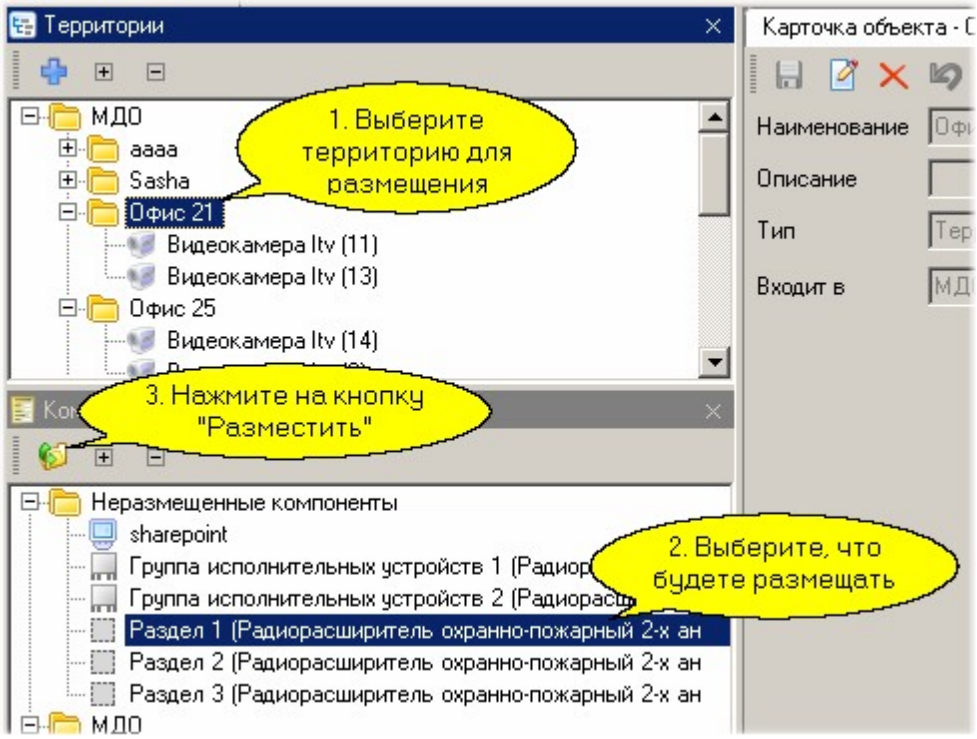


Замечание: Те параметры, которые доступны для изменения, в режиме редактирования вы можете поменять. Остальные даются справочно, поменять их невозможно, и они отображаются серым цветом даже в режиме редактирования, как это видно на рисунке выше.

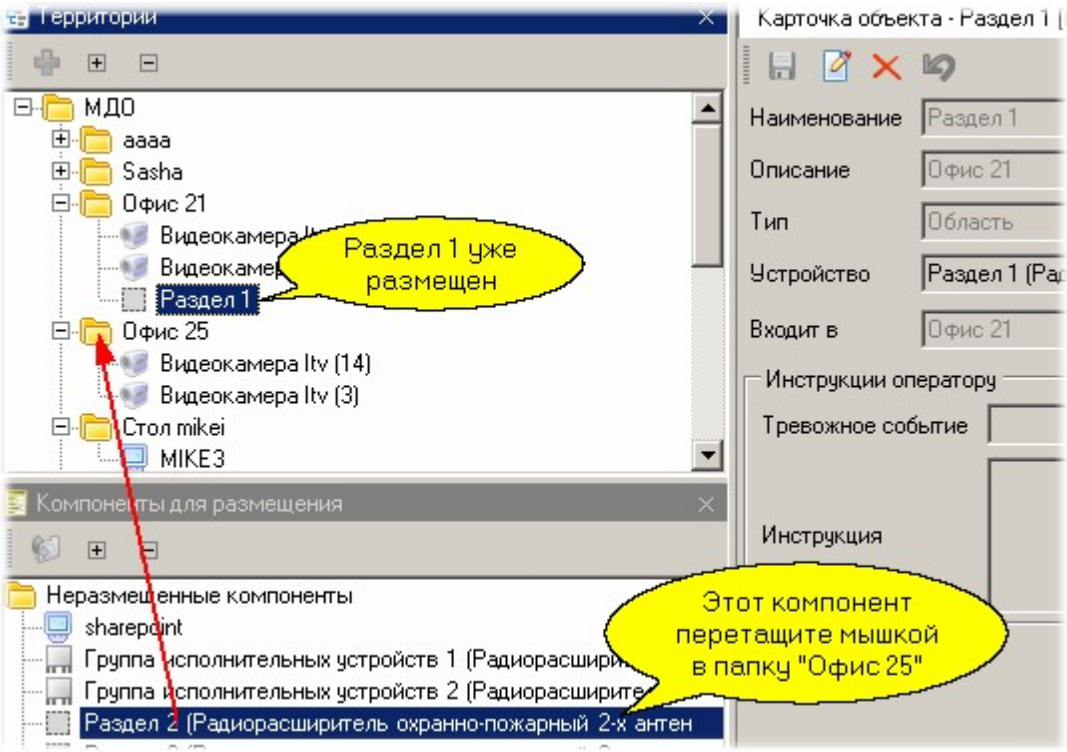
Привязка к территориям

Для осмысленного использования системы необходимо распределить ее компоненты по топологии с помощью редактора топологии[203] . Как уже упоминалось выше, все обнаруженное оборудование системы "Стрелец" автоматически распределяется в корень главной организации (СИСТЕМА или SYSTEM).

В нашем примере мы первый раздел разместим на территории "Офис 21", а второй раздел - на территории "Офис 25". Первый способ иллюстрируется следующим рисунком:

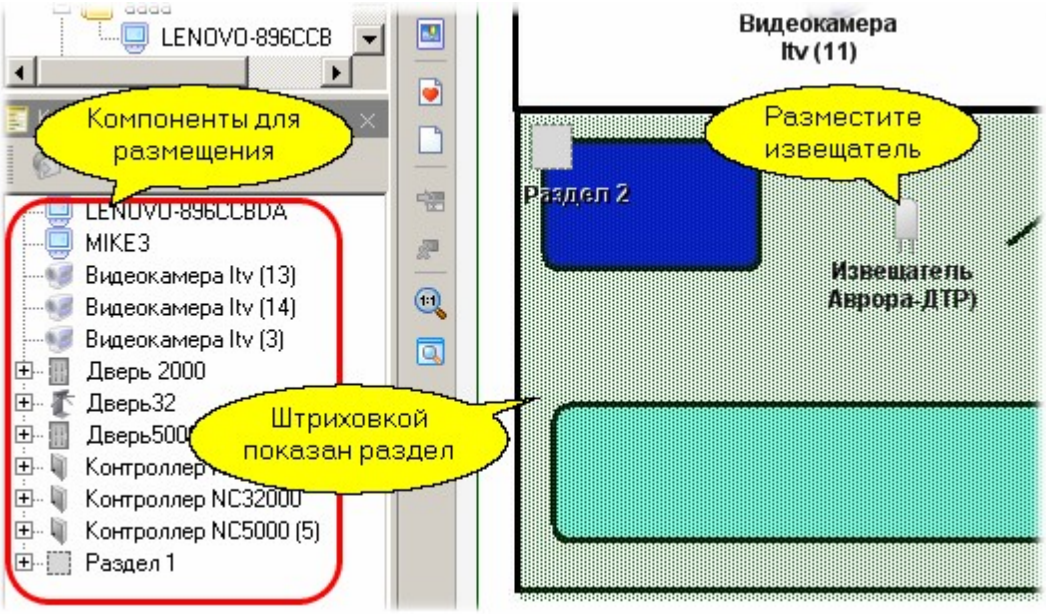


На следующем рисунке показан результат предыдущих действий:



Размещение на графическом плане

Для примера разместим раздел 2 и его датчик на графическом плане, используя для этого редактор топологии. На рисунке ниже (режим редактирования плана) мы разместили раздел 2 и его датчик на фоновой подложке плана:



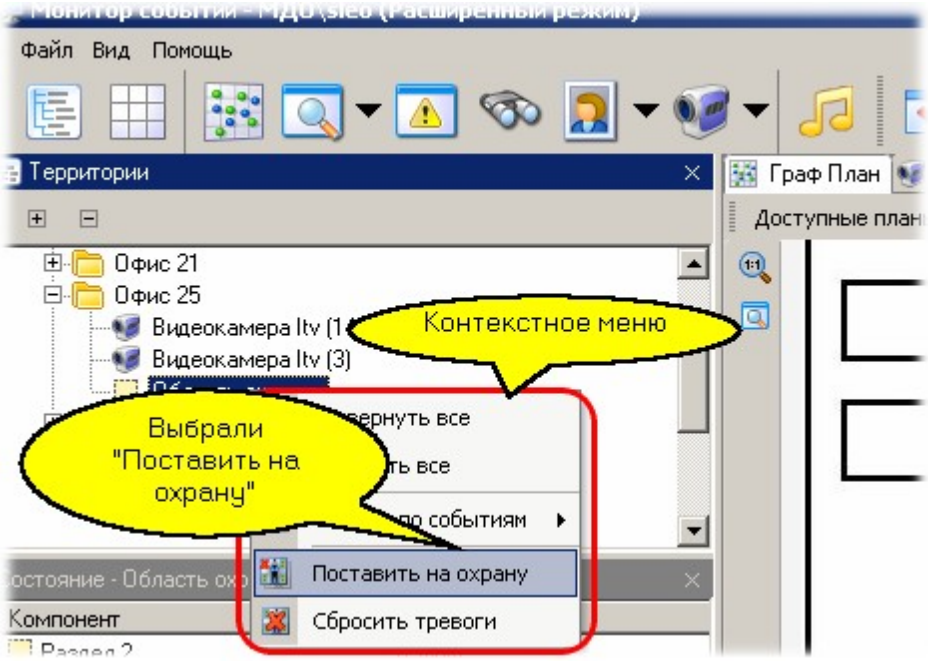
В разделе [использования системы](612) мы увидим, как будут работать размещенные компоненты.

11.7.1.2 Использование системы

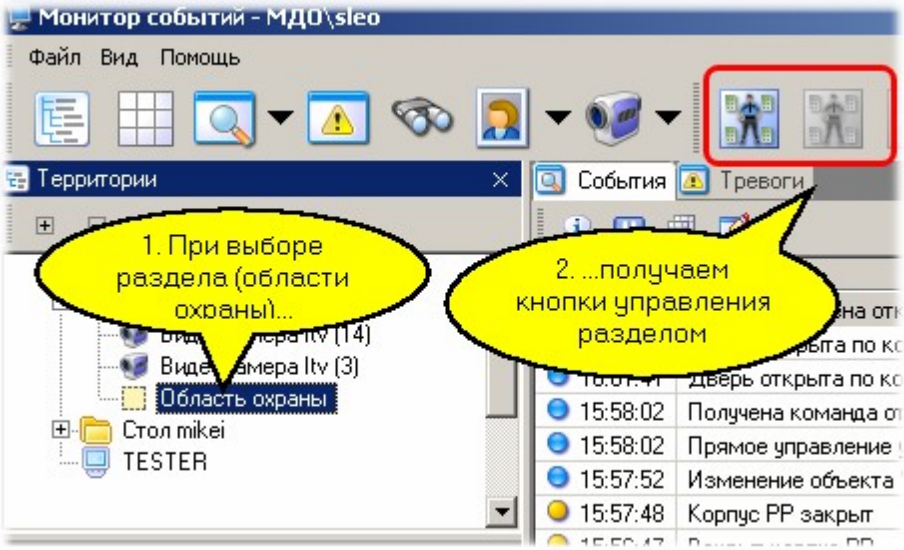
"Стрелец" в мониторе событий

Система "Стрелец" позволяет в мониторе событий обеспечить наблюдение за состоянием компонентов (статус датчиков, разделов и так далее), а также управлять ими (ставить разделы на охрану или снимать с охраны). На панели событий доступа и тревог также будут отображаться сообщения о событиях от всех имеющихся в рамках организации компонентов системы "Стрелец".

Ниже на рисунке показано контекстное меню постановки локального раздела на охрану в дереве территорий монитора событий (раздел 2 нулевого расширителя был переименован в "Область охраны" при редактировании плана территорий):

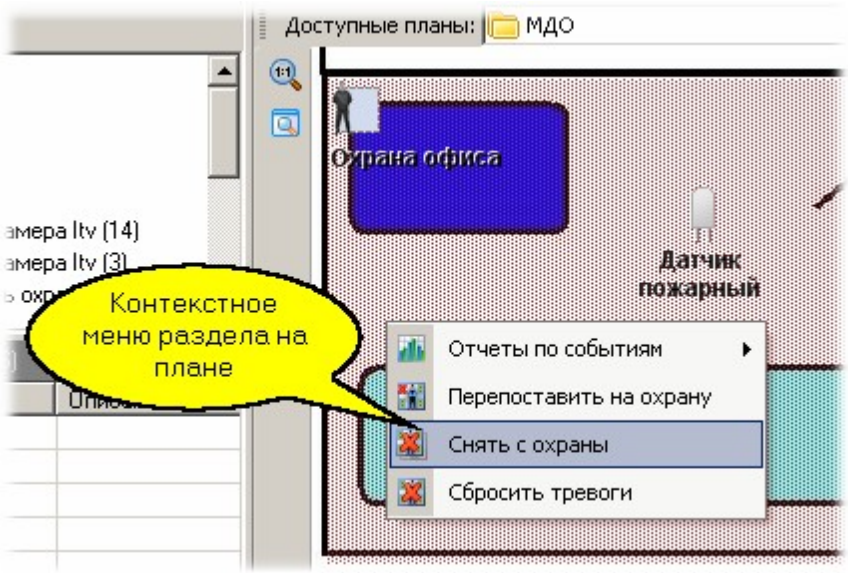


Точно так же можно ставить на охрану и снимать с охраны выбранные в мониторе событий разделы с помощью интерактивной панели инструментов монитора событий:



"Стрелец" на графических планах

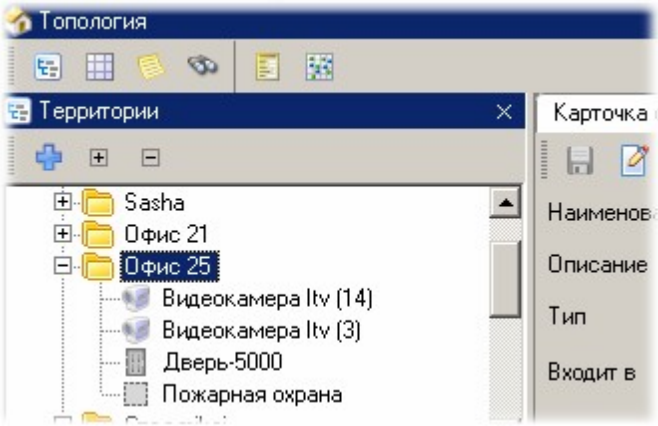
Если вы поместили компоненты системы "Стрелец" на графический план в редакторе топологии, то как и для других компонентов СКУД ParsecNET 3, мы получаем возможность наблюдения на плане статуса компонентов (разделов, извещателей) и управления ими (постановка или снятие с охраны), как показано для примера на рисунке ниже:



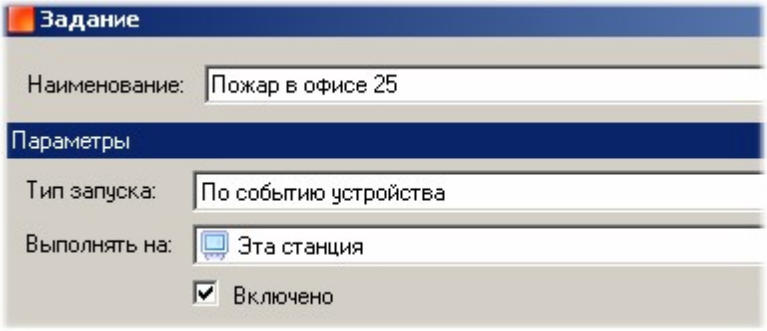
Совместная работа подсистем

Помимо возможности наблюдать и управлять работой различных подсистем, интегрированных в ParsecNET 3, имеется возможность организовать их взаимодействие при реагировании на происходящие в системе события, для чего используется редактор заданий[321].

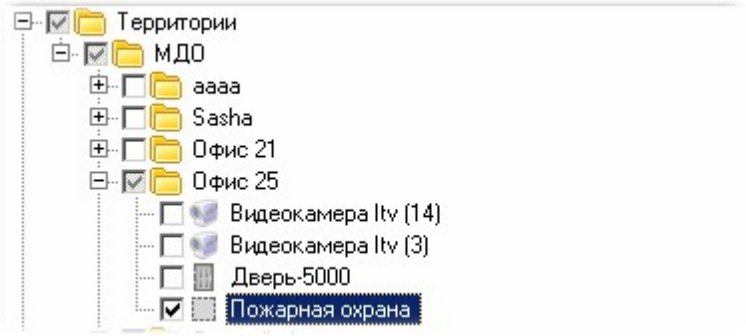
Для иллюстрации сказанного заставим по пожарной тревоге открыть дверь помещения, в котором произошло возгорание, а также включить запись происходящего на находящуюся в помещении видеокамеру. На рисунке ниже мы видим, что офис 25 имеет область охраны (причем это раздел пожарной охраны), дверь в помещение, а также две видеокамеры.



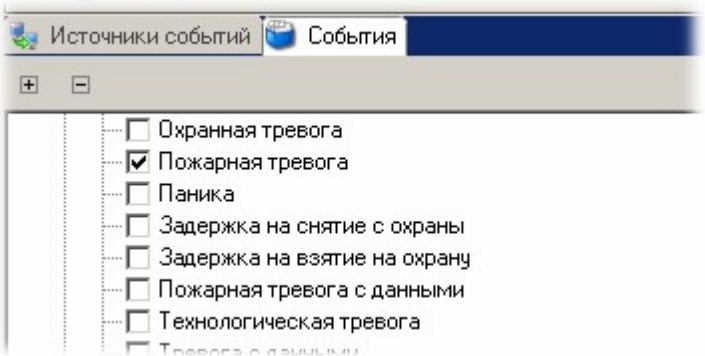
С помощью редактора заданий создадим задание, выполняющее поставленную выше задачу взаимодействия подсистем по сигналу пожарной тревоги:



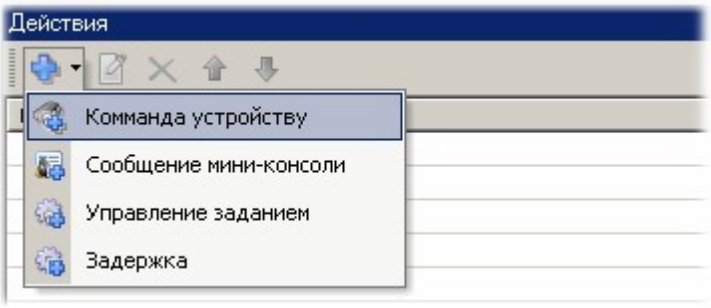
В качестве источника назначим область пожарной охраны:



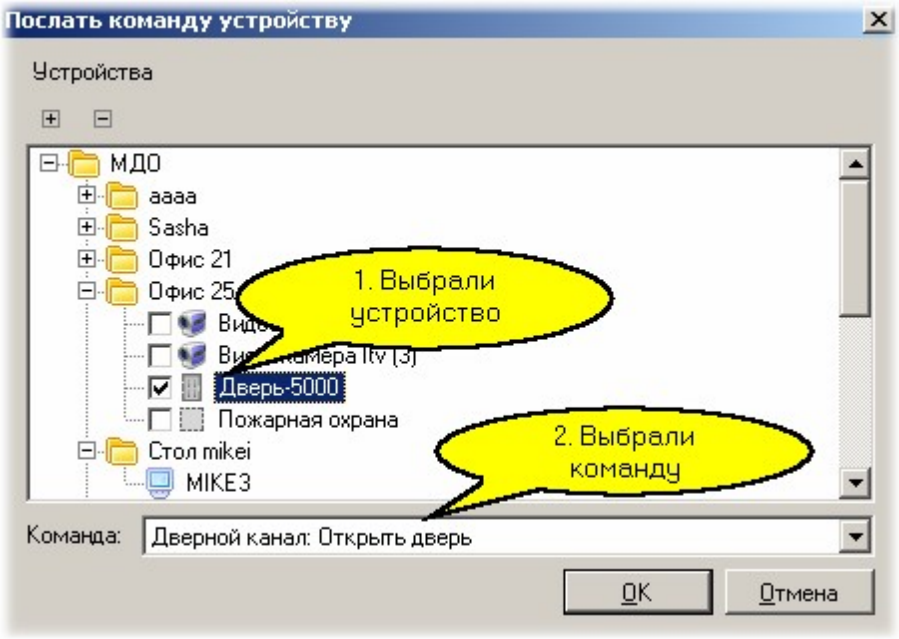
Событием, инициирующим выполнение задания, назначим пожарную тревогу:



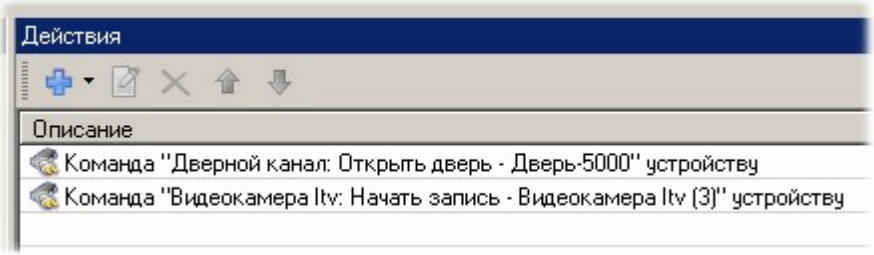
Теперь перейдем к формированию реакции на выбранное событие. Для этого на панели действий редактора заданий выбираем пункт "Добавить - Команда устройству":



В открывшемся диалоге выберем дверь и назначим ей команду "Открыть дверь":



Аналогично создадим команду для камеры для начала записи события. В результате получим такую последовательность действий по сигналу пожарной тревоги:



Таким образом можно организовать сколь угодно сложное взаимодействие любых компонентов любых подсистем, интегрированных в ParsecNET 3.

См. также:

[Монитор событий](287)

[Редактор заданий](321)

11.7.2 Система "Стрелец-Интеграл"

Данный раздел не является руководством по использованию интегрированной системы безопасности (ИСБ) "Стрелец-Интеграл", а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения ИСБ "Стрелец-Интеграл" обратитесь к оригинальному руководству.

ИСБ "Стрелец-Интеграл" является системой следующего поколения и может объединять в себе как устройства радиосистемы "СТРЕЛЕЦ-ПРО", так и устройства беспроводной системы предыдущего поколения "СТРЕЛЕЦ". Все устройства "СТРЕЛЬЦА" и "СТРЕЛЬЦА-ПРО" при этом будут работать в единой адресной системе.

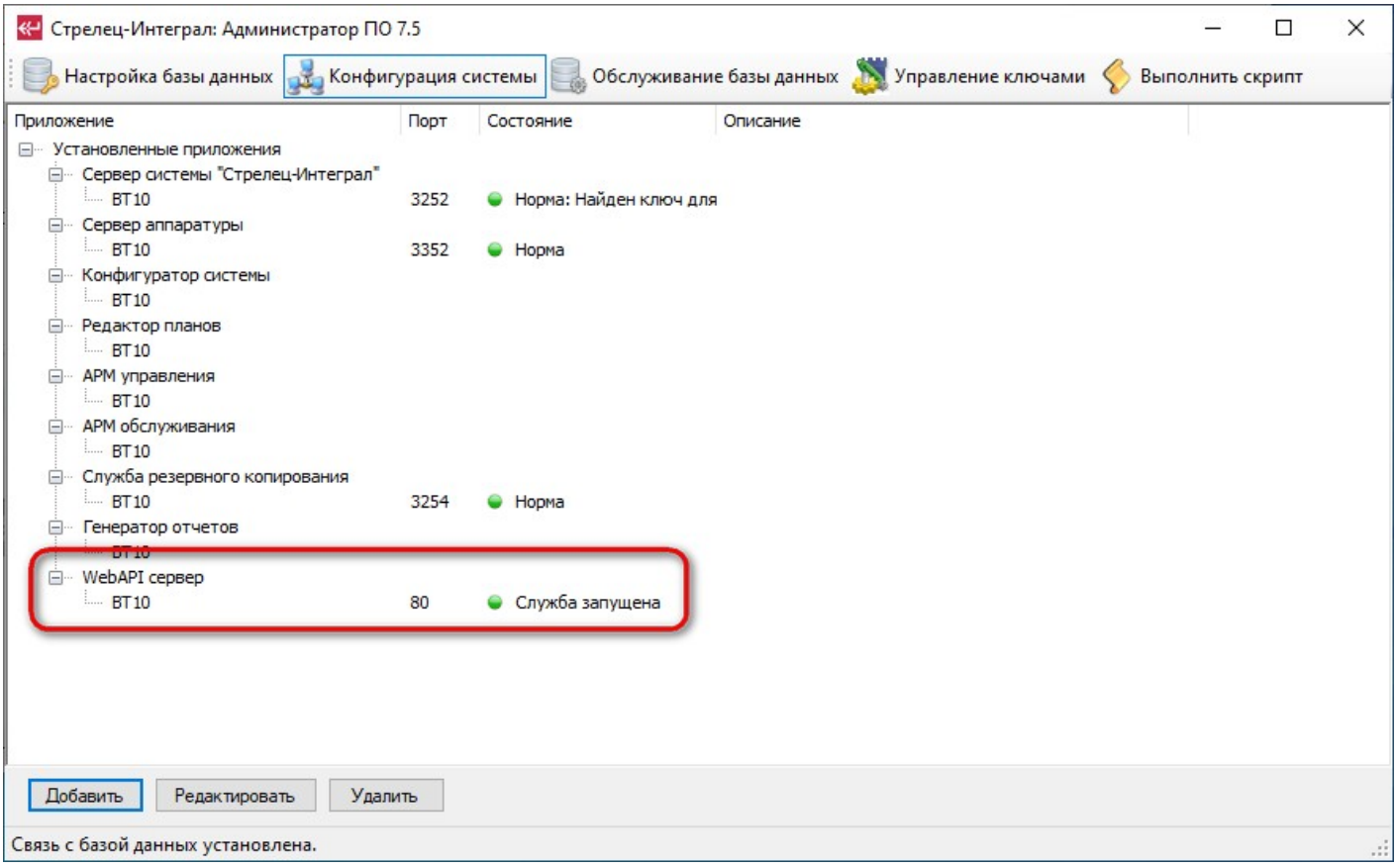
ИСБ "Стрелец-Интеграл" позволяет оборудовать охранно-пожарной сигнализацией как небольшие, так и достаточно крупные объекты.

11.7.2.1 Подключение и настройка

Установите ИСБ "Стрелец-Интеграл" и проведите необходимые для достижения Ваших целей настройки, руководствуясь эксплутационной документацией, онлайн справками и подсказками мастеров установки.

Для настройки ПО ParsecNET 3 на совместную работу с ИСБ "Стрелец-Интеграл" необходимо знать:

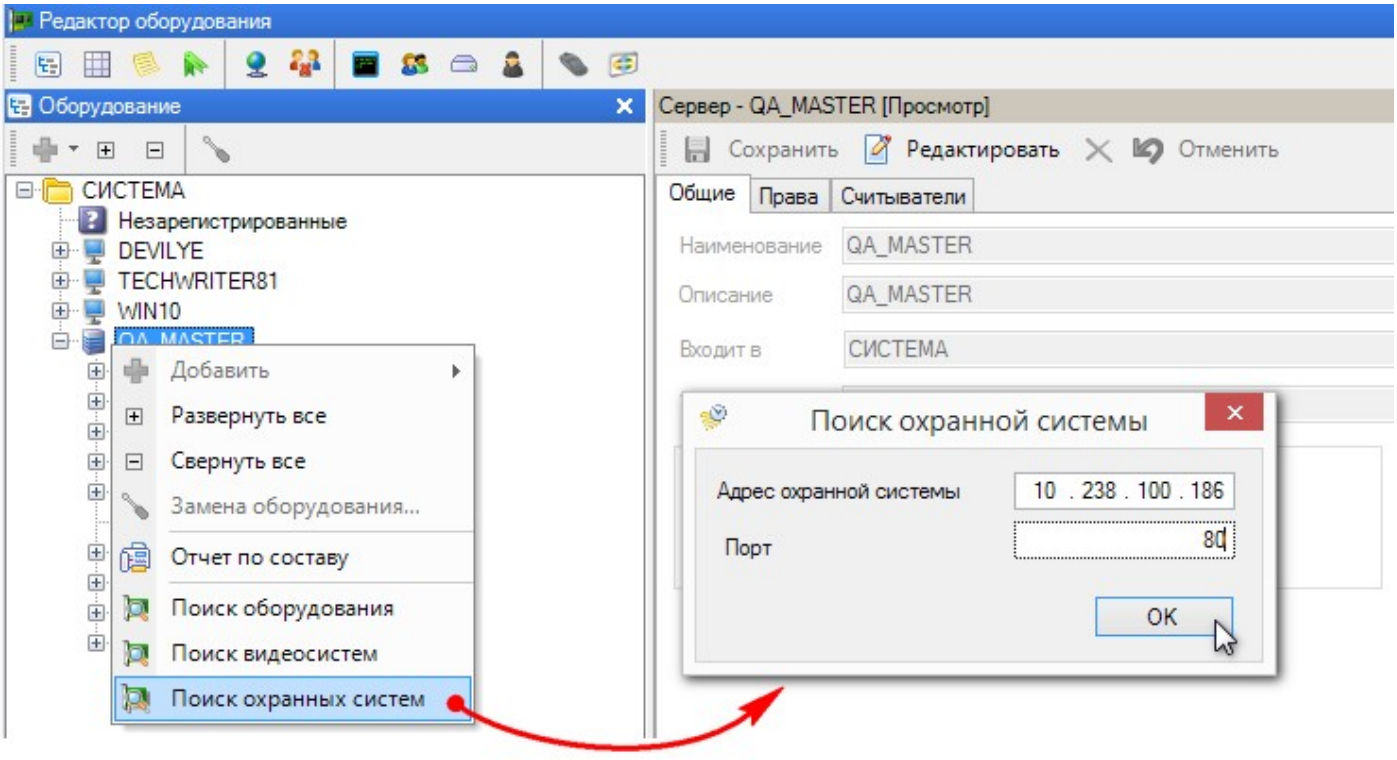
- IP-адрес ПК, на котором установлена ИСБ "Стрелец-Интеграл";
- Номер порта WebAPI сервера. Чтобы узнать его, запустите консоль Администратор ПО и перейдите на вкладку *Конфигурация системы*:



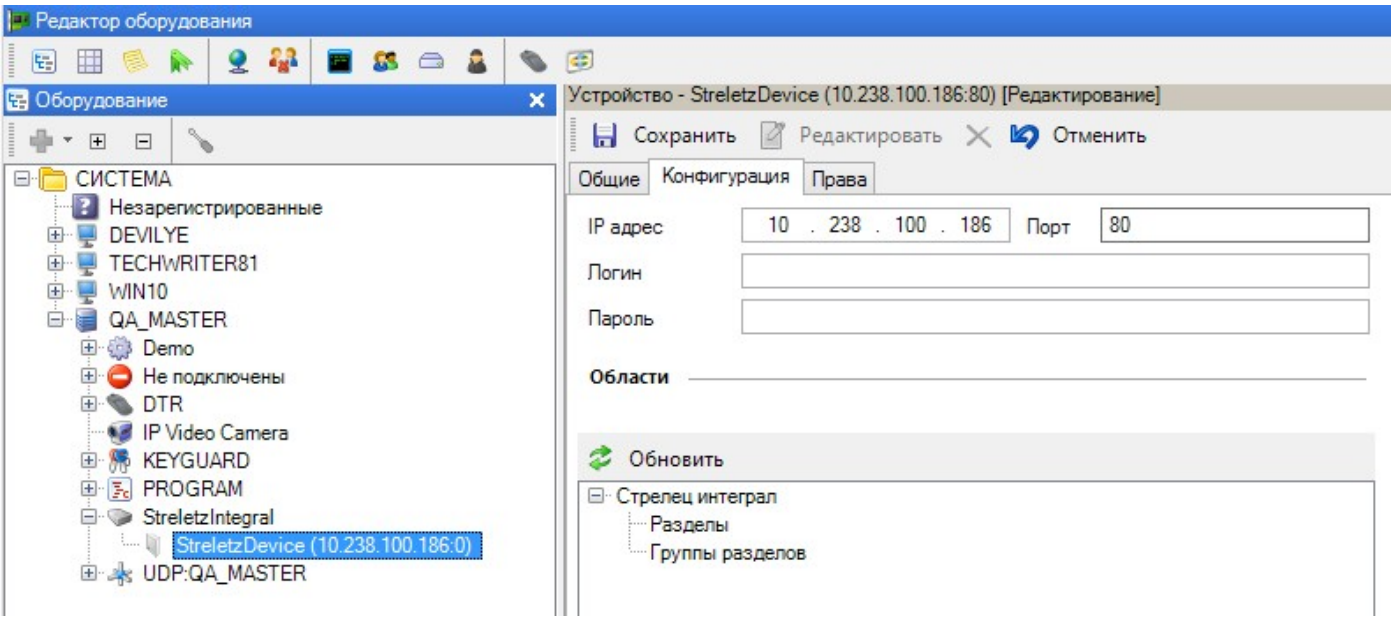
Теперь можно приступить к настройкам ПО ParsecNET 3:

1. Запустите консоль администрирования и перейдите в редактор оборудования;
2. В контекстном меню сервера и рабочей станции откройте контекстное меню и выберите команду "Поиск охранных систем";

3. В открывшемся окне введите IP-адрес ПК, на котором установлена ИСБ "Стрелец-Интеграл" и укажите порт сервера WebAPI (по-умолчанию 80, рисунок выше), после чего нажмите на кнопку *ОК*:

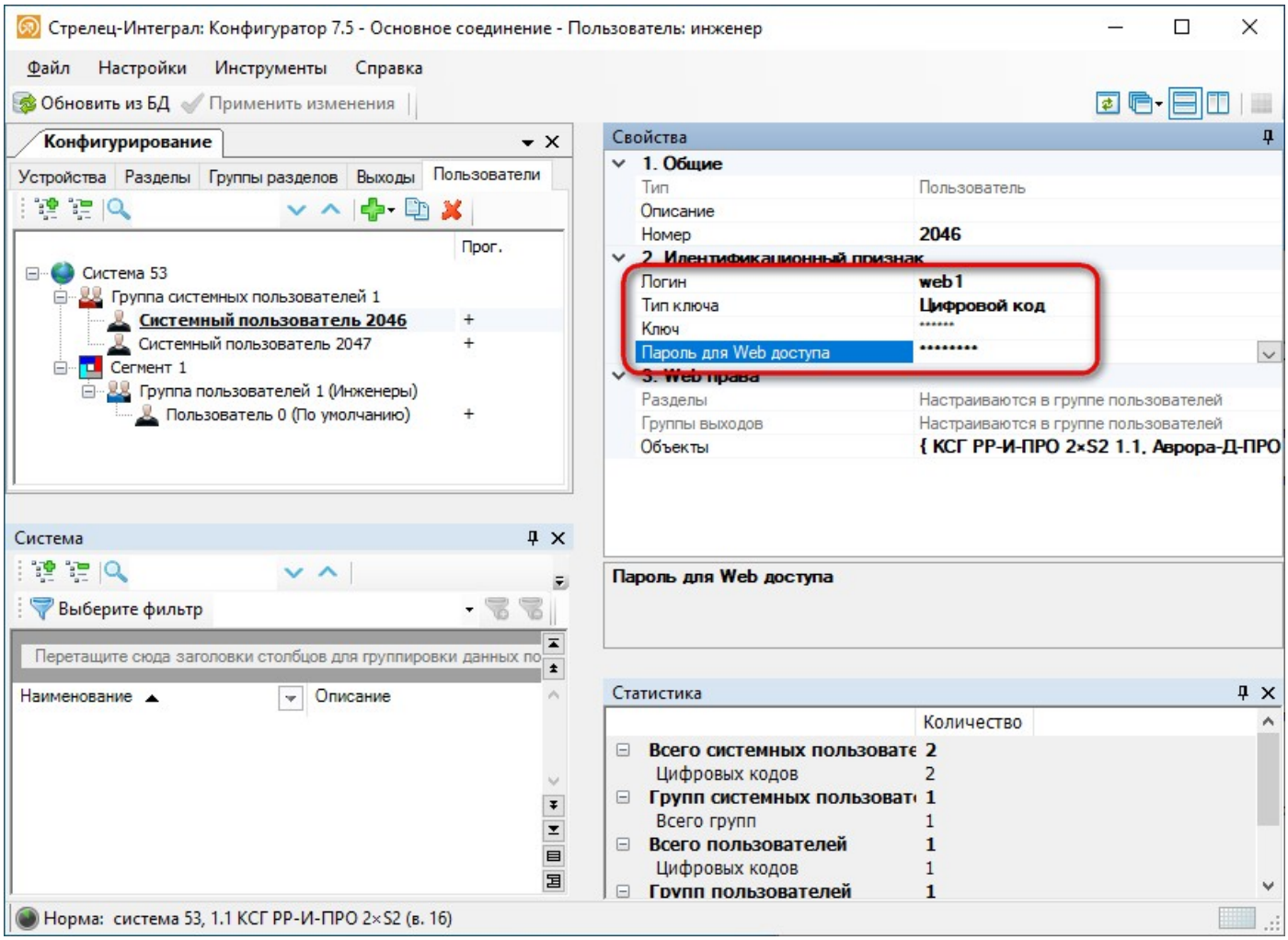


Система проведет поиск и в дереве оборудования появится новый канал StreletzIntegral и виртуальное устройство (служба ИСБ "Стрелец-Интеграл") на этом канале:

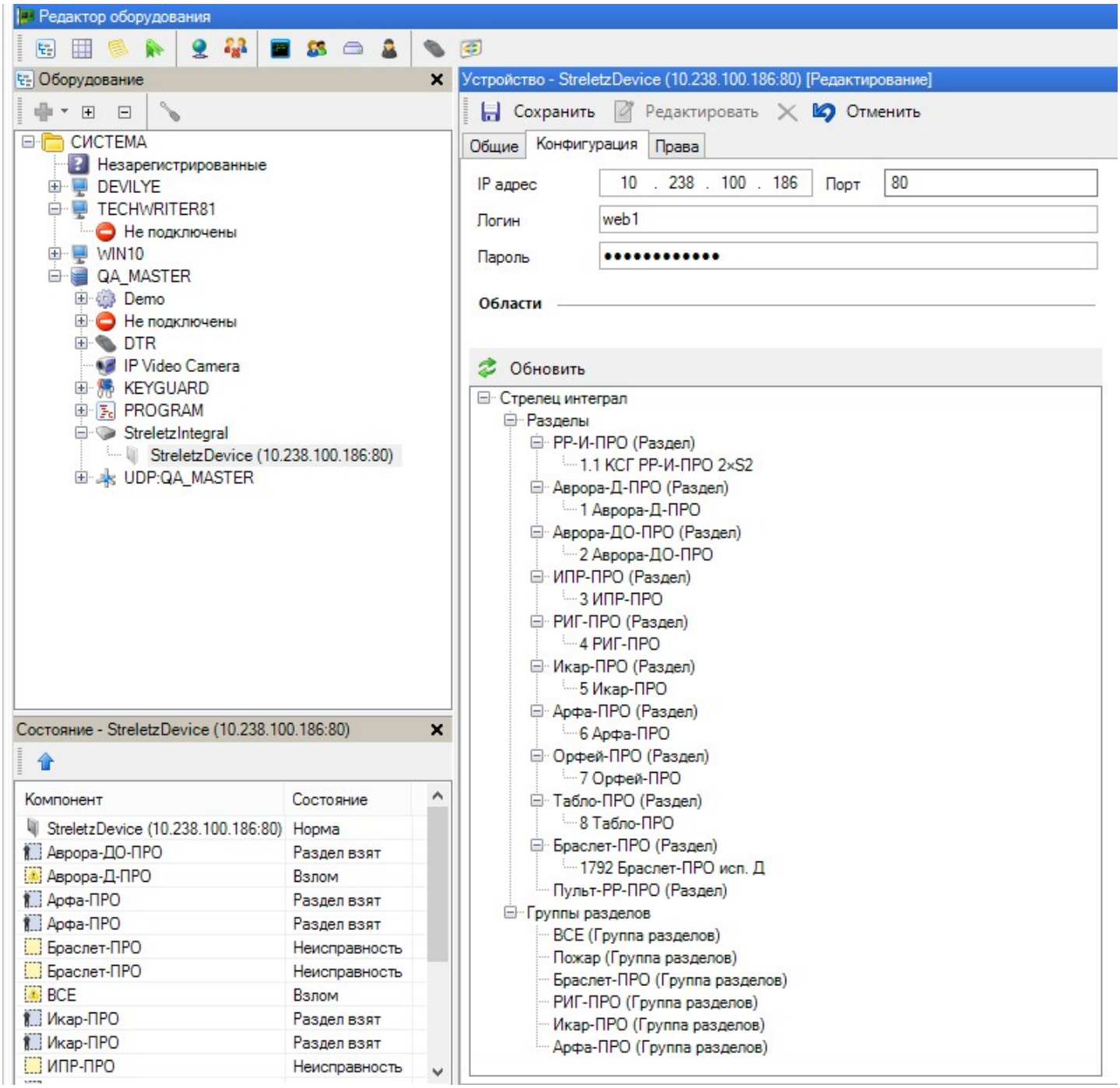


В карточке канала отображаются:

- *IP адрес* - адрес ПК, на котором установлена ИСБ "Стрелец-Интеграл";
- *Порт* - порт WebAPI сервера;
- *Логин/пароль* - логин и пароль, заданные в Конфигураторе ПО "Стрелец-Интеграл":



4. Введите логин и пароль в соответствующие поля карточки устройства и нажмите на кнопку *Обновить*. В поле ниже отобразятся задействованные в ИСБ "Стрелец-Интеграл" устройства:

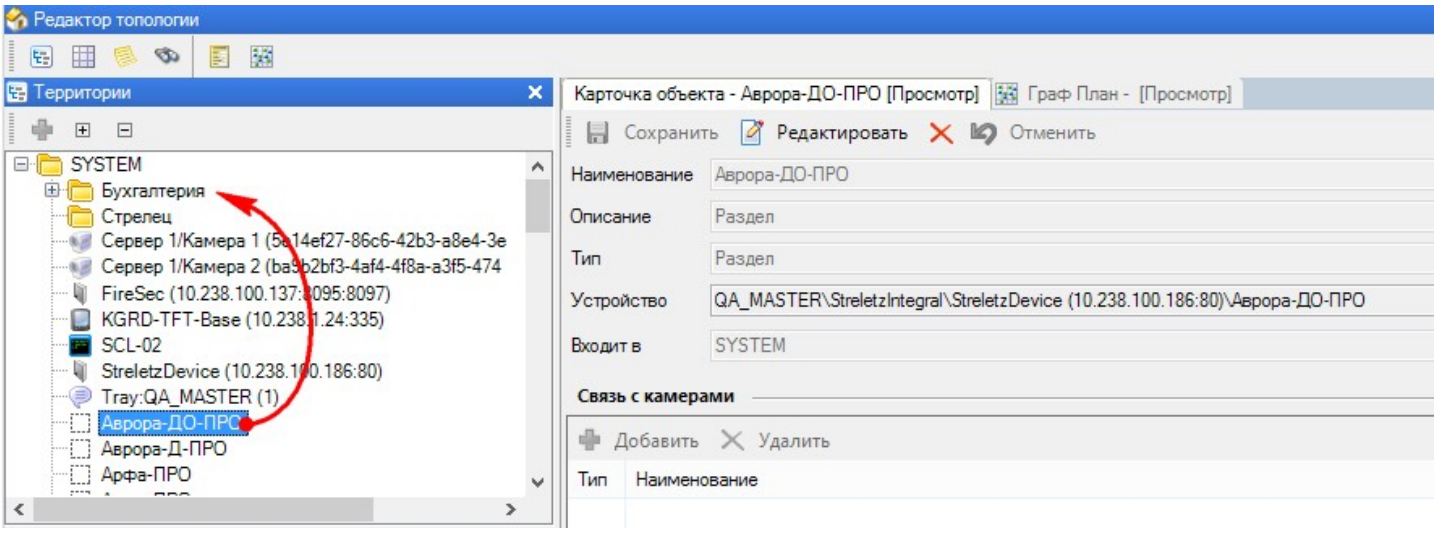


5. На вкладке *Права* необходимо выделить устройство и на правой панели указать те организации, которым это устройство будет доступно для наблюдения и управления.

Привязка к территориям

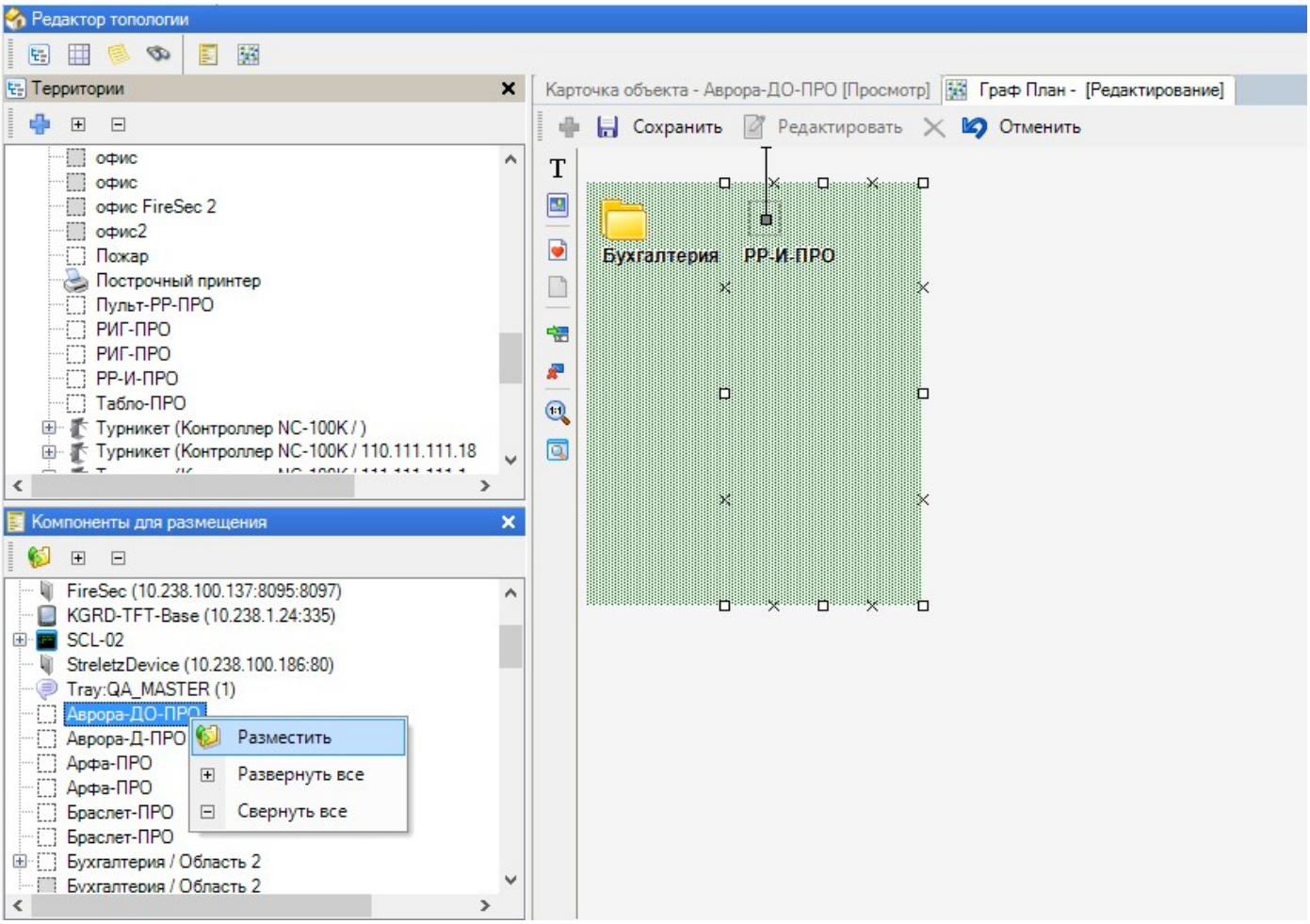
Для осмысленного использования ИСБ необходимо распределить ее устройства по территориям и помещениям с помощью редактора топологии[203]. Изначально, все обнаруженные устройства ИСБ "Стрелец-Интеграл" автоматически распределяется в корень главной организации (СИСТЕМА или SYSTEM).

Для распределения устройств по территориям необходимо сначала создать эти территории в редакторе персонала (например, Бухгалтерия на рисунке ниже), а затем просто перетащить задействованные для охраны этой территории устройства в папку территории (в примере на рисунке ниже это устройство Аврора-ДО-ПРО):



Размещение на графическом плане

Устройства ИСБ "Стрелец-Интеграл" можно размещать на графических планах так же, как и компоненты СКУД ParsecNET 3. Перетащите устройство на графплан с панели *Компоненты для размещения* или воспользуйтесь контекстным меню. Разумеется, на графплане территории следует размещать только устройства, связанные с этой территорией:



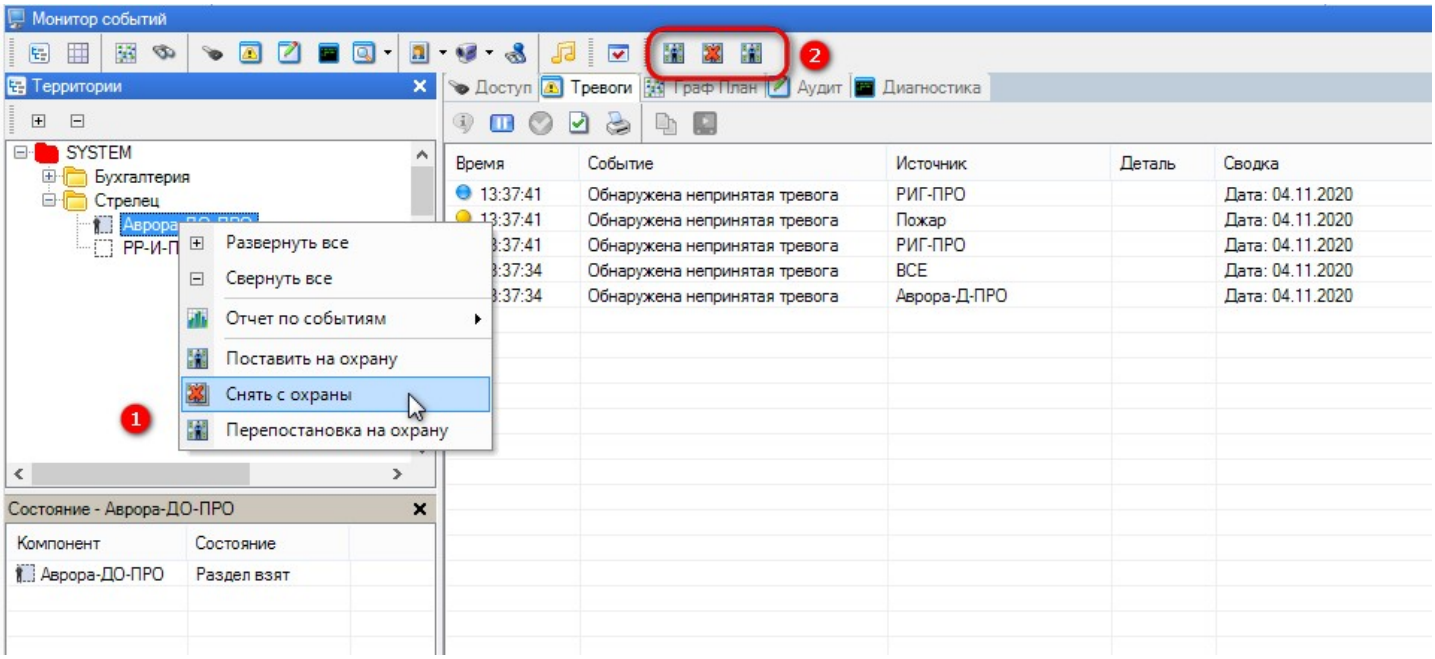
В разделе [использования системы](#)[621] будет видно, как работают размещенные компоненты.

11.7.2.2 Использование системы

"Стрелец-Интеграл" в мониторе событий

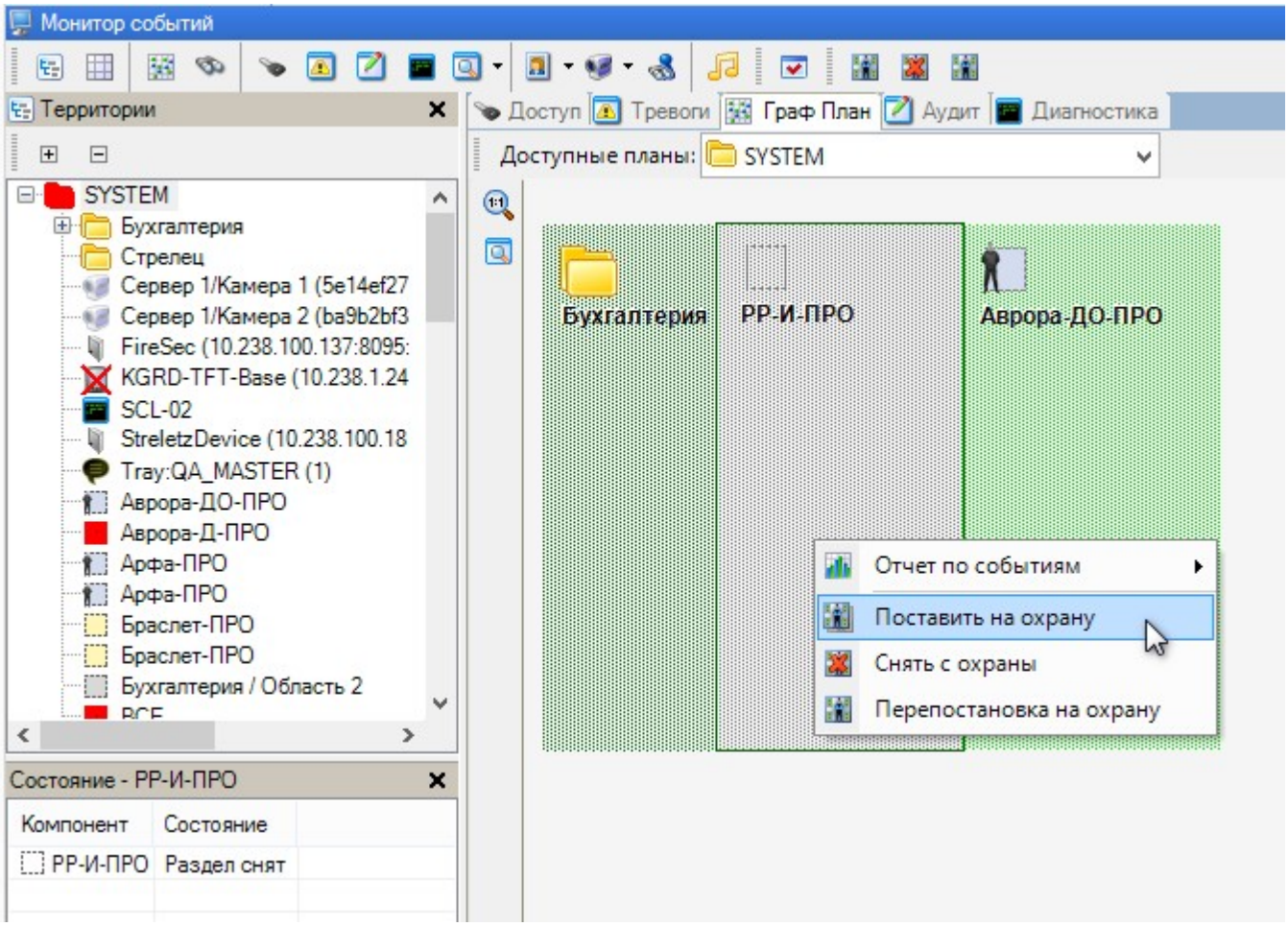
ИСБ "Стрелец-Интеграл" позволяет в Мониторе событий обеспечить наблюдение за состоянием компонентов, а также управлять ими (ставить на охрану или снимать с охраны). На панели событий доступа и тревог также будут отображаться сообщения о событиях от всех имеющихся в рамках организации компонентов ИСБ "Стрелец-Интеграл" .

Ниже на рисунке показано контекстное меню постановки локального раздела на охрану в дереве территорий монитора событий (позиция 1). Аналогичные кнопки управления расположены на панели инструментов (позиция 2):



"Стрелец-Интеграл" на графических планах

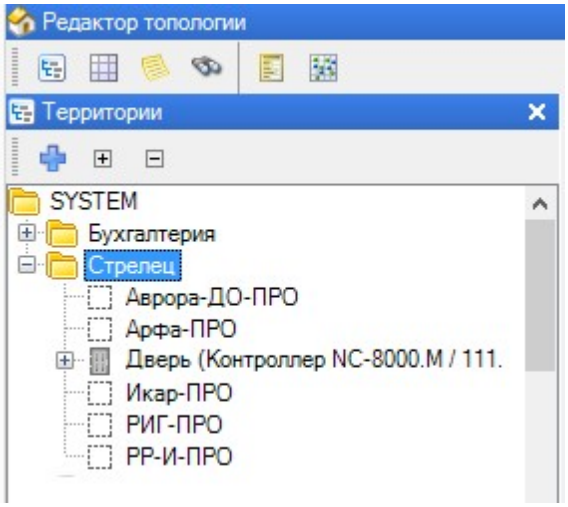
Компоненты ИСБ "Стрелец-Интеграл" помещенные на графический план в редакторе топологии, как и другие компоненты СКУД ParsecNET 3, предоставляют возможность на графплане Монитора событий наблюдать статус устройств и управлять ими (ставить или снимать с охраны):



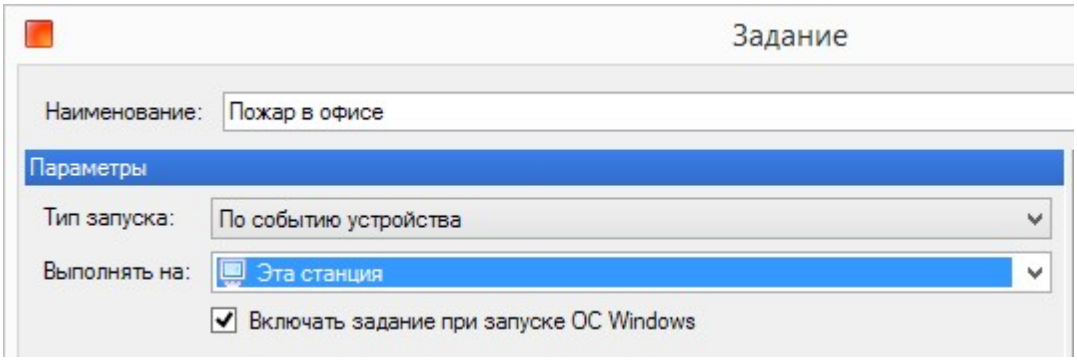
Совместная работа подсистем

Помимо возможности наблюдать и управлять работой различных подсистем, интегрированных в ParsecNET 3, имеется возможность организовать их взаимодействие при реагировании на происходящие в системе события, для чего используется редактор заданий[321].

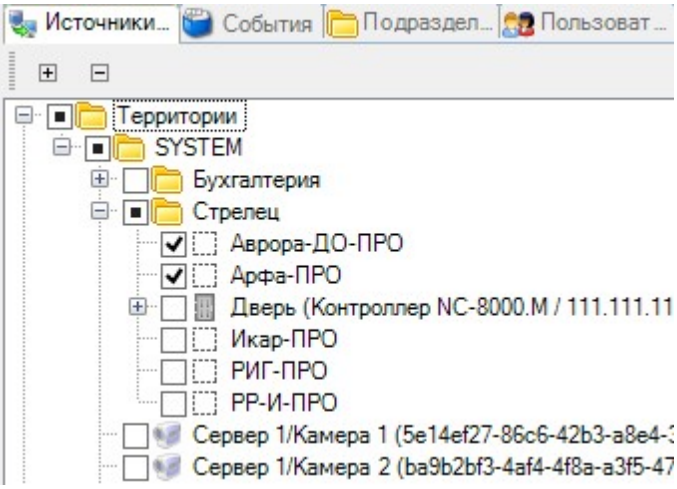
Чтобы проиллюстрировать это, создадим задание на открытие при пожарной тревоге двери помещения, в котором произошло возгорание. На рисунке ниже показана территория "Стрелец", защищенная устройствами "Стрелец-ПРО" и управляемой СКУД ParsecNET 3 дверью:



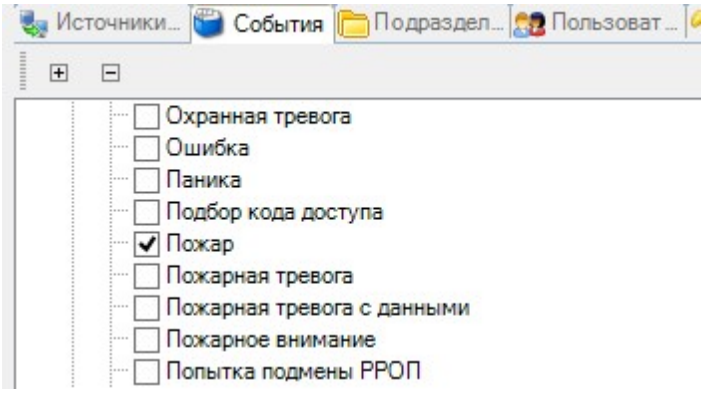
С помощью редактора заданий создайте задание для достижения взаимодействия систем по сигналу пожарной тревоги:



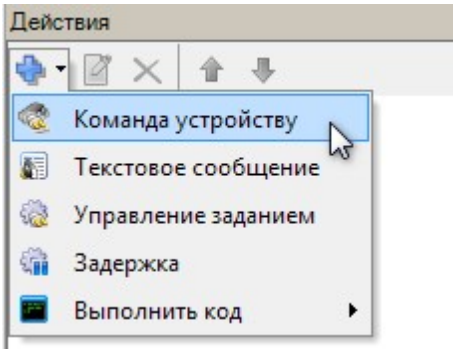
В качестве источника назначьте пожарный извещатель:



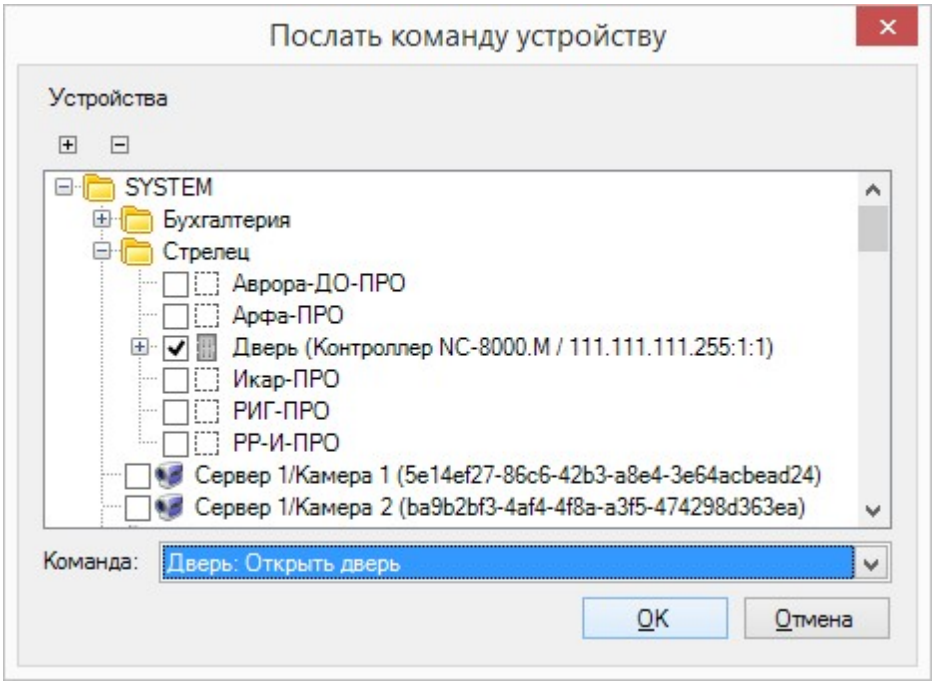
Событием, инициирующим выполнение задания, назначим "Пожар":



Теперь необходимо задать реакцию на выбранное событие. Для этого на панели действий редактора заданий выберите пункт "Добавить - Команда устройству":



В открывшемся диалоге выберите дверь и назначьте ей команду "Открыть дверь":



Таким образом можно организовать сколь угодно сложное взаимодействие любых компонентов любых систем, интегрированных в ParsecNET 3.

11.7.3 Система "Мурена"

Общие положения

Данный раздел не является руководством по использованию системы "Мурена", а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы "Мурена" обратитесь к оригинальному руководству.

Система периметральной охраны "Мурена" позволяет организовать защиту протяженных периметров с применением датчиков различных технологий. К одному блоку "Мурена " можно подключить в различных комбинациях до 4 извещателей различного типа.

- радиоволновый двухпозиционный линейный извещатель "Радон-М";
- проводноволновое средство обнаружения "Параллель-М";
- оптико-электронные пассивные инфракрасные извещатели "Сплав-М" или "МИК-01".

Количество подключаемых устройств типа "Мурена" в системе ParsecNET 3 не ограничено.

См. также:

Подключение и настройка[624]

Использование системы[627]

11.7.3.1 Подключение и настройка

До подключения охранной системы "Мурена" к системе ParsecNET 3 необходимо настроить все используемые "Мурено" блоки с помощью ее собственных средств - ParsecNET 3 не предназначен для этих целей. При этом настоятельно рекомендуется придерживаться следующей последовательности действий:

1. Остановите службу ParsecNET 3 Umirs;
2. Проведите настройки всех блоков "Мурена". Если к одному порту подключается более одного блока "Мурена", в процессе настройки им должны быть присвоены различные адреса;

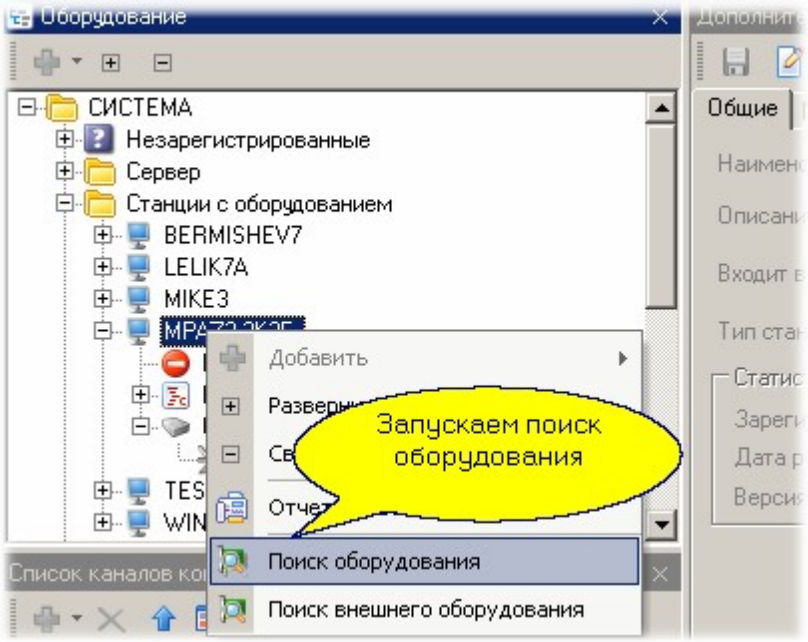
Важно: для обеспечения успешного поиска "Мурены" как минимум один блок должен иметь адрес в диапазоне от 1 до 5. Это связано с желанием ускорить поиск оборудования до приемлемой длительности.

3. Закройте все приложения охранной системы "Мурена";
4. Запустите службу ParsecNET 3 Umirs.

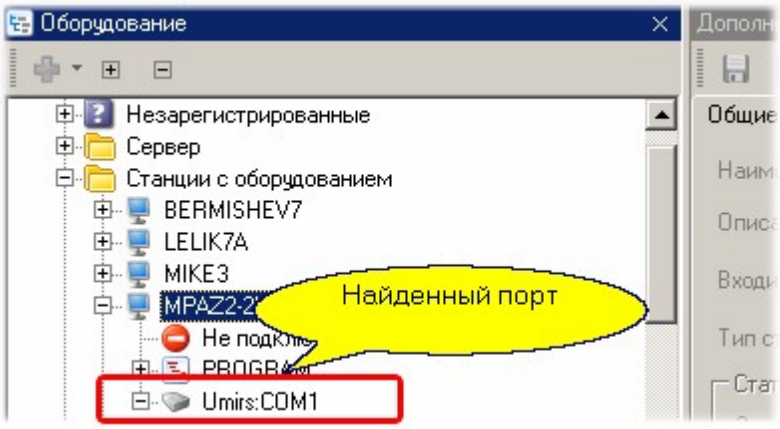
После того, как вышеуказанные действия выполнены и блоки "Мурены" подключены к COM-порту через конвертор COM - RS-485 (или к виртуальному COM-порту через конвертор USB - RS-485), можно приступить к поиску оборудования стандартными средствами:

Шаг 1. Поиск порта

В редакторе оборудования на ПК, к которому подключены блоки "Мурена", запускаем поиск оборудования.

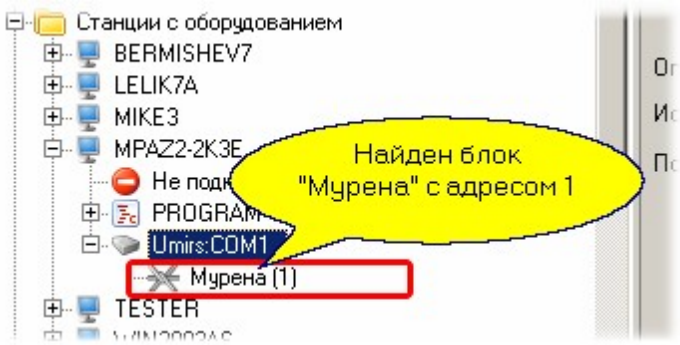


В результате появится порт "Мурена" (с именем Umirs и номером COM-порта), как показано на рисунке ниже.



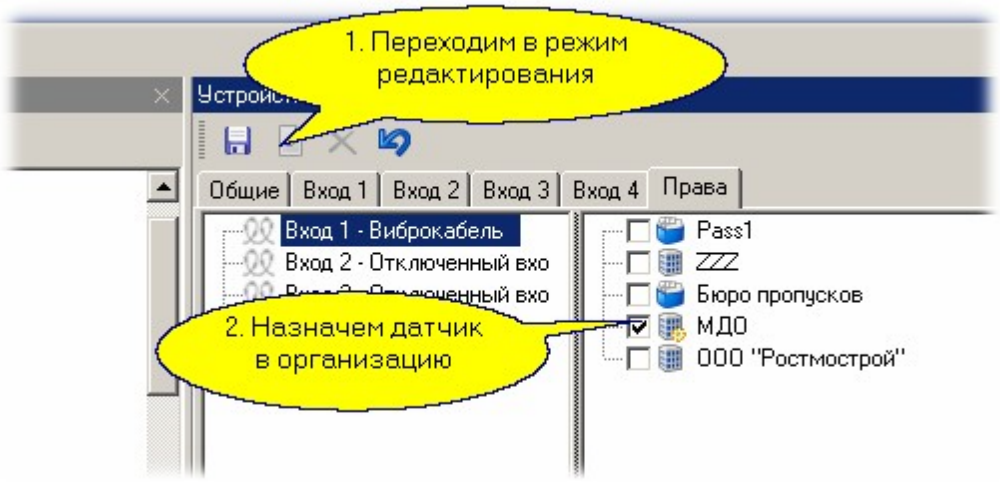
Шаг 2. Поиск блоков "Мурена"

Аналогично предыдущему шагу, на порту Umirs:COM1 (в нашем примере это COM-порт номер 1) запускаем поиск блоков "Мурена". В результате поиска должны появиться все подключенные блоки. В нашем примере - это только один блок с адресом "1" на линии RS-485:



Шаг 3. Распределение оборудования

Последний шаг - распределение оборудования по организациям. Делается это на карточке блока "Мурена" на вкладке *Права*, как показано на рисунке ниже:



Не забудьте сохранить результаты своих действий.

На этом процесс подключения и настройки заканчивается. При необходимости можно ввести датчики "Мурены" на графические планы системы.

См. также:

Система "Мурена"[624]

Использование системы[627]

11.7.3.2 Использование системы

В целом использование системы "Мурена" не отличается от использования других подсистем охраны. Установленная и сконфигурированная система будет порождать стандартные тревожные события, которые будут отображаться в мониторе событий, вызывать необходимые реакции, например, через менеджер заданий.

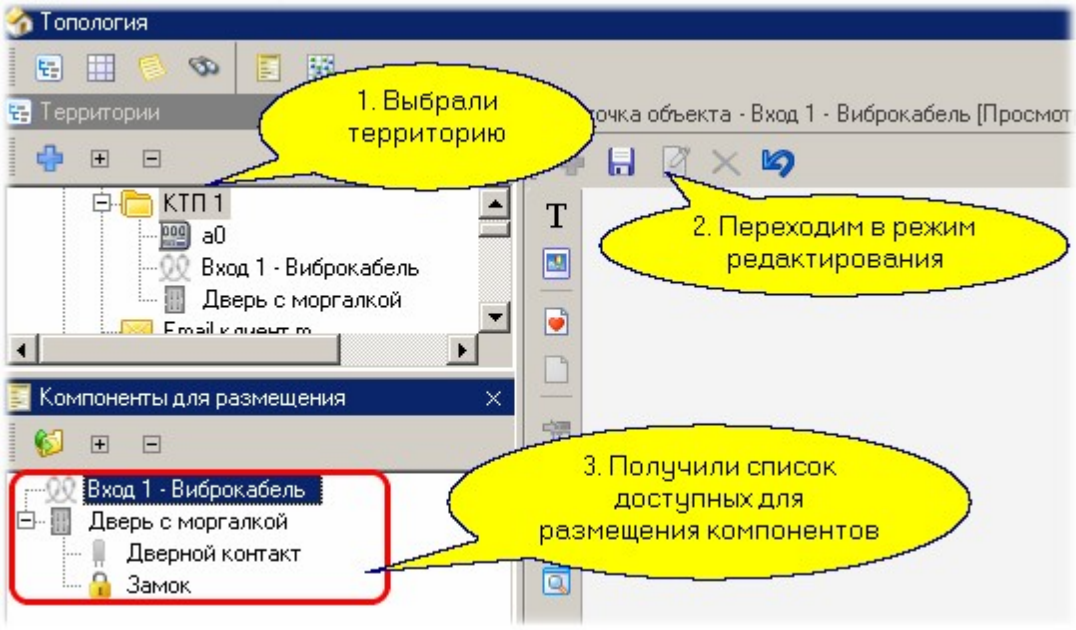
Специфическим для "Мурены" является представление ее датчиков на графических планах. Поскольку датчики "Мурены" защищают протяженные участки периметра, причем иногда не прямолинейной формы, для этих датчиков создан специальный компонент графических планов.

Ниже мы покажем, как ими пользоваться при создании графического плана объекта.

В редакторе топологии открываем закладку графического плана и создаем план для нашей территории. Мы не описываем в данном примере размещение подложки с изображением очертаний территории, перейдем сразу к размещению на плане изображения виброкабеля, проложенного по криволинейной границе периметра.

Шаг 1.

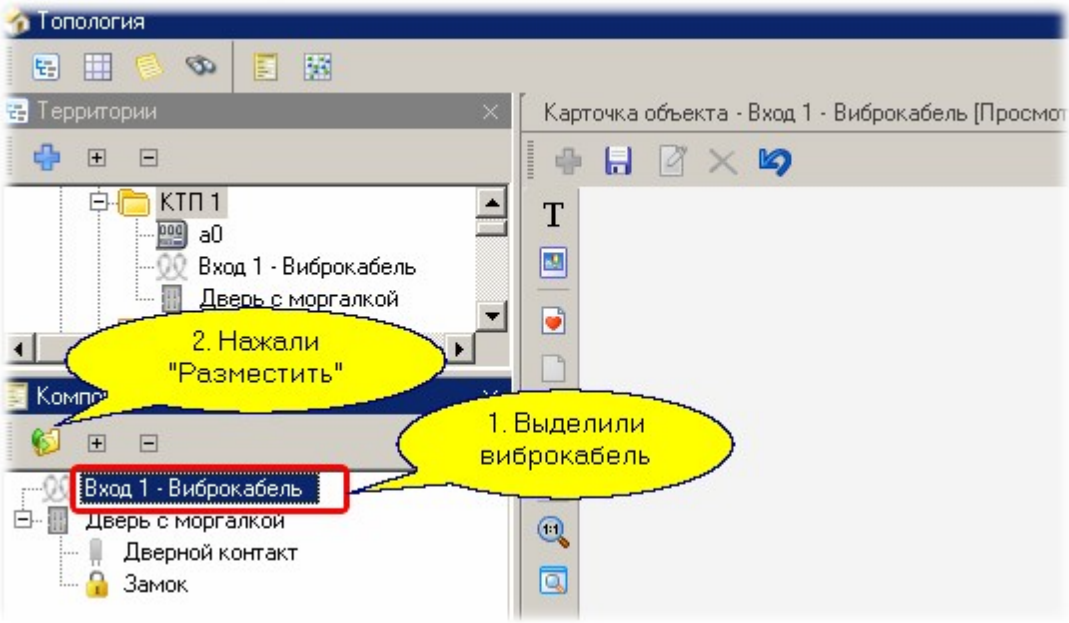
Открываем редактирование графического плана для территории, к которой относится виброкабель блока "Мурена":



Естественно, предварительно размещаемые компоненты должны быть внесены на требуемую территорию.

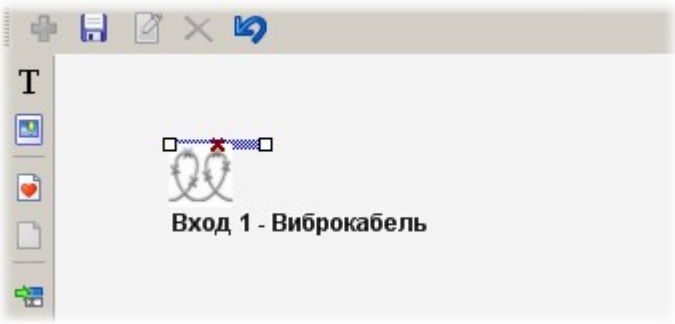
Шаг 2.

Далее с панели "Компоненты для размещения" переносим компонент "Вход 1 - виброкабель" на графический план:

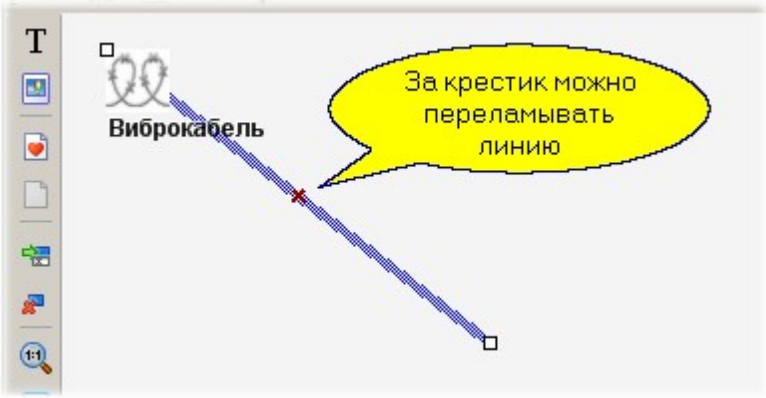


Шаг 3.

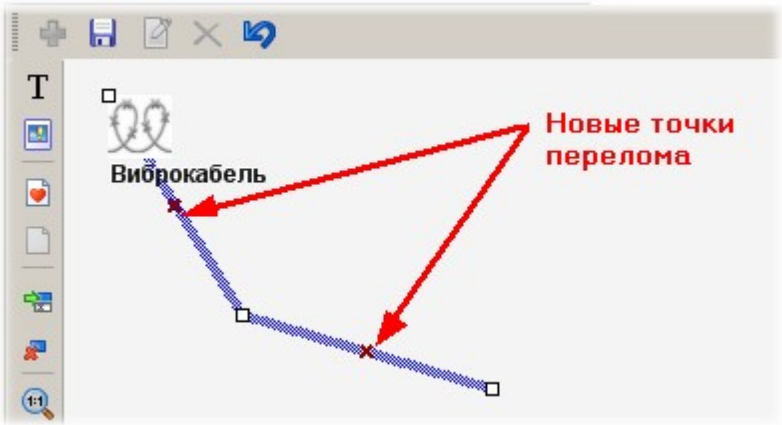
Теперь поменяем конфигурацию виброкабеля. Изначальное изображение показано на следующем рисунке:



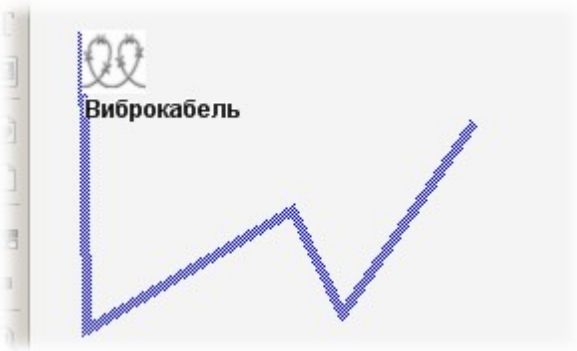
За квадратики по концам горизонтальной линии можно перемещать ее концы в любом направлении. Для примера вытянем линию по диагонали:



Как показано на рисунке, "ухватив" линию за красный крестик, ее можно переломить в любом направлении. При этом на образовавшихся новых отрезках вновь появляются крестики:



Процедуру можно повторять до тех пор, пока форма линии не станет повторять конфигурацию прокладки виброкабеля:



Шаг 4.

Сохранили графический план. Если теперь открыть вкладку графического плана в мониторе событий и инициировать тревогу, то изображение виброкабеля на плане окрасится в красный цвет. При нормальном состоянии цвет кабеля на графическом плане будет оставаться зеленым.

См. также:

Создание графпланов[208]

11.7.4 Интегрированная система охраны "Орион"

ПО ParsecNET 3 полностью поддерживает всё оборудование охранно-пожарных систем "Болид", подключаемое посредством преобразователя протоколов С2000-ПП[630] или шлюза С3000-Hub[638], и позволяет ставить и снимать территории с охраны, управлять реле вручную или по событиям от устройств (охранных датчиков). Также производится постоянный мониторинг состояний элементов системы "Орион".

Интегрированный модуль не поддерживает работу оборудования СКУД "Болид", например, контроллер доступа С2000-2.

Данный раздел не является руководством по использованию системы "Орион", а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения системы "Орион" обратитесь к соответствующему руководству.

11.7.4.1 С2000-ПП. Подключение и настройка

Общий пример передачи управления оборудованием ИСО "Орион" системе ParsecNET 3 на примере преобразователя протоколов С2000-ПП:

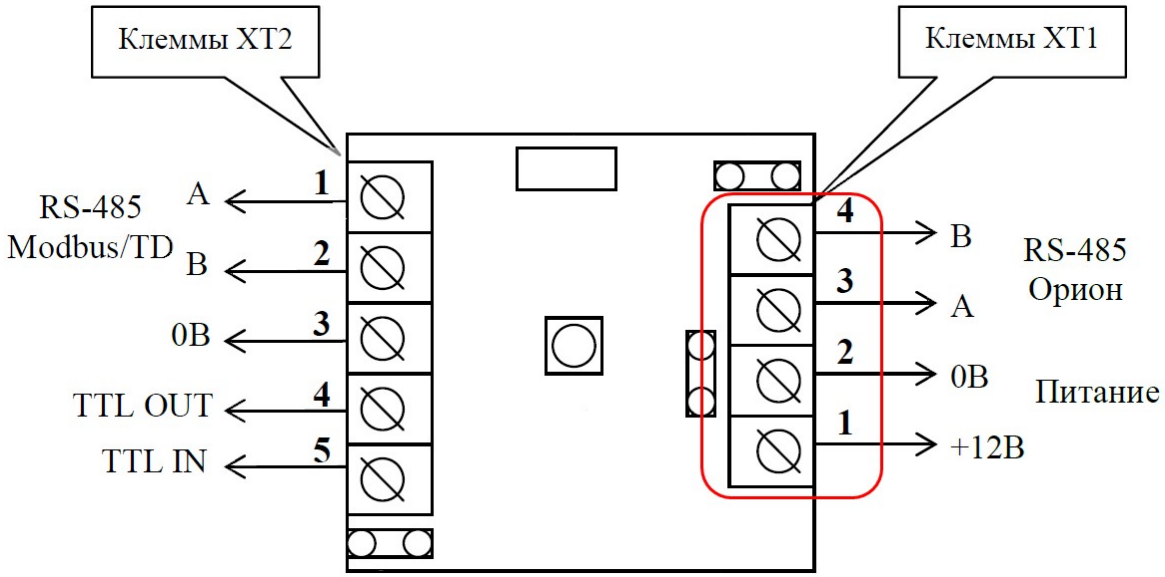
1. Организация, уже использующая систему "Орион", устанавливает оборудование и ПО ParsecNET 3.

   Для работы с системой "Орион" посредством ПО ParsecNET 3 она должна содержать подключенный и сконфигурированный своими штатными средствами С2000-ПП (см. описание в руководствах, доступных на сайте производителя);
2. ИСО "Орион" настраивается на передачу транзакций через устройство С2000-ПП, подключенное к серверу ParsecNET 3 через USB-UART преобразователь (подключение описано ниже);
3. Настройки С2000-ПП передаются в систему ParsecNET 3 посредством xml-файла, после чего пользователю доступна работа с устройствами "Болид" через ПО ParsecNET 3. Действия по экспорту-импорту настроек описаны ниже.

Экспорт настроек С2000-ПП

Подключите С2000-ПП через USB-UART преобразователь к серверу системы ParsecNET 3. При этом подсоедините USB-UART преобразователь к клеммам XT1 С2000-ПП параллельно шине RS-485 Орион (см. рис. ниже).

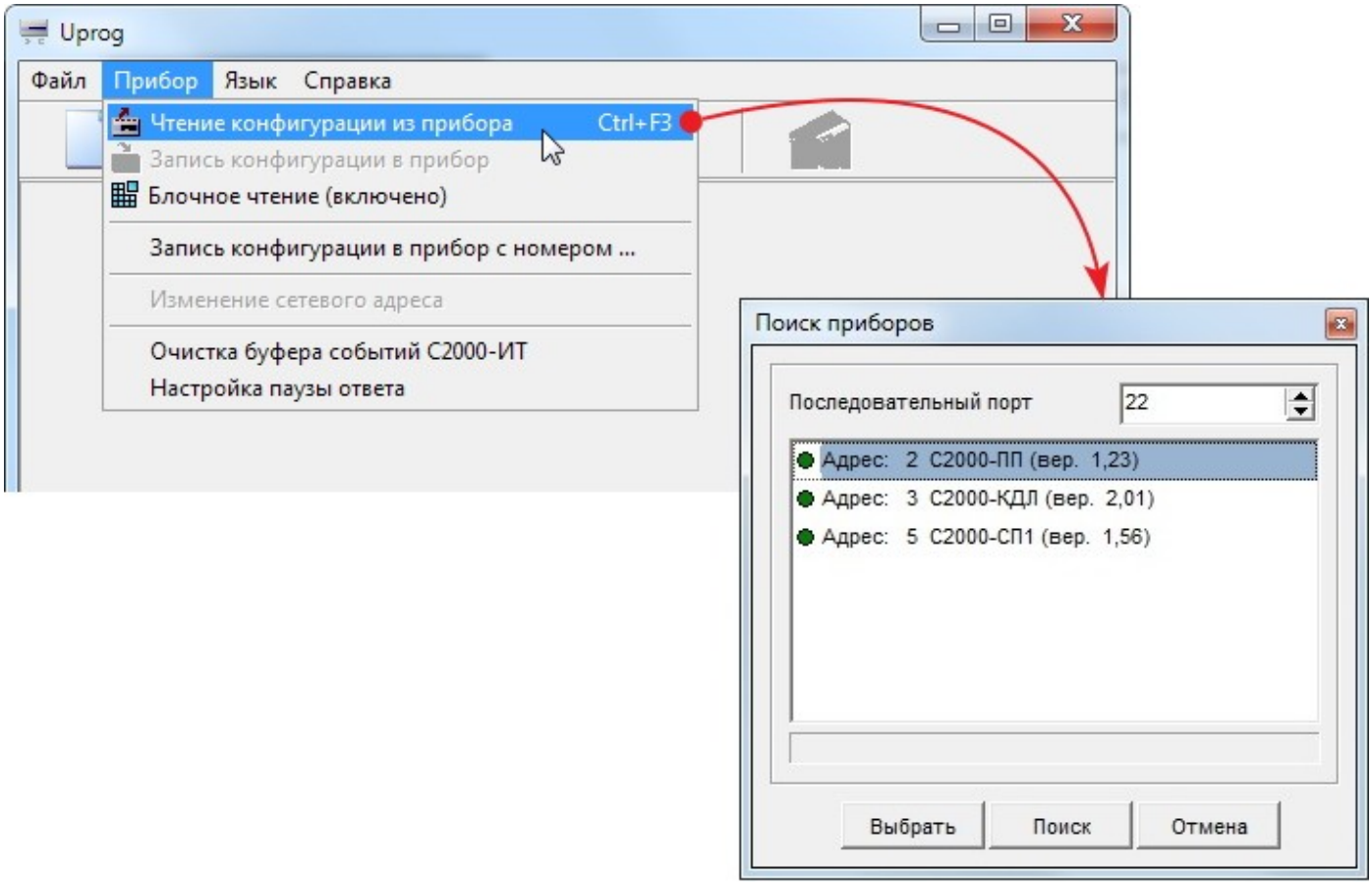
В качестве преобразователя USB-UART можно использовать преобразователь интерфейсов USB-RS485 производства "Болид".



После подключения запустите на сервере ParsecNET 3 программу Uprog, скачать которую можно с сайта производителя.

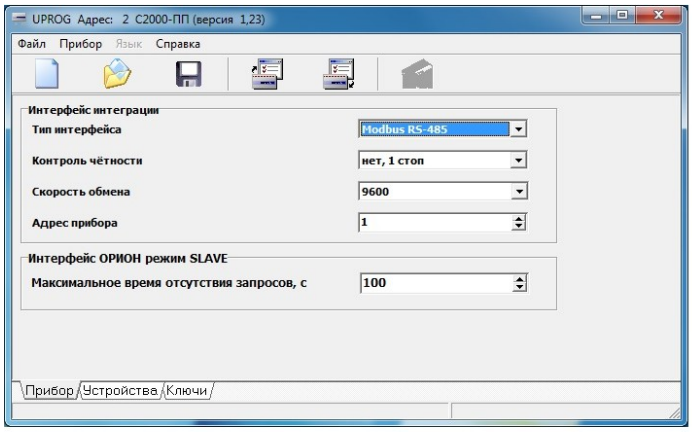
В главном меню выберите "Прибор - Чтение конфигурации из прибора". В открывшемся окне выбора порта установите номер порта, к которому подключен USB-UART преобразователь, и нажмите на кнопку *Поиск*.

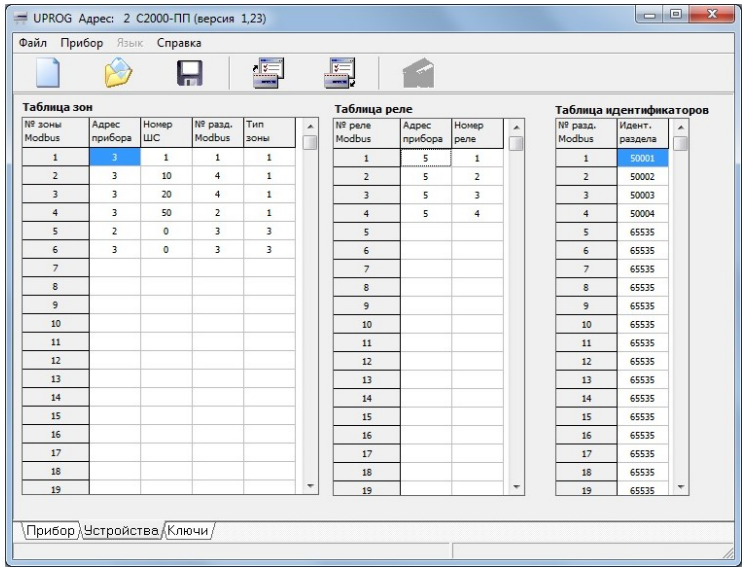
После того, как программа обнаружит подключенные к указанному порту устройства, выделите преобразователь С2000-ПП и нажмите на кнопку *Выбрать* (см. рис. ниже). Если нужное устройство на этом порту не обнаружено, проверьте правильность номера порта, при необходимости исправьте его, и повторите поиск.



Программа начнет сбор конфигурационной информации.

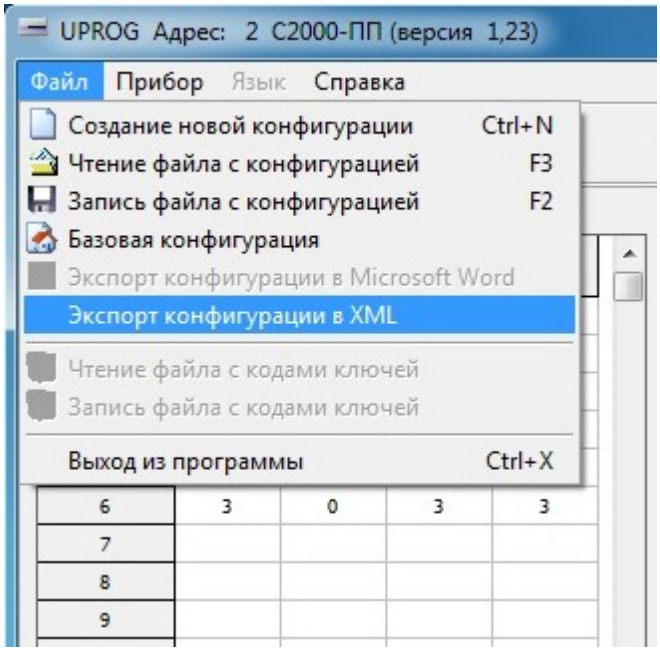
Если в процессе чтения будет появляться сообщение "Прибор не отвечает. Продолжить?", нажимайте на кнопку *Yes*, пока сбор информации не завершится. По окончании сбора информация будет выведена в окно программы в трех вкладках (см. рис. ниже).





Теперь необходимо экспортировать конфигурационные данные в файл xml.

Для этого в главном меню выберите "Файл - Экспорт конфигурации в XML" (см. рис. ниже) и сохраните файл.

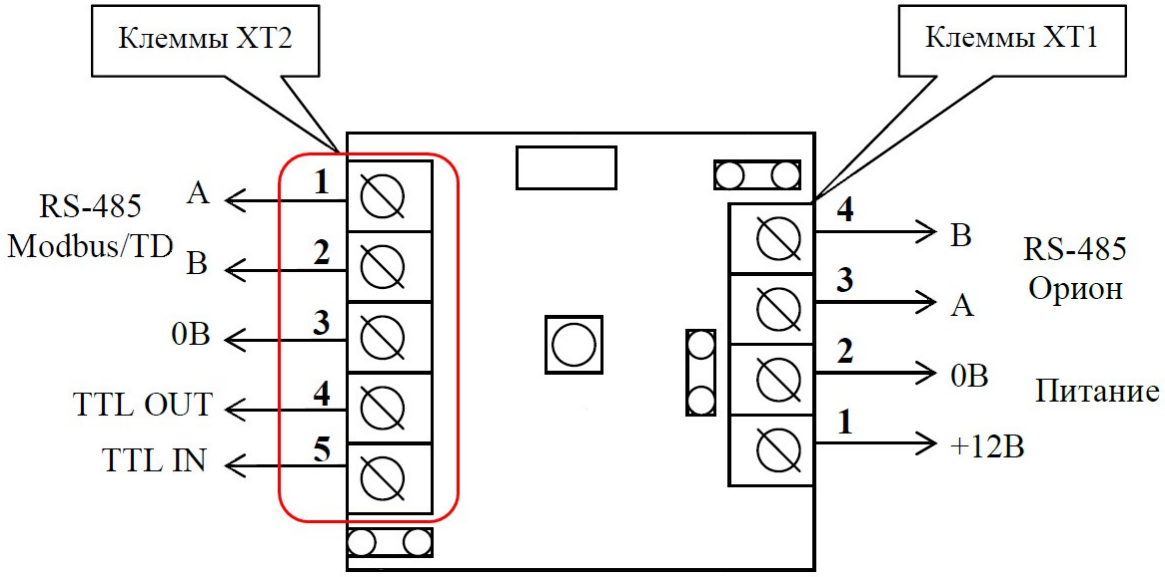


Настройка оборудования в системе ParsecNET 3

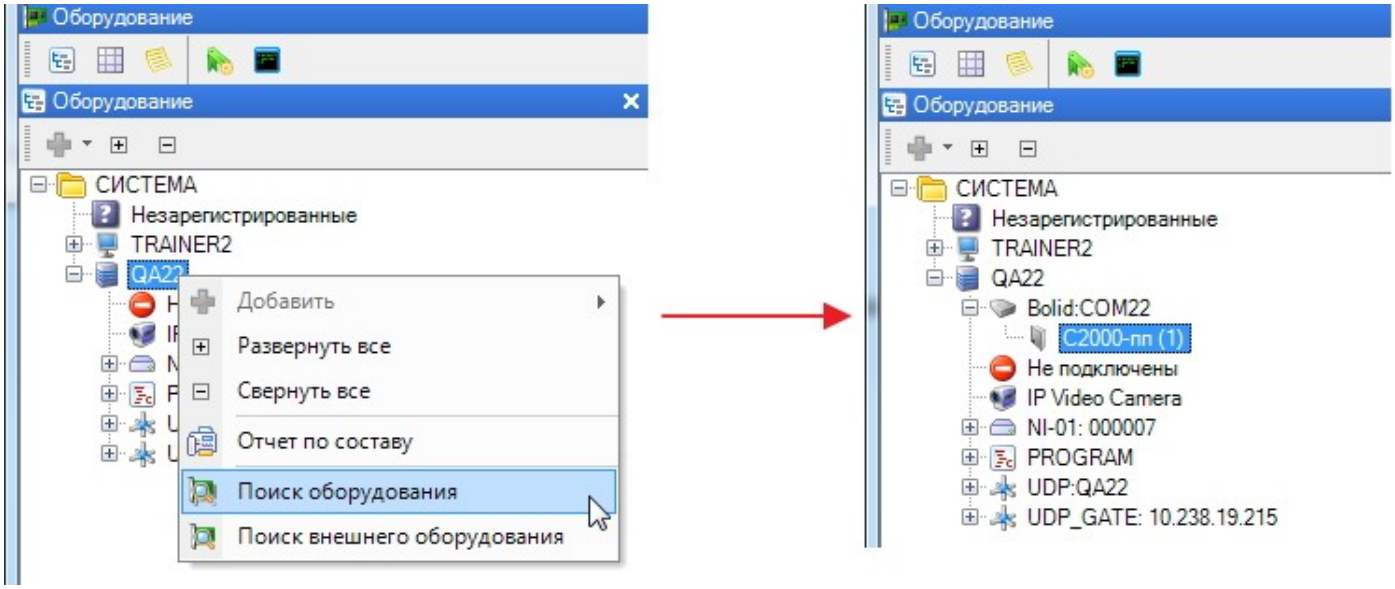
Теперь можно перейти к настройке оборудования "Болид" в системе ParsecNET 3.

Для этого первым действием измените подключение USB-UART преобразователя к С2000-ПП. Подключите преобразователь на Modbus-сторону С2000-ПП, т.е. подключите его к клеммам XT2 (см. рис. ниже).

Недопустимо подключение устройств ОПС Орион и преобразователей к одним и тем же клеммам. Каждый тип устройства должен быть подключен к своим клеммам С2000-ПП.

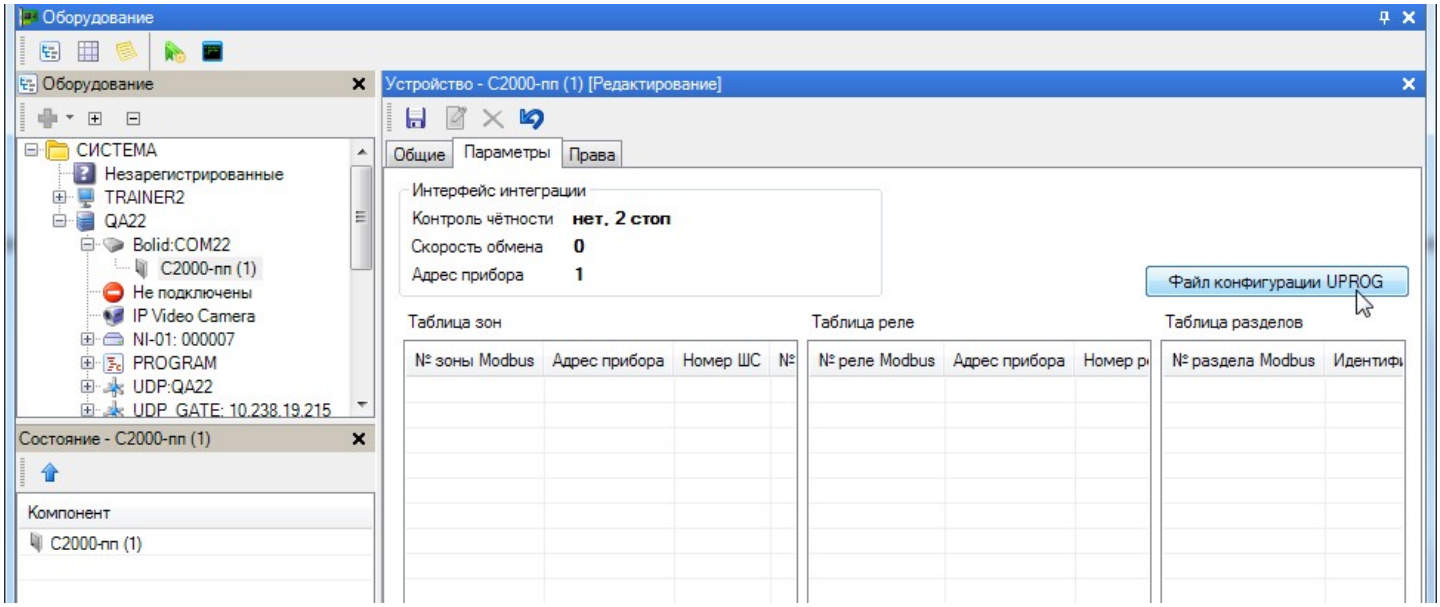


Запустите консоль администрирования ParsecNET 3 и в редакторе оборудования запустите поиск оборудования. Через некоторое время система обнаружит подключенный преобразователь протоколов С2000-ПП (см. рис. ниже).

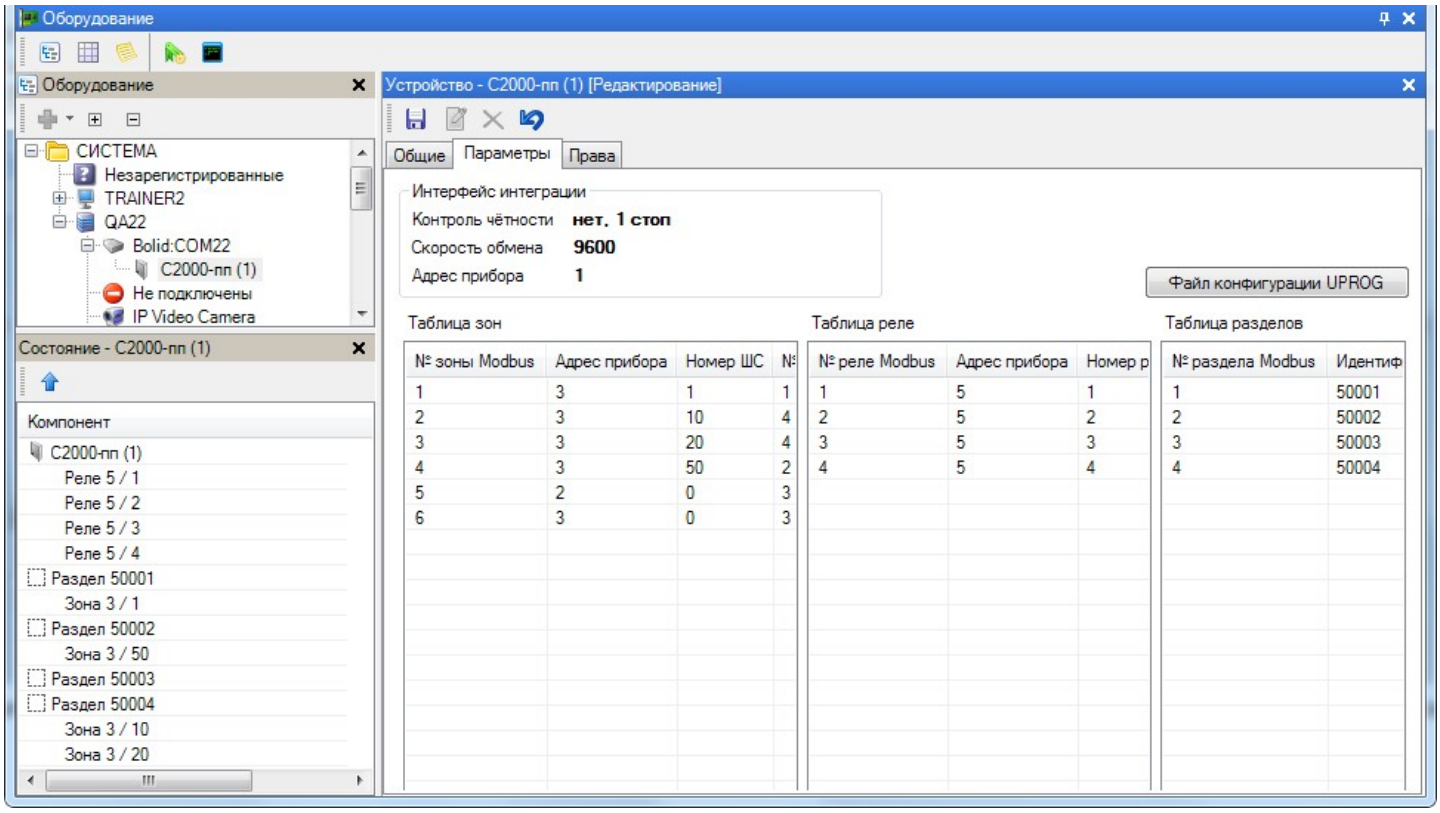


Выделите С2000-ПП и переведите его в режим редактирования настроек, нажав на кнопку  *(Редактировать)* в карточке устройства.

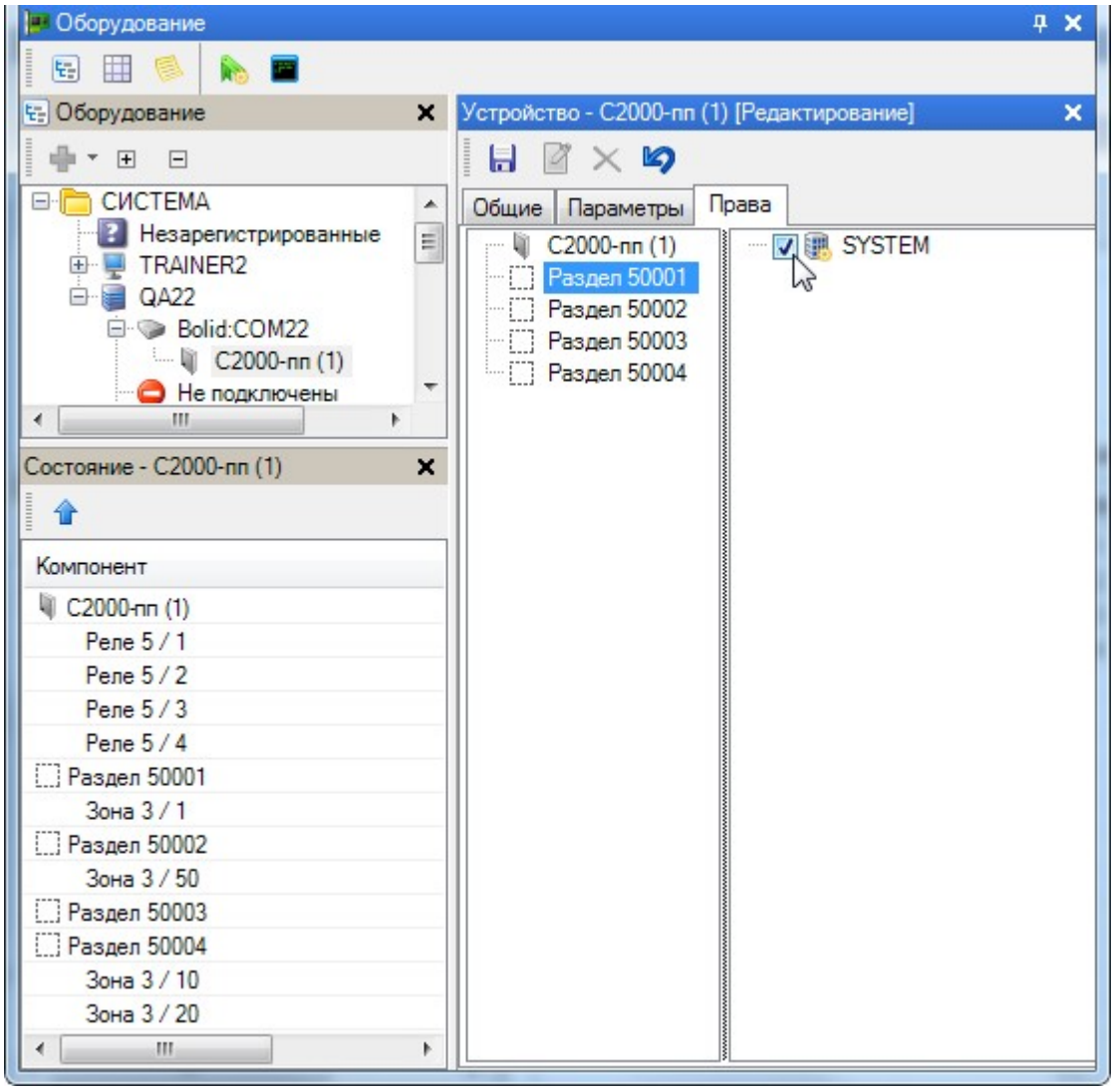
Перейдите на вкладку *Параметры* и нажмите на появившуюся кнопку *Файл конфигурации UPROG* (см. рис. ниже).



В открывшемся окне браузера укажите место расположения созданного ранее XML-файла и нажмите на кнопку *Открыть*. Конфигурационные данные будут экспортированы в ПО ParsecNET 3 (см. рис. ниже).

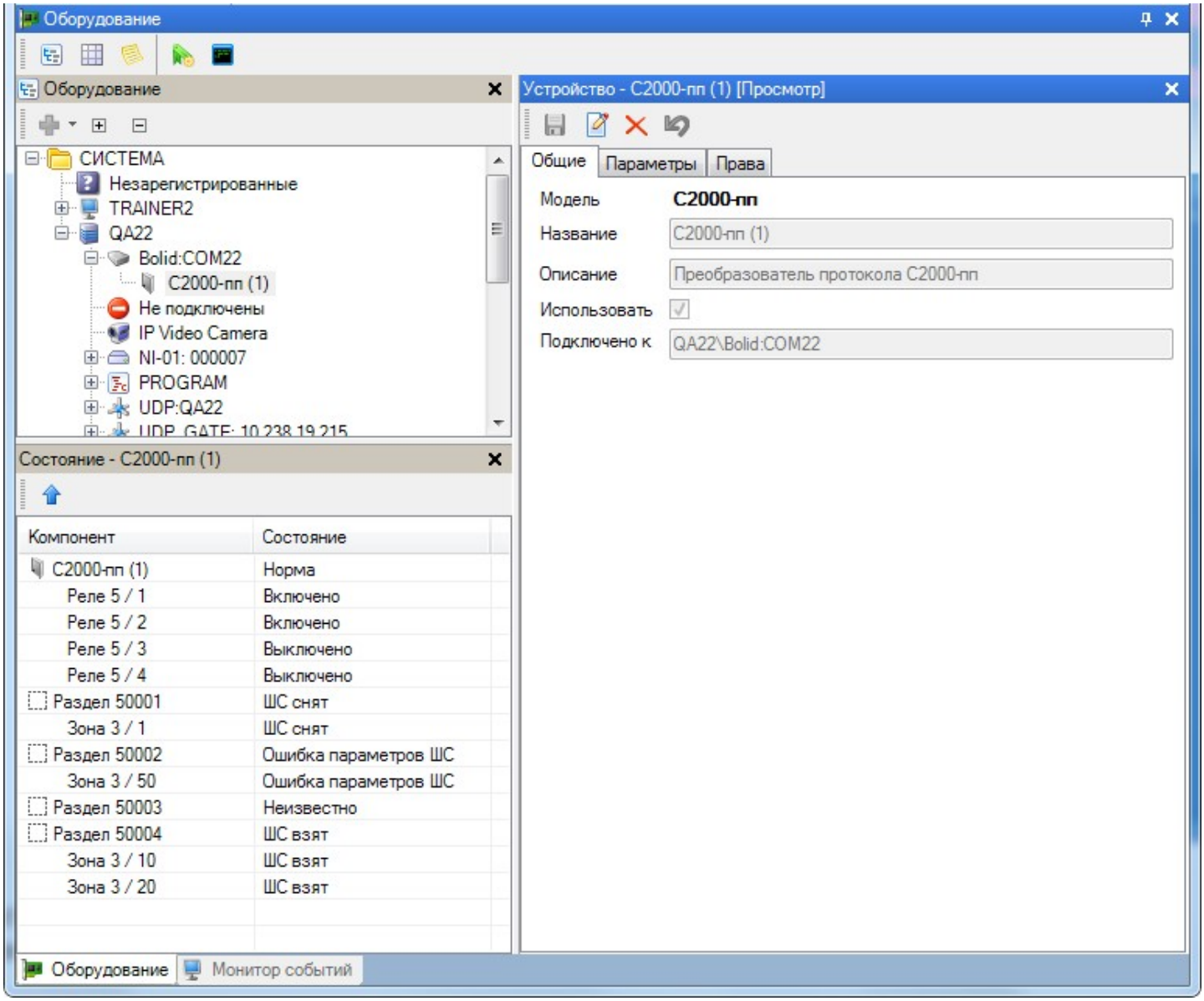


Перейдите на вкладку *Права* и предоставьте право на работу с охранными зонами нужным пользователям. В примере на рисунке ниже пользователь один - SYSTEM.



Сохраните настройки, нажав на кнопку (*Сохранить*) в карточке устройства.
На этом настройка оборудования системы "Болид" в ПО ParsecNET 3 завершена.

11.7.4.1.1 Использование С2000-ПП



Как видно на примере, изображенном на рисунке, в системе "Орион" имеются 4 реле и 4 охранные зоны, которые обслуживаются датчиками. При этом они имеют следующие состояния:

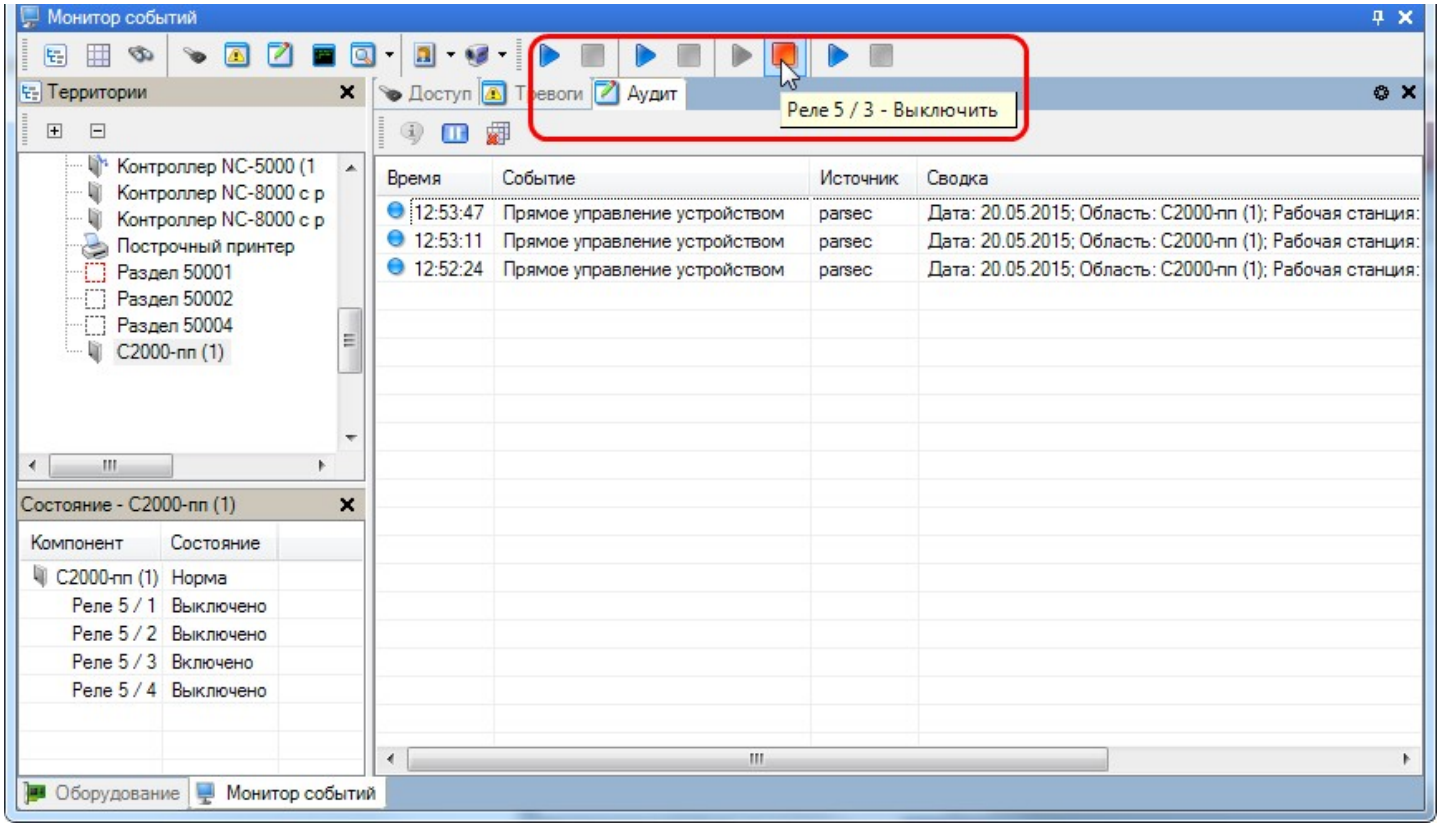
- Реле 1 и 2 - включены, т.е. подключенные к ним исполнительные устройства активны;
- Реле 3 и 4 - выключены;
- Зона 1 снята с охраны ("ШС" - шлейф состояния);
- Зона 50 - проверьте корректность настройки шлейфа состояния в системе "Болид";
- Зоны 10 и 20 взяты под охрану.

В редакторе оборудования отображаются только текущие состояния элементов охранной системы. Управление элементами и просмотр сообщений о событиях осуществляется через консоль монитора событий.

Управление реле

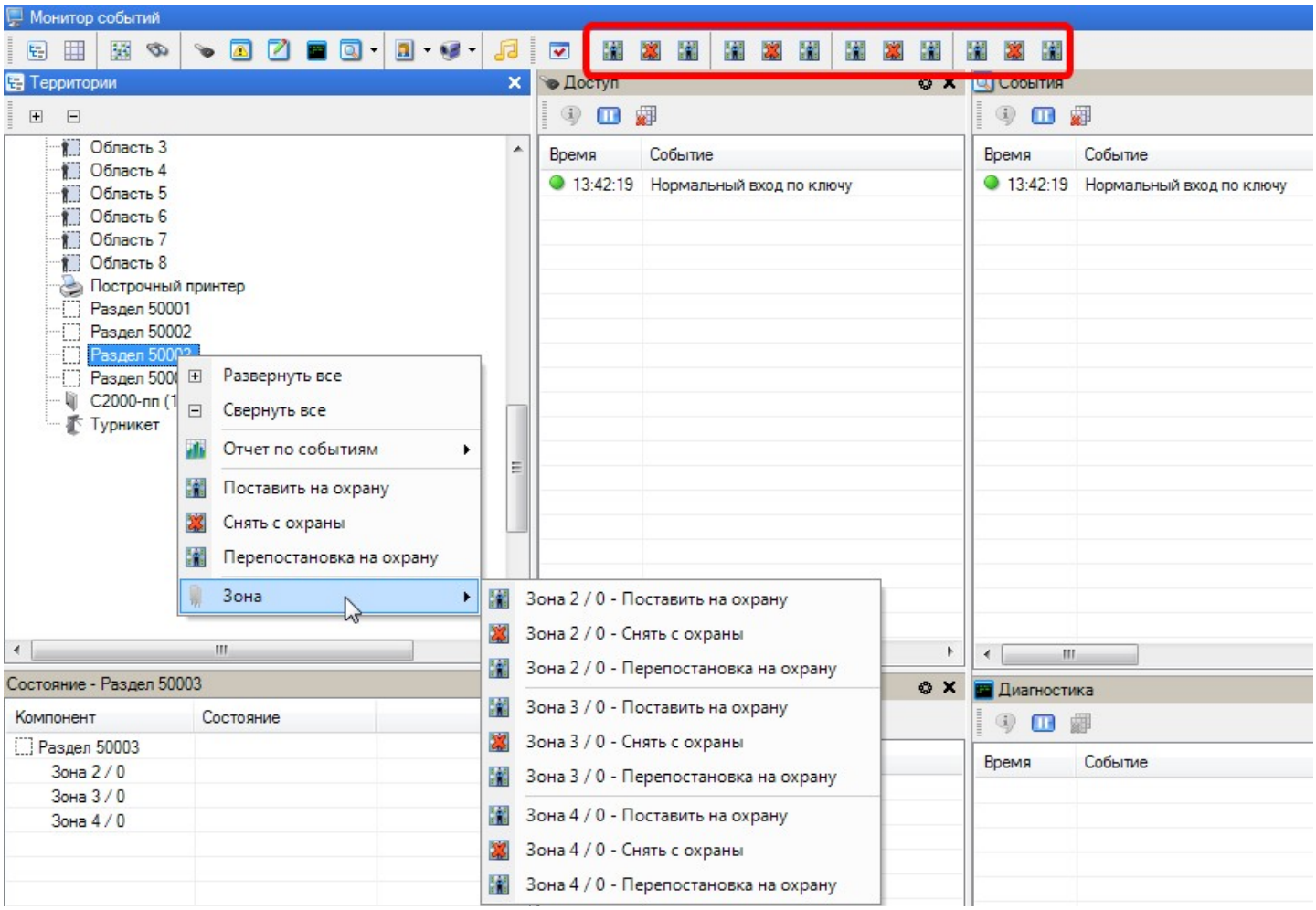
При выборе в списке территорий устройства С2000-ПП, на панели состояний отобразятся все его компоненты (реле), а на панели инструментов монитора появятся кнопки управления этими

реле. События включения и выключения реле порождают соответствующие сообщения (см. рис. ниже).



Управление разделами

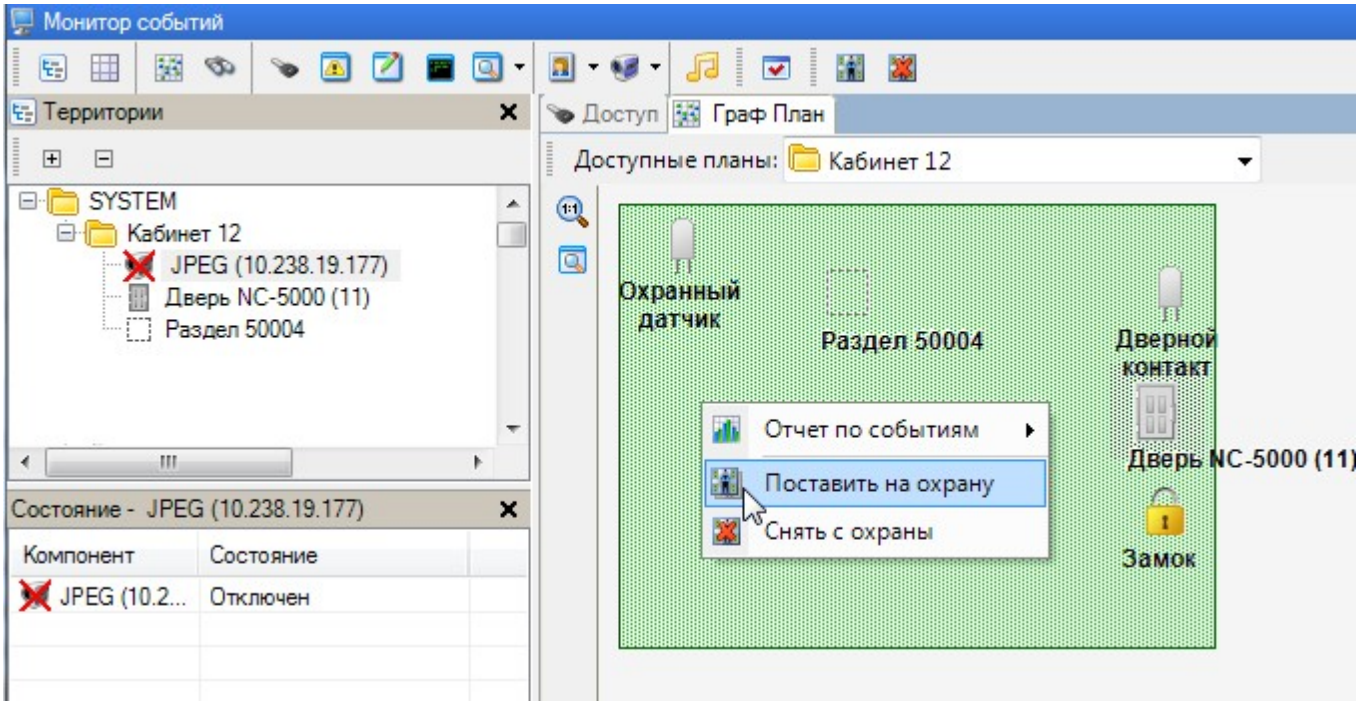
Раздел в системе "Орион" может содержать одну или несколько охранных зон, обслуживаемых каждая своим датчиком. Например, кабинет может быть защищен пожарным датчиком и датчиком движения. В таком случае раздел будет содержать две зоны. Постановка и снятие с охраны как всего раздела, так и каждой зоны в отдельности производится из контекстного меню либо с панели инструментов монитора. Изменение состояния зоны и/или раздела отображается в окне событий (см. пример на рис. ниже).



Команда "Перепостановка на охрану" используется после приема тревоги для возврата зоны под охрану. Последовательное выполнение двух действий - "Снять с охраны" и "Поставить на охрану" - имеет тот же результат.

Компоненты С2000-ПП на графических планах

Если компоненты системы размещены на графическом плане в редакторе топологии, то как и для компонентов СКУД ParsecNET 3, пользователь получает возможность наблюдения на плане в мониторе событий статуса компонентов и управления ими:



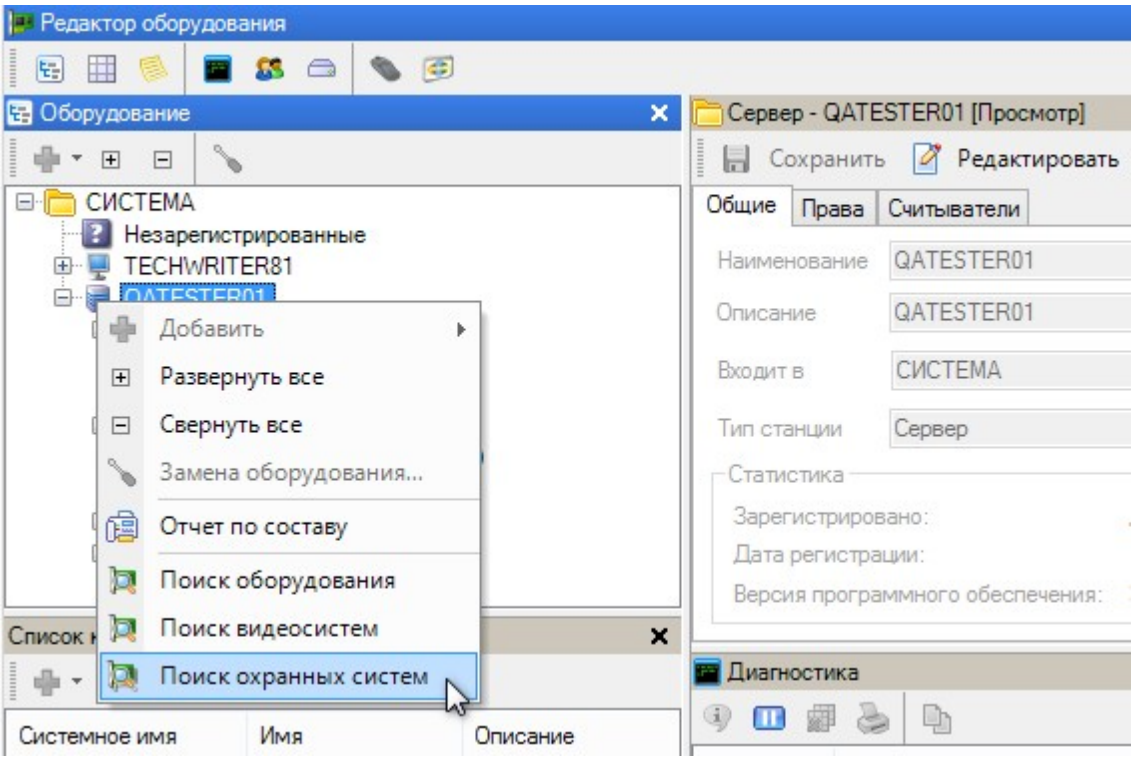
11.7.4.2 С3000-Hub. Подключение и настройка

С3000-Hub - это устройство , которое представляет из себя IP-шлюз для подключения к сети нескольких линий устройств Болид. С помощью интеграционного модуля на текущий момент реализовано выполнение такими подключенными устройствами Болид следующих команд:

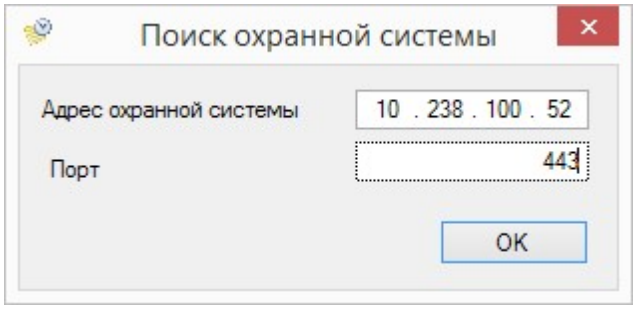
- Постановка на охрану;
- Снятие с охраны;
- Перепостановка на охрану (последовательно выполнение двух команд: "Снятие с охраны" и "Постановка на охрану").

Связь с С3000-Hub осуществляется по протоколу WebSocket, возможно обычное либо зашифрованное (wss) соединение. Для защищенного соединения необходимо предварительно сгенерировать сертификаты безопасности и импортировать его в ОС Windows на той машине, где установлен драйвер С3000-Hub. Процедура генерации сертификатов и их импорта описана в руководстве по эксплуатации С3000-Hub, доступном на сайте производителя.

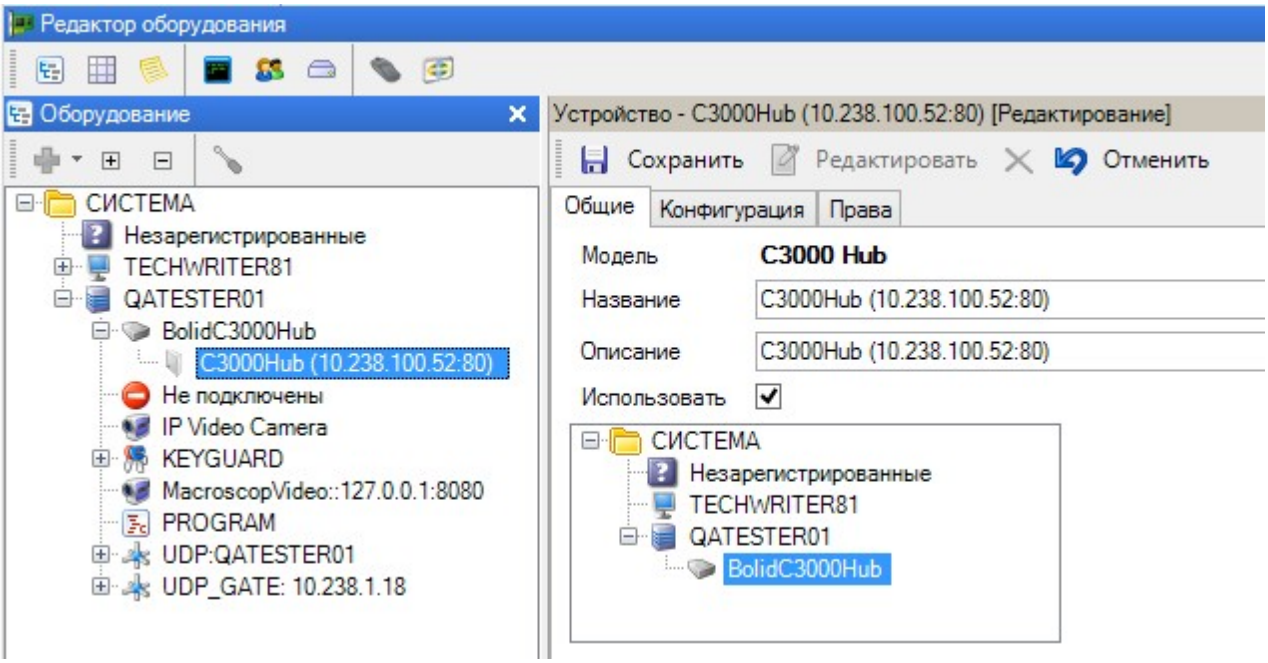
После установки и настройки шлюза С3000-Hub в редакторе оборудования ParsecNET 3 в контекстном меню выберите команду *Поиск охранных систем*:



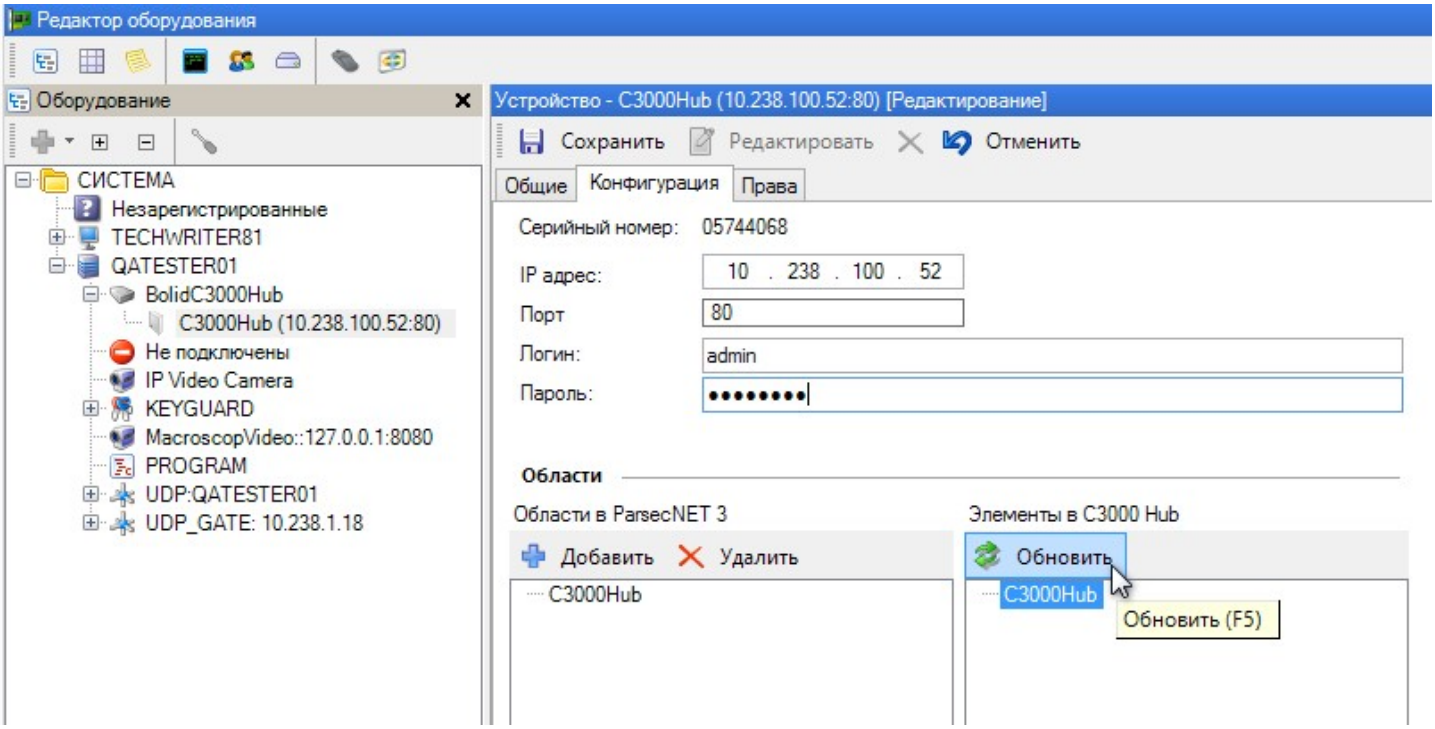
В появившемся окне введите IP-адрес шлюза и порт, который он использует для работы (80 для обычного или 443 для защищенного соединения):



После завершения поиска в дереве оборудования появится канал BolidC3000Hub. На вкладке *Общие* в режиме редактирования вы можете изменить название и описание шлюза, а также включить/выключить его использование в СКУД ParsecNET 3 (флажок *Использовать*):



На вкладке *Конфигурация* введите логин/пароль для доступа к шлюзу (по умолчанию это admin / c3000Hub), затем нажмите на кнопку *Обновить*. Это позволит обнаружить датчики и другие устройства, подключенные к шлюзу:

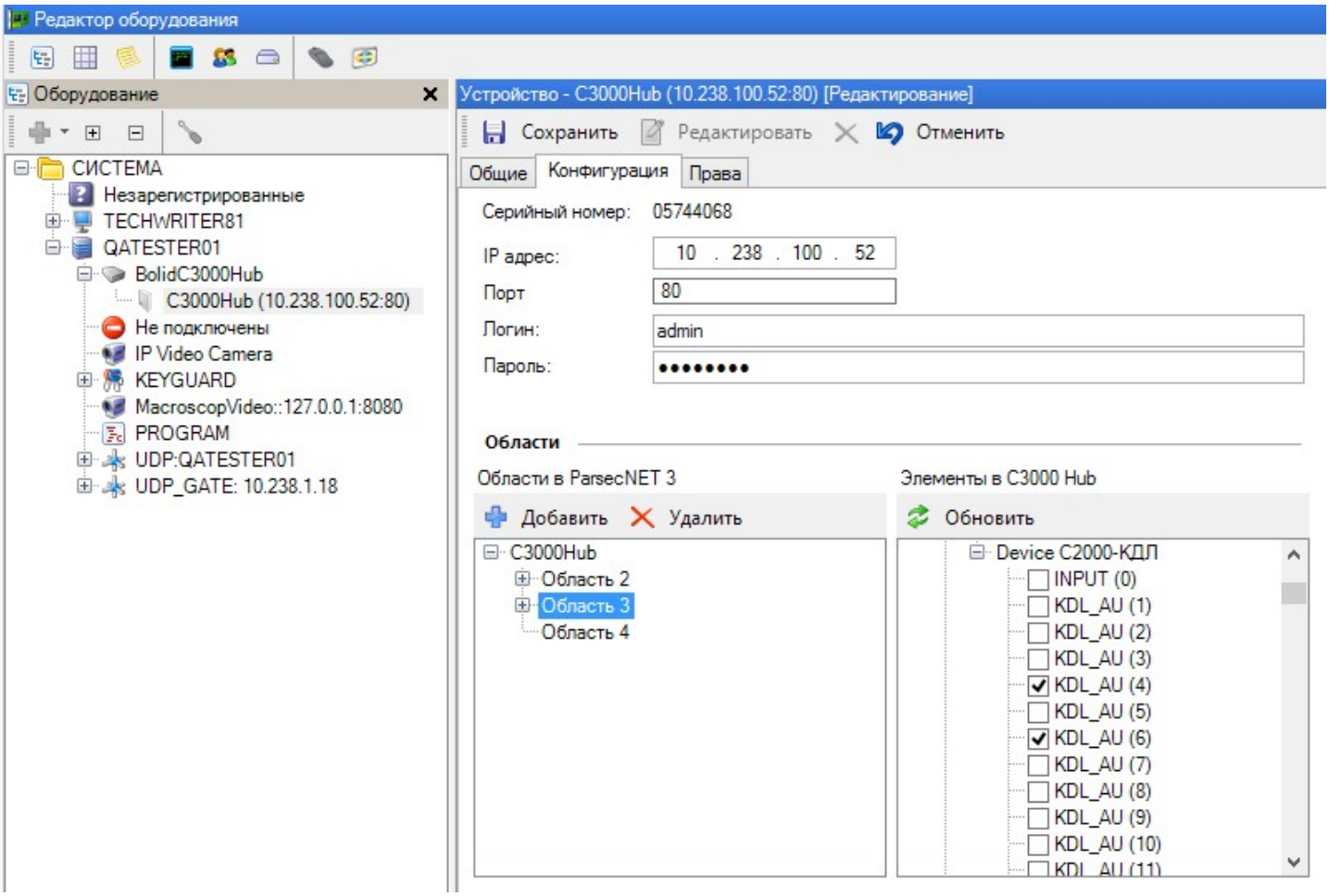


При нажатии на кнопку *Обновить* на правой панели *Элементы в C3000Hub* отобразятся сохраненные в БД либо активные устройства охранной системы. Причем если устройство сохранено в БД, то показываются сохраненные тип и версия. Если активное устройство не сохранено в БД , то после его отключения и нажатия на кнопку *Обновить* оно пропадет из этой панели.

На левой панели можно добавить охраняемые этими элементами области, которыми необходимо управлять посредством СКУД ParsecNET.

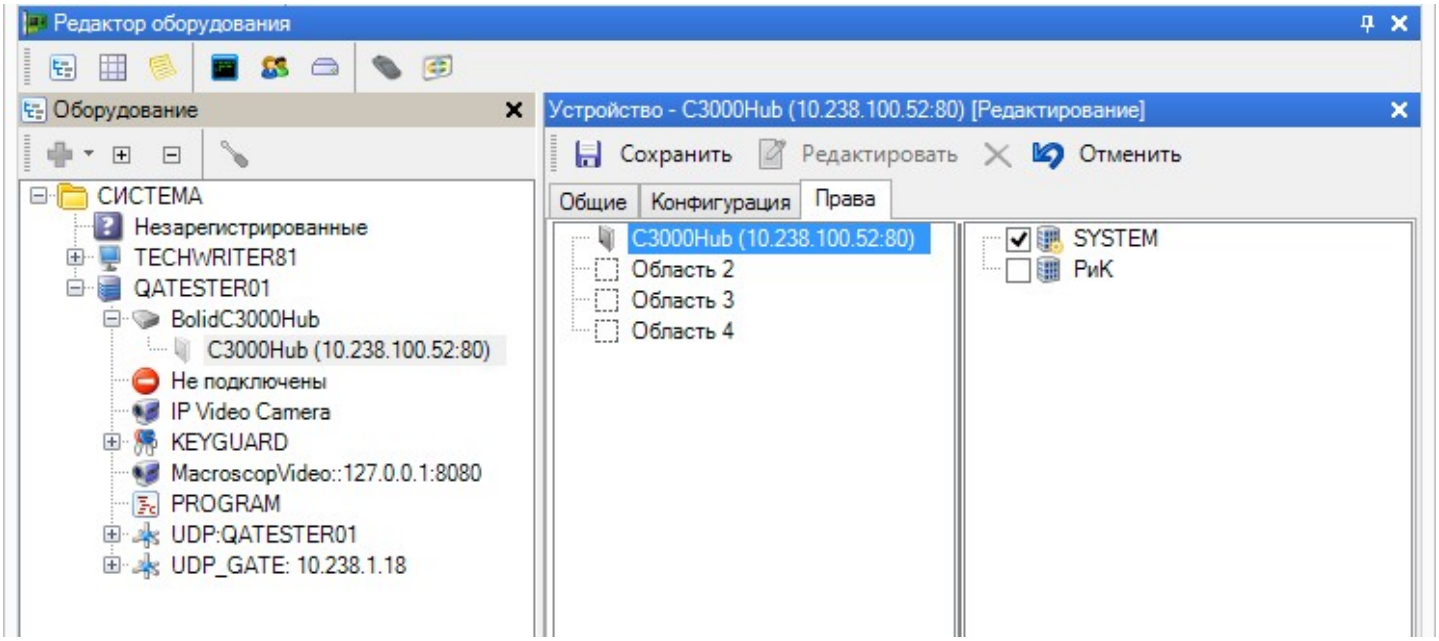
Нажимая на кнопку *Добавить*, добавьте необходимое количество охранных областей.

Выделив область, установите флажок у того датчика или устройства, которое охраняет эту область:



Установите таким способом связь территорий и задействованных для их охраны устройств.

На вкладке *Права* необходимо указать, какие организации будут иметь доступ к шлюзу и охранным областям. Для этого выделите шлюз или область и на правой панели поставьте флажки у нужных организаций. Операторы тех организаций, у которых не поставлены флажки, не смогут "видеть" этот шлюз или выбранные области в программе ParsecNET 3 и, соответственно, использовать их в своей топологии:



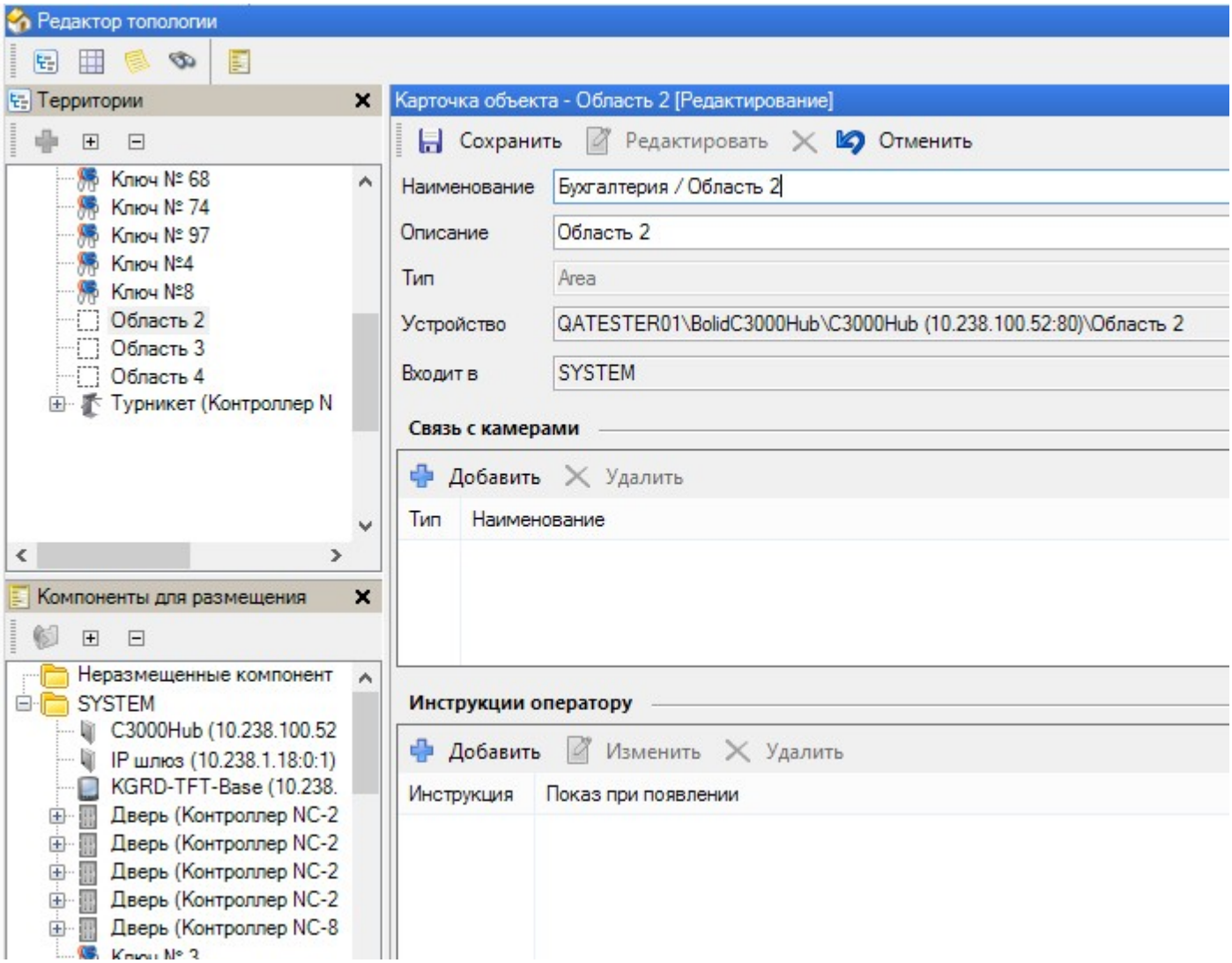
Для сохранения внесенных изменений нажмите на кнопку *Сохранить*.
На этом настройка шлюза C3000-Hub в системе ParsecNET 3 завершена.

11.7.4.2.1 Использование C3000-Hub

Редактор топологии

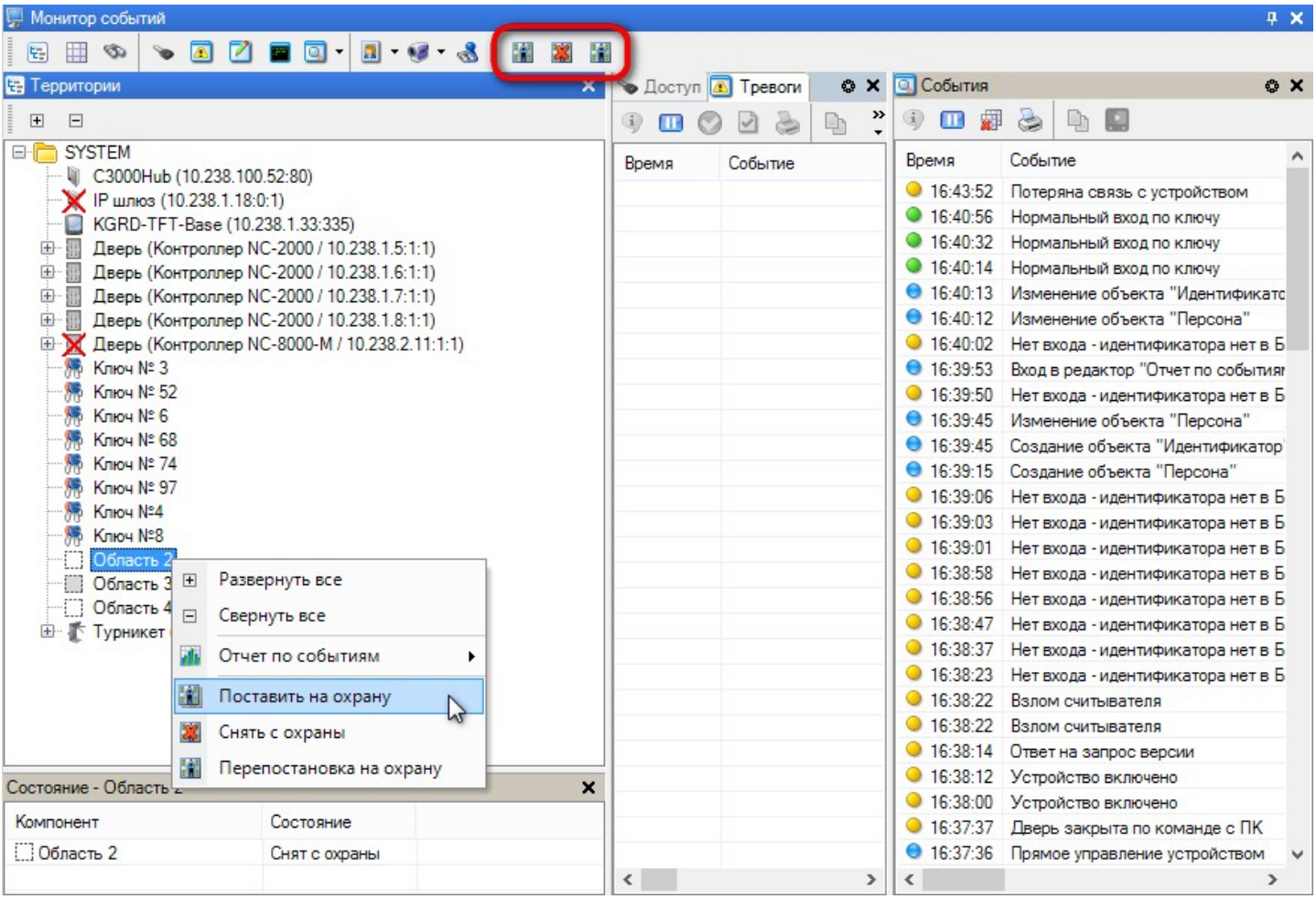
В редакторе топологии можно изменить название и/или описание охранной области так, как удобно.

Кроме этого, можно связать[211] область с видеокамерой, использованной в этой области. А также задать инструкции оператору[212] при возникновении тех или иных тревожных событий в данной области:



Монитор событий

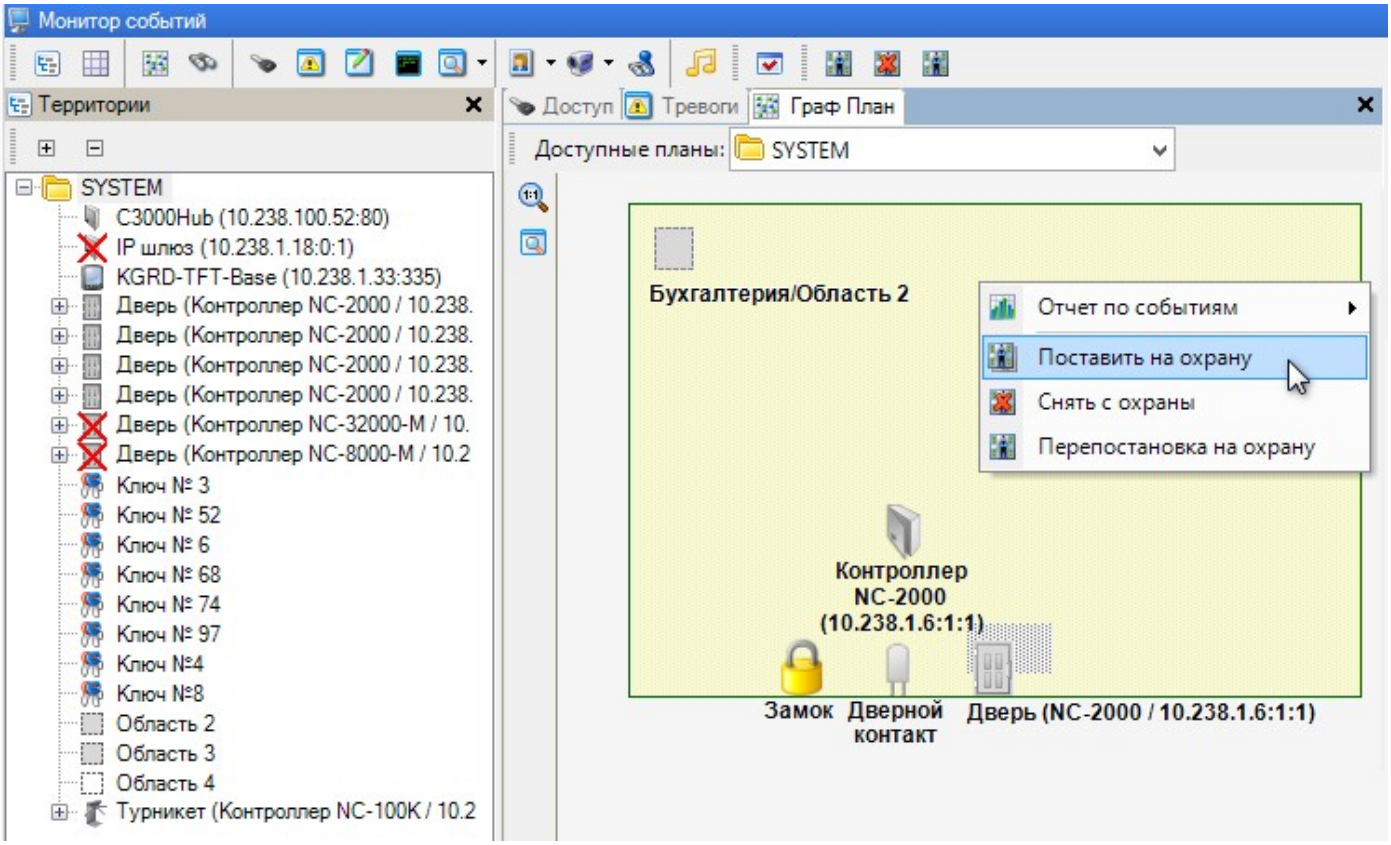
Охранная область, защищенная системой "Орион", может обслуживаться несколькими датчиками. Например, кабинет может быть защищен пожарным датчиком и датчиком движения. Постановка и снятие с охраны такой области производится из контекстного меню либо с панели инструментов монитора. Управление осуществляется сразу всеми датчиками выбранной области. Изменение состояния области, а также сообщения о событиях отображаются в окне событий (см. пример на рис. ниже).



Команда "Перепостановка на охрану" используется после приема тревоги для возврата зоны под охрану. Последовательное выполнение двух действий - "Снять с охраны" и "Поставить на охрану" - имеет тот же результат.

Компоненты C3000-Hub на графических планах

Если охраняемая область размещена на графическом плане в редакторе топологии (в нашем примере - Бухгалтерия/Область 2), то как и для компонентов СКУД ParsecNET 3, пользователь получает возможность наблюдения на графплане в мониторе событий статуса области и управления ею:

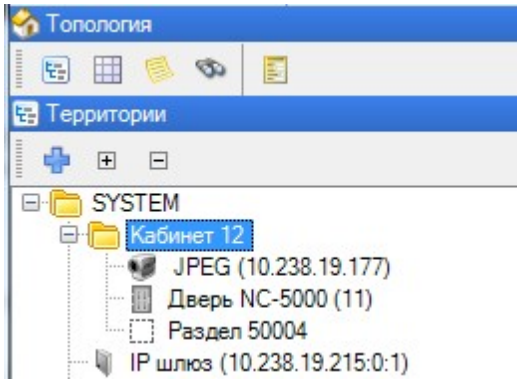


11.7.4.3 Взаимодействие систем

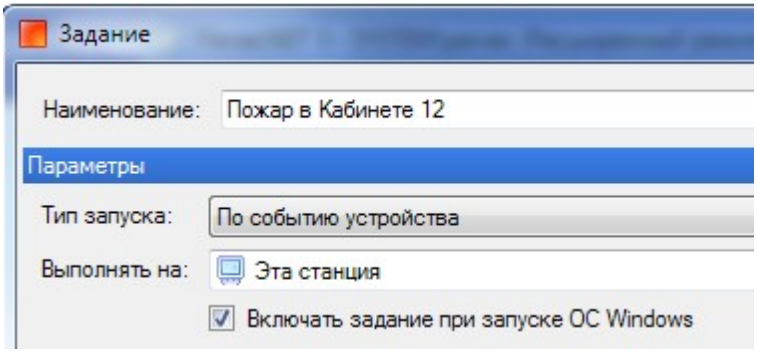
Взаимодействие систем

Помимо возможности наблюдать и управлять работой системы "Орион", интегрированной в ParsecNET 3, есть возможность организовать их взаимодействие при реагировании на происходящие события, для чего используется редактор заданий[321].

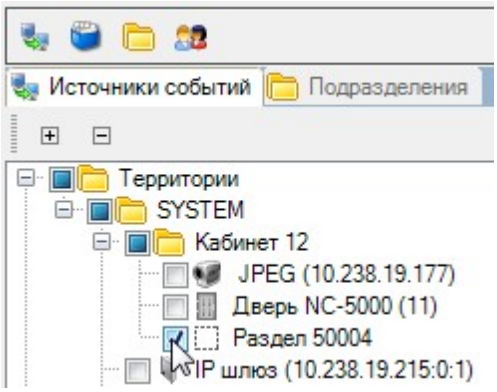
Для примера настроим систему так, чтобы по пожарной тревоге открывалась дверь помещения, в котором произошло возгорание, включалась тревога, а также запись происходящего на находящуюся в этом помещении видеокамеру. На рисунке ниже видно, что Кабинет 12 имеет раздел охраны (содержащий две зоны: датчика движения и датчика возгорания), дверь в помещение, а также видеокамера.



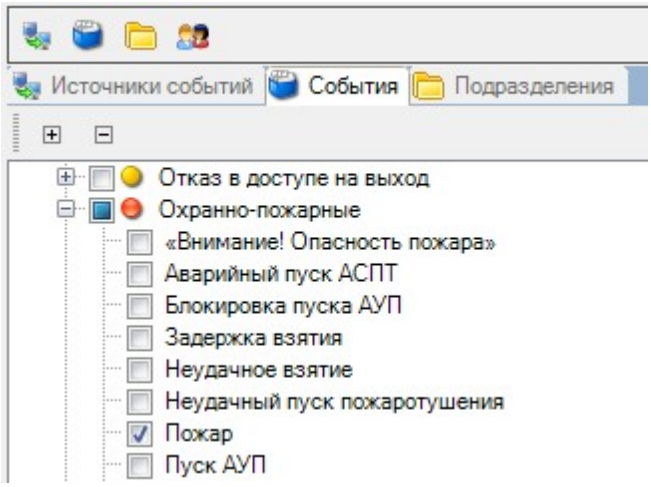
С помощью редактора заданий создайте задание, посредством которого осуществляется взаимодействие подсистем по сигналу пожарной тревоги:



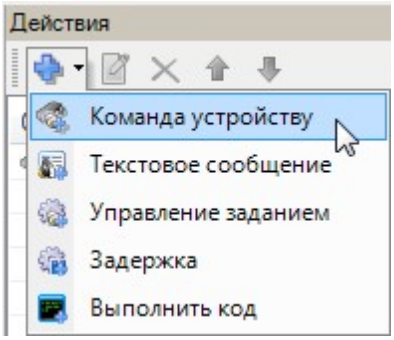
В качестве источника назначьте охранный раздел:



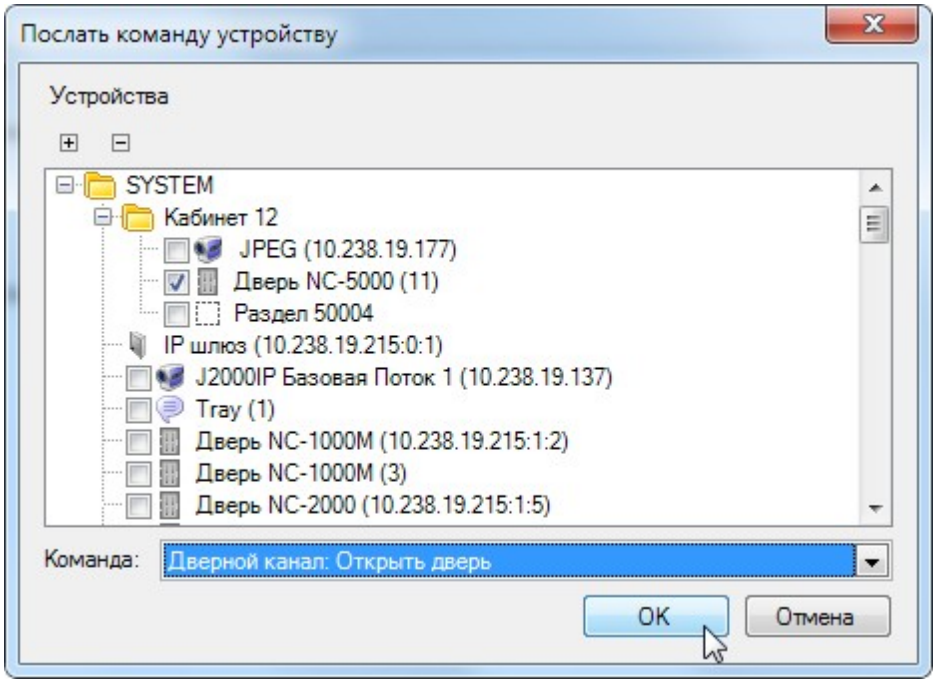
Событием, инициирующим выполнение задания, назначьте пожарную тревогу:



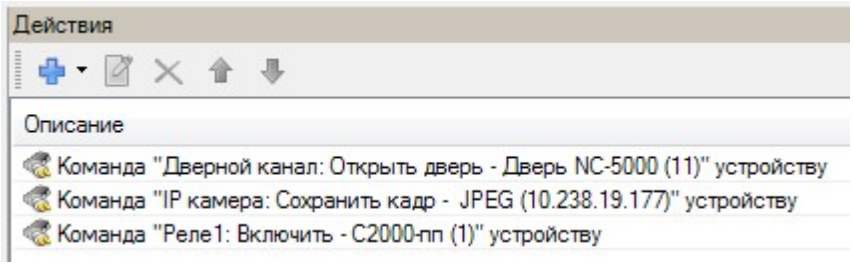
Теперь необходимо сформировать реакцию системы на выбранное событие. Для этого на панели действий редактора заданий выберите пункт "Добавить - Команда устройству":



В открывшемся диалоге выберите дверь и назначьте ей команду "Открыть дверь":



Аналогично создается команда камере сделать снимок события, а реле, к которому подключена сирена, - включить ее. В результате получается следующая последовательность действий по сигналу пожарной тревоги:



Таким способом можно организовать сколь угодно сложные взаимодействия любых компонентов любых подсистем, интегрированных в ParsecNET 3.

11.7.5 Система Firesec

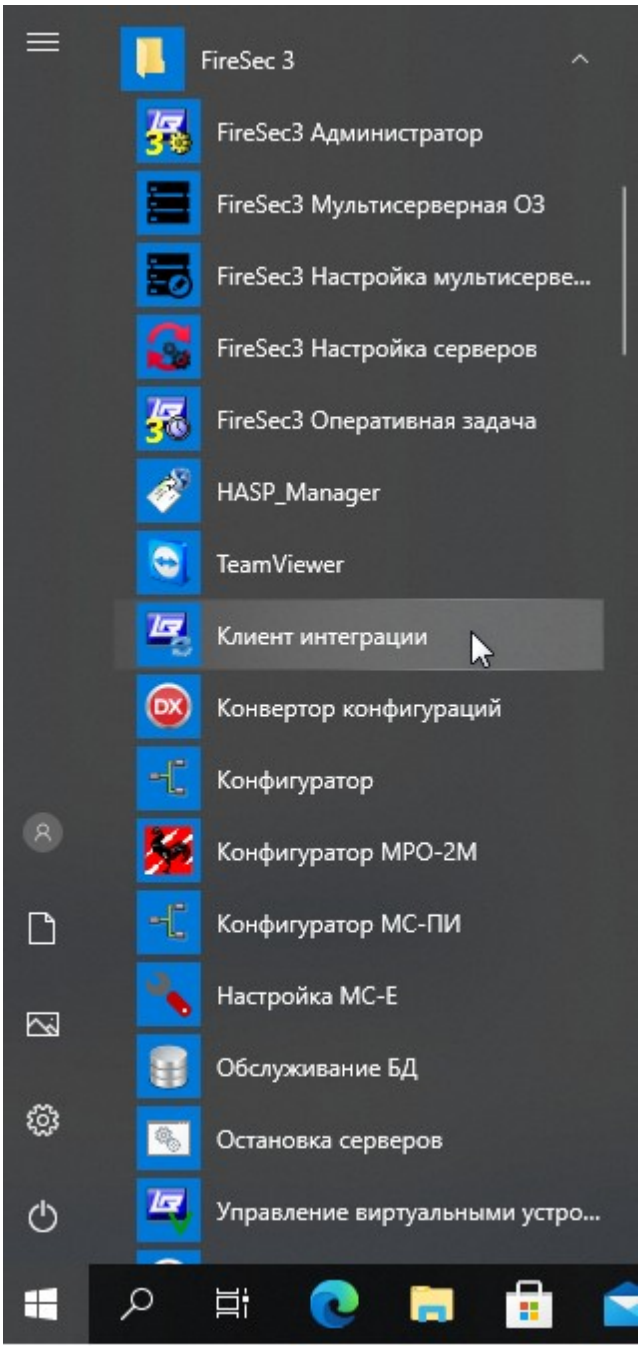
Данный раздел не является руководством по использованию ПО "FireSec", а предназначен только для описания принципов ее работы в составе СКУД ParsecNET 3. Для изучения ПО "FireSec" и ОПС "Рубеж" обратитесь к оригинальному руководству.

Модуль интеграции СКУД ParsecNET 3 и ПАК FireSec позволяет отслеживать состояние защищаемого средствами ОПС "Рубеж" объекта в реальном времени, ставить и снимать территории с охраны, а также создавать сложные алгоритмы действий, инициируемых событиями от охранных датчиков.

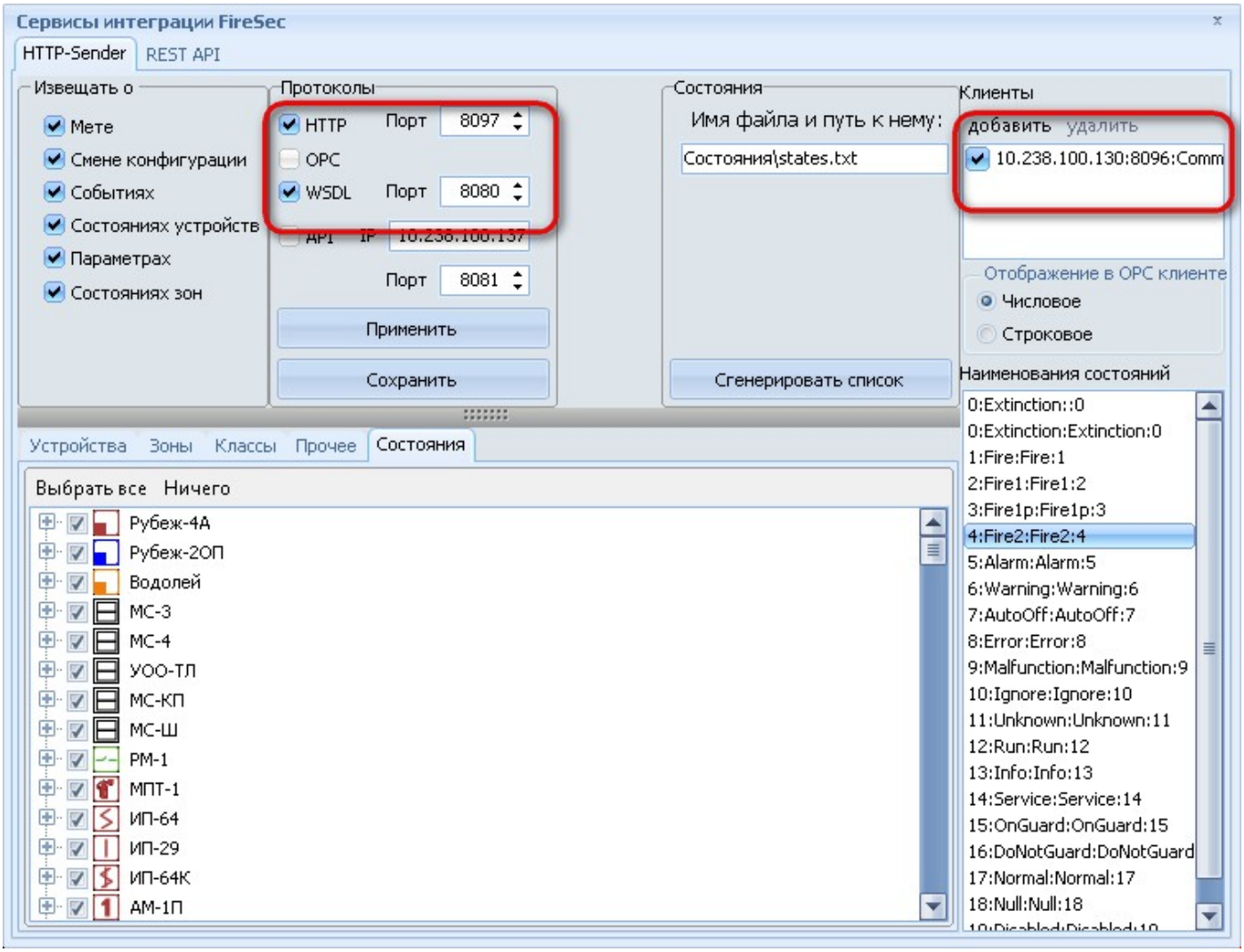
11.7.5.1 Подключение и настройка

Для настройки взаимодействия ПО ParsecNET 3 и ПО FireSec выполните следующие действия:

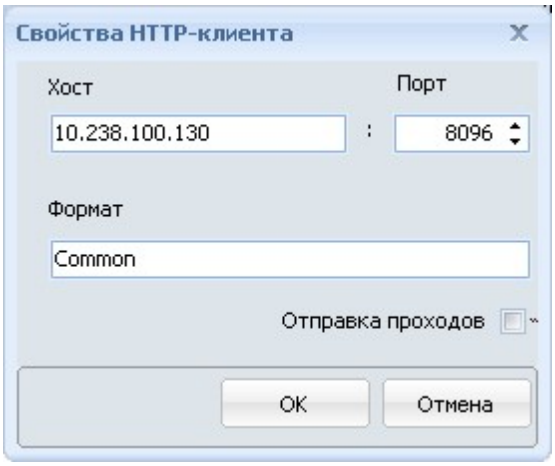
1. Установите и настройте ПО Firesec, следуя указаниям мастера настройки и Руководства по его эксплуатации;
2. Запустите клиент интеграции FireSec (Пуск - FireSec 3 - Клиент интеграции):



Откроется окно *Сервисы интеграции FireSec*:



3. В окне клиента интеграции в блоке *Протоколы* установите флажок *HTTP* и задайте порт 8097, и флажок *WSDL* и задайте порт 8080 (рисунок выше);
4. В блоке *Клиенты* нажмите на кнопку *Добавить*. Откроется окно настроек.
   Не рекомендуется добавлять больше одного сервера ParsecNET, так как это может привести к зависанию программы.



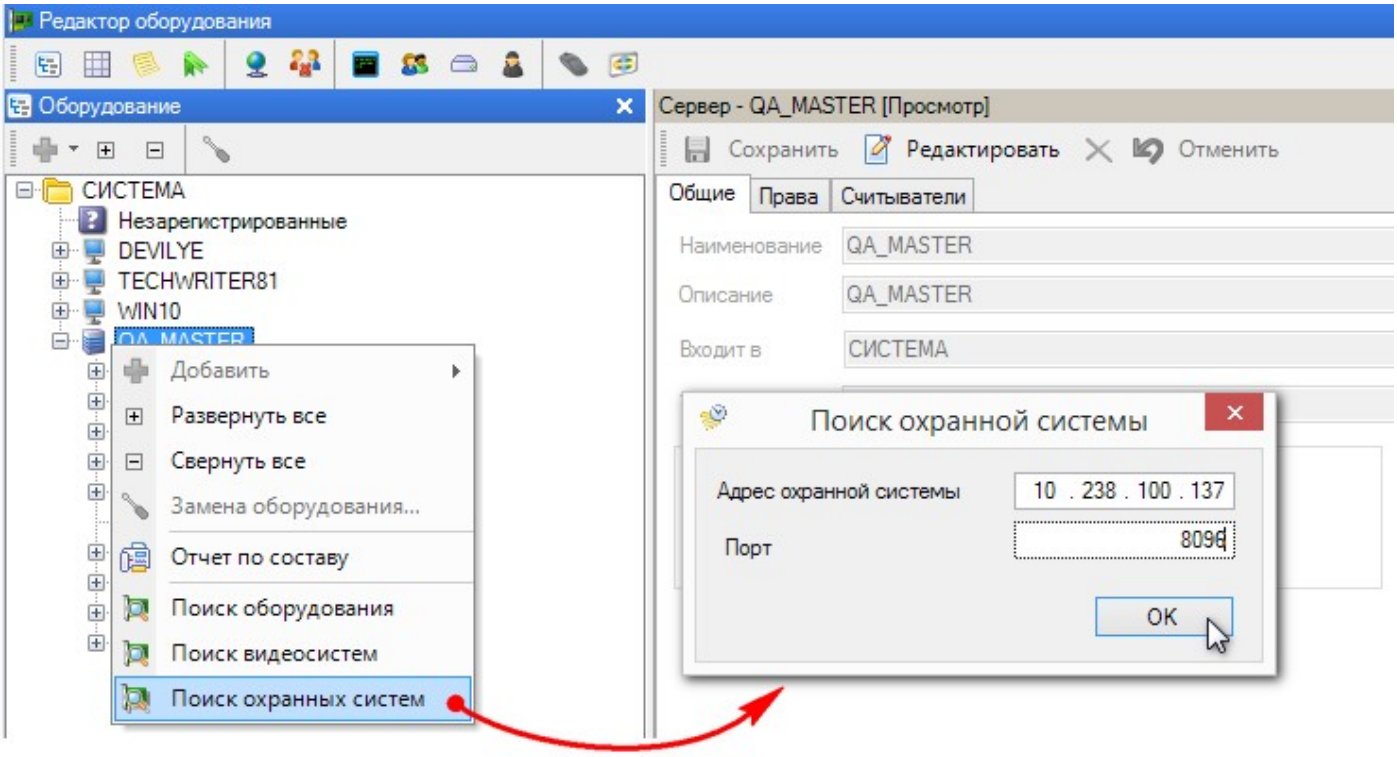
5. В открывшемся окне настроек введите:
   - в поле *Хост* введите IP-адрес ПК, на котором установлен сервер СКУД ParsecNET 3;
   - в поле *Порт* введите 8096 или 8097, (эти порты используются ParsecNET 3 для обмена данными с FireSec);
   - в поле *Формат* должно быть введено Common;

- флажок Отправка проходов ставится по необходимости.

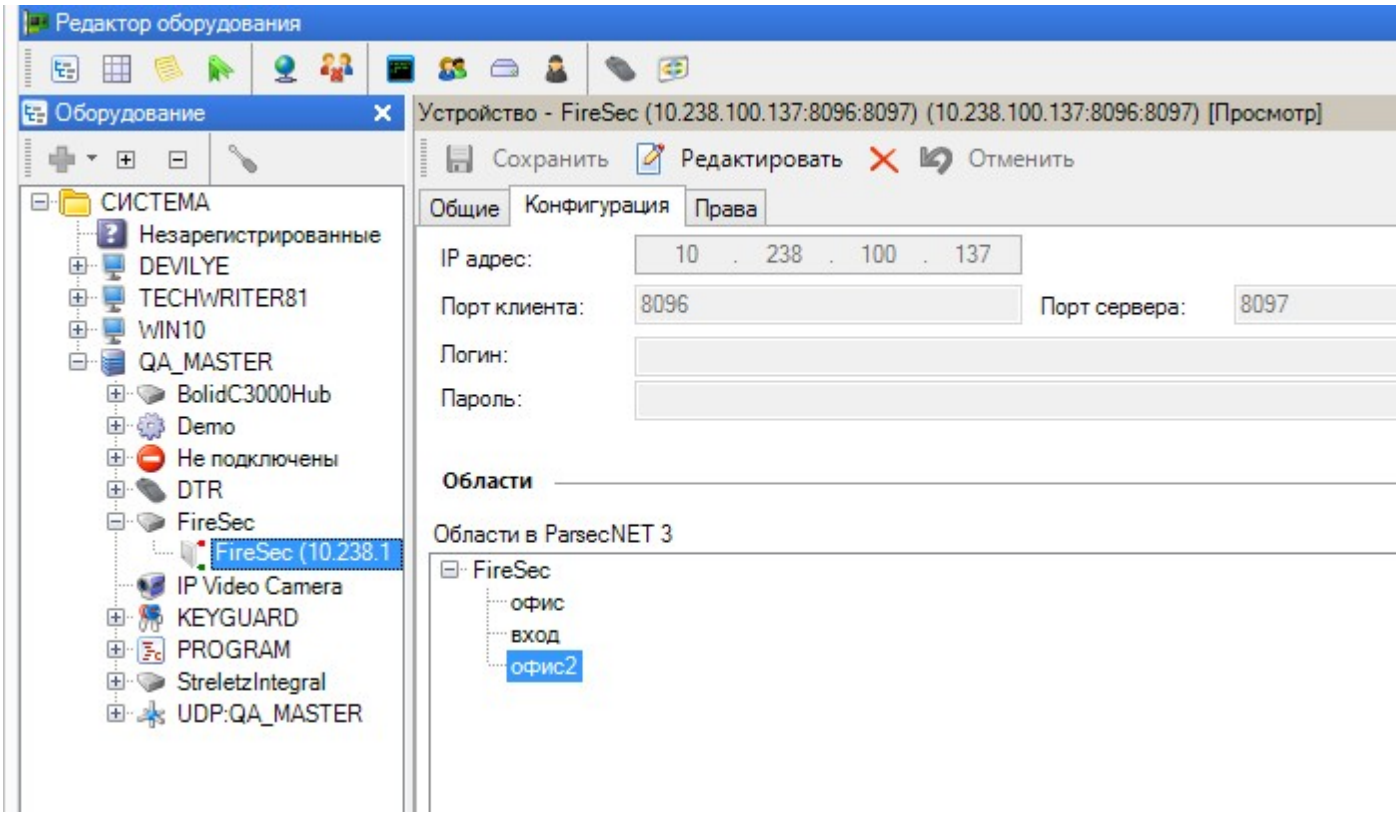
6. Нажмите на кнопку *ОК*. В списке клиентов появится запись нового клиента;
7. Установите флажок слева в строке нового клиента;
8. Сделайте остальные настройки, руководствуясь своими целями и указаниями в документации для ПО FireSec и ОПС Рубеж;
9. Закройте окно клиента интеграции FireSec.

Теперь можно перейти к настройкам ПО ParsecNET 3:

1. Запустите консоль администрирования и перейдите в редактор оборудования;
2. В контекстном меню сервера и рабочей станции откройте контекстное меню и выберите команду "Поиск охранных систем";
3. В открывшемся окне введите IP-адрес ПК, на котором установлено ПО FireSec и укажите порт 8097, после чего нажмите на кнопку *ОК*:



Система проведет поиск и в дереве оборудования появится новый канал FireSec:



В карточке канала отображаются:

- *IP адрес* - адрес ПК, на котором установлено ПО FireSec;
- *Порт клиента* - порт сервера ParsecNET 3;
- *Порт сервера* - порт сервера FireSec;
- *Лгин/пароль* - логин и пароль заданные в ПО FireSec при установке. По умолчанию логин - adm, пароль - пустое поле.

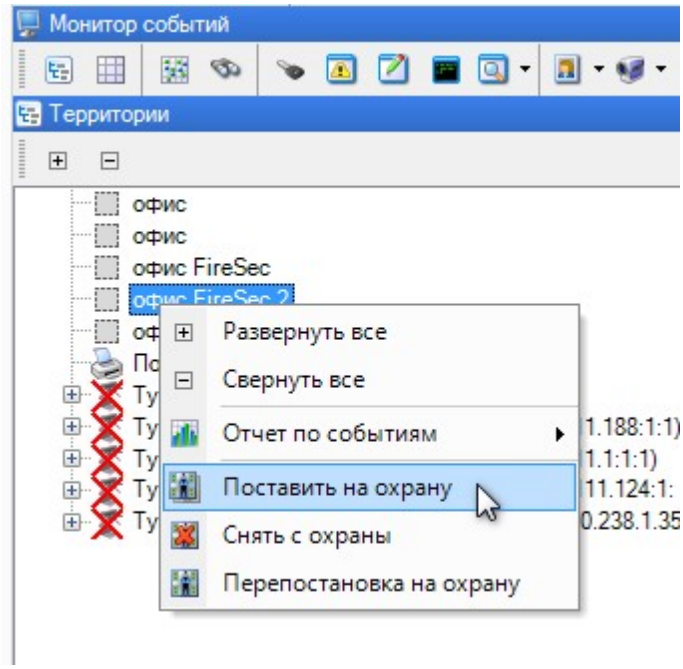
На панели области отображаются области, защищенные датчиками ОПС "Рубеж".

11.7.5.2 Использование системы

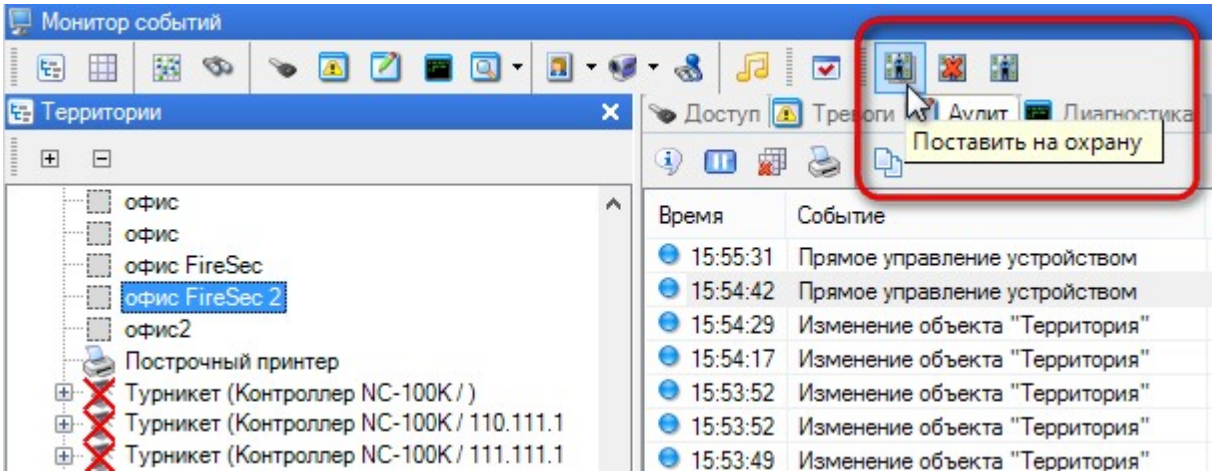
FireSec в мониторе событий

ПО FireSec позволяет в мониторе событий обеспечить наблюдение за состоянием компонентов (статус датчиков и областей), а также управлять областями (ставить на охрану или снимать с охраны).

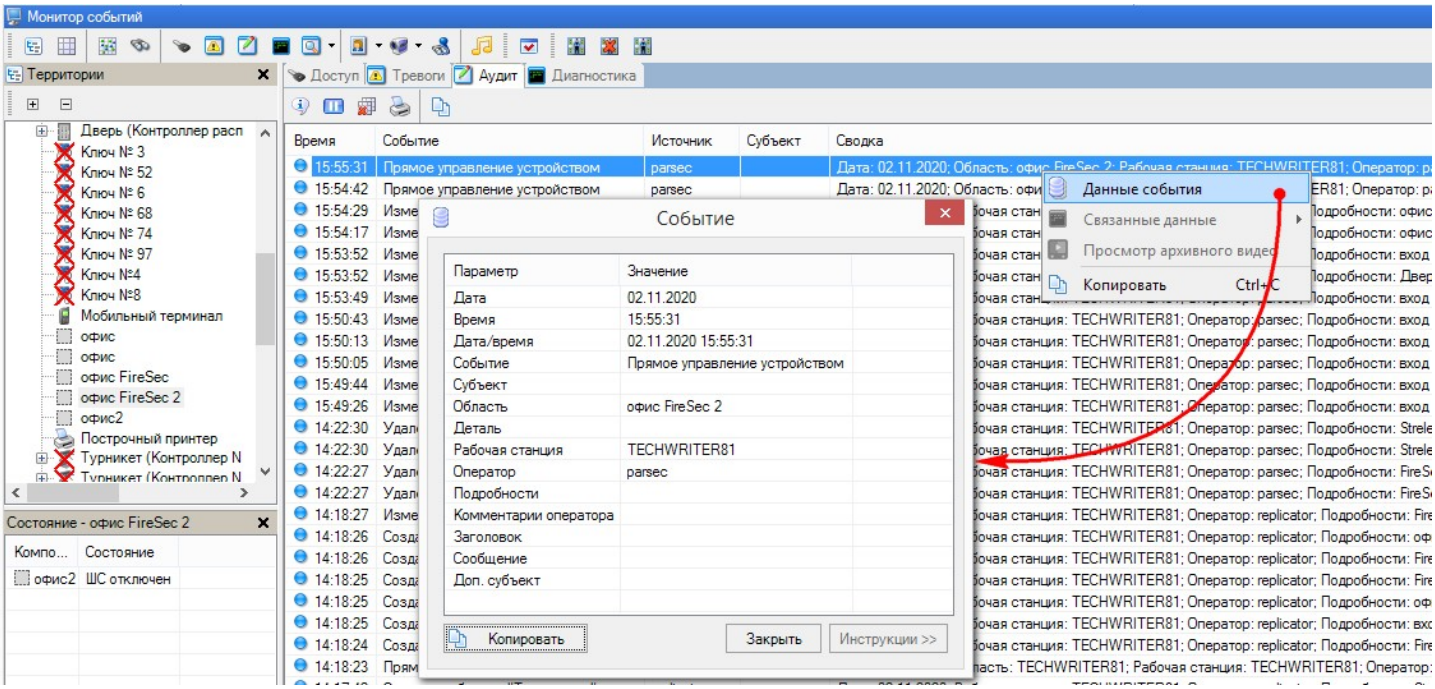
Ниже на рисунке показано контекстное меню постановки области на охрану в дереве территорий монитора событий:



Точно так же можно ставить на охрану и снимать с охраны выбранные в мониторе событий области с помощью интерактивной панели инструментов монитора событий:



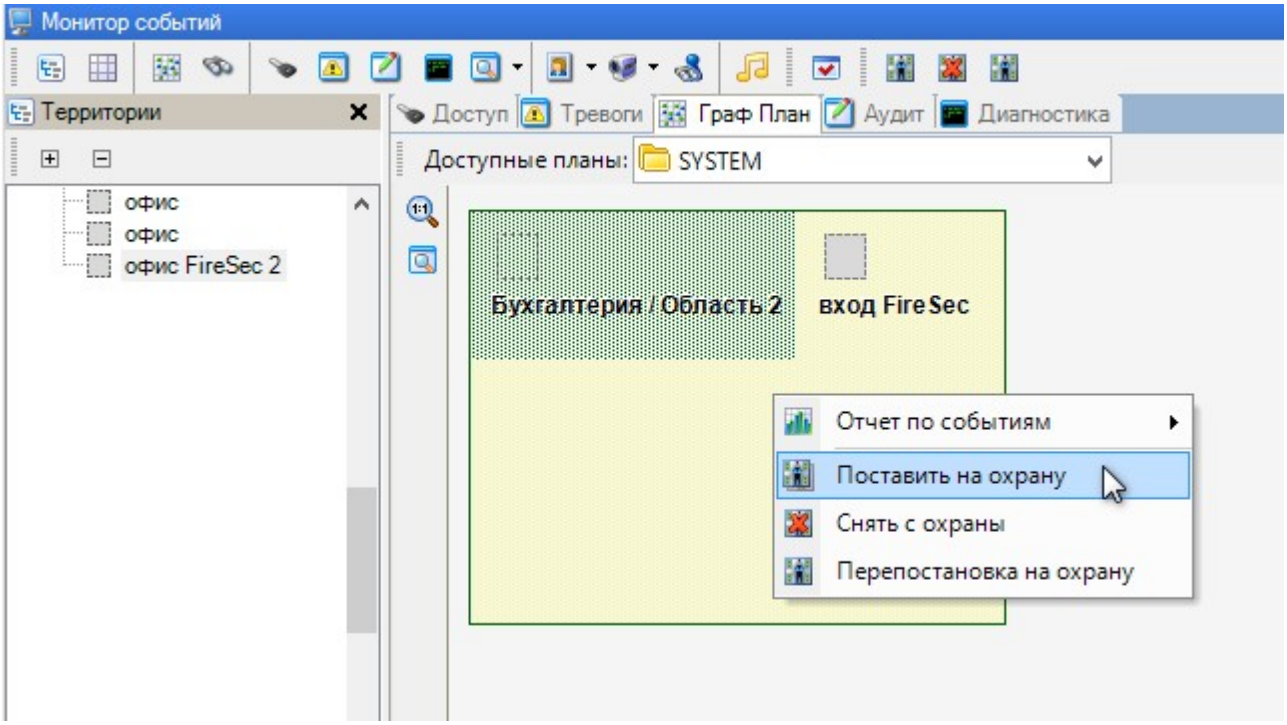
Система сформирует сообщения обо всех действиях, произведенных с областью. Из контекстного меню сообщения можно вызвать окно с подробностями действия:



На панели событий доступа и тревог также будут отображаться сообщения о событиях от всех имеющихся в рамках организации компонентов системы "Рубеж".

FireSec на графических планах

Если компоненты системы "Рубеж" помещены на графический план в редакторе топологии, то как и для других компонентов СКУД ParsecNET 3, пользователь получает возможность наблюдения на графплане Монитора событий статуса компонентов (областей, извещателей) и управления ими (постановка или снятие с охраны), как показано для примера на рисунке ниже:

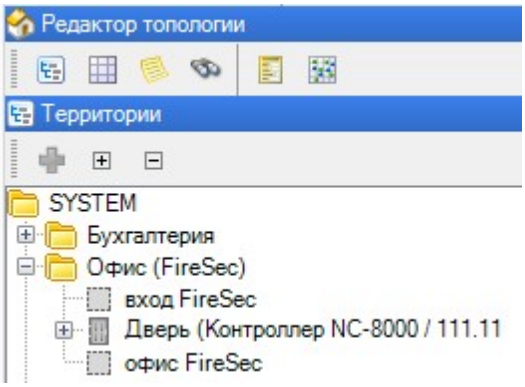


Совместная работа подсистем

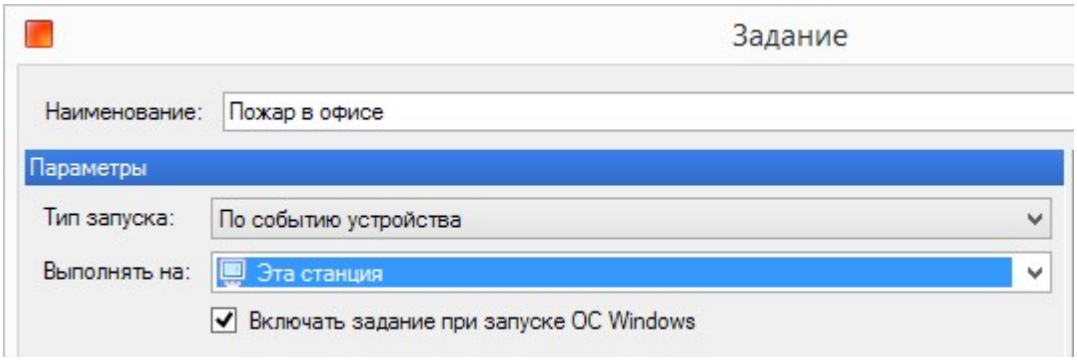
Помимо возможности наблюдать и управлять работой различных подсистем, интегрированных в ParsecNET 3, имеется возможность организовать их взаимодействие при реагировании на происходящие в системе события, для чего используется редактор заданий[321].

Чтобы проиллюстрировать это, создадим задание на открытие при пожарной тревоге двери помещения, в котором произошло возгорание. На рисунке ниже показана территория "Офис" с

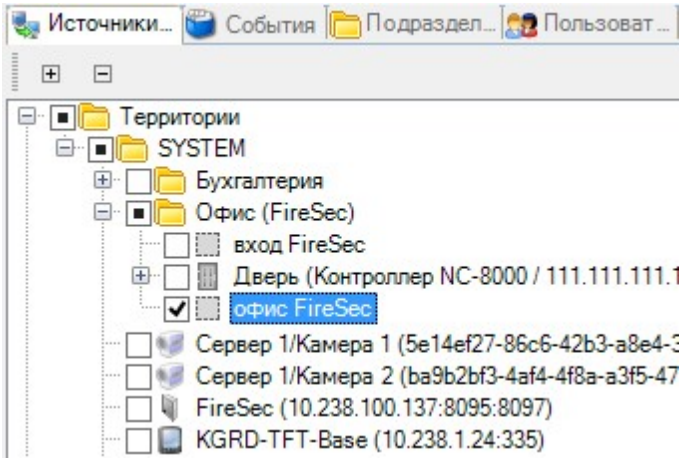
датчиком взлома (вход FireSec), пожарным датчиком (офис FireSec) и управляемой СКУД ParsecNET 3 дверью.



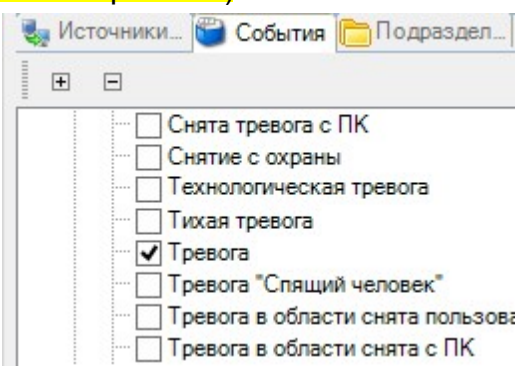
С помощью редактора заданий создайте задание для достижения взаимодействия систем по сигналу пожарной тревоги::



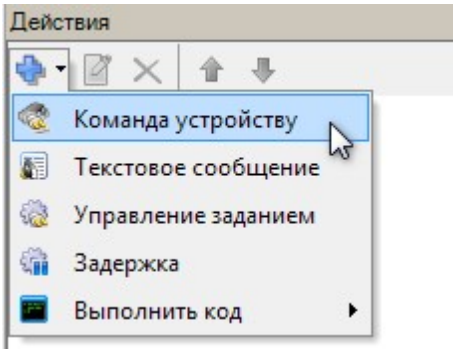
В качестве источника назначьте датчики возгорания и/или задымления:



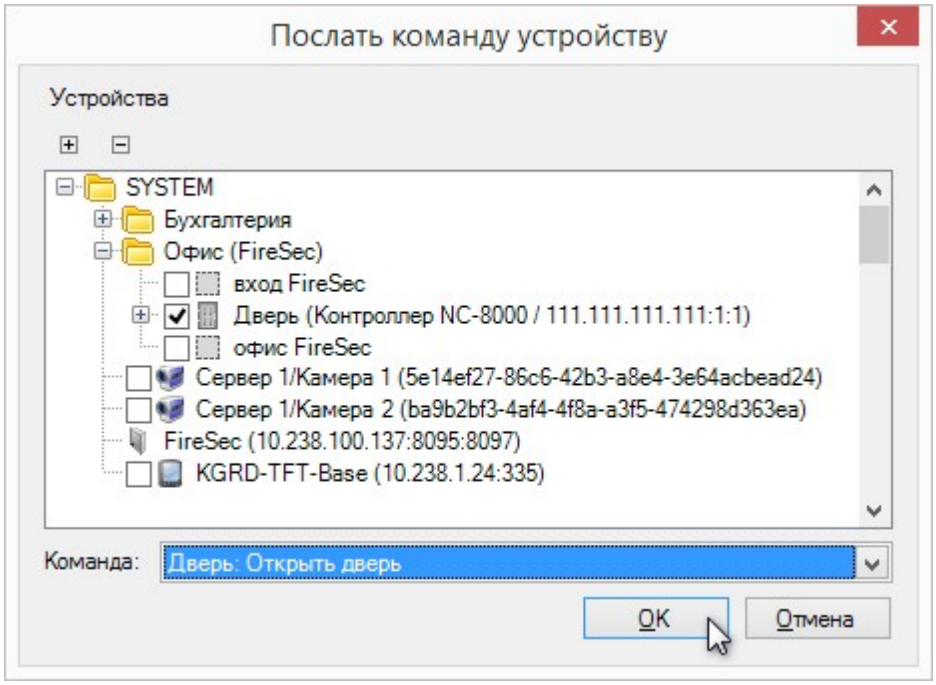
Событием, инициирующим выполнение задания, назначим тревогу (реакция всех датчиков: взлома, движения, возгорания, задымления и тому подобных интерпретируется СКУД ParsecNET 3 как "Тревога")



Теперь необходимо задать реакцию на выбранное событие. Для этого на панели действий редактора заданий выберите пункт "Добавить - Команда устройству":



В открывшемся диалоге выберите дверь и назначьте ей команду "Открыть дверь":



Таким образом можно организовать сколь угодно сложное взаимодействие любых компонентов любых систем, интегрированных в ParsecNET 3.

11.8 Интеграция с биометрическими устройствами ZKTeco и ЛКД

Использование отпечатков пальцев в СКУД обеспечивает повышенный уровень безопасности доступа.

Проведено тестирование следующих устройств ZKTeco и ЛКД:

- настольные биометрические сканеры отпечатков пальцев: ZK7500, ZK4500, ZK9500, ЛКД СО-04 00, ЛКД СО-04 01, ЛКД СО-04-02;
- настенные биометрические терминалы доступа: TF1600, TF1700 и ЛКД КО-15 00.

Из настенных терминалов поддерживаются только устройства, работающие с интеграционным пакетом Pull SDK: TF1600, TF1700 и ЛКД КО15 00 с прошивкой VER. 6.64.0012.

Для надежной работы устройств ZKTeco настойчиво рекомендуется использовать надежные каналы связи (например, не следует задействовать мобильный интернет).

Не поддерживается интеграция с устройствами ZKTeco серии SF и SC.

Не поддерживаются устройства, требующие интеграционного пакета Standalone SDK, по причине их нестабильной работы.

Если установить программу ZKAccess, поставляемую с устройствами ZKTeco, на сервер ParsecNET 3, то версия SDK будет изменена и интеграция в Parsec работать не будет. При необходимости использовать ПО ZKAccess устанавливайте его на отдельной машине!

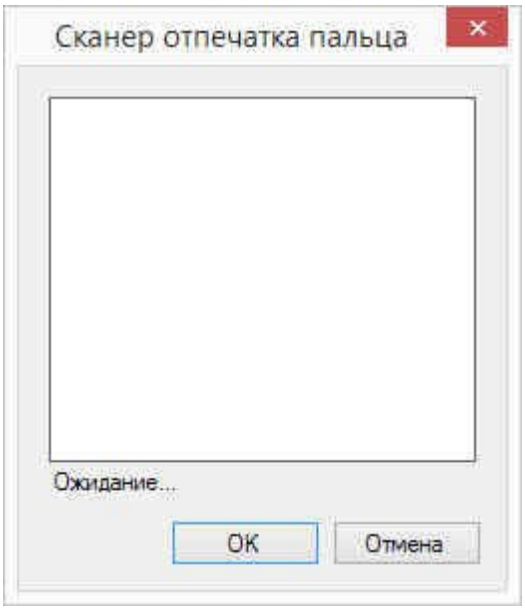
11.8.1 Настольный биометрический считыватель отпечатков

Подключение настольного биометрического считывателя

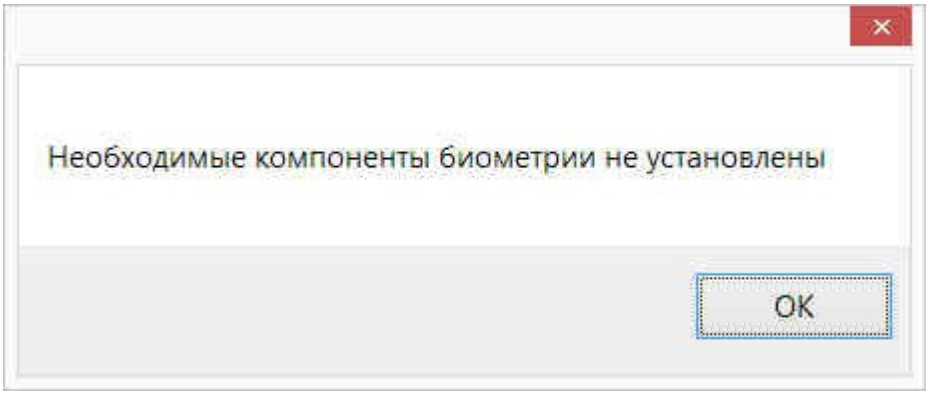
Вставьте настольный биометрический считыватель в USB-порт компьютера. Система начнет установку драйверов, дождитесь завершения процедуры.

После установки драйверов, можно приступать к использованию считывателя. Однако рекомендуется сначала проверить качество установки драйверов. Для этого можно воспользоваться двумя способами:

- перейти в диспетчер устройств и проверить, что драйвер установлен правильно:
  - правильно - драйвер "ZKTxxx Fingerprint Reader" находится в разделе "Контроллеры USB";
  - неправильно - драйвер помечен пиктограммой с восклицательным знаком.
- перейти в редактор персонала и в карточке субъекта доступа (в режиме редактирования) нажать на кнопку *Биометрические данные...*. Если появится окно сканера отпечатков пальцев, значит, драйвер установлен правильно:



Если драйвер установлен неправильно, появится сообщение об ошибке:



Если драйвер установлен неправильно или не установлен вовсе, запустите файл драйвера ZKFinger_3.0.1. из папки COMMON установочного дистрибутива системы ParsecNET 3.

После этого с настольным биометрическим считывателем можно работать, как описано в разделе[660].



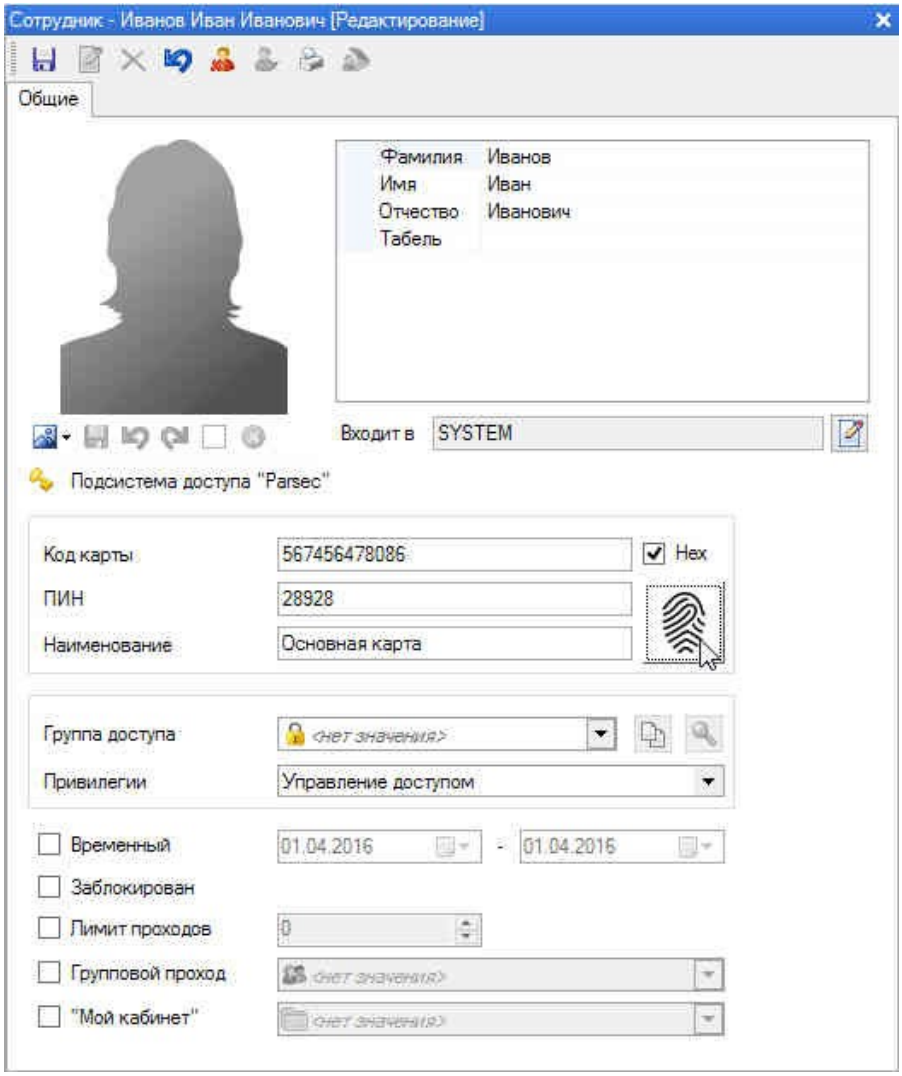
К одному ПК должен быть подключен только один настольный биометрический считыватель.

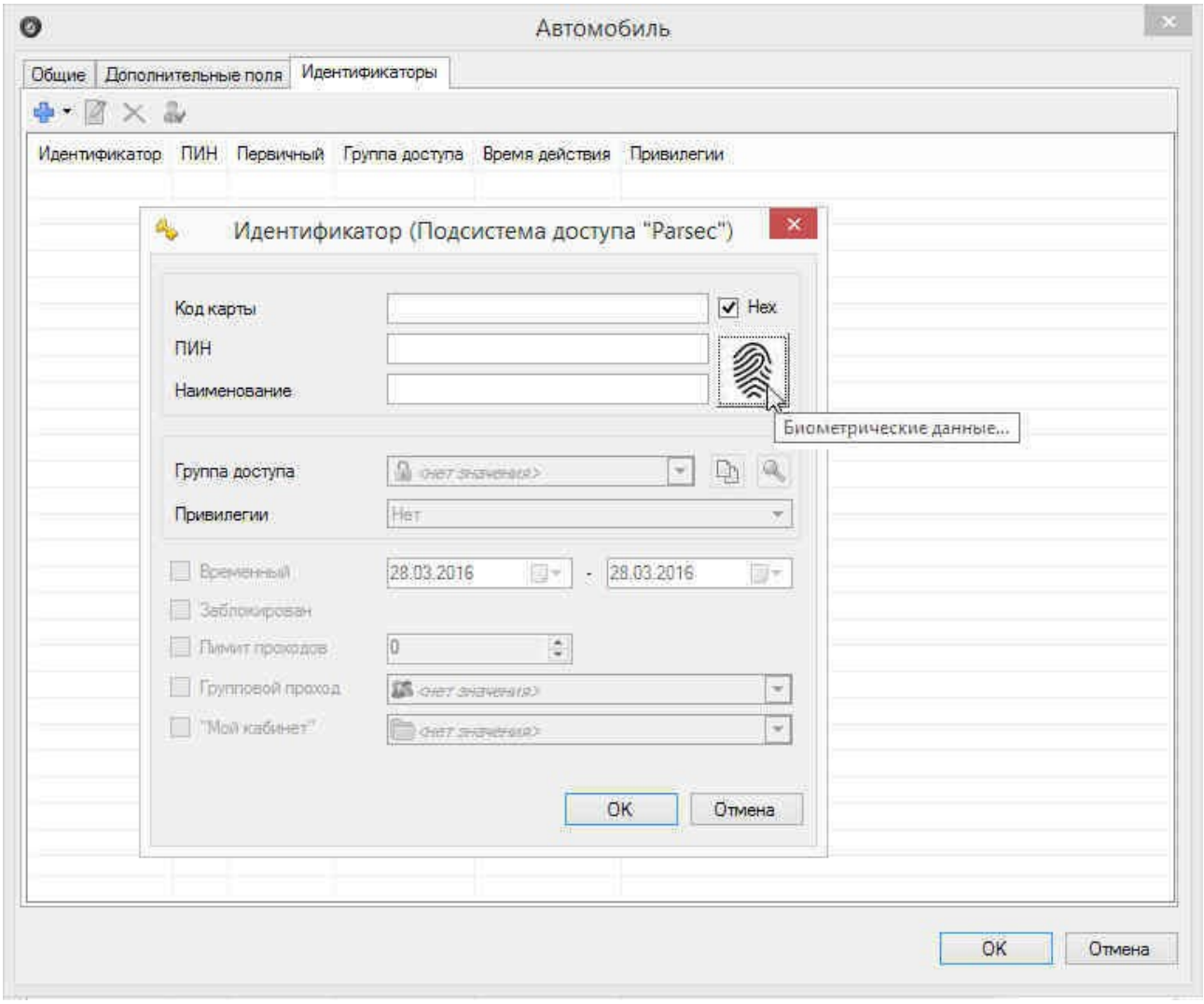
Использование настольного биометрического считывателя

После установки драйверов, можно приступать к использованию считывателя.

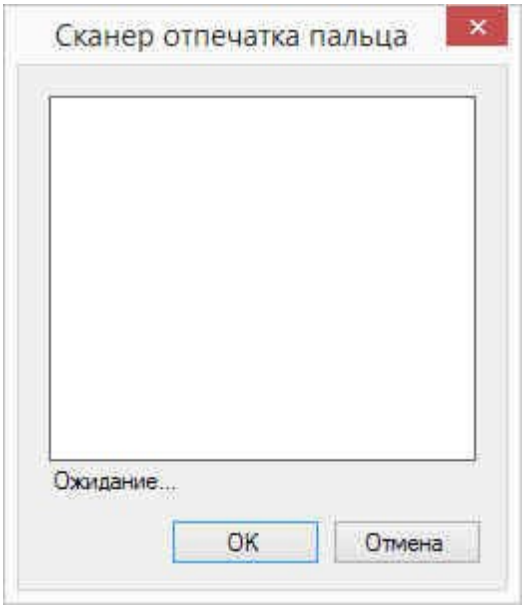
Перейдите в редактор персонала. Ввод биометрических данных возможен как при добавлении нового субъекта доступа, так и в режиме редактирования карточки уже существующего субъекта.

- Для добавления биометрических данных, нажмите на кнопку *Биометрические данные...* (аналогичные карточка сотрудника и посетителя, отличаются от карточки автомобиля):

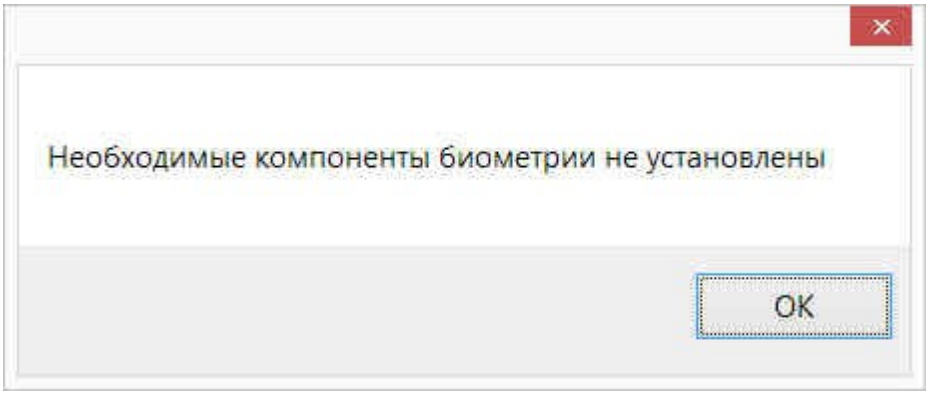

Сотрудник - Иванов Иван Иванович [Редактирование]
Общие
Фамилия Иванов
Имя Иван
Отчество Иванович
Табель
Входит в SYSTEM
Подсистема доступа "Parsec"
Код карты 567456478086
Hex
ПИН 28928
Наименование Основная карта
Группа доступа <нет значения>
Привилегии Управление доступом
Временный 01.04.2016 - 01.04.2016
Заблокирован
Лимит проходов 0
Групповой проход <нет значения>
"Мой кабинет" <нет значения>



Появится окно сканера отпечатков пальцев:



Если драйвер установлен неправильно, появится сообщение об ошибке (см. рис. ниже). В этом случае установите драйвер как описано в разделе[655].



Производитель рекомендует для идентификации использовать указательный, средний или безымянный палец.

Попросите сотрудника аккуратно и не сильно приложить подушечку пальца параллельно поверхности сканера по его центру. Сила нажатия роли не играет, на качество сканирования влияет аккуратность и точность размещения пальца.

После того, как в окне сканера появится отпечаток, нажмите на кнопку:

- *OK* - если качество сканирования Вас у страивает. Отпечаток будет помещен в базу данных СКУД ParsecNET 3 в виде математической модели. Код этой модели будет отображаться в поле *Код карты*;

С настенным биометрическим терминалом F11 в паре не удастся использовать карты с кодом больше 65535 (0000FFFF), т.к. терминал этой марки не сможет его обработать. Также это приводит к необходимости вручную исправлять код модели отпечатка пальца (в поле "Код карты"), если он больше указанного.

- *Отмена* - если качество сканирования менее 70%. После этого повторите процедуру сканирования.

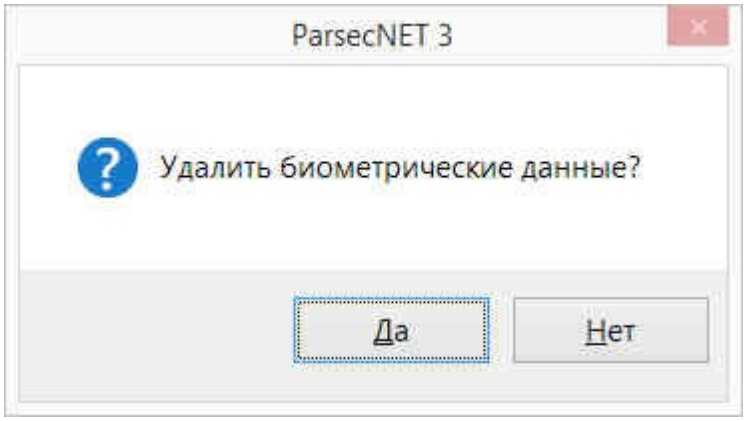
После сохранения отпечатка в БД значок на кнопке *Биометрические данные* примет следующий вид:



Если для субъекта доступа необходимо сохранить более одного отпечатка, это можно сделать, назначив ему дополнительный идентификатор[268] типа "Подсистема доступа Parsec".

После сохранения отпечатка субъекта доступа в БД СКУД, его можно использовать для идентификации этого субъекта при помощи биометрических терминалов ZKTeco или ЛКД.

Для удаления хранящихся в БД биометрических данных нажмите на кнопку  и подтвердите удаление в появившемся сообщении:



11.8.2 Настенный биометрический терминал

Подключение и настройка настенного биометрического терминала

В СКУД ParsecNET 3 биометрические терминалы доступа ZKTeco или ЛКД используются только в качестве считывателей, подключенных к контроллерам Parsec серии NC.

Установите терминал в соответствии с указаниями в его руководстве по эксплуатации.

Подключите терминал к сети Ethernet, по-умолчанию IP-адрес терминалов - 192.168.1.201. Изменение адреса осуществляется при помощи ПО терминалов.

Биометрический терминал подключается к контролерам Parsec при помощи интерфейса NI-TW.

Подключите переходник из комплекта терминала к разъему WG-OUT/WG-IN. Затем подсоедините провода переходника к плате интерфейса NI-TW в соответствии с таблицей (для внешнего считывателя):

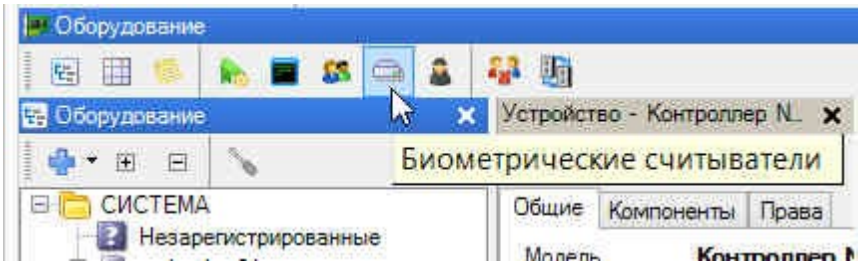
Маркировка на переходнике	Клеммная колодка READER 0 OUTDOOR на NI-TW
WD1-OUT	W1/T
WD0-OUT	W0/T
GND	GND

Если биометрический терминал будет использоваться в качестве внутреннего считывателя, провода WD1-OUT, WD0-OUT и GND переходника следует подключить к клеммной колодке READER 1 INDOOR интерфейса NI-TW.

Теперь необходимо настроить ПО ParsecNET 3, для этого запустите консоль "Администрирование" и перейдите в редактор "Оборудование".

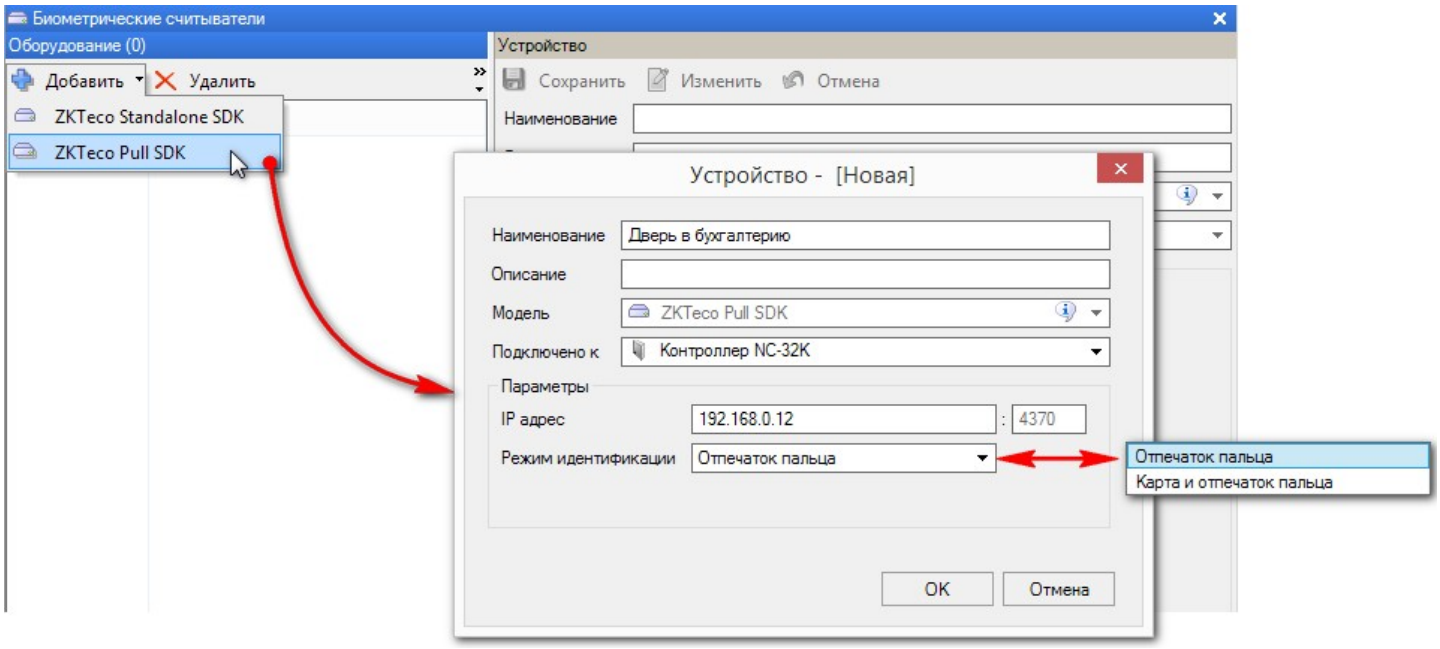
Добавление биометрического терминала производится только вручную:

- Нажмите на кнопку *Биометрические считыватели* на панели инструментов редактора:



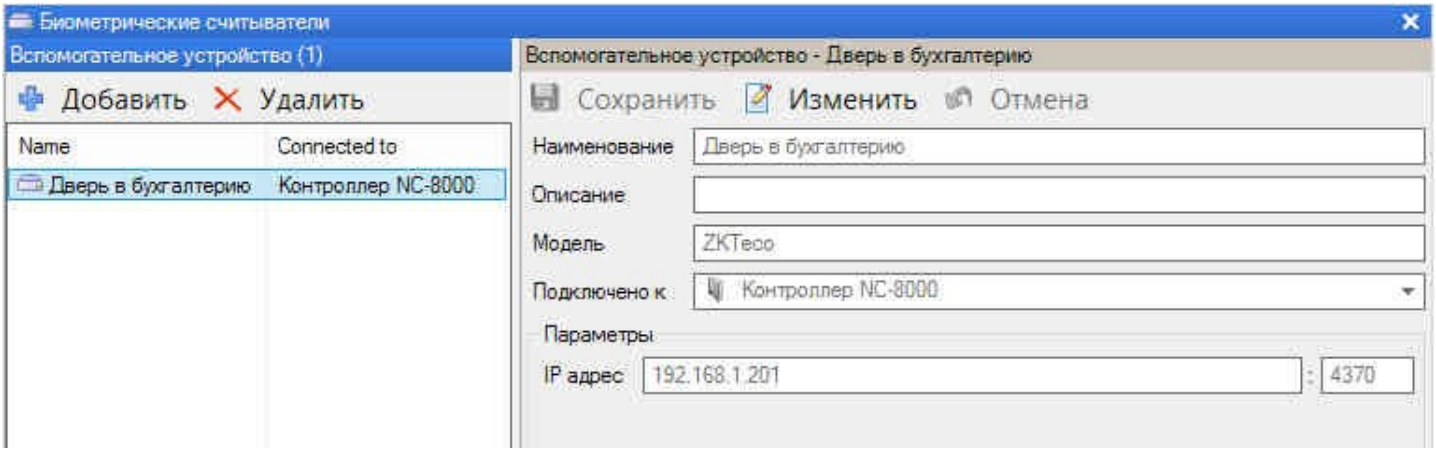
Откроется панель *Биометрические считыватели*;

- Нажмите на кнопку (*Добавить)* и в раскрывающемся списке выберите ZKTeco Pull SDK;
- Введите необходимые данные:



- нажмите на кнопку *OK*.

Биометрический считыватель будет добавлен в систему:



Теперь этот терминал может использоваться для прохода по отпечатку пальца.

Кнопка "*Монитор активности*" позволяет отслеживать прогресс загрузки отпечатков пальцев в устройства.

11.9 Интеграция с терминалами распознавания лиц

Лицо человека может быть использовано в качестве его "биометрического идентификатора". СКУД ParsecNET 3 обладает возможностью использовать следующие терминалы биометрической идентификации:

- терминалы биометрической идентификации Uface компании UniUbi[666];
- терминалы MinMoe с функцией распознавания лиц компании Hikvision[663] .

В зависимости от использующейся модели и имеющихся на борту терминала опций (считыватель бесконтактных карт, модуль измерения температуры) терминал может быть настроен в режиме двухфакторной идентификации и бесконтактной термометрии. Кроме этого терминалы могут определять наличие медицинской маски на лице пользователя.

Принцип работы модулей интеграции с терминалами биометрической идентификации Uni Ubi и Hikvision общий и аналогичен работе модуля интеграции со сканерами отпечатков пальцев ZKTeco:

- Терминалы используются в системе ParsecNET 3 только как считыватели (хотя и обладают функциями контроля доступа и имеет встроенное реле для управления замком/турникетом). Терминал идентифицирует пользователя автономно с помощью встроенного программного обеспечения;
- Терминалы подключаются к контроллеру СКУД ParsecNET 3 по протоколу Wiegand и передают уникальный код пользователя в случае успешного распознавания. Далее решение о доступе принимает контроллер СКУД ParsecNET, основываясь на данных своей БД;
- Если терминал человека не распознал, то в контроллер ничего не передается;
- Терминалы обладают собственной базой данных лиц пользователей, эта база наполняется и поддерживается в актуальном состоянии с помощью модуля интеграции в ПО ParsecNET через локальную сеть (по проводу или по WiFi, в зависимости от подключения и модели терминала);
- Соединение по сети Ethernet с сервером СКУД ParsecNET 3 (модуль интеграции работает именно на сервере) предназначено для загрузки пользователей и последующего автоматического обновления БД пользователей в терминале, а также для получения данных термометрии (какова измереннаятемпература) и получения в ПО ParsecNET событий отказа в доступе с указанием причин (неизвестный, детектор маски, превышение температуры).

Таким образом, ПО ParsecNET 3 выступает источником данных для терминала. При добавлении новой записи в БД персонала она также автоматически добавляется и во все подключенные терминалы. При изменении или удалении данных соответствующие запросы также отправляются в обслуживаемые модулями интеграции терминалы.

Кроме автоматического обновления, существует и процедура ручной загрузки БД пользователей в терминал «по нажатию кнопки», при этом сначала БД терминала очищается, а потом наполняется данными из БД Parsec.

Для нормальной работы терминалов с функцией распознавания лиц в записи пользователя должна присутствовать фотография и пользователю должен быть назначен основной идентификатор.



Группа доступа основного идентификатора в текущей версии ПО не влияет на то, будет он загружен в терминал или нет – все пользователи грузятся во все терминалы.

На текущий момент доступны следующие режимы идентификации:

- по лицу,
- по карте,
- по карте или лицу,
- по карте + лицу.

Режим выбирается для каждого терминала отдельно в карточке биометрического устройства в ПО ParsecNET 3, при этом настройка действует на всех пользователей, которые загружены в БД терминала.

Для терминалов Uni Ubi следует выбирать режим выдачи кода в формате Wiegand 34, поскольку работа с форматом Wiegand 26 приводит к ошибкам на тестировавшихся терминалах[666] .

Несмотря на то, что терминалы Hikvision корректно работают по Wiegand 26, их также рекомендуется подключать по интерфейсу Wiegand 34, что позволяет избежать проблем с кодами, в которых старший (четвертый) байт не нулевой.

Терминалы подключается к контроллеру через модуль сопряжения NI-TW (либо OMP-W02 для NC-60K/NC-60K.M).

Модуль сопряжения NI-TW необходимо использовать новой версии (серийный номер 086-00-xxxxx и выше), так как на предшествующих версиях режим Wiegand 34 не поддерживается. Перемычка на плате при этом должна быть выставлена в положение W26 – это режим автоопределения W26/W34, т.е. разбирая посылку, плата автоматически определит какой длины код ей передало устройство.

Преобразователь интерфейсов OMP-W02, применяемый для подключения считывателей Wiegand к шине OSDP, тип формата кода тоже определяет автоматически.

См. также как Настроить двухфакторную идентификацию[732]

11.9.1 Интеграция с биометрическими устройствами Hikvision

Лицензируется как PNSoft-FR[344] или PNSoft-FR1CH[344]

Терминалы биометрической идентификации серии MinMoe компании Hikvision используются для распознавания пользователей СКУД ParsecNET 3 по карте и/или по лицу, с опциональным бесконтактным термоконтролем пользователей. Также терминал может отслеживать наличие маски на пользователе.

Для работы с картами могут использоваться только карты семейства Mifare.

Модуль интеграции был протестирован и показал корректную работу со следующими моделями терминалов:

Модель	Прошивка
DS-K1T341AMF	3.2.30 (билд 20210406)
DS-K1T680D-E1	3.2.33 (билд 20210406)
DS-K1T671MF	3.2.30 (билд 20210609)
DS-K1T671TM-3XF	3.2.32 (билд 20210610)
DS-K5671-1-3XF/ZU	2.2.6 (билд 20200927) 3.2.2 (билд 20210207)

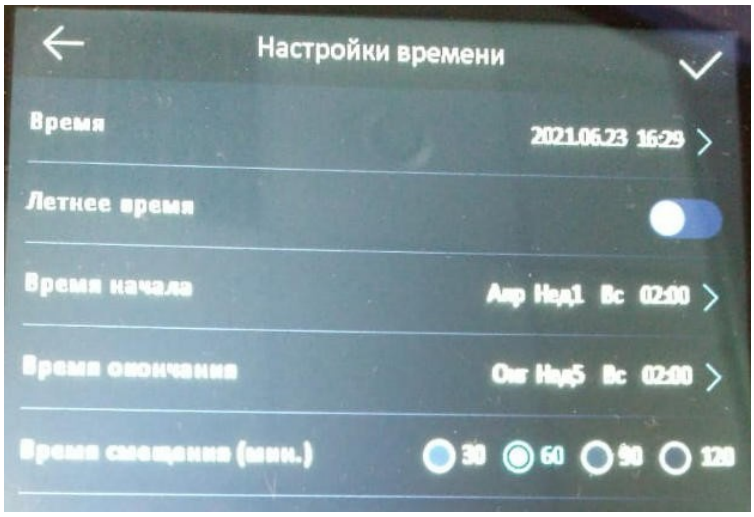


В БД терминала биометрической идентификации загружаются данные пользователей, чьи группы доступа содержат контроллер, к которому подключен этот терминал. Поэтому при выборе модели терминалов необходимо тщательно следить, чтобы объем их памяти позволял сохранить эти данные.

Для корректного распознавания лиц загруженные в БД терминалов биометрической идентификации фотографии субъектов доступа должны иметь разрешение не менее 640x480 пикселей.

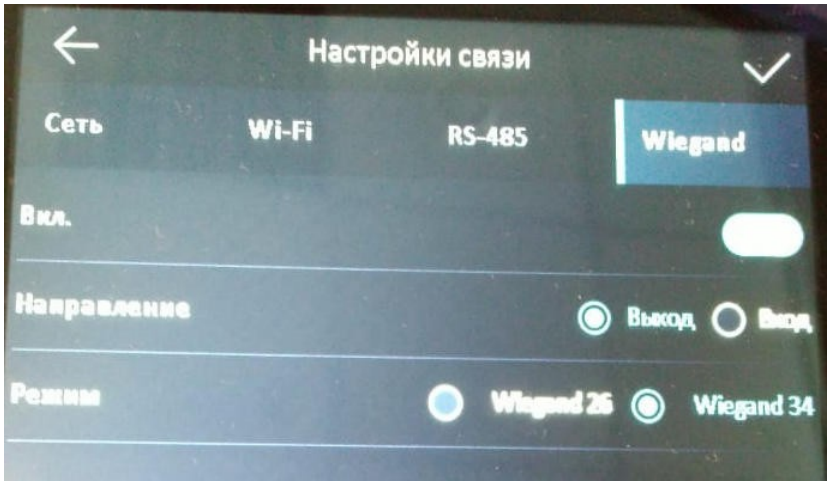
Настройка терминала биометрической идентификации состоит из следующих шагов:

1. Смонтируйте терминал в выбранном месте, активируйте и задайте свои логин и пароль, руководствуясь документацией по эксплуатации терминала;
2. Подключите терминал к контроллеру доступа и к сети Ethernet, в которой находится сервер СКУД ParsecNET 3. Терминал подключается к контроллеру доступа посредством модуля сопряжения NI-TW с серийными номерами 086-00-xxxx и выше. Код идентификатора субъекта доступа передается в формате Wiegand 34. Для этого перемычка на плате преобразователя должны быть выставлена в положение W26 (подробнее в Руководстве по эксплуатации NI-TW); Соединение по сети Ethernet с сервером СКУД ParsecNET 3 предназначено для загрузки пользователей и последующего автоматического обновления БД пользователей в терминале, а также для получения данных термометрии и получения в ПО ParsecNET 3 событий отказа в доступе с указанием причин;
3. Для доступа к настройке параметров терминала нажмите на экран терминала в любом месте и удержите нажатие 1-2 секунды. Откроется окно ввода пароля;
4. Введите пароль и нажмите на кнопку *OK*. Откроется экран *Меню*;
5. На экране *Меню* нажмите на значок *Время* и в верхней строке открывшегося окна задайте текущее время (рисунки показаны на примере терминала MinMoe модели DS-K5671-3XF/ZU):



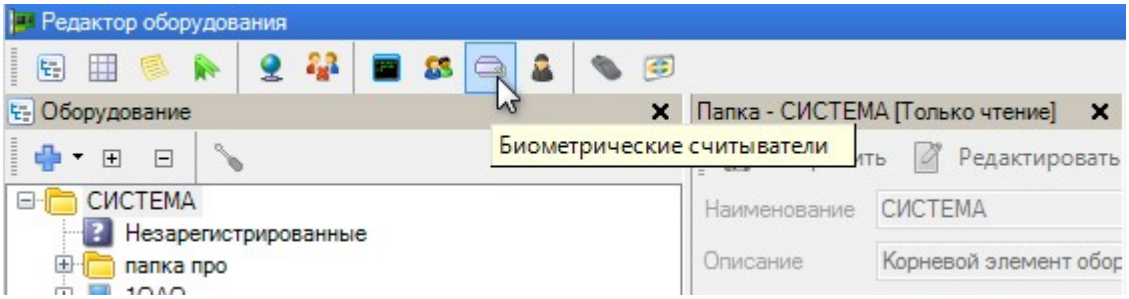
Сохраните изменения, нажав на "галочку" справа вверху экрана. Терминал вернется на экран *Меню.*

6. Нажмите на значок *Связь*;
7. В открывшемся окне на вкладке *Сеть* задайте IP-адрес;
8. Перейдите на вкладку Wiegand и установите переключатель в положение Wiegand 34:

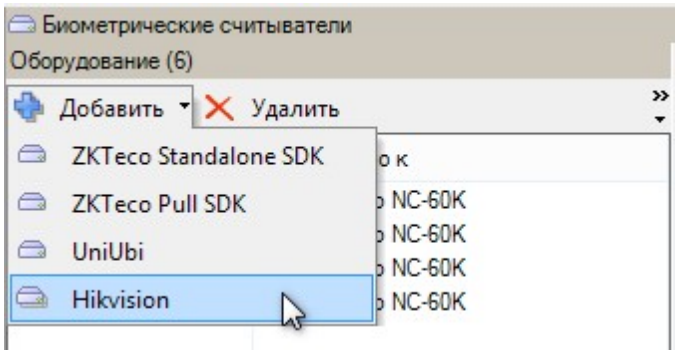


Сохраните сделанные изменения, нажав на "галочку" справа вверху экрана. Терминал вернется на экран *Меню.* Теперь можно выйти из настроек терминала и приступить к настройкам ПО ParsecNET 3.

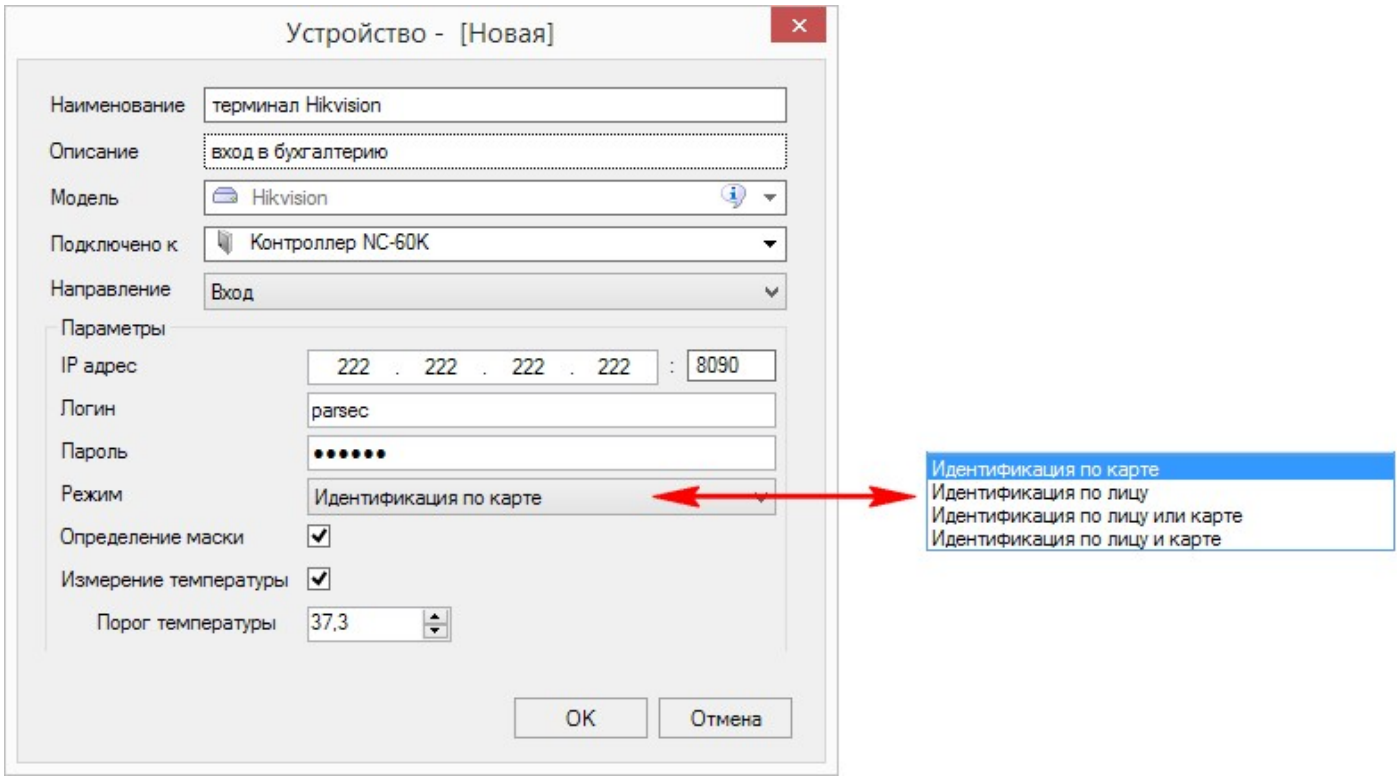
9. Откройте Редактор оборудования ПО ParsecNET 3 и нажмите на кнопку *Биометрические считыватели:*



10. На открывшейся панели нажмите на кнопку *Добавить* и в раскрывшемся списке выберите "Hikvision":



Откроется окно параметров устройства:



11. Настройте параметры работы с терминалом:

- поля *Наименование* и *Описание* рекомендуется заполнять так, чтобы позже было легко идентифицировать устройство и его местонахождение;
- *Подключено к* - из раскрывающегося списка выберите контроллер доступа, к которому подключен терминал;
- *Направление* - выберите, какое направление прохода будет защищать терминал;
- *IP-адрес* - введите адрес, заданный в настройках терминала (шаг 6);

- *Логин* и *Пароль* - введите логин и пароль для доступа к терминалу;
- *Режим* - из раскрывающегося списка выберите нужный режим прохода:
  - "Идентификация по карте" - субъект доступа идентифицируется по коду предъявленной карты;
  - "Идентификация по лицу" - субъект доступа идентифицируется, если его лицо соответствует фото в БД устройства;
  - "Идентификация по лицу или карте" - субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты;
  - "Идентификация по лицу и карте" - субъект доступа идентифицируется совместно по коду предъявленной карты и по лицу.

  Если субъект доступа отсутствует в БД, то доступ ему запрещается, а в системе формируется событие "Нет входа (или выхода) - неизвестный".
- *Определение маски* - при установленном флажке терминал будет определять, надета ли маска субъектом доступа. При ее отсутствии проход будет заблокирован с формированием в ПО ParsecNET 3 события «Нет входа – детектор маски» или «Нет выхода – детектор маски» и выдано сообщение о необходимости надеть маску;
- *Измерение температуры* - при установке флажка будет проводиться измерение температуры субъекта доступа и если она превышает лимит, установленный в поле ниже, доступ блокируется. В ПО ParsecNET 3 измеренная температура фиксируется в событии «Нет входа – температура превышена» или «Нет выхода – температура превышена». Если температура в норме, проход разрешается и формируется пара событий «Нормальный вход (или выход) по ключу» и «Температура в норме», в параметрах последнего фиксируется измеренная прибором температура.

12. Нажмите на кнопку *ОК*. Окно добавления нового устройства закроется и на панели оборудования появится новая запись;
13. Нажмите на кнопку *Передача сотрудников и посетителей* в карточке терминала. В память терминала будут загружены данные всех субъектов доступа, присутствующих в системе (фото, ФИО и первичный идентификатор). Впоследствии, все изменения в БД субъектов доступа будут автоматически синхронизироваться с БД в памяти терминала.

На этом настройка завершена. Теперь при успешной идентификации субъекта доступа на экране терминала MinMoe будет отображаться его фото, имя и идентификатор пользователя в СКУД ParsecNET 3 в 16-ном формате.

11.9.2 Интеграция с биометрическими устройствами UniUbi

Лицензируется как PNSoft-FR[344] или PNSoft-FR1CH[344]

Терминалы биометрической идентификации Uface компании UniUbi используются для распознавания пользователей СКУД ParsecNET 3 по карте и/или по лицу, с опциональным бесконтактным термоконтролем пользователей. Также терминал может отслеживать наличие маски на пользователе.

Для работы могут использоваться терминалы, читающие карты EM Marin и/или карты семейства Mifare.

Для тестирования модуля интеграции использовались терминалы:

- Uface 8T Temp;
- Uface 4;
- Uface 5 Lite;
- Uface 5;
- Uface 7T Pro.

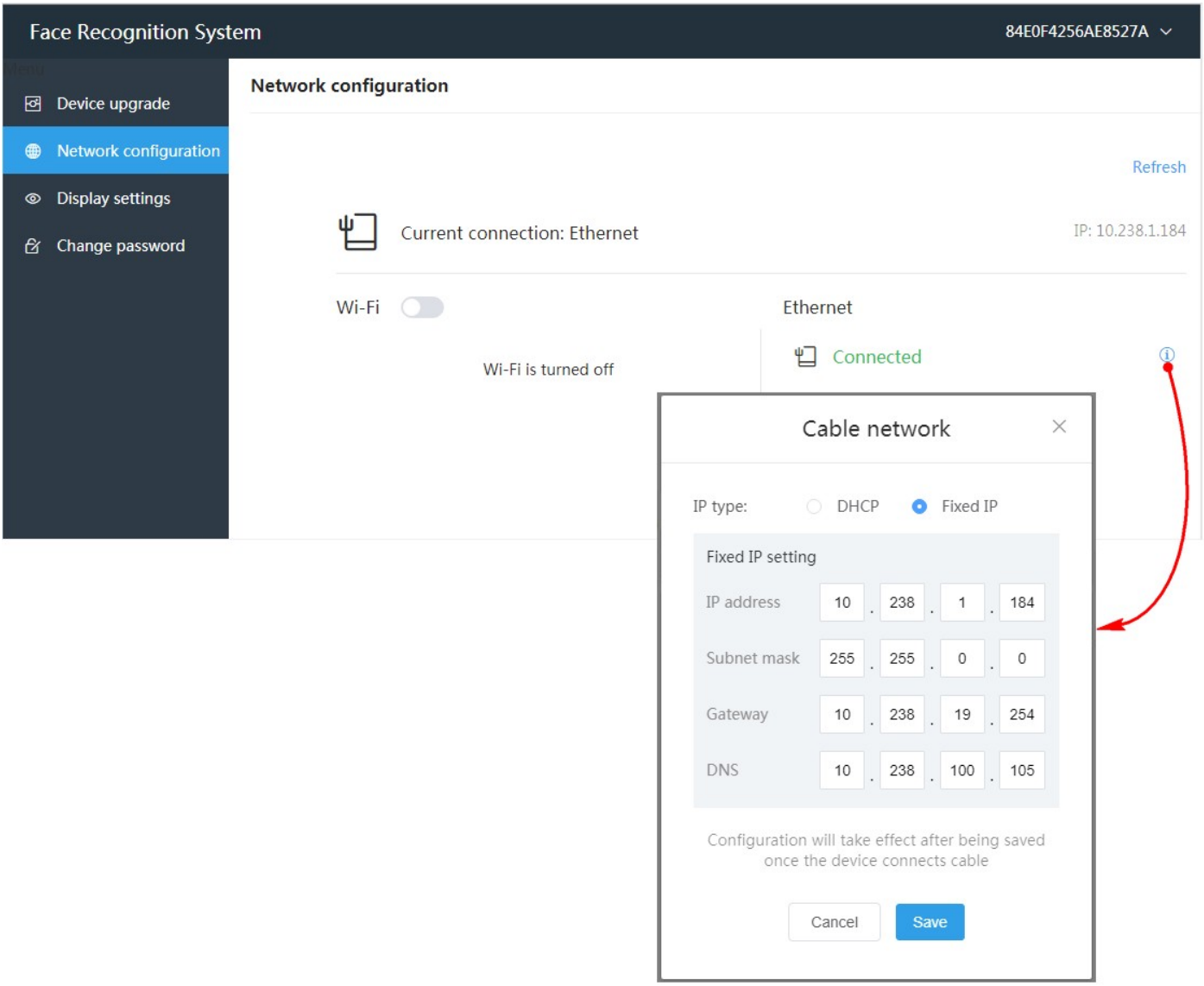


В БД терминала биометрической идентификации загружаются данные пользователей, чьи группы доступа содержат контроллер, к которому подключен этот терминал. Поэтому при выборе модели терминалов необходимо тщательно следить, чтобы объем их памяти позволял сохранить эти данные.

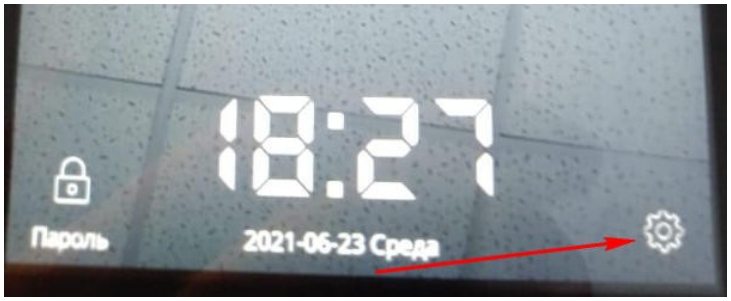
Для корректного распознавания лиц загруженные в БД терминалов биометрической идентификации фотографии субъектов доступа должны иметь разрешение не менее 128x128 пикселей.

Настройка терминала биометрической идентификации состоит из следующих шагов:

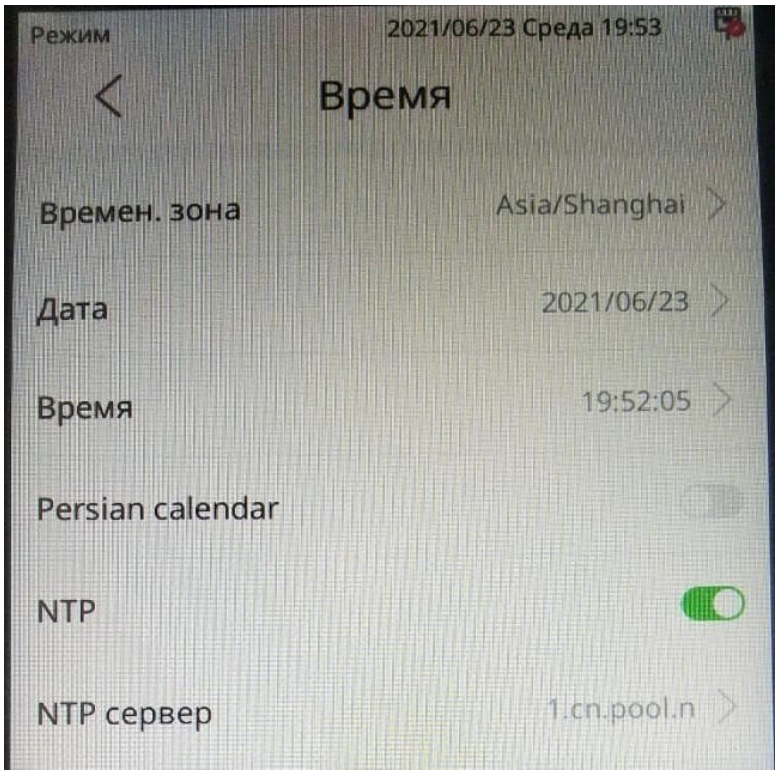
1. Смонтируйте терминал в выбранном месте и подключите его к контроллеру доступа и к сети Ethernet, в которой находится сервер СКУД ParsecNET 3. Терминал подключается к контроллеру доступа посредством модуля сопряжения NI-TW с серийными номерами 086-00-xxxx и выше. Код идентификатора субъекта доступа передается в формате Wiegand 34. Для этого перемычка на плате преобразователя должны быть выставлена в положение W26 (подробнее в Руководстве по эксплуатации NI-TW);
   Соединение по сети Ethernet с сервером СКУД ParsecNET 3 предназначено для загрузки пользователей и последующего автоматического обновления БД пользователей в терминале, а также для получения данных термометрии и получения в ПО ParsecNET 3 событий отказа в доступе с указанием причин;
2. Введите заводской IP-адрес терминала в адресной строке браузера и пропишите порт 8090. Строка должна иметь общий вид http://<device-ip>:8090 (например, http://168.12.12:8090);
3. Нажмите на клавишу Enter, в открывшемся окне введите заводской пароль и нажмите на кнопку *Log In,* откроется веб-интерфейс терминала, где можно изменить IP-адрес и/или пароль;



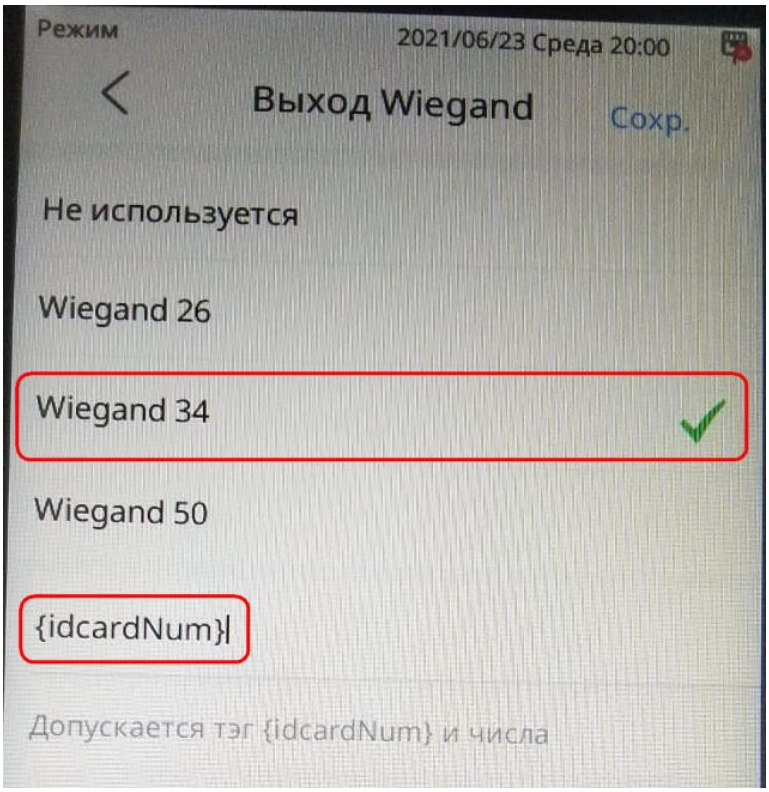
4. Для доступа к параметрам терминала нажмите на значок шестеренки в правом нижнем углу экрана терминала (рисунки показаны на примере терминала Uface модели OS-M355C1-V-R23WFC):



5. В открывшемся окне введите заводской пароль или новый пароль, установленный через веб-интерфейс (шаги 2 и 3). После нажатия на кнопку *Вход* откроется окно *Настройки*;
6. Последовательно нажмите на значки *Настройки системы* и *Время*. В открывшемся окне задайте текущее время и адрес NTP сервера точного времени (необязательно);

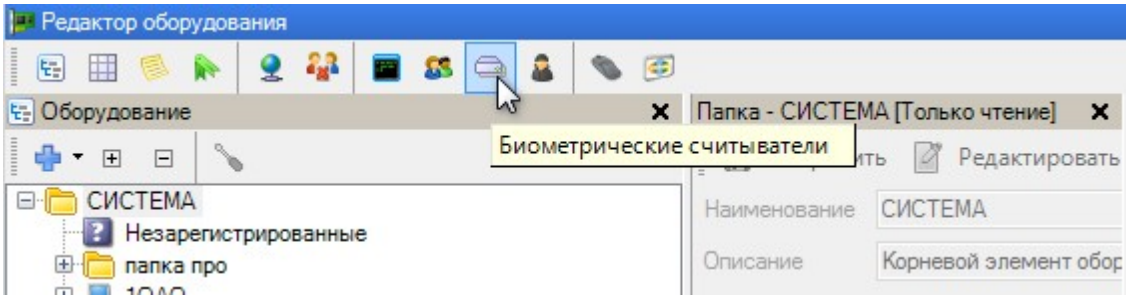


7. Вернитесь в окно *Настройки*, нажимая на стрелку влево в левом верхнем углу экрана терминала (см. рисунок выше);
8. Последовательно нажмите на значки *Параметры - Настройки распознавания - При успешном распознавании - Выход Wiegand*;
9. В открывшемся окне установите флажок Wiegand 34 и в нижней строке введите текст(без кавычек) "{idCardNum}".

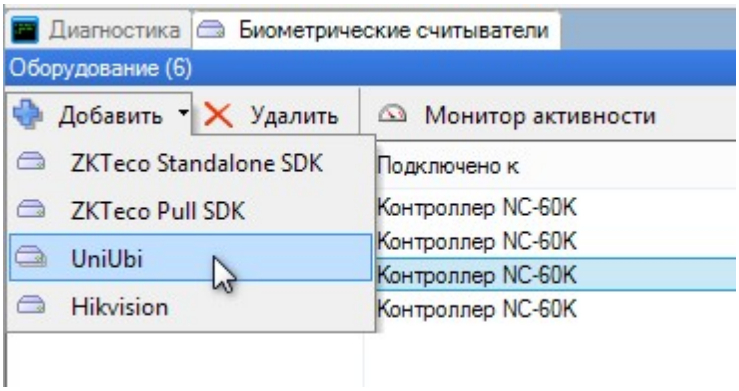


Сохраните введенные значения, нажав на значок *Сохр.* справа вверху экрана терминала. Теперь можно выйти из настроек терминала и приступить к настройкам ПО ParsecNET 3.

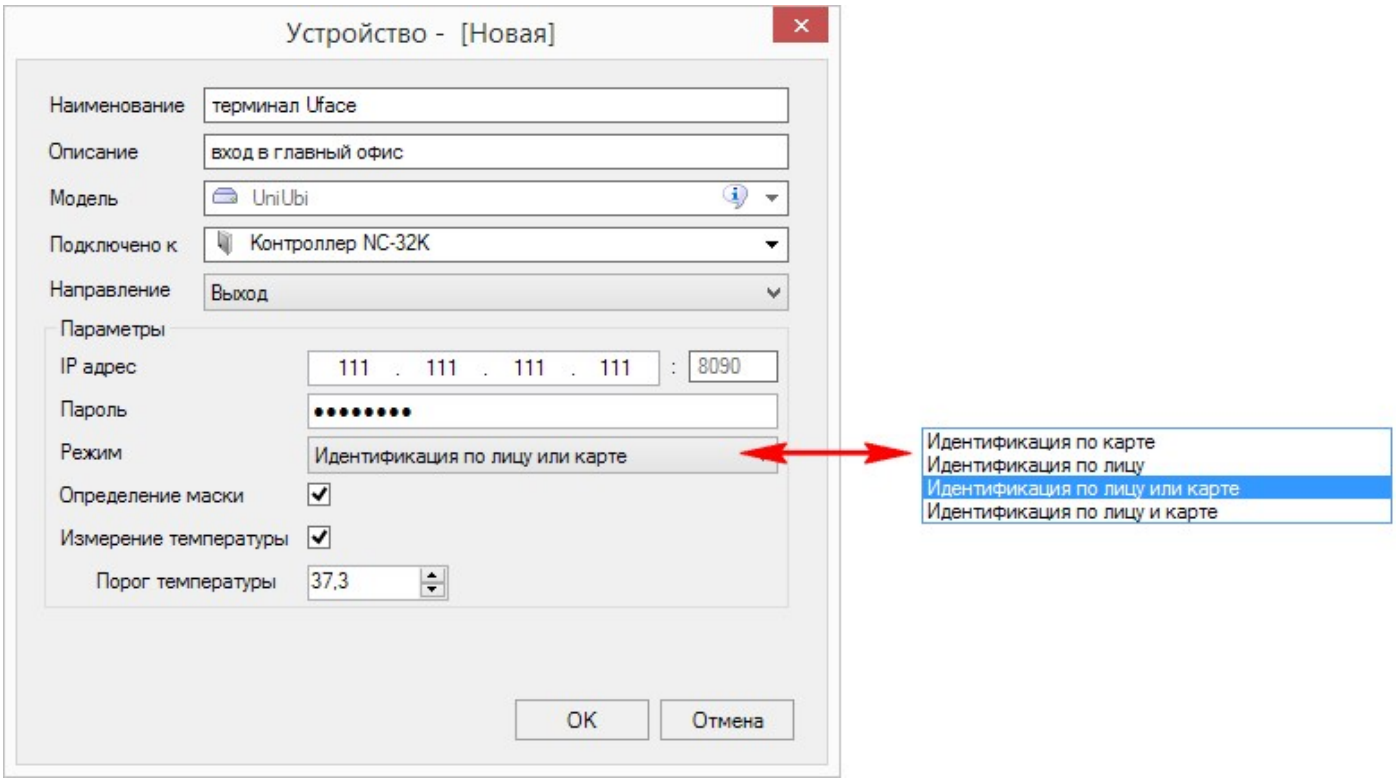
10. Откройте Редактор оборудования ПО ParsecNET 3 и нажмите на кнопку *Биометрические считыватели:*



11. На открывшейся панели нажмите на кнопку *Добавить* и в раскрывшемся списке выберите "UniUbi":



Откроется окно параметров устройства:



12. Настройте параметры работы с терминалом:

- поля *Наименование* и *Описание* рекомендуется заполнять так, чтобы позже было легко идентифицировать устройство и его местонахождение;
- *Подключено к* - из раскрывающегося списка выберите контроллер доступа, к которому подключен терминал;
- *Направление* - выберите, какое направление прохода будет защищать терминал;

- *IP-адрес* и *Пароль* - заполните данными, введенными в терминал на шаге 3;
- *Режим* - из раскрывающегося списка выберите нужный режим прохода:
  - "Идентификация по карте" - субъект доступа идентифицируется по коду предъявленной карты;
  - "Идентификация по лицу" - субъект доступа идентифицируется, если его лицо соответствует фото в БД устройства;
  - "Идентификация по лицу или карте" - субъект доступа идентифицируется либо по лицу, либо по коду предъявленной карты;
  - "Идентификация по лицу и карте" - субъект доступа идентифицируется совместно по коду предъявленной карты и по лицу.

  Если субъект доступа отсутствует в БД, то доступ ему запрещается, а в системе формируется событие "Нет входа (или выхода) - неизвестный".
- *Определение маски* - при установленном флажке терминал будет определять, надета ли маска субъектом доступа. При ее отсутствии проход будет заблокирован с формированием в ПО ParsecNET 3 события «Нет входа – детектор маски» или «Нет выхода – детектор маски» и выдано сообщение о необходимости надеть маску;
- *Измерение температуры* - при установке флажка будет проводиться измерение температуры субъекта доступа и если она превышает лимит, установленный в поле ниже, доступ блокируется. В ПО ParsecNET 3 измеренная температура фиксируется в событии «Нет входа – температура превышена» или «Нет выхода – температура превышена». Если температура в норме, проход разрешается и формируется пара событий «Нормальный вход (или выход) по ключу» и «Температура в норме», в параметрах последнего фиксируется измеренная прибором температура.

13. Нажмите на кнопку *ОК*. Окно добавления нового устройства закроется и на панели оборудования появится новая запись;
14. Нажмите на кнопку *Передача сотрудников и посетителей* в карточке терминала. В память терминала будут загружены данные всех субъектов доступа, присутствующих в системе (фото, ФИО и первичный идентификатор). Впоследствии, все изменения в БД субъектов доступа будут автоматически синхронизироваться с БД в памяти терминала.

На этом настройка завершена. Теперь при успешной идентификации субъекта доступа на экране терминала Uface будет отображаться его фото, ФИО и номер карты в десятичном формате.

11.10 Интеграция с системами распознавания документов

Модули распознавания документов предназначены для автоматизированного ввода в систему данных с паспортов РФ, загранпаспортов РФ, водительских удостоверений РФ, а также загранпаспортов других стран.

В систему ParsecNET 3 интегрированы следующие системы распознавания документов:

- Scanify производства компании Cognitive Technologies *(продажа модулей прекращена с декабря 2019)*;
- Regula от ООО "Регула";
- ABBYY производства одноименной компании.

Для каждого модуля требуется своя лицензия, а для модуля Regula также сканер производства ООО "Регула".

Отличия модулей отражены в таблице:

Модуль распознавания документов	Паспорт РФ	Загранпаспорт РФ	Водительское удостоверение			Загранпаспорт других стран	Распознавание сделанного ранее скана
			образец №1	образец №2	новых		

					образцов		
Scanify	●	●	●	●	●	●	●
Regula	●	●	●	●	●	●	●
ABBYY	●	●	●	●	●	●	●

Более подробно особенности каждого модуля описаны ниже.

Модуль Scanify

- Лицензируется как PNSoft-DS Cognitive[344];
- Распознавание водительских удостоверений РФ образцов №1 и №2[673], паспортов и загранпаспортов РФ (в том числе биометрических);
- Автоматическое определение типа сканируемого документа;
- Требование к разрешению скана документа – 300 dpi;
- Работа на 32-битных ОС (x86), либо в режиме совместимости на 64-битных ОС при установке специального приложения Parsec;
- Отдельное лицензирование ключом Cognitive Passport каждого рабочего места;
- Отдельное лицензирование каждой рабочей станции ParsecNET 3;

Использование данного модуля подразумевает наличие сканера.

Модуль Regula

- Лицензируется как PNSoft-DS Regula[344];
- Распознавание паспортов и загранпаспортов РФ, а также загранпаспортов большинства других стран;
- Распознавание водительских удостоверений новых образцов[673];
- Regula не требует дополнительного лицензирования каждого рабочего места;
- Отдельное лицензирование каждой рабочей станции ParsecNET 3;
- Работа на 32-битных и 64-битных ОС.

Использование данного модуля подразумевает приобретение специального сканера Regula.

Модуль ABBYY

- Лицензируется как PNSoft-DS ABBYY[344];
- Распознавание водительских удостоверений всех типов, паспортов и загранпаспортов РФ;
- Определение типа документа осуществляется вручную;
- Работа на 32-битных ОС (x86), либо в режиме совместимости на 64-битных ОС при установке специального приложения Parsec;
- Отдельное лицензирование ключом ABBYY каждого рабочего места;
- Отдельное лицензирование каждой рабочей станции ParsecNET 3;

Использование данного модуля подразумевает наличие сканера.

До начала работы с документами необходимо настроить соответствие[674] полей отсканированного документа и дополнительных полей субъектов доступа. По умолчанию установлено только соответствие полей ФИО и фотографии.

Работа с дополнительными полями персонала доступна только при включении расширенного режима в меню "Файл", в обычном режиме работа вкладка "Дополнительные поля" и их настройка недоступны.

Водительские удостоверения (по материалам ru.wikipedia.org)

На 2017 год в России действуют водительские удостоверения следующих форматов:

- ламинированное бумажное размером 148×105 мм с надписью «PERMIS DE CONDUIRE» (официальное название — образец № 1), выдавалось с 1999 по 2011 годы:



- пластиковое размером 85×55 мм с надписью «PERMIS DE CONDUIRE» (образец № 2), официально оформлялось также с 1999 по 2011 гг., фактически в некоторых регионах выдача прекращена раньше:



- удостоверение нового образца, соответствующее требованиям Венской конвенции о дорожном движении 1968 года (выдавалось с 2011 по 2014 годы):



- обновлённое удостоверение нового образца (с 2014 года).



11.10.1 Установка, выбор и настройка

Установка

Модуль Scanify

Продажа модулей прекращена с декабря 2019 года. Проданные ранее модули поддерживаются.

Установите программу, запустив приложение "Passport API.msi" с дистрибутивного диска, и следуя подсказкам мастера установки.

После установки на 32-разрядные станции дополнительных действий не требуется.

После установки на 64-разрядные станции необходимо далее запустить приложение "ParsecNET 3 - 32 bit converter.exe" из папки с установочными файлами ParsecNET 3. Приложение запускается на тех же компьютерах, на которых установлен Scanify Passport API. Также это приложение требуется запускать после каждого обновления системы ParsecNET 3.

Для использования модуля распознавания документов PNSoft-DS Cognitive[344] требуется:

- на сервер системы ParsecNET установить ключ защиты Parsec с лицензией на этот модуль;
- на ПК с установленным модулем распознавания документов установить ключ защиты Scanify;
- предоставить полный доступ к папке, в которую установлен модуль (адрес по-умолчанию C:\Program Files (x86)\Cognitive. В свойствах папки, на вкладке *Безопасность*, в блоке *Разрешения для пользователя <username>,* в столбце *Разрешить* должны быть установлены все флажки, кроме *Особые разрешения*).

Модуль Regula

Для использования модуля распознавания документов PNSoft-DS Regula[344] требуется:

- на сервер системы ParsecNET установить ключ защиты Parsec с лицензией на этот модуль;
- к ПК, где создается рабочее место для распознавания документов, подключить сканер Regula (приобретается отдельно) и установить пакет SDK с дистрибутивного диска "Install Regula Software".

Модуль ABBYY

Установите ПО с дистрибутивного диска "ABBYY PassportReader SDK".

ABBYY SDK версии 1.5.2 и выше необходимо устанавливать той же разрядности (32 или 64 бит), что и ParsecNET 3.

В процессе установки необходимо ввести Customer Project ID "qaPDNBtca6qBy3nzniDj" (без кавычек). В противном случае интеграция с ABBYY работать не будет.

При установке ABBYY SDK ниже 1.5.2 Customer Project ID вводить не требуется. В зависимости от разрядности ParsecNET 3 необходимо:

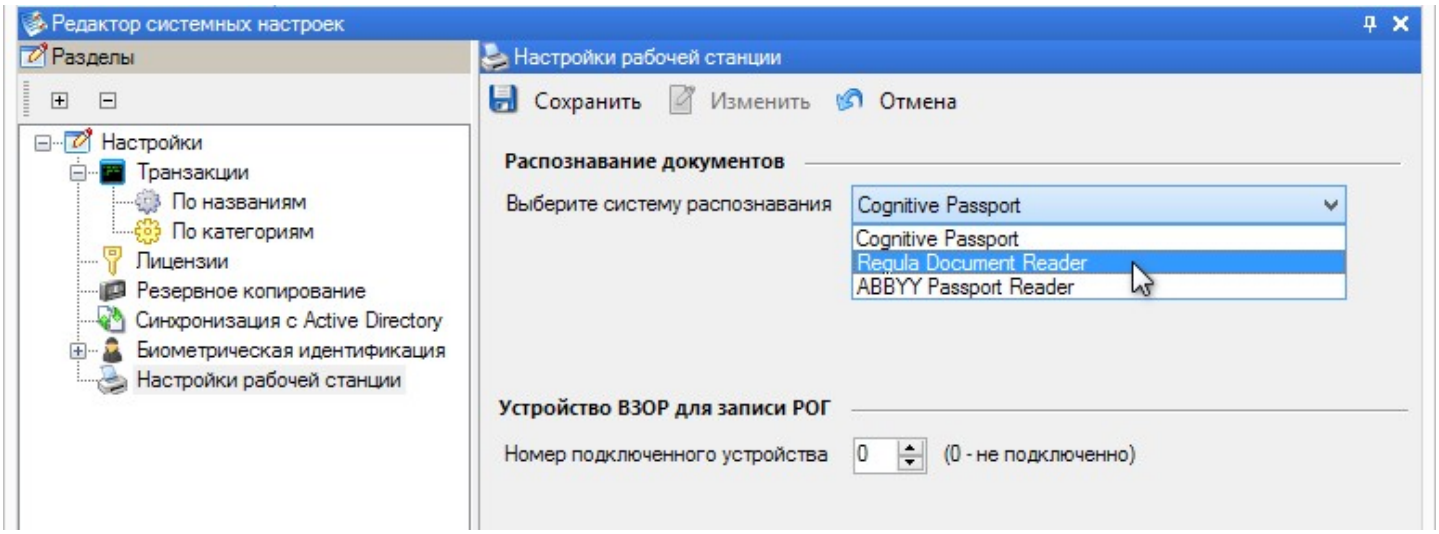
- для 64-разрядных станций необходимо запустить приложение "ParsecNET 3 - 32 bit converter.exe" из папки с установочными файлами ParsecNET 3. Приложение запускается на тех же компьютерах, на которых установлен модуль. Также это приложение требуется запускать после каждого обновления системы ParsecNET 3;
- для 32-разрядных станций дополнительных действий не требуется.

Для использования модуля распознавания документов PNSoft-DS ABBYY[344] требуется:

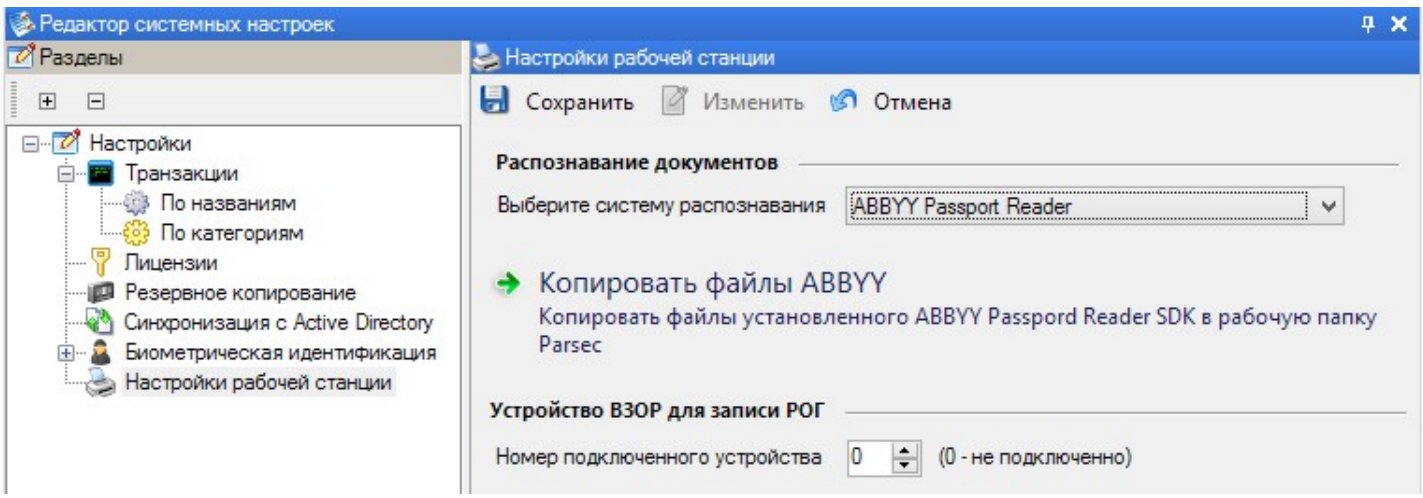
- на сервер системы ParsecNET установить ключ защиты Parsec с лицензией на этот модуль;
- на ПК с установленным модулем распознавания документов установить ключ защиты (предоставляется при покупке лицензии на PNSoft-DS ABBYY).

Выбор модуля

Выбор модуля, который будет использоваться для распознавания документов, производится в Редакторе системных настроек, в разделе *Настройки рабочей станции*:



При выборе "ABBYY Passport Reader" появится кнопка *Копировать файлы ABBYY*:



Далее, в зависимости от версий SDK и ОС Windows, выполните необходимые действия:

Версия ABBYY Pasport Reader SDK	Версия ОС Windows	
	32-битная	64-битная
1.5.2 и выше	Нажать на кнопку "Копировать файлы ABBYY", указать папку в которой установлен ABBYY, нажать на кнопку *ОК*. Файлы скопируются в рабочую папку ParsecNET 3 (по умолчанию это папка C:\Program Files\MDO\ParsecNET 3\). Если в момент копирования файлов какие-то библиотеки заняты, они могут не скопироваться в целевую директорию. Тогда это необходимо сделать вручную.	
1.5.0*	Дополнительных действий не требуется.	Запустить конвертер "ParsecNET 3 - 32 bit converter".

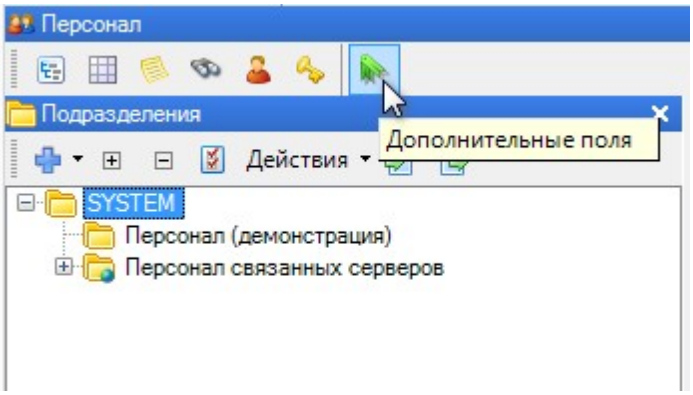
* SDK иных версий не тестировались.

Настройка

Перед настройкой соответствий необходимо завести в системе ParsecNET 3 требуемый набор дополнительных полей, так как по-умолчанию в системе присутствуют только основные поля персонала.

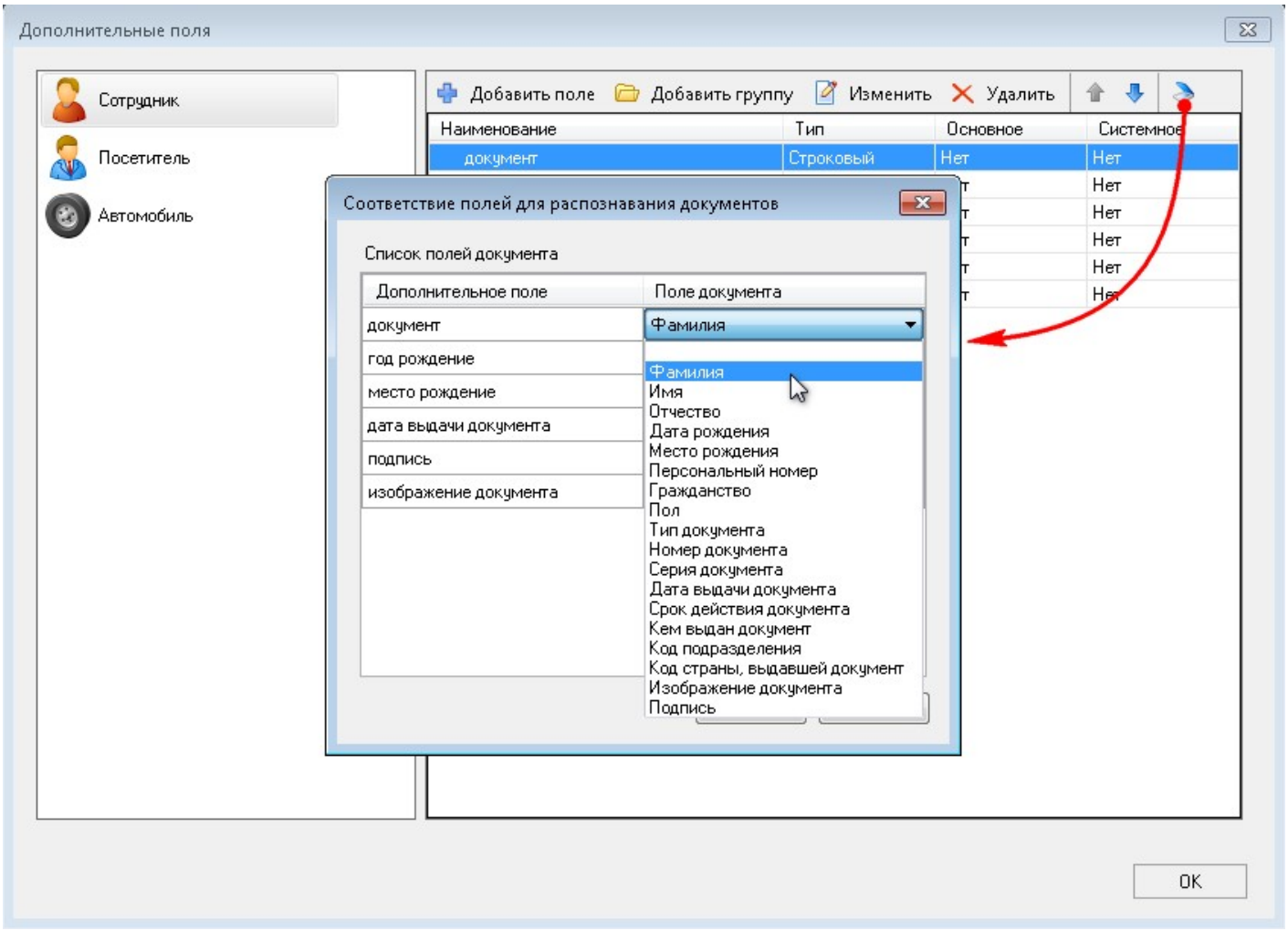
До начала работы с документами следует проставить соответствие между полями, полученными при распознавании документа, и полями (основными или дополнительными) субъекта доступа системы ParsecNET 3. Это делается в редакторе персонала:

1. Нажмите на кнопку *Дополнительные поля*:



2. В открывшемся окне выберите субъект доступа и перейдите в режим редактирования. Затем нажмите на кнопку *Настройка полей распознавания;*

3. В открывшемся диалоге выберите дополнительное поле персонала слева, а справа из раскрывающегося списка соответствующее ему поле документа, как показано на рисунке ниже:



При необходимости можно создать нужное дополнительное поле[264].

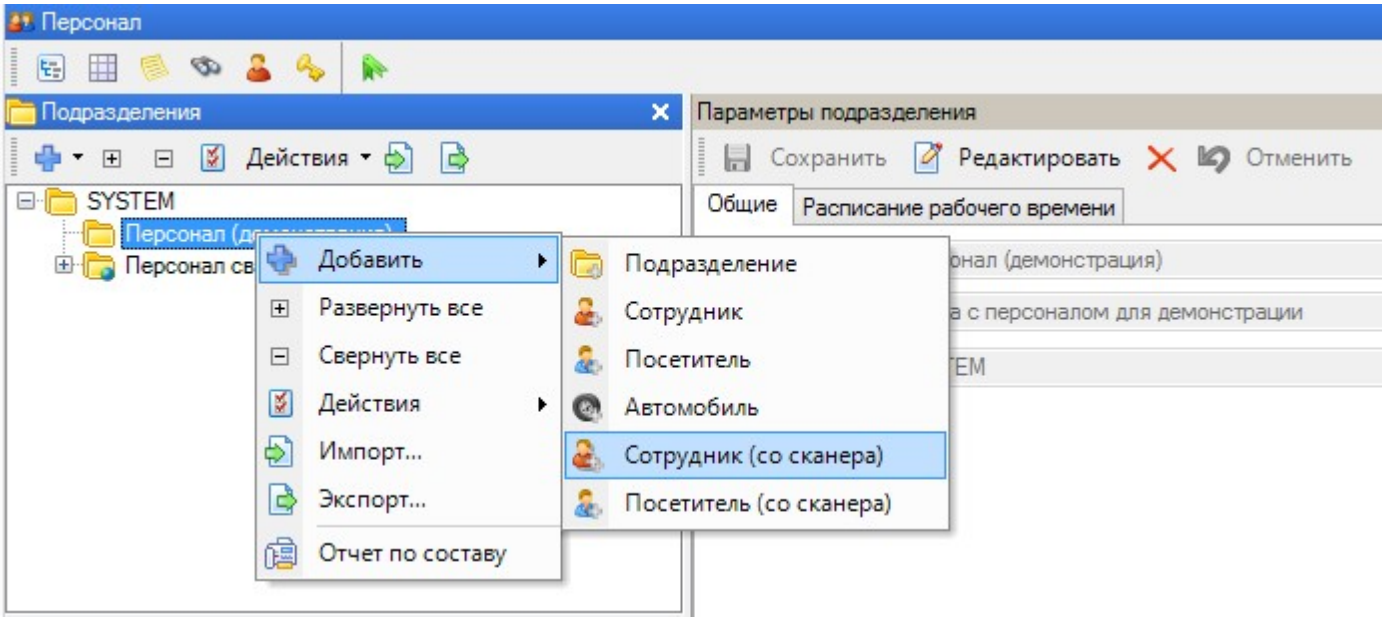
4. Повторите шаг 3 для всех дополнительных полей, которые необходимо заполнять при распознавании документов, а также для всех субъектов доступа, для которых это необходимо.

После установки соответствия всех необходимых полей можно переходить к работе с модулем[677] распознавания документов.

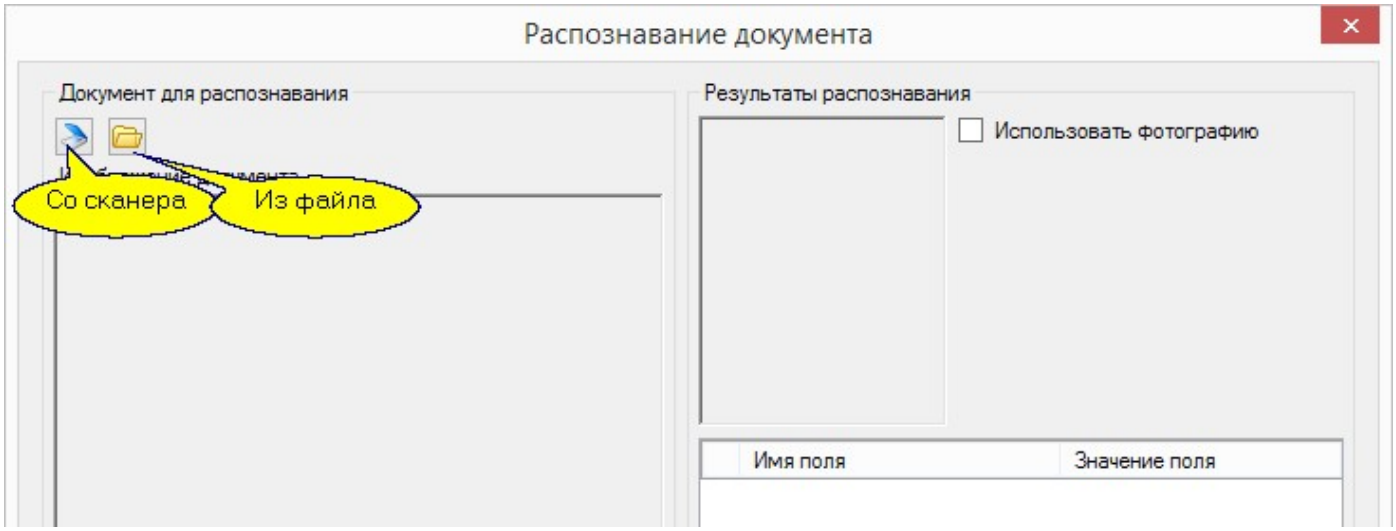
11.10.2 Работа с документами

Ввод данных из документа

В качестве примера рассмотрим работу с документами в редакторе персонала. Для этого выберите подразделение, в которое будете заносить сотрудника, и из меню выберите "Добавить - Сотрудник (со сканера)":



В появившемся диалоге можно выбрать ввод непосредственно со сканера или из файла с изображением ранее отсканированного документа:

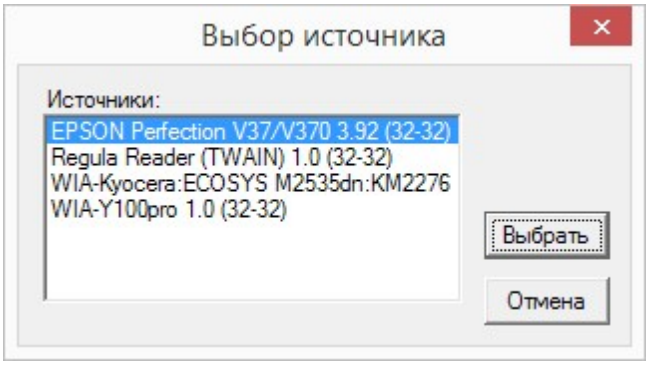


Для ввода со сканера последний должен быть подключен и доступен на компьютере, на котором мы редактируем персонал.

Для модуля ABBYY необходимо указать тип документа.

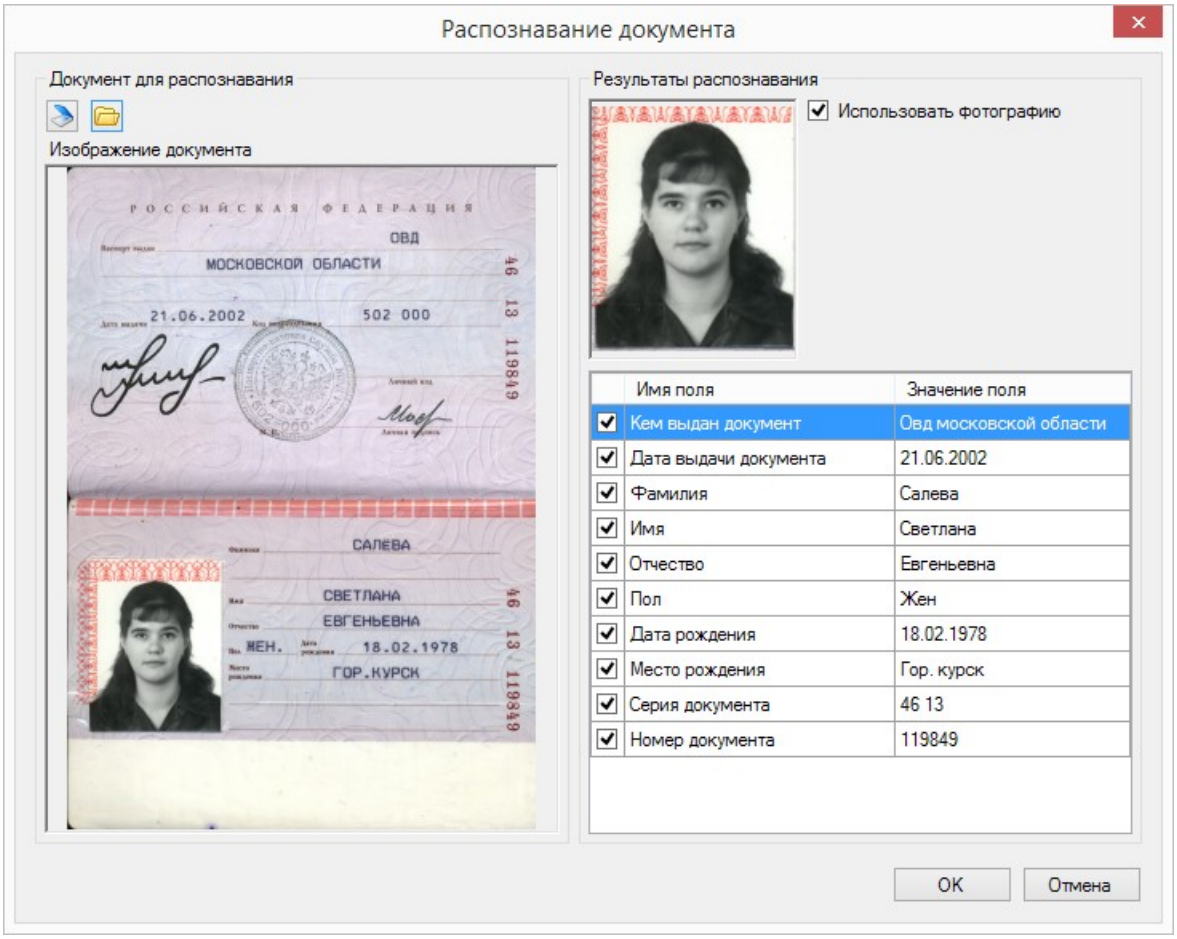
Модуль Regula распознает документы только со сканера.

После первого использования сканера его настройки сохраняются в системе, и впоследствии этот сканер будет выбираться автоматически. В случае, если к компьютеру подключены несколько сканеров, окно выбора нужного сканера открывается по нажатию на кнопку *Взять документ со сканера* при удержании клавиши *Shift.* На рисунке ниже показано окно выбора сканеров для модуля Scanify:



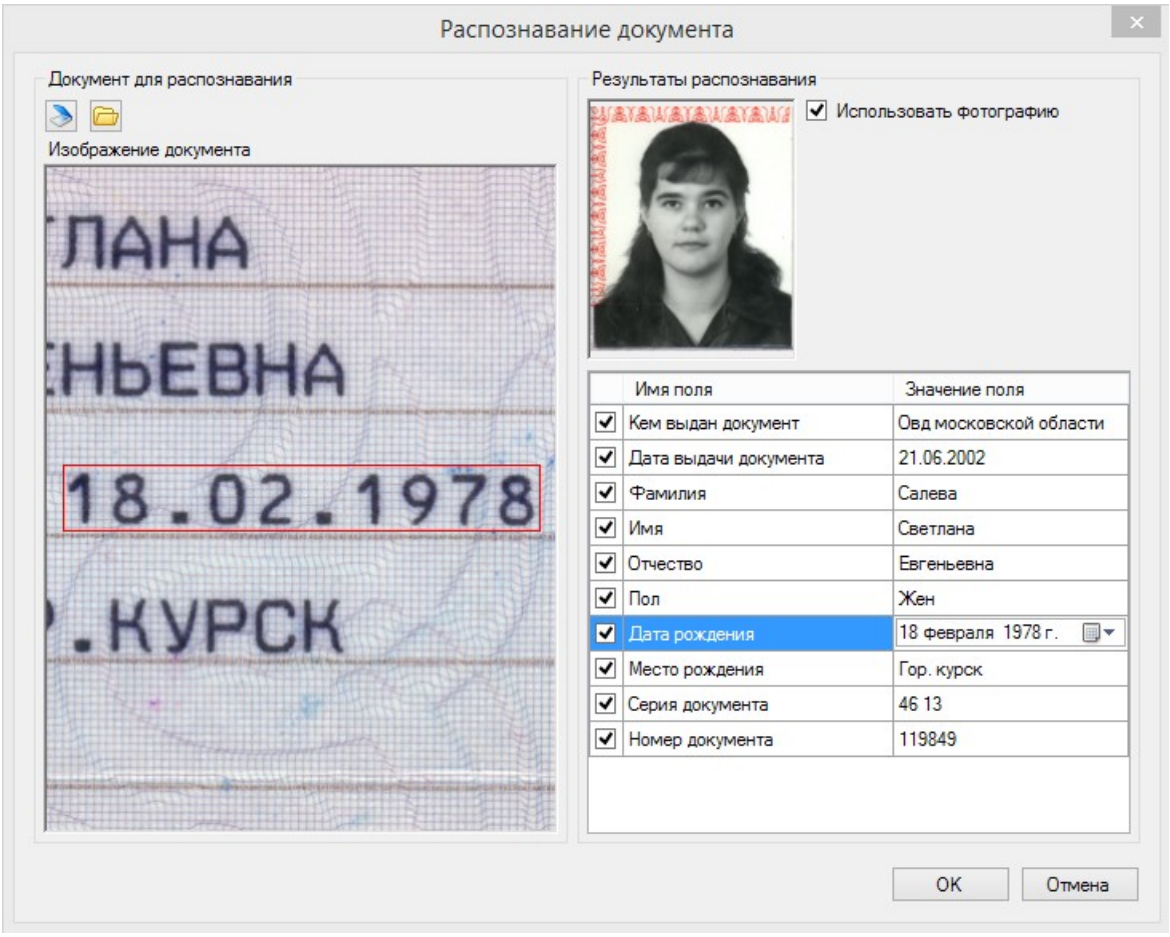
Для модуля Regula этот функционал недоступен, т.к. всегда автоматически выбирается его сканер.

Независимо от источника получения документа после распознавания мы получим изображение документа слева и все распознанные поля (включая фотографию) справа, как показано на рисунке ниже:



Если снять флажки в блоке *Результаты распознавания*, то распознанные значения не будут размещены в карточке субъекта доступа. При установленном флажке *Использовать фотографию* изображение из распознанного документа заменяет изображение в карточке субъекта доступа.

До сохранения введенного таким образом субъекта доступа можно проверить и скорректировать отдельные поля. Некорректно распознанные поля подсвечиваются розовым цветом. При позиционировании на поле появляется возможность отредактировать его значение, при этом в левой части изображение документа увеличивается и позиционируется автоматически на то место изображения, где расположено поле:



Если все данные корректны, то нажмите на кнопку *OK*, и в списке персонала (в нашем примере) появится новый сотрудник. Естественно, для определения его полномочий в системе потребуется стандартными средствами назначить сотруднику идентификатор (карточку), группу доступа и т.д.

См. также:

Настройка распознавания[674]

Редактор персонала[255]

11.11 Интеграция с системой хранения ключей KeyGuard

Модуль хранения ключей ("ключница") от компании KeyGuard предназначен для обеспечения учета и контроля выдачи ключей от помещений при помощи прикрепленных к ключам RFID-меток. В этом разделе описано добавление ключницы в систему и ее настройка. Правила работы с ключницей и расширенные настройки описаны в Инструкции по монтажу и эксплуатации системы хранения ключей KeyGuard, доступной на сайте производителя.

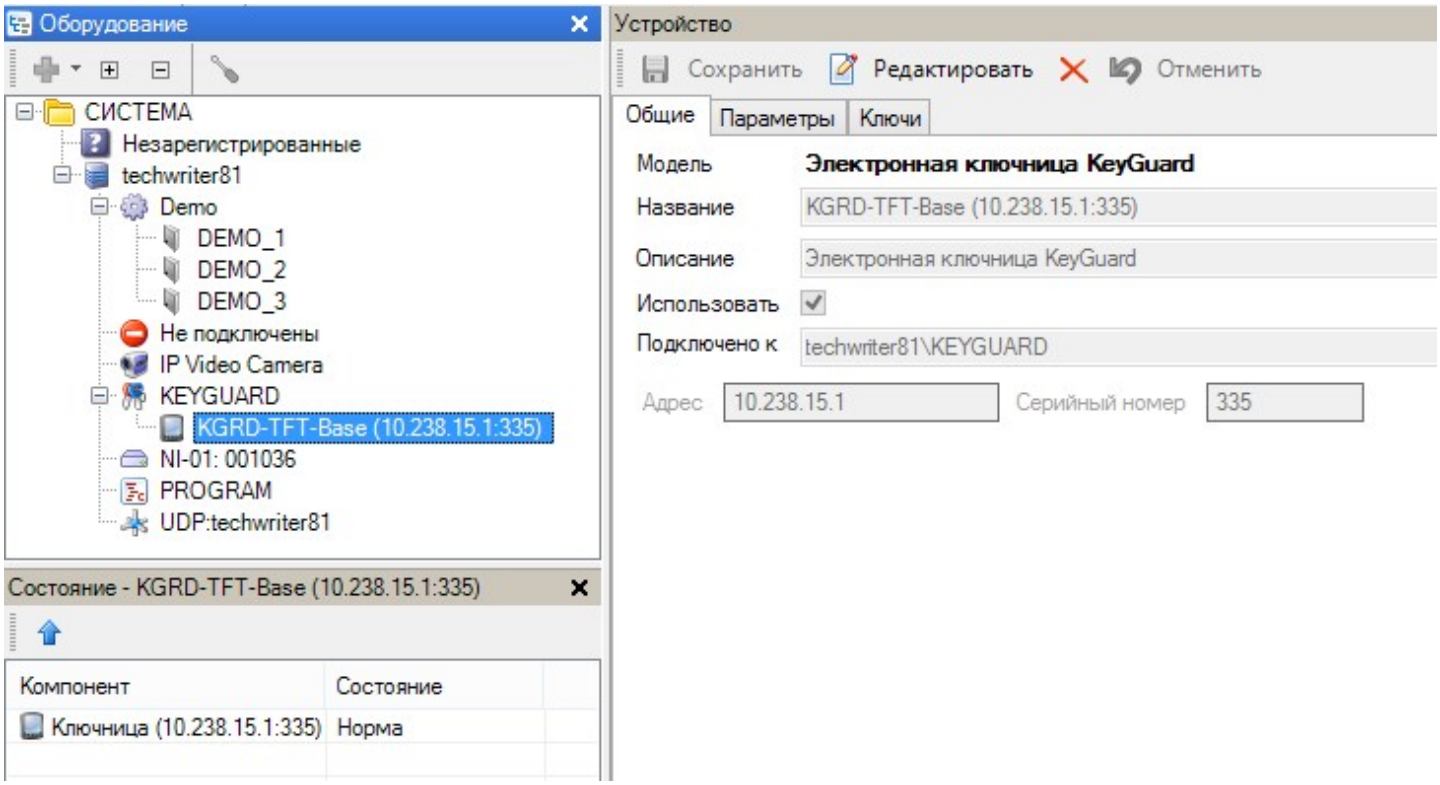
Добавление ключницы

Чтобы добавить ключницу в систему, выполните следующие действия:

1. Включите ключницу в сеть Ethernet. Сделайте это до подачи питания;
2. Включите ключницу в сеть 220В 50 Гц. Если кабель Ethernet подключен после включения системы, перезагрузите ключницу кнопкой *Перезагрузка*;
3. Переведите ключницу в режим настройки и на экране ключницы задайте IP-адреса:
   - *IP Адрес* - адрес ключницы в сети Ethernet;
   - *IP Сервер* - адрес сервера ParsecNET 3;

- *Маска подсети* - укажите ту же маску, что и у сервера ParsecNET 3;
- *Осн.шлюз* - узнайте IP адрес у своего администратора сети и введите его;
- *Порт Серв.* - по умолчанию порт сервера 8000. Если данный серверный порт уже занят, его можно изменить. В этом случае необходимо также изменить номер порта и на самом сервере.

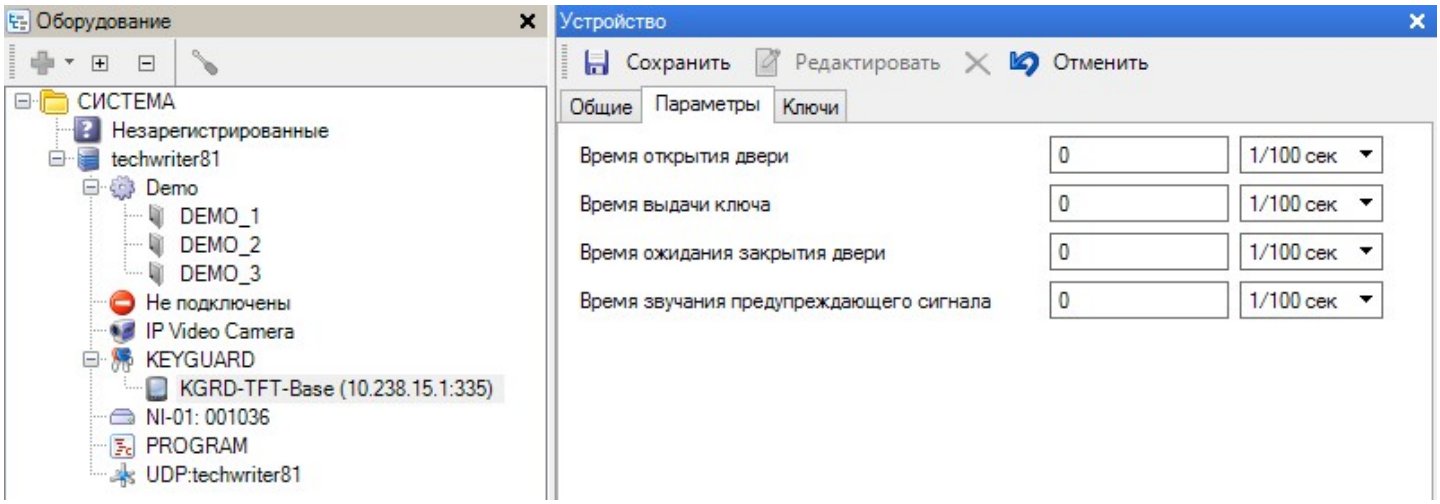
4. После этого последовательно нажмите на экране ключницы на кнопки *Сохранить* и *Перезагрузка*. Ключница готова к работе с системой ParsecNET 3;
5. В Редакторе оборудования произведите поиск оборудования. На канале KEYGUARD появится только что настроенное устройство:



Настройка параметров ключницы

Для настройки параметров ключницы выполните шаги:

1. Выберите ключницу в дереве оборудования;
2. Перейдите в режим редактирования и перейдите на вкладку *Параметры*:



3. Настройте параметры или оставьте настройки по умолчанию. Значение "0" соответствует настройкам по умолчанию, во втором поле можно выбрать размерность задаваемых параметров.

- *Время открытия двери* - время, на которое открывается дверца для доступа к модулям с ключами. По умолчанию - 10 сек;
- *Время выдачи ключа* - время, на которое разблокируются брелоки ключей, на получение которых пользователь имеет права. По умолчанию - 10 сек;

Не устанавливайте время открытия дверцы и время выдачи ключа более 50 секунд. В противном случае возможен выход из строя соленоидов замков.

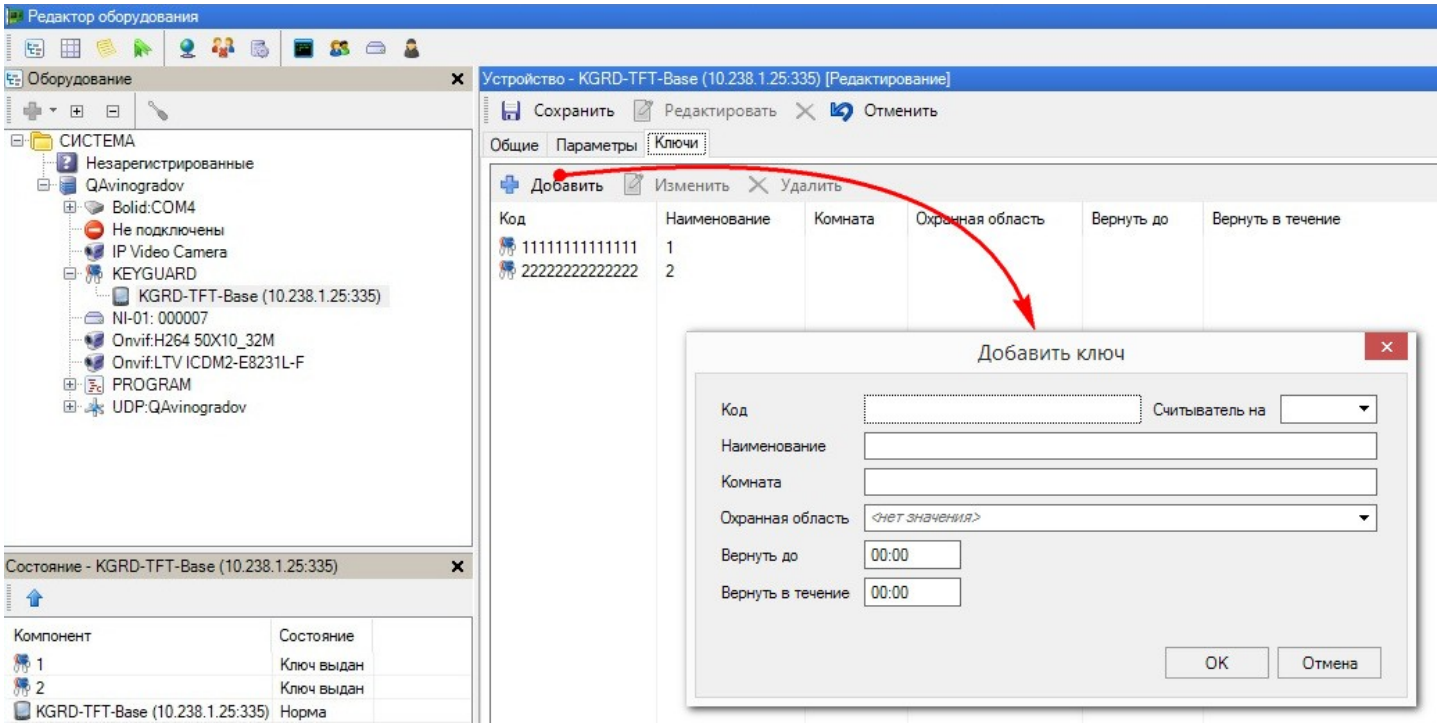
- *Время ожидания закрытия двери* - время, по истечении которого будет подаваться сигнал о незакрытой дверце ключницы. По умолчанию - 15 сек;
- *Время звучания предупреждающего сигнала* - время, в течение которого будет звучать сигнал о незакрытой дверце ключницы. По умолчанию - 15 сек.

4. Сохраните внесенные изменения.

Добавление ключей

Для добавления ключей в ключницу выполните следующие действия:

1. Выберите ключницу в дереве оборудования;
2. Перейдите в режим редактирования и перейдите на вкладку *Ключи*;
3. Нажмите на кнопку *Добавить* и в открывшемся окне задайте параметры:

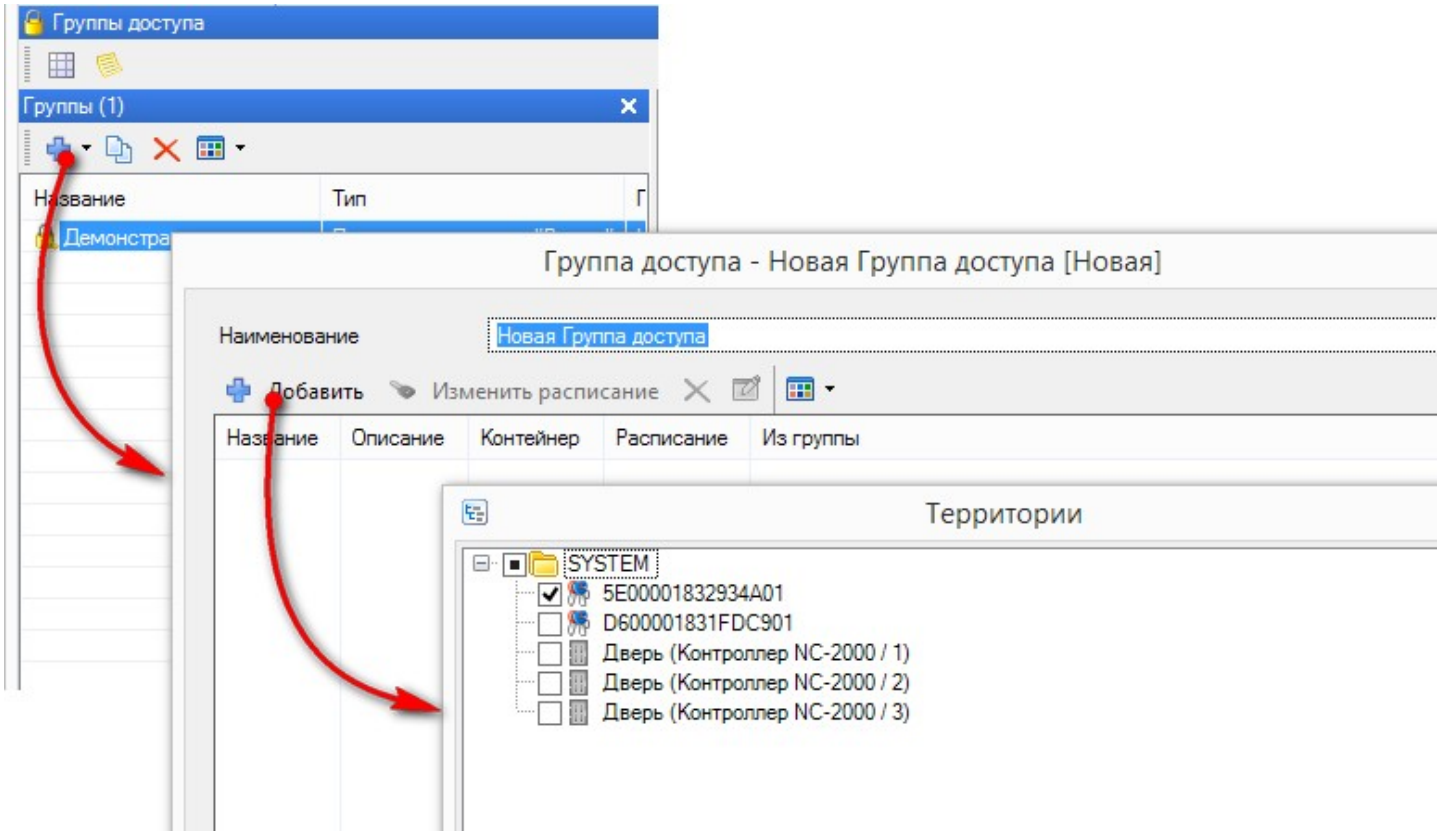


- *Код* - введите 16-ричный код ключа вручную или, если Вы используете настольный считыватель KeyGuard, вставьте ключ в его приемный слот. В последнем случае в поле *Считыватель на* необходимо указать порт, к которому подключен этот считыватель;
- *Наименование* - поле может быть отредактировано;
- *Комната* - в поле можно ввести номер комнаты в формате <число до 7 знаков + буква>. Допускаются буквы латинского или кириллического алфавита, как прописные, так и строчные. Номер можно ввести и без буквы;
- *Охранная область* - можно указать охранную область. При извлечении ключа из ячейки область будет сниматься с охраны. При возвращении ключа в свою ячейку область будет ставиться на охрану;

- *Вернуть до* - укажите время, до которого ключ должен быть возвращен в ключницу. Если ключ возвращен позже заданного времени, в системе формируется сообщение "Ключ задержан (не возвращен вовремя)";
- *Вернуть в течение* - укажите временной период, до истечения которого ключ должен быть возвращен в ключницу. Если ключ возвращен после истечения заданного периода, в системе формируется сообщение "Ключ задержан (не возвращен вовремя)".

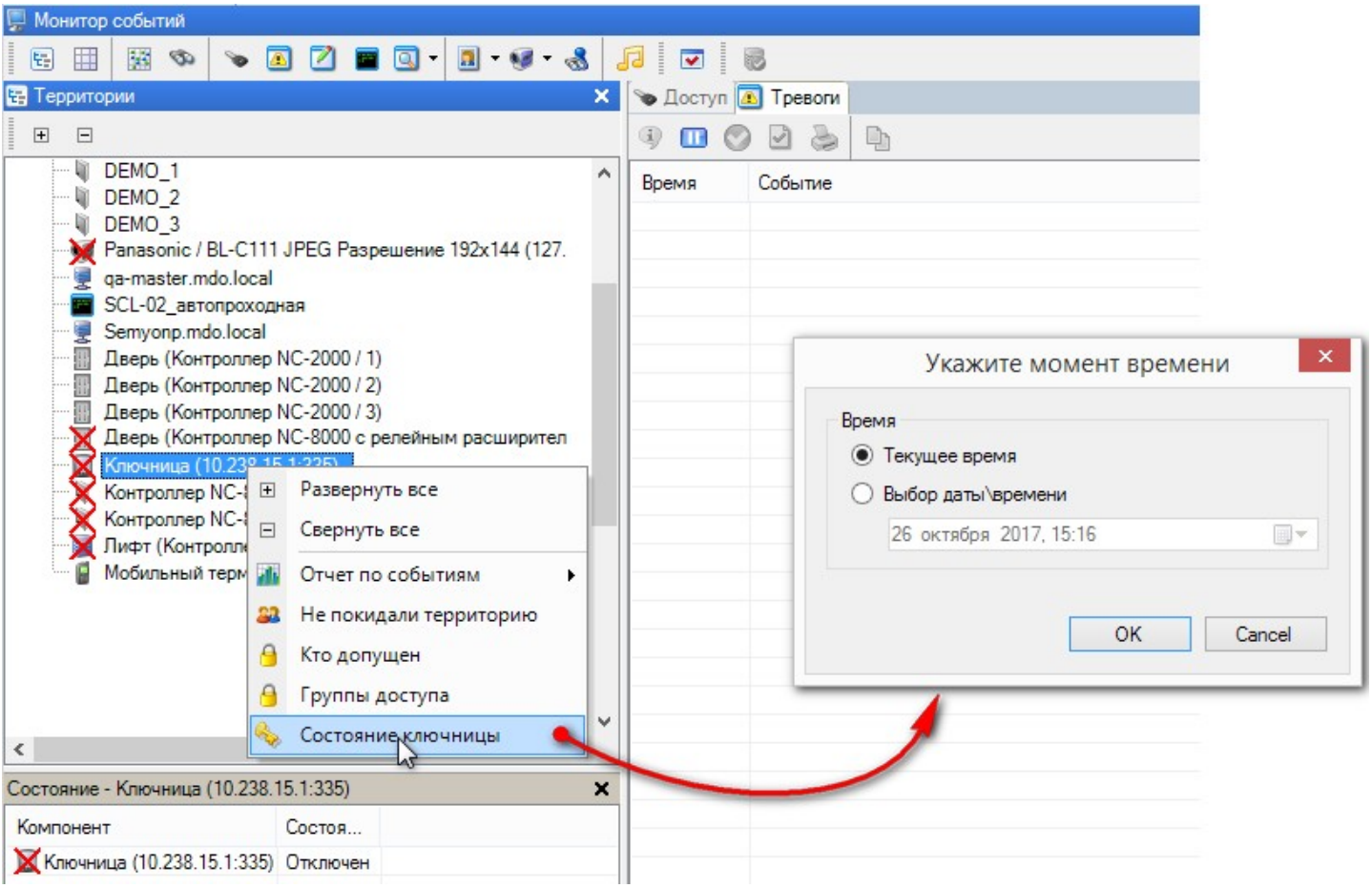
4. Сохраните сделанные настройки.

Теперь при создании или редактировании группы доступа[247] появится возможность указывать не дверь (контроллер), а ключ к двери. Все сотрудники, которым назначена данная группа доступа могут использовать свои идентификаторы для получения ключа из ключницы.

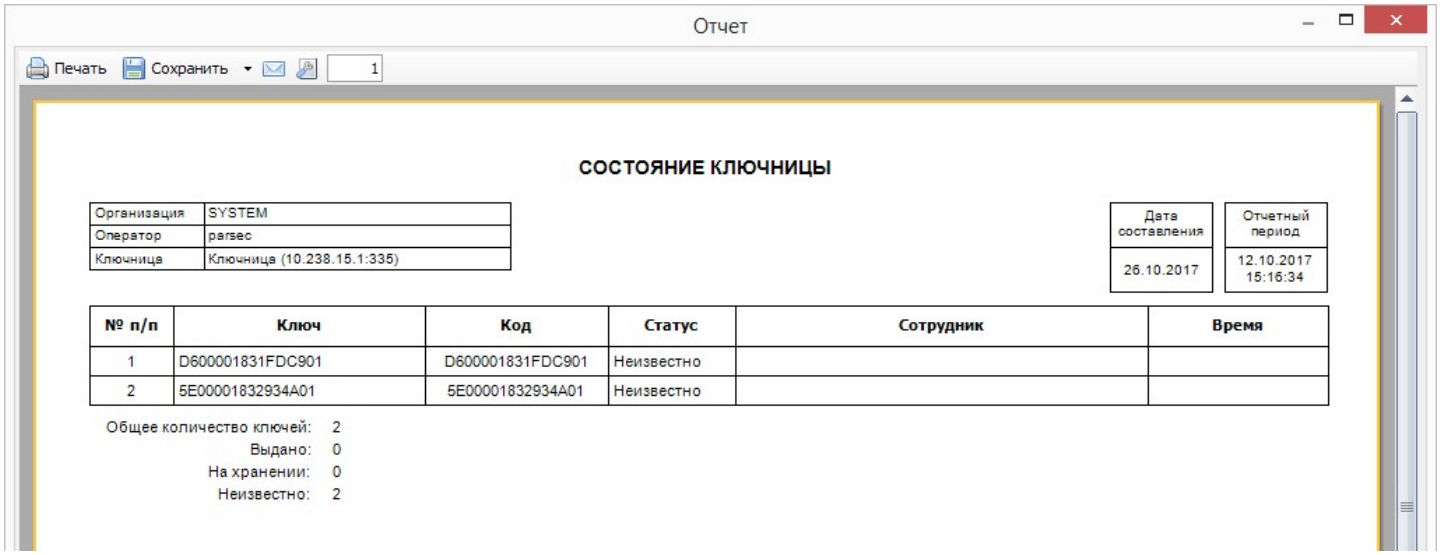


11.11.1 Отчет о состоянии ключницы

Для получения отчета о состоянии ключницы, перейдите в Монитор событий, выберите на левой панели модуль ключницы и в контекстном меню нажмите на команду "Состояние ключницы":



В открывшемся окне выберите нужный момент времени и нажмите на кнопку *OK*. Система сформирует отчет о состоянии ключницы в выбранное время:



11.12 Интеграция с домофонными системами

Лицензируется как PNSoft-IC [344]

Домофонная система - комплекс электронных, механических и программных средств обеспечения контроля доступа в охраняемые помещения. Отличительной чертой таких систем является наличие в их составе обычных или видео-домофонов.

СКУД ParsecNET 3 имеет возможность интегрирования с домофонными системами, в частности, на текущий момент произведена интеграция с домофонами компании BAS-IP Ltd.

11.12.1 Система BAS-IP

Первая домофонная система, интегрированная в СКУД ParsecNET 3, - это система производства компании BAS-IP Ltd.

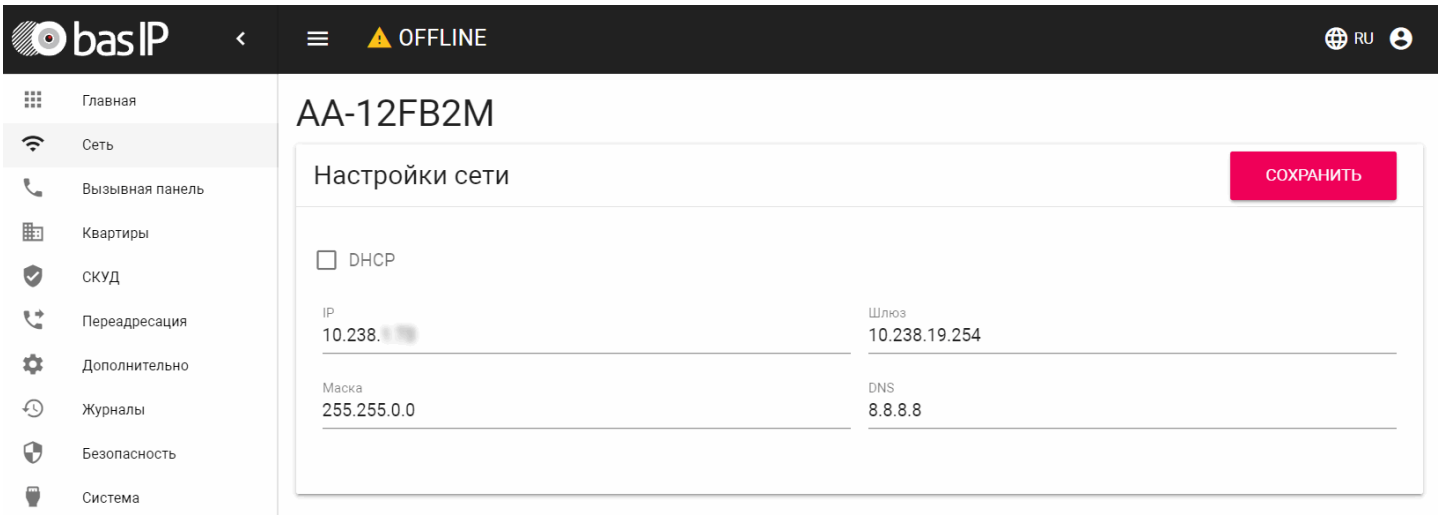
В текущей версии модуля интеграции поддерживаются панели BAS-IP, совместимые с Android Panels API 2.2.0, и имеющие функцию распознавания лиц. В частности, следующие устройства:

- av-08b
- aa-07fb
- aa-07fb2m
- aa-12fb
- aa-12fb2m
- aa-14fb
- aa-14fb2m
- aa-14fbs
- bi-02fb
- bi-04fb
- bi-06fb
- bi-08fb
- bi-12fb

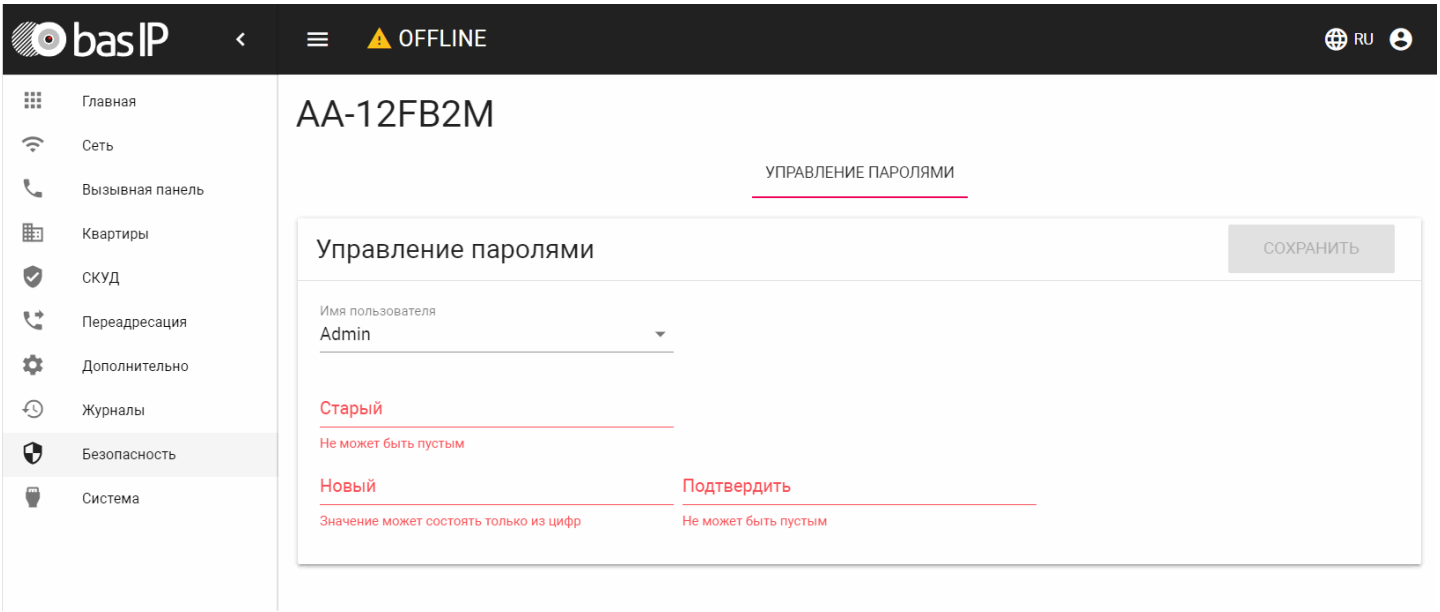
11.12.1.1 Подключение и настройка

Для настройки взаимодействия ПО ParsecNET 3 и вызывных панелей BAS-IP выполните следующие действия:

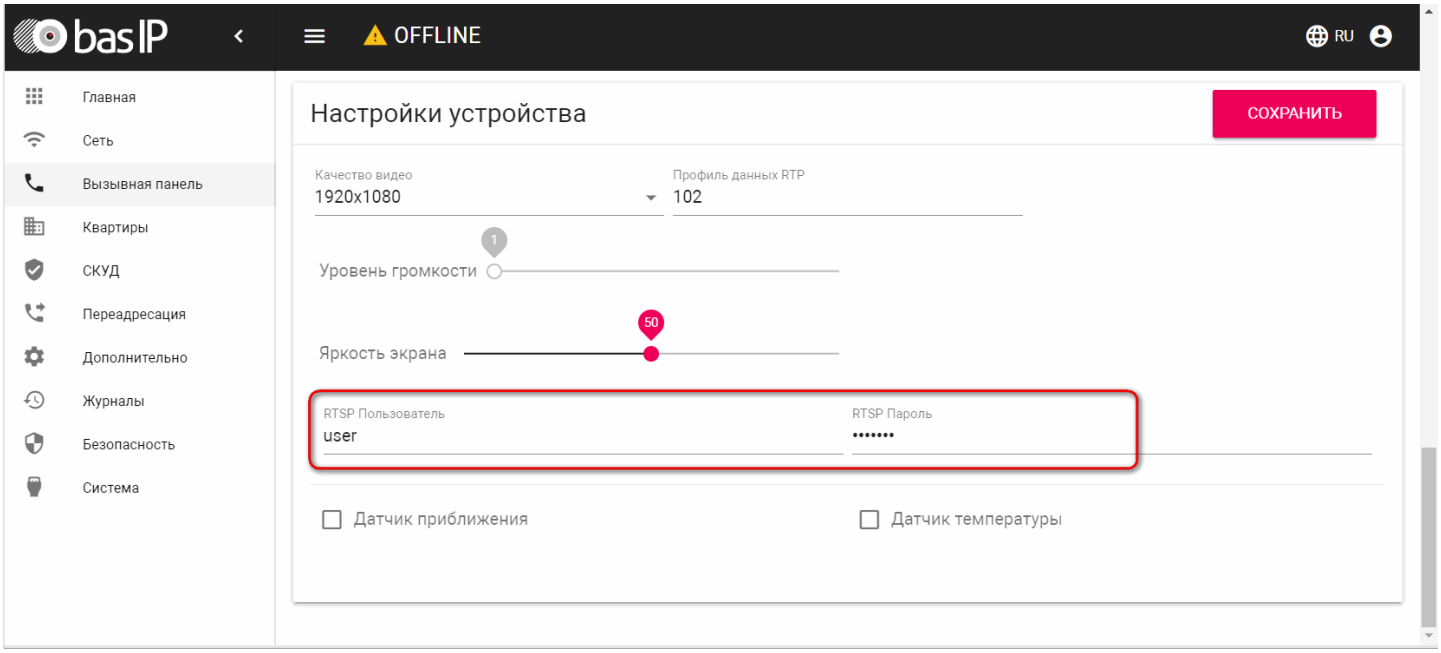
1. Установите домофон в соответствии с его Руководством по эксплуатации и подключите его к Ethernet;
2. Запустите утилиту Remote_Upgrade_Tool, доступную на официальном сайте BAS-IP.SU;
3. Узнайте текущий IP-адрес домофона и введите его в адресную строку своего браузера;
4. В окне аутентификации введите логин и пароль (по умолчанию admin/123456);
5. В открывшемся веб-интефейсе домофона задайте необходимые настройки:
   - если необходимо, в разделе *Сеть* введите новый IP-адрес, который будет назначен домофону:



   - в разделе *Безопасность* можно задать новый пароль доступа к веб-интерфейсу. **При первом входе настоятельно рекомендуется сменить пароль по умолчанию**:



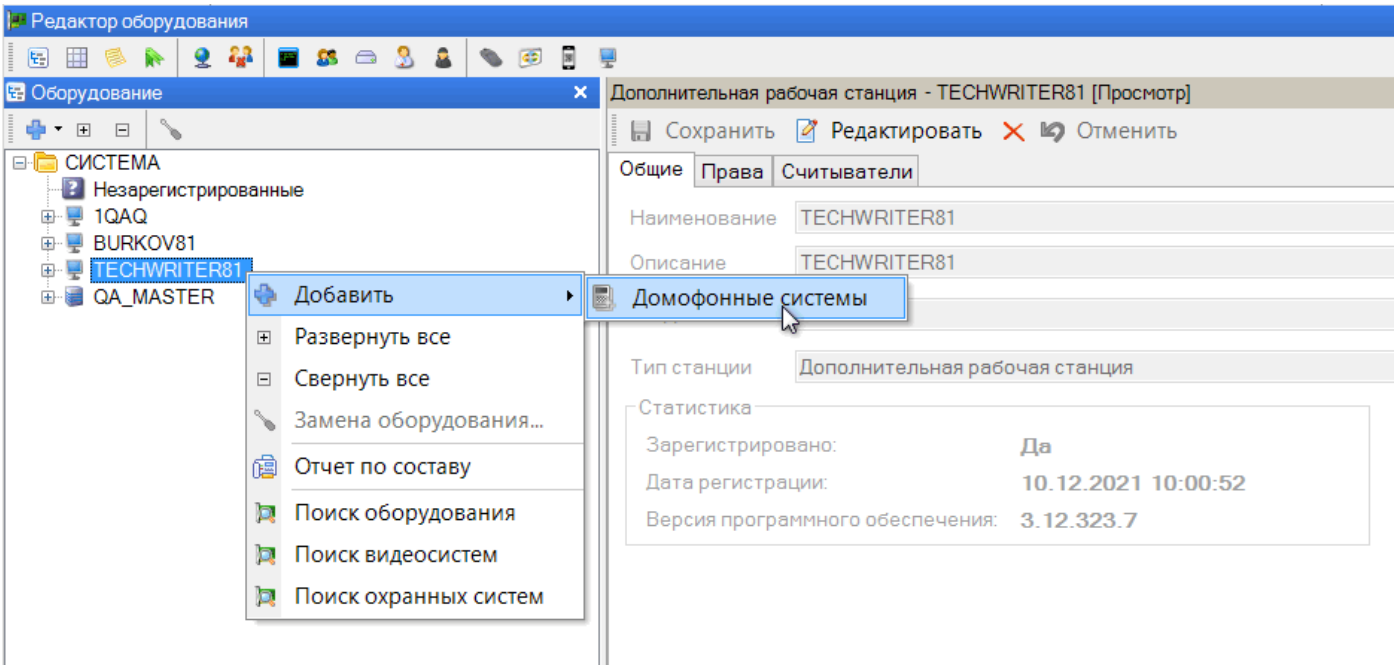
- в разделе *Вызывная панель* задайте логин и пароль для доступа к встроенной в домофон IP-камере:



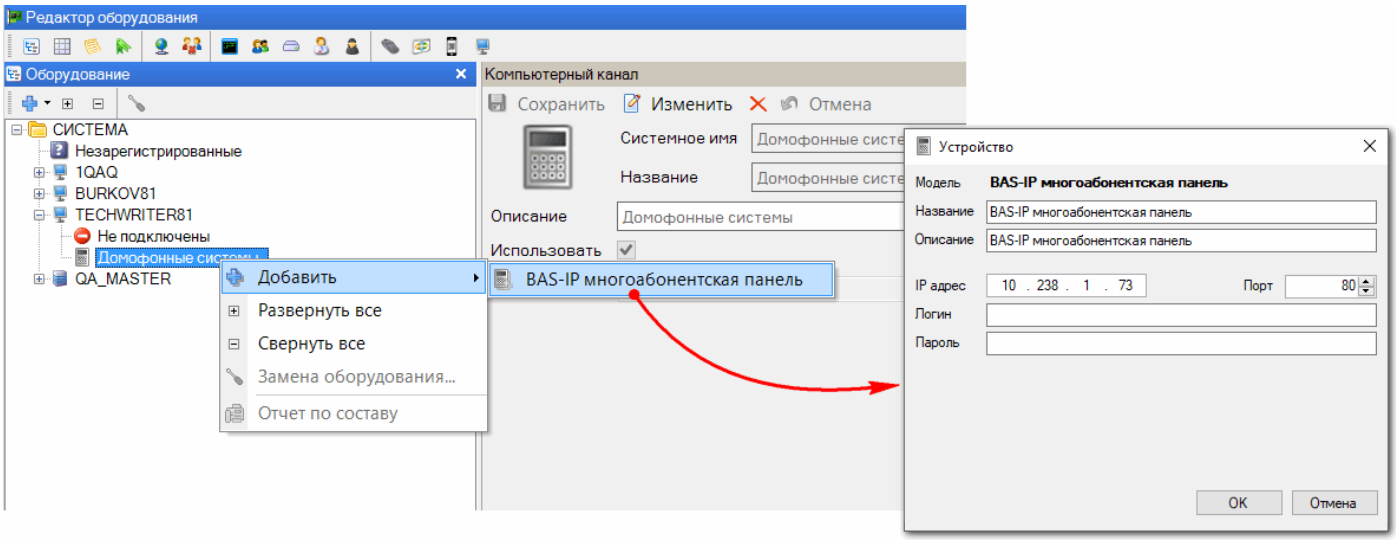
6. Задайте другие параметры, которые необходимы для работы в вашей подсети и сохраните настройки.

Теперь можно переходить к настройкам ПО ParsecNET 3:

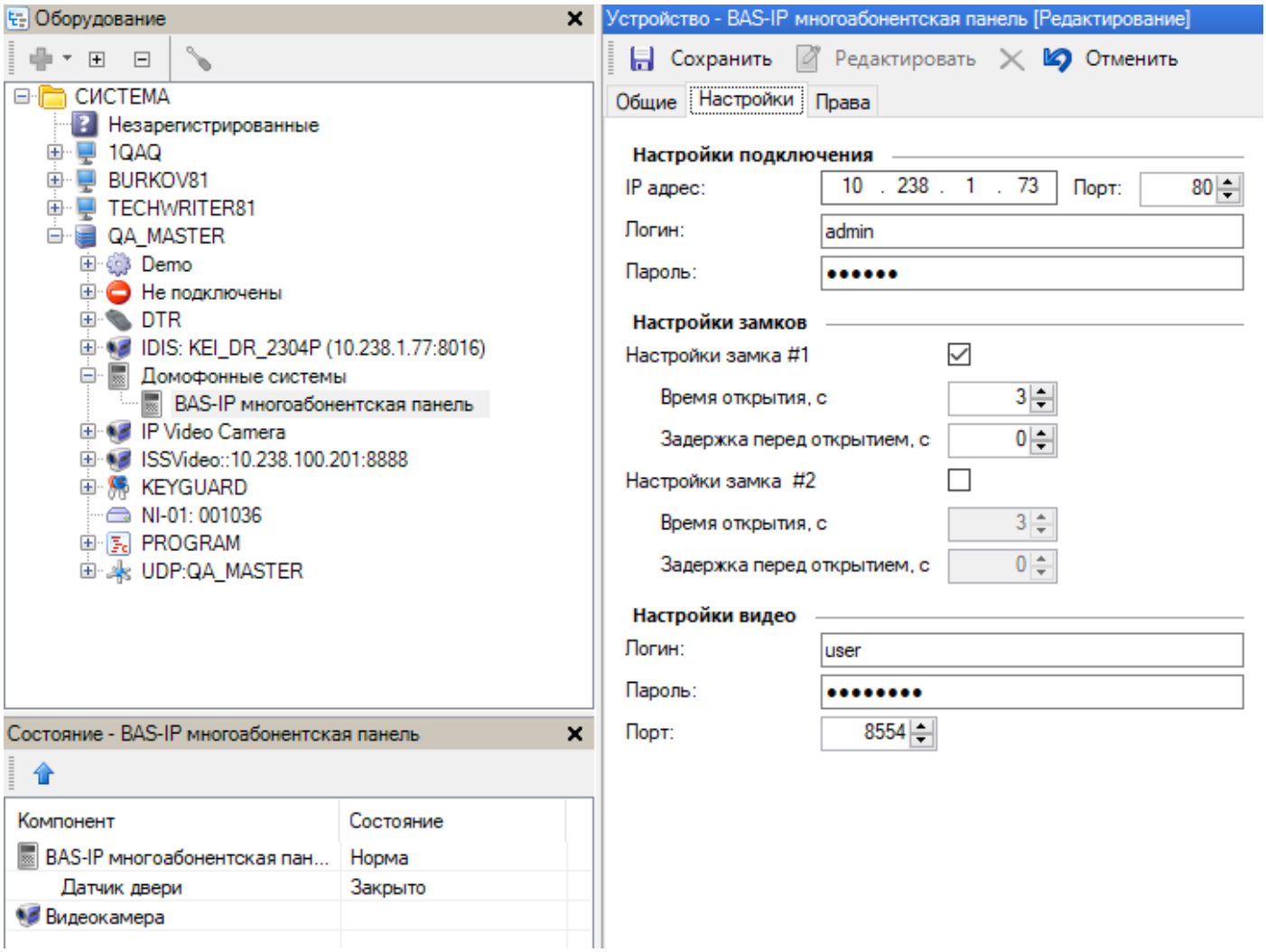
1. В Редакторе оборудования добавьте канал *Домофонные системы*:



2. Добавьте многоабонентскую панель (домофон) BAS-IP на этот канал. В окне параметров задайте нужный IP-адрес и порт, логин и пароль укажите те, которые используются для доступа к веб-интерфейсу домофона:



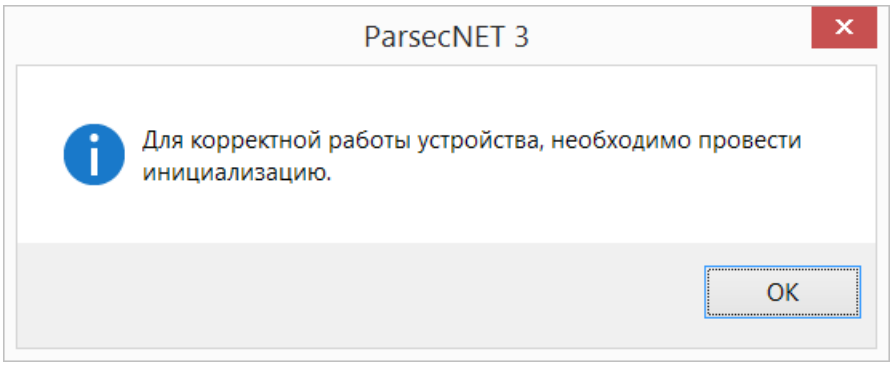
3. Перейдите в настройки домофона и задайте нужные параметры:



Настройки домофона:

- *Настройки замка #2* - установите флажок при использовании двухзамкового домофона;
- *Время открытия, с* - время в секундах, на которое будут замкнуты или разомкнуты контакты реле замка;
- *Задержка перед открытием, с* - время, по истечении которого произойдет замыкание или размыкание контактов реле замка после отправки сигнала на открытие;
- *Настройки видео* - в полях *Логин* и *Пароль* введите те логин и пароль для видеокамеры, которые были заданы в веб-интерфейсе домофона.

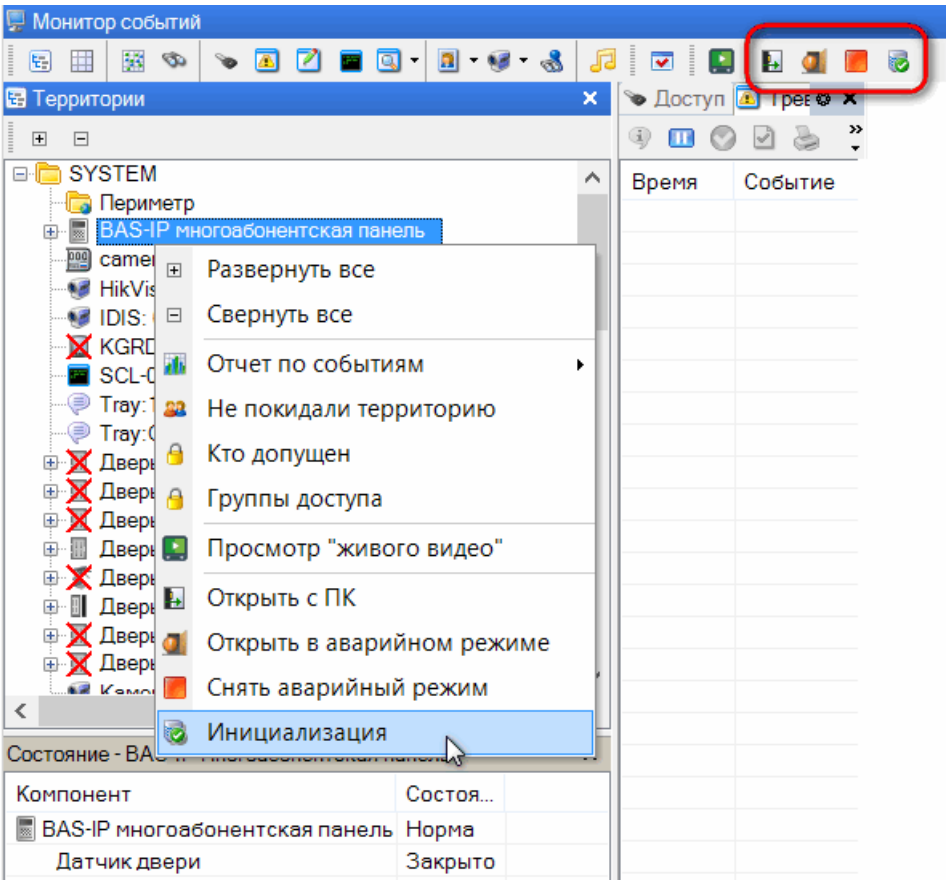
4. Сохраните сделанные настройки. Нажмите на кнопку *ОК* в появившемся системном сообщении о необходимости проведения инициализации устройства:



Такое сообщение появляется всегда при внесении изменений в настройки домофона;

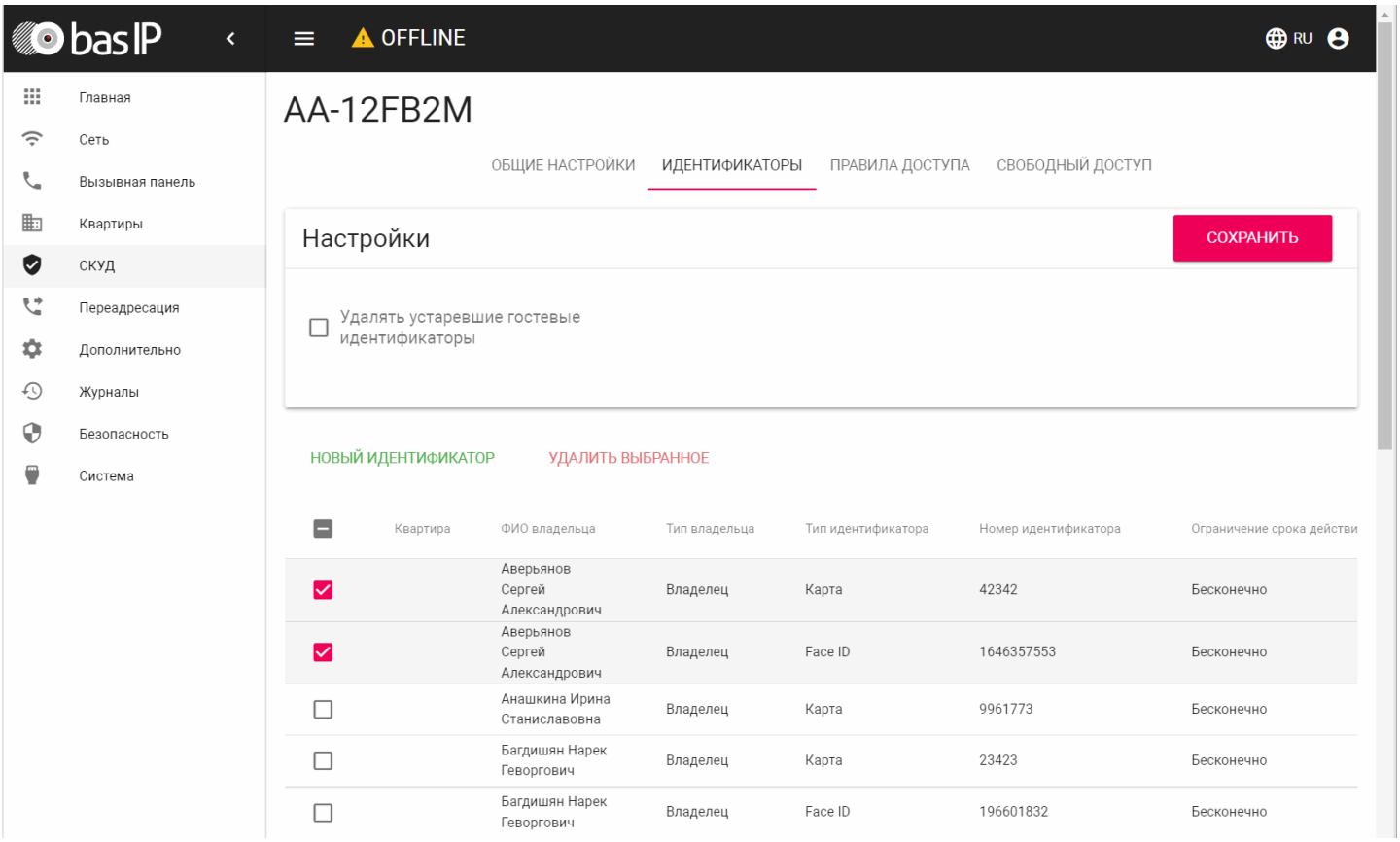
5. Для проведения инициализации выполните следующие действия:

- добавьте домофон в группу доступа. Доступ через дверь, управляемую домофоном, будет разрешен членам группы;
- в Мониторе событий выберите домофон и в контекстном меню выберите команду "Инициализация" (или выберите соответствующий значок на панели инструментов, справа от кнопок прямого управления домофоном):



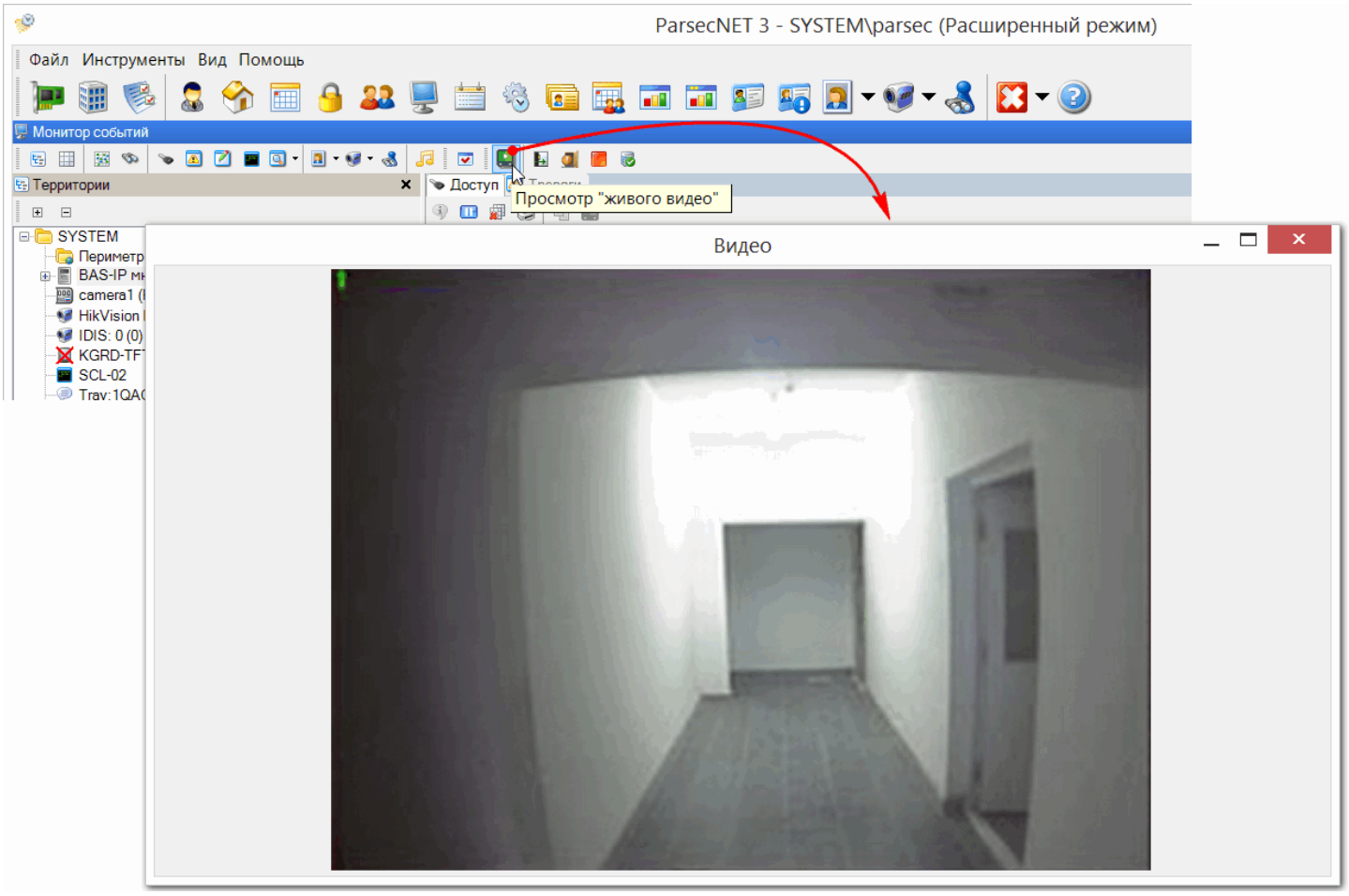
6. Дождитесь завершения инициализации.

После инициализации в веб-интерфейсе домофона в разделе *СКУД* на вкладке *Идентификаторы* отобразятся все участники группы доступа, которой назначен этот домофон, и их идентификаторы:

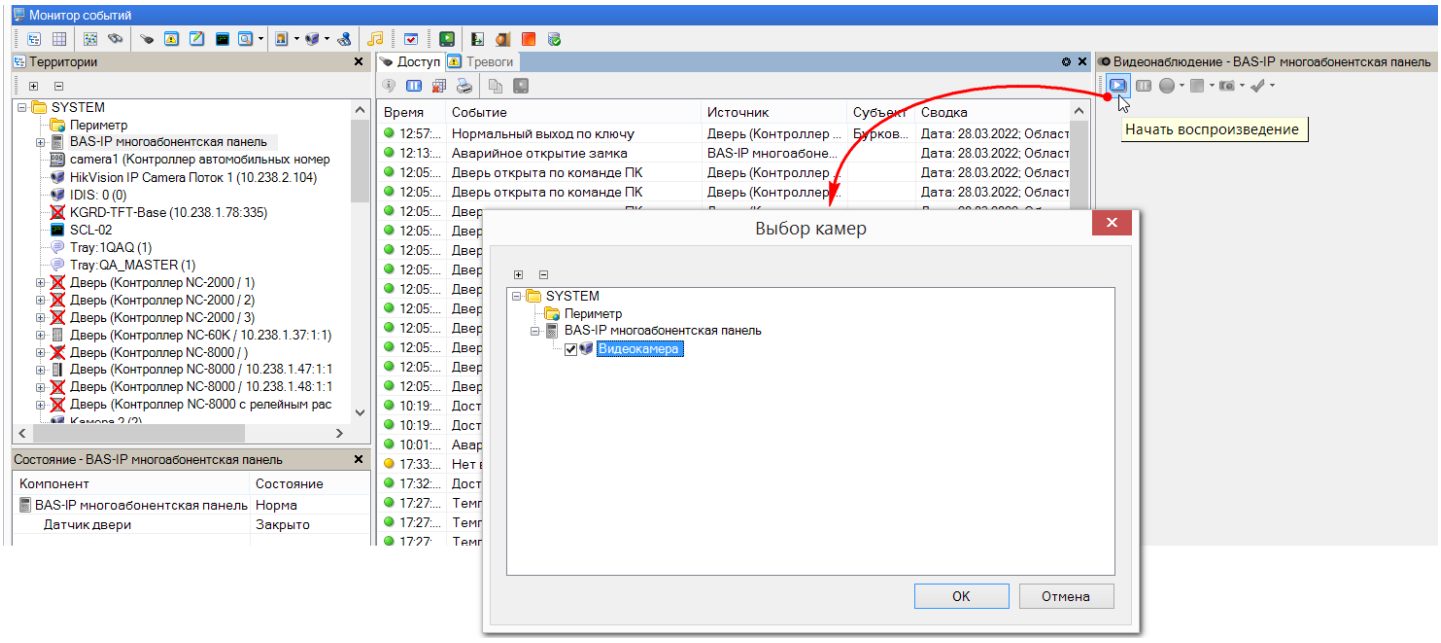


11.12.1.2 Использование системы

Изображение с веб-камеры домофона можно вывести в отдельное окно при помощи кнопки *Просмотр "живого видео"* на панели инструментов Монитора событий или одноименной командой в контекстном меню домофона либо его камеры:



Также видео можно просматривать в окне видеонаблюдения. Укажите камеру домофона:



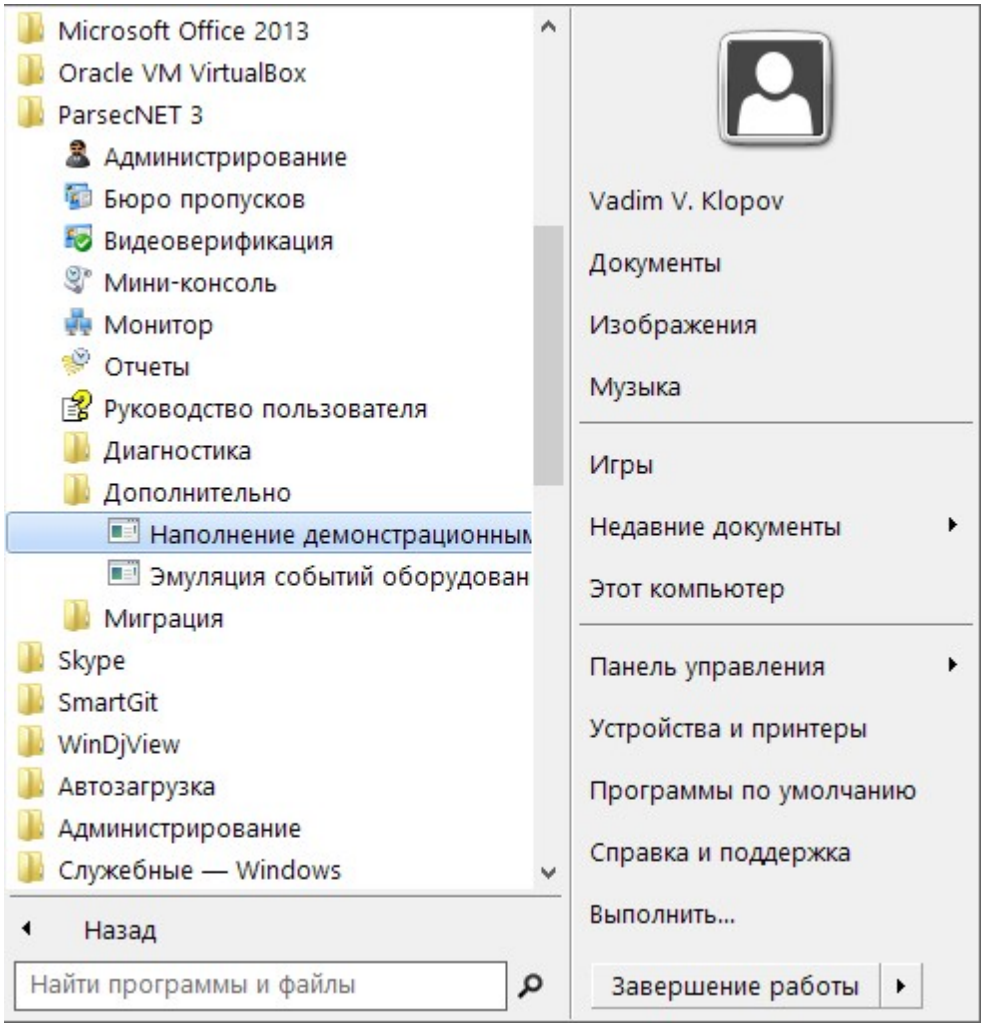
Видео используется только для просмотра в реальном времени. Архив видео не создается.

12. Демонстрационный режим

Для ознакомления с работой системы предназначен демонстрационный функционал, состоящий из двух модулей:

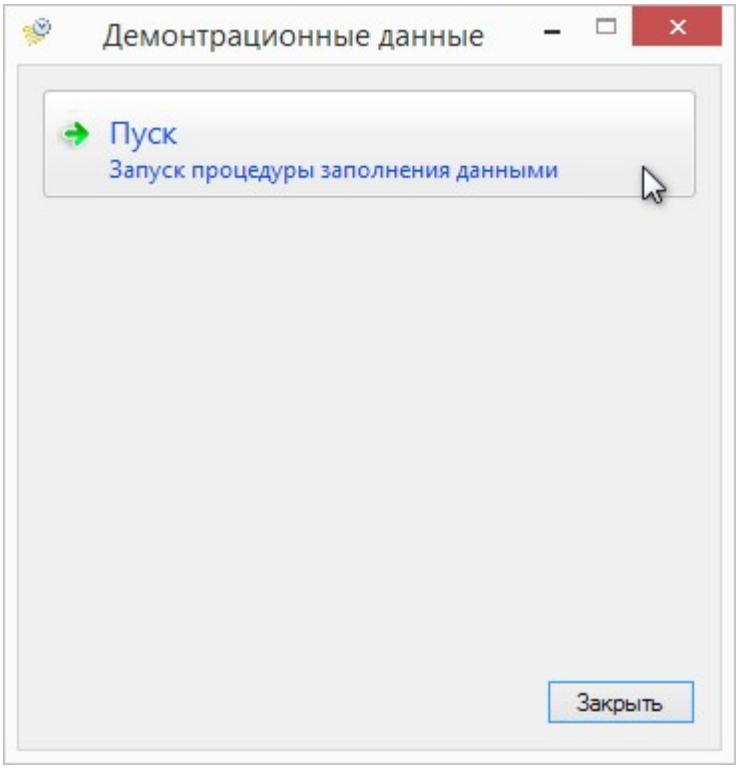
- Утилита наполнения БД[692] - создает записи об оборудовании, сотрудниках, расписаниях, группах доступа и т.п.;
- Эмулятор событий[693] - создает поток транзакций о наиболее распространенных событиях в системе.

Модули запускаются из меню "Пуск - Все программы - ParsecNET 3 - Дополнительно":

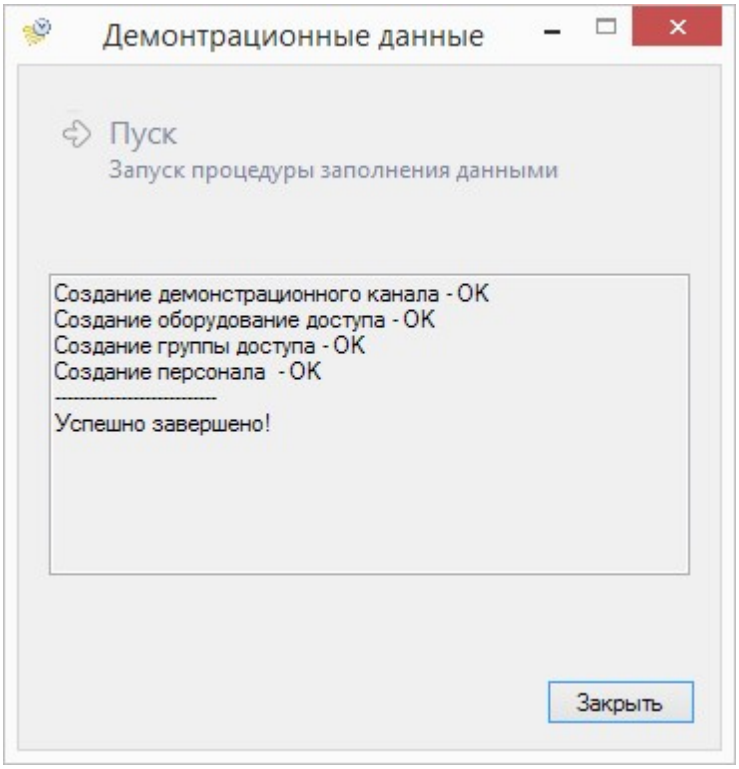


12.1 Утилита наполнения БД

Модуль демонстрационного функционала. Наполняет БД системы реальными записями об оборудовании, сотрудниках и т.д. Чтобы запустить утилиту, выберите команду "Пуск - Все программы - ParsecNET 3 - Дополнительно - Наполнение демонстрационными данными". После этого откроется окно *Демонстрационные данные*. Нажмите на кнопку *Пуск*:



Начнется процесс создания наполнения БД, об окончании которой утилита сообщит:



Нажмите на кнопку *Закрыть*.

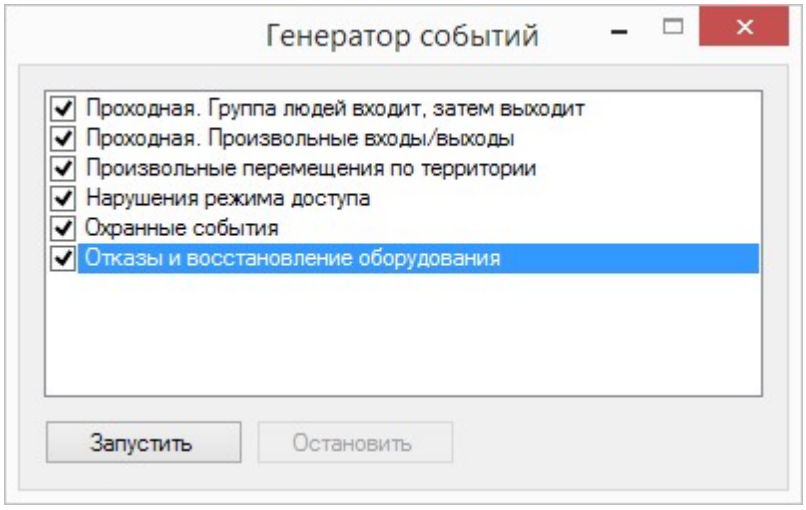
Можно переходить к эмуляции[693] событий с участием только что созданных элементов системы.

12.2 Эмулятор событий

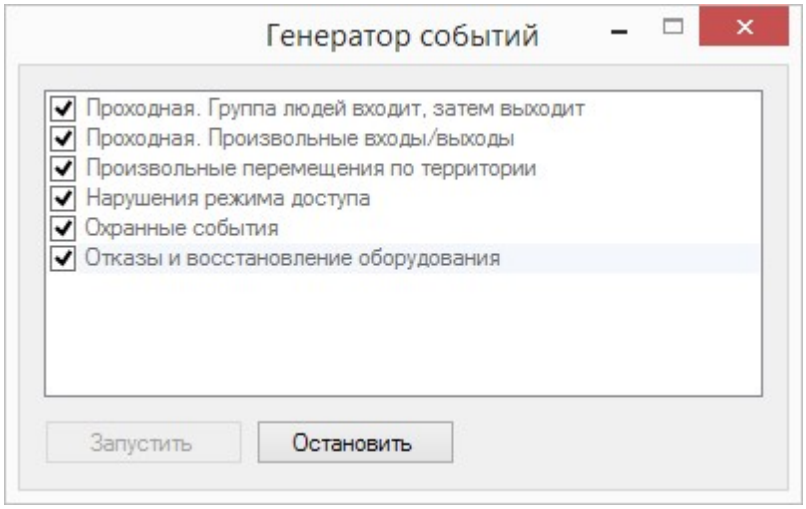
Эмулятор событий - это модуль системы, который имитирует деятельность небольшого офиса с точки зрения системы ParsecNET 3. При этом эмулируются события, связанные только с оборудованием; события с ПО ParsecNET 3 не эмулируются. Например, вход оператора в редактор персонала эмулироваться не будет.

Прежде чем запустить эмулятор, наполните[692] БД системы виртуальными данными.

Чтобы запустить утилиту, выберите команду "Пуск - Все программы - ParsecNET 3 - Дополнительно - Эмуляция событий оборудования". После запуска откроется окно выбора генерируемых событий:



Установите флажки у тех типов событий, которые нужно сгенерировать, и нажмите на кнопку *Запустить*. Утилита начнет создавать виртуальные события, которые будут отображаться системой.



Для прекращения работы утилиты нажмите на кнопку *Остановить*.
При необходимости циклы генерации можно повторять, изменяя набор типов событий.

13. Обращение в техподдержку

Если возникли проблемы, которые вы не в состоянии решить самостоятельно даже после изучения Руководства пользователя, обратитесь в Службу технической поддержки Parsec:

Тел.: +7 (495) 565-31-12 (Москва и обл.);

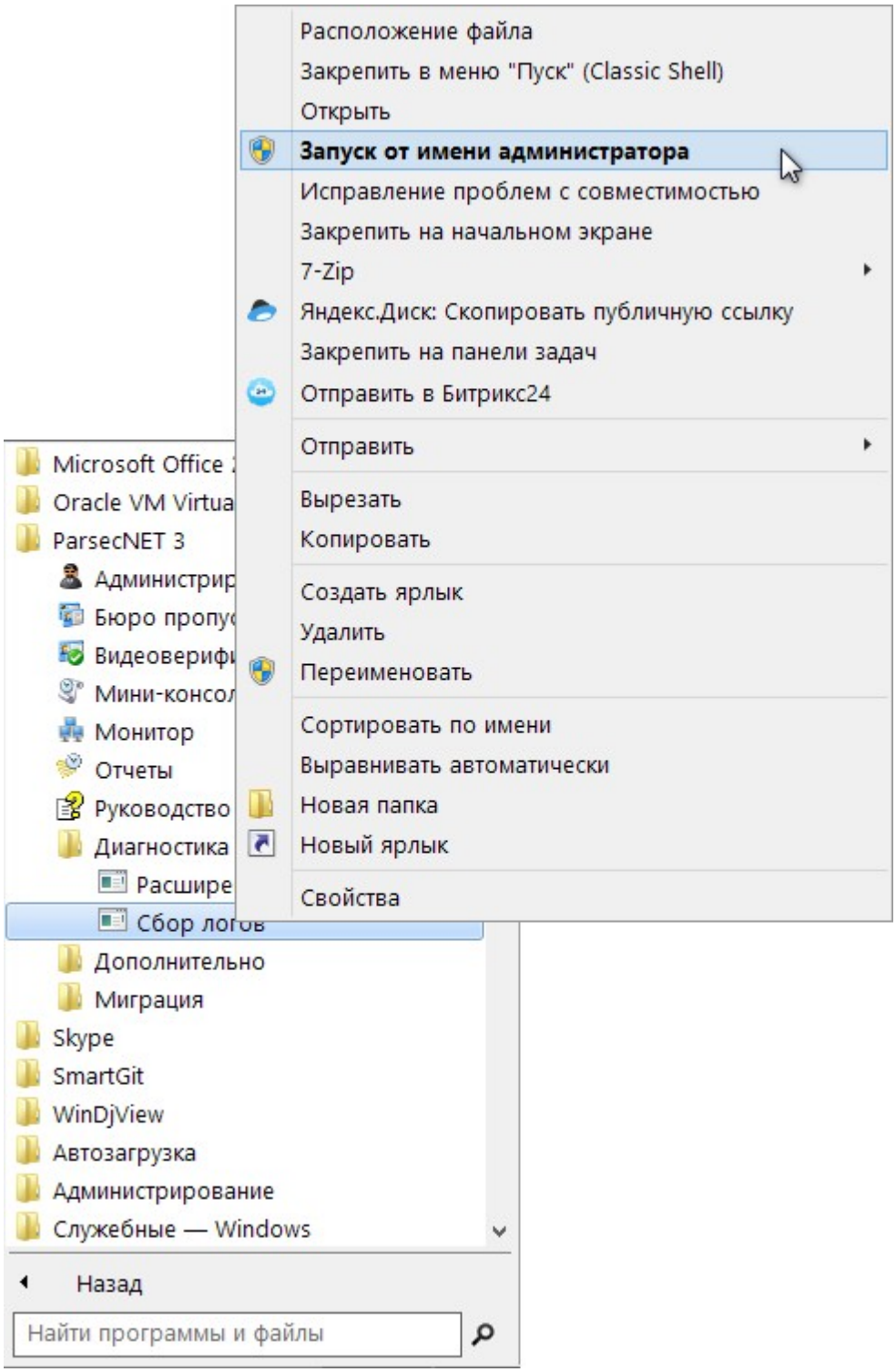
+7 (800) 333-14-98 (по России);

E-mail: support@parsec.ru;

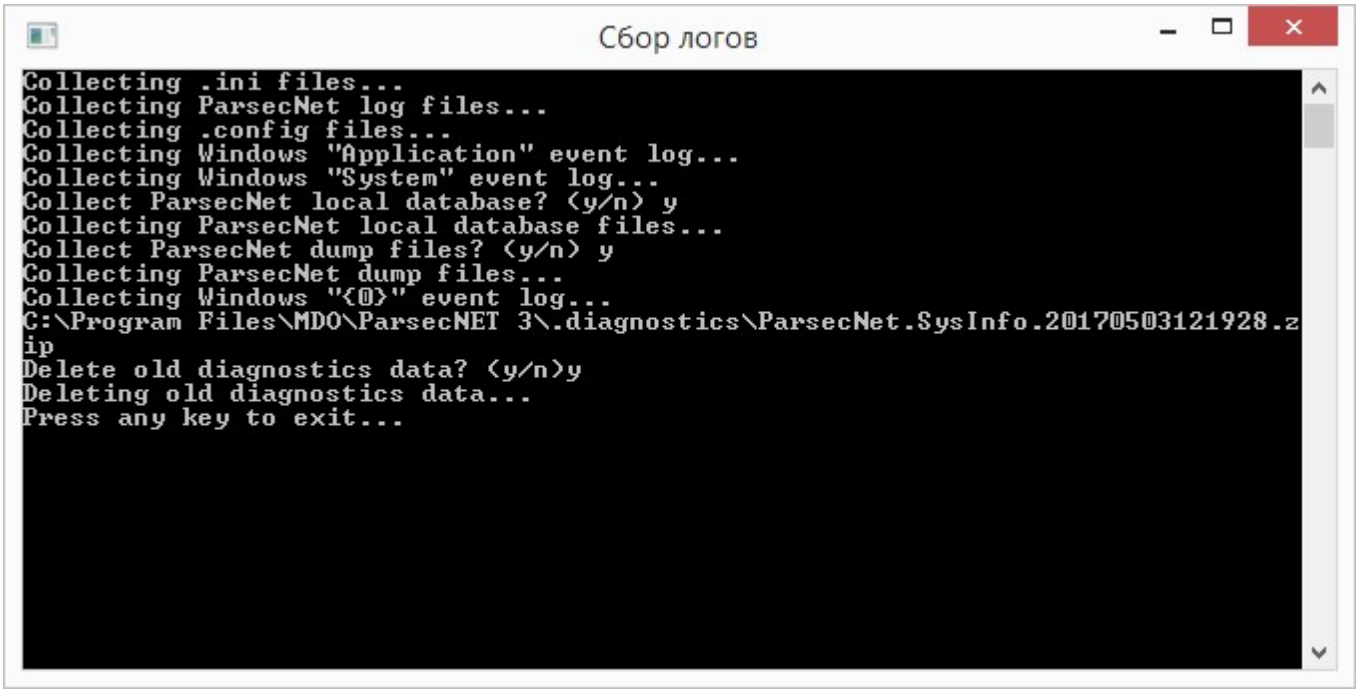
WWW: support.parsec.ru

График работы Пн.-Пт. 8:00 - 20:00 (по Московскому времени).

Оператор техподдержки может попросить Вас собрать диагностические файлы. Для этого перейдите в папку "Пуск - Все программы - ParsecNET3 - Диагностика" и запустите нужную программу от имени администратора: нажмите на строке правой клавишей мыши и выберите команду *Запуск от имени администратора*.

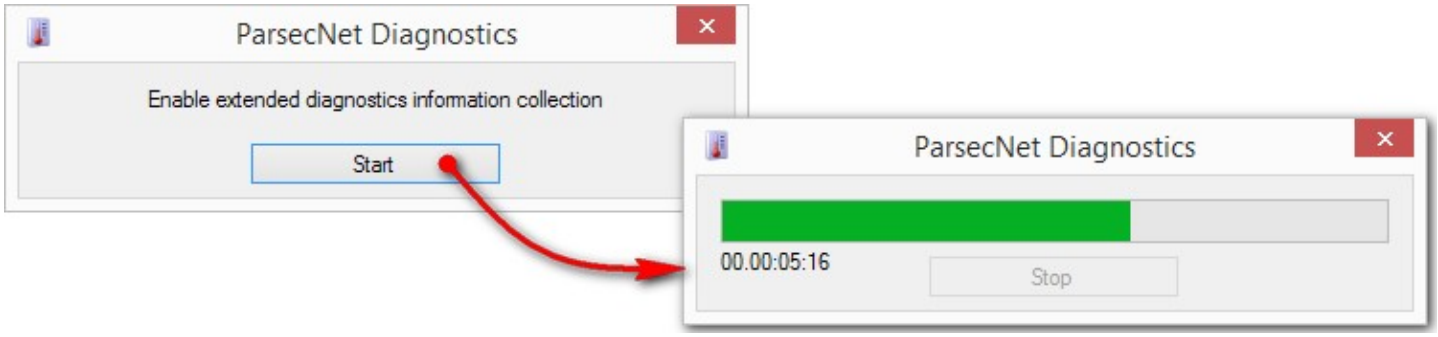


- *Сбор логов* - собирается диагностическая информация о работе системы, при запросе программы нажмите на кнопку "Y" (yes/да) или "N" (no/нет) по указанию оператора. По завершении сбора данных нажмите на любую клавишу, чтобы выйти из программы:



Файл с данными сохраняется в папке "C:\ProgramData\MDO\ParsecNET 3\.diagnostics" под именем вида "ParsecNet.SysInfo.20170503123211.zip".

- *Расширенный сбор логов* - собирается расширенная диагностическая информация. Запустите программу сбора данных, нажав на кнопку *Start*, воспроизведите проблему и завершите программу кнопкой *Stop*.



Данные будут сохранены в два архива с именами вида "ParsecNet.SysInfo.20170503123411.zip" и "ParsecNet.Logs.Old.20170503123430.zip" в паке по адресу "C:\Program Files\MDO\ParsecNET 3\.diagnostics".

14. Контроллеры

Ниже приведена сводная таблица некоторых функциональных особенностей контроллеров. Технические характеристики контроллеров см. в паспортах соответствующих устройств.

Контроллеры	NC-1000M	NC-2000-IP	NC-5000	NC-8000, NC-8000-D	NC-32K.M, NC-32K-IP	NC-60K/ NC-60K.M	NC-100K-IP	NC-100K-IP.M
Распи доступа	●	●	●	●	●	●	●	●

сания*	сменные	●	●	●	●	●	●	●	●
	дни-исключения	●	●	●	●	●	●	● (240 дней)	●
	праздничные дни (колич.)	16	16	16	32	>32	32	64	32
	временные интервалы в настройках дня**	до 4	до 4	до 4	до 4 (недельное) 4 (сменное)	до 4 (недельное) 4 (сменное)	до 4 (недельное) 4 (сменное)	до 4 (недельное) 4 (сменное)	до 4 (недельное) 4 (сменное)
Антипассбэк		●	●	●	●	●	●	●	●
Емкость памяти (колич. польз.)		1024	2000	5120	8000	32766	60000	102000	200000
Емкость буфера транзакций (события)		700	1000	3000	16000	24500	32000	53000	32000
Управление турникетом		●	●	●	●	●	●	●	●
Управление картоприемником		●	●	●	●	●	●	●	●
Управление шлюзом		-	-	-	●	●	●	●	●
Алкотестер					●	●	●	●	●
Комментарий					Можно подключить до 4 считывателей		Можно подключить до 8 считывателей по шине OSDP (4 на вход и 4 на выход), считыватель картоприемника по интерфейсу Wiegand, а также до 7 устройств через преобразователь Wiegand-OSDP (OMP-W02)	Может управлять одновременно турникетом и картоприемником (одновременно можно подключить 3 считывателя: вход, выход, картоприемник).	Можно подключить: - до 8 считывателей по шине OSDP (4 на вход и 4 на выход); - считыватель картоприемника по интерфейсу Wiegand; - до 7 устройств через преобразователь Wiegand-OSDP (OMP-W02); - 2 считывателя по интерфейсу Parsec.

Таким фоном выделены снятые с производства модели

*Общее количество расписаний в контроллере зависит от модели (63 ячейки у 100K и 15 у остальных) и от содержимого - расписание занимает 1 или 2 ячейки в зависимости от количества разных рабочих дней в текущем цикле. Для контроллера 32K доступно создание 256 расписаний, т.е. можно создать свое расписание практически на каждый день года.

**Использование более двух интервалов в день для недельных расписаний доступа у "младших" контроллеров может привести к уменьшению количества доступных шаблонов настройки дня. Как и в расписаниях рабочего времени это ограничение накладывают возможности используемых контроллеров.

Подробности создания праздников[238] и дней-исключений[241] изложены в соответствующих разделах.

15. Список транзакций

При возникновении того или иного события система генерирует сообщение. Список сообщений приведен в таблице ниже:

Сообщение	Описание
Контроллеры доступа серии NC	
Взлом двери	Если установлена опция «Взлом не на охране», то данное событие будет возникать и при несанкционированном открывании двери, не поставленной на охрану.
Дверь после взлома закрыта	Закрыта дверь, открытая несанкционированным способом (ранее было событие "Взлом двери").
Взлом считывателя	Нарушение связи между контроллером и считывателем (взлом, нарушение линии связи, неисправность считывателя).
Считыватель восстановлен	Восстановление ранее нарушенной связи между контроллером и считывателем.
Взлом внутреннего считывателя	Нарушение связи между контроллером и внутренним считывателем (взлом, нарушение линии связи, неисправность считывателя).
Внутренний считыватель восстановлен	Восстановление ранее нарушенной связи между контроллером и внутренним считывателем.
Аварийное открывание двери	Дверь открыта в связи с подачей сигнала на вход контроллера Emergency.
Аварийное открывание сброшено	Дверь закрыта, в связи с прекращением сигнала на входе контроллера Emergency.
Невозможно поставить на охрану	Невозможно поставить защищаемое помещение на охрану по одной из причин: дверь не закрыта (для определения этого состояния должен быть установлен дверной контакт); на данный момент активирован вход тревоги (сработал охранный датчик).
Обрыв датчика двери	Обрыв шлейфа дверного контакта. Данное событие может возникнуть только при подключении дверного контакта по схеме с возможностью контроля 4-х состояний и включенной опцией «DC с 4 состояниями» в настройках параметров контроллера. Не относится к контроллерам серии NC-32K.
КЗ цепи датчика двери	Короткое замыкание в линии дверного контакта. Данное событие может возникнуть только при подключении дверного контакта с возможностью контроля 4-х состояний и включенной опцией «DC с 4 состояниями» в настройках контроллера. Не относится к контроллерам серии NC-32K.
Датчик двери восстановлен	Восстановлено нормальное состояние шлейфа дверного контакта после обрыва или короткого замыкания. Не относится к контроллерам серии NC-32K.

Обрыв охранного датчика	Обрыв шлейфа охранного датчика. Данное событие может возникнуть только при подключении охранного датчика по схеме с возможностью контроля 4-х состояний и включенной опцией «Шлейф датчика с 4 состояниями» в настройках параметров контроллера.
КЗ цепи охранного датчика	Короткое замыкание в линии охранного датчика. Данное событие может возникнуть только при подключении охранного датчика по схеме с возможностью контроля 4-х состояний и включенной опцией «Шлейф датчика с 4 состояниями» в настройках параметров контроллера.
Шлейф охраны восстановлен	Восстановлено нормальное состояние шлейфа охранного датчика после обрыва или короткого замыкания
Начало быстрой загрузки пользователей	Начало загрузки контроллера (инициализация).
Конец быстрой загрузки пользователей	Окончание загрузки контроллера (инициализация).
Снята тревога с ПК	Охранно-пожарная тревога с компьютера снята оператором.
Дверь оставлена открытой	Фактически открытая дверь не была закрыта до окончания времени двери. Данное событие может возникнуть только при наличии дверного контакта, позволяющего определить состояние двери. Если для данной двери в настройках Двери в ПО установлен флажок «Звук открытой двери», то вместе с появлением этой транзакции считыватели начнут издавать сигнал, извещающий о том, что дверь оставлена открытой.
Незакрытая дверь закрыта	Закрыта дверь, ранее оставленная открытой (ранее было событие "Дверь оставлена открытой")
Выключен сигнал незакрытой двери	К считывателю поднесен ключ, имеющий привилегию отключения звука открытой двери. При этом звуковой сигнал на считывателе выключается.
Снята абсолютная блокировка ключом	При переходе контроллера в режим Off-Line с включенной абсолютной блокировкой, к считывателю поднесен ключ, имеющий привилегию управления охраной. В данной ситуации такой ключ имеет право отключить абсолютную блокировку. Это функция введена для того, чтобы при переходе контроллера в режим Off-Line дать возможность снять полную блокировку двери.
Тревога "Спящий человек"	В помещении, в которое вошел сотрудник, отсутствует движение в течении заданного времени (отслеживается датчиками).
Турникет занят	Контроллеру, работающему в турникетном режиме, и находящемуся на данный момент в открытом состоянии на вход или на выход, отправлена команда открытия турникета. Турникетный режим поддерживают контроллеры NC-1000 / NC-5000 версий NC1K07 / NC5K06 и выше соответственно, а также NC-8000, NC-32K и NC-100K-IP.
Нормальный вход по ключу	К внешнему считывателю поднесен ключ, имеющий доступ в данную дверь.
Нормальный выход по ключу	К внутреннему считывателю поднесен ключ, имеющий доступ в данную дверь.
Запрос на вход (при фактическом проходе)	Возникает при включенной опции фактического прохода, когда к наружному считывателю поднесен ключ, имеющий доступ в данную дверь.
Запрос на выход (при фактическом проходе)	Возникает при включенной опции фактического прохода, когда к внутреннему считывателю поднесен ключ, имеющий доступ в данную дверь.
Запрос на проход (при фактическом проходе)	Возникает при включенной опции фактического прохода, когда к считывателю поднесен ключ, имеющий доступ в данную дверь. Транзакция генерируется, если используются контроллеры, не умеющие определять направление прохода.

Фактический вход	Осуществлен фактический авторизованный вход, т.е. к внешнему считывателю был поднесен ключ, имеющий доступ через данную точку прохода, после чего фактически открыта дверь или провернут турникет (сработал дверной контакт). Данное событие может возникнуть только при наличии дверного контакта, позволяющего определить открывание двери, и при установленном в настройках контроллера флажке «Фактический проход».
Фактический выход	Осуществлен фактический авторизованный вход, т.е. к внутреннему считывателю был поднесен ключ, имеющий доступ через данную точку прохода, после чего фактически открыта дверь или провернут турникет (сработал дверной контакт). Данное событие может возникнуть только при наличии дверного контакта, позволяющего определить открывание двери, и при установленном в настройках контроллера флажке «Фактический проход».
Фактический вход не совершен	Для NC-8000. антипасс.
Фактический выход не совершен	Для NC-8000. События формируются контроллерами с прошивкой версии 3.5 и выше в режиме фактического прохода, если после события «Запрос на фактический выход» за отведенное время (время замка либо 5 секунд, если время замка равно 0) проход не был совершён (не сработал дверной контакт или датчик проворота турникета).
Фактический выход по кнопке DRTE	Осуществлен фактический выход по нажатию кнопки DRTE, после чего фактически открыта дверь (сработал дверной контакт). Данное событие может возникнуть только при наличии дверного контакта, позволяющего определить открывание двери, и при установленном в настройках контроллера флажке «Фактический проход».
Фактический вход по кнопке DRTE	Событие генерируются в турникетном режиме контроллерами NC-8000, NC-100K-IP. Осуществлен фактический вход с открыванием турникета по нажатию кнопки DRTE (разблокировано реле турникета на вход), провернут турникет (сработало реле проворота). Данное событие может возникнуть только при наличии датчика проворота, позволяющего определить проворот, и при установленном в настройках контроллера флажке «Фактический проход».
Фактический выход по кнопке RTE	Событие генерируются в турникетном режиме контроллерами NC-8000, NC-100K-IP. Осуществлен фактический выход с открыванием двери по нажатию кнопки RTE (разблокировано реле турникета на выход), после чего фактически провернут турникет (сработало реле проворота). Данное событие может возникнуть только при наличии датчика проворота, позволяющего определить проворот, и при установленном в настройках контроллера флажке «Фактический проход».
Выход по дистанционной кнопке	Дверь открыта нажатием дистанционной кнопки DTRE (например, с рабочего места секретаря или охранника). При этом флажок «Фактический проход» в настройках контроллера не установлен.
Открывание двери по RTE	Дверь открыта нажатием кнопки RTE. При этом флажок «Фактический проход» в настройках контроллера не установлен.
Турникет открыт на вход по кнопке DRTE	Турникет открыт на вход нажатием на кнопку DRTE. При этом флажок «Фактический проход» в настройках контроллера не установлен.
Турникет открыт на выход по кнопке RTE	Турникет открыт на выход нажатием на кнопку RTE. При этом флажок «Фактический проход» в настройках контроллера не установлен.
Турникет открыт на вход по команде ПК	Турникет открыт на вход с ПК.
Турникет открыт на выход по команде ПК	Турникет открыт на выход с ПК.

Турникет закрыт по команде ПК	Турникет закрыт с ПК.
Дверь открыта по команде ПК	Дверь открыта по команде, поступившей с ПК. Если для данной двери установлена опция автозакрывания, то дверь будет автоматически закрыта по истечении времени замка. Если опция автозакрывания не установлена, то дверь будет закрыта соответствующей командой с ПК, либо если контроллер по причине отсутствия связи с ПК перейдет в режим Off-Line.
Дверь закрыта по команде с ПК	Дверь закрыта по команде, поступившей с ПК (автоматически при установленном в настройках контроллера флажке "Автозакрывание двери", либо по команде оператора).
Дверь открыта по временному профилю	Дверь открыта по расписанию (используется стандартное расписание доступа).
Дверь закрыта по временному профилю	Дверь закрыта по расписанию (используется стандартное расписание доступа).
Область поставлена на охрану по временному профилю	Только для NC-8000. Охранная область поставлена на охрану по расписанию (используется стандартное расписание доступа).
Область снята с охраны по временному профилю	Только для NC-8000. Охранная область снята с охраны по расписанию (используется стандартное расписание доступа).
Дверь закрыта по Off-Line	Дверь, открытая с ПК, закрыта в связи с переходом контроллера в режим Off-Line. Дверь закрывается не сразу, а через 20 секунд после перехода.
Включение реле по ВП	Зарезервировано на будущее.
Выключение реле по ВП	Зарезервировано на будущее.
Выключен звук тампера корпуса	Звук сработавшего тампера корпуса отключён поднесением к считывателю карты с привилегией «Управление охраной».
Вход - первый идентификатор предъявлен	При групповом проходе к внешнему считывателю поднесена первая карта.
Выход - первый идентификатор предъявлен	При групповом проходе к внутреннему считывателю поднесена первая карта.
Вход - второй идентификатор предъявлен	При групповом проходе к внешнему считывателю поднесена вторая карта.
Выход - второй идентификатор предъявлен	При групповом проходе к внутреннему считывателю поднесена вторая карта.
Выход запрещен - гостевая карта	Данная транзакция возникает при работе контроллера серии NC-32K/NC-32K-IP в режиме «Запрет выхода посетителей» и поднесении гостевой карты на выход.
Нет доступа по блокировке	К считывателю поднесен ключ, имеющий доступ в данную дверь, но в данный момент включена блокировка двери. Если включена относительная блокировка, а ключ имеет привилегию прохода при блокировке, то доступ через данную дверь будет разрешен и это событие не возникнет. Направление прохода не определяется.
Нет входа - режим блокировки	К внешнему считывателю поднесен ключ, имеющий доступ в данную дверь, но в данный момент включена блокировка двери. Если включена относительная блокировка, а ключ имеет привилегию прохода при блокировке, то доступ через данную дверь будет разрешен и это событие не возникнет.

Нет выхода - режим блокировки	К внутреннему считывателю поднесен ключ, имеющий доступ в данную дверь, но в данный момент включена блокировка двери. Если включена относительная блокировка, а ключ имеет привилегию прохода при блокировке, то доступ через данную дверь будет разрешен и это событие не возникнет.
Нет ключа в БД устройства	К внешнему считывателю поднесен ключ, не занесенный в базу данных контроллера, и не имеющий соответственно доступа в данную дверь. Это может быть как ключ, не занесенный в систему, так и ключ какого-либо пользователя системы, но имеющего группу доступа, не позволяющую ему проходить через эту дверь (и поэтому не занесенного в БД именно этого контроллера). Направление прохода не определяется.
Нет входа - идентификатора нет в БД	К внешнему считывателю поднесен ключ, не занесенный в базу данных контроллера, и не имеющий соответственно доступа в данную дверь. Это может быть как ключ, не занесенный в систему, так и ключ какого-либо пользователя системы, но имеющего группу доступа, не позволяющую ему проходить через эту дверь (и поэтому не занесенного в БД именно этого контроллера). Также при распознании лица внешней СРЛ.
Нет выхода - идентификатора нет в БД	К внутреннему считывателю поднесен ключ, не занесенный в базу данных контроллера, и не имеющий соответственно доступа в данную дверь. Это может быть как ключ, не занесенный в систему, так и ключ какого-либо пользователя системы, но имеющего группу доступа, не позволяющую ему проходить через эту дверь (и поэтому не занесенного в БД именно этого контроллера). Также при распознании лица внешней СРЛ.
Нет входа - неизвестный	Запрет при попытке входа пользователя, лицо которого отсутствует БД системы.
Нет выхода - неизвестный	Запрет при попытке выхода пользователя, лицо которого отсутствует БД системы.
Нет доступа - режим охраны	Дверь находится на охране, а к считывателю поднесен ключ, имеющий доступ в данную дверь, но не имеющий привилегий снятия (управления) с охраны. Направление прохода не определяется.
Нет входа - режим охраны	Дверь находится на охране, а к внешнему считывателю поднесен ключ, имеющий доступ в данную дверь, но не имеющий привилегий снятия (управления) с охраны.
Нет выхода - режим охраны	Дверь находится на охране, а к внутреннему считывателю поднесен ключ, имеющий доступ в данную дверь, но не имеющий привилегий снятия (управления) с охраны.
Нет входа - антипассбэк	Попытка повторного входа при включенном режиме антипассбэка и отсутствии у пользователя привилегии повторного прохода при антипассбэке.
Нет выхода - антипассбэк	Попытка повторного выхода при включенном режиме антипассбэка и отсутствии у пользователя привилегии повторного прохода при антипассбэке.
Нет доступа временной профиль	К считывателю поднесен ключ, имеющий группу доступа с временным профилем, запрещающим доступ в данную дверь в данный момент времени.
Нет входа по временному профилю	Вход ограничен по времени расписанием доступа. Была произведена попытка входа в интервал времени, когда проход запрещён.
Нет выхода по временному профилю	В настройках контроллера NC-100K-IP или NC-8000установлен флажок "Запрет выхода вне расписания". Была произведена попытка выхода в интервал времени, когда проход запрещён.
Выход вне временного профиля	В настройках контроллера NC-100K-IP или NC-8000 не установлен флажок "Запрет выхода вне расписания". Был произведен выход и сгенерировано данное событие. В других контроллерах выход вне расписания разрешен всегда с генерацией данного события.

Нет входа - не выполнены правила для двух идентификаторов	Вход при групповом проходе запрещен по одной из двух причин: вторая карта не приложена к считывателю в течение заданного времени либо вторая карта не входит в одну из групп группового прохода.
Нет выхода - не выполнены правила для двух идентификаторов	Выход при групповом проходе запрещен по одной из двух причин: вторая карта не приложена к считывателю в течение заданного времени либо вторая карта не входит в одну из групп группового прохода.
Вход по двум идентификаторам	Осуществлен корректный вход при групповом проходе.
Выход по двум идентификаторам	Осуществлен корректный выход при групповом проходе.
Нет доступа под принуждением - блокировка	К клавиатурному считывателю поднесен ключ, имеющий доступ в данную дверь, и набран код принуждения, но в данный момент включена блокировка двери. Если включена относительная блокировка, а ключ имеет привилегию прохода при блокировке, то доступ через данную дверь будет разрешен с генерацией события о принуждении, но данное событие не возникнет. Направление прохода не определяется.
Нет доступа под принуждением - режим охраны	Дверь с клавиатурным считывателем находится на охране. К поднесен ключ, имеющий доступ в данную дверь, но не имеющий привилегий снятия (управления) с охраны, и набран код принуждения. Направление прохода не определяется.
Нет доступа под принуждением - временной профиль	К клавиатурному считывателю поднесен ключ, имеющий группу доступа с временным профилем, запрещающим доступ в данную дверь в данный момент времени, и набран код принуждения.
Нет входа под принуждением - антипассбэк	Попытка повторного входа с набором кода принуждения при включенном режиме антипассбэка и отсутствии у пользователя привилегии повторного прохода при антипассбэке.
Нет выхода под принуждением - антипассбэк	Попытка повторного выхода с набором кода принуждения при включенном режиме антипассбэка и отсутствии у пользователя привилегии повторного прохода при антипассбэке.
Снята абсолютная блокировка под принуждением	При переходе контроллера с включенной абсолютной блокировкой в режим Off-Line, к клавиатурному считывателю поднесен ключ, имеющий привилегию управления охраной, и набран код принуждения. В данной ситуации такой ключ имеет право отключить абсолютную блокировку. Это функция введена для того, чтобы при переходе контроллера в режим Off-Line дать возможность снять полную блокировку двери.
Вход под принуждением	Осуществлен вход в помещение с набором кода принуждения.
Выход под принуждением	Осуществлен выход из помещения с набором кода принуждения.
Выход вне временного профиля под принуждением	В настройках контроллера NC-100K-IP или NC-8000 не установлен флажок "Запрет выхода вне расписания". Был произведен выход с набором кода принуждения.
Фактический вход под принуждением	Осуществлен фактический вход в помещение с набором кода принуждения.
Фактический выход под принуждением	Осуществлен фактический выход из помещения с набором кода принуждения.
Канал поставлен на охрану под принуждением	Охранная область взята на охрану с набором кода принуждения.
Канал снят с охраны под принуждением	Охранная область снята с охраны с набором кода принуждения.
Нет доступа под принуждением	К клавиатурному считывателю поднесен ключ, не имеющий права прохода черех эту точку прохода, и набран код принуждения.

Запрос на проход под принуждением (при фактическом проходе)	Возникает при включенной опции фактического прохода, когда к клавиатурному считывателю поднесен ключ, имеющий доступ в данную дверь, и набран код принуждения. Направление прохода не определяется.
Отладка	Системное событие, используется в отладочном режиме
Карта сдана в картоприемник	Событие свидетельствующее о том, что карта сдана в картоприёмник, данная опция доступна только на контроллерах NC-32K и NC-100K-IP.
Антипассбэк сброшен	Удалены все настройки режима антипассбэк для всех пользователей.
Удалена временная карта	Данное событие появляется при установленном в свойствах контроллера NC-100K-IP флажке "Удалять карты при выходе через картоприёмник" при заборе временный карты картоприёмником.
Нет выхода - привилегии	Субъект доступа с картой, имеющей привилегию "Гостевая карта" пытается выйти не с использованием картоприемника, а с использованием внутреннего считывателя.
Нет входа - вне срока действия идентификатора	Попытка выхода по временной карте до начала или после истечения ее периода действия. Транзакция только для NC-100K-IP, остальные контроллеры передадут сообщение "Нет ключа в БД устройства".
Нет выхода - вне срока действия идентификатора	Попытка выхода по временной карте до начала или после истечения ее периода действия. Транзакция только для NC-100K-IP, остальные контроллеры передадут сообщение "Нет ключа в БД устройства".
Нет выхода через картоприемник - сотрудник	Субъект доступа с картой, у которой не установлена привилегия "Гостевая карта" пытается выйти с использованием картоприемника, вместо внутреннего считывателя.
Нормальный выход посетителя	К внутреннему считывателю поднесен ключ посетителя, имеющий доступ в данную дверь в текущий момент времени.
Фактический выход посетителя	Осуществлен фактический авторизованный выход посетителя, т.е. к внутреннему считывателю был поднесен ключ, имеющий доступ через данную точку прохода, после чего фактически открыта дверь или провернут турникет (сработал дверной контакт). Данное событие может возникнуть только при наличии дверного контакта, позволяющего определить открывание двери, и при установленном флажке «Фактический проход» в настройках контроллера.
Доступ предоставлен	Эта транзакция генерируется вместо "Нормальный вход по ключу" (и подобных), если у карты имеется привилегия "Управление доступом".
В доступе отказано	Эта транзакция генерируется вместо событий отказа в доступе, если у карты имеется привилегия "Управление доступом".
Ключ выдан	Keyguard. Процедура выдачи ключа, соответствующего предъявленному идентификатору, выполнена корректно.
Ключ возвращен	Keyguard. Процедура возврата ключа, соответствующего предъявленному идентификатору, выполнена корректно.
Неизвестный ключ выдан	Keyguard. Из ключницы физически изъят ключ, не добавленный в нее через ПО Parsec.
Неизвестный ключ возвращен	Keyguard. В ключницу физически вставлен ключ, не добавленный в нее через ПО Parsec.
Ключ задержан (не возвращен вовремя)	Keyguard. Ключ не возвращен в ключницу по истечении заданного периода времени или до наступления заданного момента времени.
Замените батарейку часов	Необходимо заменить батарейку встроенных часов устройства.
База данных очищена. Нет данных на загрузку	Транзакция возникает при инициализации контроллера, не состоящего ни в одной группе доступа, либо его группа доступа не назначена ни одному

	идентификатору, т.е. загружать в БД контроллера нечего.
Нет входа - идентификатор заблокирован	Для NC-8000. Вход запрещен, т.к. идентификатор заблокирован.
Нет выхода - идентификатор заблокирован	Для NC-8000. Выход запрещен, т.к. идентификатор заблокирован.
Нет входа - исчерпан лимит проходов	Для NC-8000. Вход запрещен, т.к. разрешенное количество проходов исчерпано.
Нет выхода - исчерпан лимит проходов	Для NC-8000. Выход запрещен, т.к. разрешенное количество проходов исчерпано.
Нет входа - отказ по максимуму в помещении	Для NC-8000. Вход запрещен, т.к. в помещении (на территории) не может находиться большее количество субъектов доступа.
Нет выхода - отказ по минимуму в помещении	Для NC-8000. Выход запрещен, т.к. в помещении (на территории) не может находиться меньшее количество субъектов доступа.
Нет входа - отказ по разрешению входа	Для NC-8000. Попытка входа идентификатора с привилегией "Вход запрещен".
Нет выхода - отказ по разрешению выхода	Для NC-8000. Попытка выхода идентификатора с привилегией "Выход запрещен".
Нет входа - жесткий доступ	Для NC-8000. Отказ во входе. Субъект не отмечен на обязательных предшествующих точках прохода.
Нет выхода - жесткий доступ	Для NC-8000. Отказ в выходе. Субъект не отмечен на обязательных предшествующих точках прохода.
Событие домофона	Транзакция от единственной интегрированной модели домофона.
Нет выхода - посетитель не входил	Для NC-8000. Транзакция возникает при включенной опции "Запрещен выход незарегистрированных посетителей", если через точку прохода пытается выйти посетитель, который вошел через другую точку.
Неверный ПИН	Для NC-60K/NC-60K.M. Ввод неверного ПИН-кода при попытке прохода в режиме "Карта + ПИН".
Доступ разрешен - ожидание подтверждения оператора	Сообщение об отказе в доступе, так как на точке прохода, на которой включен режим ожидания подтверждения прохода оператором по кнопке, истекло время ожидания действия оператором.
Доступ запрещен - нарушено правило доступа	Не выполнено какое-либо условие прохода по 2 идентификаторам, например, идентификаторы принадлежат разным субъектам доступа.
Сервисный режим включен	Для NC-8000-E. Включен режим, при котором открыт доступ на все этажи, независимо от прав предъявленного ключа.
Сервисный режим выключен	Для NC-8000-E. Выключен сервисный режим. Доступ на этажи предоставляется в соответствии с правами предъявляемых идентификаторов.
База данных устройства переполнена. Загрузка невозможна	База данных контроллера переполнена. Дальнейшая загрузка пользователей невозможна.
Вход с подтверждением	Транзакция генерируется при успешном подтверждении личности первого субъекта доступа вторым субъектом при входе.
Выход с подтверждением	Транзакция генерируется при успешном подтверждении личности первого субъекта доступа вторым субъектом при выходе.
Вход сопровождающего	Транзакция генерируется при фактическом входе сопровождающего в течение заданного времени после входа первого субъекта доступа.

Выход сопровождающего	Транзакция генерируется при фактическом выходе сопровождающего в течение заданного времени после выхода первого субъекта доступа.
Вход без сопровождения	Транзакция генерируется при отсутствии фактического входа сопровождающего в течение заданного времени после входа первого субъекта доступа. По умолчанию это тревожное событие.
Выход без сопровождения	Транзакция генерируется при отсутствии фактического выхода сопровождающего в течение заданного времени после выхода первого субъекта доступа. По умолчанию это тревожное событие.
Ключ из другой ключницы выдан	Транзакция Keyguard. Пользователь получил свой ключ, который находился не в той ключнице, к которой приписан.
Ключ из другой ключницы возвращен	Транзакция Keyguard. Пользователь вернул свой ключ не в ту ключницу, к которой тот приписан.
Сообщения о событиях только для расширенных QR-кодов	
Нет входа - QR код из другой группы	Вход запрещен. Контроллер точки прохода не входит ни в одну группу контроллеров из указанных в QR-коде.
Нет выхода - QR код из другой группы	Выход запрещен. Контроллер точки прохода не входит ни в одну группу контроллеров из указанных в QR-коде.
Нет входа - QR код вне временного интервала	Вход запрещен. Предъявленный QR-код не имеет права прохода в данное время.
Нет выхода - QR код вне временного интервала	Выход запрещен. Предъявленный QR-код не имеет права прохода в данное время.
Нет входа - QR код вне срока действия	Вход запрещен. Срок действия предъявленного QR-кода истек или еще не наступил.
Нет выхода - QR код вне срока действия	Выход запрещен. Срок действия предъявленного QR-кода истек или еще не наступил.
Вход по QR коду	Осуществлен вход по QR-коду.
Выход по QR коду	Осуществлен выход по QR-коду.
Оборудование	
Доступ запрещен - нарушено правило доступа	Открывание корпуса контроллера (при установленном тампере корпуса).
Корпус устройства закрыт	Корпус контроллера закрыт после открывания
Тревога	Активирован охранный датчик в режиме охраны (если используется и установлен в Редакторе оборудования).
Тревога восстановлена	Пропадание сигнала от охранного датчика (в режиме охраны).
Устройство выключено	Полное выключение питания контроллера (сетевого и аккумулятора). Данное событие с реальным временем отключения возникает только при следующем включении контроллера.
Устройство включено	Восстановлено питание контроллера после его полного отключения.
Батарея разряжена	Данная транзакция появляется при разрядке батарейки только у контроллера доступа NC-32K.
Батарея восстановлена	Батарея восстановлена. Заряд в норме.
Сетевое питание отключено	Выключено сетевое питание контроллера. Работа от резервного аккумулятора.
Сетевое питание восстановлено	Восстановлено ранее отключенное сетевое питание контроллера.

Аккумулятор разряжен	Напряжение резервного аккумулятора контроллера ниже нормы. Возникает только при установленном аккумуляторе и отсутствии сетевого питания в течение времени, достаточного для разряда аккумулятора.
Аккумулятор восстановлен	Напряжение аккумулятора достигло нормы (после включения сетевого питания).
Область поставлена на охрану с ПК	Защищаемая область поставлена на охрану по команде с ПК.
Область снята с охраны с ПК	Защищаемая область снята с охраны по команде с ПК.
Область поставлена на охрану пользователем	При взятии на охрану пользователем при помощи карты. При работе с контроллерами доступа.
Область снята с охраны пользователем	При снятии с охраны пользователем при помощи карты. При работе с контроллером доступа.
Переход в автономный режим	При потере связи с контроллером формируется эта транзакция.
Ответ на запрос версии	Plug and Play при обнаружении устройства
Аппаратный сброс устройства	При нажатии на кнопку перезагрузки на плате устройства.
Конфигурация устройства 1	Скрытая
Конфигурация устройства 2	Скрытая
Конфигурация устройства 3	Скрытая
Получена команда открыть дверь	Оператор отдал команду открыть дверь с ПК. При нормальной связи с контроллером дверь откроется и появится событие "Дверь открыта по команде ПК".
Получена команда закрыть дверь	Оператор отдал команду закрыть дверь с ПК. При нормальной связи с контроллером дверь закроется и появится событие "Дверь закрыта по команде ПК". При установленной для данной точки прохода опции "Автозакрывание двери", ручная подача команды не требуется.
Получена команда открыть турникет на вход	Оператор отдал команду на открытие турникета на вход с ПК. При нормальной связи с контроллером турникет откроется на вход и появится событие "Турникет открыт на вход по команде ПК".
Получена команда открыть турникет на выход	Оператор отдал команду на открытие турникета на выход с ПК. При нормальной связи с контроллером турникет откроется на вход и появится событие "Турникет открыт на выход по команде ПК".
Получена команда закрыть турникет	Оператор отдал команду закрыть турникет с ПК. При нормальной связи с контроллером турникет закроется и появится событие "Турникет закрыт по команде ПК".
Получена команда установить абсолютную блокировку	Оператор дал команду с ПК включить абсолютную блокировку. При нормальной связи с контроллером блокировка должна включиться и появиться событие "Прямое управление устройством". Любой доступ при этом запрещен; блокировка используется только в экстренных ситуациях.
Включена абсолютная блокировка	Включена абсолютная блокировка командой с ПК. При включенной абсолютной блокировке любой доступ через данную точку прохода запрещен, за исключением перехода в режим Off-Line.
Получена команда снять абсолютную блокировку	Оператор дал команду с ПК выключить абсолютную блокировку. При нормальной связи с контроллером блокировка должна выключиться и

	появиться событие "Прямое управление устройством".
Снята абсолютная блокировка с ПК	Отключена с ПК ранее включенная абсолютная блокировка.
Получена команда установить относительную блокировку	Оператор дал команду с ПК включить относительную блокировку. При нормальной связи с контроллером блокировка должна включиться и появиться событие "Прямое управление устройством". После этого проход разрешен только пользователям, имеющим соответствующую привилегию. Относительная блокировка может использоваться при видеоверификации для подтверждения прохода оператором.
Включена относительная блокировка	Включена относительная блокировка командой с ПК. При включенной относительной блокировке ключи, имеющие привилегию прохода при блокировке, сохраняют права доступа через данную дверь.
Получена команда снять относительную блокировку	Оператор дал команду с ПК выключить относительную блокировку. При нормальной связи с контроллером блокировка должна выключиться и появиться событие "Прямое управление устройством".
Снята относительная блокировка	Снята относительная блокировка точки прохода по команде с ПК.
Получена команда включить реле	Оператор дал команду с ПК включить реле контроллера. При нормальной связи с контроллером реле должно включиться.
Включение реле с ПК	Дополнительное реле контроллера включено по команде с ПК. При этом реле будет находиться во включенном состоянии с момента подачи команды и до тех пор, пока с ПК не поступит команда на его выключение. Время задержки и время работы реле, устанавливаемые для него в Редакторе оборудования, в данном случае игнорируются.
Получена команда выключить реле	Оператор дал команду с ПК выключить реле контроллера. При нормальной связи с контроллером реле должно выключиться.
Выключение реле с ПК	Дополнительно реле контроллера выключено по команде с ПК (если было ранее включено).
Получена команда поставить на охрану	Оператор дал команду с ПК поставить точку прохода или область на охрану. При нормальной связи с контроллером точка прохода или область в зависимости от её состояния либо встанет на охрану, либо не встанет.
Получена команда снять с охраны	Оператор дал команду с ПК снять точку прохода или область с охраны.
Получена команда снять тревогу	Оператор дал команду с ПК снять с тревогу.
Включена аппаратная блокировка	Аппаратная блокировка аналогична по действию относительной блокировке с тем лишь отличием, что включается не программным путем, а с помощью специальной кнопки или тумблера.
Выключена аппаратная блокировка	Отключена ранее включенная аппаратная блокировка точки прохода (ранее было событие "Включена аппаратная блокировка").
Фатальная ошибка устройства	Только для NC-100K-IP, возможна при ошибках в сетевом стеке.
Програмный сброс устройства	Только для NC-2000, не используется.
Получено СМС	При получении SMS на номер модема (с текстом СМС).
Запрос на работу с ключами	Предъявлен идентификатор, которому назначена та же группа доступа, что и программной ключнице.
Ключ может быть выдан	Данный ключ может быть выдан предъявителю текущего идентификатора.
Ключ может быть забран	Данный ключ может быть забран у предъявителя текущего идентификатора.

Ключ не может быть выдан	Предъявитель текущего идентификатора не имеет прав на получение данного ключа.
Ключ не может быть забран	Предъявитель текущего идентификатора не имеет прав на сдачу данного ключа.
Неизвестный ключ	Вместо идентификатора ключа, зарегистрированного в ключнице, к считывателю поднесена другой идентификатор.
Ключ выдан	Процедура выдачи ключа по предъявленному идентификатору выполнена корректно.
Ключ возвращен	Процедура возврата ключа по предъявленному идентификатору выполнена корректно.
Запуск "Ключницы"	Запущен инструмент "Ключница" (программная).
Выход из "Ключницы"	Закрыт инструмент "Ключница" (программная).
Потеряна связь с биометрическим терминалом	Прекратилась связь с биометрическим терминалом Hikvision или UNI-UBI
Восстановлена связь с биометрическим терминалом	Возобновилась связь с биометрическим терминалом Hikvision или UNI-UBI
Ошибка при передаче данных в биометрический терминал	При передаче данных из БД СКУД в БД биометрического терминала возникла ошибка.
Нет входа - неизвестный	Запрет при попытке входа пользователя, которого нет в БД терминала распознавания лиц.
Нет выхода - неизвестный	Запрет при попытке выхода пользователя, которого нет в БД терминала распознавания лиц.
Нет входа по лицу - детектор маски	Запрет на вход из-за отсутствия медицинской маски у пользователя.
Нет выхода по лицу - детектор маски	Запрет на выход из-за отсутствия медицинской маски у пользователя.
Температура превышена, в доступе на вход отказано	Запрет на вход из-за превышения заданной температуры тела у пользователя.
Температура превышена, в доступе на выход отказано	Запрет на выход из-за превышения заданной температуры тела у пользователя.
Температура в норме	Температура тела не выше заданной границы.
Верификация по лицу не пройдена	Распознанное лицо не соответствует предъявленному идентификатору.
Ключ шифрования записан	В считыватель QR-кодов марки Parsec записан новый ключ шифрования либо восстановлен заводской ключ шифрования.
Настройки считывателя записаны	В считыватель QR-кодов марки Parsec внесены новые параметры настройки.
AC-08	
Обрыв клавиатуры (нет связи)	Нарушена связь между охранным контроллером AC-08 и клавиатурой AKD-01.
Связь с клавиатурой восстановлена	Восстановлена связь между охранным контроллером AC-08 и клавиатурой AKD-01.

Обрыв датчика в области	Нарушена связь между охранным контроллером и охранным датчиком.
КЗ датчика в области	Произошло короткое замыкание у датчика в области.
Неисправность восстановлена	Произошло восстановление неисправности (связь восстановлена).
Постановка на охрану	Получена команда постановить на охрану, идет процесс постановки на охрану.
Тревога в области снята пользователем	Снятие тревоги с клавиатуры AKD-01.
Тревога в области снята с ПК	Оператор принял тревогу в области с ПК.
Область поставлена на охрану от ПК с пропуском зон	Защищаемая область поставлена на охрану по команде с ПК оператором с пропуском охранных зон.
Область поставлена на охрану пользователем с пропуском зон	Область взята на охрану с пропуском зон.
Неправомочные действия пользователя	При работе с клавиатурой AKD - 01 если у оператора нет прав на выполнение данной операции.
Нельзя сконфигурировать – охрана	Попытка загрузить новые настройки с ПК пока контроллер на охране.
Конфигурация сохранена	Внесенные изменения в конфигурацию контроллера успешно сохранены.
Невозможно поставить на охрану с ПК - область не активна	В конфигурации контроллера данная область не активизирована.
Невозможно поставить на охрану с ПК - уже на охране	При попытке поставить область на охрану область не встала на охрану, область уже взята на охрану.
Невозможно поставить на охрану с ПК - в области нет зон	Оператор не может взять на охрану область, т.к. в данной области не установлены зоны.
Невозможно поставить на охрану с ПК - область в процессе постановки	Оператор уже запустил постановку области на охрану с клавиатуры AKD-01. Не удается поставить зону на охрану, потому что команда "поставить на охрану" уже послана.
Невозможно поставить на охрану с ПК - недопустимый номер области	При взятии области на охрану с ПК, выбрана область с номером, который не может существовать. При использовании ПО, в котором можно создавать количество областей больше 8.
Невозможно поставить на охрану с ПК - неисправность в непропускаемой зоне	В зоне, которая не является пропускаемой, произошло повреждение, а область, включающую в себя данную зону, пытались взять на охрану.
Невозможно поставить на охрану с клавиатуры - область не активна	Не включена область в охранном контроллере при постановке области на охрану с клавиатуры
Невозможно поставить на охрану с клавиатуры - уже на охране	Область уже поставлена на охрану, повторная установку на охрану невозможна.
Невозможно поставить на охрану с клавиатуры - в	Не настроены зоны в охранном контроллере

области нет зон	
Невозможно поставить на охрану с клавиатуры - область в процессе постановки	Пользователь при помощи клавиатуры AKD-01 отдал команду – взять на охрану. Данная операция невозможна – оператор уже отдал команду взять на охрану.
Невозможно поставить на охрану с клавиатуры - недопустимый номер области	Не удаётся поставить зону на охрану с AKD-01, неверно задан номер области
Невозможно поставить на охрану с клавиатуры - неисправность в непропускаемой зоне	Постановка на охрану области с клавиатуры при неисправном датчике
Взлом клавиатуры	Сработал тампер клавиатуры охранного контроллера (корпус клавиатуры открыт).
Клавиатура закрыта	Корпус клавиатуры закрыт.
Аргус. ОПС Стрелец	
Локальный раздел снят с охраны ПК	Защищаемый раздел снят с охраны командой с ПК, поданной оператором.
Локальный раздел поставлен на охрану с ПК	Защищаемый раздел установлен на охрану командой с ПК, поданной оператором.
Локальный раздел снят с охраны под принуждением	Защищаемый раздел снят с охраны «под принуждением».
Автоматический сброс пожарных тревог и неисправностей	Выполнен автоматический сброс всех тревожных событий по типу: пожарных тревог и неисправностей.
Ручной сброс пожарных тревог и неисправностей	Выполнена команда сброс всех тревожных событий с устройства управления по типу: пожарных и неисправностей в разделе(разделах).
Автоматическое снятие с охраны	В системе произошло автоматическое снятие с охраны (указанных разделов).
Автоматическая постановка(перевзятие)	В системе произошла автоматическая постановка под охрану с повторной постановкой не установленных зон на охрану.
Локальный раздел снят с охраны пользователем	Защищаемый раздел снят с охраны по команде с устройства пользователем.
Локальный раздел поставлен на охрану пользователем	Защищаемый раздел поставлен на охрану по команде с устройства пользователем.
Глобальный раздел снят с охраны пользователем	Защищаемый глобальный раздел снят с охраны по команде с устройства пользователем.
Глобальный раздел поставлен на охрану пользователем	Защищаемый глобальный раздел поставлен на охрану по команде с устройства пользователем.
Глобальный раздел снят с охраны	Защищаемый глобальный раздел переведен в режим не на охране.
Глобальный раздел поставлен на охрану	Защищаемый глобальный раздел переведён в режим охраны.

Охранная тревога	В разделе, который установлен на охрану, произошла тревога (сработал датчик охранный).
Пожарная тревога	Пришла тревога с пожарного датчика.
Сброс паники	Произведен сброс круглосуточного раздела/тревожной кнопки("Паника").
Паника	Сработал круглосуточный раздел/тревожная кнопка("Паника").
Задержка на снятие с охраны	Начался отсчет времени на вход в охраняемый раздел для ввода кода на снятие с охраны.
Задержка на взятие на охрану	Начался отсчет времени на выход из охраняемого раздела
Пожарное внимание	Сработал один из пожарных датчиков, включенных в раздел с двойной сработкой (по сработке первого идет событие “Внимание” по сработке второго формируется событие “Пожар”).
Пожарная тревога с данными	Пришла тревога с пожарного датчика, у которого включена передача аналогового значения задымленности/температуры.
Технологическая тревога	Пришла тревога с технологического датчика.
Тревога с данными	Пришла тревога от технологического датчика, у которого включена передача аналогового значения, контролируемого фактора.
Общая неисправность дочернего устройства	Неисправность дочернего устройства.
Восстановлено основное питание дочернего устройства	Восстановление напряжение на входе основного питания на дочернем устройстве.
Отсутствует основное питание дочернего устройства	Падение напряжения на входе основного питания на дочернем устройстве.
Восстановлено резервное питание дочернего устройства	Восстановление напряжение на входе резервного питания на дочернем устройстве.
Отсутствует резервное питание дочернего устройства	Падение напряжения на входе резервного питания на дочернем устройстве.
Восстановлена связь с дочерним устройством	Восстановлена ранее нарушенная связь с дочерним устройством.
Отсутствует связь с дочерним устройством	Пропала связь с дочерним радиоустроством.
Запыление дымовой камеры	Высокая концентрация пыли в дымовой камере датчика.
Неисправность ручного обхода адресов восстановлена	Выключена функция ручной обход адреса.
Неисправность ручного обхода адресов	Включена функция ручной обход адреса.
Неисправность автоматического обхода адресов восстановлена	Выключена функция автоматический обход адреса.
Неисправность автоматического обхода адресов	Включена функция автоматический обход адреса.

Внешняя помеха устранена	Исчезла помеха в радиоэфире на той же частоте что и у устройства радиоканальной системы.
Внешняя помеха	Обнаружена помеха в радиоэфире на той же частоте что и у устройства радиоканальной системы.
Аккумулятор РРОП восстановлен	Данная транзакция появляется при восстановлении заряда батареи устройства РРОП.
Аккумулятор РРОП разряжен	Данная транзакция появляется при снижении заряда резервной батареи устройства РРОП.
Неисправность аккумулятора РРОП восстановлена	Восстановлена неиспраность батареи на устройстве РРОП, появляется после события "Аккумулятор РРОП неисправен".
Аккумулятор РРОП неисправен	Возникла проблема с батареей устройства РРОП, необходимо проверить аккумулятор и при необходимости его заменить.
Сетевое питание РРОП восстановлено	Восстановление напряжение на входе основного питания устройства РРОП.
Отсутствует сетевое питание РРОП	Падение напряжения на входе основного питания устройства РРОП.
Неисправность сигнальной линии "Аккорд-512" восстановлена	Восстановлении линии на приборе приемно-контрольно-охранно-пожарном (Снят с производства).
Неисправна сигнальная линия "Аккорд-512"	Произошла неисправность линии на приборе контрольно-охранно-пожарном (Снят с производства).
Связь с дочерним РРОП восстановлена	Восстановление связи с одним из устройств, подключенных к РРОП, ранее с которым была потяряна связь.
Отсутствует связь с дочерним РРОП	Потеряна связь с одним из устройств, подключенных к РРОП.
Неисправность сигнальной линии "Радуга-2А" восстановлена	Восстановлении линии на приборе приемно-контрольно-пожарном (Снят с производства).
Неисправна сигнальная линия "Радуга-2А"	Произошла неисправность линии на приборе контрольно-пожарном (Снят с производства).
Линия связи с ПЦН восстановлена	Восстановление линии связи с пультом централизованного наблюдения.
Обрыв линии связи с ПЦН	Линия связи с пультом централизованного наблюдения нарушена.
Линия связи с устройством передачи извещений восстановлена	Линия интерфейса с устройством передачи извещений восстановлена.
Обрыв линии связи с устройством передачи извещений	Линия интерфейса с устройством передачи извещений нарушена.
Коммуникатор связи с ПЦН восстановлен	Восстановлена работа передатчика на пульте центрального наблюдения.
Неисправность коммуникатора связи с ПЦН	Произошла неисправность передатчика на пульте центрального наблюдения.
Код доступа к РРОП изменен	Изменен код доступа к радиорасширителю охранно-пожарному.
Программирование РРОП	Произведено программирование радиорасширителя охранно-пожарного.

Код пользователя изменен	Произведено изменение кода пользователя.
Программирование свойств системного устройства	Произведена настройка системного устройства в программе.
Программирование свойств дочернего устройства	Произведена настройка дочернего устройства в программе.
Удаление дочернего устройства	Произведено в программе удаление дочернего устройства.
Удаление ключа TouchMemory	Произведено удаление ключа TouchMemory.
Добавление ключа TouchMemory	Произведено добавление нового ключа TouchMemory.
Изменение состава ключей TouchMemory	Внесены изменения в программе в составе ключей TouchMemory.
Включение питания РРОП	Произведено включение питания радиорасширителя охранно-пожарного из программы.
Выключение питания РРОП	Произведено выключение питания радиорасширителя охранно-пожарного из программы.
Включение питания коммуникационного устройства	Подано питание для коммуникационного устройства (передатчика).
Выключение питания коммуникационного устройства	Отключено питания от коммуникационного устройствава (передатчика).
Деактивация релейных выходов РРОП	Релейные выходы радиорасширителя охранно-пожарного вернулись в исходное состояние (деактивировались).
Активация релейных выходов РРОП	Активированы релейные выходы радиорасширителя охранно-пожарного.
Деактивация удаленных релейных выходов	Релейные выходы удаленного устройства вернулись в исходное состояние(деактивировались).
Активация удаленных релейных выходов	Активированы релейные выходы удаленного устройства.
Включение групп исполнительных устройств	Команда на включение групп(ы) исполнительных устройства.
Отключение групп исполнительных устройств	Команда на выключение групп(ы) исполнительных устройства
Отключение блока речевого оповещения	Команда на остановку (окончание) запуска (прекращение воспроизведения сообщений) речевыми оповещателями выполнена устройством.
Запуск блока речевого оповещения	Команда на запуск речевых оповещателей выполнена устройством.
Команда на отключение аналоговой трансляции речевых сообщений	Отправлена команда из программы на отключение аналоговой трансляции речевых сообщений.
Команда на запуск аналоговой трансляции	Отправлена команда из программы на включение аналоговой трансляции речевых сообщений.

речевых сообщений	
Отключение аналоговой трансляции речевых сообщений	Команда получена на отключение аналоговой трансляции речевых сообщений, устройство в режим отключение.
Запуск аналоговой трансляции речевых сообщений	Команда получена на включение аналоговой трансляции речевых сообщений, устройство в режим включения.
Команда на выключение всех реле в группе	Послана команда устройству на выключения всех активированных реле в заданной группе.
Корпус РРОП закрыт	Корпус радиоканального расширителя закрыт после открывания.
Вскрыт корпус РРОП	Открыт корпуса радиоканального расширителя.
Подбор кода доступа	Попытка подбора кода доступа.
Попытка подмены дочернего устройства	В эфире существует два дочерних устройства (датчика и т.д.) с одинаковыми кодами на одном адресе.
Попытка подмены РРОП	В эфире существует два радиорасширителя с одинаковыми кодами на одном адресе.
Несанкционированное управление удаленным исполнительным устройством	Попытка управления удаленным устройств без прав доступа.
Попытка подмены системного устройства	В эфире существует два системных устройства с одинаковыми кодами на одном адресе.
Устройство выключено	Полное выключение питания контроллера (сетевого и аккумулятора).
Раздел взят на охрану	Охраняемая территория взята под охрану.
Раздел снят с охраны	Охраняемая территория снята с охраны.
Тревога	Активирован охранный датчик в режиме охраны.
Пожарная тревога	Сработали оба пожарных датчика, включенных в раздел с двойной сработкой (по сработке первого идет событие “Внимание” по сработке второго формируется событие “Пожар”).
Мурена (система охраны периметра)	
Преодоление	Преодоление порога хотя бы в одном диапазоне.
Преодоление по НЧ каналу	Произошло событие на вибрационном средстве обнаружения. Определяющее наличие тревожного состояния по анализу сигнала в одном частотном диапазоне, а именно, в низкочастотном (от 0 до 10 Гц).
Преодоление по ВЧ каналу	Произошло событие на вибрационном средстве обнаружения. Определяющее наличие тревожного состояния по анализу сигнала в одном частотном диапазоне, а именно, в низкочастотном (от 20 до 150 Гц).
Преодоление по НЧ и ВЧ каналам	Произошло событие на вибрационном средстве обнаружения. Определяющее наличие тревожного состояния по анализу сигнала в двух частотных диапазонах, а именно, в низкочастотном (от 0 до 10 Гц) и высокочастотном (от 20 до 150 Гц).
ОПС Болид	
Восстановление сети 220 В	_
Авария сети 220 В	_

Тревога проникновения	Нарушение охранного шлейфа сигнализации (ШС), взятого на охрану.
Помеха	Повышение сигнала в измерительном канале датчика, но меньше уровня тревоги.
Помеха устранена	_
Активация УДП	Нажата кнопка (переключатель и т.п.) адресного или контролируемого с помощью ШС устройства, предназначенного для дистанционного запуска противопожарного оборудования.
Восстановление УДП	Устройство дистанционного пуска переведено в исходное состояние.
Неудачное взятие	В момент постановки под охрану ШС был нарушен или неисправен.
Предъявлен код принуждения	Предъявлен код принуждения.
Тест	Срабатывание пожарного дымового извещателя «ДИП-34А» при специальном тестовом воздействии (поднесении магнита или нажатии тестовой кнопки) не в режиме тестирования.
Включение режима тестирования	ШС переведен в режим «Тестирование».
Выключение режима тестирования	ШС вышел из режима «Тестирование».
Восстановление контроля	Восстановление (включение) контроля программируемого технологического ШС.
Задержка взятия	Включилась задержка на выход (задержка взятия на охрану).
ШС взят	ШС взят на охрану.
Идентификация	Пользователь ввёл код для управления (например, для постановки на охрану или снятия с охраны).
Восстановление технологического ШС	–
Нарушение технологического ШС	–
Пожар	Обычно это срабатывание двух пороговых извещателей в шлейфе сигнализации, либо истекла задержка перехода в «Пожар» после срабатывания порогового извещателя, либо превышение измеряемой величиной (температура или задымленность) порога «Пожар» в адресно-аналоговой зоне.
Нарушение 2 технологического ШС	Другое нарушение технологического ШС.
Восстановление нормы пожарного оборудования	–
Пожар 2	Состояние «Пожар» не менее двух ШС или автоматических адресных извещателей, принадлежащих одной контролируемой области (одному разделу), либо «Пожар» в зоне, контролирующей ручной извещатель.
Неисправность пожарного оборудования	Неисправность пожарного оборудования. Это либо внутренняя неисправность адресного извещателя (неисправность оптической системы «ДИП-34А»), либо нарушение цепей контроля массы и давления прибора «С2000-КПБ».
Неизвестное устройство	_
«Внимание! Опасность пожара»	Обычно это срабатывание одного порогового теплового пожарного извещателя, не подтвержденное срабатыванием порогового дымового

	извещателя, величина измеряемого адресно-аналоговым извещателем фактора пожара (температура, задымленность) превысила порог «Внимание».
Обрыв ШС	Обрыв шлейфа сигнализации или контролируемой цепи адресного расширителя.
Обрыв ДПЛС	Обрыв двухпроводной линии связи.
Восстановление ДПЛС	Восстановление двухпроводной линии после обрыва или КЗ.
Тихая тревога	Нарушение тревожного ШС.
Понижение уровня	Понижение уровня воды или давления («Поток-3Н»).
Норма уровня	Восстановление уровня воды или давления («Поток-3Н»).
Повышение уровня	Повышение уровня воды или давления («Поток-3Н»).
Аварийное повышение уровня	Превышение аварийного уровня воды или давления («Поток-3Н»).
Повышение температуры	Температура превысила максимально допустимое значение.
Аварийное понижение уровня	Понижение уровня воды или давления ниже аварийного значения («Поток-3Н»).
Температура в норме	Температура в установленных границах («температурная» зона «С2000-КДЛ»).
Тревога затопления	Срабатывание датчика затопления (протечки).
Восстановление датчика затопления	Восстановление датчика затопления (протечки).
Неисправность термометра	Неисправность измерителя температуры («температурная» зона «С2000-КДЛ»).
Восстановление термометра	Восстановление измерителя температуры («температурная» зона «С2000-КДЛ»).
Локальное программирование	–
Неисправность канала связи	Неисправность канала передачи извещений абоненту.
Восстановление канала связи	Восстановление канала передачи извещений абоненту.
ШС снят	ШС снят с охраны.
Сброс тревоги ШС	Сброшено состояние «тревога» или «пожар».
Восстановление ШС	Восстановление нормы снятого охранного ШС.
Тревога входа	Тревога входной зоны.
Нарушение ШС	Нарушение снятого охранного ШС.
Обрыв выхода	Обрыв цепи нагрузки релейного выхода.
КЗ выхода	Короткое замыкание цепи нагрузки релейного выхода.
Восстановление выхода	Восстановление релейного выхода (восстановление после неисправности цепи нагрузки выхода).
Выход отключен	Управление выходом (реле) недоступно из-за отсутствия связи с ним: потеряна связь контроллера «С2000-КДЛ» с адресным релейным модулем «С2000-СП2», либо потеряна связь «С2000-АСПТ» с подключенными к нему «С2000-КПБ».

Выход подключен	Восстановлено управление выходом (реле): восстановлена связь контроллера «С2000-КДЛ» с потерянным ранее адресным релейным блоком «С2000-СП2», либо восстановлена связь «С2000-АСПТ» с «С2000-КПБ».
Изменение состояния выхода	Изменение состояния исполнительного выхода: включение, включение в прерывистом режиме, выключение.
Насос включен	_
Насос выключен	_
Ошибка при автоматическом тестировании	Выявлен сбой (неисправность) в оборудовании.
Срабатывание цепи пуска	_
Неудачный пуск пожаротушения	Неудачный запуск автоматической установки пожаротушения (пусковой импульс был выдан, но не зафиксирован выход огнетушащего вещества).
Ручной тест	Запуск ручного теста.
Задержка автоматического пуска	Выполнилось условие пуска аппаратуры управления пожаротушением и идет отсчет задержки перед выдачей пускового импульса.
Автоматика выключена	Режим автоматического запуска АУП выключен.
Отмена пуска АСПТ	Пуск АУП был отменен (например, во время задержки запуска была нажата кнопка «СБРОС» прибора «С2000-АСПТ», либо с пульта дана команда «ОТМЕНИТЬ ПУСК»).
Тушение	Идет тушение (после выдачи пускового импульса зафиксирован выход огнетушащего вещества).
Аварийный пуск АСПТ	Аварийный пуск аппаратуры пожаротушения (пускового импульса не было, но зафиксирован выход огнетушащего вещества).
Пуск АУП	Выдан импульс пуска аварийной установки пожаротушения
Блокировка пуска АУП	Пуск АУП был заблокирован (например, во время задержки запуска была открыта дверь в защищаемое помещение).
Автоматика включена	Режим автоматического пуска АУП включен.
Открыт корпус прибора	_
Пуск речевого оповещения	Выполнен запуск речевого оповещения (РО).
Сброс пуска речевого оповещения	Отмена пуска речевого оповещения.
Закрыт корпус прибора	_
Срабатывание клапана	Клапан приточно-вытяжной вентиляции или дымоудаления перешел в рабочее состояние.
Восстановление клапана	Клапан приточно-вытяжной вентиляции или дымоудаления перешел в исходное состояние.
Отказ клапана	Клапан не перешел в рабочее или исходное состояние.
Ошибка клапана	Некорректное состояние цепей контроля клапана.
Внутренняя зона восстановлена	_
Задержка пуска РО	Идёт задержка перед пуском РО.
Останов задержки пуска АУП	Отсчёт задержки пуска пожаротушения остановлен.

Ошибка параметров ШС	ШС неработоспособен из-за ошибок параметров конфигурации.
ШС отключен	Отключен ШС: потеряна связь контроллера «С2000-КДЛ» с адресным извещателем или расширителем, либо потеряна связь «С2000-АСПТ» с подключенными к нему «С2000-КПБ».
ШС подключен	Подключен ШС: восстановлена связь «С2000-КДЛ» с потерянным ранее адресным извещателем или расширителем, либо восстановлена связь «С2000-АСПТ» с «С2000-КПБ».
Нет связи ДПЛС1	Потеряна связь с извещателем по ветви 1 кольцевой ДПЛС.
Нет связи ДПЛС2	Потеряна связь с извещателем по ветви 2 кольцевой ДПЛС.
Восстановлена связь ДПЛС1	Восстановлена связь с одним или несколькими адресными извещателями по ветви 1 кольцевой ДПЛС.
Отключен РИП	Выходное напряжение резервированного источника питания (РИП) отключено (выполнена команда отключения выходного напряжения).
Включен РИП	Выходное напряжение РИП включено (выполнена команда включения выходного напряжения).
Перегрузка РИП	Перегрузка резервированного источника питания (РИП).
Устранена перегрузка РИП	Перегрузка источника питания резервированного (РИП) устранена.
Неисправность ЗУ РИП	Неисправность зарядного устройства РИП.
Восстановление ЗУ РИП	Неисправность зарядного устройства РИП устранена.
Авария питания	Напряжение питания прибора вышло за допустимые границы.
Восстановление питания	Напряжение питания прибора пришло в норму после аварии.
Восстановление батареи	Напряжение системной батареи пришло в норму.
Восстановлена связь ДПЛС2	Восстановлена связь с одним или несколькими адресными извещателями по ветви 2 кольцевой ДПЛС.
Неисправность батареи	Батареи нет, либо обобщённая неисправность батареи.
Сброс прибора	Перезапуск прибора.
Необходимо обслуживание	Требуется обслуживание извещателя (например, запылена дымовая камера извещателя «ДИП-34А»).
Ошибка теста АКБ	АКБ не прошла тест и признана непригодной для дальнейшей эксплуатации.
Пониженная температура	Температура ниже минимально допустимого значения («температурная» зона «С2000-КДЛ»).
АКБ разряжена	Предупреждение о скором разряде батареи.
Разряд резервной батареи	Предупреждение о скором разряде резервной батареи (в пожарных радиоканальных извещателях).
Восстановление резервной батареи	Резервная батарея в норме (в пожарных радиоканальных извещателях).
Короткое замыкание ШС	Короткое замыкание шлейфа сигнализации или контролируемой цепи адресного расширителя.
Короткое замыкание ДПЛС	Короткое замыкание двухпроводной линии связи (ДПЛС) прибора «С2000-КДЛ».
Сработка датчика	Неподтверждённое срабатывание пожарного извещателя
Отключение ветви RS-485	Отключение кольцевого интерфейса прибора отRS-485 одной ветви.
Восстановление ветви RS-485	Восстановление ветви кольцевогосвязи интерфейса с прибором RS-485.

Срабатывание СДУ	Срабатывание датчика сигнализатора давления (СДУ).
Отказ СДУ	Отказ датчика СДУ.
Авария ДПЛС	Авария двухпроводной линии связи прибора «С2000-КДЛ» (обычно некорректные уровни напряжения в линии).
Отметка наряда	Срабатывание цепи контроля наряда.
Раздел снят по принуждению	Раздел снят по принуждению.
Раздел взят на охрану	Раздел взят на охрану.
Раздел снят с охраны	Раздел снят с охраны.
Потеряна связь с прибором	–
Восстановлена связь с прибором	–
Включение пульта С2000М	–
Ошибки	
Потеряна связь с устройством	Нарушена связь с контроллером. При этом все действия, связанные с подачей команд в контроллер или проверкой статуса, становятся недоступными.
Неверная модель устройства	При добавлении устройства задаваемый адрес указывает на отличающуюся модель. Например, добавляется NC-8000, а вводится адрес, по которому находится NC-100K-IP.
В БД устройства недостаточно места для загрузки расписаний	В памяти контроллера недостаточно места для загрузки расписания, в каждом контроллере есть ограничения по загрузке определенного количества расписаний в зависимости от модели.
Невозможно загрузить в устройство несовместимое расписание	В контроллер была попытка сохранить расписание. Расписание не было сохранено из-за ошибки несовместимости модели контроллера и типа расписания
Потеряна связь с портом	_
Рабочая станция отключена	Потеряна связь с одной из рабочих станций.
Сетевое устройство отключено	Потеря связи с CNC-02-IP.
Ошибка (см. подробности)	Детальное описание ошибки можно посмотреть в подробностях.
Рабочая станция подключена	Восстановление связи с одной из рабочих станций.
Сетевое устройство подключено	Восстановление связи с CNC-02-IP.
Восстановлена связь с устройством	Восстановлена ранее нарушенная связь с контроллером (см. событие Потеряна связь с устройством).
Восстановлена связь с портом	Восстановление связи с CNC-12-IP или CNC-14-IP
Поиск оборудования запущен	Произведен поиск оборудования вручную или автоматически после перезапуска службы.

Поиск оборудования завершен	Закончен поиск оборудования запущенный вручную или автоматически после перезапуска службы.
Обнаружена непринятая тревога	Возникает при открытии монитора после возникновения тревоги, чтобы ее можно было принять.
Рабочая станция сменила адрес	Данное сообщение появляется при смене IP-адреса рабочей станции, а также, если существует несколько станций с одинаковым ID.
В БД заканчивается свободное место	Сообщает о том, что в БД сервера скоро закончится свободное место.
Ключ защиты не обнаружен	Сообщение генерируется, если при старте сервера системы (службы сервера) отсутствует ключ защиты.
Ключ защиты отключен	Сообщение генерируется, если при работающем сервере системы (службы сервера) физический ключ защиты удален.
Ключ защиты подключен	Сообщение генерируется, если при работающем сервере системы (службы сервера) физический ключ защиты вставлен.
Изменение состояния ключа системы	Сообщение генерируется при обновлении данных в ключе защиты (запись из файла обновления лицензии).
Видео	
Включение записи	Запись с камеры в архив системы видеонаблюдения включена оператором или при выполнении задания автоматизации.
Запись выключена	Остановлена запись на видеокамере по действию оператора в программе или по макро действию
Установка на охрану	Видеосистема ИСБ "Интеллект". Оператор послал команду "Поставить на охрану". После этого видеокамера при регистрации тревожного события производит запись.
Снятие с охраны	Видеосистема ИСБ "Интеллект". Оператор снял с охраны видеокамеру. Ранее было событие "Установка на охрану".
Засветка	Видеосистема Macroscop. Событие возникает при засветке камеры, если включен соответствующий детектор.
Обнаружен путь	Видеосистема Macroscop. ПО системы видеонаблюдения распознало движение объектов по определенному маршруту.
Создана запись в видеоархиве	В архиве на сервере видеосистемы создана новая запись.
Обнаружен автономер	ПО системы видеонаблюдения распознало номер транспортного средства.
Движение	ПО системы видеонаблюдения обнаружило наличие движения в контролируемой зоне (детектор движения должен быть включен).
Добавлен коментарий	Оператор ввел комментарий в диалоговом окне, которое появляется при разрешении прохода субъекту доступа в модуле видеоверификации.
Установлен маркер записи видео	Событие возникает при пометке кадра в Мониторе событий.
Сохранен кадр изображения	Кадр с IP-камеры сохранен в базу Parsec.
Сохранена история кадров	Последовательность кадров с IP-камеры сохранена в базу Parsec.
Сигнал потерян	Связь с видеокамерой прервалась.
Сигнал восстановлен	Связь с видеокамерой восстановлена.

Обнаружен оставленный предмет	Видеосистема Trassir, Macroscop. ПО системы видеонаблюдения распознало в контролируемой зоне предмет, остающийся неподвижным дольше допустимого интервала времени. Чувствительность и размер предмета задаются предварительно.
Обнаружено лицо (детектор лиц)	Видеосистема Trassir, Macroscop. ПО системы видеонаблюдения распознало в контролируемой зоне объект, соответствующий параметрам «лицо человека». Объект выделяется на изображении рамкой.
Обнаружен огонь	Видеосистема Trassir или Macroscop обнаружила огонь в поле наблюдения.
Обнаружен дым	Видеосистема Trassir или Macroscop обнаружила дым в поле наблюдения.
Огонь погашен	Огонь в поле наблюдения видеосистемы Trassir или Macroscop более не обнаруживается.
Дым прекратился	Дым в поле наблюдения видеосистемы Trassir или Macroscop более не обнаруживается.
Обнаружен человек	Видеосистема Trassir или Macroscop обнаружила человека в поле наблюдения.
Детектирован звук	Видеосистема Trassir или Macroscop обнаружила звук в радиусе действия микрофонов.
Звук прекращен	Звук в радиусе действия микрофонов видеосистемы Trassir или Macroscop более не обнаруживается.
Вторжение	Видеосистема Trassir или Macroscop обнаружила движение в охраняемой зоне.
Пересечение линии	Видеосистема Trassir, Macroscop или Интеллект обнаружила пересечение установленной в поле наблюдения границы.
Тревога	Автоматический сигнал тревоги по заданному событию.
Пользовательская тревога	Сигнал тревоги, поданный вручную.
Аудит	
Вход в систему	Оператор запустил какую-либо консоль ParsecNET (Администрирование, Бюро пропусков, Видеоверификация, Монитор,Отчеты).
Выход из системы	Оператор закрыл консоль ParsecNET (Администрирование, Бюро пропусков, Видеоверификация, Монитор,Отчеты).
Задание запущено	Оператор в программе ParsecNET запустил задание или задание запущено автоматически.
Вход в редактор "Группы доступа"	Оператор в программе ParsecNET открыл инструмент "Группы доступа".
Выход из редактора "Группы доступа"	Оператор в программе ParsecNET закрыл инструмент "Группы доступа".
Запуск "Монитора событий"	Оператор в программе ParsecNET открыл инструмент "Монитора событий".
Приём тревоги оператором	Оператором принята тревога, находившаяся в очереди тревог. Принятая тревога удаляется из очереди тревог и появляется соответствующее событие о приеме тревоги оператором.
Прямое управление устройством	Оператор с ПК выполнил непосредственное действие с оборудованием, например: открыть дверь.
Изменение внешнего вида	Оператор в программе ParsecNET изменил внешний вид консоли (оконный, полноэкранный, панель команд, панель задач).
Запуск отчёта по событиям	Оператор в программе ParsecNET в окне инструмента "Отчёт по событиям" нажал на кнопку "Сформировать".

Вход в редактор "Бизнес-отчёты"	Оператор в программе ParsecNET открыл инструмент "Бизнес-отчёты".
Выход из редактора "Бизнес-отчёты"	Оператор в программе ParsecNET закрыл инструмент "Бизнес-отчёты".
Вход в редактор "Оборудование"	Оператор в программе ParsecNET открыл инструмент "Оборудование".
Выход из редактора "Оборудование"	Оператор в программе ParsecNET закрыл инструмент "Оборудование".
Вход в редактор "Задания"	Оператор в программе ParsecNET открыл инструмент "Задания".
Выход из редактора "Задания"	Оператор в программе ParsecNET закрыл инструмент "Задания".
Вход в редактор "Операторы"	Оператор в программе ParsecNET открыл инструмент "Операторы".
Выход из редактора "Операторы"	Оператор в программе ParsecNET закрыл инструмент "Операторы".
Вход в редактор "Организации"	Оператор в программе ParsecNET открыл инструмент "Организации", данный функционал доступен при лицензии PnSoft-PRO.
Выход из редактора "Организации"	Оператор в программе ParsecNET закрыл инструмент "Организации", данный функционал доступен при лицензии PnSoft-PRO.
Вход в редактор "Персонал"	Оператор в программе ParsecNET открыл инструмент "Персонал".
Выход из редактора "Персонал"	Оператор в программе ParsecNET закрыл инструмент "Персонал".
Вход в редактор "Топология"	Оператор в программе ParsecNET открыл инструмент "Топология".
Выход из редактора "Топология"	Оператор в программе ParsecNET закрыл инструмент "Топология".
Вход в редактор "Шаблоны печати"	Оператор в программе ParsecNET открыл инструмент "Шаблоны печати".
Выход из редактора "Шаблоны печати"	Оператор в программе ParsecNET закрыл инструмент "Шаблоны печати".
Вход в редактор "Расписания"	Оператор в программе ParsecNET открыл инструмент "Расписания".
Выход из редактора "Расписания"	Оператор в программе ParsecNET закрыл инструмент "Расписания".
Вход в редактор "Системные настройки"	Оператор в программе ParsecNET открыл инструмент "Системные настройки".
Выход из редактора "Системные настройки"	Оператор в программе ParsecNET закрыл инструмент "Системные настройки".
Выход из "Монитора событий"	Оператор в программе ParsecNET закрыл инструмент или отдельную консоль "Монитор событий".
Вход в "Бюро пропусков"	Оператор в программе ParsecNET открыл инструмент или запустил отдельную консоль "Бюро пропусков".
Выход из "Бюро пропусков"	Оператор в программе ParsecNET закрыл инструмент или отдельную консоль "Бюро пропусков".

Вход в редактор "Отчет по событиям системы"	Оператор в программе ParsecNET открыл инструмент "Отчет по событиям".
Выход из редактора "Отчет по событиям системы"	Оператор в программе ParsecNET закрыл инструмент "Отчет по событиям".
Вход в редактор "Поправки рабочего времени"	Оператор в программе ParsecNET открыл инструмент "Поправки к рабочему времени".
Выход из редактора "Поправки рабочего времени"	Оператор в программе ParsecNET закрыл инструмент "Поправки к рабочему времени".
Вход в редактор "Отчеты бюро пропусков"	Оператор в программе ParsecNET открыл инструмент "Отчеты бюро пропусков".
Выход из редактора Отчеты бюро пропусков"	Оператор в программе ParsecNET закрыл инструмент "Отчеты бюро пропусков".
Создание объекта "Группа доступа"	Оператор в программе ParsecNET добавил новый объект в редакторе групп доступа.
Изменение объекта "Группа доступа"	Оператор в программе ParsecNET внес изменения в группу доступа.
Удаление объекта "Группа доступа"	Оператор в программе ParsecNET удалил группу доступа.
Создание объекта "Бизнес-отчёт"	Оператор в программе ParsecNET создал новый шаблон в редакторе "Бизнес-отчеты".
Изменение объекта "Бизнес-отчёт"	Оператор в программе ParsecNET внес изменения в шаблон в редакторе "Бизнес-отчеты".
Удаление объекта "Бизнес-отчёт"	Оператор в программе ParsecNET удалил шаблон в редакторе "Бизнес-отчеты".
Создание объекта "Оборудование"	Оператор в программе ParsecNET добавил новый элемент в Редакторе оборудования.
Изменение объекта "Оборудование"	Оператор в программе ParsecNET внес изменения в объект Редактора оборудования.
Удаление объекта "Оборудование"	Оператор в программе ParsecNET удалил объект в Редакторе оборудования.
Создание объекта "Задача пользователя"	Оператор в программе ParsecNET создал новое задание в Редакторе заданий.
Изменение объекта "Задача пользователя"	Оператор в программе ParsecNET внес изменения в Редакторе системных настрое или в Редакторе заданий (например, сохранил настройки резервного копирования).
Удаление объекта "Задача пользователя"	Оператор в программе ParsecNET удалил задание в Редакторе заданий.
Создание объекта "Группа безопасности"	Оператор в программе ParsecNET добавил новую группу в Редакторе операторов.
Изменение объекта "Группа безопасности"	Оператор в программе ParsecNET внес изменения в карточке группы операторов.
Удаление объекта "Группа безопасности"	Оператор в программе ParsecNET удалил группу в Редакторе операторов.
Создание объекта "Оператор"	Оператор в программе ParsecNET добавил нового оператора в Редакторе операторов.

Изменение объекта "Оператор"	Оператор в программе ParsecNET внес изменения в карточке оператора.
Удаление объекта "Оператор"	Оператор в программе ParsecNET удалил объект в Редакторе операторов.
Создание объекта "Подразделение"	Оператор в программе ParsecNET добавил новое подразделение в Редакторе персонала.
Изменение объекта "Подразделение"	Оператор в программе ParsecNET внес изменения в карточке подразделения.
Удаление объекта "Подразделение"	Оператор в программе ParsecNET удалил подразделение в Редакторе персонала.
Создание объекта "Персона"	Оператор в программе ParsecNET добавил новый объект (сотрудник, посетитель или автомобиль) в Редакторе персонала.
Изменение объекта "Персона"	Оператор в программе ParsecNET внес изменения в карточке объекта (сотрудника, посетителя или автомобиля).
Удаление объекта "Персона"	Оператор в программе ParsecNET удалил объект (сотрудника, посетителя или автомобиля) в Редакторе персонала.
Создание объекта "Организация"	Оператор в программе ParsecNET добавил новый объект в Редакторе организаций. Данный функционал доступен при лицензии PnSoft-PRO.
Изменение объекта "Организация"	Оператор в программе ParsecNET внес изменения в карточке объекта в Редакторе организаций. Данный функционал доступен при лицензии PnSoft-PRO
Удаление объекта "Организация"	Оператор в программе ParsecNET удалил объект в Редакторе организаций. Данный функционал доступен при лицензии PnSoft-PRO
Создание объекта "Территория"	Оператор в программе ParsecNET добавил новый объект в Редакторе топологии.
Изменение объекта "Территория"	Оператор в программе ParsecNET внес изменения в Редакторе топологии.
Удаление объекта "Территория"	Оператор в программе ParsecNET удалил объект в Редакторе топологии.
Создание объекта "Шаблон пропуска"	Оператор в программе ParsecNET добавил новый объект в Редакторе шаблонов печати.
Изменение объекта "Шаблон пропуска"	Оператор в программе ParsecNET внес изменения в объекте в Редакторе шаблонов печати.
Удаление объекта "Шаблон пропуска"	Оператор в программе ParsecNET удалил объект в Редакторе шаблонов печати.
Создание объекта "Расписание"	Оператор в программе ParsecNET добавил новое расписание в Редакторе расписаний.
Изменение объекта "Расписание"	Оператор в программе ParsecNET внес изменения в карточке расписания.
Удаление объекта "Расписание"	Оператор в программе ParsecNET удалил расписание в Редакторе расписаний.
Создание объекта "Заявка посетителя"	Оператор в программе ParsecNET в инструменте, в отдельной консоли или в web-интерфейсе "Бюро пропусков" создал заявку на пропуск для посетителя.
Изменение объекта "Заявка посетителя"	Оператор в программе ParsecNET в инструменте, в отдельной консоли, в web-интерфейсе "Бюро пропусков" или при помощи скрипта в Редакторе заданий внес изменения в заявку на пропуск для посетителя.

Удаление объекта "Заявка посетителя"	Оператор в программе ParsecNET в инструменте, в отдельной консоли "Бюро пропусков" или при помощи скрипта в Редакторе заданий удалил заявку на пропуск для посетителя. Заявка должна быть в статусе ниже "Согласована".
Создание объекта "Поправка рабочего времени"	Оператор в программе ParsecNET в редакторе "Поправки к рабочему времени" создал новую поправку к рабочему времени.
Изменение объекта "Поправка рабочего времени"	Оператор в программе ParsecNET в редакторе "Поправки к рабочему времени" изменил поправку к рабочему времени.
Удаление объекта "Поправка рабочего времени"	Оператор в программе ParsecNET в редакторе "Поправки к рабочему времени" удалил поправку к рабочему времени.
Создание объекта "Шаблон отчета по событиям системы"	Оператор в программе ParsecNET добавил новый шаблон отчета в редакторе "Отчеты по событиям".
Изменение объекта "Шаблон отчета по событиям системы"	Оператор в программе ParsecNET внес изменения в шаблон отчета по событиям системы.
Удаление объекта "Шаблон отчета по событиям системы"	Оператор в программе ParsecNET удалил шаблон отчета в редакторе "Отчеты по событиям".
Создание объекта "Идентификатор"	Оператор в программе ParsecNET в Редакторе персонала добавил новый идентификатор в карточке субъекта доступа.
Изменение объекта "Идентификатор"	Оператор в программе ParsecNET в Редакторе персонала внес изменения в карточке добавленного идентификатора.
Удаление объекта "Идентификатор"	Оператор в программе ParsecNET в Редакторе персонала удалил добавленный ранее не первичный идентификатор у одного из субъектов доступа.
Вход разрешен оператором	В модуле видео верификации при открывании турникета или двери на вход
Выход разрешен оператором	В модуле видео верификации при открывании турникета на выход
Проход разрешен оператором	Оператор в программе ParsecNET в окне видеоверификации разрешил проход (вход или выход) по карте.
Доступ запрещен оператором	Оператор в программе ParsecNET в окне видеоверификации запретил проход (вход или выход) по карте.
Нет реакции оператора	Оператор в программе ParsecNET никак не отреагировал на появления события о прикладывании идентификатора в модуле видео верификации при установленном флажке "Таймаут сессии".
Резервное копирование успешно завершено	Данное событие свидетельствует о том, что резервная копия базы данных ParsecNET успешно создана.
Резервное копирование не произведено, или произведено с ошибкой	Данное событие свидетельствует о том, что резервная копия базы данных ParsecNET не создана.
Экспорт данных успешно завершен	Данное событие свидетельствует о том, что загрузка персонала из ParsecNET в файл выполнена.
Экспорт данных не завершен из за ошибки	Данное событие свидетельствует о том, что загрузка персонала из ParsecNET в файл не выполнена, описание ошибки см. сообщение во всплывающем окне.

Изменена/назначена фотография	Субъекту доступа было добавлено фото, либо его фото было изменено.
Задание выполнено успешно	Задание запустилось в соответствии с заданными условиями, либо вручную.
Задание завершено с ошибками	Задание завершено с ошибками.
Действие задания выполнено успешно	Действия, запрограммированные в задании, выполнены успешно.
Действие задания завершено с ошибками	Во время выполнения действий, запрограммированных в задании, возникли ошибки.
Неуспешная попытка входа в систему	При попытке оператора войти в систему возникли ошибки (неправильно введен логин и/или пароль).
Отчет отправлен на печать	Сформированный отчет отправлен на печать.
Отчет сохранен в файл	Сформированный отчет сохранен в файл выбранного формата.
Отчет сформирован	Запрашиваемый оператором отчет сформирован.
Распознавание лиц и термометрия	
Вход без верификации по лицу	Вход в режиме "Идентификация по карте с необязательной верификацией по лицу"
Выход без верификации по лицу	Выход в режиме "Идентификация по карте с необязательной верификацией по лицу"
Субъект распознан по лицу	Событие формируется при успешной идентификации человека в случае включенного режима прохода "Идентификация по лицу" или "Идентификация по карте или лицу". Также это событие генерируется от IP-камеры в режиме распознавания лиц (система распознавания лиц Parsec).
Успешная верификация по лицу	Событие формируетсяя в случае включенного режима "Идентификация по карте с верификацией по лицу" после получения подтверждения на запрос ExternalAuthorization в случае успешной верификации субъекта доступа.
Верификация по лицу не пройдена»	Событие формируется в случае включенного режима "Идентификация по карте с верификацией по лицу" после получения отказа на запрос ExternalAuthorization.
Температура в норме	Событие формируется после проведения термометрии, когда человек распознан системой, и его температура ниже пороговой.
Нет входа – температура превышена	Событие формируется в случае отказа в доступе после проведения термометрии, когда человек распознан системой, но его температура выше пороговой.
Нет выхода – температура превышена	
Нет входа – детектор маски	Событие формируется в случае отказа в доступе при срабатывании детектора маски.
Нет выхода – детектор маски	
Домофоны BAS-IP	
Доступ разрешён - мастер код	Успешная идентификация по введенному мастер коду. Проход разрешен.
Доступ разрешён по карте	Успешная идентификация по считанной карте. Проход разрешен.

Доступ разрешён по команде с ПК	Точка прохода открыта командой прямого управления с ПК.
Доступ разрешён - лицо распознано	Успешная идентификация по лицу. Проход разрешен.
Доступ разрешен хостом вызова	Доступ открыт командой из точки назначения (например, нажатием на кнопку домофона в квартире).
Замок открыт по кнопке "Выход"	Замок открыт по нажатию кнопки выхода внутри охраняемого периметра (например, кнопки выхода из подъезда).
Аварийное открытие замка	Замок открыт по нажатию кнопки аварийного выхода.
Замок открыт по кнопке свободного доступа	Точка прохода открыта по нажатию кнопки свободного прохода на домофоне.
Доступ запрещен - идентификатор не найден	Предъявленный идентификатор не найден в БД. Доступ запрещен.
Доступ запрещен - не правильный код	Введенный код отсутствует в БД. Доступ запрещен.
Доступ запрещен - неизвестный	Лицо не распознано. Доступ запрещен.
Доступ запрещен - неизвестная карта	Предъявленная карта не имеет права прохода. Доступ запрещен.
Дверь оставлена открытой	Превышено время открытия замка.
Доступ разрешен - неизвестный идентификатор	Разрешен доступ идентификатору, присутствующему в БД домофона, но отсутствующему в БД ParsecNET 3.

16. Если вам надо...

Ниже вы найдете ответы на типовые вопросы по работе с системой. Вы можете использовать их для поиска более подробной информации по решению возникающих задач.

Быстро запустить небольшую систему

Для того, чтобы запустить небольшую систему (например, на 2-3 двери) вам потребуется всего несколько минут. Установите программное обеспечение сервера системы, подключите оборудование и следуйте инструкциям, приведенным в разделе Быстрый старт. Несколько несложных манипуляций за компьютером - и ваша система уже работает.

Подключить или сконфигурировать оборудование, настроить жесткий доступ или антипассбэк

Для этих целей служит Редактор оборудования. Подробно работа редактора рассмотрена в соответствующем разделе 62.

Редактор оборудования позволит вам:

- Подключить или удалить из системы контроллеры или рабочие станции
- Настроить все их параметры. Например, для контроллера доступа определить время работы замка, наличие периферии, такой, как дверной контакт или кнопка запроса на выход.

- Подключить настольные считыватели или заставить систему в качестве настольного считывателя использовать считыватель на одной из дверей для контроллера, подключенного к данному ПК.

При этом вы можете конфигурировать не только оборудование, подключенное к вашему ПК, но и к другим компьютерам системы.

В редакторе оборудования вы можете оперативно посмотреть статус выбранных устройств и их компонент - например, состояние дверного контакта выбранного контроллера, наличие сетевого питания и состояние аккумулятора источника питания контроллера.

Также редактор оборудования позволяет настроить специальные режимы работы, а именно:

- Проход под принуждением
- Запрет двойного прохода по одной карте или антипассбэк
- Режим жесткого доступа, разрешающий проход через двери только в определенном порядке.

О настройке данных режимов можно почитать в подразделе Специальные режимы прохода[159].

Ввести субъекта доступа и назначить ему права доступа

Права субъектов доступа в части прохода в те или иные помещения, возможность управлять определенными областями охраны определяются группой доступа, которая присвоена субъекту. Если нет ни одной группы доступа, то никто из субъектов доступа не получит никаких прав в системе.

Группы доступа создаются в Редакторе групп доступа[245]. В разделе Быстрый старт показано, как быстро создать хотя бы одну группу доступа для того, чтобы субъекты доступа начали ходить через двери.

Сами субъекты доступа создаются в Редакторе персонала[255]. Каждому субъекту необходимо, как минимум:

- Указать его фамилию. Имя и отчество не являются обязательными полями.
- Задать группу доступа (выбрать из имеющихся).
- Присвоить идентификатор (карточку), которой он будет пользоваться при проходах.

База данных субъектов доступа позволяет вести кадровый учет, поскольку вы можете для персонала специфицировать любое количество дополнительных полей, которые можно группировать (например, группа паспортных данных, группа данных автомобиля). Кроме того, поля можно типизировать, то есть определять, будет ли данное поле строкой, числом, датой. В дальнейшем это позволит легко организовать поиск персонала по выбранным полям.

Субъект доступа может иметь в базе данных фотографию, которая может использоваться при печати на его карточке, а также в Модуле видеоверификации[506].

Добавить оператора со специфическими правами

После установки системы в ней существует только один оператор с максимальными правами и паролем по-умолчанию. Во-первых, если вы хотите закрыть доступ к системе посторонним людям, ***смените поумолчательный пароль*** на другой.

Теперь, если вам надо дать доступ к системе еще кому-либо, причем ограничив его права, с помощью Редактора операторов[191] проделайте простые шаги:

- Создайте новую группу операторов
- Назначьте этой группе набор прав, который необходим

- Добавьте в эту группу оператора, задав ему имя и пароль.

Теперь новый оператор может входить в систему под своим именем и пользоваться теми инструментами и возможностями, которые вы ему дали при создании новой группы операторов.

Замечание: для упрощения входа в систему можно при создании оператора присвоить ему карту, и тогда вместо ручного ввода имени и пароля для входа в систему достаточно будет поднести карту к настольному считывателю.

Настроить рабочий экран специальным образом

Система позволяет для каждого оператора настроить вид его рабочего стола, в том числе разрешить или запретить оператору менять это внешний вид. Например, для охранника можно настроить монитор событий, который займет весь экран ПК, и при этом заблокировать изменение этого вида самим охранником.

Подробно о настройке внешнего вида пользовательского интерфейса можно прочитать в разделе Поведение окон программы 45.

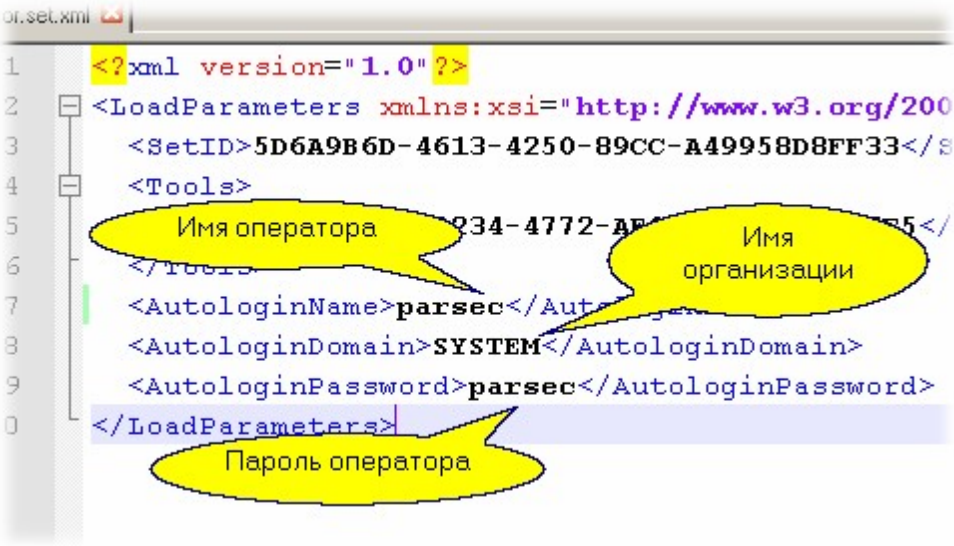
Обеспечить автоматический вход в систему

Иногда требуется обеспечить автоматический запуск системы вместе с запуском Windows, однако подстановка ссылки на приложение не позволит этого сделать, поскольку при старте приложения система запрашивает имя и пароль оператора. Данная задача решается с использованием автологина. Суть ее в следующем.

Для каждого приложения системы ParsecNET 3 имеется файл, определяющий при запуске конфигурацию приложения. Такие файлы имеют двойное расширение *.set.xml и расположены в установочной директории системы. по-умолчанию это директория

C:\Program Files\MDO\ParsecNET 3

Для того, чтобы, например, обеспечить автологин в мониторе событий системы необходимо взять файл ***monitor.set.xml*** и внести в него параметры, показанные на рисунке:



После сохранения файла запускаем монитор событий - вход систему произойдет без участия оператора.



Автологин снижает защищенность системы, поэтому настоятельно не рекомендуется использовать автологин с административными правами, а использовать его, например, на рабочем месте охранника или работника бюро пропусков.

Входить в систему по карте

Если вам не хочется каждый раз при входе в систему вводить имя оператора и пароль, то можно воспользоваться настольным считывателем. Для того, чтобы эта функция работала, требуется выполнение двух условий:

- Наличие в системе настольного считывателя, подключенного к конкретному компьютеру
- Присвоить оператору, помимо имени и пароля, карту, по которой будет осуществляться вход в систему.

После выполнения обоих условий при появлении начального диалога входа в систему вместо ввода имени и пароля вручную достаточно поднести карту к настольному считывателю, и загрузка приложения пройдет без ручного набора.

Подробнее о создании и редактировании оператора можно посмотреть в разделе Редактор операторов[191].

Озвучить транзакции в мониторе событий

Вы можете индивидуально озвучить любую из транзакций системы, сопоставив с транзакцией звуковой файл (типа WAV). Например, при транзакции прохода субъекта доступа компьютер может сообщить голосом "Пользователь вошел". Естественно, что соответствующие файлы вам надо подготовить самим.

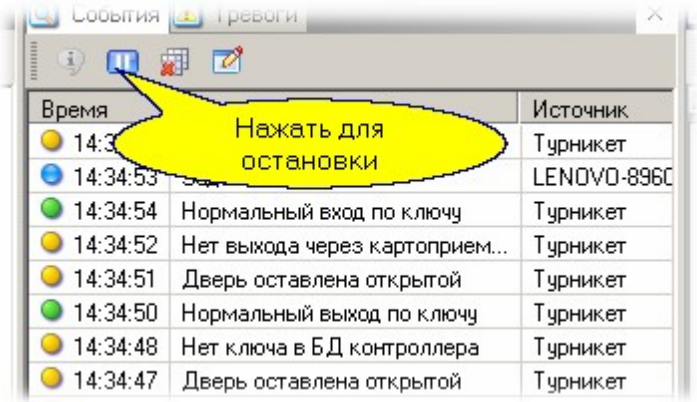
Для настройки озвучивания транзакций сделайте следующее:

Детально рассмотреть транзакцию в мониторе событий

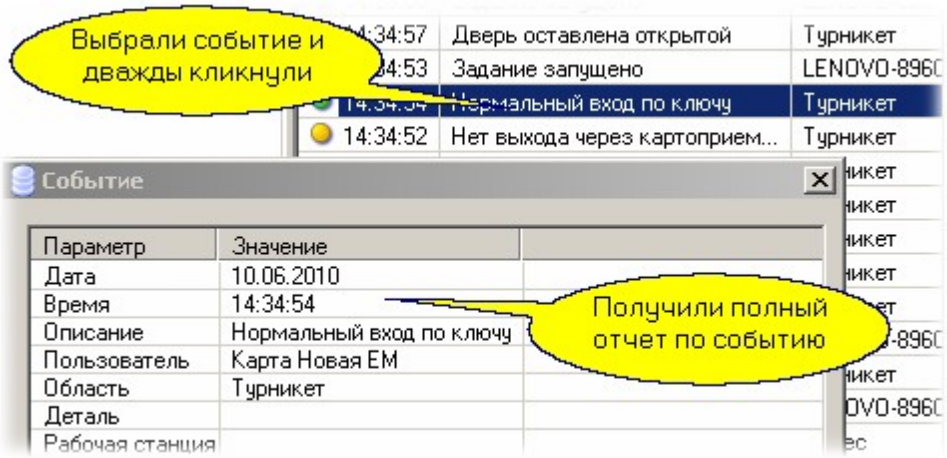
В крупных системах события в мониторе событий могут появляться достаточно быстро, и не всегда можно успеть рассмотреть детали интересующего вас события. Это, конечно, можно сделать потом с использованием генератора отчетов о событиях системы, но можно сделать и непосредственно в мониторе событий.

Для этого необходимо:

- Остановить прокрутку событий в мониторе событий (она будет остановлена на время, указанное в настройках окна событий монитора, по-умолчанию это 10 секунд). Для остановки следует нажать кнопку:



- Выбрать интересующее событие в списке событий и дважды щелкнуть по нему мышкой. В результате появится окно, в котором будут выведены все параметры выбранного события. События при этом могут продолжать поступать в монитор событий и отображаться независимо от состояния окна просмотра.



- После просмотра окно следует закрыть.

Настроить двухфакторную идентификацию

Для двухфакторной идентификации можно использовать терминалы биометрической идентификации[661] Uni Ubi и Hikvision (идентификация по лицу и карте) и некоторые сканеры отпечатков пальцев ZKTeco (идентификация по отпечатку пальца и карте[660])[654].

Кроме этого можно использовать соответствующую функциональность контроллеров NC-8000 и NC-60K/NC-60K.M, которые поддерживают двухфакторную идентификацию.

Для этого требуется подключить к контроллеру дополнительный выделенный считыватель (если проход в 2 стороны, то 2 считывателя).

Таким образом, в случае, например, двустороннего турникета с идентификацией по правилу карта+лицо и наличия контроллера NC-8000, нужно будет выполнить следующие шаги:

- подключить 2 считывателя PNR-P19 (или иные) на канал READER1. Если подключаются считыватели с интерфейсом Wiegand, используйте плату NI-TW;
- подключить 2 терминала через одну плату NI-TW (OMP-W02) на канал READER2;

- выставить перемычку на плате NC-8000 в положение раздельной работы двух каналов считывателей (см. Руководство по эксплуатации).

Также нужно правильно настроить контроллер в режиме двухфакторной идентификации. Обратите внимание, что при использовании терминалов биометрической идентификации Uni Ubi и Hikvision включать режимы с распознаванием лиц в настройках контроллера нельзя. Так как распознавание лиц происходит внутри терминалов, а Система получает от них только код пользователя, который уже проверяет на соответствие записи в своей БД. Распознавание лиц посредством функционала Системы осуществляется программными модулями, работающими через Parsec FR Onvif.

Иными словами, в случае использования терминалов биометрической идентификации Uni Ubi и Hikvision контроллер ничего о распознавании лиц не знает, для него терминал - это просто считыватель, который присылает код пользователя.

Такая схема позволяет также работать с картами Mifare в защищенных режимах (встроенные в терминал считыватели читают только UID без всякой защиты).

17. Контакты

Техническая поддержка:
Телефон для звонков по Москве и Московской обл.: **+7 (495) 565-31-12**

Бесплатный телефон для звонков по России: **+7 (800) 333-14-98**

Web: **www.support.parsec.ru**

E-mail: **support@parsec.ru**

Отдел технической поддержки работает в будни **с 8:00 до 20:00.**