Руководство Пользователя RusGuard Soft

Компания "RusGuard"

18.10.2017.

Оглавление

Общие сведения 6

Системные требования ... 8
История версий ... 10
Требования к квалификации пользователя ... 22
Используемые сокращения и термины ... 23

Установка ПО RusGuard и необходимых компонентов 25

Варианты конфигурации и установки ... 25
Состав программного комплекса и дистрибутив ... 27
Обязательные требования и рекомендации по установке ... 29
Установка сервера RusGuard ... 31
SQL-сервер не установлен ... 36
SQL-сервер установлен ... 39
Установка компонента Возможности рабочего стола ... 42
Установка SQL-сервера и настройка сервера отчетов ... 48
Установка АРМ и утилит RusGuard ... 61

Быстрый старт 65

АРМ RusGuard 76

Модуль Конфигурация оборудования ... 79
Поиск устройств для подключения ... 82
Редактирование CAN-адреса ... 85
Синхронизация устройств с БД ... 86
Управление контроллерами и конвертерами ... 87
Управление настройками контроллера ... 88
Настройка точки доступа ... 92
Настройка точки доступа типа "Шкафы/витрины" ... 115
Настройка интерфейса Rbus ... 119
Сервисные функции (управление контролером и точкой доступа) ... 121
Режимы индикации считывающего устройства ... 122
Ведение базы адресов электронной почты ... 125
Настройка и использование GSM-модема ... 129
Поиск устройств в модуле ... 133
Модуль Конфигурация СКУД ... 135
Модуль Конфигурация рабочих мест ... 155
Модуль Конфигурация системы ... 172
Ведение базы данных пользователей ... 172
Настройка длины ключа ... 178
Типы дней ... 178

Графики работы ... **181**
Рабочие зоны ... **190**
Реакции ... **193**
Метки ... **206**
Шаблоны пропусков ... **207**
Настройка Mifare ... **210**
Отчеты ... **214**
Стандартные отчеты ... **217**
Аудит действий операторов ... 217
Картотека сотрудников ... 219
Кто прописан в контроллер ... 220
Контроль посещаемости ... 221
Статистика проходов ... 222
Настраиваемые отчеты ... **224**
Опоздания за месяц ... 226
Отработанное время ... 228
Отработанное время (расширенный) ... 229
Системные события ... 230
Табель Т13 ... 233
Уход раньше времени за месяц ... 235
Управление шаблонами отчетов ... **236**
Модуль Планы ... **239**
Типы событий и их обозначение ... **244**
Статусы точек доступа ... **246**
Модуль Фотоидентификация ... **248**
Модуль Статистика ... **252**
Модуль "Табло посетителей" ... **255**
Мобильные приложения **256**
Типовые операции **257**
SQL не устанавливается автоматически ... **257**
Настройка подписок сервера Отчетов ... **257**
Настройка автозапуска ... **260**
Если изменено имя компьютера ... **262**
Настройка полномочий операторов при помощи меток ... **262**
Создание учетной записи оператора АРМ ... **263**
Создание учетной записи оператора АРМ (Мониторинг) ... **264**
Создание учетной записи оператора АРМ_2 ... **265**
Создание учетной записи сотрудника ... **267**
Подключение устройств ... **269**
Подключение устройств (существующий уровень доступа) ... **269**
Подключение устройств (новый уровень доступа) ... **271**
Настройка режима Запрета повторного входа ... **274**
Настройка доступа к отчетам через web-интерфейс ... **275**
Использование режима повторного приложения карточки ... **278**
Создание шаблонов пропусков и вывод на печать ... **281**

Проход по решению оператора ... 282
Настройка режима прохода по решению оператора ... 282
Использование режима прохода по решению оператора ... 282
Автоматическое распознавание документов ... 283
Настройка автоматического распознавания ... 283
Использование автоматического распознавания ... 283
Настройка реакции: запись видео на камеру Ivideon ... 285

Типичные ошибки и их исправление 286

Имя ПК задано кириллическими символами ... 286
Сервер недоступен ... 292
Не удается запустить ПО ... 293
Не удается загрузить модуль Отчеты ... 294
Не удается зайти на сервер отчетов ... 295
Некорректное отображение отработанного времени ... 297
Ошибка репозитория типов драйверов ... 298
Ошибка серверных служб ... 299
Ошибки при восстановлении резервной копии ... 300

Служебные программы и утилиты 301

Утилита RusGuard агент ... 301
Управление данными системы RusGuard ... 313
Сетевые настройки контроллеров ... 316
Расширенные сетевые настройки контроллеров ... 318
Сервисный конфигуратор оборудования ... 321
Обновление прошивки контроллера ... 331
Информация о системе ... 337
Универсальный импорт из файлов (утилита) ... 339
Рассылка отчетов (утилита) ... 343

Обслуживание ПО RusGuard Soft 348

Резервное копирование и восстановление БД ... 348
Удаление ПО RusGuard Soft ... 353
Обновление ПО RusGuard Soft ... 356
Настройка цветовой схемы ... 361
Обращение в службу поддержки RusGuard ... 361

Интеграции и установка стороннего ПО 363

Оборудование ИСО "Орион" (НВП Bolid) ... 363
Ivideon Video ... 378
Интеграция с видеорегистраторами Panasonic ... 389
ABBYY PassportReader SDK ... 390

Интеграция с 1С "БИТ" ... 393
Модуль Формула для учета рабочего времени ... 401
Интеграция с ISS ... 402

Периферийные устройства 407

Подключение считывателя Z-2 USB/USB MF ... 407
Подключение конвертера CAN-USB CAN-bus-USBnp Marathon ... 413
Подключение и настройка шлюза MOXA MGate MB3180 ... 420
Подключение считывателя ZKTeco ... 424
Подключение сетевого биометрического считывателя ... 425
Настройка контроллера ACS-102-CE (WF) с WiFi модулем MicRotic mAP2nD ... 434

Индекс 443

Общие сведения

Программное обеспечение RusGuard Soft - новейшая разработка специалистов компании "РусГард". Многосерверный принцип, примененный в ПО RusGuard, позволяет создавать единые интегрированные системы безопасности на объектах любой сложности и любого масштаба - от одного здания, до распределенных на региональном уровне крупных промышленных объектов.

Основные особенности ПО RusGuard Soft:

- Полный пакет ПО поставляется бесплатно;
- Количество контроллеров в системе – неограниченно;
- Количество пользователей в системе – неограниченно;
- Количество удаленных рабочих мест в системе – неограниченно;
- Полная поддержка всех современных операционных систем семейства Windows, как x32 так и x64 разрядных версий;
- Встроенный модуль автоматического распознавания документов;
- Интеграция в систему IP-камер с возможностью просмотра живого видео, записи архива и др.;
- Поддержка USB GSM модемов для отправки SMS;
- Большой набор интеграций с внешними системами: Bolid, ISS, ITV, 1c, VisitorControl и др.;
- Открытый пакет полного серверного API на базе стандартизированных технологий SOAP.

ПО RusGuard Soft создано в среде Microsoft Visual Studio 2015 (.NET 4.6) с использованием самых современных и передовых технологий в сфере разработки программного обеспечения, позволяющих совместно с техническими особенностями оборудования, создавать единую комбинированную систему, включающую в себя неограниченное количество серверов оборудования, локальных серверов БД и др., с организацией как локальных центров мониторинга, так и централизованных.

ПО RusGuard Soft постоянно развивается и обновляется, чтобы обеспечить выполнение новых задач, возникающих в сфере обеспечения безопасности. Полный пакет ПО, так же как и обновления, поставляется бесплатно.

Скачать полный пакет ПО RusGuard Soft

Внимание: перед использованием ПО RusGuard Soft ознакомьтесь с положениями Лицензионного соглашения.

Системные требования

Поддерживаемые ОС

Серверная часть

- Windows 7 with Service Pack 2 (Home Premium, Professional, Enterprise, Ultimate)
- Windows 8/8.1 (все редакции)
- Windows 10 (Pro, Enterprise). Для установки ПО на "N" версиях Windows 10 необходимо **вручную** скачать Media Feature Pack и установить его в системе. В противном случае возникает ошибка репозитория 298.
- Windows 2008 Server R2 (Web Edition, Standard, Enterprise, Datacenter)
- Windows 2012 Server/Windows 2012 Server R2 (все редакции)
- Windows 2016 Server

Предупреждение: Установка сервера RusGuard на ОС Windows 7 Starter (ST), Windows 7 Home Basic (HB) и Windows 10 Home не поддерживается.

Клиентская часть

- Все редакции Windows 7, Windows 2008 Server R2, Windows 8\8.1, Windows 10, Windows 2012 Server\2012 Server R2, Windows 2016 Server (Desktop Experience).

Примечание: Ввиду прекращения продаж ОС Windows 7, Windows 2008 Server R2, Windows 8 на новых объектах для сервера и АРМ рекомендуется использовать Windows 10 или Windows 2016 Server (Desktop Experience).

Минимальные системные требования для установки сервера RusGuard

- ЦП - Intel Core i3 или выше
- ОЗУ ≥ 4Гб
- Объем жесткого диска ≥100Гб
- Любая из поддерживаемых ОС

Минимальные требования для установки АРМ RusGuard

- ЦП - Intel Core i3 или выше
- ОЗУ ≥ 2Гб
- Объем жесткого диска ≥ 100Гб
- Любая из поддерживаемых ОС

Рекомендуемая системная конфигурация для сервера RusGuard

- ЦП - Intel Core i5
- ОЗУ ≥ 8Гб
- Объем жесткого диска ≥ 500Гб
- ОС – Windows 2016 Server (Desktop Experience)

Примечание: Приведены средние значения характеристик серверов. В конкретных системах, в особенности при больших нагрузках (свыше 100 контроллеров, более 10 АРМ, и т.д.) рекомендуется обратиться в службу технической поддержки для уточнения требований к серверу.

Поддерживаемые СУБД

- MS SQL Server 2014
- MS SQL Server 2016

Предупреждение: С версии 1.7.0 ПО RusGuard Soft прекращена поддержка MS SQL Server 2008 R2 и MS SQL Server 2012. Перед установкой обновлений ПО RusGuard Soft необходимо обновить установленную версию MS SQL Server. Инструкции по обновлению.

Примечание: Выбор редакции MS SQL Server (Express, Standart и др.) определяется нагрузкой на систему. При больших нагрузках (свыше 100 контроллеров, более 10 000 пользователей) рекомендуется обратиться в службу технической поддержки для уточнения рекомендованной редакции MS SQL Server.

История версий

Версия 1.11.1

1. Реализована возможность групповой смены ключей сотрудников.
2. Реализована возможность настройки цвета ячейки при использовании модуля Фотоидентификация 248.
3. Реализована возможность выбора типа добавочного поля.

Версия 1.11.0

Обновление интеграции с системой видеонаблюдения ISS

- Возможность размещения камер на планах в системе RusGuard. С планов возможет просмоттр как On-line видео, так и переход к архивным записям.
- Запуск записи определенных камер по любому событию в СКУД (настройка через реакции 193).
- Переход к связанному архивному видеофрагменту, записанному по реакции, из логов.

Работа с сотрудниками

- Возможность группового назначения\изменения индивидуальных уровней доступа выбранным сотрудникам, а также назначения\изменения сроков действия ключей выбранных сотрудников.
- Реализована возможность глобального поиска сотрудника\группы с позиционированием найденного в дереве групп без необходимости перехода в раздел ***Все сотрудники***.
- Реализована возможность глобального поиска (в независимости от нахождения в разделах модуля конфигурирования) сотрудника по считыванию карты с настольного считывателя и отображения карточки сотрудника.

Оборудование

Добавлены целый ряд настроек контроллеров, позволяющих более гибко конфигурировать оборудование для выполнения любых задач, в частности:

- Настройка цветовой схемы индикации считывателей.
- Настройка тактики звуковой сигнализации на считывателях.
- Настройки блокировки точки доступа при подборе кода.

Версия 1.10.0

Важно: Для установки этой версии рекомендуется использовать прошивку оборудования версии 3 или новее (прошивка и инструкция по ее обновлению распространяется вместе с дистрибутивом ПО).

4. Внедрен функционал для поддержки работы с защищенной областью памяти карт Mifare Plus и Classic 210.

Основные возможности

- Полная эмиссия карт из ПО RusGuard (требуется считыватель Z2-USB MF-RG);
- Работа с картами MF Classic 1K\4K\Mini и MF Plus S\SE\X\EV1 (эмиссия на уровень SL1 или SL3);
- Возможность эмиссии карт MF PLUS как с уровня SL0 на заданный, так и с уровня SL1 на SL3;
- Отсутствие мастер карты. Управление всеми ключами доступа считывателя к картам осуществляется централизованно с сервера;
- Гибкие настройки, позволяющие с легкостью заменять существующие карты на карты MF с последующим блокированием считывания иных карт;
- Возможность одновременного создания нескольких профилей (совокупность ключей доступа к карте, параметров расположения данных на карте и т.д.). Контроллер может обрабатывать до 5 профилей одновременно.

2. Разработан новый интерфейс работы со считывателями RDR-202-Multi - RBus 119

Возможности интерфейса:

- Работа (обмен данными и управление режимами индикации) по двухпроводной шине;
- Шифрованный протокол взаимодействия контроллера со считывателем;
- Возможность в онлайн режиме управлять разрешенными для чтения типами карт (отключать чтение любого из поддерживаемых считывателем RDR-202 форматов карт).

3. Внедрены дополнительные настройки для контроллеров:
   - Постановка на охрану по срабатыванию геркона;
   - Ручное управление каналами питания и их перезапуск;
   - Тактики исполнительных устройств: *Взлом*, *Оставлено открытым*.
4. В АРМ реализованы новые возможности:
   - Выбор цветовой схемы 361;
   - Групповое редактирование уровней доступа для сотрудников;
   - Звуковое оповещение в модуле планов;
5. В настройки контроллеров добавлена возможность выбора часового пояса его расположения. Теперь при построении распределенных систем с контроллерами в разных часовых поясах корректно отрабатывается функционал УРВ. Исправлены ошибки отображения времени в отчетах по УРВ.
6. В ***Архиве событий*** внедрена возможность сохранения шаблонов настроек (как в отчетах по УРВ).

7. Значительно расширен состав логируемых действий для отчета по Аудиту действий операторов.
8. Оптимизированы серверные процессы для уменьшения нагрузки на сервер при одновременной работе с большим количеством удаленных АРМ.
9. Обновлена интеграция с системой Ivideon 378, обеспечена поддержка последних версий Ivideon Server. Внедрена возможность просмотра архива недоступной камеры.

Версия 1.9.0

- Реализована интеграция с биометрическими терминалами, настольными биометрическими USB считывателями. Со списком поддерживаемого оборудования можно ознакомится на сайте http://www.rgsec.ru/biometriya;
- Добавлена поддержка нового контроллера с возможностью работы в режиме "Шкафы\Витрины 115".

Версия 1.8.0

Подробное описание версии:

- Добавлен редактор макетов пропусков Шаблоны пропусков 207. В нем вы можете создавать шаблоны пропусков, настраивая:
  - размер карточки;
  - фон (возможно использование фото из карточки сотрудника);
  - текст (возможна привязка полей из карточки сотрудника и дополнительных полей).

ПО поддерживает неограниченное количество пропусков, доступное количество зависит от типа лицензии.

- Создан модуль Табло посетителей, где в режиме реального времени отображается количество сотрудников и гостей, находящихся в пределах выбранной рабочей зоны.
- Обеспечена интеграция с NVR Panasonic 389 со СКУД RusGuard, которая позволяет:
  - просматривать online-видео с камер через модуль ***Планы***;
  - просматривать архивные записи;
  - настраивать реакции в системе (видеозапись любых событий СКУД) с возможностью их ассоциированного просмотра непосредственно из логов.
- Обеспечена возможность интеграции с любыми online SMS шлюзами.
- Обеспечена возможность сохранения цветного фото при использовании функции распознавания документов.

Кроме того, исправлена ошибка долгого обнаружения настольного считывателя при создании нового сотрудника.

Версия 1.7.2

Доработана отчетность по учету рабочего времени.

Версия 1.7.1

- В модуле Отчеты 214 добавлены два настраиваемых отчета: Отработанное время и Отработанное время (расширенный). Существенно увеличена скорость построения настраиваемых отчетов для баз с большим количеством сотрудников

Версия 1.7.0

Важно: Для установки этой версии рекомендуется использовать прошивку оборудования версии 1.85 или новее (прошивка и инструкция по ее обновлению распространяется вместе с дистрибутивом ПО).

1. Обеспечена полная поддержка возможности установки сервера и АРМ RusGuard на ОС Windows 10;
2. Существенно переработан модуль Отчеты 214.

В частности:

- Добавлены новые отчеты 214 по учету рабочего времени:
  - Табель Т13
  - Опоздания
  - Уход раньше времени
  - Табель сводный
- Добавлен новый отчет 214 "Картотека сотрудников"
- Изменен алгоритм выдачи прав операторам на доступ к модулю (доступ предоставляется только средствами АРМ в модуле Конфигурация системы 172, без необходимости дополнительной настройки прав пользователей ОС сервера, сервера Отчетов и т.д.);
- Добавлена возможность сохранения собственных вариантов (шаблонов настроек) отчетов "Системные события", "Табель Т13", "Опоздания", "Уход раньше времени". Количество пользовательских вариантов для каждого отчета в системе не ограничено;
- Переработан шаблон отчета "Отлучки", расширен спектр параметров учета, обеспечена возможность формировать сводную сокращенную версию отчета в конце;

3. При поиске сотрудника обеспечена возможность поиска по полному или частичному совпадению с критерием.
4. Обеспечена поддержка функции переноса слов для оптимального форматирования текстовых полей карточки сотрудников.
5. При настройке контроллера ACS-103 реализованы режимы "Блокировка" для двери, "Аварийное открытие" для турникета, "Контроль доп. платы защит" для турникета и др.

Версия 1.6.0

Подробное описание версии:

Важно: в связи с устранением ряда ошибок, а также добавления нового функционала в ПО и оборудование, при установке новой версии ПО необходимо обновить прошивку оборудования до вер. 1.80 (прошивка и инструкция по обновлению доступна вместе с дистрибутивом ПО).

1. При автоматической установке ПО RusGuard SQL Server 2008 Express заменен на SQL Server 2014 Express.
2. Добавлен гибкий функционал разграничения прав групп операторов на работу с сущностями системы (точки доступа, группы сотрудников, уровни доступа и др.). Введено понятие "Меток 206", которые привязываются к сущностям системы и группам пользователей (операторов). Соответственно оператор может видеть, редактировать и др. в системе только те сущности, метки которых есть в списке его группы. Количество присваиваемых меток каждой сущности неограниченно.
3. Добавлен функционал аудита действий операторов.
4. Модуль ***Отчеты*** 214:
   - Добавлен шаблон отчета ***Аудит действий*** операторов;
   - Обновлен шаблон отчета ***Системные события***. Время события стало выводиться с секундами.
5. В модуль АРМ ***Конфигурирование системы*** 172 перенесены функции редактирования дополнительных полей сотрудника и фотографий из дополнительной утилиты.
6. В АРМ реализована функция поиска в списке должностей при присваивании ее сотруднику.
7. Память контроллеров ACS-102 и ACS-103 расширена до 60 000 ключей.
8. Для контроллеров в режиме "Дверь" добавлен новый вход: кнопка Аварийного выхода.
9. В список поддерживаемых интерфейсов считывателей добавлены новые протоколы
10. Реализованы новые тактики исполнительных устройств: ***Индикация снятия с охраны 1*** и ***Индикация снятия с охраны 2***.
11. Добавлена поддержка точки доступа типа "Турникет" для контроллеров ACS-103.
12. Оптимизирована скорость обработки операций присвоения уровней доступа группам и добавления точки доступа в уровень доступа, при количестве сотрудников в группе более 100 000.
13. Оптимизирована скорость записи ключей в контролеры при их количестве более 100 000 (для контроллеров ACS-105-CE (10K) с памятью на 10 млн. ключей).
14. Изменен функционал добавления в Уровень доступа Точки доступа и Уровня доступа – Сотруднику\Группе. При добавлении в списке отображаются только не добавленные\не назначенные Точки доступа \ Уровни доступа.
15. Модуль ***Фотоидентификации*** 248:
    - новая логика режима “Проход по двум лицам”;

- устранена ошибка при работе с интегрированными IP камерами, при которой в окне видеоизображения выводилась надпись: “Достигнут конец”.

16. Измена текстовая формулировка событий для Заблокированных ключей
17. Также устранены следующие ошибки:
    - ошибка работы ПО с оборудованием при организации сети через NAT;
    - некорректное отображения времени изменения свойств сотрудника;
    - появление некорректных событий, событий с некорректным временем, а также событий “Нарушен срок действия ключа” и “Нарушено расписание” при действительных правах ключа.

Версия 1.5.0

Подробное описание версии:

1. Реализован новый модуль ***Статистика*** 252. Модуль выводит оперативную сводку по подключенному оборудованию и его состоянию.
2. Модуль ***Конфигурация СКУД*** 135:
    - реализована настройка ***Скрыть PIN код***;
    - изменена логика удаления Сотрудника\Группы и Точки доступа из Уровня доступа.
    - введены дополнительные контекстные меню при выборе Группы\Уровня доступа и Сотрудника\Точки доступа.
3. В редакторе фотографий добавлены предустановленные пропорции размеров вертикальной ориентации.
4. Модуль ***Планы*** 239:
    - возможность перехода из окна логов по двойному щелчку мышью на событие на план с устройством;
    - для устройств, показанных на нескольких планах, реализована возможность выведения списка для выбора нужного и перехода на него;
    - расширен функционал окна ***Список тревог***; вторая вкладка с плоским списком тревог, маркированных временем;
    - возможность управления всеми устройствами 243 на выбранном плане вызовом контекстного меню плана с командами управления из дерева планов.
5. Для модуля ***Фотоидентификация*** добавлено стандартное окно логов.
6. Во всех окнах логов событий добавлена возможность скопировать ***Имя устройства***.
7. Добавлена возможность автоматического запуска АРМ и аутентификации оператора после перезагрузки ПК.
8. Модуль ***Отчеты*** 214:
    - шаблон отчета ***Системные события*** позволяет вводить не только интервал дат, но и времени;

- создан новый шаблон отчета ***Отлучки расширенный*** с выводом как итоговой информации, таки и всех проходов сотрудника в течении суток.

9. Оптимизирована работа АРМ с количеством контроллеров более 2 000.
10. Изменения установщика:
    - устранен эффект "зависших консольных окон"
    - реализована обязательная проверка установленной .NET 4.5.2.
    - удалена возможность установки АРМ на WindowsXP
11. Прочие ошибки:
    - устранены ошибки модуля интеграции с ISS;
    - устранены ошибки редактирования рабочих графиков и зон.

Версия 1.4.0

Подробное описание версии:

1. Реализована интеграция с видеосистемой ISS. Функционал модуля интеграции позволяет строить в системе ISS полное дерево оборудования RusGuard для ручного и автоматического (посредством реакций, скриптов и макрокоманд) управления им из системы ISS. В ISS могут передаваться любые события из системы RusGuard для архивирования и их дальнейшей обработки, например, воспроизведения связанных видеофрагментов архивных записей;
2. Введено понятие срока действия уровня доступа. При присвоении уровня доступа сотруднику или группе можно задать срок его действия (до конкретного года, месяца, числа, часа, минуты). По истечении заданного срока данный уровень доступа автоматически удаляется у конкретного сотрудника или группы, у кого истек срок его действия. Один и тот же уровень доступа можно присвоить разным сотрудникам или группам с разным сроком действия.
3. Реализована возможность создания новой должности сотрудника непосредственно из окна выбора должностей без перехода в общий список.
4. В редакторе фотографий реализована возможность поворота изображения.
5. Набор фильтров для окна логов расширен возможностью выбора источника события.
6. В списках сотрудников появилась
7. Пиктограмма, отображающая факт наличия хотя бы одной присвоенной сотруднику фотографии.
8. Добавлен поиск в модуле конфигурирования оборудования (поиск по имени конвертеров, имени контроллеров, имени точек доступа). При полном или частичном совпадении происходит переход в дереве на найденное устройство.
9. Изменения в модуле ***Планы***:
    - поиск по имени плана, имени устройства на плане. При полном или частичном совпадении происходит переход в дереве планов на нужный.

- индикация тревожных планов, статистика по тревогам. При наличии тревог на планах отображается количество планов с устройствами в тревоге, а также предоставляется функционал быстрого перехода на план с устройствами в тревоге.

10. В модуле ***Конфигурация оборудования*** реализована возможность переименования IP конвертеров и присвоения им любого имени.
11. В настройки точки доступа типа "Дверь" реализована возможность настройки входа “Ручная блокировка”, т.е. при нарушении цепи точка доступа блокируется, проход возможен только по картам с определенными правами;
12. В настройки точки доступа типа "Турникет" добавлен функционал настройки входа “Внешнее разрешение”.
13. Расширен список тактик исполнительных устройств.
14. Доработан модуль интеграции с ОПС Болид: Переработан драйвер ОПС Болид в связи с выпуском нового преобразователя С2000-ПП вер. 1.2. Основная рекомендуемая для внедрения конфигурация: Пульт С2000М вер. 2.06, С2000-ПП вер. не ниже 1.23. Скачать новую прошивку для С2000-ПП.
15. Реализовано несколько новых шаблонов отчетов.
16. Реализована возможность создания рабочих графиков сотрудников и групп (графики для расчета отработанного времени и построения в автоматическом режиме дисциплинарных отчетов). Назначенные графики можно редактировать как в групповом режиме, так и вносить индивидуальные корректировки на уровне сотрудника (к примеру, связанные с командировками, болезнями и т.д). Рабочие графики можно создавать как вручную, так и используя автоматический механизм предустановок.

Версия 1.3.0

Подробное описание версии:

1. Интеграция сервера RusGuard с облачным сервисом **RusGuardCloud**.
2. Возможность ***Скрыть личные данные*** в настройках модуля АРМ ***Фотоидентификация*** 248.

Когда опция активна, в модуле ***Фотоидентификация*** отображается только фото и событие, без загрузки личных данных сотрудника.

3. Вывод количества сотрудников в группе.
4. Вывод статуса отправки тестового письма в учетной записи рассылки Email.

Версия 1.2.0

Подробное описание версии:

- Возможность настройки фильтра для отображения логов событий.

Настройки редактируются индивидуально для каждого созданного АРМ и сохраняются при перезагрузке ПО.

- Функция выбора тактики работы "Исполнительных устройств" в настройках контроллеров. Например, включение световой индикации в случае взятия под охрану охранной группы.

Версия 1.1.0

Подробное описание версии:

1. Интегрирован контроллер ACS-103-CE/C-DIN
2. Расширенная интеграция с видеоподсистемой Ivideon 378:
   - возможность просмотра видеоархива;
   - возможность записи видеофрагментов по реакциям на события в системе с последующим их просмотрам через логи произошедших событий.
3. Интеграция с оборудованием ИСО "Орион" (НВП Болид) 363:
   - добавление в систему разделов, зон и реле;
   - возможность назначить разделам и зонам тип датчиков (охранные: общий вид, ИК, геркон; пожарные: общий вид, дымовой, ИПР);
   - возможность прикрепить разделы, зоны и реле к планам, управлять и наблюдать состояния через модуль ***Планы*** 239 АРМ;
   - возможность просматривать события, относящиеся к разделам и зонам, из архива событий.

4. Возможность настройки ***Реакций*** 193 в модуле ***Конфигурация системы*** 172. При возникновении событий, удовлетворяющих определенным фильтрам, функция позволяет выполнять следующие типы действий в заданные промежутки времени:

4.1. Расписания. Поддерживается:

- глобальный список расписаний реакций;
- настройка в каждом расписании до 4 временных интервалов в течении суток.

4.2. Реакции. Поддерживается:

- возможность назначить расписание действия реакции;
- формирование списка событий и действий (количество не ограничено);
- подключение/отключение любых событий/действий существующей реакции с установкой признака активности;
- настройка порядка выполнения действий.

4.3. Список событий. Поддерживаемые типы:

- События от устройств. Настройки для срабатывания:
  - перечень устройств или все;
  - перечень событий или все;
  - набор конкретных сотрудников или групп сотрудников, сотрудников, которые должны участвовать в событии, либо любые известные сотрудники;

- срабатывать ли в случае событий, в которых фигурируют неизвестные системе сотрудники/карты.

4.4. Список действий. Поддерживаемые типы:

- Запись видео. Настройки:
  - камера, с которой следует осуществлять запись;
  - длительность записи в секундах.
- Отправка SMS. Настройки:
  - GSM модем;
  - отправка текста события или произвольного текста;
  - формирование списка сотрудников и групп сотрудников, которым следует отправить сообщение
  - возможность указать, что сообщение следует отправлять сотрудникам, участвовавшим в событии;
  - возможность выбрать, следует ли отправить сообщение на все телефонные номера, закрепленные за сотрудниками, или на какие-то конкретные. В последнем случае указывается перечень порядковых номеров телефонов сотрудников из их записных книжек.
- Отправка Email. Настройки:
  - адрес Email-рассылки, с которого будут рассылаться сообщения;
  - отправка текста события или произвольного текста
  - формирование списка сотрудников и групп сотрудников-адресатов;
  - возможность указать, что сообщение следует отправлять тем сотрудникам, участвовавшим в событии;
  - возможность выбрать, следует ли отправить сообщение на все email-адреса, закрепленные за сотрудниками, или на какие-то конкретные. В последнем случае указывается перечень порядковых номеров телефонов сотрудников из их записных книжек.
- Выполнение внешней программы. Данная реакция исполняется на сервере. Поэтому все пути должны соответствовать путям на сервере, хотя настройка выполняется в АРМ. Указываются:
  - полный путь к запускаемому файлу;
  - по желанию: полный путь к рабочему каталогу;
  - по желанию: аргументы.

5. Усовершенствована работа с архивом событий.

- возможность узнать, есть ли какие-либо дополнительные данные, связанные с событием (пиктограмма). Поддерживаемые данные:
  - видеоролик, связанный с событием, с возможностью просмотра.

Версия 1.0.4

Подробное описание версии:

1. Усовершенствована процедура установки:
   - Предусмотрена возможность установки вручную и экспресс-установки 31 с автоматической инсталляцией и настройкой MS SQL Server и Сервера отчетов (MS Reporting Services).
   - Добавлена возможность установки сервера RusGuard и удаленных АРМ на Windows 8 и Windows 2012 Server
2. Управление логами событий

   В утилите RusGuard агент 301 создана вкладка ***Управление событиями*** 310, которая позволяет:
   - Вручную удалить события, которые произошли до определенной даты
   - Настраивать автоматическое удаление событий, указав период времени, в течении которого события должны храниться, а также расписание удаления (раз в сутки, раз в неделю с указанием дня недели, раз в месяц (с указанием числа месяца)).
3. Ввод дополнительных данных сотрудников. Любое количество номеров телефонов и email-адресов
4. Усовершенствована работа с фотографиями сотрудников
   - Нефиксированное количество фотографий сотрудников;
   - Возможность формирования списка фотографий сотрудников с указанием имен и порядка отображения фото в утилите Управление данными системы RusGuard 313 (вкладка ***Редактор изображений***). Данные используются для формирования списка фотографий сотрудников, доступных оператору АРМ при редактировании данных сотрудника;
   - Для привязки фотографий к карточкам сотрудников теперь можно использовать не только загружаемые графические файлы, но и подключенные к АРМ сканеры и Web-камеры;
   - Редактирование фотографий:
     - изменение размера
     - яркость
     - регулировка контраста
     - кадрирование
5. Настройка списка дополнительных полей сотрудников:

В утилите Управление данными системы RusGuard 313 может быть задан произвольный список дополнительных полей сотрудников. Для этого требуется указать имя поля, тип данных (текст, целое число, дробное число, дата/время), обязательность заполнения, значение по умолчанию и порядок отображения полей.

В соответствии с этими настройками формируется список дополнительных полей доступных оператору АРМ при редактировании данных сотрудника.

6. Усовершенствована работа со списками сотрудников:
   - Поиск по полю ***Дополнительно*** карточек сотрудника;

- Просмотр доступных каждому сотруднику точек доступа, расписаний, операций с точками прохода при различных вариантах приложения карточки (блокировка, режим "открыть надолго" и т.д.).

7. Распознавание документов - при редактировании данных пользователя оператор может распознавать различные типы документов. Для распознавания используется подключенный к АРМ сканер или файл на диске, содержащий отсканированный ранее документ.

Поддерживаются следующие типы документов:

- Паспорт РФ (старого и нового образца)
- Водительское удостоверение (старого и нового образца)
- Загранпаспорт (старого и нового образца)

При распознавании из документа импортируется (и, при необходимости, сохраняется) следующая информация:

- Поля документа
- Изображение документа
- Фотография

8. Интеграция с подсистемой видеонаблюдения Ivideon 378:
   - Доступ к локальному серверу Ivideon из системы синхронизация камер;
   - Доступ к Личному кабинету пользователя системы Ivideon, синхронизация закрепленных за учетной записью пользователя личного кабинета удаленных серверов и привязанных к нему камер;
   - Возможность привязки камер к планам в модуле ***Планы*** 239 АРМ 239 и просмотра видео с них;
   - Возможность задать тип содержимого Камера для произвольного количества ячеек экрана в модуле ***Фотоидентификация*** 248 АРМ 248, а также указать, с какой камеры следует отображать видео.
9. Усовершенствован модуль ***Фотоидентификация*** 248 АРМ 248
   - При настройке модуля ***Фотоидентификация*** для тех ячеек, типом содержимого которых является ***Фотоидентификация***, теперь можно указать, какую конкретно фотографию посетителя отображать при проходе.

Требования к квалификации пользователя

В ПО RusGuard Soft предусмотрена удобная процедура экспресс установки 31, когда одновременно устанавливается (и развертывается) SQL-сервер, сервер RusGuard, а также, по необходимости, остальные компоненты программного комплекса. Процедура выполняется автоматически через стандартный установщик Windows и не требует специальных навыков. Квалификация системного администратора может потребоваться для настройки разветвленных архитектур, подразумевающих разнесение серверов БД, SQL-сервера и сервера RusGuard, а также большое число удаленных клиентов, на которых устанавливается АРМ RusGuard.

Условно можно выделить три типа пользователей программного комплекса:

Инсталлятор – пользователь, осуществляющий установку, развертывание и первоначальную настройку ПО RusGuard Soft. Эти действия требуют навыков администрирования ОС Windows и СУБД MS SQL на уровне “продвинутого пользователя ПК”.

Администратор – пользователь, осуществляющий расширенную настройку системы под конкретные требования, а также обеспечивающий её дальнейшее сопровождение. Для работы с простыми конфигурациями системы RusGuard администратору достаточно минимальных навыков администрирования ОС Windows (вариант экспресс установки). В сложных сетях, включающих несколько удаленных серверов и АРМ, требуются профессиональные навыки администрирования ОС Windows и СУБД MS SQL.

Оператор – пользователь, использующий установленную систему для выполнения своих служебных обязанностей: мониторинг, наблюдение, управление системой, выгрузка отчетов. Операторы системы проходят обучение работе с тем набором модулей системы RusGuard, к которым они имеют доступ.

Используемые сокращения и термины

Сокращения и аббревиатуры

SID - уникальный идентификатор контроллера, который формируется автоматически и не может быть изменен

АРМ - автоматизированное рабочее место

БД - база данных

ОС - операционная система

ОЗУ - оперативное запоминающее устройство, оперативная память

ПК - персональный компьютер

ПО - программное обеспечение

СКУД - система контроля и управления доступом

СУБД - система управления базами данных

УРВ - учет рабочего времени

ЦП - центральный процессор

Термины

Драйвер, *драйвер устройства* - интерактивный индикатор устройства, интегрированного в систему, управляемую ПО RusGuard. Отображается на планах, позволяет управлять устройством через АРМ.

Группа пользователей - элемент настройки системы. Позволяет группировать учетные записи пользователей АРМ RusGuard, исходя из их полномочий, назначать полномочия нескольким пользователям одновременно. Назначение прав осуществляется только на уровне Групп.

Модуль АРМ – компонент Рабочего места, выполняющий определенную функциональную нагрузку. Состав модулей, доступных для определенного Рабочего места определяется Администратором системы.

Пользователь - учетная запись пользователя (оператора, администратора) АРМ RusGuard, предоставляющая доступ к определенному набору рабочих мест.

План - графическая схема объекта с расположенными на ней драйверами устройств. Также существует "дерево планов" – иерархическое объединение отдельных Планов.

- вариант конфигурации интерфейса к АРМ RusGuard, настраиваемая администратором для различных групп операторов, в зависимости от их задач. Каждый тип рабочего места имеет собственный набор доступных модулей АРМ, либо различную конфигурацию одинаковых модулей.

Сотрудник - учетная запись лица, осуществляющего контролируемый системой доступ на оборудованный СКУД объект.

Событие - значимое для системы событие на точке доступа, регистрируемое средствами системы, сохраняемое в БД и доступное для построения отчетов. Например, вход, выход, взлом и т.д.

Точка доступа - точка, через которую сотрудники осуществляют доступ на объект и покидают его. На точках доступа устанавливаются устройства СКУД (контроллеры). Подключенные к системе контроллеры поддерживают четыре типа точек доступа: дверь, двойная дверь, турникет и шлагбаум (ворота).

Реакция - настраиваемое действие (обычно уведомление), которое выполняется системой по определенному пользователем графику ("расписанию") и определяется возникновением событий разного типа.

Установка ПО RusGuard и необходимых компонентов

Варианты конфигурации и установки

Варианты конфигурации и установки

Одно из преимуществ программного комплекса RusGuard Soft - гибкость настройки и возможность развертывания разных конфигураций, адаптированных под конкретную ИТ-инфраструктуру и решения определенных задач. В настоящем документе описываются стандартные варианты конфигурации и установки ПО RusGuard Soft.

Прежде чем приступить к установке ПО, необходимо определиться с вариантом развертывания.

Основные варианты конфигурации

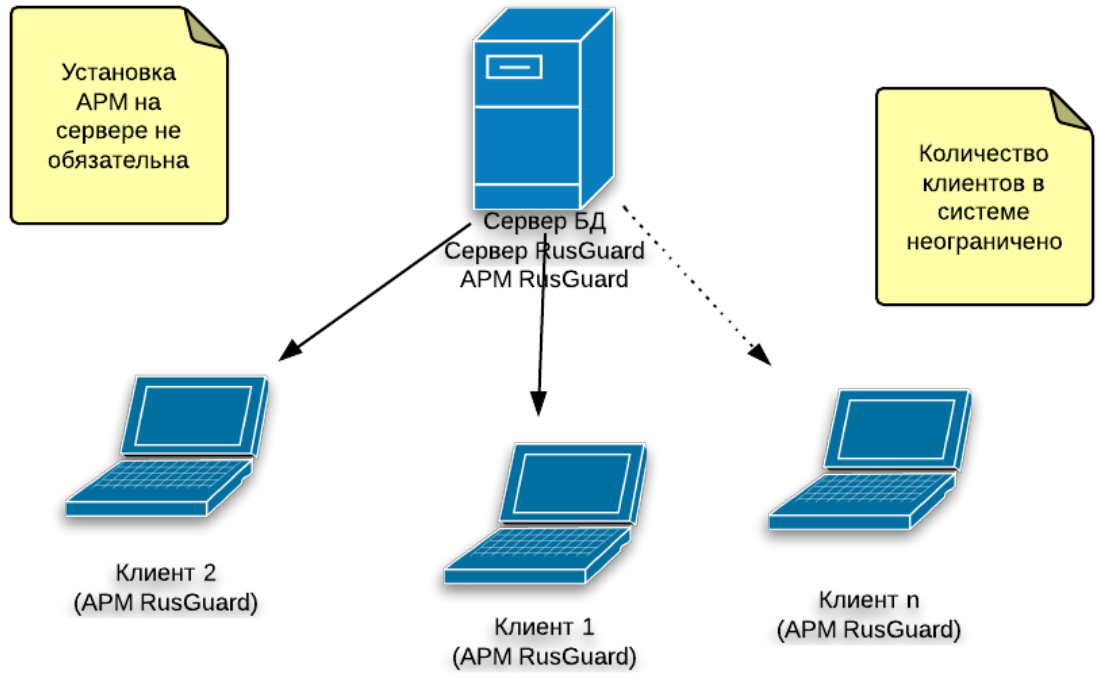


Рисунок 1 - Вариант конфигурации 1. Все элементы программного комплекса установлены на одном компьютере. Дополнительные клиенты настраиваются по необходимости

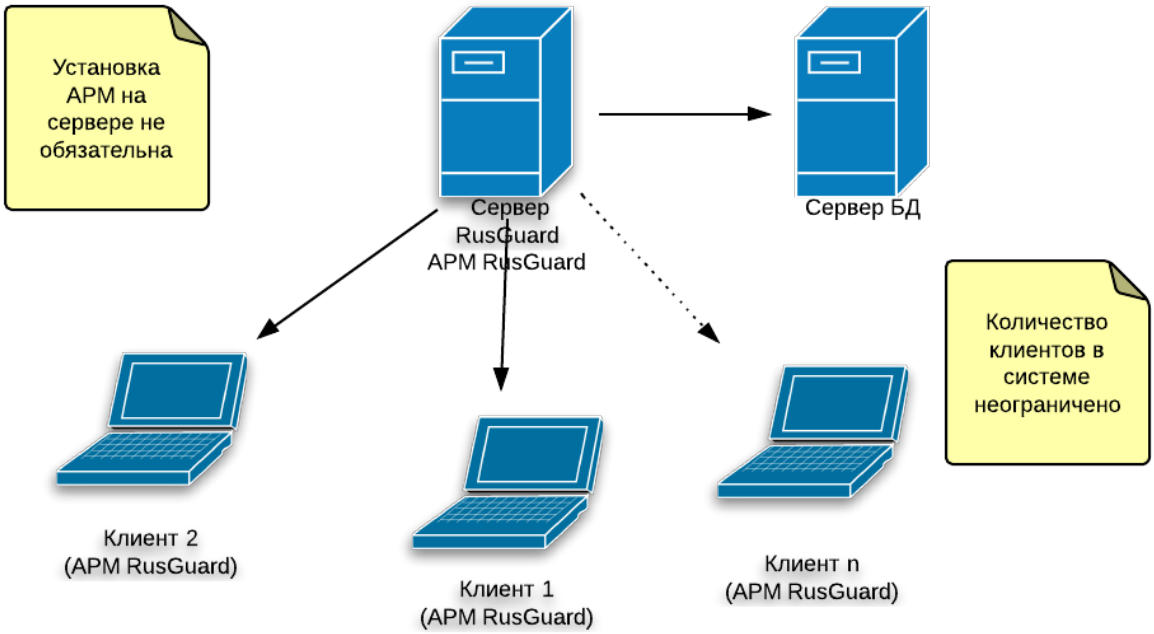


Рисунок 2 - Вариант конфигурации 2. Сервер БД развернут отдельно от сервера RusGuard. АРМ может быть установлено на сервере 1, а также на неограниченном числе клиентов

Основные варианты установки

Выбор варианта установки, прежде всего, зависит от желаемого состава программных компонентов ПО RusGuard Soft, устанавливаемых на определенный ПК. В первом случае при запуске установочного файла следует выбрать все элементы программного комплекса и запустить процесс инсталляции.

Во втором случае следует выбрать только те элементы, которые необходимо установить на конкретный сервер (сервер RusGuard) или клиент (АРМ, утилиты).

В зависимости от выбранной конфигурации развертывания ПО RusGuard Soft выбирается способ установки (или использования существующего) MS SQL Server:

- MS SQL Server устанавливается автоматически, на том же ПК, на котором устанавливается сервер RusGuard (см. рис. 1);
- MS SQL Server уже установлен на том же ПК, на котором устанавливается сервер RusGuard, или же установка (использование существующего) MS SQL Server производится на отдельный сервер (см. рис. 2).

Состав программного комплекса и дистрибутив

Состав программного комплекса

Программный комплекс состоит из следующих элементов:

Серверная часть (Сервер RusGuard)

Включает следующие системные службы (процессы):

- Сервер данных (`DataServer`)
- Сервер оборудования (`DeviceServer`)
- Координатор операций (`OperationCoordinator`)
- Брокер ресурсов (`ResourceBroker`)
- Диспетчер облака (`CloudDispatcher`)

АРМ, включающего следующие модули:

- Конфигурация оборудования 79
- Конфигурация СКУД 135
- Конфигурация рабочих мест 155
- Конфигурация системы 172
- Отчеты 214
- Планы 239
- Табло посетителей 255
- Фотоидентификация 248
- Статистика 252

Служебные программы и утилиты:

- RusGuard агент 301
- Управление данными системы RusGuard 313
- Сетевые настройки контроллеров 316
- Расширенные сетевые настройки контроллеров 318
- Сервисный конфигуратор оборудования 321
- Обновление прошивок оборудования 331

Во время использования программного комплекса может потребоваться подключение периферийных устройств:

- Универсального настольного считывателя Z-2 USB – RG 407

Состав дистрибутива

- Установочные файлы ПО RusGuard Soft
- Пакет пользовательской документации
- Дополнительное ПО и драйверы устройств (папка Redistributables)

- ABBYY PassportReader 390: драйвер ключа защиты и модуль распознавания документов
- Ivideon Video 378: модули видеосервера и удаленного клиента
- Z-2 Usb: драйверы для настольного считывателя Z-2 USB – RG 407
- Драйверы настолького биометрического считывателя ZkTeco USB Scaner 424
- Пакет установочных файлов для интеграции с Panasonic NVR 389

Примечания:

Дистрибутив MS SQL Server в редакции x86, а также его языковые редакции доступны на сайте компании Microsoft (файлы SQLEXPRADV_**_**).

Последние версии ПО RusGuard Soft, служебные программы и утилиты, а также обновленные прошивки для оборудования вы можете бесплатно скачать на сайте компании RusGuard.

Обязательные требования и рекомендации по установке

Таблица 1 - Требования к установке		
Значимость	Описание	Компонент
	Для корректной установки MS SQL Server на Windows 10, Windows Server 2014/2016 необходима установка компонента NetFramework 3.5. Установка выполняется через панель управления.	Серверная часть
	Перед установкой серверной части необходимо произвести обновление ОС. После установки обновлений необходимо перезагрузить ПК и повторно запустить поиск обновлений.	Серверная часть
	Некоторые из антивирусов могут блокировать установку требуемых системных компонент[1]. Отключите их на время установки ПО.	Серверная часть
	Для корректной работы всех сервисов и служб имя компьютера должно содержать только латинские символы (кириллические символы недопустимы). Если в имени компьютера содержатся кириллические символы, переименуйте его и перезагрузите ПК. **Внимание**: Крайне нежелательно использовать одинаковые имя пользователя и имя компьютера.	Серверная часть
	Установку серверной части рекомендуется производить на чистую ОС. Наличие пользовательских программ на сервере, таких как: ***торрент-клиенты, Skype[2], Firewall[3], а также других специализированных серверных WEB-приложений[4]***, использующих протоколы HTTP и HTTPS (***80 и 443 порты***), может привести к неработоспособности сервера RusGuard.	Серверная часть
	Перед установкой серверной части системы полностью сконфигурируйте ОС (если необходимо, измените те или иные параметры), задайте: • имя сервера • логин • пароль администратора системы (при использовании данной учетной записи при установке) • и т.д.	Серверная часть

Таблица 1 - Требования к установке		
	Изменение конфигурации ОС после установки сервера RusGuard нарушит его работу.	
	Чтобы предотвратить ошибки, не запускайте установку с сетевого ресурса. Скопируйте дистрибутив на локальный диск.	Серверная часть
	Установку серверной части RusGuard Soft рекомендуется производить на ПК, не входящем в домен. После успешной установки всех компонентов ПО ПК можно добавлять в домен.	Серверная часть
	Установку системы необходимо запускать от имени локального Администратора ОС .	Все элементы
	Отключите Брандмауэр Windows (***Пуск > Панель управления > Брандмауэр Windows***)[2].	Серверная часть

 - необходимое требование.

 - рекомендация.

Примечания к таблице

1. Антивирус ESET NOD32 блокирует установку модуля: RusGuard\Memcached\Memcached64\ServiceEx.exe.
2. Если в Skype включено "Использовать порты 80 и 443 в качестве входящих альтернативных", это может нарушить функционирование сервера RusGuard. Чтобы это отключить, в главном меню программы выберите пункт ***Инструменты > Настройки…***, в группе ***Дополнительно*** выберите пункт ***Соединение*** и снимите флаг ***Использовать порты 80 и 443 в качестве входящих альтернативных***. Перезапустите Skype.
3. Для подключения к серверу RusGuard, удаленные клиенты используют HTTP и HTTPS протоколы (80 и 443 порты на сервере). Включенный Брандмауэр Windows (с настройками по умолчанию), а также ряд других Firewall и антивирусов со встроенными модулями Firewall могут блокировать данные подключения, что приведет к невозможности установки соединения АРМ с сервером. При необходимости использования данных программ, обратитесь к системному администратору для их настройки.
4. Установка другого специализированного ПО, использующего технологии WEB сервисов, после установленного сервера RusGuard может изменить системные настройки и привязки протоколов HTTP и HTTPS (80 и 443 порты), что приведет к неработоспособности сервера RusGuard. В случае необходимости развертывания подобных систем на одном ПК с сервером RusGuard обратитесь к системному администратору.

Установка сервера RusGuard

Предварительные действия

Перед установкой **необходимо** выполнить следующие действия

- ознакомиться с требованиями и рекомендациями по установке 29.
- обновить ОС, а затем перезагрузить ПК и повторно запустить поиск обновлений.
- кроме того, если используется ОС Windows 2016 Server убедитесь, что установлена редакция с поддержкой компонент рабочего стола (Desktop Experience) (см. рис. 3). Данный вариант установки выбирается при развертывании ОС, далее его активизировать невозможно.

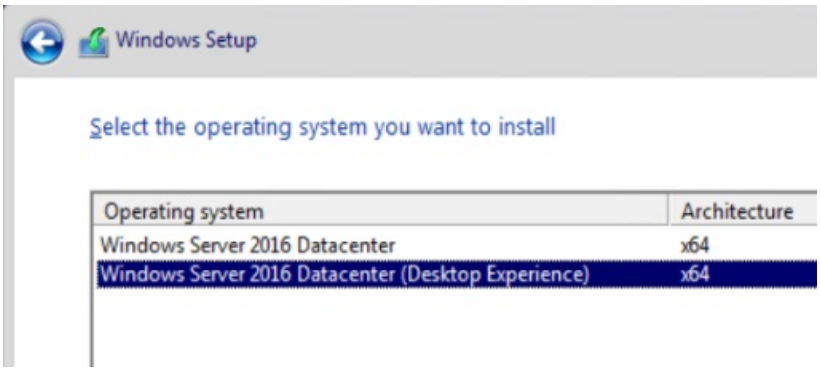


Рисунок 3 - Настройка компонентов Desktop Experience

Для того чтобы установить сервер RusGuard:

1. Зайдите в каталог, где хранится дистрибутив RusGuard Soft (это может быть папка на компьютере или компакт-диск).
2. Запустите установочный файл setup.exe двойным щелчком мыши по пиктограмме . Обратите внимание, что начинать установку следует от имени локального Администратора (см. рис. 4).

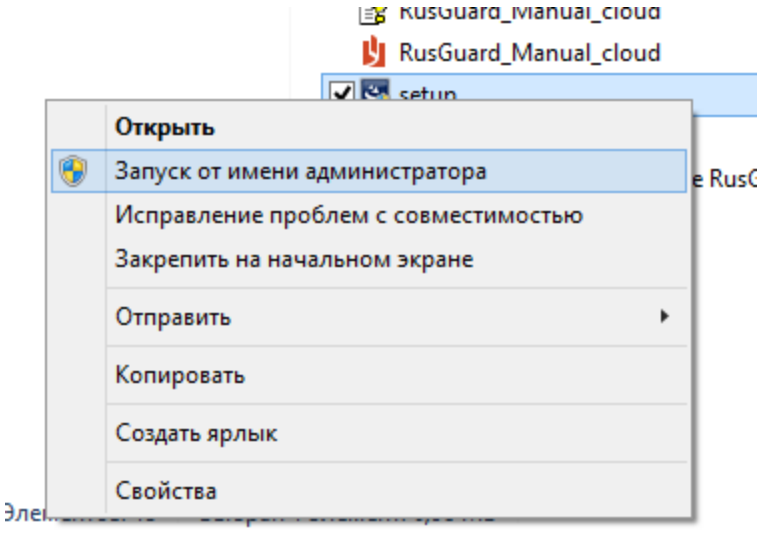


Рисунок 4 - Запуск от имени локального Администратора

Система автоматически запустит пошаговый процесс установки. Процесс достаточно прозрачен и стандартен. Шаги описаны ниже.

Вначале загружается экран приветствия, происходит автоматическая проверка прав текущего пользователя.

Здесь и далее:

- Для перехода к следующему шагу используйте кнопку Далее >.
- Для возврата к предыдущему шагу используйте кнопку < Назад.
- Для выхода из мастера установки используйте кнопку Отмена.

Если на ПК уже было установлено ПО RusGuard, мастер установки предложит сначала удалить его, а затем установить ПО заново. Настройки подключения и БД при этом сохраняются.

3. Мастер установки предложит ознакомиться с условиями лицензионного соглашения. Чтобы продолжить процесс, необходимо активировать пункт ***Я принимаю условия лицензионного соглашения***. Только после этого переход к следующему этапу станет возможен.

Вы также можете распечатать лицензионное соглашение.

4. Затем Мастер установки сообщает путь к папке, в которой по умолчанию будет установлено ПО (см. рис. 5). Вы можете указать другой путь (кнопка Изменить...).

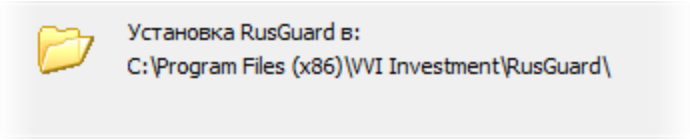


Рисунок 5 - Путь к папке, где по умолчанию устанавливается ПО

5. Мастер установки проверит наличие компонент IIS, NET.Framework 4.6 и компонента Visual C++ 2015 Update 1. Не обнаружив компоненты на локальном ПК, мастер выполняет их установку из дистрибутивного пакета.

Если на ПК уже установлена более новая версия компонента Visual C++ 2015 Update 1, отображается сообщение об ошибке. Игнорируйте его и продолжайте выполнять процедуру согласно подсказкам Мастера установки (см. рис. 6).

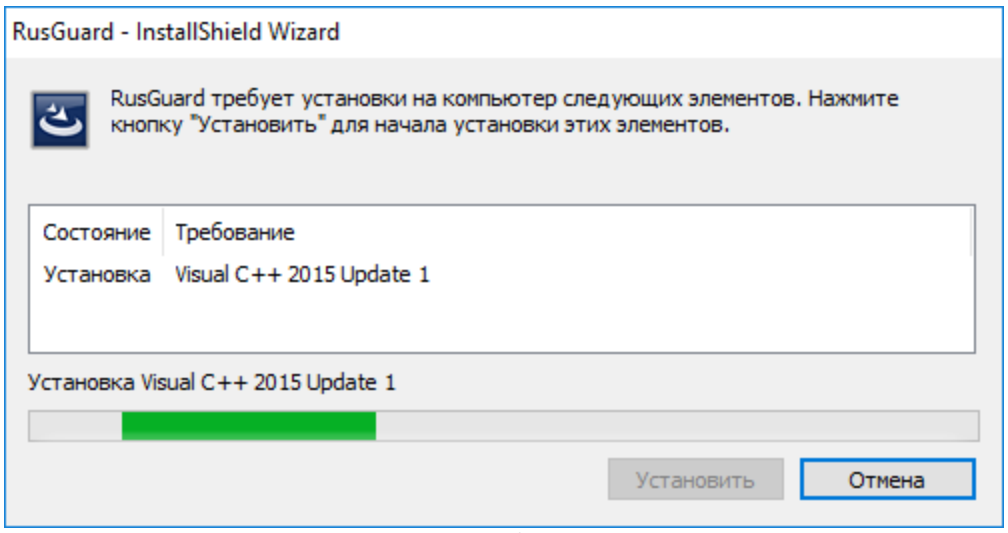


Рисунок 6 - Установка необходимых компонентов

Внимание: После установки компонент система может потребовать перезагрузить ПК. Обязательно выполните перезагрузку, если после этого установка не возобновится автоматически, необходимо запустить процесс заново.

6. Далее необходимо выбрать, какие компоненты ПО будут установлены (см. также Варианты конфигурации и установки 25).

По умолчанию не выбран ни один компонент. Чтобы разрешить установку требуемых компонентов нажмите на кнопку  возле названия нужного компонента и в раскрывшемся контекстном меню разрешите его установку. Для установки серверной части выберите Сервер RusGuard (см. рис. 7).

Примечание: Другие компоненты ПО RusGuard Soft также могут быть установлены одновременно с серверной частью, если это необходимо для выбранной конфигурации. Это никак не повлияет на инсталляцию SQL-сервера и серверной части ПО RusGuard.

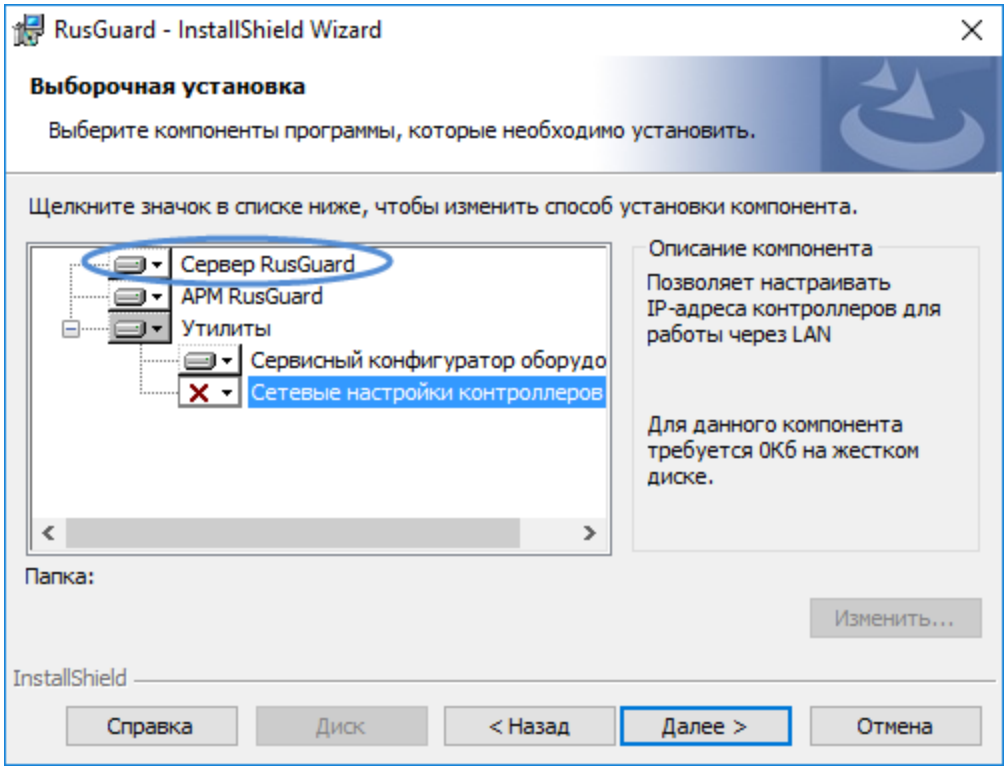
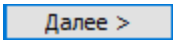


Рисунок 7 - Выбор элементов ПО для установки. На рисунке показан вариант, когда выбрана установка только сервера Rus Guard

7. На следующем этапе выполняется автоматическая проверка выполнения предварительных требований к установке. Если все они выполнены, вы сможете сразу перейти к следующему шагу.

Обратите внимание, что после нажатия на кнопку 

необходимо немного подождать: выполняется конфигурация сторонних компонентов (IIS и .NET Framework 4.6) (см. рис. 8).

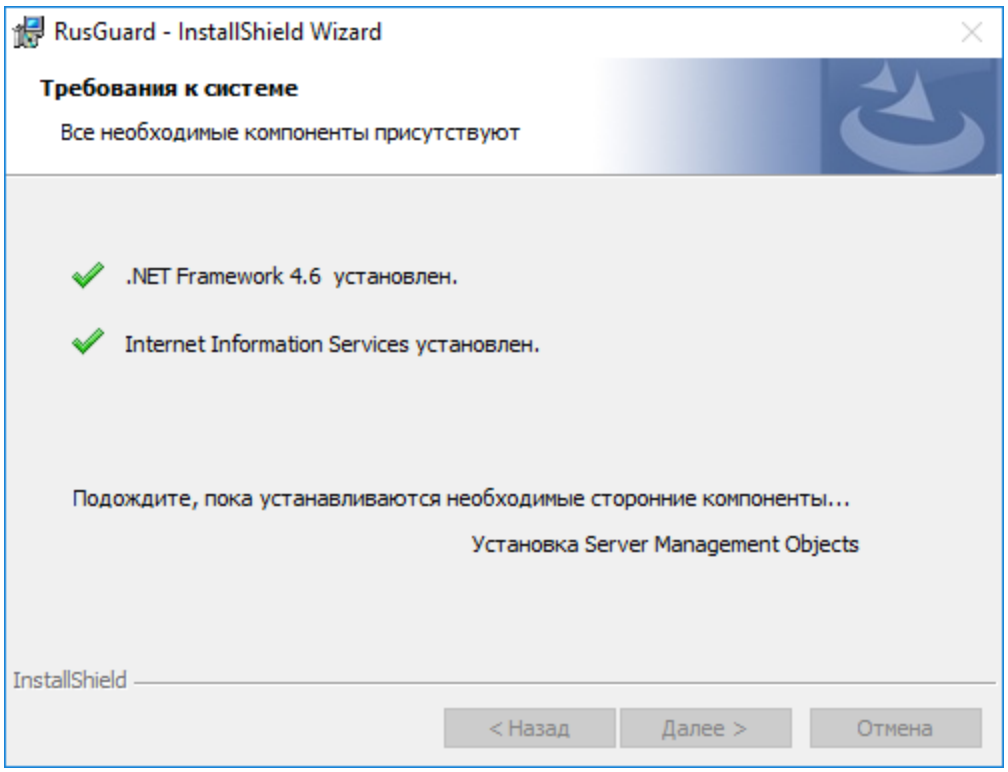


Рисунок 8 - Установка и конфигурирование необходимых компонентов

Когда все необходимые компоненты обнаружены и сконфигурированы, установку можно продолжить.

При запуске процесса установки возникает дополнительное окно с черным фоном. Это начинает работать средство командной строки для обработки образа диска (дистрибутива) DISM.exe (см. рис. 9). Процесс выполняется автоматически. **От пользователя не требуется никаких дополнительных действий**.

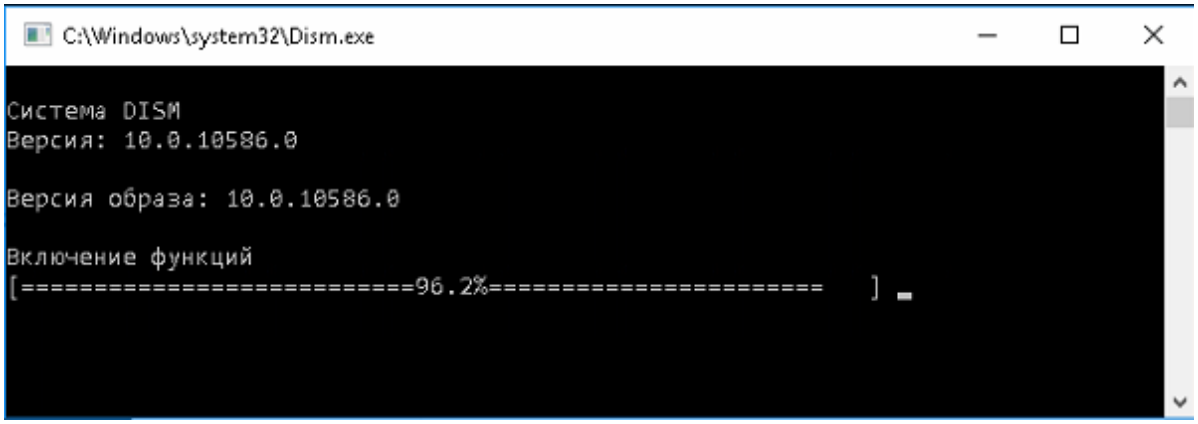


Рисунок 9 - Процесс обработки образа диска средством DISM.exe

8. В следующем окне выбирается режим установки сервера RusGuard в зависимости от наличия/отсутствия установленного ранее SQL-сервера (см. рис. 10).

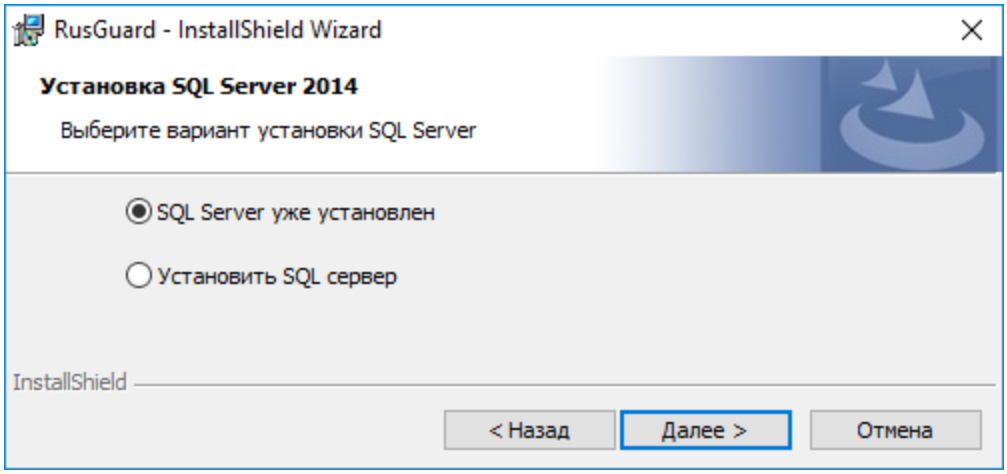


Рисунок 10 - Выбор режима установки

Выберите нужный вариант и перейдите к следующему шагу. Дальнейшая процедура установки зависит от выбранного варианта. Обратитесь к соответствующему разделу Руководства ниже.

SQL-сервер не установлен

Начало процедуры см. в разделе Установка сервера RusGuard. 31

Для того чтобы установить SQL-сервер одновременно с сервером RusGuard:

1. На восьмом шаге установки выберите пункт ***Установить SQL-сервер***.
2. Введите пароль администратора SQL-сервера. (см. рис. 11).

Требования к паролю связаны с настройками конкретной системы Windows и их список не всегда отображается установщиком.

Имя пользователя администратора SQL-сервера по умолчанию "**sa**".

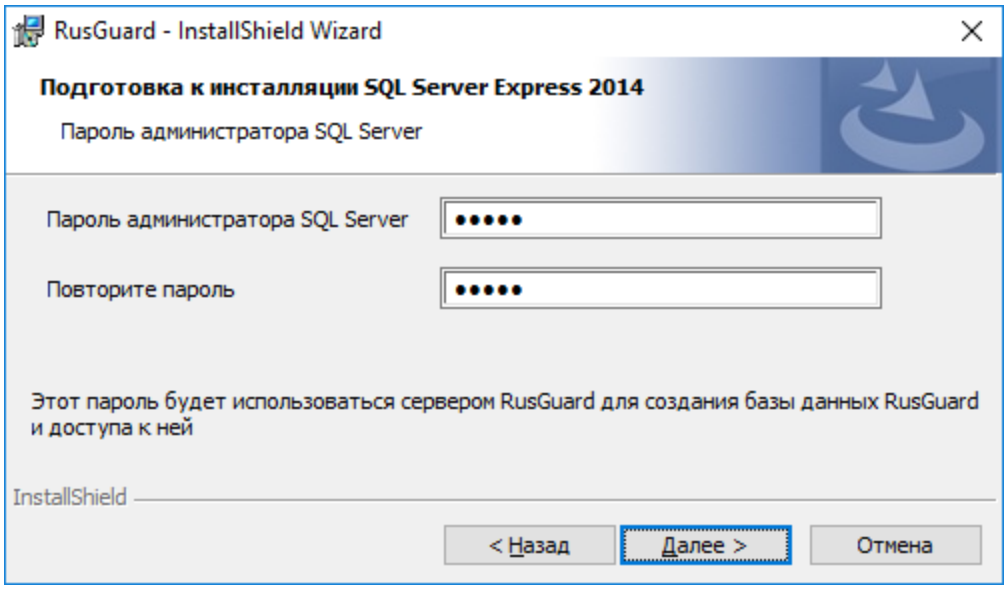


Рисунок 11 - Ввод пароля администратора SQL-сервера

3. В следующем шаге необходимо ввести данные учетной записи Windows, которая будет использоваться для запуска служб SQL-сервера (см. рис. 12).

Вы можете ввести учетные данные администратора или любого пользователя, даже если он не работает на данном ПК (или в домене). Требования к паролю аналогичны требованиям, приведенным в предыдущем шаге (определяются настройками ОС).

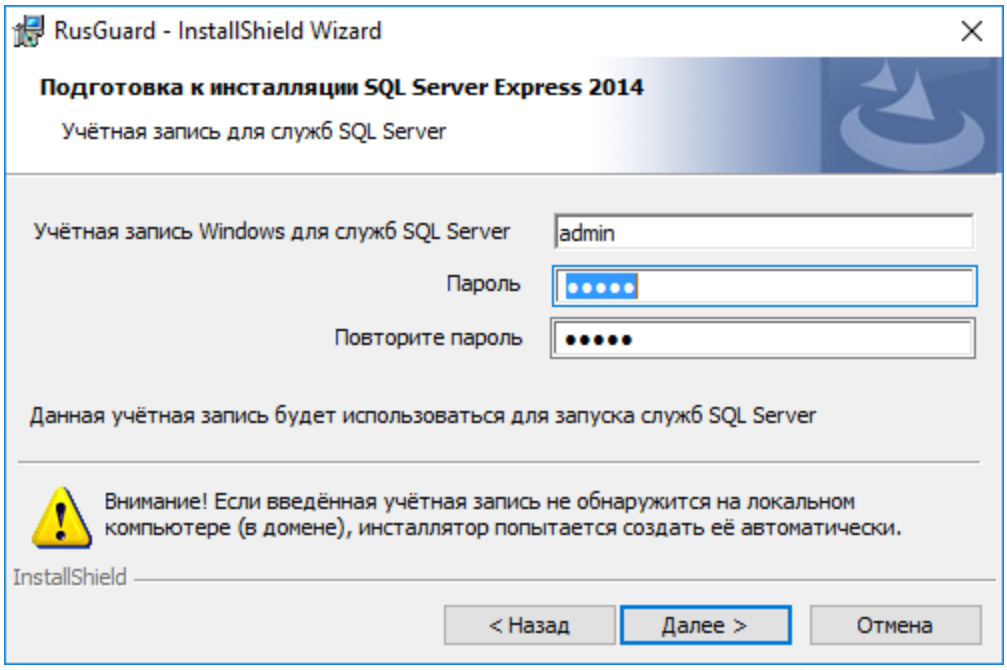


Рисунок 12 - Ввод учетных данных пользователя Windows для запуска служб SQL-сервера

4. В следующем окне вводится (создается) учетная запись администратора сервера отчетов. Вы можете ввести те же учетные данные, что были использованы в предыдущем шаге (см. рис. 13).

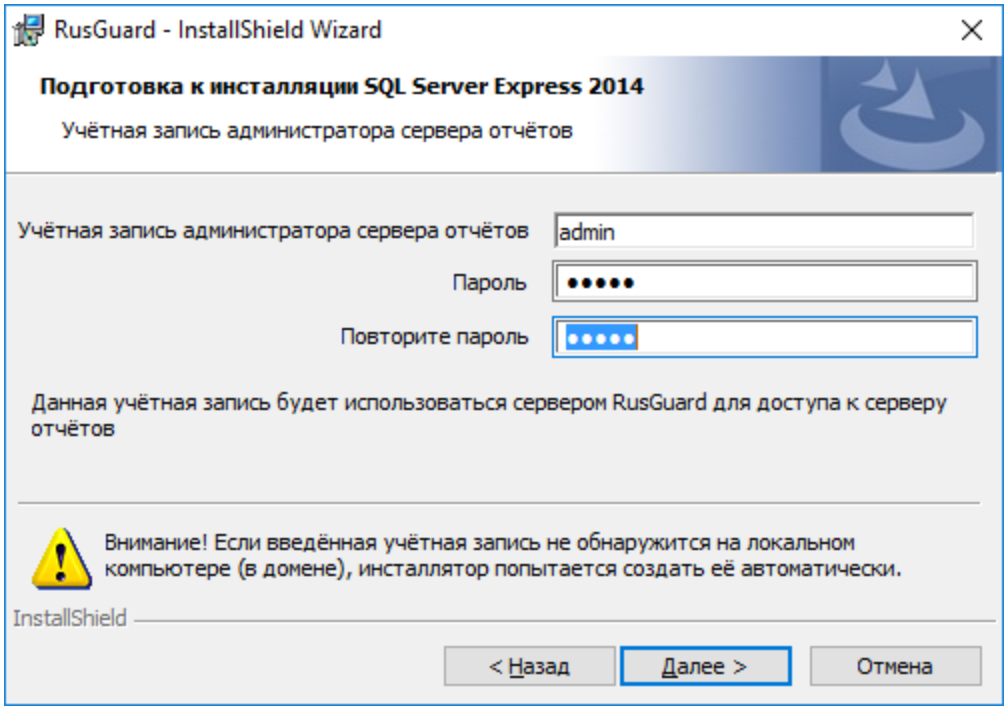


Рисунок 13 - Ввод учетных данных пользователя Windows для администрирования сервера отчетов

Примечание: Если ПО RusGuard было ранее установлено на ПК, а затем удалено, все формы ввода учетных данных (для SQL-сервера и сервера отчетов) будут заполнены автоматически теми данными, которые использовались ранее.

5. После ввода учетных данных администратора сервера отчетов начинается автоматическая установка SQL-сервера.

В случае возникновения ошибок на данном этапе рекомендуется выполнить установку SQL-сервера вручную 48, а затем установить ПО RusGuard.

6. Если установка осуществлена без сбоев и ошибок, мастер установки автоматически загружает следующий экран с сообщением о том, какие компоненты ПО RusGuard будут установлены. Это может быть только Сервер RusGuard или Сервер RusGuard в сочетании с любыми другими компонентами программного комплекса (см. также раздел Установка АРМ и утилит RusGuard 61).

7. Нажмите на кнопку Установить, чтобы запустить процесс установки ПО RusGuard.

Мастер установки приступит к инсталляции. В случае успешного ее завершения отобразится соответствующее сообщение.

8. Прежде чем выйти из мастера установки, пользователь может сохранить данные о процессе установки , а также вызывать журнал установщика. Чтобы завершить процесс, нажмите на кнопку Готово.

Примечание: При установке Сервера RusGuard автоматически устанавливается утилита RusGuard Agent. Эта утилита позволяет осуществлять оперативный мониторинг и

управление серверными процессами. Подробнее о функциях и использовании утилиты см. в разделе "Служебные программы и утилиты" > "Утилита RusGuard агент" 301.

Внимание: При установке новой версии ПО RusGuard (обновлении) возможен конфликт версии ПО и БД, может потребоваться обновление БД 356.

SQL-сервер установлен

Начало процедуры см. в разделе Установка сервера RusGuard. 31

Этот вариант установки, как правило, используется в сложных архитектурах, подразумевающих разнесение сервера БД, сервера RusGuard и клиента (клиентов) с АРМ (см. варианты конфигурации 25).

Для того чтобы установить Сервер RusGuard с SQL-сервером, установленном на этом же ПК, либо развернутом на отдельном ПК:

1. На восьмом шаге установки ПО выберите пункт ***SQL-сервер уже установлен***.

Обратите внимание, что если ранее был установлен SQL-сервер версии 2008 или 2012, необходимо обновить его до версии 2014. В противном случае установка ПО невозможна. Отобразится соответствующее сообщение .

Как и в процедуре установки Сервера RusGuard в конфигурации, где SQL-сервера еще нет, установщик потребует ввести учетную запись администратора SQL-сервера для создания БД RusGuard, а также учетную запись администратора на сервере отчетов (см. рис. 14 и 15).

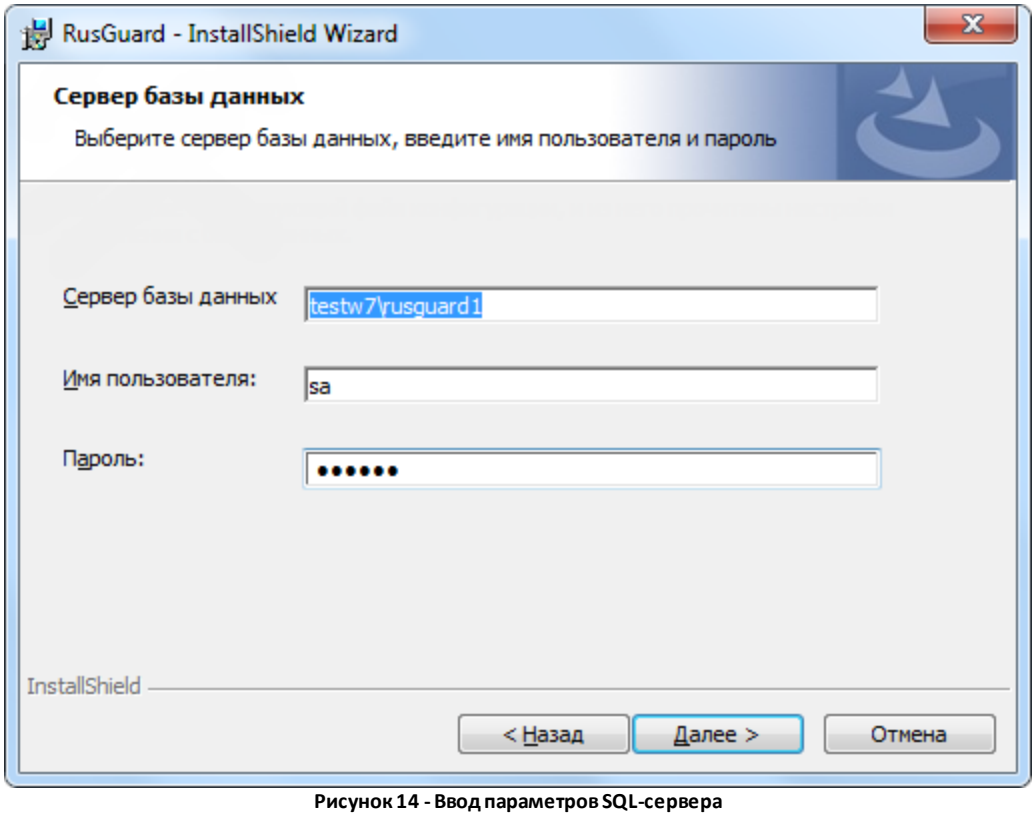


Рисунок 14 - Ввод параметров SQL-сервера

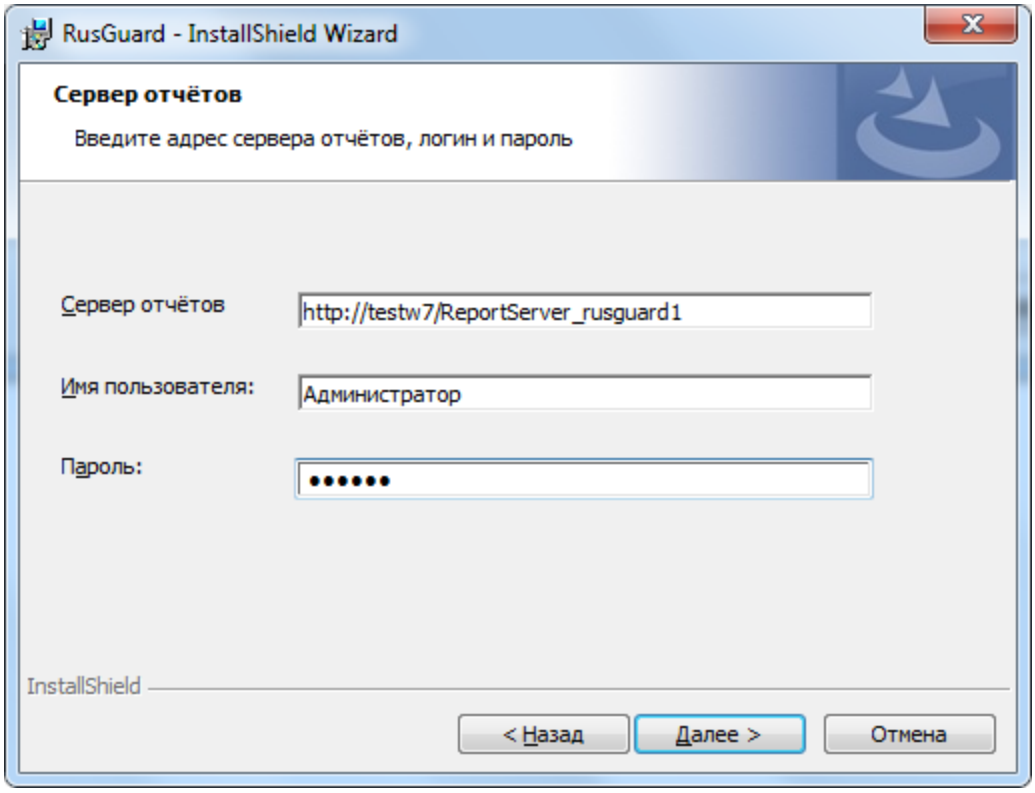


Рисунок 15 - Ввод параметров Сервера отчетов

Примечание: Если ПО RusGuard было ранее установлено на ПК, а затем удалено, все формы ввода учетных данных (для SQL-сервера и сервера отчетов) будут заполнены автоматически теми данными, которые использовались ранее).

2. Введите имена и пароли, соответствующие учетным записям для каждой из форм установщика (см. табл. 2 и 3).

Таблица 2 - Ввод адреса сервера БД и учетных данных администратора	
Поле	Значение и требования к заполнению

Сервер базы данных	Адрес сервера БД, формируемый по следующему правилу:
	`[Имя компьютера]\[Название экземпляра]`
	Если сервер RusGuard и сервер БД развертываются на одном компьютере, адрес примет вид:
	`.\[Название экземпляра]`
	Значение параметра "Название экземпляра" зависит от типа экземпляра SQL Server ("Экземпляр по умолчанию", "Именованный экземпляр"), выбранного при его установке.
	Примеры:
	`.\SqlExpress` – подключение к локальному SQL-серверу с именем инстанса SqlExpress

Таблица 2 - Ввод адреса сервера БД и учетных данных администратора	
	`ServerSQL` – подключение к удаленному SQL-серверу (ServerSQL) с пустым именем инстанса
Имя пользователя	sa (от "super administrator")
Пароль	Пароль, заданный при установке сервера RusGuard (если устанавливался одновременно с SQL-сервером), либо при установке SQL-сервера (если конфигурация подразумевает его самостоятельную установку).

Таблица 3 - Формат ввода адреса сервера отчетов	
Поле	Формат заполнения
Сервер отчетов	`http://Имя сервера отчетов/ReportServer_Имя инстанса SQL` **Примеры**: `http://ServerSQL /ReportServer_SqlExpress` – подключение к серверу отчетов (ServerSQL) с именем инстанса SqlExpress `http://ServerSQL/ReportServer` – подключение к серверу отчетов (ServerSQL) с пустым именем инстанса **Предупреждение**: Недопустимо использование в строке подключения адресов типа `127.0.0.1` и `localhost`.

3. Затем установщик сообщает о готовности установить выбранные компоненты ПО RusGuard (только Сервер RusGuard или Сервер и другие компоненты программного комплекса в **любом сочетании** (см. также раздел Установка АРМ и утилит RusGuard 61). Чтобы приступить к установке, нажмите на кнопку Установить.

Процесс установки начнется автоматически.

4. При отсутствии сбоев и ошибок система сообщит об успешной установке выбранных компонентов ПО и предложит завершить процесс, а также сохранить и/или загрузить сводные данные о нем. Чтобы выйти из установщика и закончить процедуру, нажмите на кнопку Готово.

Примечание: Обратите внимание, что при установке Сервера RusGuard автоматически устанавливается утилита RusGuard Agent. Эта утилита позволяет осуществлять оперативный мониторинг и управление серверными процессами. Подробнее о функциях и использовании утилиты см. в разделе Служебные программы и утилиты > Утилита RusGuard агент 301.

Внимание: При установке новой версии ПО RusGuard (обновлении) возможен конфликт версии ПО и БД, может потребоваться обновление БД 356.

Установка компонента Возможности рабочего стола

При установке (или обновлении) сервера RusGuard на Windows Server 2008 R2 или Windows Server 2012 необходимо включить компонент сервера Возможности рабочего стола". Этот компонент необходим для корректной работы интеграции с Panasonic.

Windows Server 2008 R2

Для того чтобы установить компонент:

1. Запустить диспетчер сервера.
2. В меню ***Действие*** выбрать ***Добавить компоненты*** (см. рис. 16).

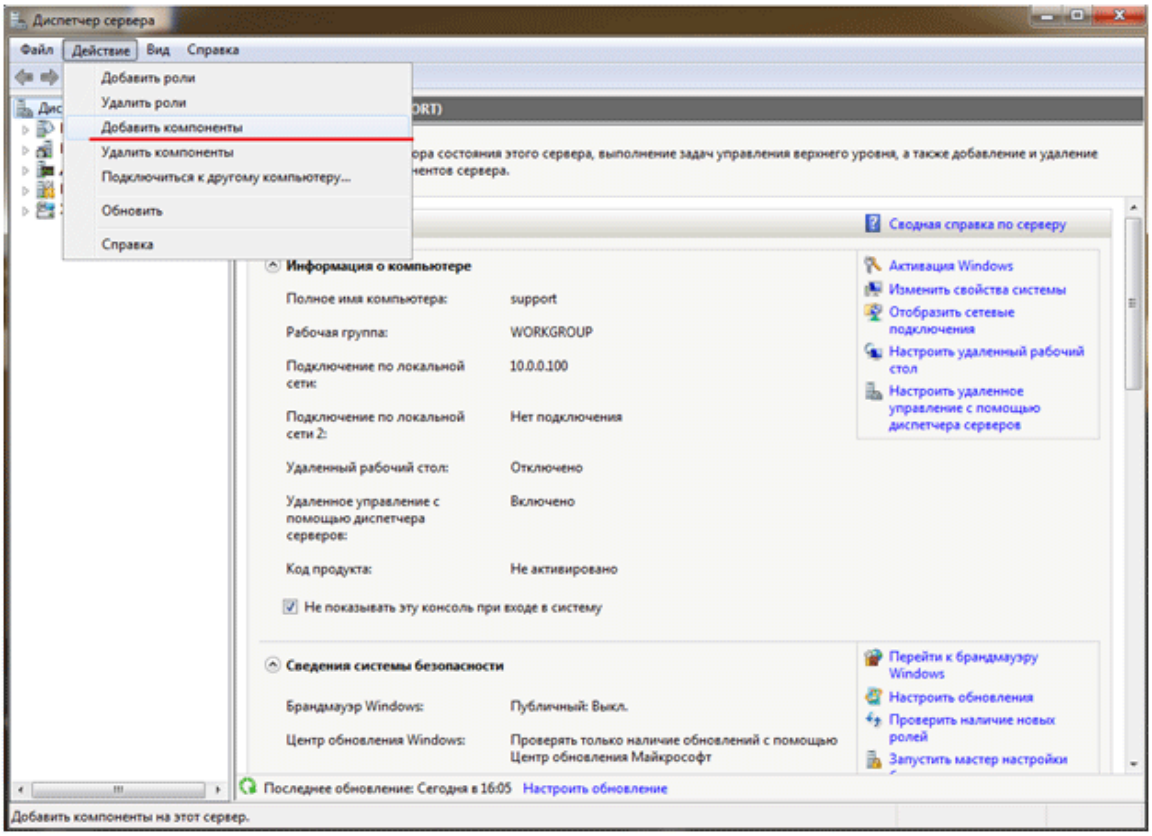


Рисунок 16 - Установка компонента "Возможности рабочего стола". Меню

3. В открывшемся окне установите флаг ***Возможности рабочего стола*** и нажмите кнопку ***Далее*** (см. рис. 17).

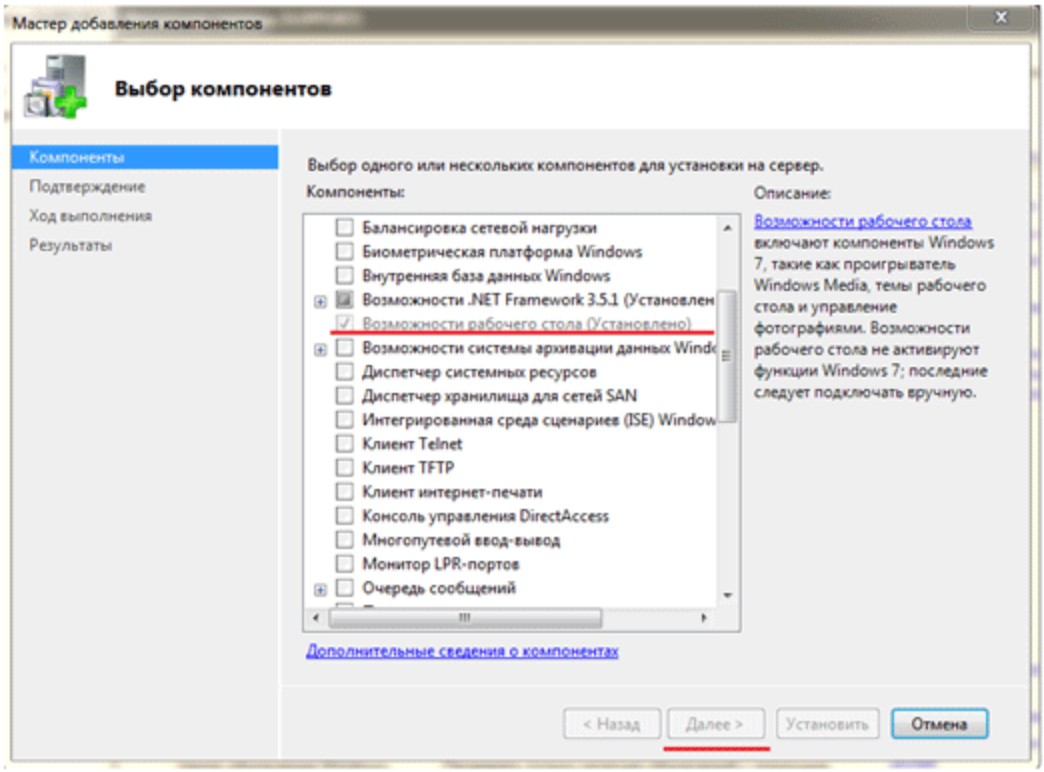


Рисунок 17 - Установка компонента "Возможности рабочего стола". Установка настроек

4. Примите изменения. При необходимости, после окончания процесса установки перезагрузить сервер.

Windows Server 2012

Для того чтобы установить компонент:

1. Запустить диспетчер сервера.
2. В меню ***Управление*** выбрать ***Добавить роли и компоненты*** (см. рис. 18).

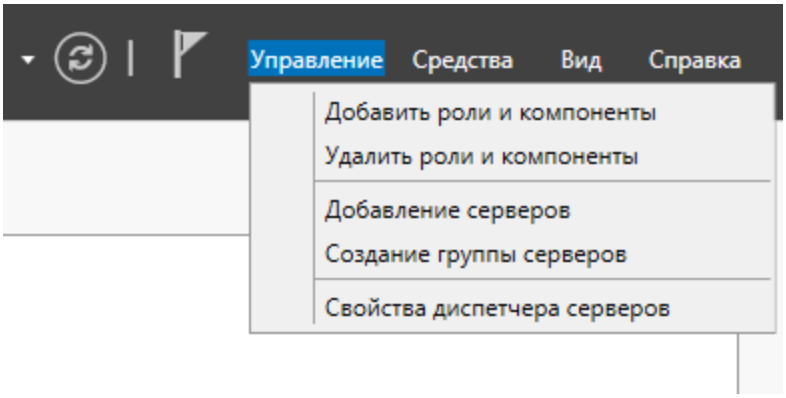


Рисунок 18 - Установка компонента "Возможности рабочего стола". Запуск

3. На первом окне мастера нажмите на кнопку ***Далее*** (см. рис. 19).

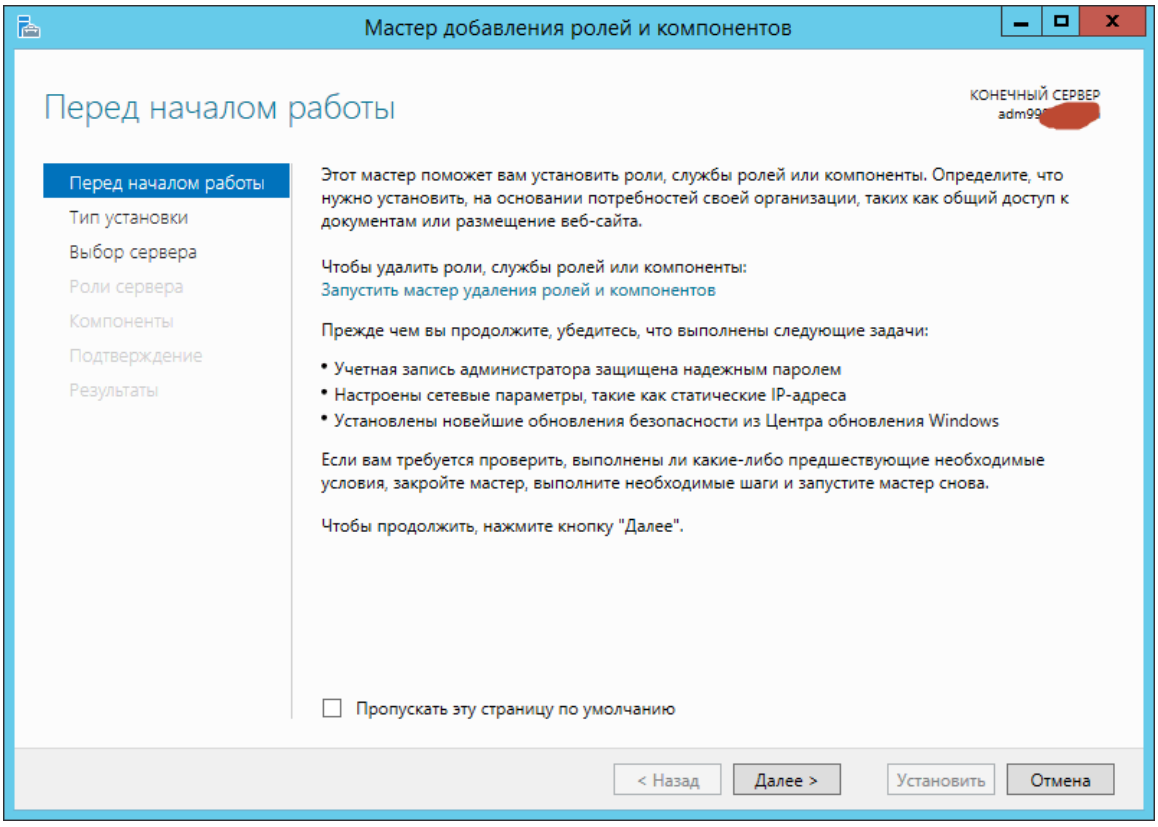


Рисунок 19 - Установка компонента "Возможности рабочего стола". Windows Server 2012 R2

4. Оставьте флаг ***Установка ролей и компонентов*** активным (см. рис. 20). Не меняйте настройки пула (локальный) (см. рис. 21).

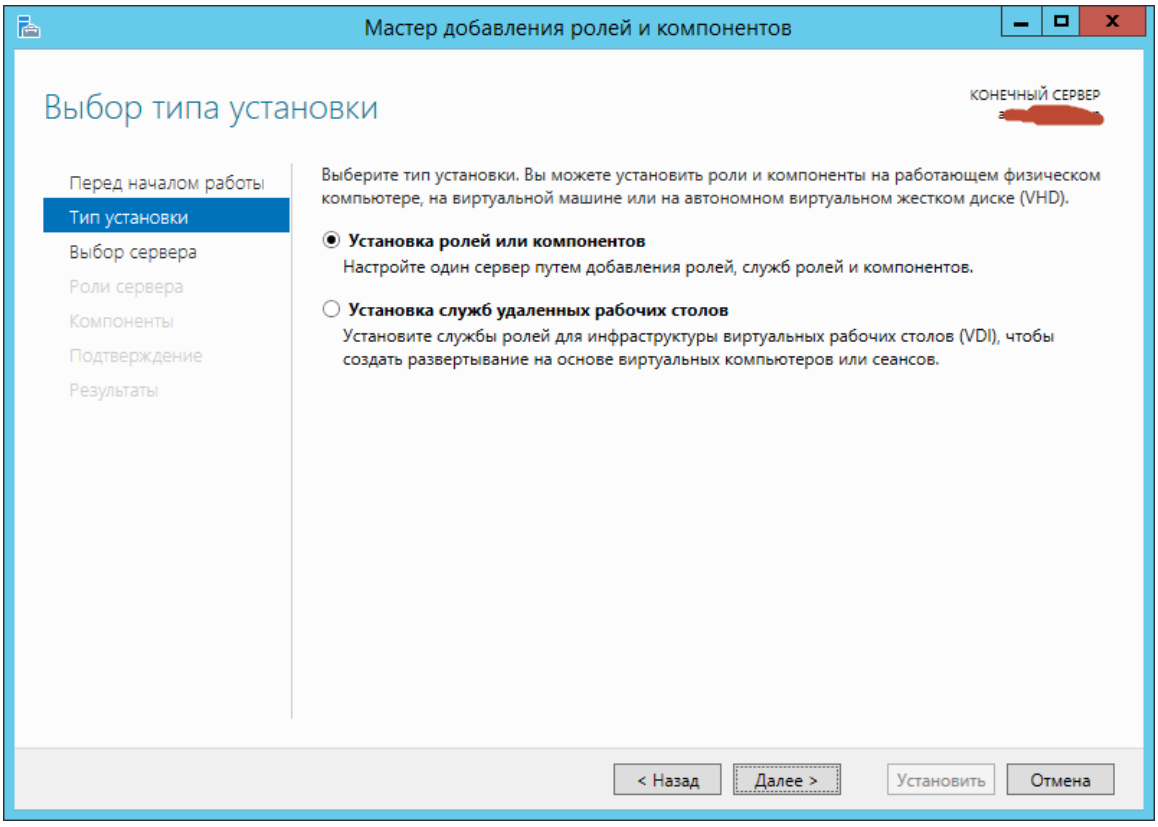


Рисунок 20 - Установка компонента "Возможности рабочего стола". Windows Server 2012 R2

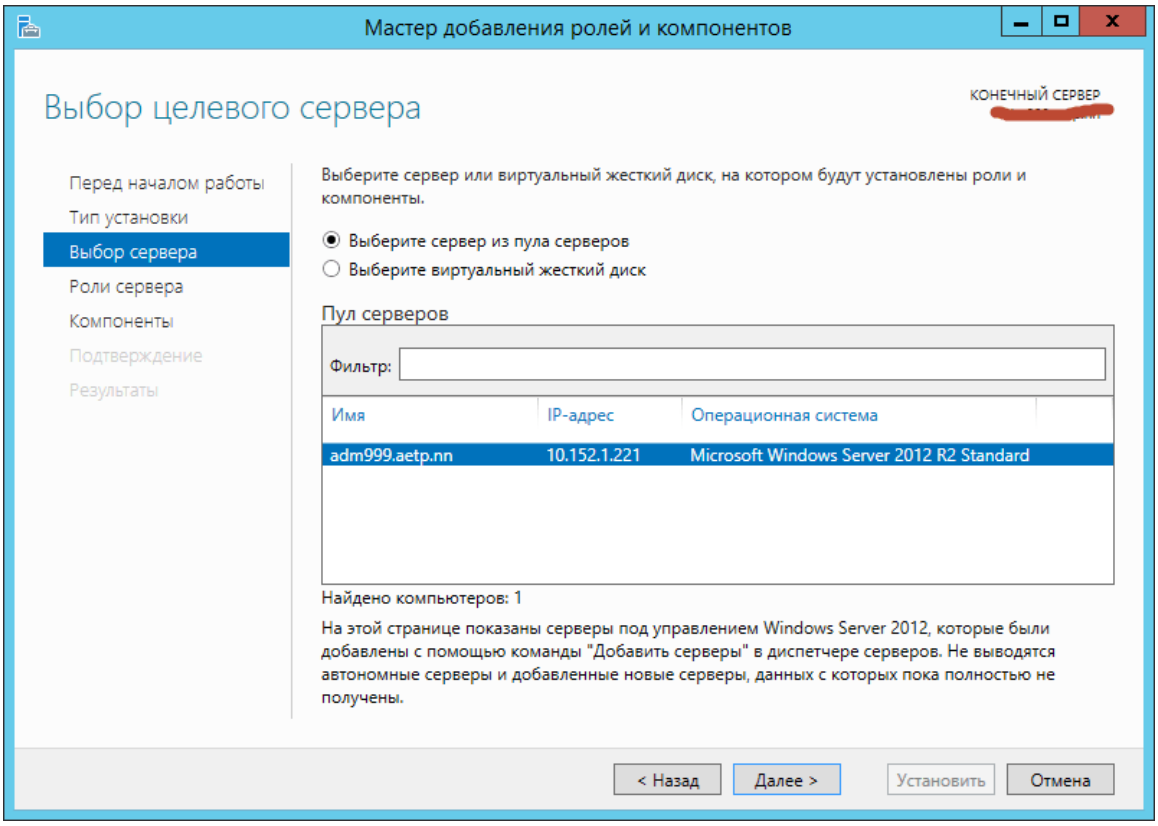


Рисунок 21 - Установка компонента "Возможности рабочего стола". Windows Server 2012 R2

5. Не меняйте настройки выбора ролей, нажмите на кнопку ***Далее*** (см. рис. 22).

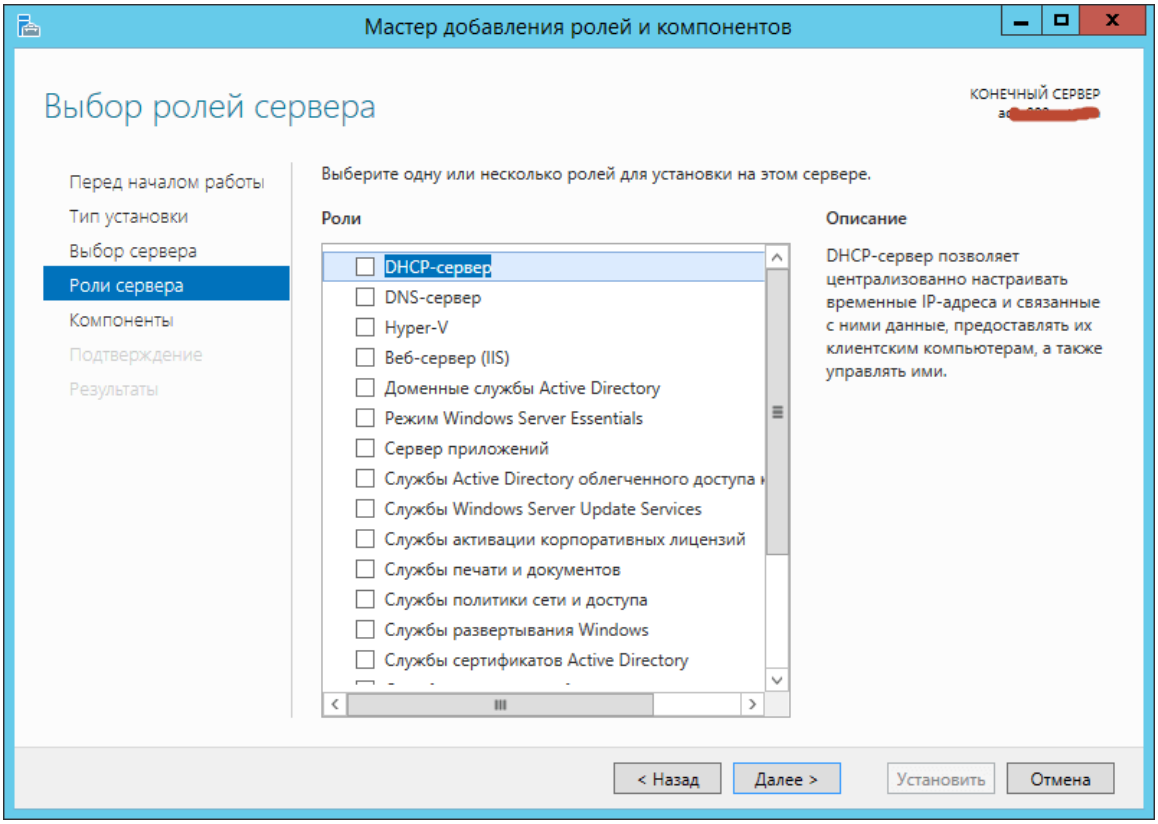


Рисунок 22 - Установка компонента "Возможности рабочего стола". Windows Server 2012 R2

6. На шаге выбора компонентов установите флаг ***Возможности рабочего стола*** (см. рис. 23). Нажмите на кнопку ***Далее***.

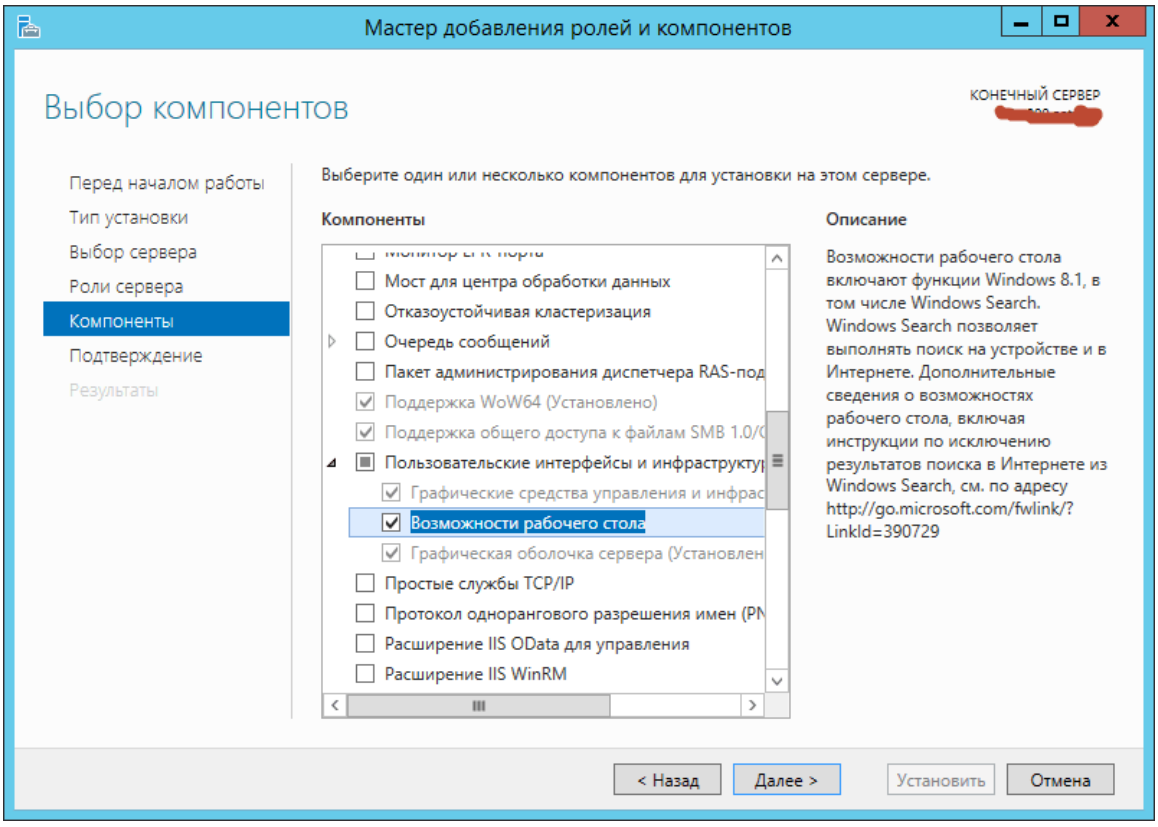


Рисунок 23 - Установка компонента "Возможности рабочего стола". Windows Server 2012 R2

7. Нажмите на кнопку ***Установить***.
8. При необходимости перезагрузить сервер.

Установка SQL-сервера и настройка сервера отчетов

Введение

Внимание: Данный раздел предназначен для самостоятельного разворачивания SQL – сервера (2-й тип установки 26). В случае использования "Express"- установки (т.е. все компоненты серверной части ПО RusGuard, включая SQL-сервер, разворачиваются на одном ПК одновременно) **данный раздел пропускается**.

Выбор дистрибутивного пакета зависит от операционной системы, под управлением которой вы работаете. Версии, отличные от указанных в описании дистрибутивного пакета, можно скачать на сайте компании Microsoft (см. табл. 4).

Таблица 4 - Имена дистрибутивных пакетов Microsoft SQL Server 2008 R2 Express

Имя исполняемого файла	Описание
SQLEXPRADV_x86_ENU.exe	Английская версия Microsoft SQL Server 2014 Express для 86-разрядной ОС Windows. http://download.microsoft.com/download/E/A/E/EAE6F7FC-767A-4038-A954-49B8B05D04EB/ExpressAdv%2032BIT/SQLEXPRADV_x86_ENU.exe
SQLEXPRADV_x86_RUS.exe	Русская версия Microsoft SQL Server 2014 Express для 86-разрядной ОС Windows. http://download.microsoft.com/download/4/E/3/4E38FD5A-8859-446F-8C58-9FC70FE82BB1/ExpressAdv%2032BIT/SQLEXPRADV_x86_RUS.exe
SQLEXPRADV_x64_ENU.exe	Английская версия Microsoft SQL Server 2014 Express для 64-разрядной ОС Windows. http://download.microsoft.com/download/E/A/E/EAE6F7FC-767A-4038-A954-49B8B05D04EB/ExpressAdv%2064BIT/SQLEXPRADV_x64_ENU.exe
SQLEXPRADV_x64_RUS.exe	Русская версия Microsoft SQL Server 2014 Express для 64-разрядной ОС Windows. http://download.microsoft.com/download/4/E/3/4E38FD5A-8859-446F-8C58-9FC70FE82BB1/ExpressAdv%2064BIT/SQLEXPRADV_x64_RUS.exe

Процедура установки Microsoft SQL Server 2014 Express в простейшем случае

Примечание: Полная инструкция от производителя, а также требования к системе и методы решения проблем при установке, находится по адресу http://msdn.microsoft.com/ru-ru/library/ms143219.aspx.

Для того чтобы установить Microsoft SQL Serer 2014 Express:

1. Запустите соответствующий установочный файл (см. таблицу выше).

Запуск осуществляется с правами администратора.

Внимание: У учетной записи, под которой вы производите установку SQL Server, обязательно должен быть задан пароль (это требуется для нормальной работы Сервера отчетов, при пустом пароле невозможно будет на нем авторизоваться). Если пароль не задан, завершите установку SQL Server, задайте пароль и запустите установочный файл снова.

2. В разделе ***Планирование*** (***Planning***) выберите пункт ***Средство проверки конфигурации*** (***System Configuration Checker***) (см. рис. 24).

В случае возникновения ошибок, устраните их причины и повторите проверку, нажав на кнопку ***Включить*** заново. Чтобы выйти из текущего окна, нажмите на кнопку OK.

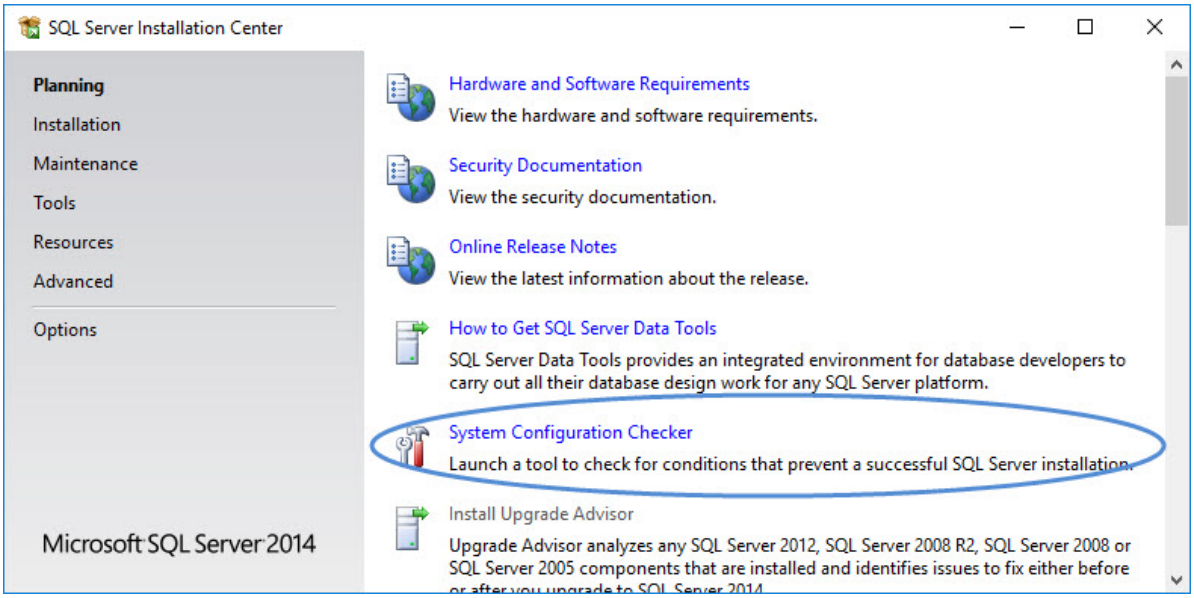


Рисунок 24 - Окно установщика SQL-Сервера. Раздел "Планирование"

3. В разделе ***Установка*** выберите пункт ***Новая установка или добавление компонентов к существующей установке*** (см. рис. 25).

В следующем окне отобразится текст лицензионного соглашения.

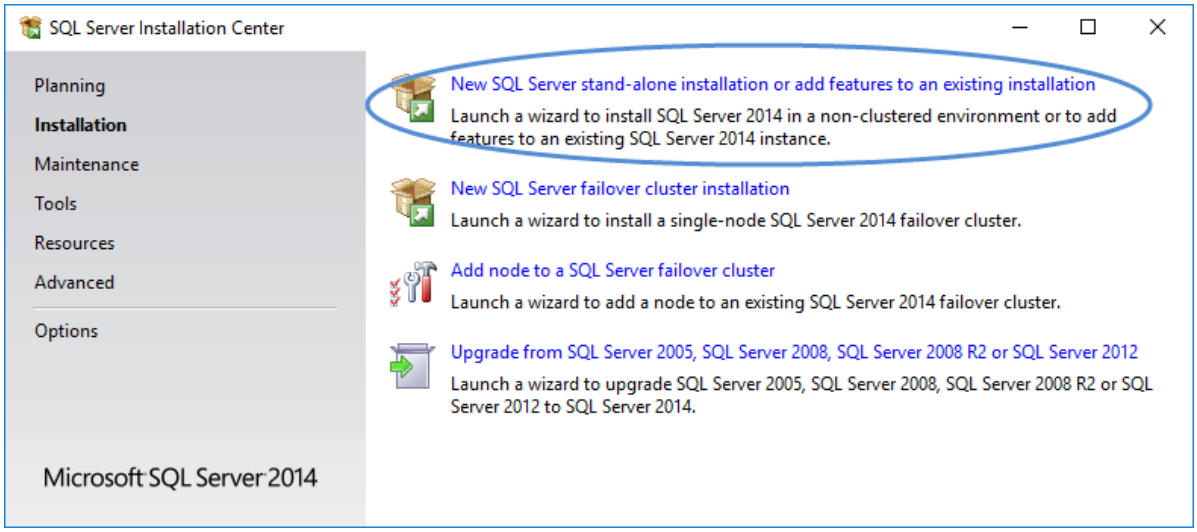


Рисунок 25 - Установка SQL Server. Раздел "Установка"

4. Ознакомьтесь с лицензионным соглашением и установите флажок напротив ***Я принимаю условия лицензионного соглашения***. Нажмите на кнопку Далее > / Next >.

5. Укажите, нужно ли выполнить обновление компонентов с сайта Microsoft (см. рис. 26), перейдите к следующему шагу. При положительном ответе система автоматически проверит наличие обновлений и установит доступные.

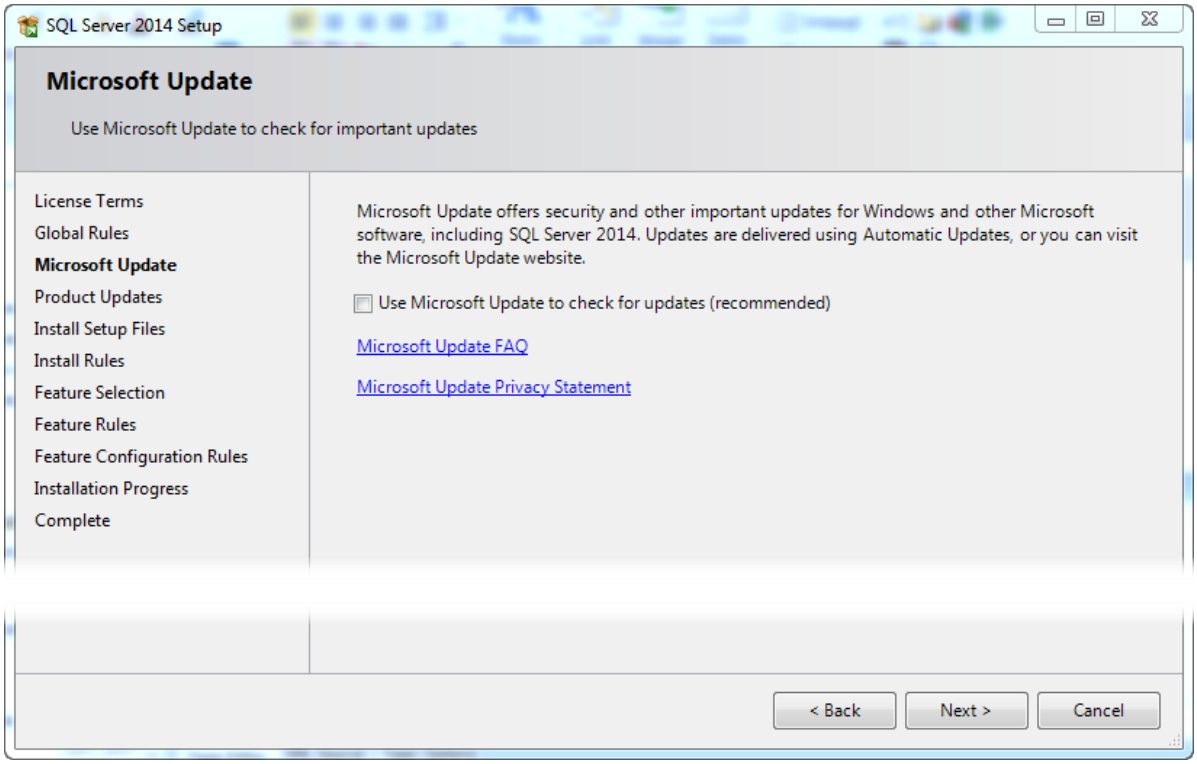


Рисунок 26 - Установка SQL Server 2014. Проверка наличия обновлений

6. Выберите компоненты для установки, установив флажки напротив названий нужных (см. рис. 27, где отмечены обязательные для установки компоненты).

Обязательные компоненты:

- ***Службы компонента Database Engine***
- ***Службы Reporting Services***

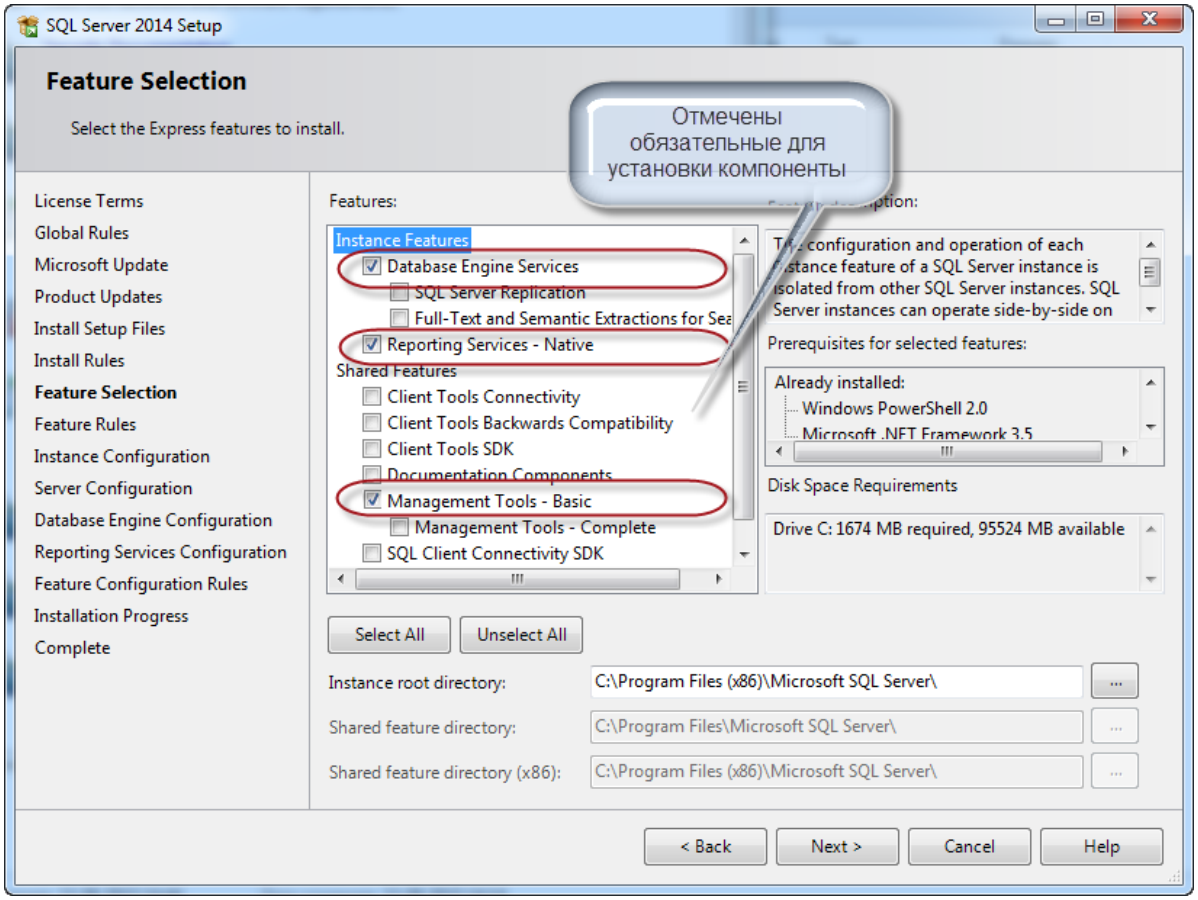


Рисунок 27 - Установка SQL Server. Выбор компонентов

6. Выберите вариант ***Именованный экземпляр (Named Instance)***. В качестве имени экземпляра введите `SQLExpress` (см. рис. 28). Нажмите на кнопку Далее >.

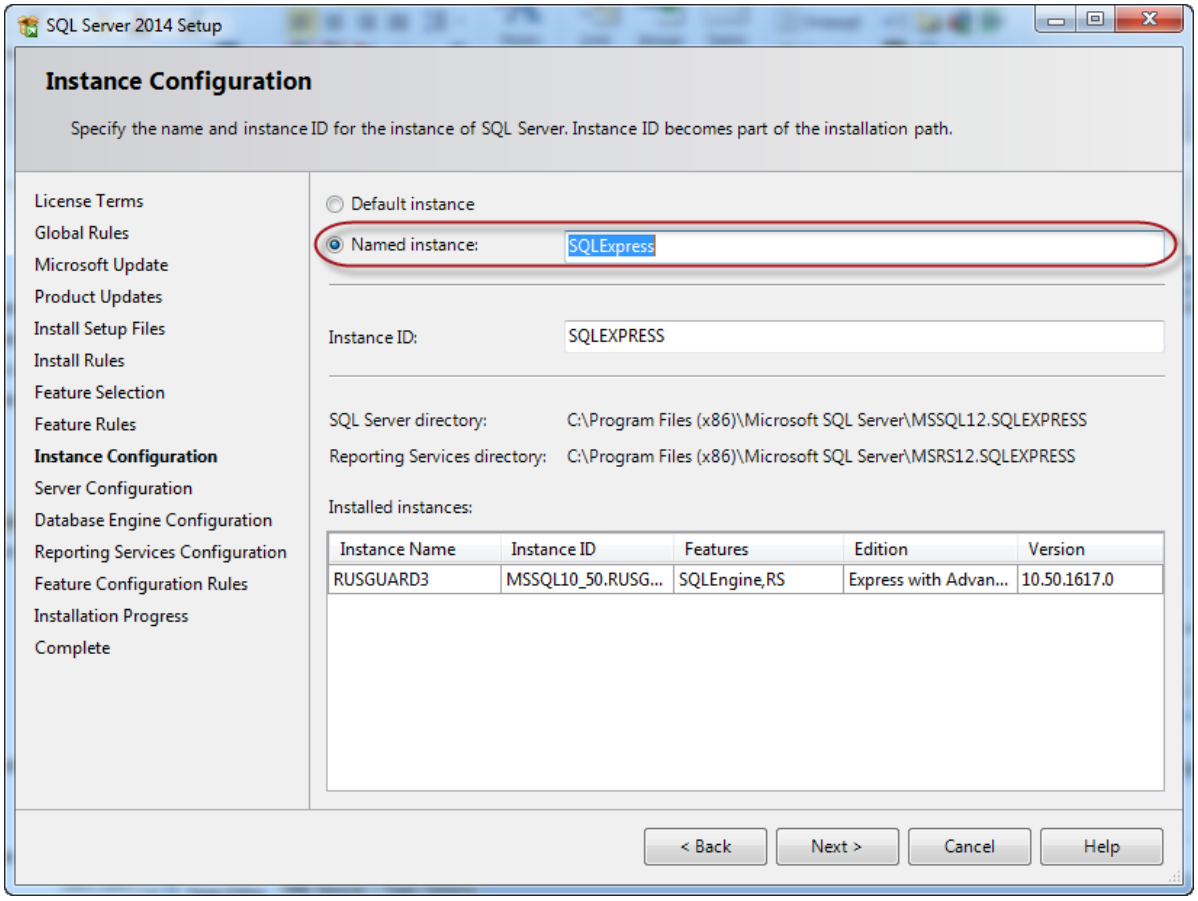


Рисунок 28 - Установка SQL Server. Настройка экземпляра

7. На этапе настройки компонента Database Engine (см. рис. 29) выберите смешанный режим проверки подлинности и задайте пароль для учетной записи системного администратора SQL Server (по умолчанию, имя пользователя "sa").
   Если не назначен ни один администратор SQL Server, нажмите на кнопку Добавить текущего пользователя / Add Current User.

   Перейдите к следующему этапу.

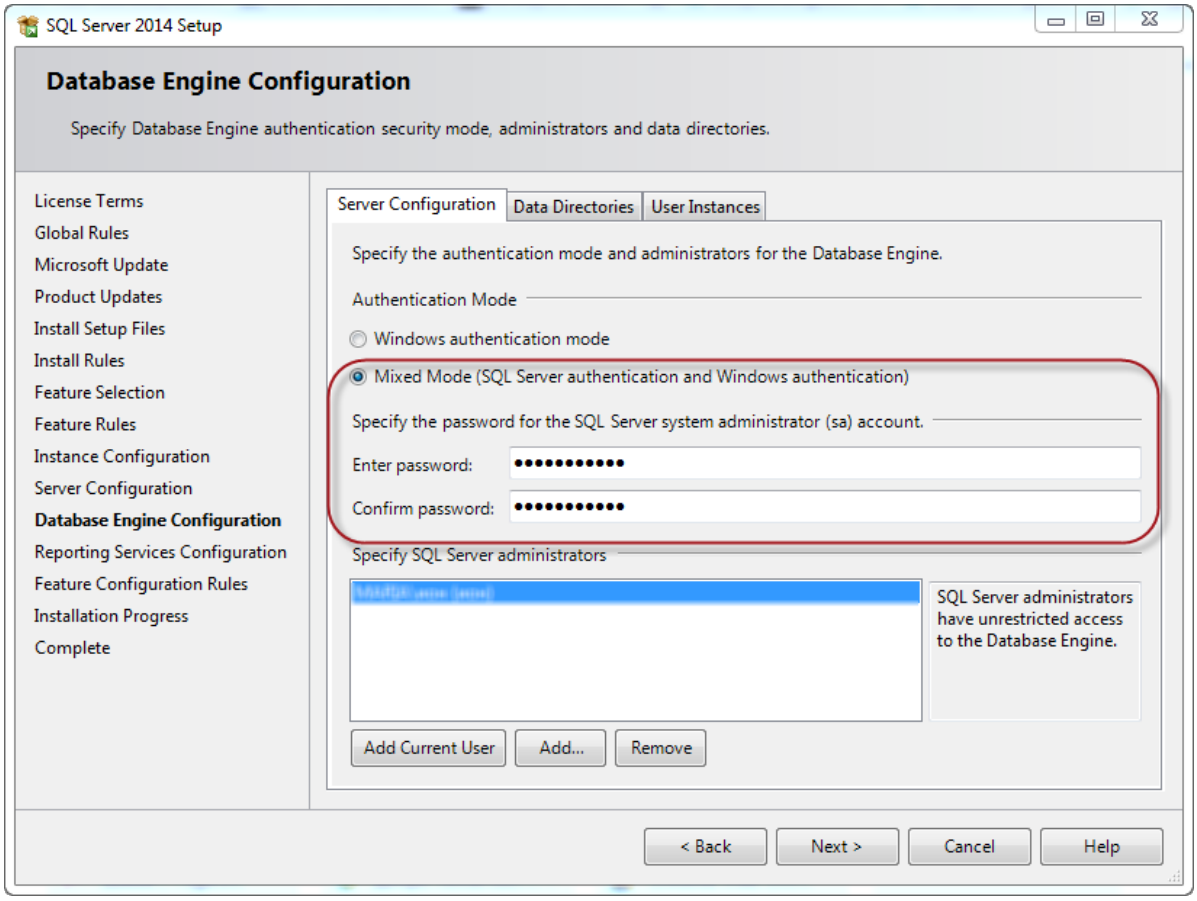


Рисунок 29 - Установка SQL Server. Настройка компонента Database Engine. Выбор режима проверки подлинности

11. На этапе настройки служб Reporting Services выберите ***Установить конфигурацию по умолчанию для работы в собственном режиме*** (см. рис. 30). Нажмите на кнопку Далее >.

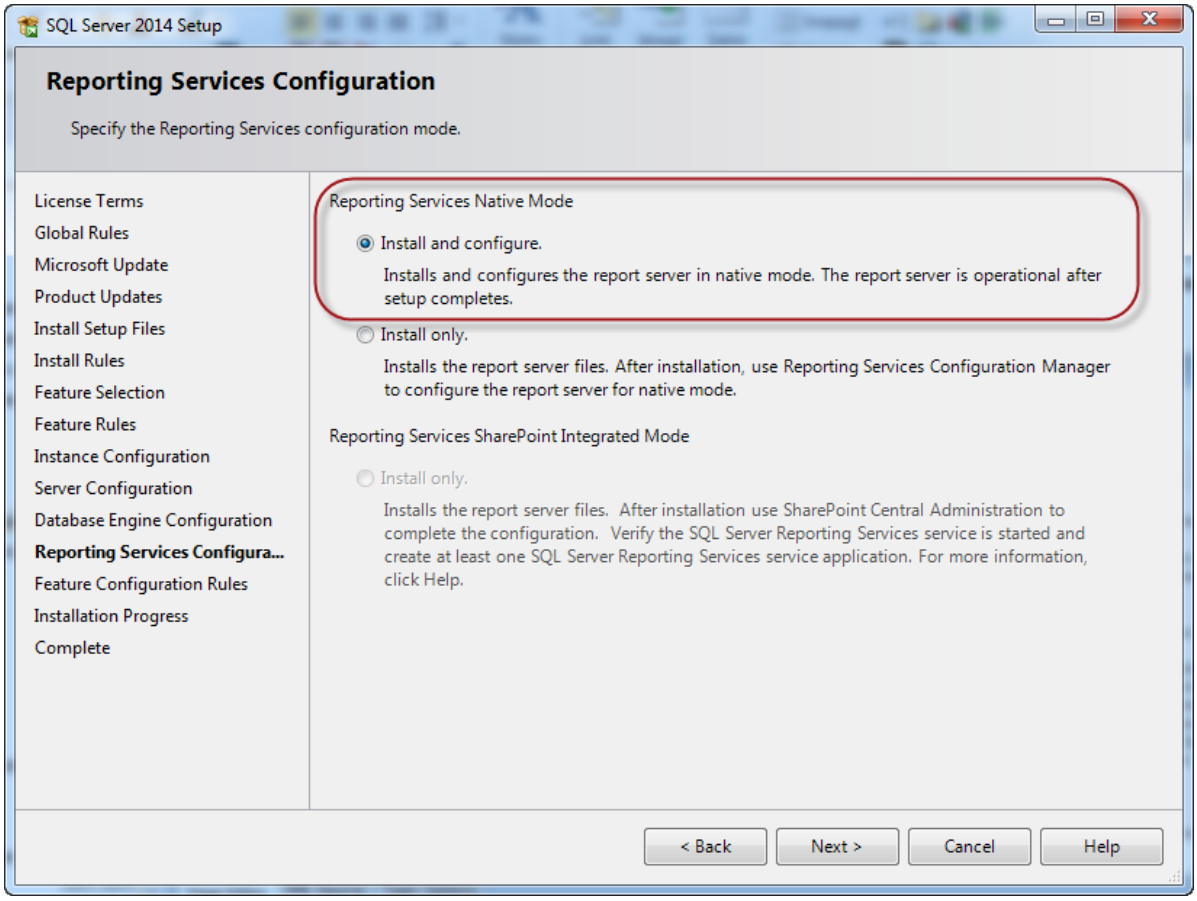


Рисунок 30 - Установка SQL Server. Настройка служб Reporting Services

12. На следующем этапе вы можете указать, какие сведения передавать в отчетах об ошибках корпорации Microsoft. Если дополнительные настройки отчетов об ошибках не требуются, нажмите на кнопку Далее > и дождитесь завершения установки.

В случае успешного завершения процедуры, в следующем экране отобразится соответствующее сообщение.

13. Закройте окно.

Конфигурация SQL-сервера

Конфигурация SQL-севера необходима, чтобы обеспечить доступ к нему с других компьютеров (сервер RusGuard и сервер БД развернуты на разных компьютерах).

Для того чтобы выполнить конфигурацию SQL-сервера:

1. В меню ***Пуск***, выберите ***Microsoft SQL Server 2014*** > ***Средства Настройки (Configuration Tools)***, запустите утилиту ***Диспетчер конфигурации SQL Server (Configuration Manager)***.
2. Выберете в левой навигационной панели пункт ***Сетевая конфигурация SQL Server (SQL Server Network Configuration)***, подпункт ***Протоколы для SQLExpress*** (***Protocols for SQLExpress***) (см. рис. 31).

Примечание: Если при установке SQL Server вы ввели имя экземпляра, отличное от SQLExpress, то название узла будет отличаться. В общем случае оно формируется по правилу `Протоколы для [Название экземпляра]`.

Если статус TCP/IP ***Отключен (Disabled)***, щелкните правой кнопкой мыши в строке TCP/IP и выберите в контекстном меню команду ***Включить (Enable)***.

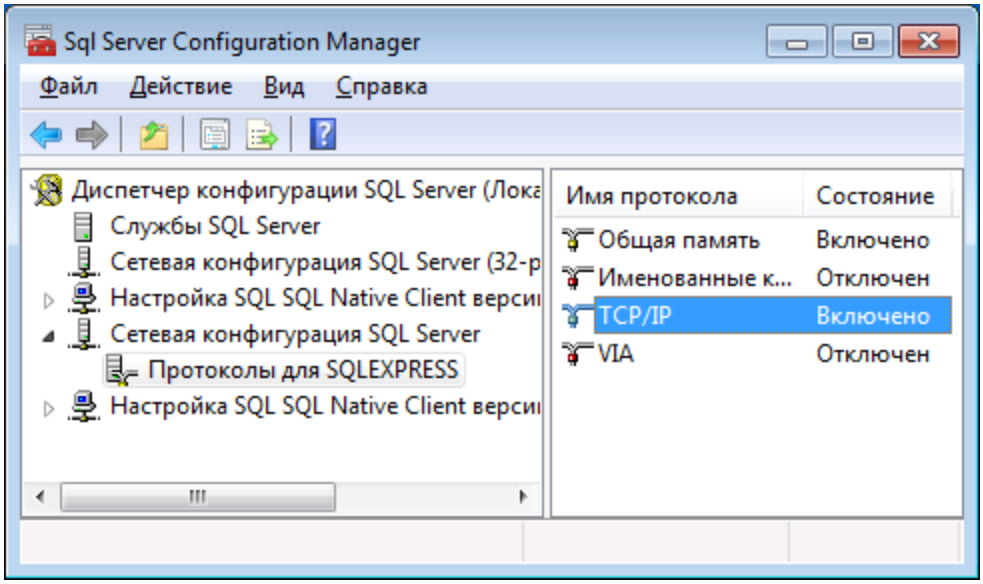


Рисунок 31 - Конфигурация SQL Server

2. Перейдите в раздел ***Службы SQL Server (SQL Server Services)*** левой навигационной панели. В списке справа выберите ***SQL Server (SQLExpress)***.

Примечание: Если при установке SQL Server вы ввели имя экземпляра, отличное от SQLExpress, то название узла будет отличаться. В общем случае оно формируется по правилу `SQL Server [Название экземпляра]`.

Щелкните правой кнопкой мыши в строке ***SQL Server (SQLExpress)*** и выберите в контекстном меню команду ***Перезапустить (Resume)***.

Настройка сервера отчетов

Предлагаем ознакомиться с краткой инструкцией по настройке Reporting Services в простейшем случае.

Полная инструкция от производителя находится по адресу http://msdn.microsoft.com/ru-ru/library/ms159624.aspx.

Для того чтобы настроить сервер отчетов:

1. Запустите браузер Internet Explorer от имени администратора.
2. Введите в адресную строку браузера адрес сервера отчетов.
   - Если во время установки SQL Server вы выбрали ***Экземпляр по умолчанию***, то адрес сервера отчетов примет вид `http://localhost/Reports`.

- Если во время установки SQL Server вы выбрали ***Именованный экземпляр*** с именем SQLExpress, то адрес сервера отчетов примет вид `http://localhost/Reports_SQLExpress`

Для примера рассмотрим случай, когда был выбран ***Именованный экземпляр*** с именем MyServer. Адрес сервера БД примет вид `http://localhost/Reports_MyServer`.

Также адрес сервера отчетов можно посмотреть через Диспетчер конфигурации сервера отчетов (Reporting Services Configuration Manager). Чтобы открыть его, нажмите на кнопку Пуск, найдите среди программ нужную версию SQL Сервера, выберите пункт ***Диспетчер конфигурации сервера отчетов (Reporting Services Configuration Manager)*** и запустите утилиту (см. рис. 32).

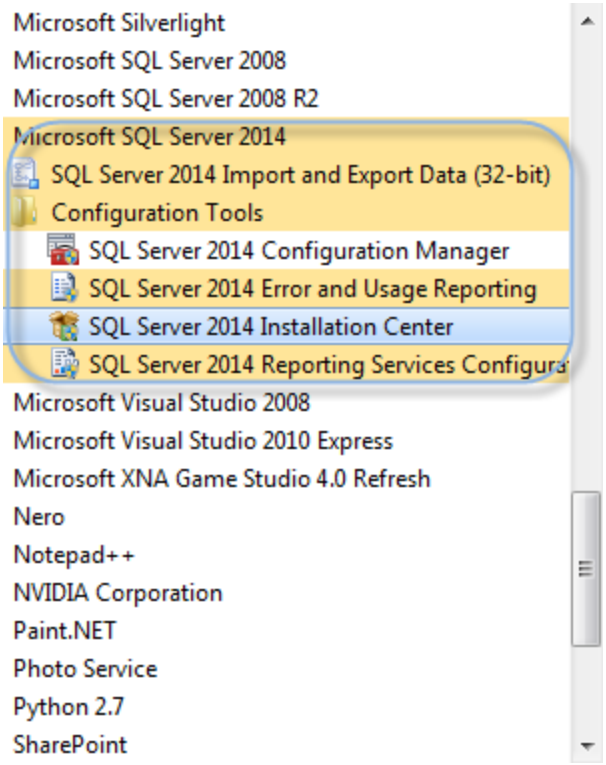


Рисунок 32 - Настройка сервера отчетов. Диспетчер конфигурации сервера отчетов

На рисунке ниже (см. рис. 33) показано, как найти адрес сервера отчетов.

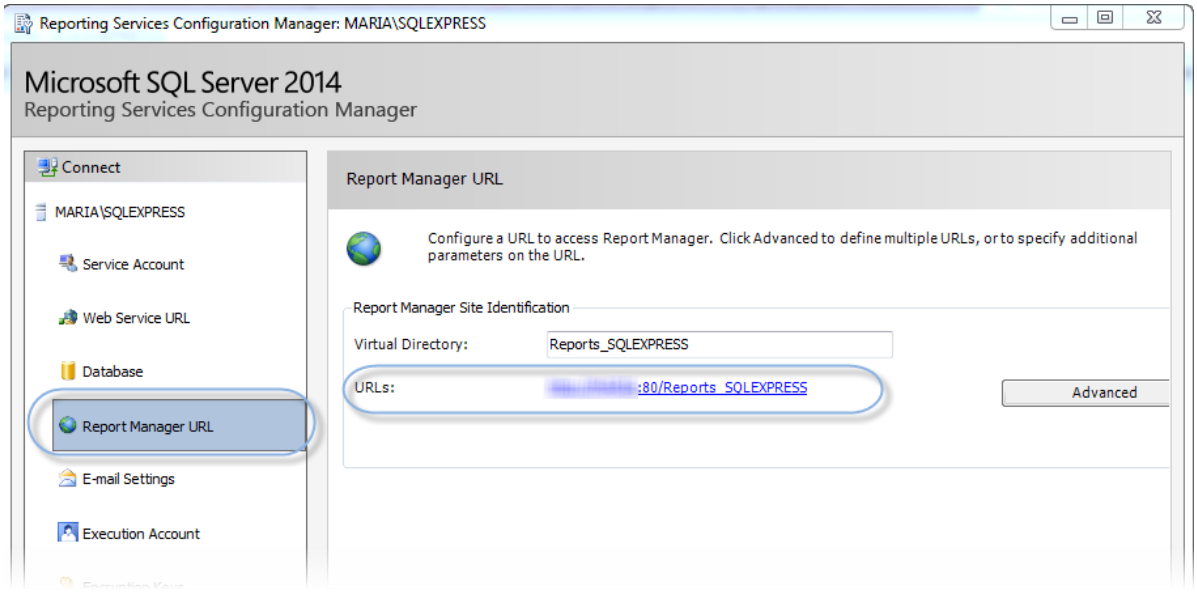


Рисунок 33 - Настройка сервера отчетов. Ссылка на сервер отчетов

3. В появившемся диалоговом окне введите логин и пароль учетной записи Windows, под которой вы производили установку SQL Server.

Внимание: Если в окне браузера появится сообщение об ошибке (см. рис. 34), выполните действия, описанные в шаге 4. В противном случае, переходите сразу к шагу 5.

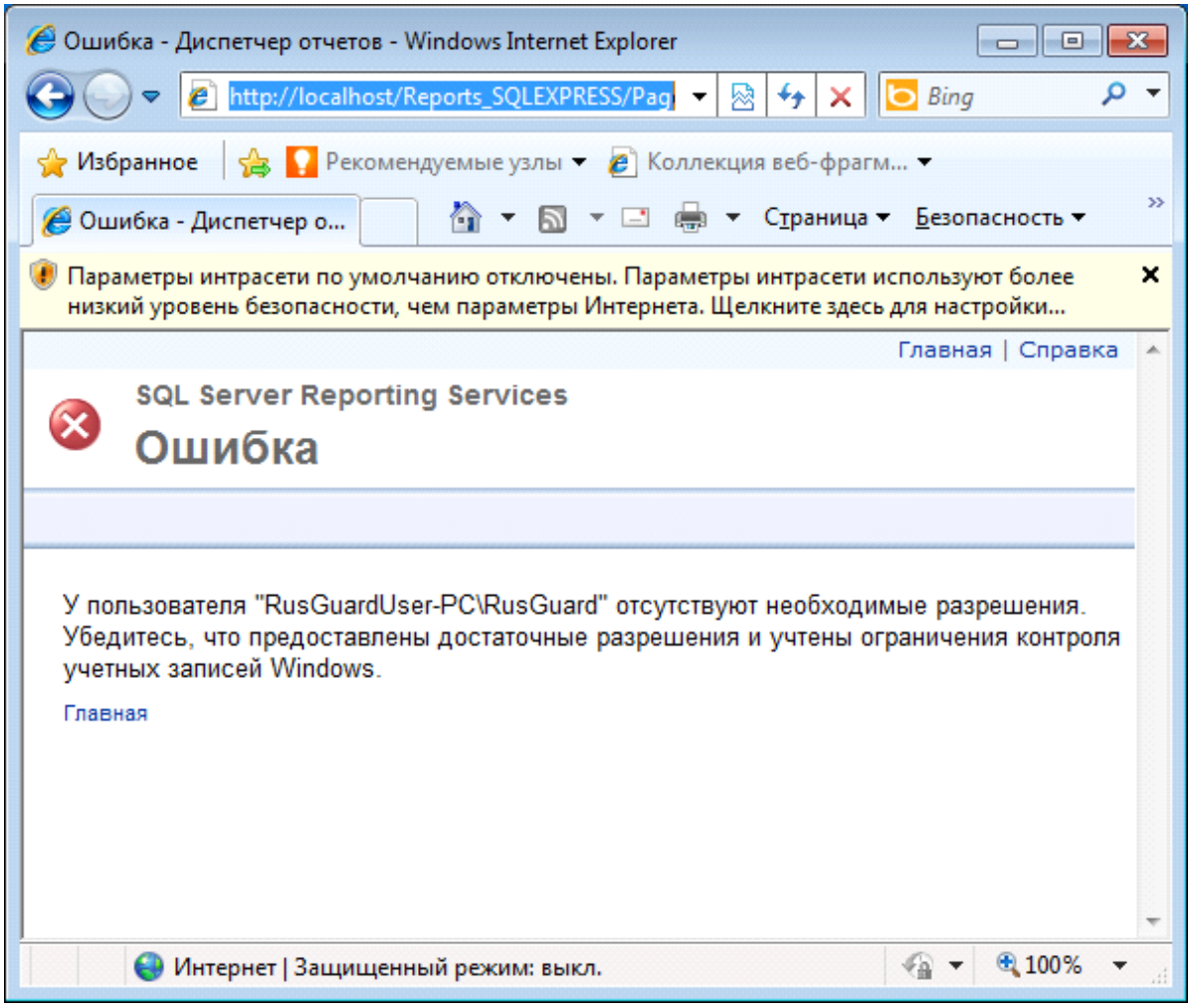


Рисунок 34 - Настройка сервера отчетов. Сообщение об ошибке в браузере

4. Щелкните правой кнопкой мыши в сообщении ошибке.

Отобразится контекстное меню (см. рис. 35). Выберите в нем команду ***Включить параметры интрасети*** и нажмите на кнопку ***Да***.

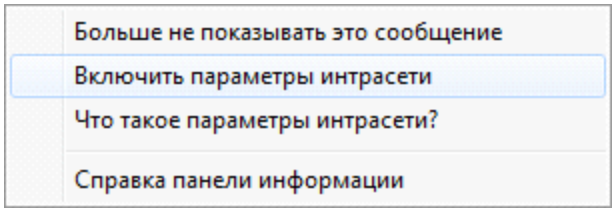


Рисунок 35 - Настройка сервера отчетов. Устранение ошибки

Закройте Internet Explorer и снова начните процедуру с 1 шага.

5. Перейдите по ссылке ***Настройки веб-сайта > Безопасность***. Нажмите на кнопку ***Создать назначение ролей*** (см. рис. 36).

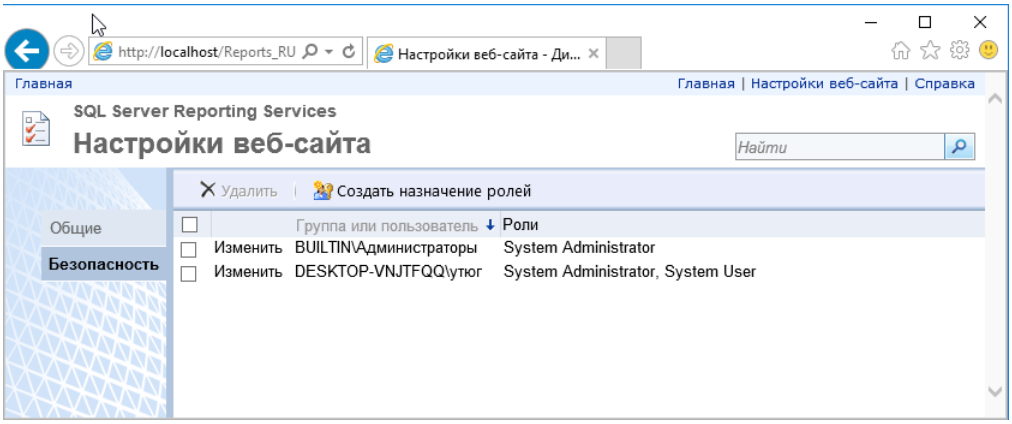


Рисунок 36 - Настройка сервера отчетов. Настройка сайта

6. Введите учетные данные записи Windows, под которой вы производили установку SQL Server. Установите флажки напротив всех ролей (см. рис. 37) и нажмите на кнопку ***ОК***.

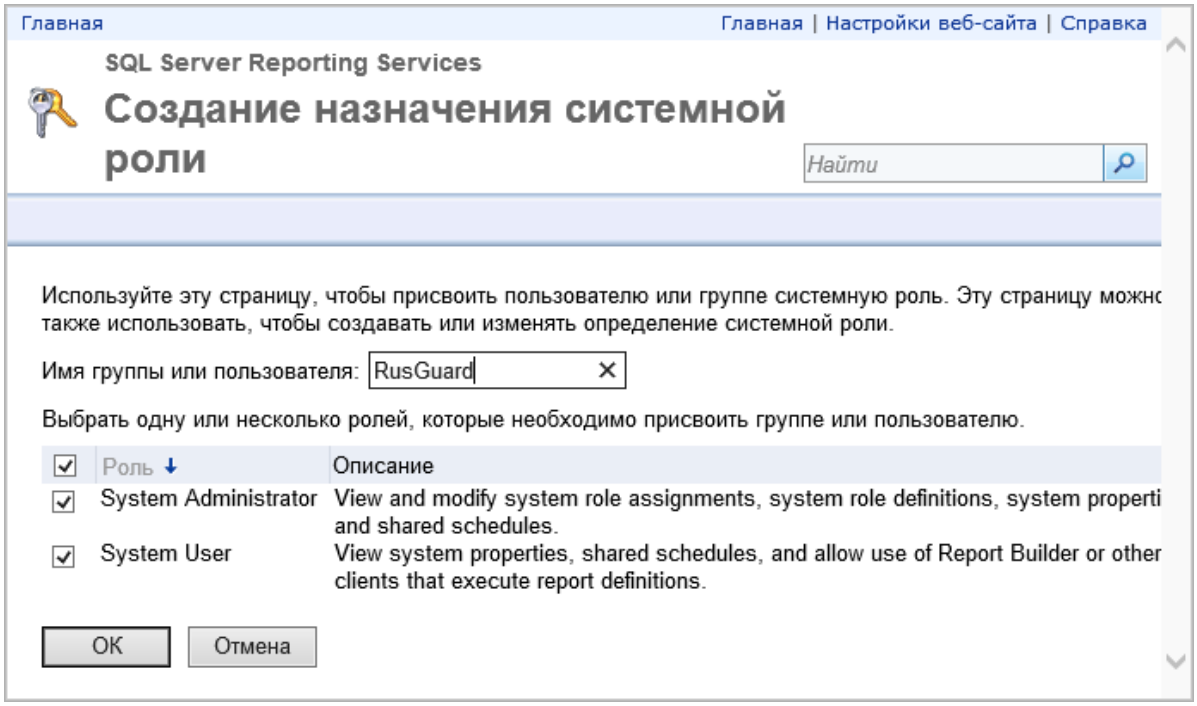


Рисунок 37 - Настройка сервера отчетов. Назначение системных ролей

7. Перейдите по ссылке ***Главная*** и нажмите на кнопку ***Параметры папки*** (см. рис. 38).

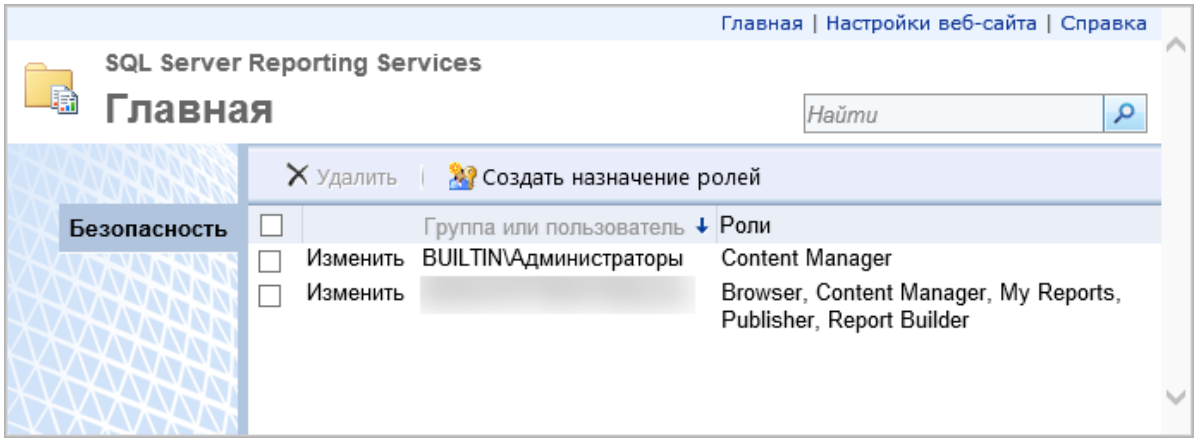


Рисунок 38 - Настройка сервера отчетов. Диспетчер отчетов

8. Введите учетные данные записи Windows, под которой вы производили установку SQL Server (или выберите в списке групп/пользователей и нажмите на ссылку ***Изменить*** слева от названия). Установите флажки напротив всех ролей (см. рис. 39) и нажмите на кнопку ***Применить***.

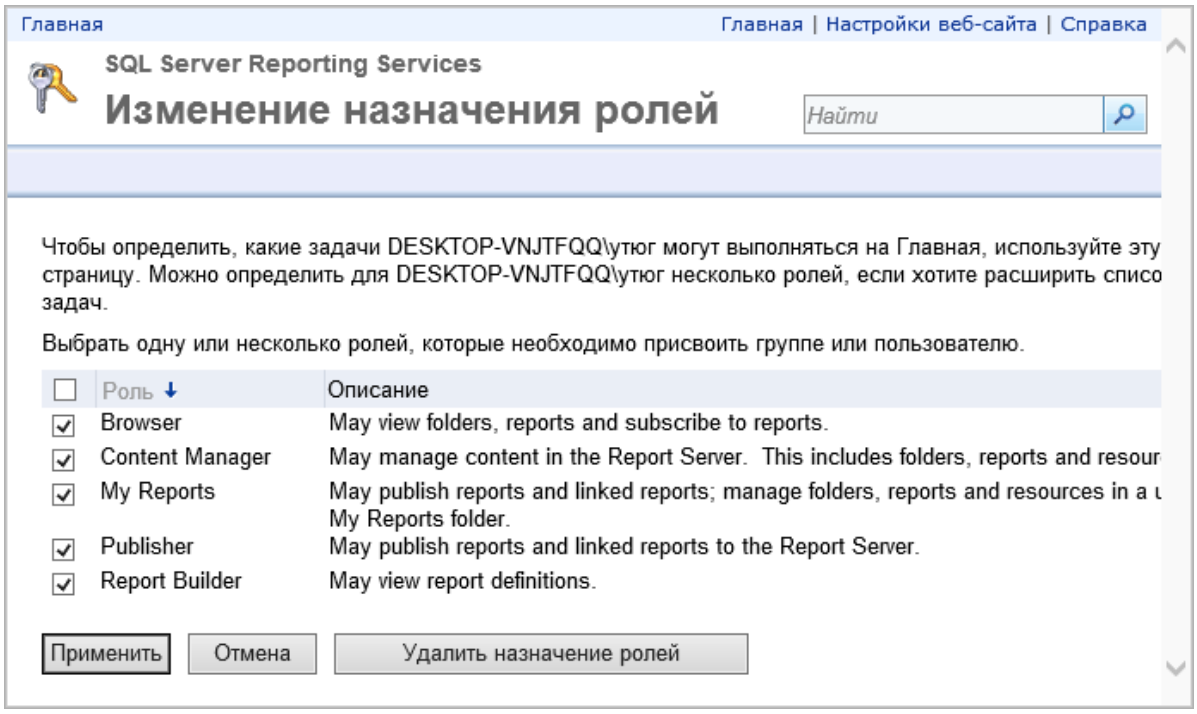


Рисунок 39 - Настройка сервера отчетов. Создание назначения ролей

9. Закройте браузер.

См. также раздел Управление шаблонами отчетов 236

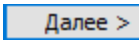
Установка АРМ и утилит RusGuard

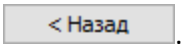
АРМ и утилиты RusGuard могут устанавливаться как вместе с сервером (при простейшем варианте конфигурации, когда все компоненты программного комплекса расположены на одном компьютере), так и отдельно.

Для того чтобы установить АРМ и (или) утилиты RusGuard:

1. Зайдите в каталог, где хранится дистрибутив RusGuard Soft (это может быть папка на компьютере или компакт-диск).
2. Запустите установочный файл setup.exe двойным щелчком мыши по пиктограмме  .

Система запустит пошаговый процесс установки. Сначала загружается экран приветствия, происходит автоматическая проверка прав текущего пользователя.

- Для перехода к следующему шагу используйте кнопку 

.
- Для возврата к предыдущему шагу используйте кнопку 

.
- Для выхода из мастера установки используйте кнопку 

.

3. Сначала мастер установки предложит ознакомиться с условиями лицензионного соглашения. Чтобы продолжить процесс, необходимо активировать пункт ***Я принимаю условия лицензионного соглашения***. Только после этого переход к следующему этапу станет возможен.

Вы также можете распечатать лицензионное соглашение.

Обратите внимание, что если на компьютере ранее были установлены какие-либо компоненты ПО RusGuard Soft, вместо лицензионного соглашения отобразится список доступных операций, из которого следует выбрать ту, которую пользователь намерен выполнить (см. рис. 40). Для установки дополнительных компонентов выберите пункт ***Изменить*** и перейдите к следующему шагу.

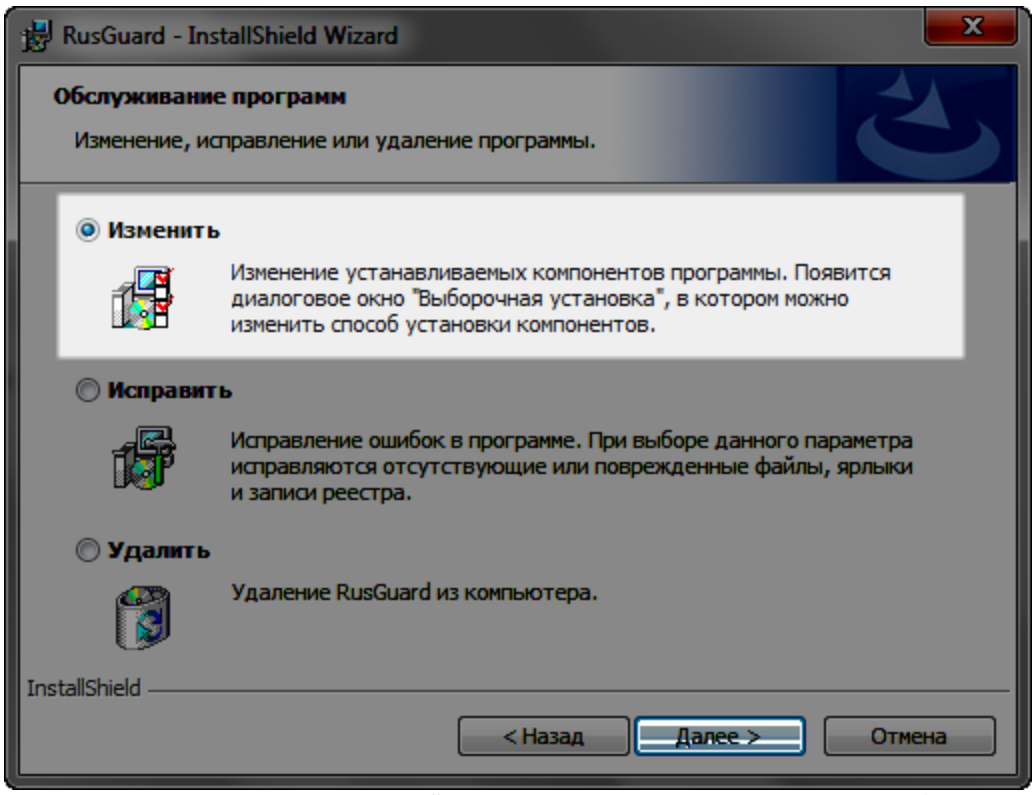


Рисунок 40 - Список доступных операций. Для установки дополнительных компонентов выберите "Изменить"

4. При первичной установке в следующем шаге мастер сообщает путь к папке, в которой по умолчанию будет установлено ПО (см. рис. 41). Вы можете указать другой путь (кнопка Изменить...). Если же на компьютере ранее были установлены другие компоненты ПО RusGuard, этот шаг пропускается.

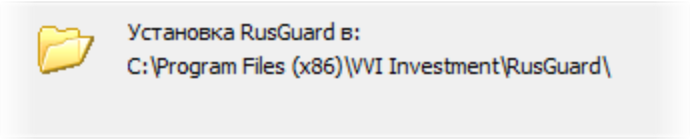


Рисунок 41 - Путь к папке, где по умолчанию устанавливается ПО

5. В следующем шаге необходимо выбрать, какие компоненты ПО будут установлены (см. также Варианты конфигурации и установки 25).

По умолчанию не выбран ни один компонент. Для разрешения установки нужных компонентов нажмите на кнопку возле названия нужного компонента и в раскрывшемся контекстном меню разрешите его установку. Выберите APM RusGuard и (или) Утилиты (см. рис. 42). Вы можете установить все утилиты одновременно, либо каждую из них по отдельности.

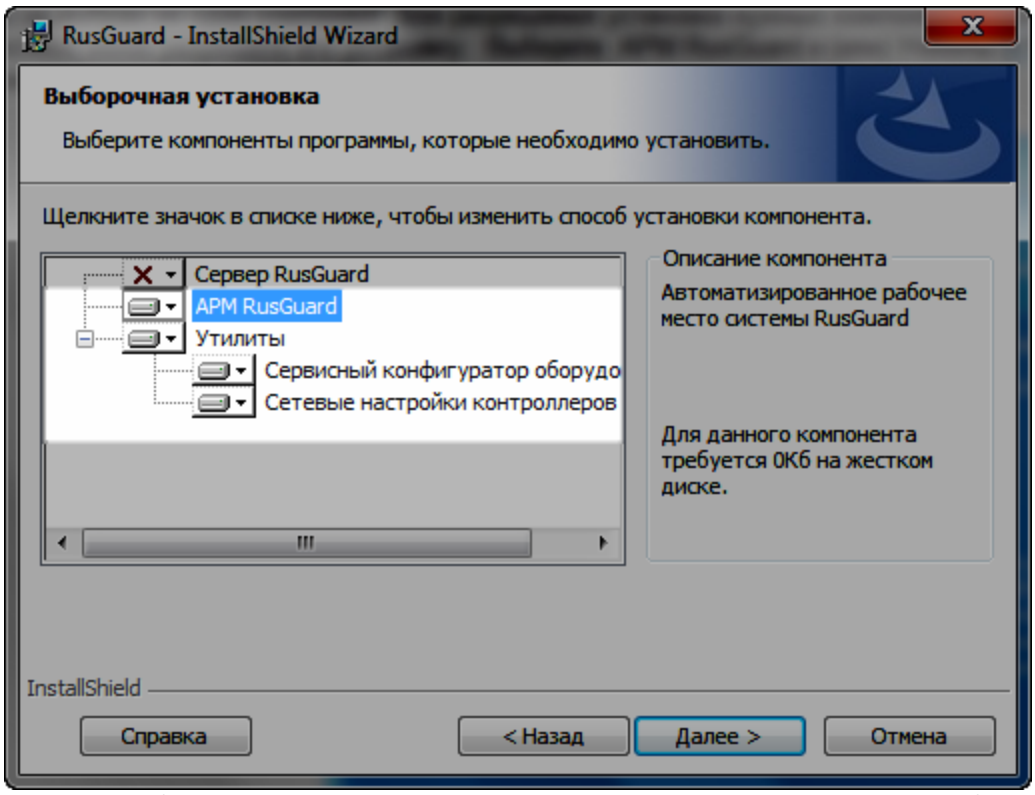


Рисунок 42 - Выбор элементов ПО для установки. На рисунке показан вариант, когда для установки выбраны все компоненты, кроме серверной части

6. На следующем этапе выполняется автоматическая проверка выполнения предварительных требований к установке. Если все они выполнены, вы можете сразу перейти к следующему шагу.
7. Запустите процесс установки (Далее >).

Мастер автоматически выполнит установку выбранных компонентов. В случае отсутствия ошибок, через несколько минут отобразится сообщение о завершении процесса (см. рис. 43).

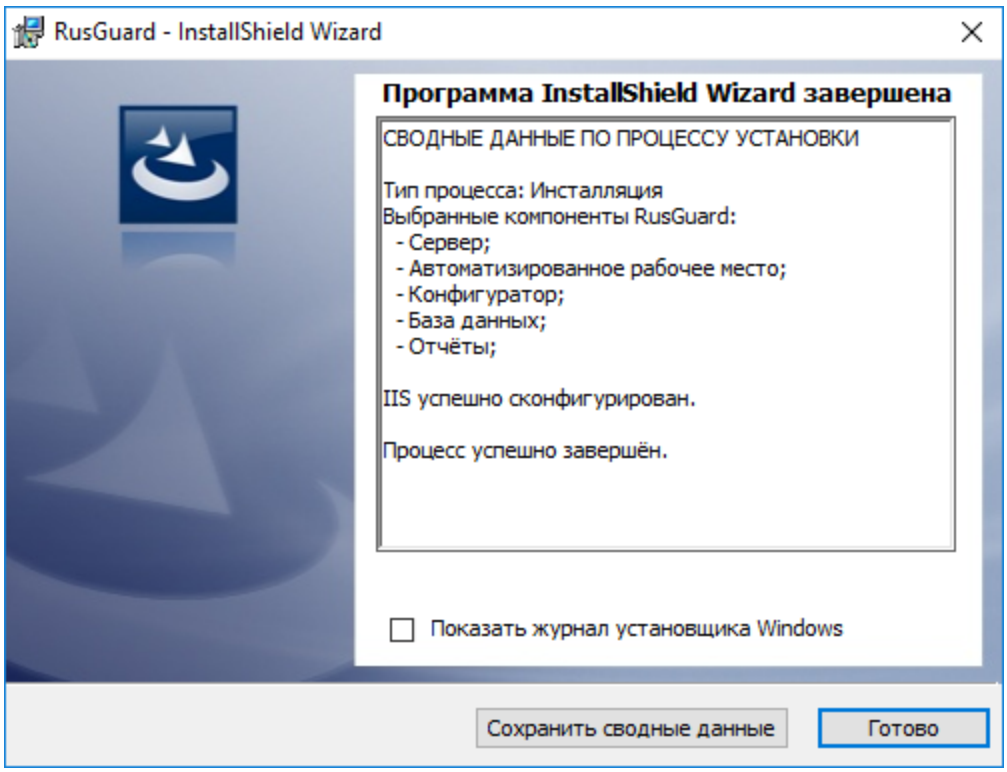


Рисунок 43 - Завершена установка АРМ RusGuard

8. Прежде чем выйти из мастера установки, пользователь может сохранить данные о процессе установки, а также вызывать журнал установщика. Чтобы завершить процесс, нажмите на кнопку Готово.

Быстрый старт

Используя данный раздел, пользователь может оперативно создать карточку сотрудника и оформить ему пропуск через определенную точку доступа (см. рис. 1). Для корректного выполнения всех операций должна быть выполнена установка (монтаж) и первичная настройка всех необходимых программных и аппаратных средств (контроллеров).

Оборудование подключается по LAN (см. также раздел "Периферийные устройства").

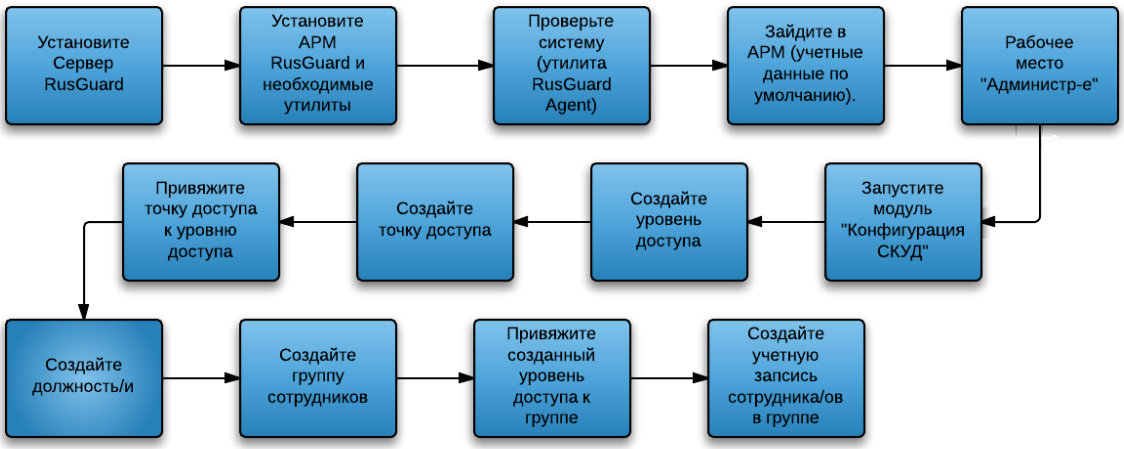
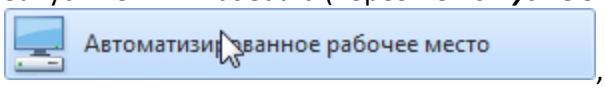


Рисунок 1 - Быстрый старт. Общая схема.
Используйте ссылки на иллюстрации для перехода в соответствующие разделы

Для того чтобы оперативно развернуть программный комплекс RusGuard Soft.

1. Выполните процедуру экспресс установки сервера RusGuard 36, а также установите АРМ RusGuard 61 и другие необходимые компоненты программного комплекса.

Проверьте работоспособность системы, используя утилиту RusGuard агент 301.

2. Запустите АРМ RusGuard (через меню ***Пуск*** ОС Windows **>** папка RusGuard **>** строка 

, либо через ярлык  на рабочем столе или в панели задач).

При загрузке необходимо ввести адрес сервера и учетные данные (см. табл. 1). При первой загрузке поля формы ввода учетных данных пустые, в дальнейшем автоматически загружаются данные, использованные текущим пользователем ПК (см. рис. 2).

В качестве логина для первого запуска АРМ RusGuard используется имя "*admin*" (то есть, первый пользователь автоматически загружает все модули АРМ в качестве администратора, имеющего полный доступ к функциям АРМ), пароль не требуется.

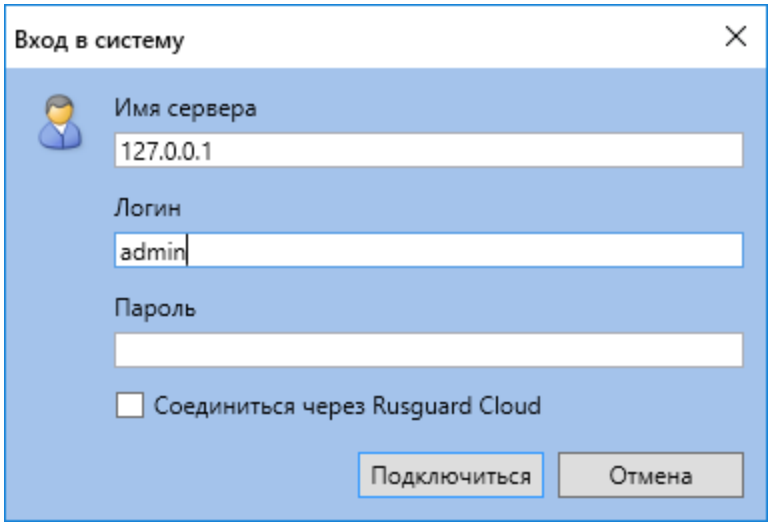


Рисунок 2 - Ввод учетных данных пользователя АРМ RusGuard

Обратите внимание, что в ***Диспетчере служб IIS*** (***Панель управления*** > ***Все элементы панели управления*** > ***Администрирование***) должен быть запущен Default Web Site. В противном случае при попытке запуска АРМ возникает ошибка.

Таблица 1 - Формат заполнения поля Имя сервера	
Тип конфигурации	Формат поля

Локальный вариант, АРМ запускается с ПК, на котором установлен сервер RusGuard	`localhost`
	`127.0.0.1 (предпочтительный вариант)`
	`Имя компьютера`
	Подсказка Чтобы узнать имя компьютера, откройте ***Панель управления > Система и безопасность > Система > Просмотр имени этого компьютера*** (в разных версия ОС Windows последовательность действий и окон может незначительно различаться)

Распределенная архитектура, АРМ и сервер RusGuard разнесены	`IP-адрес сервера (предпочтительный вариант)` `Имя сервера`

Подсказка APM RusGuard поддерживает все стандартные комбинации клавиш ОС Windows (например, ***Ctrl + C*** для копирования или ***Ctrl + V*** для вставки текста).

После ввода учетных данных загружается список предустановленных рабочих мест, которые по умолчанию доступны администраторам АРМ:

- ***Администрирование***
- ***Планы и отчеты***

В дальнейшем возможна настройка разграничения прав доступа к АРМ (в зависимости от полномочий оператора).

3. Выберите АРМ ***Администрирование*** и нажмите на кнопку Ок.

4. Зайдите в модуль ***Конфигурация СКУД***.

В левой части экрана отобразится дерево функций (см. рис. 3).

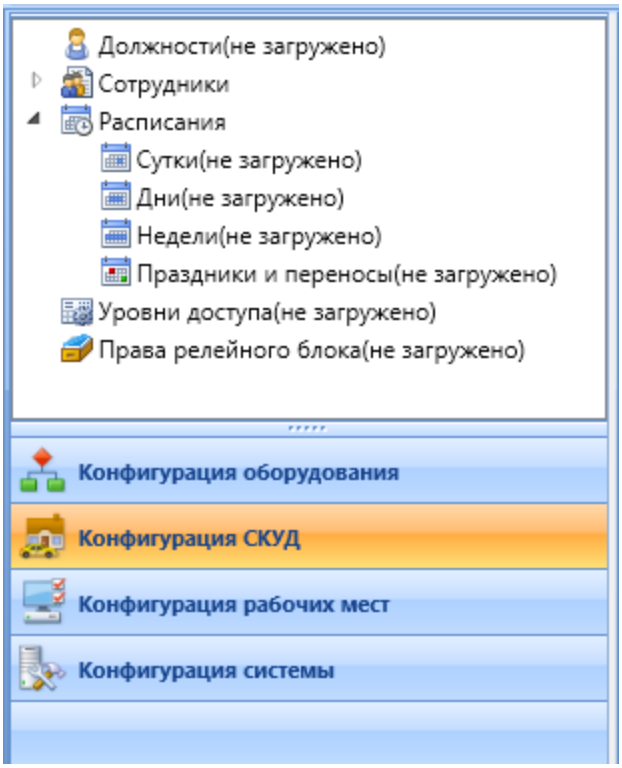


Рисунок 3 - Функции модуля Конфигурация СКУД

5. Зайдите в список ***Уровни доступа***. При первом запуске системы этот список пуст.
6. Создайте уровень доступа.

Для этого выполните следующую последовательность действий:

i. Нажмите на кнопку ***Добавить уровень доступа*** в панели инструментов модуля ***Конфигурация СКУД***.

Загрузится диалоговое окно для ввода уровня доступа.

ii. Заполните поле ***Имя*** (обязательно) и, если необходимо, поле ***Описание***. Нажмите на кнопку Добавить.

Новый уровень доступа появится в списке ***Уровни доступа*** под введенным пользователем именем.

Пользователь может создать любое количество уровней доступа.

7. Привяжите к созданному уровню доступа точку доступа.

Для этого выполните следующую последовательность действий:

i. Установите курсор мыши на строку созданного уровня доступа. Убедитесь, что в центральной части окна активна вкладка ***Точки доступа***. В этой вкладке отображается список настроенных для уровня доступа точек, но при первом запуске АРМ этот список пуст.

ii. Нажмите на кнопку  ***Добавить точку доступа*** в панели инструментов модуля ***Конфигурация СКУД***.

Откроется окно ***Добавление точки доступа***. В верхней части окна находится поле ***Устройство точки доступа*** (см. рис. 4).

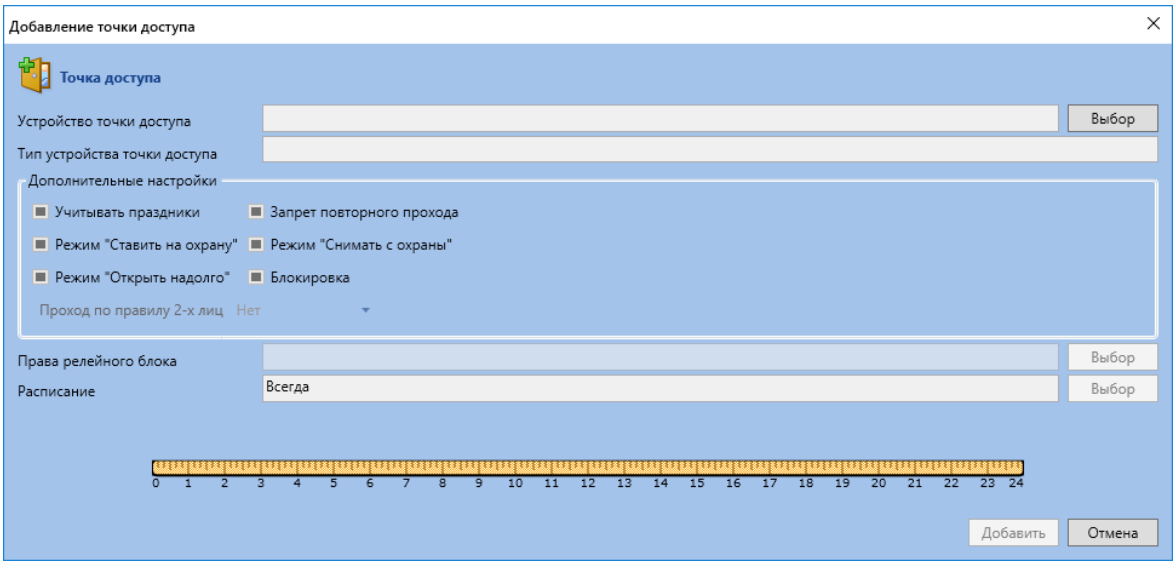


Рисунок 4 - Привязка точки доступа к уровню доступа

iii. Нажмите на кнопку Выбор напротив поля ***Устройство точки доступа***.

Загрузится окно ***Список точек доступа***. В окне четыре вкладки, в каждой по списку доступных устройств четырех видов: Двусторонние двери, Односторонние двери, Шлагбаумы и Турникеты.

Обратите внимание на особенности создания уровня доступа для точек доступа типа "Шкафы/Витрины" 117.

iv. Установите курсор мыши на строку с названием нужного устройства и нажмите на кнопку Выбрать внизу активного окна.

Данные о выбранной точке доступа загрузятся в окно ***Добавление точки доступа***.

v. Нажмите на кнопку Добавить.

Если ошибок нет, система привяжет точку доступа к текущему уровню доступа. Название точки доступа отобразится в списке на вкладке ***Точки доступа***. Обратите внимание, что по умолчанию проход через вновь созданную точку доступа возможен всегда.

8. Перейдите к пункту ***Должности*** навигационной панели модуля ***Конфигурация СКУД***.

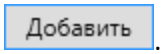
Этот пункт также предназначен для отображения списка, но при первом запуске АРМ он пуст.

9. Создайте одну или несколько должностей (если это необходимо для ведения базы данных сотрудников).

Для этого выполните следующую последовательность действий:

i. Нажмите на кнопку  ***Добавить должность*** в панели инструментов модуля ***Конфигурация СКУД***.

ii. Откроется окно ввода должности. Заполните поля ***Имя*** (обязательно) и ***Описание*** (если требуется).

iii. Нажмите на кнопку 

.

Созданная должность появится в списке ***Должности*** навигационной панели.

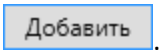
11. Создайте группу сотрудников (если это необходимо или если в системе нет групп сотрудников), а затем карточку сотрудника. Для этого:

12. Находясь в модуле АРМ ***Конфигурация СКУД***, зайдите в список ***Сотрудники***.

13. Нажмите на кнопку  ***Добавить группу сотрудников*** в панели инструментов модуля ***Конфигурация СКУД***.

Откроется окно ***Добавление группы сотрудников***.

14. Заполните поля ***Имя*** (обязательно) и ***Описание*** (если требуется).

15. Нажмите на кнопку 

.

Созданная группа появится в списке ***Сотрудники*** навигационной панели. Обратите внимание, что на вкладке ***Настройки группы сотрудников*** вы можете сразу же привязать к созданной группе метки 206.

Примечание: Группы сотрудников могут содержать любое количество подгрупп.

16. Присвойте заранее созданный уровень доступа созданной группе.

Для этого выполните следующую последовательность действий:

i. Установите курсор на названии созданной группы. Откройте вкладку ***Настройки группы сотрудников*** в центральной части экрана.

ii. Нажмите на кнопку  в панели инструментов.

Активируется возможность управления уровнями доступа группы (область ***Уровни доступа*** внизу главного экрана). По умолчанию список уровней доступа пуст. В правой части экрана отображаются кнопки  и  . Пока список пуст, активна только кнопка  . Кнопка  позволяет удалять уровни доступа, когда список уже сформирован (см. рис. 5).

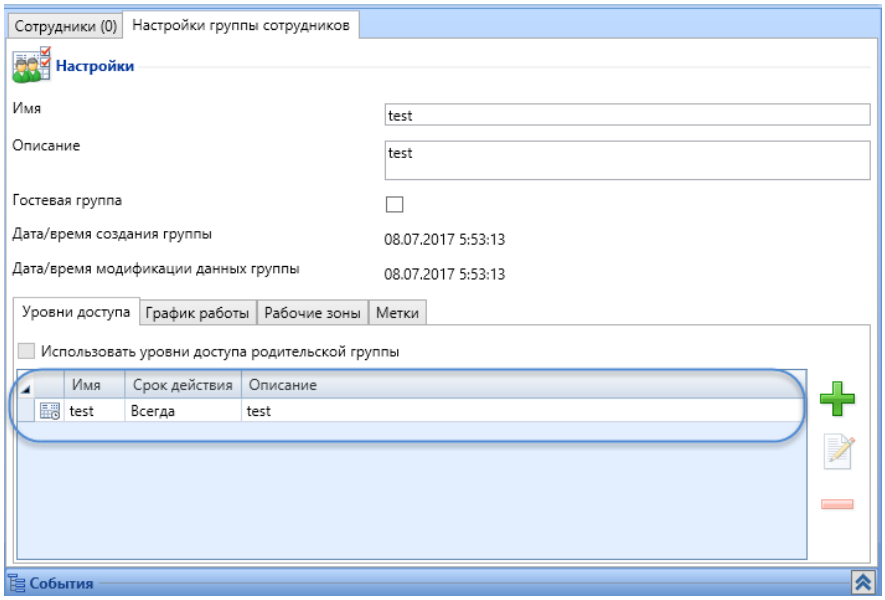
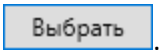


Рисунок 5 - Присвоение уровней доступа группе пользователей

iii. Чтобы добавить уровень доступа группе, нажмите на кнопку  .
Откроется список доступных групп.

iv. Установите курсор на названии нужной группы и нажмите на кнопку  .
Название группы появится в списке уровней доступа группы.

v. Нажмите на кнопку  в панели инструментов. Чтобы отменить все изменения, нажмите на кнопку  ***Отменить изменения***.

17. Создайте карточку сотрудника внутри группы.

Для этого выполните следующую последовательность действий:

i. Зайдите в созданную группу.

ii. Нажмите на кнопку  ***Добавить сотрудника*** в панели инструментов модуля ***Конфигурация СКУД***.

iii. Откроется окно ***Добавление новых сотрудников в группу*** (см. рис. 6). По умолчанию, карточка пустая.

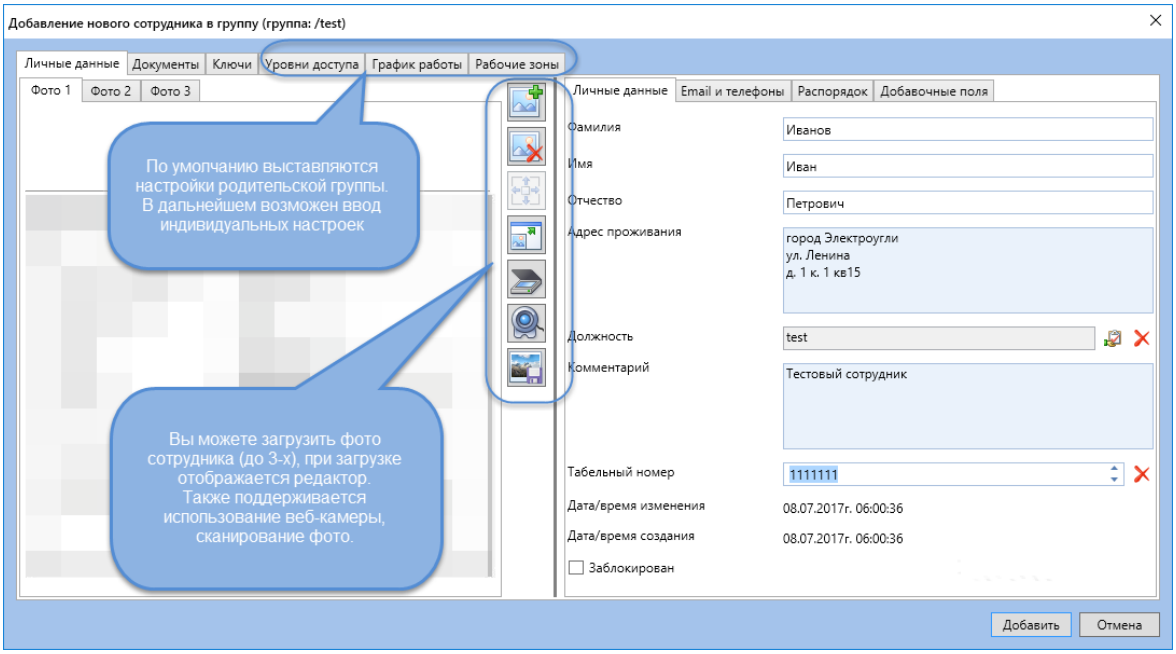
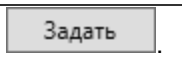


Рисунок 6 - Окно ввода данных о сотруднике

iv. Окно состоит из трех вкладок, предназначенных для ввода персональных данных (см. табл. 2) и их привязки к СКУД для предоставления или ограничения доступа.

Таблица 2 - Краткое описание интерфейса окна ввода данных о сотруднике

Вкладка	Назначение	Обязательные поля (минимальные необходимые данные)
Личные данные	Ввод паспортных и контактных данных лица, создание и сохранение фотографий сотрудника, данных о его положении в организации	Фамилия или Имя или Отчество (любой из вариантов) В этой вкладке также можно указать должность, используя ранее созданный список (нажмите на кнопку )
Ключи	Считывание ключей и PIN-кодов, биометрических данных	Чтобы обеспечить возможность использования карточки, следует ввести хотя бы один ключ. Но сохранение данных возможно и без ключа. PIN-коды могут использоваться дополнительно, если этого требуют внутренние правила
Уровни доступа	Список, в котором отображаются настроенные в системе уровни доступа. По умолчанию используются уровни доступа родительской группы.	Настроек по умолчанию достаточно для функционирования системы. Но пользователь может присвоить пользователю уровень доступа, отличный от уровня родительской группы.

v. Перейдите на вкладку ***Ключи***. Нажмите на кнопку 

.

Загрузится окно ***Добавить ключ*** (см. рис. 7).

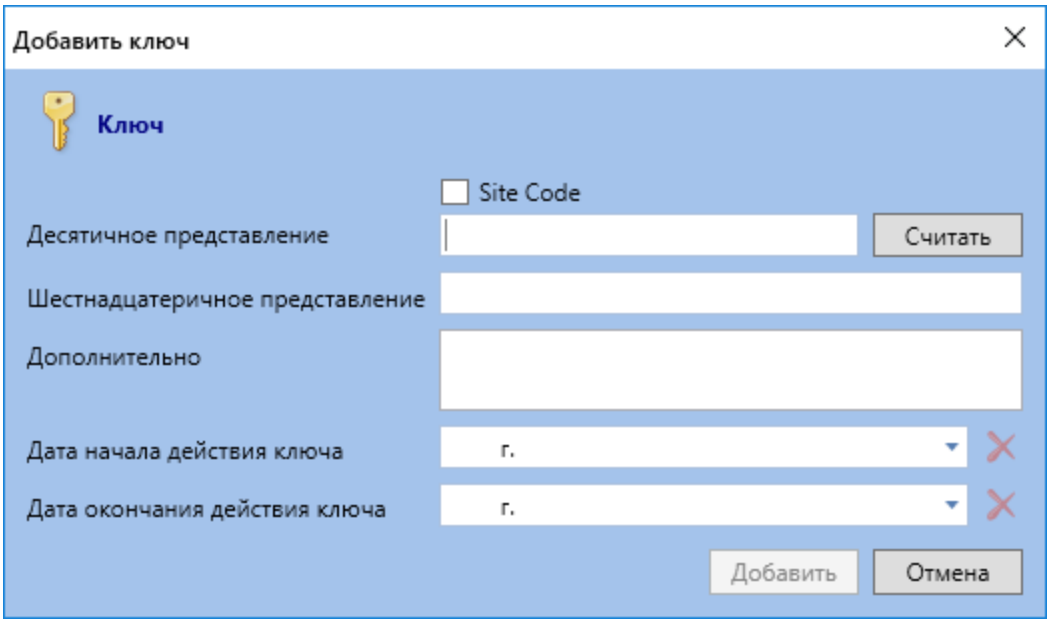


Рисунок 7 - Окно "Добавить ключ"

vi. Заполните форму. Для этого либо считайте код ключа (Считать), используя подключенное устройство для считывания, либо введите код вручную.

Подсказка Если код карты неизвестен, приложите карту к любому контроллеру, подключенному в систему. Затем найдите код в соответствующем отчете и скопируйте его в окно ***Добавить ключ*** (используйте стандартные комбинации клавиш Windows). Будьте внимательны при копировании данных (разрядность кода).

vii. Если это необходимо, введите даты начала и окончания срока действия карточки (если даты не указаны, ключ считается действующим "Всегда"). Нажмите на кнопку Добавить.

Данные о ключе импортируются на вкладку ***Ключи*** карточки сотрудника.

viii. Если используется идентификация по биометрическим параметрам, перейдите на вкладку ***Биометрия ключ 1*** (или 2) (см. рис. 8). Для настройки параметров необходимо присутствие пользователя и наличие подключенного сетевого или настольного считывателя.

Вкладки становятся активными в зависимости от наличия и количества настроенных ключей. Например, если настроен Ключ 1 на соседней вкладке ***Ключи***, то доступна вкладка ***Биометрия ключ 1***.

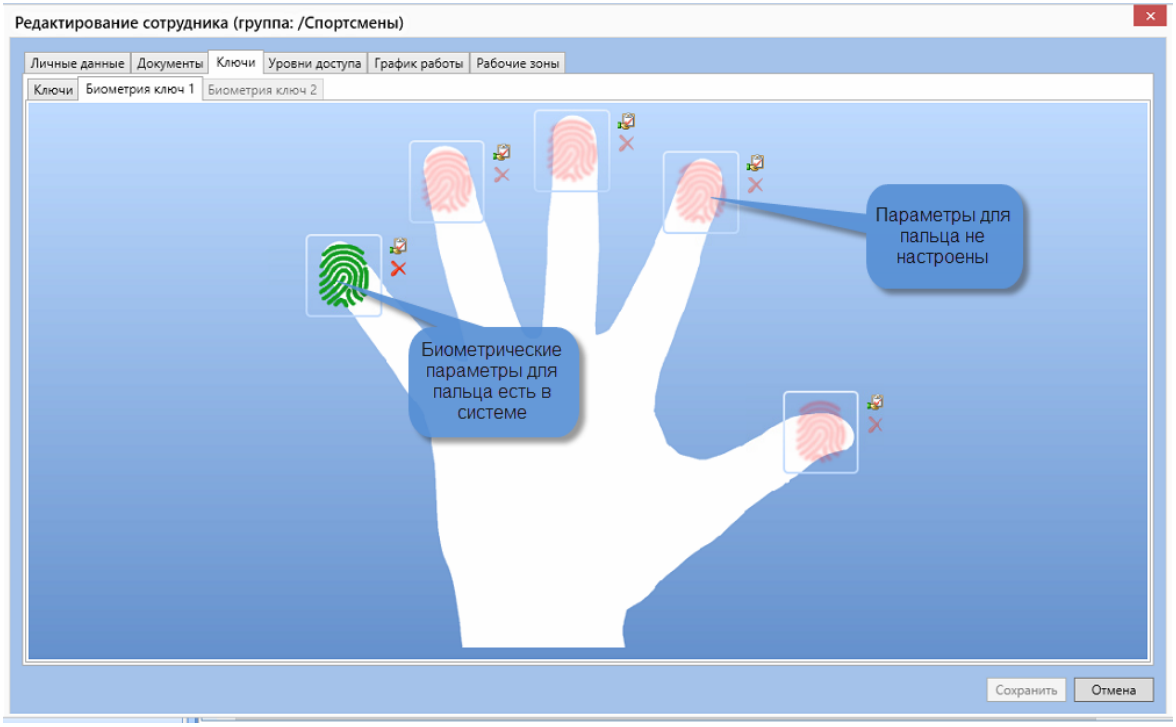


Рисунок 8 Окно настройки биометрических параметров

ix. Щелкните пиктограмму  возле изображения пальца, данные для которого планируется считать и сохранить. Пользователь должен приложить палец к устройству.

x. Если необходимо, выполните повторное считывание (опция ***Проверить***) (см. рис. 9). Сохраните данные. В дальнейшем их можно отредактировать или удалить.

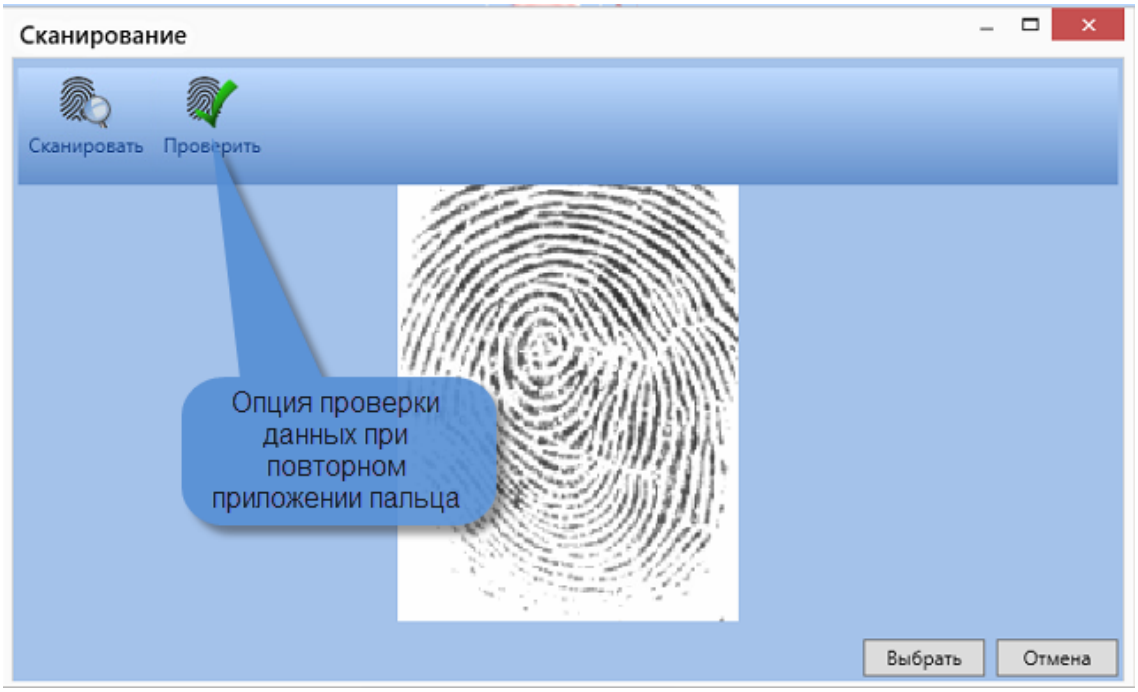


Рисунок 9 - Проверка корректности считанных параметров

xi. Если ввод данных о сотруднике завершен, нажмите на кнопку Добавить.

Система сохранит данные, краткая информация появится на вкладке ***Сотрудники*** в центре экрана (см. рис. 10).

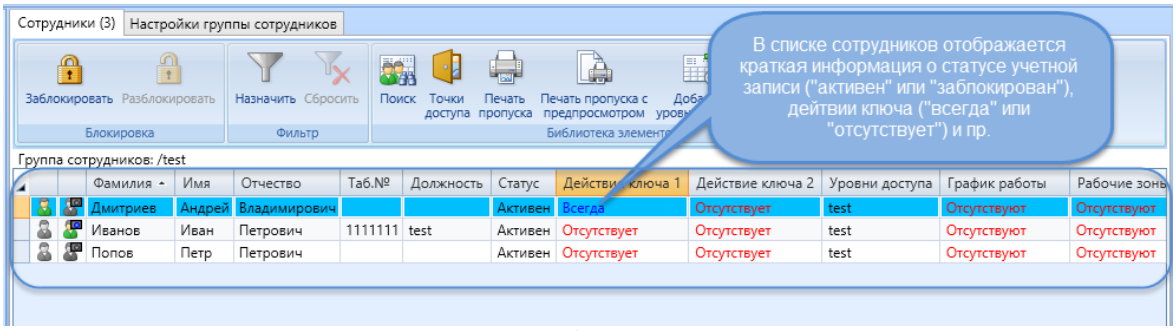


Рисунок 10 - Данные о введенном сотруднике в списке. Обратите внимание, что статус сотрудника активен, только если для него оформлена карточка

После ввода данных о сотруднике, система начинает учет действий, осуществляемых им с помощью ключа, и формирует соответствующую отчетность.

Оперативный мониторинг событий в системе можно осуществлять непосредственно из модуля ***Конфигурация СКУД***, развернув список событий (см. рис. 11).

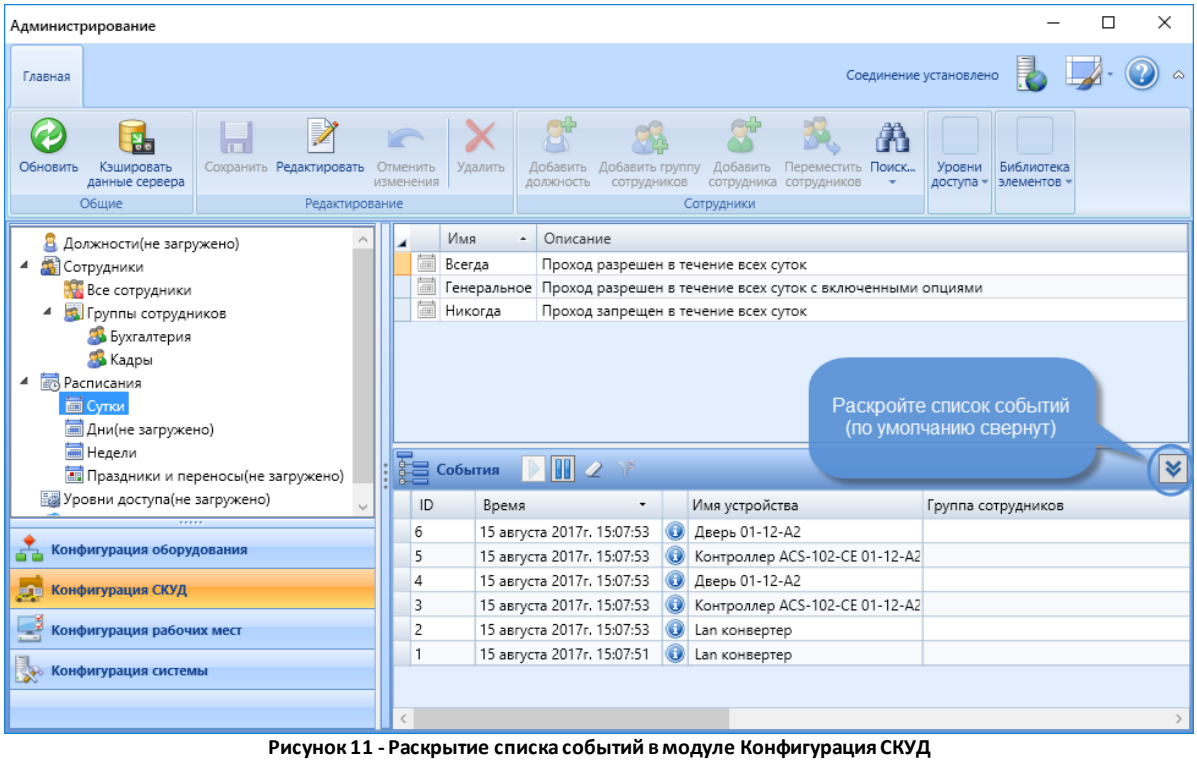


Рисунок 11 - Раскрытие списка событий в модуле Конфигурация СКУД

18. Если необходимо, вы можете немедленно выполнить настройку графиков работы[181]. Использование этой функции позволит немедленно начать формировать отчетность о рабочем времени.
19. Настройте рабочие зоны[190], если необходимо.

После ввода данных о сотруднике, система начинает учет действий, осуществляемых им с помощью ключа, и формирует соответствующую отчетность.

Для обеспечения полноценной работы с ПО RusGuard Soft на следующих этапах необходимо создать требуемые типы рабочих мест (т.е. типов доступа к функциям и модулям ПО), завести пользователей.

Все эти действия выполняются через АРМ RusGuard. Обратите внимание, что в некоторых конфигурациях требуется заведение учетных записей пользователей непосредственно на Сервере отчетов. Это позволяет пользователям обращаться к отчетам через веб-интерфейс, не устанавливая АРМ (если для их работы не нужны другие его модули).

Демонстрационное видео процесса

APM RusGuard

Назначение

APM RusGuard - приложение для управления СКУД, состоящее из нескольких модулей, предназначенных для:

- Настройки самого приложения (составления комбинаций модулей, доступных разным типам пользователей);
- Ведения базы данных пользователей приложения;
- Ведения базы данных сотрудников, т.е. лиц, доступ которых на определенный объект контролирует система;
- Ведения базы данных контрольных устройств;
- Ведения отчетности по действиям сотрудников, а также системным событиям;
- Составления планов доступа;
- Интеграции и синхронизации объектов перечисленных баз данных (списков) для обеспечения функционирования СКУД и сбора данных.

Доступ к APM осуществляется через учетную запись (имя пользователя + пароль).

Интерфейс

Интерфейс модульного приложения APM RusGuard (см. рис. 1) состоит из трех основных элементов

- Панели управления сверху;
- Навигационной панели слева;
- Центрального экрана.

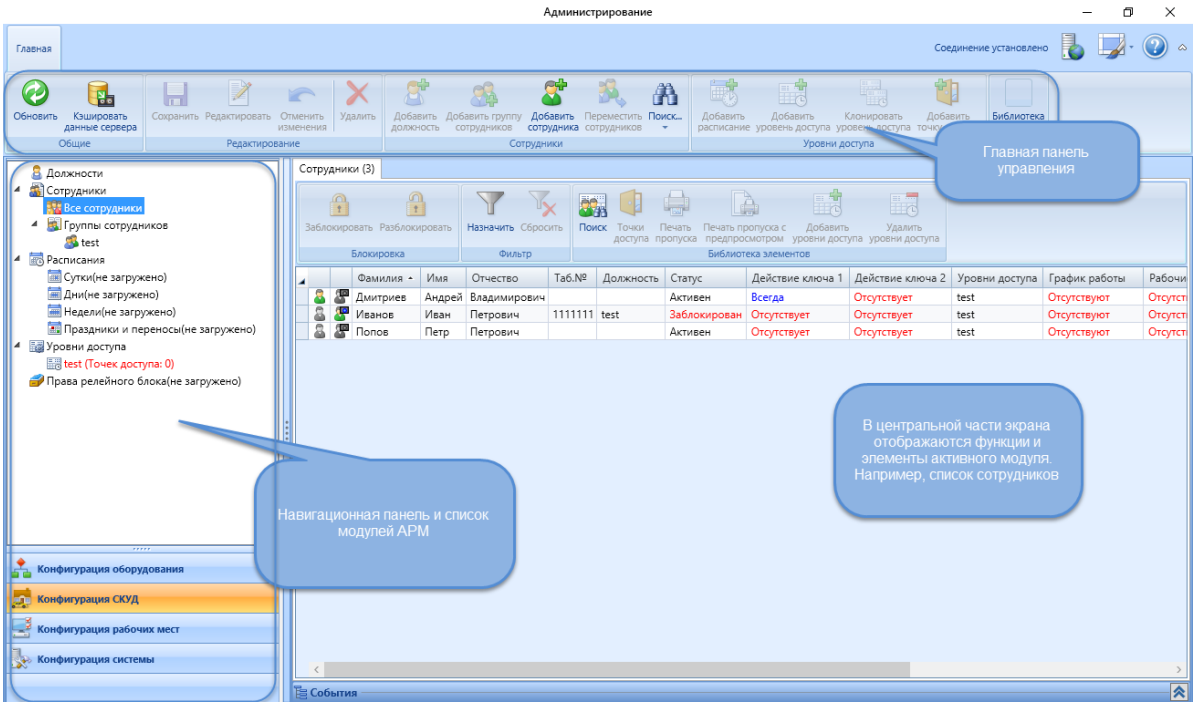


Рисунок 1 - APM RusGuard. Навигационная панель и центральный экран. Пример отображения

В начале работы пользователь выбирает один из доступных модулей в навигационной панели (на иллюстрации выше показан весь список модулей, однако в реальности их количество может быть другим, в зависимости от роли текущего пользователя).

При выборе одного из модулей в навигационной панели раскрывается иерархическая структура модуля (обычно это список элементов базы данных, управление которой выполняется через модуль).

Также, при выборе модуля меняется панель управления наверху экрана. При переходе в определенный модуль на панели управления отображаются все предусмотренные для него кнопки и пиктограммы, но часть из них может быть неактивна. Это значит, что для активизации функции необходимо перейти на другой уровень иерархии выбранного модуля.

Также при выборе модуля (и уровня иерархии внутри него) меняется вид центрального экрана. На иллюстрации выше в центральном экране отображен список всех сотрудников (этот уровень иерархии выбран в навигационной панели). В центральном экране также есть отдельная панель управления.

Стандартные элементы интерфейса ARM RusGuard

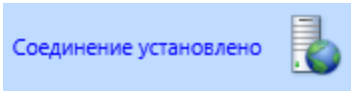
Ряд элементов интерфейса (кнопки, пиктограммы) повторяется во всех модулях и имеет одинаковую функцию.

Таблица 1. Стандартные элементы интерфейса APM RusGuard	
Кнопка/Пиктограмма	Функция

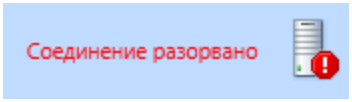
Таблица 1. Стандартные элементы интерфейса APM RusGuard	
	Редактирование настроек. Обычно, нажатие на эту кнопку активирует дополнительные элементы управления, необходимые для редактирования выбранного объекта
	Сохранение изменений
	Отмена изменений
	Удаление выбранного элемента
	Обращение к серверу БД для обновления данных (например, отчетов или списков).
	Развертывание иерархического списка
	Свертывание иерархического списка

Примечание: В APM RusGuard действуют стандартные сочетания клавиш ОС Windows для копирования, вставки, выделения, и т.д. (Ctrl+X, Ctrl+C, Ctrl+V).

В правом верхнем углу отображается состояние соединения с сервером:



- соединение установлено, работает нормально.



- соединение с сервером отсутствует.

Пользователь может уменьшить или свернуть левую боковую панель.

Чтобы уменьшит ширину панели, установите курсор мыши на разделительную линию (см. рис. 2) и потяните влево.

Чтобы скрыть левую панель, щелкните дважды по разделительной линии.

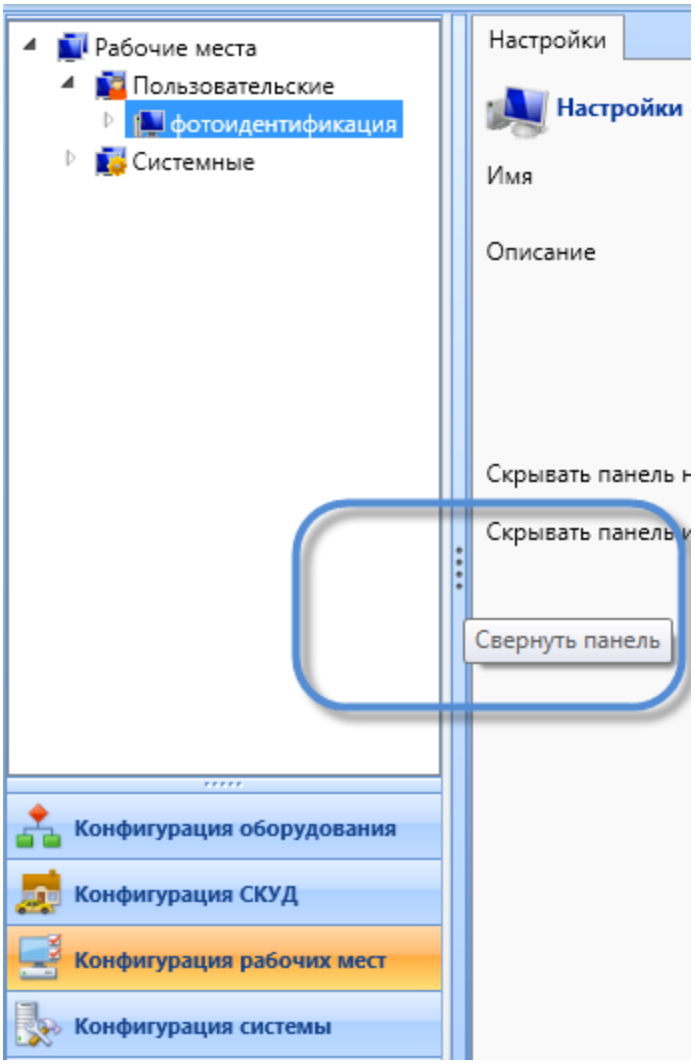


Рисунок 2 - APM RusGuard. Разделительная линия между боковой панелью и центральным экраном

В модулях ***Конфигурация СКУД*** и ***Планы*** отображается список системных событий. По умолчанию список свернут (см. рис. 3), но его можно раскрыть. Для этого щелкните мышью по пиктограмме  в нижней левой части экрана. Чтобы снова скрыть список, щелкните по пиктограме  в нижней правой части экрана.

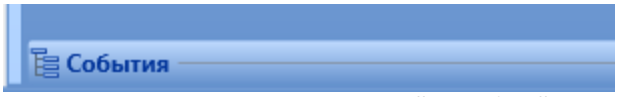


Рисунок 3 - APM RusGuard. Свернутый лог событий

Модуль Конфигурация оборудования

Общие сведения

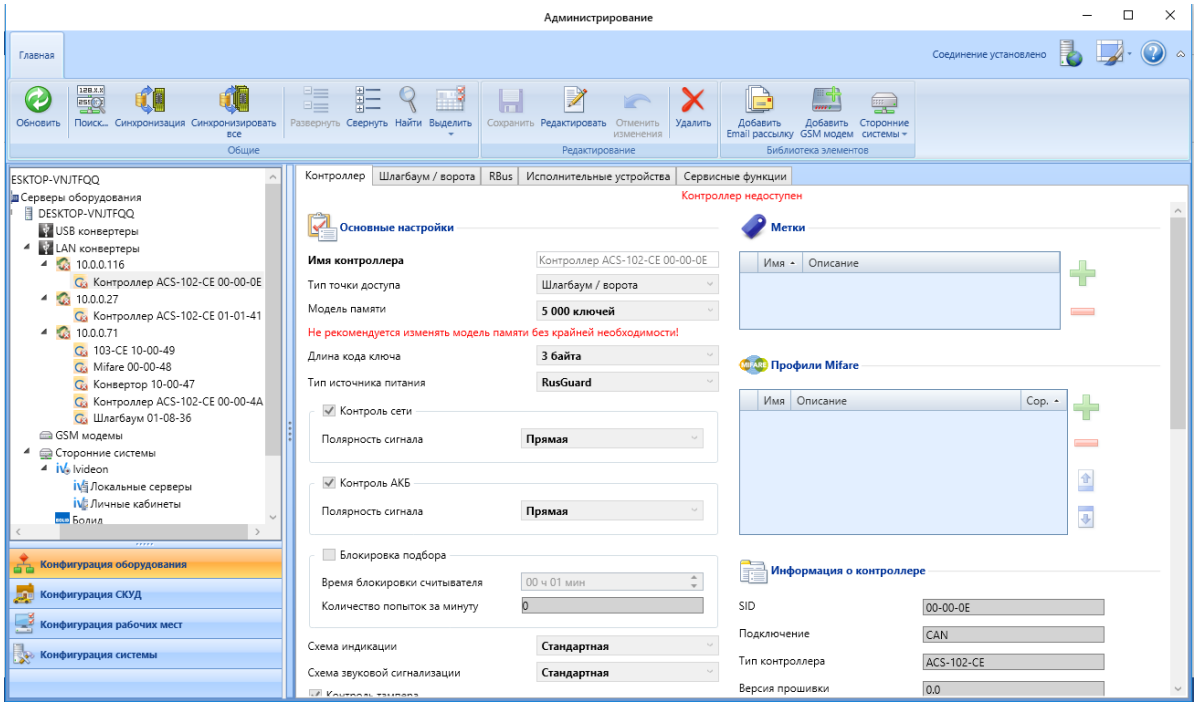


Рисунок 4 - АРМ RusGuard. Модуль Конфигурация оборудования.

Модуль ***Конфигурация оборудования*** (см. рис. 4) предназначен для настройки аппаратной инфраструктуры СКУД, а также другим интегрированным оборудованием и системами (см. раздел "Интеграция и установка стороннего ПО").

Интерфейс модуля

В **левой навигационной панели** отображается иерархический список от сервера к контроллерам.

Контроллеры в списке делятся на две группы:

- Подключенные через CAN-USB конвертеры

Подключенные через LAN-CAN конвертеры

В левой навигационной панели также отображается текущий статус конвертеров (см. табл. 1) и контроллеров (см. табл. 2).

Таблица 1 - Статусы конвертера	
Пиктограмма	Значение
	Конвертер подключен и функционирует нормально
	Не совпадают настройки контроллера и сервера
	Соединение с конвертером отсутствует ("конвертер не подключен")

Таблица 1 - Статусы конвертера	
	Статус устройства не определен, запуск процесса опроса
	Конвертер удален из БД
	Потеряно соединение с сервером, через который подключен конвертер

Таблица 2 - Статусы контроллера	
Пиктограмма	Значение
	Устройство подключено и функционирует нормально
	Соединение с контроллером отсутствует
	Статус устройства не определен, запуск процесса опроса
	Контроллер удален из БД
	Сервер оборудования недоступен
	Обобщенный статус тревоги. Взлом, тревога охранного входа, разряд АКБ, отсутствие доступа к сети и т.д.
	Не совпадают настройки драйвера из базы данных и контроллера (необходимо выполнить синхронизацию)

В верхней панели управления расположены кнопки для выполнения операций по настройке оборудования (прежде всего, контроллеров). Если кнопка неактивна, это означает, что операция невозможна в настоящий момент, либо неприменима к выбранному в иерархическом списке элементу.

Часть кнопок имеет стандартные функции 76.

Используя модуль, пользователь может:

- Редактировать настройки контроллеров
- Управлять функциями и режимами работы точек доступа, оборудованных контроллерами (дверей, турникетов, двухсторонних дверей и т.д.)

Поиск устройств для подключения

ПО RusGuard поддерживает подключение контроллеров к серверу по LAN.

В режиме CAN-LAN контроллеры могут объединятся в сеть двумя способами:

- каждый контроллер подключается непосредственно к сети Ethernet;
- группа контроллеров объединяется по шине CAN; последний\первый подключается к сети Ethernet.

Соответственно, предусмотрено два режима поиска для каждого типа подключений.

Также, для CAN-LAN устройств, помимо широковещательного поиска, предусмотрена функция поиска по IP-адресу, она позволяет находить устройства, находящиеся за пределами локальной сети (разделенные шлюзами, и т.д.).

Широковещательный поиск (LAN-устройства)

Для того чтобы найти CAN-LAN устройства (широковещательный поиск):

1. Загрузите модуль ***Конфигурация оборудования***.
2. Нажмите на кнопку  в верхней панели управления.

Откроется окно ***Поиск устройств***

3. Оставайтесь на вкладке ***LAN устройства***. Нажмите на кнопку 

.
4. Откроется окно для выбора сервера оборудования (см. рис. 5). Выберите нужный вариант и подтвердите выбор.

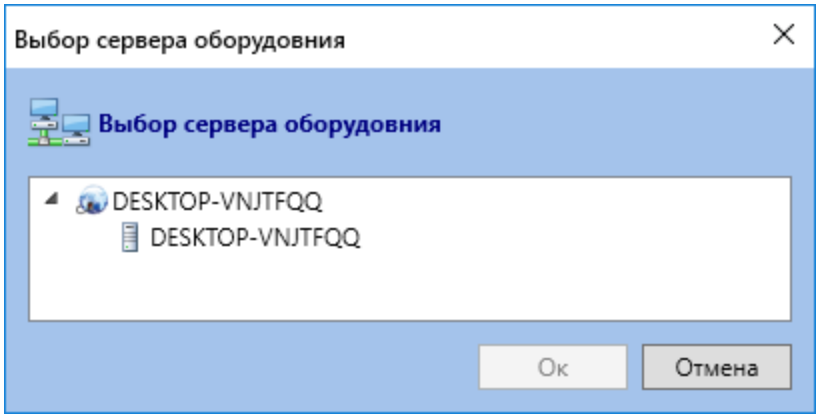


Рисунок 5 - Выбор сервера оборудования для поиска устройства

Система выполнит поиск, сообщая о процессе в отдельном окне. Затем загрузится список найденных конвертеров. При щелчке мыши в строке с информацией об определенном конвертере ниже загружается список подключенных через него контроллеров (см. рис. 6).

Обратите внимание, что при поиске LAN устройств в списке результатов также указывается способ выполнения поиска.

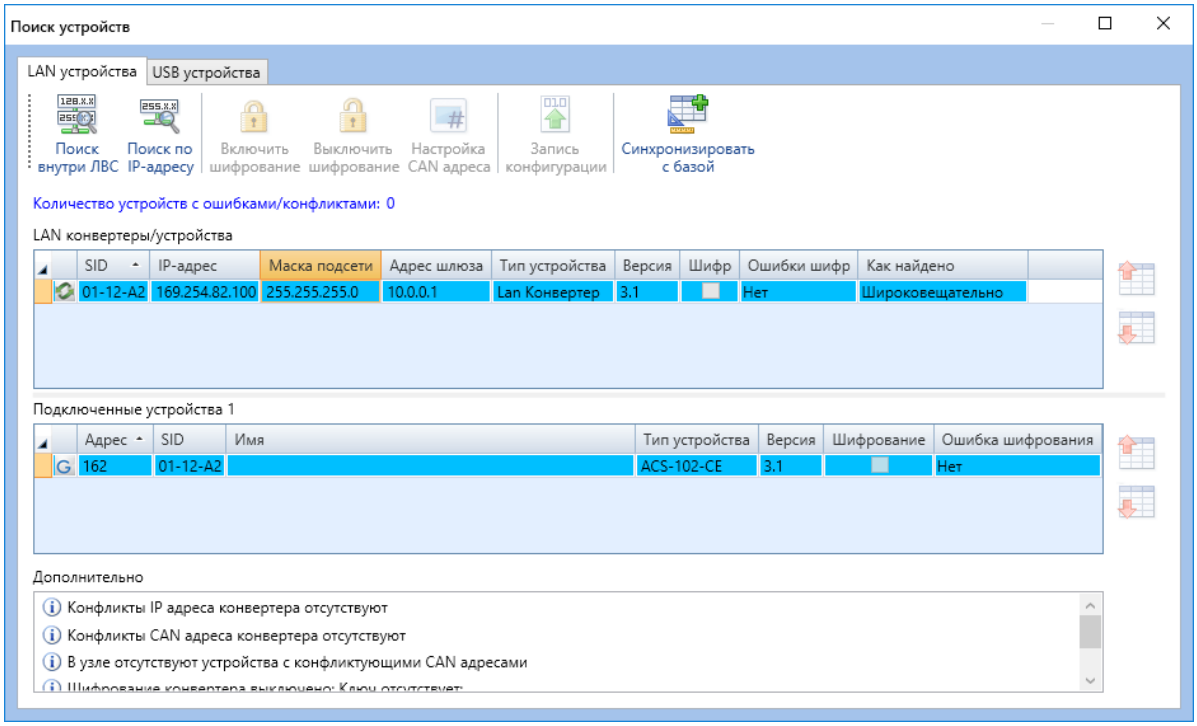


Рисунок 6 - APM RusGuard. Модуль Конфигурация оборудования. Результат широковещательного поиска CAN-LAN устройств

Используя список контроллеров, пользователь может редактировать CAN-адреса контроллеров.

Для того чтобы найти устройство по IP-адресу:

1. Загрузите модуль Конфигурация оборудования.
2. Нажмите на кнопку  в верхней панели управления.

Откроется окно ***Поиск устройств***

3. Оставайтесь на вкладке ***LAN устройства***. Нажмите на кнопку 

.

Откроется окно для ввода IP-адреса (см. рис. 7).

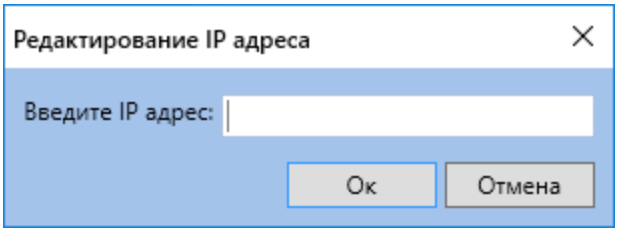
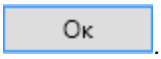


Рисунок 7 - APM RusGuard. Модуль Конфигурация оборудования. Окно ввода IP-адреса для поиска

4. Введите IP-адрес и нажмите на кнопку 

.

Отобразится окно для выбора сервера.

5. Выберите нужный сервер и нажмите на кнопку Ок.

Система приступит к поиску. В случае успешного результата, данные об устройстве будут выведены в окне результатов.

Поиск устройств, подключенных по USB

Для того чтобы выполнить поиск CAN-USB устройства:

1. Загрузите модуль ***Конфигурация оборудования***.
2. Нажмите на кнопку  в верхней панели управления.

Откроется окно ***Поиск устройств*** (при первом запуске окно пустое) (см. рис. 8).

Примечание: При повторном запуске поиска система предложит сначала очистить окно.

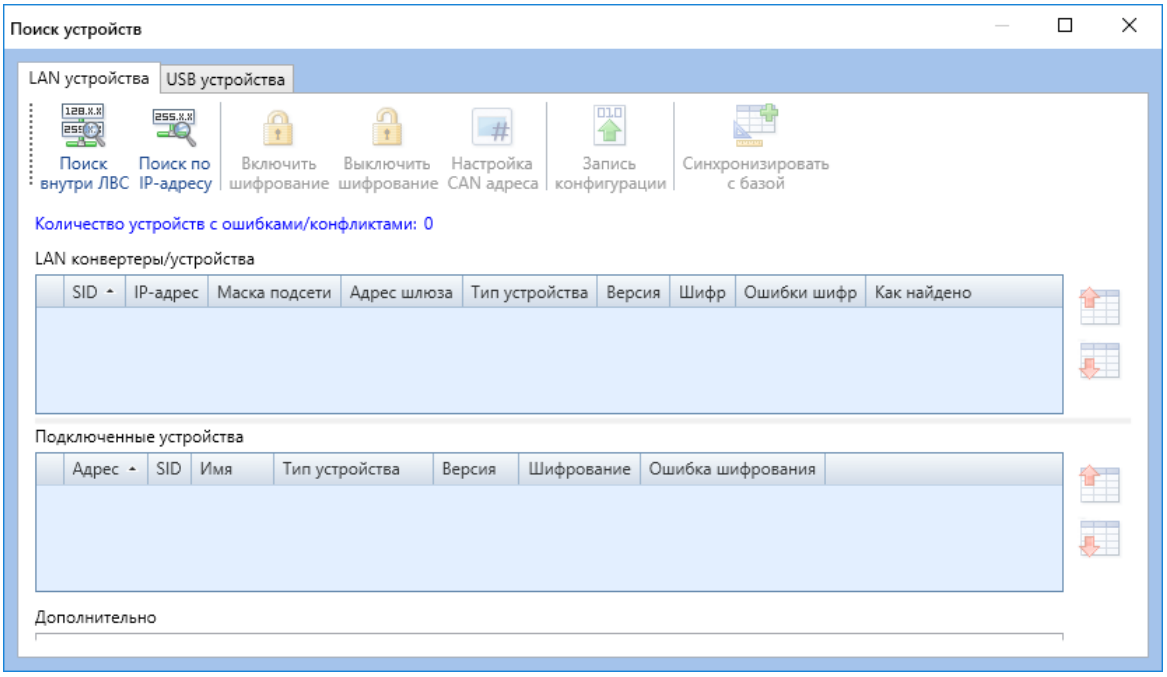


Рисунок 8 - АРМ RusGuard. Модуль Конфигурация оборудования. Окно поиска

3. Перейдите на вкладку ***USB устойства***, нажмите на кнопку  в панели управления.

Загрузится список серверов оборудования.

4. Выберите тот сервер, на котором требуется выполнить поиск. Нажмите на кнопку Ок.

Примечание: Поиск может быть выполнен с любого сервера, находящегося в системе, обслуживаемой ПО RusGuard.

Система выполнит поиск и отобразит его результаты в отдельном окне.

5. Нажмите на кнопку Закрыть.

Данные о найденных устройства загрузятся в основное окно поиска. Сначала в верхней части окна (список ***USB-конвертеры***) отобразится список найденных USB-конвертеров и краткая информация о них, включая статус подключения.

6. Щелкните мышью по нужному устройству, чтобы загрузить ниже список подключенных к нему контроллеров.

В списке ***Подключенные устройства*** загрузится список контроллеров и краткая информация о каждом из них, включая текущий статус подключения.

Ниже, в области ***Дополнительно***, отображаются статусы операций поиска. При отсутствии в системе ошибок выводятся общая информация. При обнаружении конфликтов в системе в окне отображается информация об ошибках.

Внимание: Если в процессе поиска обнаружены ошибки, дальнейшее добавление устройств в систему невозможно.

Возможные ошибки:

- совпадают CAN адреса у устройств на шине. Необходимо изменить CAN-адрес 85 одного из них.
- попытка добавления устройства с SID, который уже есть в БД с другим адресом CAN. Для устранения ошибки необходимо изменить CAN-адрес 85 в соответствии с адресом в БД, выйти из окна поиска, удалить устройство из БД и выполнить операцию повторно.

Редактирование CAN-адреса

CAN-адреса присваиваются устройствам в интервале от 1 до 255. В редких случаях адреса устройств, установленные по умолчанию, совпадают. В таком случае необходимо изменить CAN-адрес одного из них.

Для того чтобы отредактировать CAN-адрес:

1. Выполните поиск USB или LAN устройства. В списке результатов выделите нужный контроллер в списке ***Подключенные устройства*** окна ***Поиск устройств***.
2. Щелкните по строке с данными о контроллере дважды правой кнопкой мыши, либо нажмите на кнопку  в верхней панели экрана.

Откроется окно, со списком доступных номеров CAN (от 1 до 255, минус уже занятые адреса) (см. рис. 9).

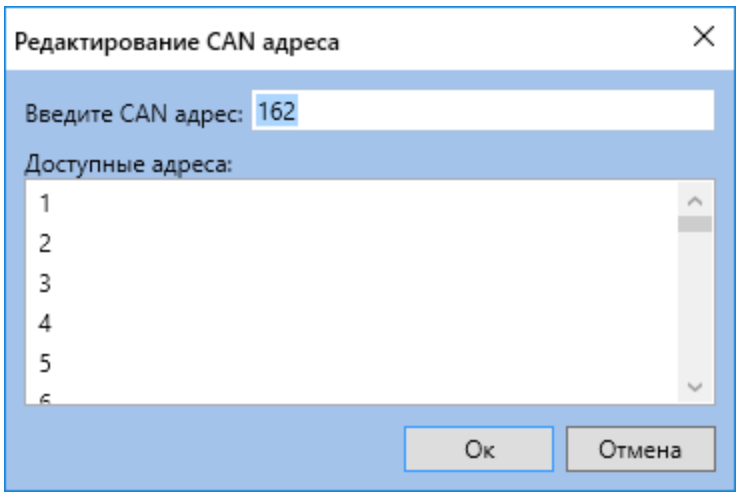


Рисунок 9 - АРМ RusGuard. Модуль Конфигурация оборудования. Редактирование CAN-адреса

3. Выберите нужный номер в списке ***Доступные адреса*** и выделите его в списке.
4. Номер отобразится в поле ***Введите CAN адрес*** вместо текущего.
5. Нажмите на кнопку Ок.

Система применит требуемые изменения.

Синхронизация устройств с БД

Синхронизация с БД выполняется при подключении нового устройства или при изменении конфигурации старого.

Синхронизация нового устройства

Поиск необходимо выполнять, если к системе, обслуживаемой ПО RusGuard были подключены новые устройства. После того, как устройство успешно найдено, необходимо синхронизировать его с базой данных, т.е. интегрировать его в базу данных для полноценного управления устройством через АРМ RusGuard.

Для того чтобы выполнить синхронизацию нового устройства с базой данных:

1. В зависимости от типа нового устройства, выполните поиск наиболее подходящим методом.
2. После того, как устройство (устройства) найдено, нажмите на кнопку  ***Синхронизировать с базой*** в верхней панели инструментов окна поиска.

Кнопка доступна только тогда, когда в списке результатов есть новые устройства**.**

Система выполнит конфигурацию устройства и его интеграцию с текущей БД.

Найденные устройства появятся в иерархическом списке элементов системы (устройство) модуля ***Конфигурация оборудования***.

Синхронизация изменений конфигурации устройства

Функция синхронизации необходима для принудительной перезаписи всех параметров и ключей из БД в выбранный контроллер  ***Синхронизировать*** или все контроллеры в системе  ***Синхронизировать все***.

При выявлении различий конфигурации устройства и сервера, устройство помечается пиктограммой  в навигационной панели слева. Несоответствие конфигураций может возникнуть при изменении параметров устройства через утилиту ***Сервисный конфигуратор оборудования*** 321 либо в результате временного использовании данного устройства под управлением другого сервера.

Для того чтобы синхронизировать одно устройство с БД:

1. Загрузите модуль ***Конфигурация оборудования*** APM RusGuard.
2. Найдите нужный контроллер в левой навигационной панели и выделите его.
3. Нажмите на кнопку  ***Синхронизация*** в верхней панели инструментов.

Система синхронизирует новые настройки с БД.

Обратите внимание, что кнопка активна, только если операция имеет смысл (т.е. есть изменения в конфигурации).

Устройство, конфигурация которого была изменена, можно найти по отображаемому статусу 80.

Для того чтобы синхронизировать несколько устройств с БД:

1. Загрузите модуль ***Конфигурация оборудования*** APM RusGuard.

Если конфигурация одного или нескольких контроллеров была изменена,  ***Синхронизировать все*** кнопка в верхней панели инструментов активна

2. Нажмите на кнопку  ***Синхронизировать все*** в верхней панели инструментов.

Система выполнит синхронизацию настроек.

Обратите внимание, что кнопка активна, только если операция имеет смысл (т.е. есть изменения в конфигурации).

Устройство(а), конфигурация которого(ых) была изменена, можно найти по отображаемому статусу 80.

Управление контроллерами и конвертерами

Если в навигационной панели слева выбран конкретный контроллер, открывается экран настройки функций самого устройства и точки доступа, на которой оно установлено (см. рис. 10).

- На вкладке ***Контроллер*** 88 вводятся общие настройки устройства;
- На вкладке ***Дверь/Две двери/Турникет/Шлагбаум-Ворота/Шкафы-Витрины*** 92 (зависит от типа точки доступа) вводятся настройки точки доступа. Название вкладки зависит от типа точки доступа, который указывается на вкладке ***Контроллер***;
- Вкладка ***Сервисные функции*** 121 позволяет управлять контроллером и точкой доступа (отображается не для всех типов точек доступа).
- Вкладка ***Исполнительные устройства*** отображает информацию об исполнительных устройствах контроллера.
- Вкладка ***Rbus*** предназначена для настройки параметров интерфейса RBus, необходимого при использовании smart-карт MiFare.

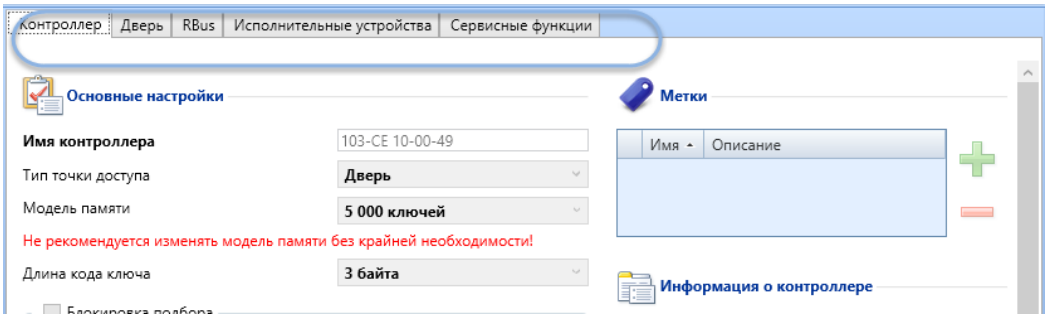


Рисунок 10 - АРМ RusGuard. Модуль Конфигурация оборудования. Настройка контроллера. Вид по умолчанию

Управление настройками контроллера

Редактирование настроек режима функционирования контроллера

Для того чтобы выполнить настройку контроллера:

1. Найдите нужный контроллер через функцию поиска или в списке в левой навигационной панели.
2. Перейдите на вкладку ***Контроллер*** (вкладка по умолчанию).
3. Нажмите на кнопку  ***Редактировать*** в верхней панели инструментов.

Редактируемые поля активируются.

Предупреждение: для разных типов контроллеров набор настроек может отличаться от описанного.

4. Внесите нужные значения в поля области ***Основные настройки*** (см. рис. 11 и табл. 3)).

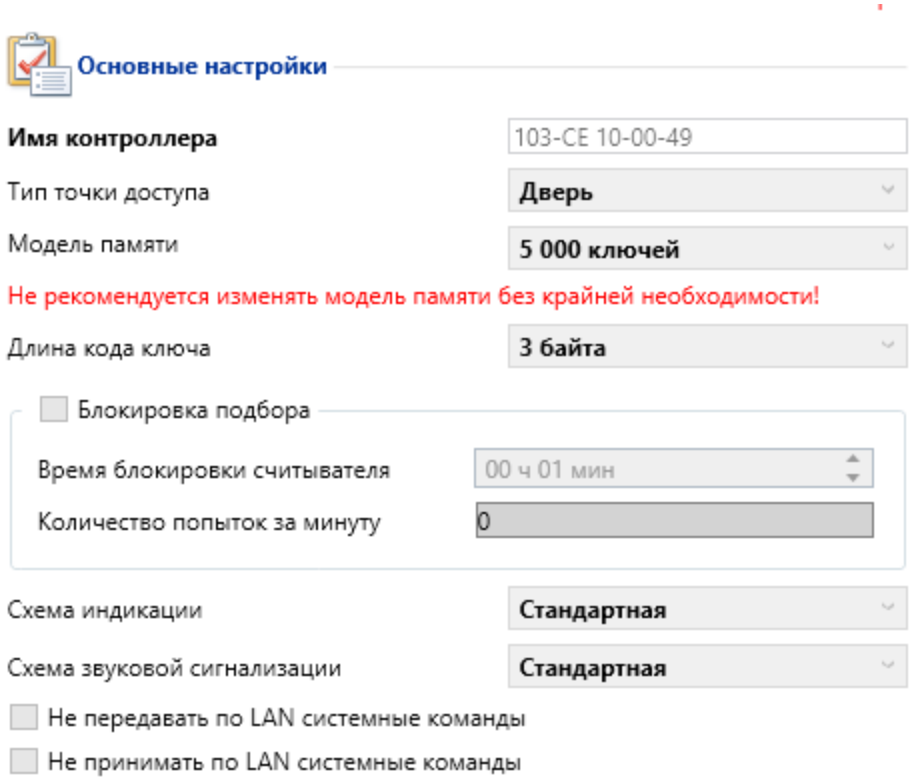


Рисунок 11 - APM RusGuard. Модуль Конфигурация оборудования. Настройка контроллера

Таблица 3 - Основные настройки контроллера	
Настройка	Описание
Имя контроллера	Поле ввода. Имя контроллера. По умолчанию в этом поле отображается название модели и серийный номер. Пользователь может ввести любое другое значение (максимум 32 символа), измененные данные сохраняются в самом устройстве
Тип точки доступа	Список. Вариант по умолчанию: Дверь. Доступны также Двусторонняя дверь, Шлагбаум/ворота, Шкафы/Витрины и Турникет. От выбранного варианта зависят настройки в соседней вкладке (настройки точки доступа) **Предупреждение**: Для разных типов контроллеров список доступных типов точек доступа может отличаться
Модель памяти	Список. стандартное устройство способно запоминать от 5 до 32 тысяч ключей.

Таблица 3 - Основные настройки контроллера		
		Предупреждение: По умолчанию установлено минимальное значение, и его не рекомендуется менять без крайней необходимости
Длина кода ключа		Список. По умолчанию установлено значение 3 байта. Параметр определяет значимую длину кода ключа
Блокировка подбора	***Время блокировки считывателя***	
	Количество попыток за минуту	
Тип источника питания		Список. Вариант ***RusGuard*** подразумевает использование встроенного блока питания (модели контроллеров -В, -ВМ). Если выбран вариант ***Внешний БП***, входы РС1 и РС2 используются для контроля внешнего БП (тип входов – “сухой контакт”)
Контроль сети		Флаг. Доступен при выборе типа источника питания ***Внешний БП***. Выполняет контроль сигнала пропадания напряжения питания на внешнем БП (вход РС1)
Контроль АКБ		Флаг. Доступен при выборе типа источника питания ***Внешний БП.*** Выполняет контроль сигнала разряда АКБ на внешнем БП (вход РС2)
Контроль тампера		Флаг. Определяет необходимость контроля тампера корпуса контроллера. По умолчанию отключен
"Тихий" режим считывателей		Флаг. По умолчанию не используется. При установке флага на зуммер считывателя не выводятся сигналы разряда АКБ, пропадания Сети, сигнала незакрытой двери и ряд других
Схема индикации		
Схема звуковой индикации		
Не передавать по LAN системные команды		
Не принимать по LAN системные команды		

5. Добавьте метки к контроллеру, если требуется ограничить доступ к нему операторов. Для этого:

a. Щелкните пиктограмму  в области ***Метки*** (по умолчанию список меток пустой, если же его использовали, в нем отображаются ранее добавленные метки) (см. рис. 12).

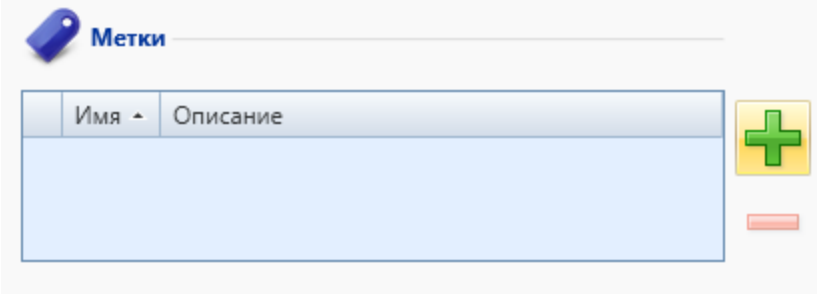


Рисунок 12 - АРМ RusGuard. Модуль Конфигурация оборудования. Настройка контроллера (метки)

Откроется окно ***Выбор меток*** со списком доступных меток (отображаются все метки системы 206, кроме тех, которые уже привязаны к данному устройству).

b. Выделите нужную метку в списке и нажмите на кнопку Добавить.

Выбранная метка появится в списке.

Чтобы удалить метку из списка привязанных, выделите ее в списке и щелкните пиктограмму  .

6. Если в системе настроены профили для работы со smart-картами Mifare 210, добавьте нужные в области ***Профили Mifare*** (см. рис. 13).

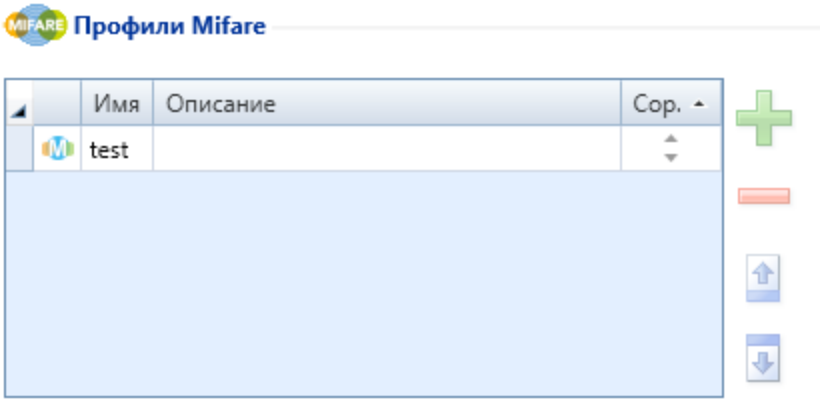


Рисунок 13 - АРМ RusGuard. Модуль Конфигурация оборудования. Настройка контроллера (профили Mifare)

a. Нажмите на кнопку  в области ***Профили Mifare***. Откроется список доступных профилей (по стандартной лицензии не больше одного). К одному контроллеру можно привязать до пяти профилей Mifare.

b. Выберите нужный профиль (или несколько профилей) для привязки к устройству и подтвердите выбор. Название профиля отобразится в области ***Профили Mifare***.

Если используются профили Mifare, то необходимо выполнить настройку интерфейса Rbus[119] на соответствующей вкладке.

8. Выберите устройства (операции), которыми управляет контроллер. Набор операций зависит от типа точки доступа (допустим, замок и сирена для двери, или светофор, возврат/принятие карты, открытие/закрытие шлагбаума). Для этого предназначены восемь реле, которые отображаются в области ***Назначение выходов*** (см. рис. 14).

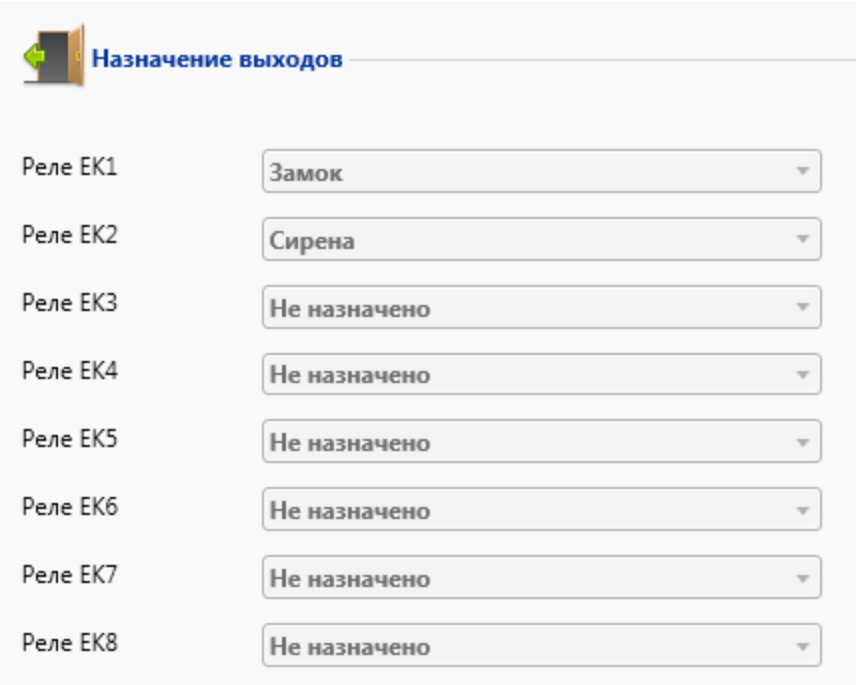


Рисунок 14 - АРМ RusGuard. Модуль Конфигурация оборудования. Реле контроллера (тип точки доступа "Дверь")

8. Чтобы сохранить результат, нажмите на кнопку  .

Для отмены действий нажмите на кнопку  .

Данные в областях ***Информация о контроллере*** и ***Информация о конвертере*** не могут быть отредактированы на этой вкладке. Это справочная информация.

Настройка точки доступа

Настройка параметров точки доступа осуществляется на второй вкладке главного экрана, когда выбран контроллер. Название вкладки зависит от типа точки доступа (см. рис. 15).

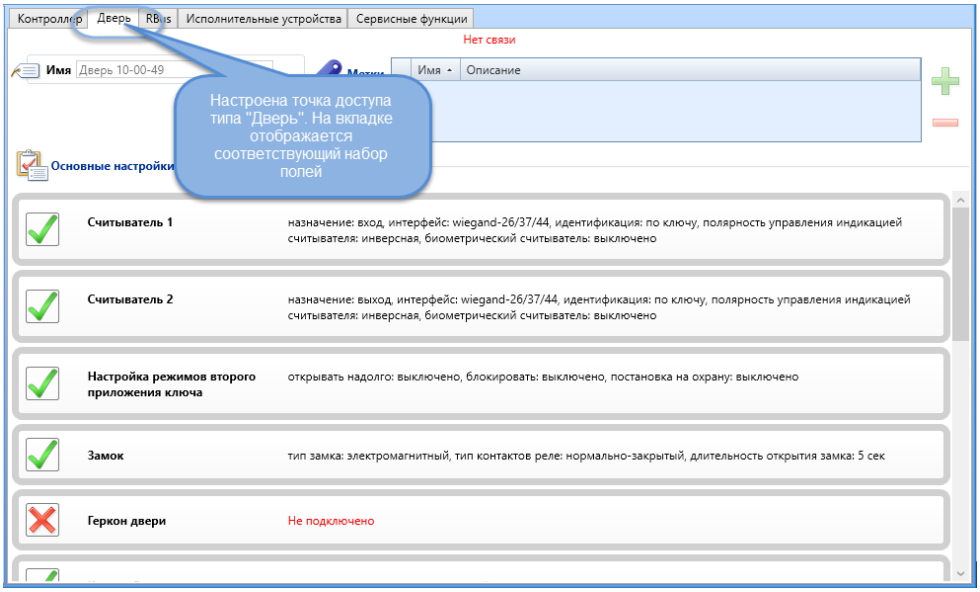


Рисунок 15 - APM RusGuard. Модуль Конфигурация оборудования. Настройка режима работы точки доступа.

Дверь

Параметры точки доступа типа "дверь" (см. табл. 4) настраиваются на соответствующей вкладке. Параметры могут использоваться в различных сочетаниях. Окончательный набор параметров также зависит от настроек реле контроллера.

Основная особенность этого типа точки доступа: два считывателя, один из которых отвечает за вход, а другой - за выход.

 возле названия параметра означает, что параметр используется.

 означает, что параметр не используется.

Таблица 4 - Параметры точки доступа типа "Дверь"

Поле	Описание
Дверь	Поле ввода. По умолчанию именем точки доступа (в данном случае, двери) является серийный номер контроллера. Пользователь может ввести любое значение (максимум 32 символа). Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
Считыватель 1	Флаг для настройки 1-го считывающего устройства. При щелчке мышью по строке раскрывается еще несколько полей для настройки параметров Считывателя 1:

<table>
<tr><th colspan="3">Таблица 4 - Параметры точки доступа типа "Дверь"</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><td>Назначение</td><td>Список. Доступны варианты "вход" и "выход".</td></tr>
<tr><td>Интерфейс</td><td>Список. Поддерживаются интерфейсы связи карта-считыватель Wiegand-26 и TouchMemory. По умолчанию выбран первый вариант</td></tr>
<tr><td>Идентификация</td><td>Установлено значение "по ключу", редактирование невозможно</td></tr>
<tr><td>Полярность управления индикацией считывателя</td><td>Прямая или инверсная. По умолчанию установлено значение "инверсная"(зависит от типа считывателя)</td></tr>
<tr><td rowspan="4">Биометрический считыватель</td><td>IP адрес</td></tr>
<tr><td>Порт</td></tr>
<tr><td>Пароль</td></tr>
<tr><td>Тип идентификации (список)</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Считыватель 2</td><td colspan="2">Флаг для настройки 2-го считывающего устройства. При щелчке мышью по строке раскрывается еще несколько полей (см. выше). Используется для настройки параметров второго считывателя, который, обычно работает на "выход".

Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Настройка режимов второго приложения ключа</td><td colspan="2">Флаг для настройки действий при повторном приложении карточки-ключа. При щелчке мышью по строке раскрываются список функций, которые могут быть использованы как вместе, так и по отдельности:
Открывать надолго
Блокирование/Разблокирование
Постановка/снятие с охраны</td></tr>
</table>

<table>
<tr><th colspan="2">Таблица 4 - Параметры точки доступа типа "Дверь"</th></tr>
<tr><td></td><td>Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Замок</td><td>Флаг для настройки режима работы замка. При щелчке мышью по строке раскрывается список параметров:
Тип замка (список)
Тип контактов реле. Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. замок закрыт.
Длительность открытия замка (ввод, шаг шкалы - 1 сек.)
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Геркон двери</td><td>Флаг для настройки режима работы устройства "геркон" (герметичный контакт) на двери. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td colspan="3">Подключено</td><td>Флаг. Если флаг установлен, режим работы для дверей типа "геркон" активен</td></tr>
<tr><td colspan="3">Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. дверь закрыта.</td></tr>
<tr><td colspan="3">Контроль прохода</td><td>Флаг. Если флаг установлен, геркон выполняет контроль прохода</td></tr>
<tr><td colspan="3">Время ожидания закрытия</td><td>Поле ввода времени (шаг - 1 сек)</td></tr>
<tr><td>Запрет повторного прохода</td><td>Если флаг установлен, повторный проход по одной и той же карточке невозможен (режим АПБ). Это позволяет избежать передачи</td><td>Режим</td><td>Выбор режима из списка (Глобальный или локальный)</td></tr>
</table></td></tr>
</table>

Таблица 4 - Параметры точки доступа типа "Дверь"

	карточки третьим лицам. Для повторного входа необходимо осуществить выход. Эта операция регистрируется через настройку "зон", которые различаются цифровыми идентификаторами	***Зона со стороны выхода***	Назначение зоны выхода (число) Обратите внимание, что ПО RusGuard поддерживает настройку вложенных зон. Если настроены вложенные зоны, то для них зоной со стороны входа является зона со стороны входа более высокого (внешнего) уровня. Используется только при выборе ***Глобального*** режима
		Зона со стороны входа	Назначение зоны со стороны входа (число) Обратите внимание, что ПО RusGuard поддерживает настройку вложенных зон. Если настроены вложенные зоны, то для них зоной со стороны входа является зона со стороны входа более высокого (внешнего) уровня. Используется только при выборе ***Глобального*** режима

Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.

Кнопка "выход"

Флаг для настройки режима работы выхода. При щелчке мышью по строке раскрывается список параметров:

Подключено	Флаг. Если флаг установлен, кнопка используется.
Тип контактов	Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. кнопка не нажата.
Открывать надолго по кнопке "выход"	Флаг. Если флаг установлен, используется возможность надолго открыть дверь на выход

<table>
<tr><th colspan="3">Таблица 4 - Параметры точки доступа типа "Дверь"</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><td>Длительность нажатия</td><td>Поле ввода, в котором указывается продолжительность нажатия кнопки, чтобы надолго открыть дверь. Шаг - 1 сек.</td></tr>
<tr><td colspan="2">Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
</table></td></tr>
<tr><td>Программируемый вход</td><td colspan="2"></td></tr>
<tr><td>Кнопка "звонок"</td><td colspan="2">Флаг для настройки режима работы кнопки "звонок". При щелчке мышью по строке раскрывается список параметров:<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, кнопка используется.</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. кнопка не нажата.</td></tr>
<tr><td colspan="2">Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
</table></td></tr>
<tr><td>Кнопка аварийного открытия двери</td><td colspan="2">Флаг для настройки режима работы кнопки аварийного открытия. При щелчке мышью по строке раскрывается список параметров:<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, кнопка используется.</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. кнопка не нажата.</td></tr>
<tr><td colspan="2">Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th colspan="4">Таблица 4 - Параметры точки доступа типа "Дверь"</th></tr>
<tr><td>Сирена</td><td colspan="3">Флаг для настройки сирены. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td colspan="2">Подключено</td><td>Флаг. Если флаг установлен, кнопка используется.</td></tr>
<tr><td colspan="2">Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. сирена отключена.</td></tr>
<tr><td rowspan="3">Тактика срабатывания (список)</td><td>Включить</td><td>Сирена работает непрерывно</td></tr>
<tr><td rowspan="2">Включить на время</td><td>Время включения - Поле ввода, Указывается продолжительность фазы работы сирены</td></tr>
<tr><td>Пауза между включениями - Поле ввода. Вводится продолжительность паузы</td></tr>
<tr><td>Неограниченный цикл</td><td>Полное время срабатывания</td><td>Поле ввода общей продолжительности работы сирены</td></tr>
<tr><td colspan="2">Включать сирену при взломе двери</td><td>Флаг. Если флаг установлен, сирена срабатывает при взломе двери</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Проход по разрешению оператора</td><td colspan="3">Флаг. Если флаг установлен проход выполняется с разрешения оператора системы.

В модуле Конфигурация рабочих мест 155 также необходимо настроить отображение кнопок для принятия решения оператором в модуле Фотоидентфикация 248.

При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td>Информирование оператора о входе</td><td>Флаг. Если флаг установлен, оператор уведомляется о входе</td></tr>
<tr><td>Информирование оператора о выходе</td><td>Флаг. Если флаг установлен, оператор информируется о выходе</td></tr>
</table></td></tr>
</table>

<table>
<tr><th colspan="3">Таблица 4 - Параметры точки доступа типа "Дверь"</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><td>Время принятия решений</td><td>Поле ввода. Время вводится в секундах</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Охранный вход 1</td><td colspan="2">Флаг для настройки режима работы охранного входа 1. При щелчке мышью по строке раскрывается список параметров:<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. дверь закрыта.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Охранный вход 2</td><td colspan="2">Флаг для настройки режима работы охранного входа 2. При щелчке мышью по строке раскрывается список параметров:<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. дверь закрыта.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Задержка постановки на охрану</td><td colspan="2">Флаг для настройки задержки постановки двери на охрану. При щелчке мышью по строке раскрывается список параметров:<table>
<tr><td>Время задержки</td><td>Поле ввода продолжительности задержки (в секундах)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th colspan="3">Таблица 4 - Параметры точки доступа типа "Дверь"</th></tr>
<tr><td></td><td colspan="2">Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Задержка срабатывания тревоги</td><td colspan="2">Флаг для настройки задержки срабатывания тревоги при постановке двери на охрану. При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>Время задержки</td><td>Поле ввода продолжительности задержки (в секундах)</td></tr></table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Аварийное открытие</td><td colspan="2">Флаг для настройки функции аварийного открытия двери. При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>По системной команде</td><td>Если флаг установлен, возможно аварийное открытие двери по системной команде (например, при срабатывании противопожарной системы).</td></tr></table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Контроль платы питания</td><td colspan="2"></td></tr>
</table>

Две двери

Параметры точки доступа типа "Две двери" настраиваются на двух вкладках ***Дверь 1*** и ***Дверь 2***. При этом для каждой двери может быть настроен только один считыватель. В остальном настройка выполняется также, как для точки доступа типа "Дверь".

Параметры могут использоваться в различных сочетаниях. Окончательный набор параметров также зависит от настроек реле контроллера.

 возле названия параметра означает, что параметр используется.

 означает, что параметр не используется.

Турникет

Параметры точки доступа типа "турникет" (см. табл. 5) настраиваются на соответствующей вкладке. Параметры могут использоваться в различных сочетаниях. Окончательный набор параметров также зависит от настроек реле контроллера.

 возле названия параметра означает, что параметр используется.

 означает, что параметр не используется.

Таблица 5 - Параметры точки доступа типа "Турникет"

Поле	Описание
Турникет	Поле ввода. По умолчанию именем точки доступа (в данном случае, турникета) является серийный номер контроллера. Пользователь может ввести любое значение (максимум 32 символа). Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
Считыватель 1	Флаг для настройки 1-го считывающего устройства. При щелчке мышью по строке раскрывается еще несколько полей для настройки параметров Считывателя 1:

Назначение	Список. Доступны варианты "вход" и "выход".
Интерфейс	Список. Поддерживаются интерфейсы связи карта-считыватель Wiegand-26 и TouchMemory. По умолчанию выбран первый вариант
Идентификация	Установлено значение "по ключу", редактирование невозможно
Полярность управления индикацией считывателя	Прямая или инверсная. По умолчанию установлено значение "инверсная"(зависит от типа считывателя)
Биометрический считыватель	IP адрес
	Порт
	Пароль
	Тип идентификации (список)

<table>
<tr><td></td><td>Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Считыватель 2</td><td>Флаг для настройки 2-го считывающего устройства. При щелчке мышью по строке раскрывается еще несколько полей (см. выше). Используется для настройки параметров второго считывателя, который, обычно работает на "выход".

Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Картоприемник</td><td>Флаг для настройки устройства для учета возврата карт.
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Интерфейс считывателя</td><td>Список. Поддерживаются интерфейсы связи карта-считыватель Wiegand-26 и TouchMemory. По умолчанию выбран первый вариант</td></tr>
<tr><td>Контроль тампера</td><td>Флаг. Если флаг установлен, осуществляется контроль взлома тампера</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. тампер закрыт</td></tr>
<tr><td>Контроль заполнения картоприемника</td><td>Флаг. Если флаг установлен, осуществляется контроль заполнения устройства</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. устройство не заполнено до конца</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Реле "Принять карту"</td><td>Если флаг установлен, используется функция приема карты.
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Реле "Вернуть карту"</td><td>
Флаг. Если флаг установлен, используется функция возврата карты.
<table>
<tr><td>Подключено</td><td>Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Управление на вход</td><td>
<table>
<tr><td>Подключено</td><td>Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Управление на выход</td><td>
<table>
<tr><td>Подключено</td><td>Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Геркон прохода</td><td>
Флаг для настройки режима работы устройства "геркон" (герметичный контакт) на турникете. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td colspan="3">Подключено</td><td>Флаг. Если флаг установлен, режим работы "геркон" активен</td></tr>
<tr><td colspan="3">Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. турникет закрыт.</td></tr>
<tr><td colspan="3">Контроль прохода</td><td>Флаг. Если флаг установлен, контролируется проход</td></tr>
<tr><td colspan="3">Время ожидания закрытия</td><td>Поле ввода времени (шаг - 1 сек)</td></tr>
<tr><td>Запрет повторного прохода</td><td>Если флаг установлен, повторный проход по одной и той же карточке невозможен (режим АПБ, чаще всего настраивается именно для турникетов). Это позволяет избежать передачи карточки третьим лицам. Для повторного входа</td><td>Режим</td><td>Выбор режима из списка</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>необходимо осуществить выход. Операция регистрируется через настройку "зон", которые различаются цифровыми идентификаторами</td><td>Зона со стороны выхода</td><td>Назначение зоны выхода (число). Обратите внимание, что ПО RusGuard поддерживает настройку вложенных зон. Если настроены вложенные зоны, то для них зоной со стороны входа является зона со стороны входа более высокого (внешнего) уровня.
Используется только при выборе Глобального режима</td></tr>
<tr><td></td><td></td><td>Зона со стороны входа</td><td>Назначение зоны со стороны входа (число)
Обратите внимание, что ПО RusGuard поддерживает настройку вложенных зон. Если настроены вложенные зоны, то для них зоной со стороны входа является зона со стороны входа более высокого (внешнего) уровня.
Используется только при выборе Глобального режима</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Кнопка аварийного открытия двери</td><td>
Флаг для настройки режима работы кнопки аварийного открытия. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, кнопка используется.</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. кнопка не нажата.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Проход по разрешению оператора</td><td>Флаг. Если флаг установлен проход выполняется с разрешения оператора системы.

В модуле Конфигурация рабочих мест 155 также необходимо настроить отображение кнопок для принятия решения оператором в модуле Фотоидентфикация 248.</td></tr>
</table>

<table>
<tr><td></td><td>
При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td>Информирование оператора о входе</td><td>Флаг. Если флаг установлен, оператор уведомляется о входе</td></tr>
<tr><td>Информирование оператора о выходе</td><td>Флаг. Если флаг установлен, оператор информируется о выходе</td></tr>
<tr><td>Время принятия решений</td><td>Поле ввода. Время вводится в секунд</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Задержка постановки на охрану</td><td>
Флаг для настройки задержки постановки точки доступа на охрану. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td>Время задержки</td><td>Поле ввода продолжительности задержки (в секундах)</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Задержка срабатывания тревоги</td><td>
Флаг для настройки задержки срабатывания тревоги при постановке точки доступа на охрану. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td>Время задержки</td><td>Поле ввода продолжительности задержки (в секундах)</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Аварийное открытие</td><td>
Флаг для настройки функции аварийного открытия турникета. При щелчке мышью по строке раскрывается список параметров:
<table>
<tr><td>По системной команде</td><td>Если флаг установлен, возможно аварийное открытие турникета по системной команде (например, при срабатывании противопожарной системы).</td></tr>
</table>
</td></tr>
</table>

	Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
Контроль платы питания	

Шлагбаум/Ворота

Параметры точки доступа типа "шлагбаум/ворота" (см. табл. 6) настраиваются на соответствующей вкладке. Параметры могут использоваться в различных сочетаниях. Окончательный набор параметров также зависит от настроек реле контроллера.

 возле названия параметра означает, что параметр используется.

 означает, что параметр не используется.

Таблица 6 - Параметры точки доступа типа "Шлагбаум/Ворота"

Поле	Описание
Шлагбаум/Ворота	Поле ввода. По умолчанию именем точки доступа (в данном случае, турникета) является серийный номер контроллера. Пользователь может ввести любое значение (максимум 32 символа). Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
Считыватель 1	Флаг для настройки 1-го считывающего устройства. При щелчке мышью по строке раскрывается еще несколько полей для настройки параметров Считывателя 1:

Назначение	Список. Доступны варианты "вход" и "выход".
Интерфейс	Список. Поддерживаются интерфейсы связи карта-считыватель Wiegand-26 и TouchMemory. По умолчанию выбран первый вариант
Идентификация	Установлено значение "по ключу", редактирование невозможно

<table>
<tr><td></td><td>
<table>
<tr><td>Полярность управления индикацией считывателя</td><td>Прямая или инверсная. По умолчанию установлено значение "инверсная"(зависит от типа считывателя)</td></tr>
<tr><td rowspan="4">Биометрический считыватель</td><td>IP Адрес</td></tr>
<tr><td>Порт</td></tr>
<tr><td>Пароль</td></tr>
<tr><td>Тип идентификации (список)</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Считыватель 2</td><td>Флаг для настройки 2-го считывающего устройства. При щелчке мышью по строке раскрывается еще несколько полей (см. выше). Используется для настройки параметров второго считывателя, который, обычно работает на "выход".

Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Картоприемник</td><td>Флаг для настройки устройства для учета возврата карт.
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Интерфейс считывателя</td><td>Список. Поддерживаются интерфейсы связи карта-считыватель Wiegand-26 и TouchMemory. По умолчанию выбран первый вариант</td></tr>
<tr><td>Контроль тампера</td><td>Флаг. Если флаг установлен, осуществляется контроль взлома тампера</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. тампер закрыт</td></tr>
<tr><td>Контроль заполнения картоприемника</td><td>Флаг. Если флаг установлен, осуществляется контроль заполнения</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>устройства</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. устройство не заполнено до конца</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Реле "Принять карту"</td><td>Флаг. Если флаг установлен, используется функция приема карты.
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Реле "Вернуть карту"</td><td>Флаг. Если флаг установлен, используется функция возврата карты.
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Управление на вход</td><td>Флаг. Установите для настройки управления на вход.</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Управление на выход</td><td>
Флаг. Установите, для использования функции.
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, функция используется.</td></tr>
<tr><td>Тип контактов реле</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый</td></tr>
<tr><td>Длительность импульса (сек)</td><td>Поле ввода. Указывает продолжительность импульса в секундах.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Датчик проезда</td><td>
<table>
<tr><td>Подключено</td><td>Флаг. Если флаг установлен, датчик активен</td></tr>
<tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-закрытый, т.е. проезд закрыт.</td></tr>
<tr><td>Контроль прохода</td><td>Флаг. Если флаг установлен, контролируется проход</td></tr>
<tr><td>Время ожидания закрытия</td><td>Поле ввода времени (шаг - 1 сек)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td rowspan="3">Запрет повторного прохода</td><td rowspan="3">Если флаг установлен, повторный проезд по одному пропуску невозможен (режим АПБ). Это позволяет избежать передачи пропусков третьим лицам. Для повторного входа необходимо осуществить выход. Операция регистрируется через настройку "зон", которые различаются цифровыми идентификаторами</td><td>Режим</td><td>Выбор режима из списка</td></tr>
<tr><td>Зона со стороны выхода</td><td>Назначение зоны выхода (число).

Обратите внимание, что ПО RusGuard поддерживает настройку вложенных зон. Если настроены вложенные зоны, то для них зоной со стороны входа является зона со стороны входа более высокого (внешнего) уровня.</td></tr>
<tr><td>Зона со стороны входа</td><td>Назначение зоны со стороны входа (число).

Обратите внимание, что ПО RusGuard поддерживает настройку вложенных зон. Если настроены вложенные зоны, то для них зоной со стороны входа является зона со стороны входа более высокого (внешнего) уровня.</td></tr>
</table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.
</td></tr>
<tr><td>Время проезда</td><td>Установка времени, за которое необходимо проехать через шлагбаум (сек).

Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Контроль сигнала "Открыто"</td><td>Контроль состояния шлагбаума.

Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
</table>

<table>
<tr><td>Кнопка аварийного открытия двери</td><td>Флаг для настройки режима работы кнопки аварийного открытия. При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>Подключено</td><td>Флаг. Если флаг установлен, кнопка используется.</td></tr><tr><td>Тип контактов</td><td>Список: нормально-открытый или нормально закрытый. По умолчанию установлен нормально-открытый, т.е. кнопка не нажата.</td></tr></table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Проход по разрешению оператора</td><td>Флаг. Если флаг установлен проход выполняется с разрешения оператора системы.

В модуле Конфигурация рабочих мест 155 также необходимо настроить отображение кнопок для принятия решения оператором в модуле Фотоидентфикация 248.

При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>Информирование оператора о входе</td><td>Флаг. Если флаг установлен, оператор уведомляется о входе</td></tr><tr><td>Информирование оператора о выходе</td><td>Флаг. Если флаг установлен, оператор информируется о выходе</td></tr><tr><td>Время принятия решений</td><td>Поле ввода. Время вводится в секундах</td></tr></table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Задержка постановки на охрану</td><td>Флаг для настройки задержки постановки точки доступа на охрану. При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>Время задержки</td><td>Поле ввода продолжительности задержки (в секундах)</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Задержка срабатывания тревоги</td><td>Флаг для настройки задержки срабатывания тревоги при постановке точки доступа на охрану. При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>Время задержки</td><td>Поле ввода продолжительности задержки (в секундах)</td></tr></table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
<tr><td>Аварийное открытие</td><td>Флаг для настройки функции аварийного открытия шлагбаума/ворот. При щелчке мышью по строке раскрывается список параметров:
<table><tr><td>По системной команде</td><td>Если флаг установлен, возможно аварийное открытие ворот/шлагбаума по системной команде (например, при срабатывании противопожарной системы).</td></tr></table>
Чтобы отредактировать значение, нажмите на кнопку  в панели инструментов.</td></tr>
</table>

Шкафы/Витрины

Общие настройки точки доступа типа "Шкафы/Витрины" сходны с настройками точки доступа типа "Дверь", особенности описаны в соответствующем разделе 115.

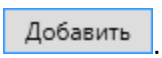
Привязка меток к точкам доступа

К любому типу точки доступа может быть привязана метка (о создании меток см. здесь 206).

Для того чтобы привязать метку к точке доступа:

1. Зайдите в панель настроек нужной точки доступа.
2. Нажмите на кнопку  в панели инструментов.
3. В области ***Метки*** нажмите на пиктограмму  .

Загрузится общий список меток системы (кроме тех, которые были ранее привязаны к данной точке доступа.)

4. Выберите нужную метку и нажмите на кнопку 

.

Добавленная метка отобразится в списке привязанных (см. рис. 16).

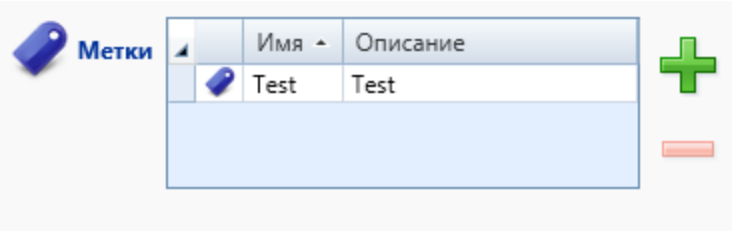


Рисунок 16 - АРМ RusGuard. Модуль Конфигурация оборудования. Привязка меток к точке доступа

5. Сохраните изменения ( ).

Чтобы удалить метку из списка привязанных, выделите ее в списке и щелкните пиктограмму .

Настройка параметров биометрического считывателя

Если в СКУД используются биометрические считыватели, их параметры настраиваются в областях ***Считыватель 1*** и ***Считыватель 2*** при настройке точки доступа (см. описание полей в таблицах выше). Для настройки необходимо указать IP-адрес терминала, порт, пароль, а также выбрать один из доступных типов идентификации (см. рис. 17).

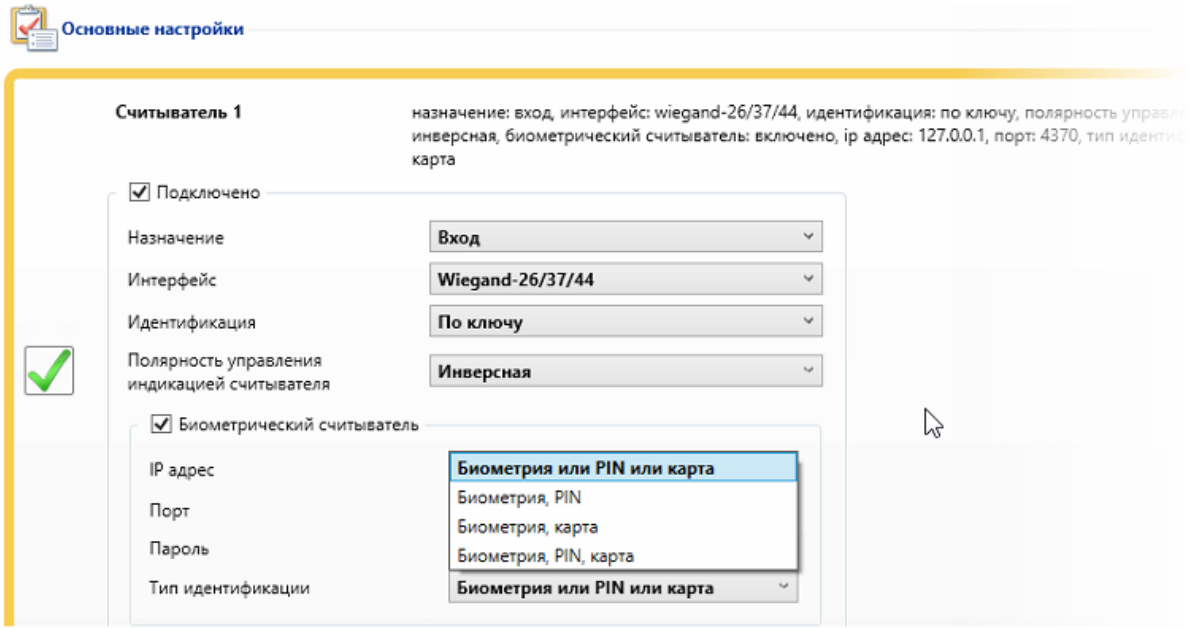


Рисунок 17 - АРМ RusGuard. Модуль Конфигурация оборудования. Настройка параметров биометрического считывателя

Настройка точки доступа типа "Шкафы/витрины"

ПО RusGuard позволяет настраивать доступ к шкафам и витринам.

Общие настройки для этого типа точки доступа совпадают с настройками для дверей, но существует ряд особенностей:

- Помимо вкладки с названием точки доступа, где вводятся базовые настройки контроллера, появляется вкладка ***Дверцы***. Здесь может быть настроено до 8 релейных блоков, к каждому из которых может быть привязано до 10 исполнительных устройств (контролирующих доступ к дверцам, ячейкам и т. д.).

Обратите внимание, что настройки релейных блоков и привязанных к ним исполнительных устройств определяются настройками контроллера и не могут быть отредактированы отдельно.

- При настройке точки доступа данного типа также настраиваются ***Права релейного блока*** в модуле ***Конфигурация СКУД***. Права релейного блока затем привязываются к уровню доступа и позволяют настроить доступ сотрудника не только к определенной зоне внутри помещения в определенное время, но и к определенным шкафам и дверцам (ячейкам и т. д.).

Настройка прав релейного блока

Для того чтобы настроить права релейного доступа:

1. Настройте точку доступа типа "шкафы/дверцы".
2. Перейдите в модуль ***Конфигурация СКУД***.
3. Перейдите к разделу ***Права релейного блока*** в навигационной панели слева. По умолчанию список прав пуст. Вызовите контекстное меню (щелчок правой кнопкой мыши) (см. рис. 18).

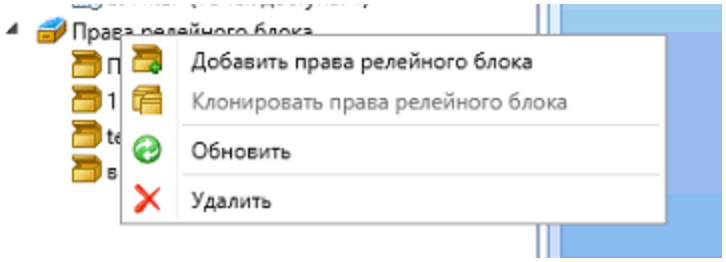


Рисунок 18 - APM RusGuard. Модуль Конфигурация СКУД. Создание прав релейного доступа

4. Выберите пункт Добавить права релейного блока. Обратите внимание, что если ранее были созданы права релейного блока, вы можете клонировать их настройки.

Откроется диалоговое окно.

5. Введите параметры прав в диалоговом окне и сохраните их. Новый пункт появится в навигационной панели слева. Перейдите к нему.
6. Щелкните пиктограмму  в верхней панели инструментов сверху. Откроется диалог создания элемента. Под элементом понимается конкретная дверца или ячейка (либо несколько ячеек и т. д.) (см. рис. 19).

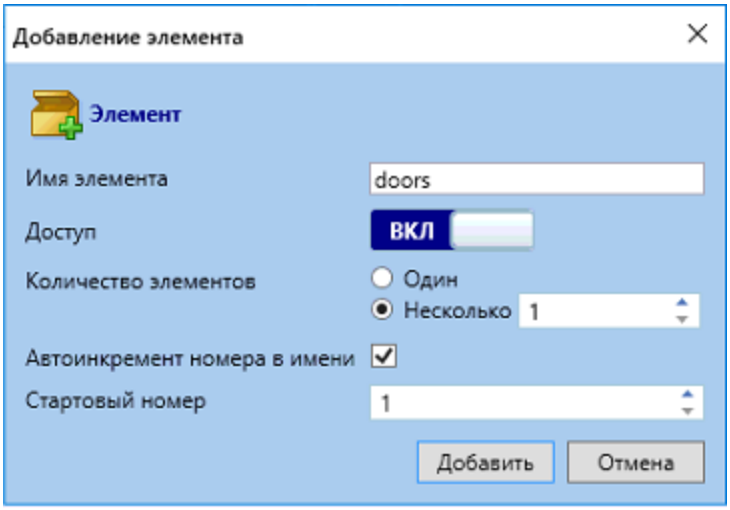


Рисунок 19 - АРМ RusGuard. Модуль Конфигурация СКУД. Создание элемента

7. Введите параметры доступа к элементу:
   - Имя
   - Доступ (включен или выключен)
   - Количество элементов (вы можете настроить права для одного элемента или нескольких). Если вы хотите привязать к блоку прав несколько элементов сразу, вы можете использовать для наименования каждого элемента функцию ***Автоинкремент номера в имени***. При этом название каждого элемента состоит из имени и порядкового номера, начиная с единицы. Если эта функция оключена, все элементы имеют одинаковые называния.

Обратите внимание, что номер прибавляется к групповому названию названию элемента. То есть, если в поле Имя элемента введено "тест" и выбрано количество элементов Один, элемент будет называться "тест". Если в дальнейшем при редактировании этого элементы будет создан элемент "тест 2" в количестве Элементов которого указано Несколько и выбран способ наименования Автоинкремент номера в имени, элементы будут называться "1 тест 2", "2 тест 2", "3 тест 2" и т. д.

8. Нажмите на кнопку ***Добавить***.

Система сохраняет настройки. Элементы отображаются в списке прав (см. рис. 20). Вы можете откредактировать этот список, добавить в него элементы или удалить.

Вы также можете выборочно включать и отключать доступ к отдельным элементам списка, даже если при их создании доступ был отмечен как включенный.

9. Закончив настройку, щелкните пиктограмму  в верхней панели инструментов.

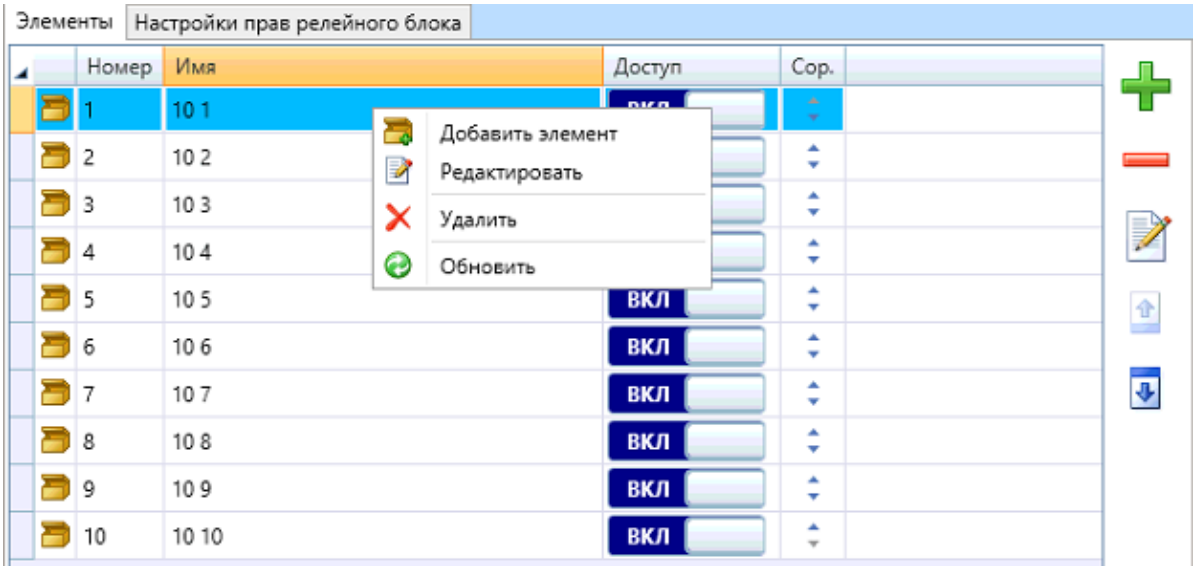


Рисунок 20 - APM RusGuard. Модуль Конфигурация СКУД. Список элементов прав релейного блока

Привязка прав релейного блока к уровню доступа

Права релейного блока применяются только в рамках уровня доступа. Так они привязываются к учетной записи сотрудника (параметрам его пропуска).

Для того чтобы привязать права релейного блока к уровню доступа:

1. Настройте точки доступа типа "шкафы/витрины".
2. Настройте права релейного блока, как описано выше.
3. Создайте уровень доступа, включающий точки доступа типа "шкафы/витрины". Либо отредактируйте существующий, дополнив его точками доступа данного типа.
4. В настройках уровня доступа вызовите список прав релейного блока и выберите нужный пункт в списке настроенных прав (см. рис. 21).
5. Примените настройки.

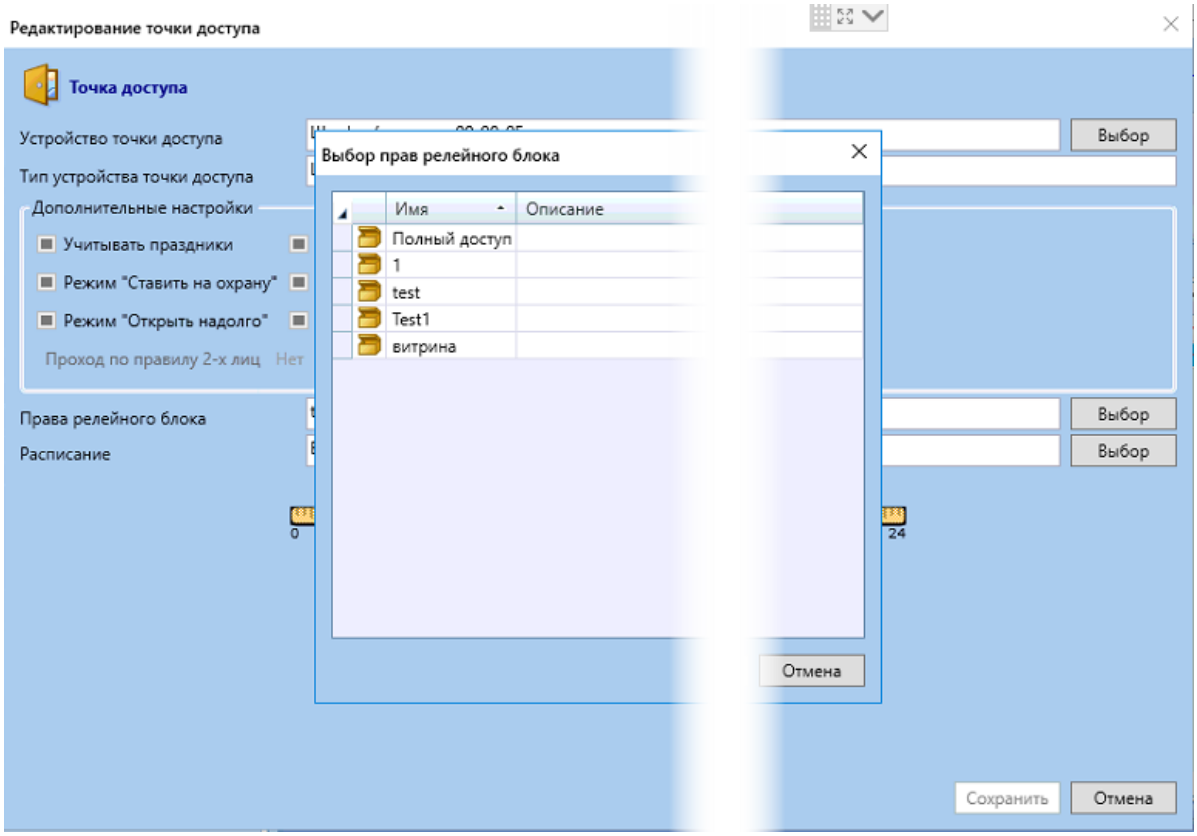


Рисунок 21 - АРМ RusGuard. Модуль Конфигурация СКУД. Привязка прав релейного блока к уровню доступа

Настройка интерфейса Rbus

Настройки на вкладке ***Rbus*** выполняются, если в системе заданы профили для работы со смарт-картами Mifare, и эти карты будут использоваться для прохода в точках доступах, обслуживаемых устройством (см. табл. 7) .

Обратите внимание, что для работы с картами Mifare необходимо подключить специальный считыватель (RDR-202-Multi) и установить новую версию прошивки. Иначе вкладке не отображается в интерфейсе.

Чтобы отредактировать параметры полей, необходимо щелкнуть пиктограмму  в панели управления.

Таблица 6 - Параметры интерфейса Rbus

Поле	Описание
Обще настройки	***Контроль тампера считывателя***: установите флаг, чтобы система реагировала на событие физического повреждения считывателя ***Тип данных с дополнительного выхода Wiegand***: выберите один из вариантов ***Стандартный*** или ***Двоично-десятичный***. Поле обеспечивает работу считывателя с интерфейсом Wiegand, который используется в других видах карт ***Тактика обработки данных***
Аутентификация	Вы может установить режим импорта настроек аутентификации из профиля Mifare, либо использовать настройку контроллера (режим UID)
Блокировка	Если не установлен флаг ***Подключено***, не действуют режимы подменю ***Счетчик проходов*** кроме пункта ***Интервал для внешнего разрешения***. В пункте ***Источник*** определяется считыватель, используемый для записи на карту и проверки временных интервалов и счетчиков В пункте ***Блокировать*** определяется направление блокировки прохода при активации этого режима на карте
Счетчик проходов	Функция разработана для тех случаев, когда необходимо учитывать количество и время проходов лица. Например, если карта используется для оплаты проезда, посещения музея и т.д. • Если не установлен флаг ***Подключено***, действует только опция ***Блокировать ключ после крайнего прохода***. • Поле ***Количество проходов*** определяет количество проходов, которое будет записано на карту при восстановлении счетчика проходов. При нулевом значении этого пункта проходы с карты списываться не будут. • Если установлен флаг ***Блокировать ключ при обнулении счетчика***, карта блокируется до восстановления счетчика проходов.

	• Режим ***Блокировать ключ после крайнего прохода*** задает временную блокировку ключа после каждого прохода на указанное в пункте время. Этот режим не зависит от положения флага ***Подключено***. • Поле ***Восстановление счетчика после первого прохода*** определяет интервал после первого прохода, после которого восстанавливается счетчик проходов на карте . Пункт работает, если время восстановления не равно нулю и если активен режим ***Циклически***. Если восстановление счетчика происходит в пределах времени нахождения в зоне, то время начала интервала нахождения в зоне не меняется, а начало интервала восстановления после первого прохода обновляется. • Поле ***Восстановление счетчика после крайнего прохода*** определяет интервал, в течение которого карта не должна проходить через точку доступа для того, чтобы был восстановлены счетчики проходов и циклов на карте. Восстанавливается и начало интервала нахождения в зоне. Пункт работает, если время восстановления не равно нулю и если активен режим ***Циклически***. • Поле ***Счетчик циклов*** определяет сколько раз возможно автоматическое восстановление счетчика проходов на карте. При каждом восстановлении счетчика проходов счетчик циклов уменьшается. Нулевое значение этого параметра не ограничивает количество восстановлений счетчика. • Флаги ***Сообщение о первом проходе*** и ***Сообщение о крайнем проходе*** вызывают при записи на карту служебное уведомление с кодом 0xFE, в котором передаются время первого или время крайнего проходов, а также содержимое счетчиков прохода и циклов записываемые на карту. • Поле ***Интервал для внешнего разрешения*** определяет время, в течение которого после первого прохода ключ не будет проверяться на внешнее разрешение. Считыватель, на котором будет формироваться этот интервал, определяется параметрами сигнала внешнего разрешения и не зависит от параметров подменю ***Блокировка***. Этот пункт не зависит от положения флага ***Подключено***. • Поле ***Интервал нахождения в зоне*** определяет время после первого прохода, в течение которого проход не будет заблокирован. Нулевое значение интервала не ограничивает это время. • Поле ***Интервал блокировки при нарушении*** задает время после исчерпания интервала нахождения в зоне, в течение которого карта будет заблокирована. По истечении времени всех блокировок первый же проход начнет новый интервал нахождения в зоне. При нулевом значении параметра блокировка карты не снимается.

	Действие указанных функции и параметров возможно только при аутентификации карты по профилю Mifare 210 и при отключенном режиме ***По решению оператора***. При данных настройках отключается функция ***ключ + PIN код***.
Разрешенные типы карт	Считыватель позволяет использовать все типы карт, но по умолчанию все варианты отключены. Поэтому, даже если все остальные настройки выполнены корректно, система не заработает до тех пор, пока в этом поле не будут активированы нужные типы карт

Сервисные функции (управление контролером и точкой доступа)

Вкладка ***Сервисные функции*** содержит две "под-вкладки": ***Контроллер*** и вкладка с названием, которое определяется типом точки доступа. В примере на иллюстрации ниже (см. рис. 22) это "Дверь".

На "под-вкладке" ***Контроллер*** отображается текущее состояние устройства, список доступных команд для управления им, а также лог событий.

Возможности управления точкой доступа через набор "*команд*" предусмотрены в нескольких модулях АРМ. В модуле ***Планы*** 239 для этого используются драйверы устройств и точек доступа. В модуле ***Фотоидентификация*** 248 - функция разрешения/запрета на проход. При штатном режиме использования АРМ рекомендуется использовать функции управления в модуле ***Планы***.

В модуле ***Конфигурация оборудования*** доступ к командам выполняется через под-вкладку точки доступа на вкладке ***Сервисные функции***. На "под-вкладке" отображается текущее состояние точки доступа, список доступных команд для управления ею, а также лог событий

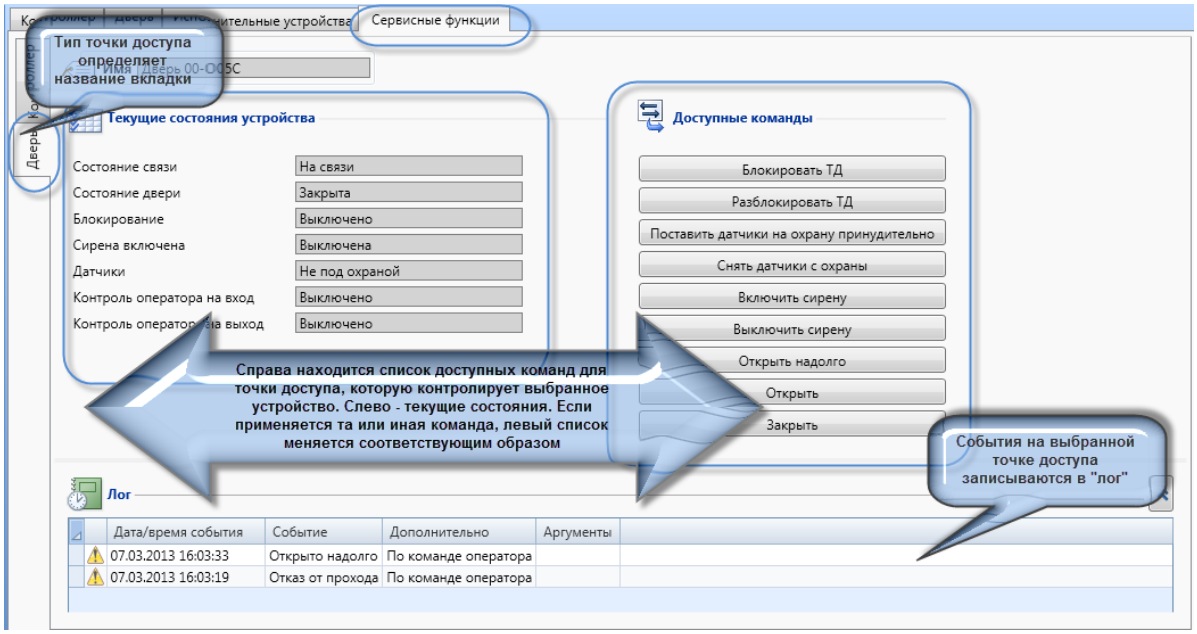


Рисунок 22 - АРМ RusGuard. Модуль Конфигурация оборудования. Управление точкой доступа

Режимы индикации считывающего устройства

На схемах ниже (см. рис. 23, 24 и 25) показана индикация считывающего устройства в зависимости от режима работы, настроенного для точки доступа. На схемах показан тип и продолжительность светового сигнала, а также тип и длительность звукового сигнала, если он предусмотрен.

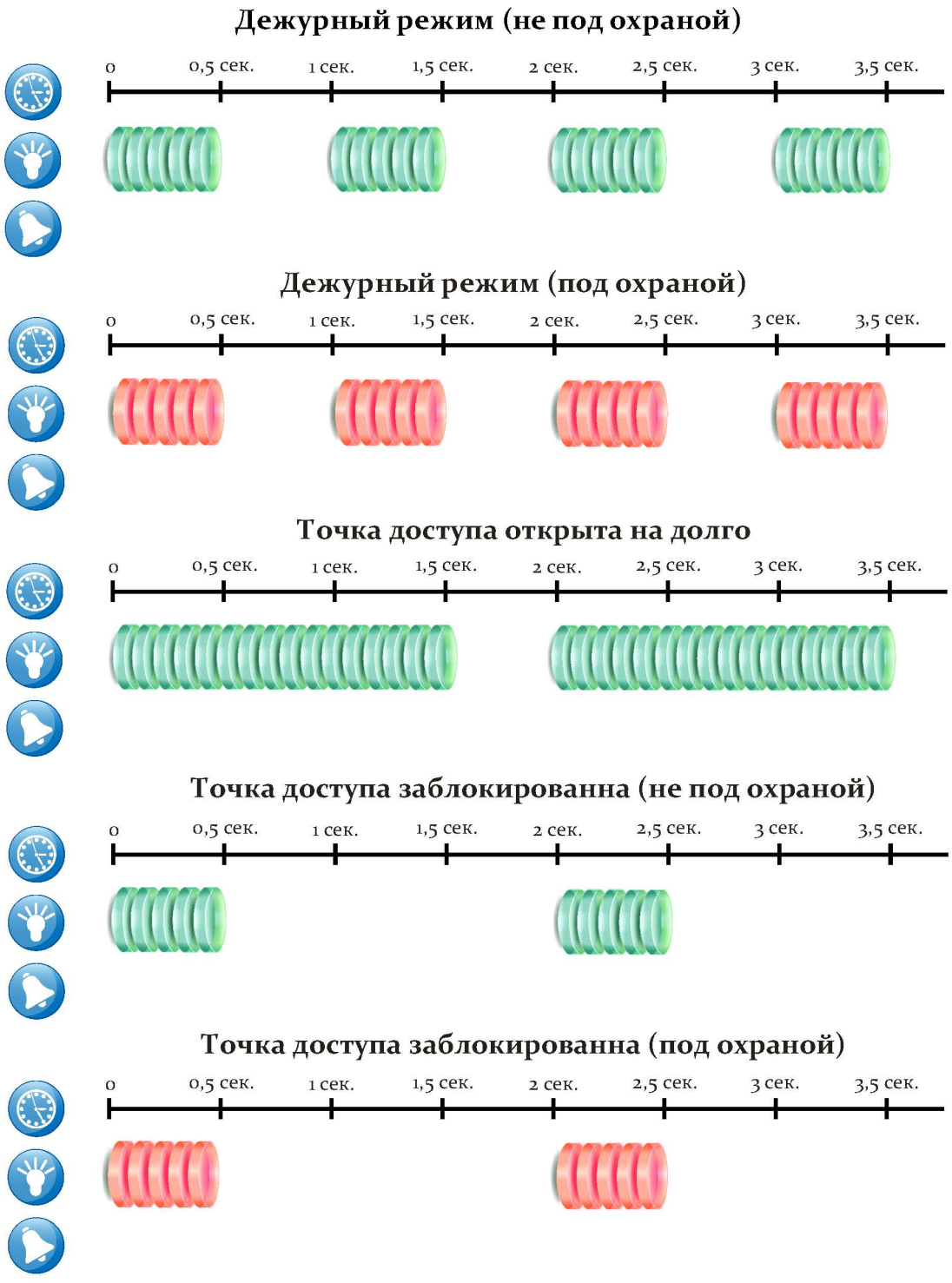


Рисунок 23 - Индикаторы считывающего устройства. Схема 1.

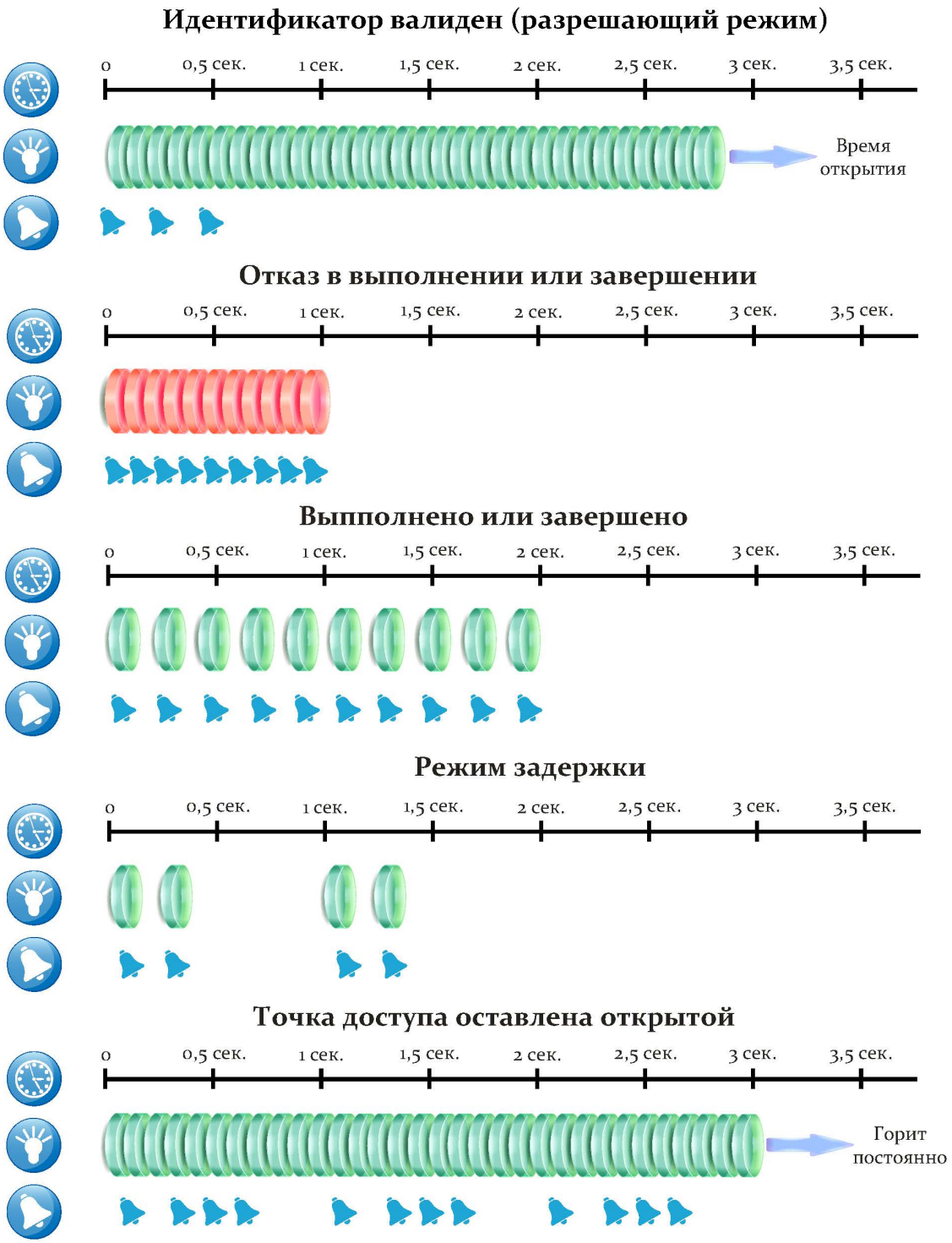


Рисунок 24 - Индикаторы считывающего устройства. Схема 2.

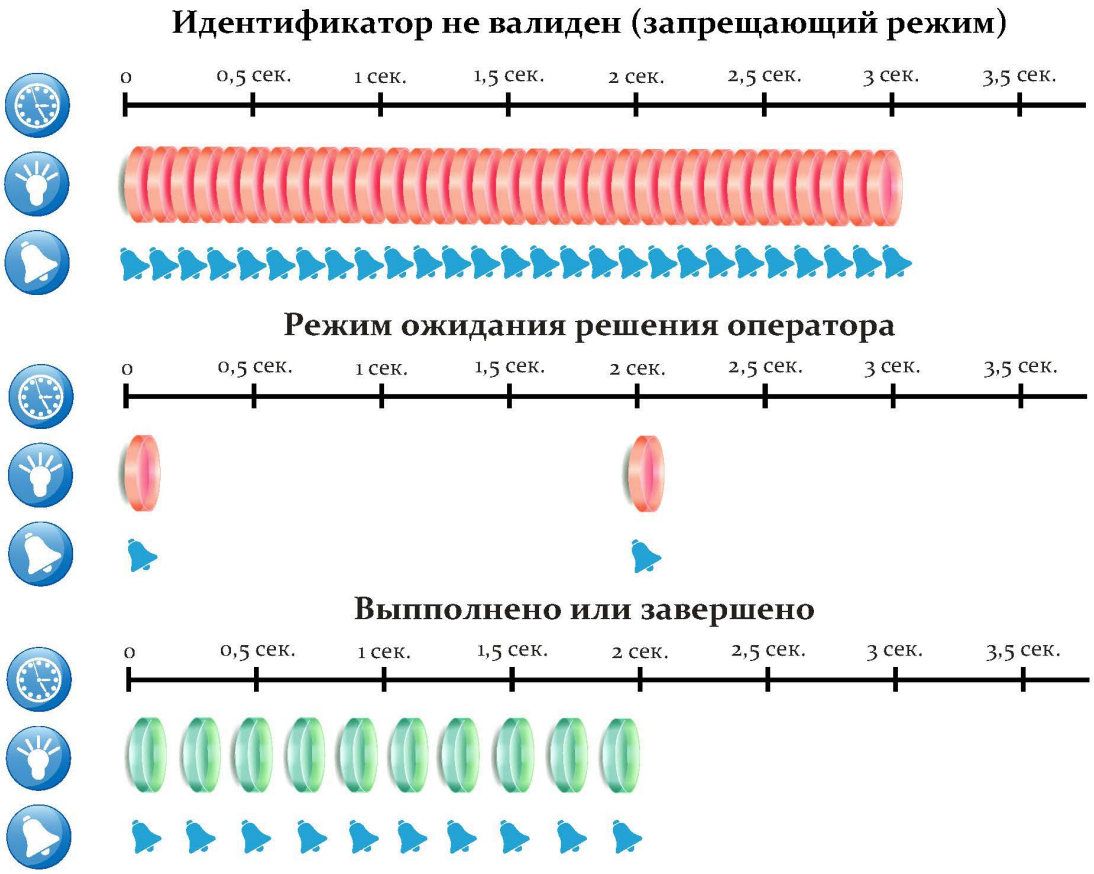


Рисунок 25 - Индикаторы считывающего устройства. Схема 3.

Ведение базы адресов электронной почты

Для рассылки уведомлений пользователям систем, обслуживаемых ПО RusGuard (в частности, связанных с настроенными *Реакциями* 193), необходима настройка адресов электронной почты. Настройка осуществляется в модуле ***Конфигурация оборудования***.

Для того чтобы ввести адрес электронной почты для рассылки:

1. Зайдите в модуль ***Конфигурация оборудования*** 79 АРМ.
2. В левой навигационной панели выберите пункт ***Адреса email рассылки***. Установите на нем курсор.
3. В панели управления нажмите на кнопку  ***Добавить email рассылку***.

Откроется окно для ввода данных о получателе и настройке рассылки (см. рис. 26).

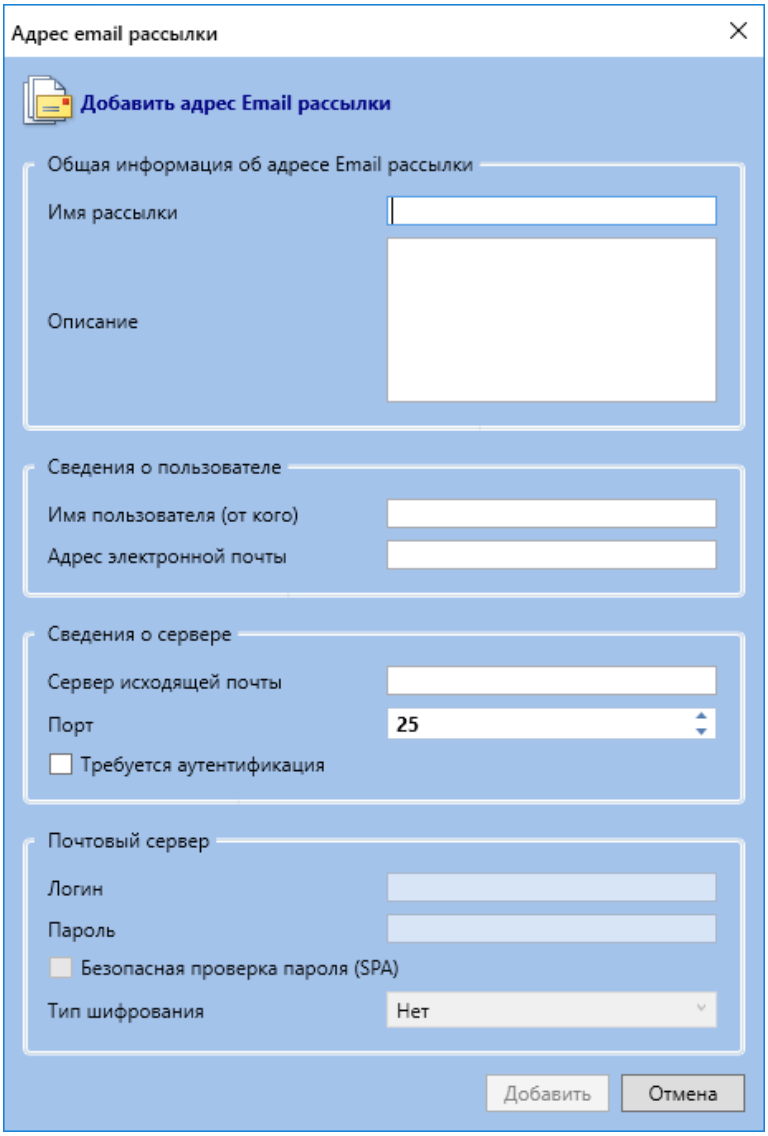


Рисунок 26 - Ввод данных о рассылке

4. Заполните поля формы. Нажмите на кнопку Добавить.

Кнопка активируется после заполнения всех обязательных полей. Обязательные поля: ***Понятное имя***, ***Адрес электронной почты***, ***Север исходящей почты***, ***Порт***, ***Пользователь*** и ***Пароль***.

Система выполнит сохранение данных. Имя адресата (поле ***Понятное имя***) отобразится в иерархическом списке навигационной панели слева.

Для редактирования и/или использования адреса (разовая отправка) перейдите в нужную строку.

Для того чтобы выполнить разовую отправку сообщения:

1. Найдите нужный адрес электронной почты в списке ***Адреса email рассылки*** навигационной панели (см. рис. 27).

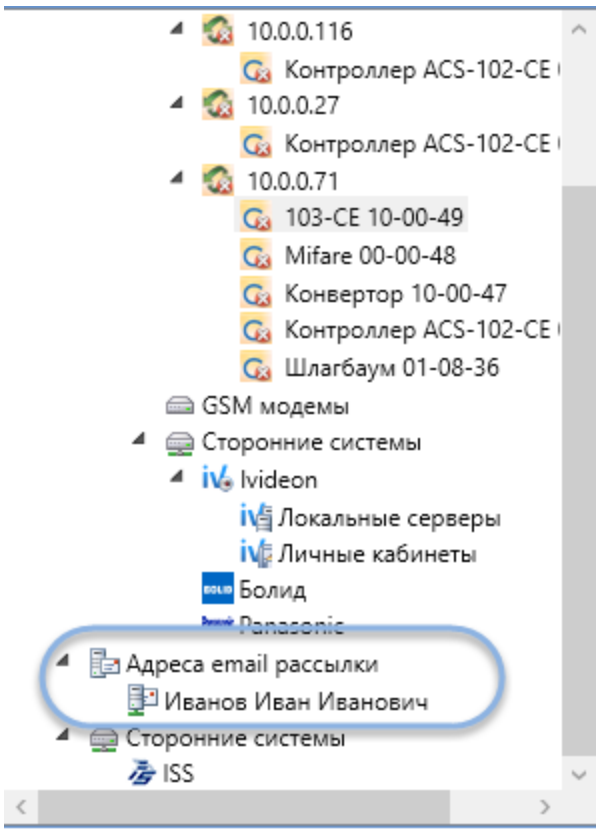


Рисунок 27 - Список адресов электронной почты

2. Откройте вкладку ***Сервисные функции*** главного экрана (см. рис. 28).

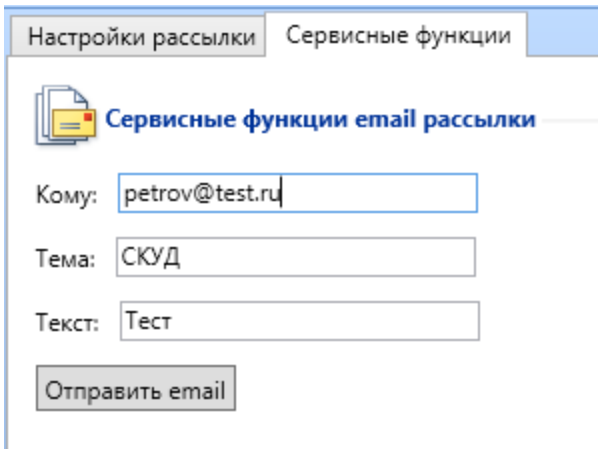


Рисунок 28 - Создание сообщения для отправки по электронной почте

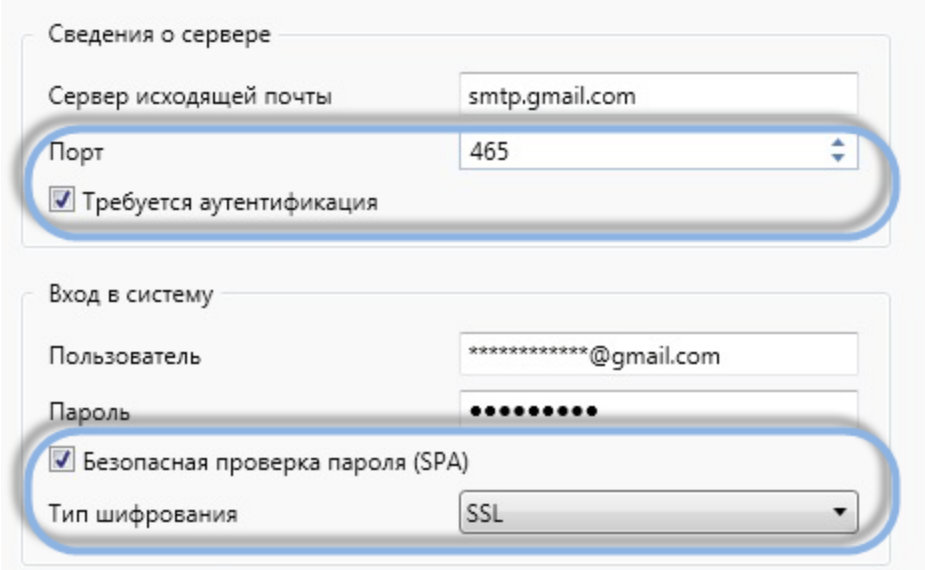
3. Заполните форму (см. рис. выше), нажмите на кнопку Отправить email.

Система выполнит отправку при условии, что данные на вкладке ***Настройки рассылки*** корректны.

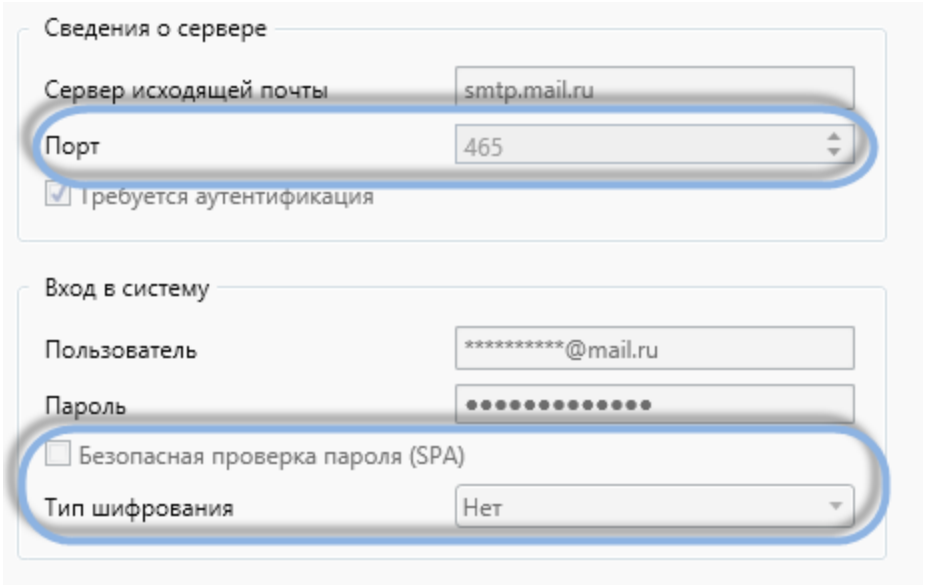
Образцы настройки рассылки на основные почтовые сервисы

Настройки для разных почтовых сервисов различаются параметрами серверов, прежде всего, портами (см. иллюстрации ниже).

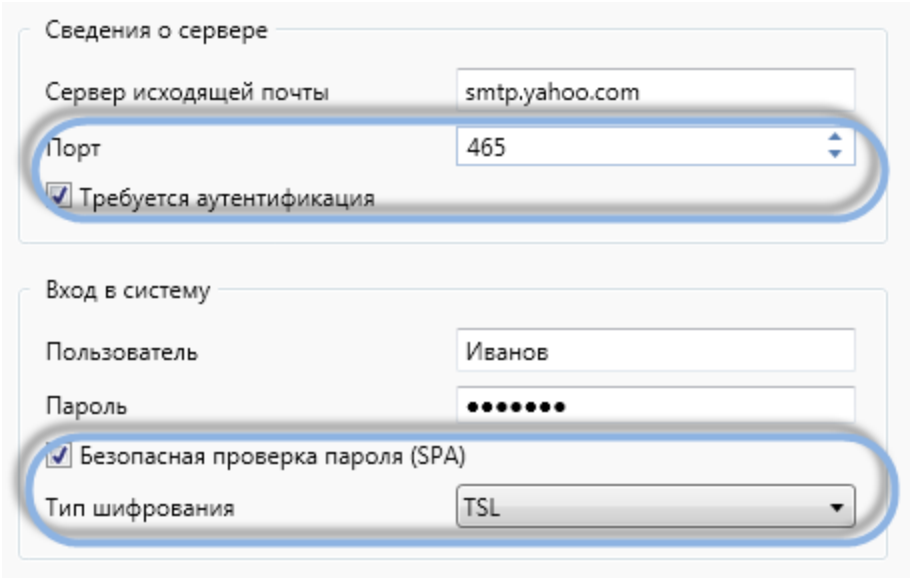
GMAIL.COM



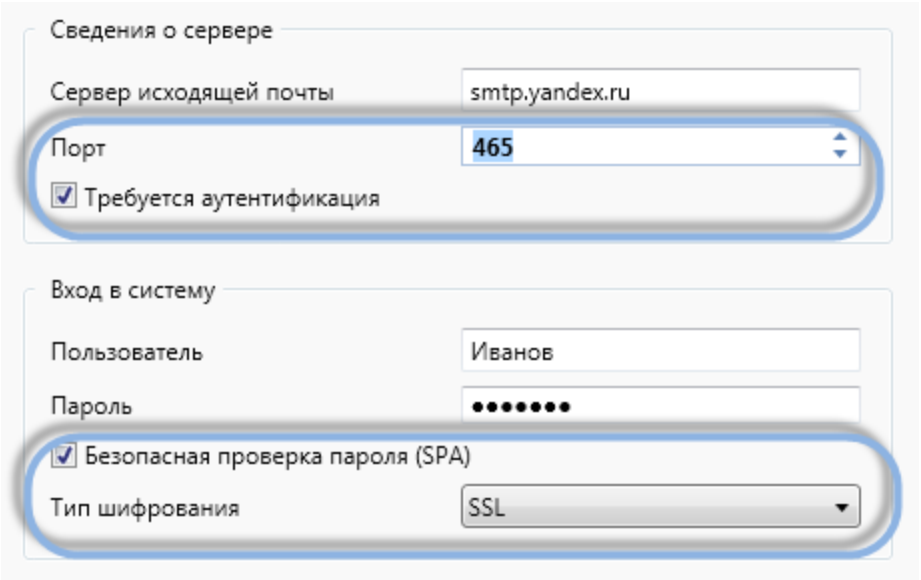
MAIL.RU



YAHOO.COM



YANDEX.RU



Настройка и использование GSM-модема

Для рассылки SMS-уведомлений пользователям систем, обслуживаемых ПО RusGuard (в частности, связанных с настроенными *Реакциями* 193), необходима настройка GSM-модема. Настройка осуществляется в модуле ***Конфигурация оборудования***.

Настройка устройства

Для того чтобы настроить GSM-модем:

1. Зайдите в модуль ***Конфигурация оборудования*** 79 АРМ.

2. В левой навигационной панели выберите пункт ***GSM-модемы***. Установите на нем курсор.
3. В панели управления нажмите на кнопку  ***Добавить GSM-модем***. Откроется окно выбора сервера оборудования.
4. Выберите нужный вариант и подтвердите действие.

Откроется окно для ввода параметров устройства (см. рис. 29).

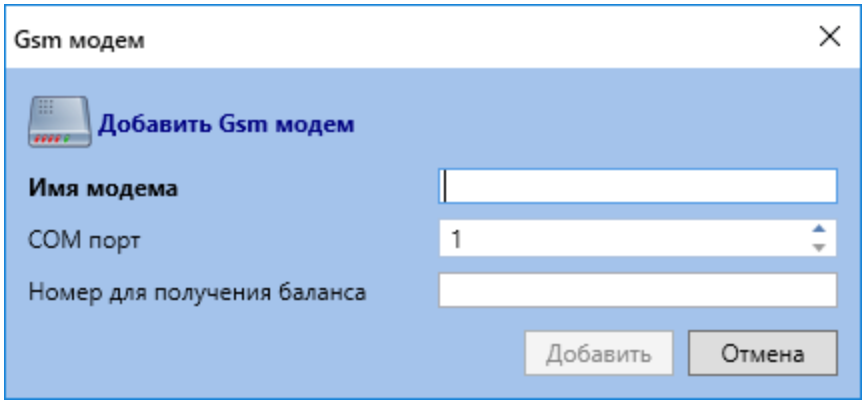


Рисунок 29 - Ввод параметров GSM-модема

5. Заполните обязательные поля (***Имя модема*** и ***COM порт***). Нажмите на кнопку Добавить.

Поле ***Номер для получения баланса*** может потребоваться, если вы захотите использовать функцию запроса баланса средств. Номер может быть введен как на этапе первоначальной настройки устройства, так и позднее.

Система выполнит сохранение данных. Строка с именем настроенного устройства (поле ***Имя модема***) отобразится в иерархическом списке навигационной панели слева (см. рис. 30).

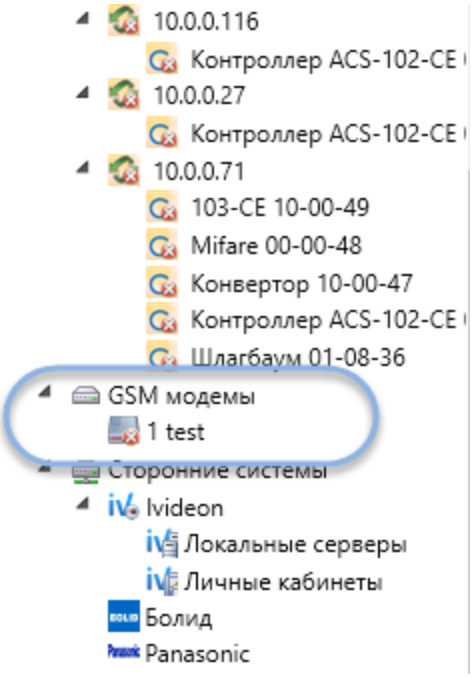


Рисунок 30 - Отображение настроенного модема в навигационной панели

Чтобы начать работать с устройством (отредактировать данные, запросить баланс или выполнить разовую отправку SMS), щелкните мышью по его названию. В главном экране загрузится интерфейс для работы с модемом, состоящий из двух вкладок ***Настройки модема*** и ***Сервисные функции*** (см. рис. 31).

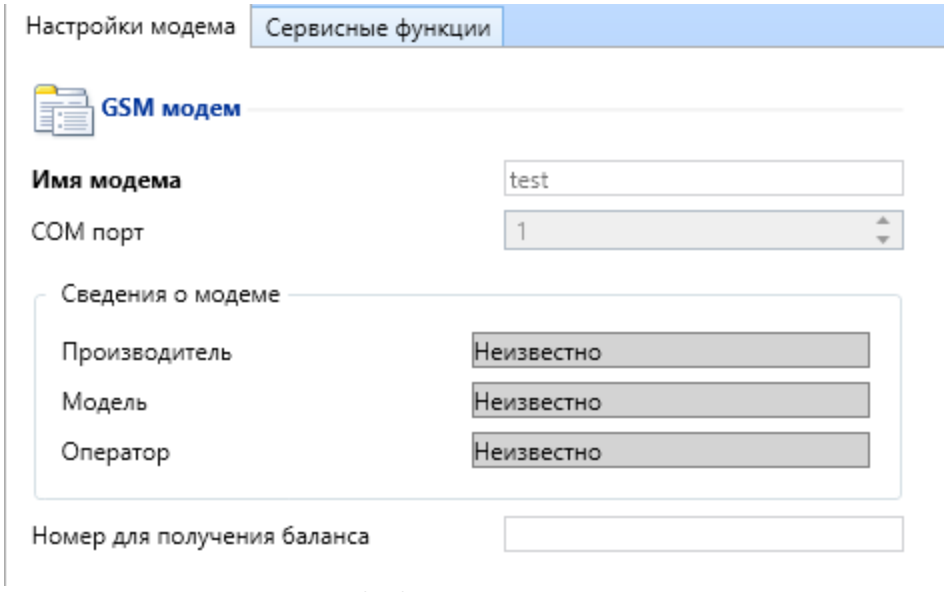


Рисунок 31 - Экран управления модемом

Использование GSM-модема

Вы можете:

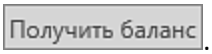
- отредактировать параметры модема

- запросить баланс
- выполнить разовую отправку SMS-сообщения

Для того чтобы отредактировать параметры модема:

1. Выберите нужное устройство в навигационной панели.
2. Оставаясь на вкладке ***Настройки модема*** (открывается по умолчанию), нажмите на кнопку  ***Редактировать*** в панели управления сверху.
3. Внесите необходимые изменения.
4. Нажмите на кнопку  ***Сохранить*** в панели управления сверху.

Для того чтобы запросить баланс средств на счете:

1. Выберите нужное устройство в навигационной панели.
2. Оставаясь на вкладке ***Настройки модема*** (открывается по умолчанию), нажмите на кнопку  ***Редактировать*** в панели управления сверху.
3. Введите номер телефона для запроса баланса в соответствующее поле, если номер отсутствует.
4. Нажмите на кнопку  ***Сохранить*** в панели управления сверху. Перейдите на вкладку ***Сервисные функции*** (при попытке перейти в другой экран без сохранения изменений, система потребует сохранить или отменить их).
5. Нажмите на кнопку 

.

Система направит запрос, данные поступят на указанный номер.

Для того чтобы выполнить разовую отправку SMS:

1. Выберите нужное устройство в навигационной панели.
2. Перейдите на вкладку ***Сервисные функции***.
3. Введите телефонный номер адресата сообщения в соответствующие поля. Введите текст сообщения.
4. Нажмите на кнопку 

. Кнопка активна только при корректном заполнении полей формы.

Система выполнит отправку сообщения.

Поиск устройств в модуле

Быстрый поиск устройств по имени

Если вы точно знаете имя устройства, вы можете быстро найти его через функцию быстрого поиска панели управления:

1. Щелкните мышью пиктограмму 

в панели управления.

Отобразится окно ввода параметров поиска (см. рис. 32).

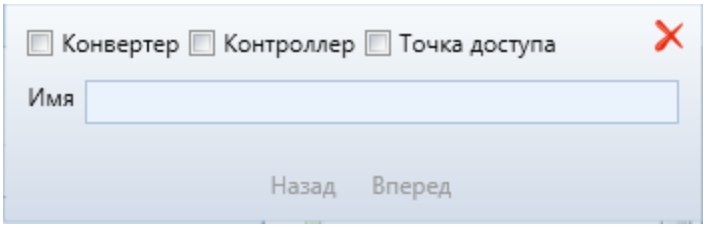


Рисунок 32 - APM RusGuard. Модуль Конфигурация оборудования. Форма быстрого поиска

2. Введите имя устройства в поле ***Имя*** и укажите тип устройства (установите соответствующий флаг).
3. Щелкните мышью ссылку ***Вперед***.

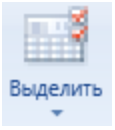
Система выполнит поиск. Если устройство с указанным именем найдено, оно выделяется в списке слева.

Чтобы закрыть окно поиска, щелкните пиктограмму  в верхнем правом углу этого окна.

Выделение устройств одного типа

Если необходимо синхронизировать несколько устройств одного типа внутри сложной конфигурации, можно выделить их топологии, используя специальную функцию.

Для того чтобы выделить все устройства одного типа:

1. Щелкните мышью пиктограмму 

в верхней панели управления.
2. Выберите тип устройств для выделения в меню, которое раскроется (см. рис. 33).

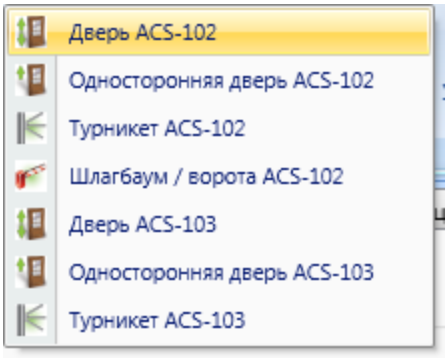


Рисунок 33 - АРМ RusGuard. Модуль Конфигурация оборудования. Меню функции выделения устройств по типу

Устройства выбранного типа выделяются в топологии (подсвечиваются синим). Доступна функция синхронизации 86.

Модуль Конфигурация СКУД

Общие сведения

Данный модуль позволяет вести базы данных сотрудников, должностей, точек доступа, а также вести производственные календари на сутки, определенные дни, недели, настраивать взаимосвязи между этими БД. Здесь же выполняется оформление пропусков для сотрудников (см. рис. 34).

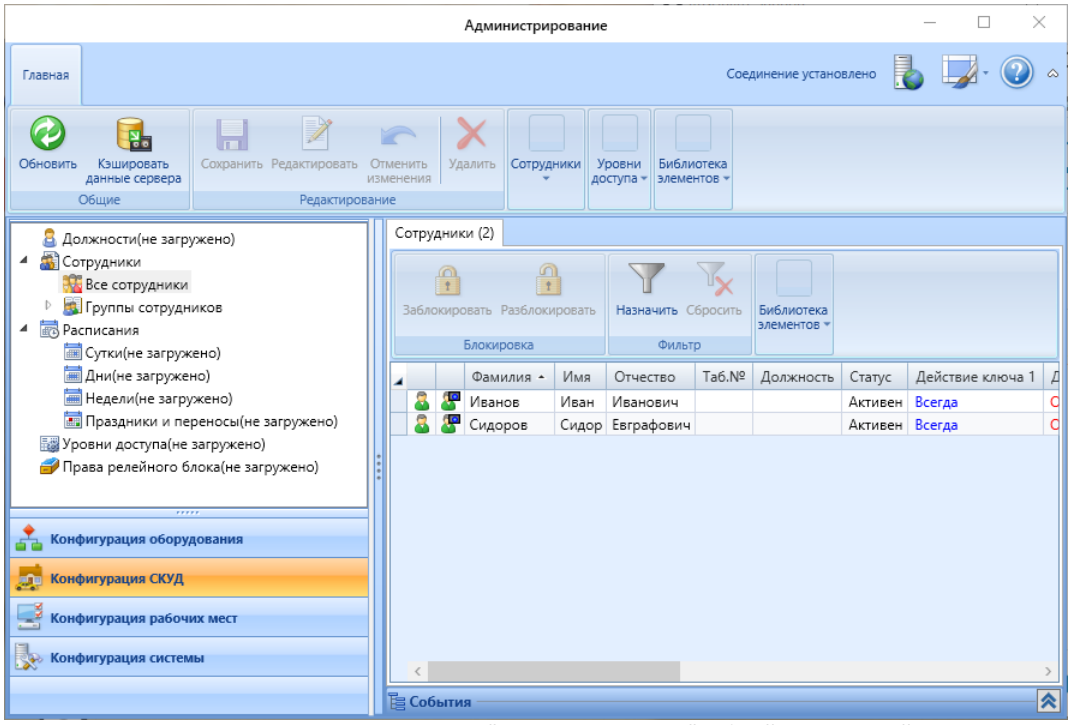


Рисунок 34 - APM RusGuard. Модуль "Конфигурация СКУД". Общий вид интерфейса

В левой части экрана отображается список настраиваемых сущностей (должности, сотрудники, расписания, уровни доступа, права релейного блока). Наверху расположена панель инструментов. Активность кнопок панели инструментов зависит от выбранной сущности. Например, только перейдя к списку ***Все сотрудники*** или зайдя в определенную группу, можно добавить нового сотрудника. Если выбран пункт ***Уровни доступа*** слева, в панели управления активируется возможность создания уровня доступа.

В центральном окне отображаются свойства выделенной сущности (группы сотрудников, уровня доступа, расписания). Чтобы отредактировать параметры конкретного элемента, всегда сначала необходимо нажать на кнопку  в верхней панели инструментов.

В нижней части экрана предусмотрена возможность просмотра списка событий. По умолчанию список скрыт.

Привязка меток группам сотрудников

Метки 206 в APM RusGuard привязываются к группам сотрудников 69, но не к отдельным сотрудникам (см. рис. 35).

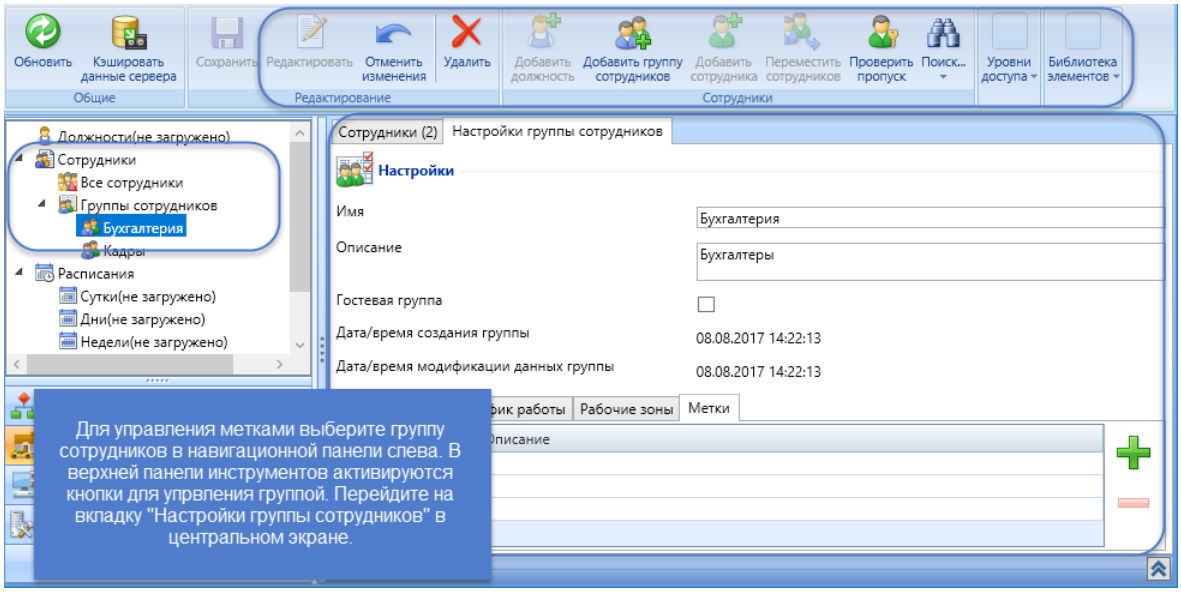
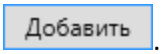


Рисунок 35 - АРМ RusGuard. Модуль "Конфигурация СКУД". Привязка меток

Для того чтобы привязать метку к группе сотрудников:

1. Перейдите к настройкам нужной группы сотрудников (вкладка ***Настройки группы сотрудников***).
2. Нажмите на кнопку  в верхней панели управления.
3. В области ***Метки*** нажмите на пиктограмму  .

Загрузится общий список меток системы (кроме тех, которые были ранее привязаны к уровню доступа.)

4. Выберите нужную метку и нажмите на кнопку  .

Добавленная метка отобразится в списке привязанных (см. рис. 36).

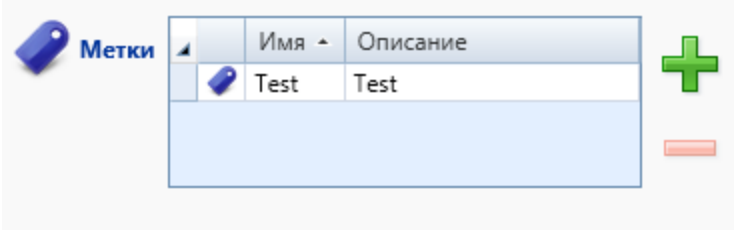


Рисунок 36 - АРМ RusGuard. Модуль "Конфигурация СКУД"
Привязка меток группе сотрудников

5. Сохраните изменения ().

Чтобы удалить метку из списка привязанных, выделите ее в списке и щелкните пиктограмму  .

Ведение базы данных сотрудников

База данных сотрудников состоит из общего списка сотрудников и списка групп сотрудников. Учетная запись сотрудника обязательно должна создаваться внутри определенной группы. См. раздел Быстрый старт 65 > Создание учетной записи 70.

При перезапуске АРМ может потребоваться обновление данных.

Обратите внимание, что при обновлении списка сотрудников внутри группы вы можете обновить как только список сотрудников выбранной группы, так и все дерево групп сотрудников (см. рис. 37).

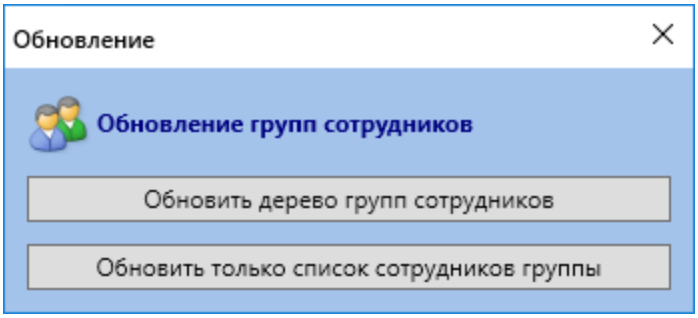


Рисунок 37 - АРМ RusGuard. Модуль Конфигурация СКУД. Обновление списка сотрудников

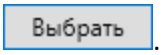
Создание учетной записи и уровня доступа сотрудника. Оформление пропуска

Уровень доступа редактируется непосредственно в карточке сотрудника. Кроме того, возможно редактирование уровня доступа для группы сотрудников из общего списка.

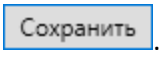
По умолчанию, сотруднику присваивается уровень доступа родительской группы, но возможно присвоение ему другого и/или дополнительного уровня доступа.

Для того чтобы присвоить сотруднику дополнительный, альтернативный уровень доступа:

1. Откройте карточку нужного сотрудника.
2. Перейдите на вкладку ***Уровни доступа***.
3. Чтобы добавить уровень доступа, нажмите на кнопку  .

   В новом окне загрузится список доступных уровней доступа.
4. Выберите нужный уровень доступа, нажмите на кнопку 

.

   Название выбранного уровня доступа отобразится в списке на вкладке ***Уровни доступа*** карточки сотрудника.
5. Чтобы применить изменения, нажмите на кнопку 

.

Чтобы удалить уровень доступа из списка, используйте кнопку  .

Чтобы использовать уровень/уровни доступа родительской группы, установите соответствующий флаг.

Вы можете настроить срок действия уровня доступа для сотрудника:

1. Выполните привязку уровня доступа к сотруднику, как описано выше.
2. Оставаясь на вкладке ***Уровни доступа***, выделите присвоенный уровень доступа в списке и щелкните пиктограмму  .

Откроется окно для редактирования параметров уровня доступа, где вы можете указать срок его действия (см. рис. 38). По умолчанию выбран вариант ***Всегда***.

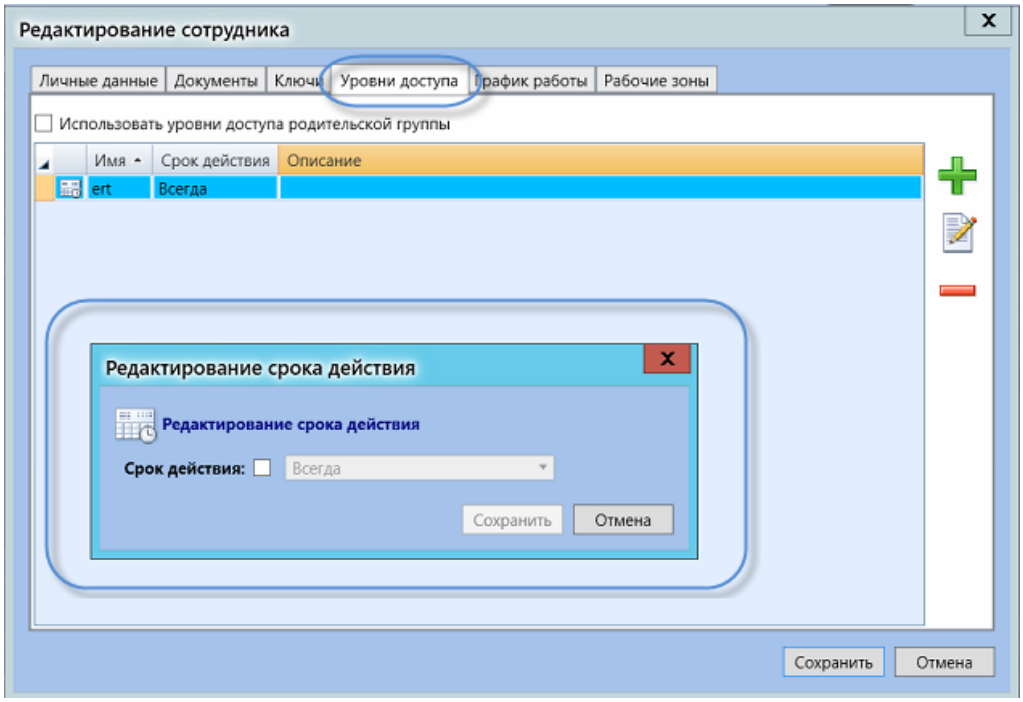
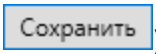


Рисунок 38 - АРМ RusGuard. Модуль Конфигурация СКУД. Настройка срока действия уровня доступа сотрудника

3. Чтобы настроить определенную дату, установите флаг ***Срок действия*** и введите дату в поле ввода.
4. Сохраните изменения (кнопка ).

Обратите внимание на особенности создания уровня доступа для точки доступа типа "Шкафы/Витрины" 117.

Групповые операции с учетными записями сотрудников

ПО RusGuard позволяет выполнять групповые операции с учетными записями сотрудников. Для доступа к этим функциям необходимо загрузить список сотрудников и перейти в центральный экран модуля (см. рис. 39).

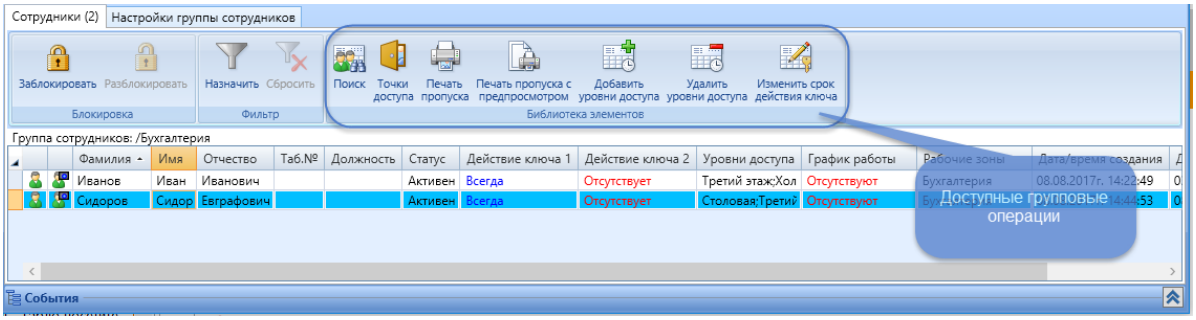
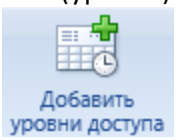
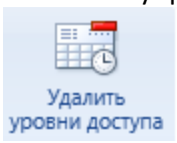
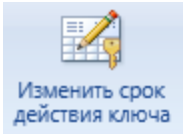


Рисунок 39 - APM RusGuard. Модуль Конфигурация СКУД. Групповые операции со списком сотрудников

Система позволяет привязать уровень доступа нескольким сотрудникам одновременно. Чтобы привязать уровень (уровни) доступа к нескольким сотрудникам, выделите их в списке и нажмите на кнопку 

в панели управления над списком. Обратная процедура выполняется при помощи кнопки 

.

Также, групповое редактирование доступно для настройки срока действия ключа. Чтобы изменить срок действия ключа у нескольких сотрудников, выделите нескольких сотрудников в списке (это может быть общий список сотрудников или список сотрудников определенной группы). Щелкните пиктограмму 

в панели управления списка. Откроется диалоговое окно (см. рис. 40), где вы сможете ввести новые параметры ключей (одного или двух) для выбранных сотрудников. Обратите внимание, что вы можете автоматически исключить сотрудников, с истекшим сроком действия ключа.

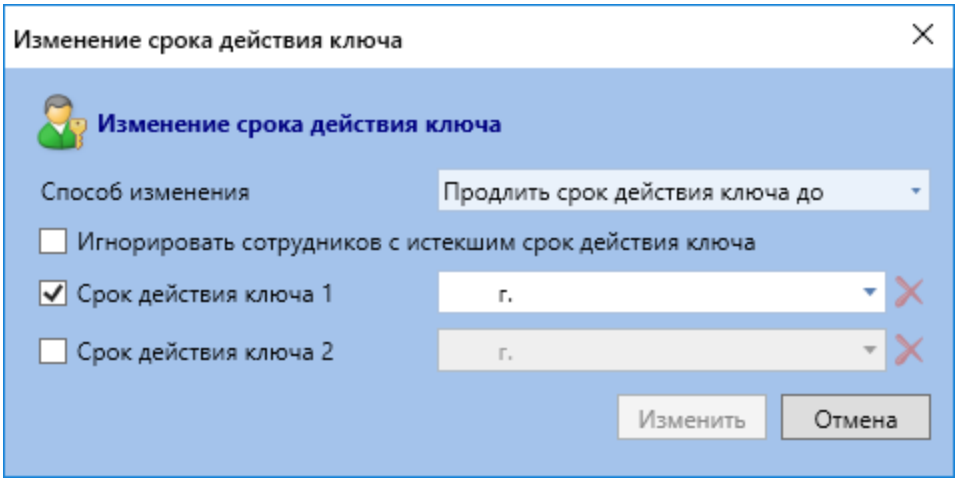


Рисунок 40 - APM RusGuard. Модуль Конфигурация СКУД. Настройка срока действия ключа для группы сотрудиников

Служебные операции: фильтрация, поиск, блокировка, перемещение, импорт

Для того чтобы отфильтровать список сотрудников:

1. Через иерархический список в левой навигационной панели раскройте список сотрудников (функция фильтрации доступна как в полном списке, так и в списках сотрудников внутри групп, интерфейс функции в обоих случаях одинаков).

2. Нажмите на кнопку  .

Откроется окно ***Редактирование фильтра сотрудников*** (см. рис. 41).

В этом окне отображаются все доступные фильтры. По умолчанию фильтры настроены так, чтобы отображался полный список сотрудников.

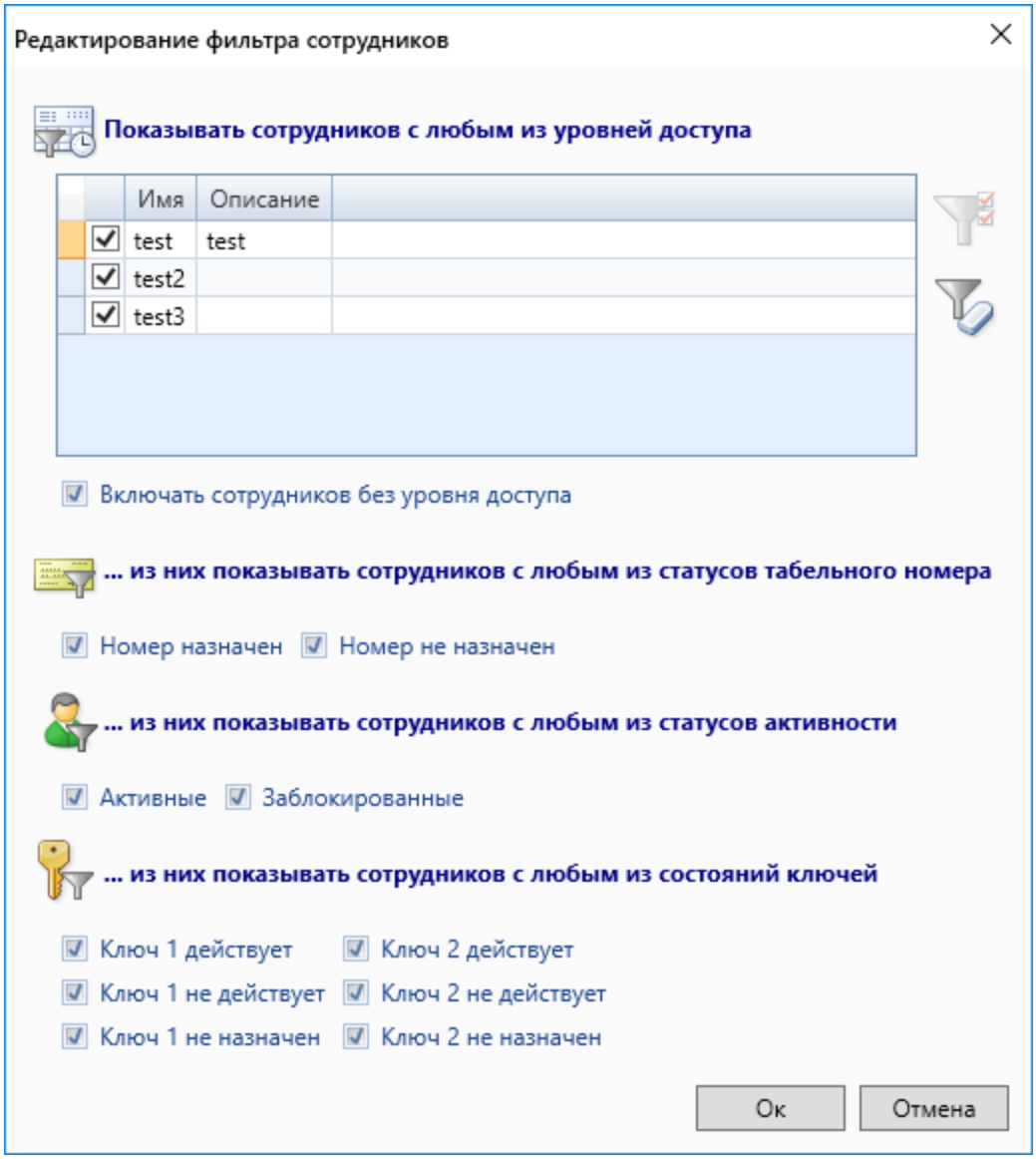


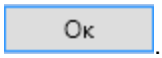
Рисунок 41 - АРМ RusGuard. Модуль Конфигурация СКУД. Окно настройки фильтра списка сотрудников

3. Задайте необходимые фильтры, снимая/устанавливая флажки, напротив определенных параметров. Сотрудники с соответствующим признаком исключаются из списка, если флажок снят, и отображаются, если флажок установлен. АРМ

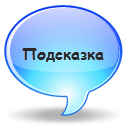
поддерживает использование нескольких фильтров одновременно, порядок (приоритетность фильтрации) соответствует расположению фильтров в списке, т.е. сначала применяется верхний фильтр, затем следующий за ним и т.д.

АРМ позволяет фильтровать сотрудников по следующим признакам:

- Уровень доступа. Пользователь может отфильтровать список по одному или нескольким уровням доступа. Также предусмотрена возможность вывода учетных записей сотрудников, уровень доступа для которых не назначен.
- Наличие табельного номера (присваивается в карточке сотрудника, нужен для бухгалтерских целей);
- Активность учетной записи;
- Наличие и статус ключей (один ключ, два ключа, один активный ключ, два активных ключа, и т.д. в любом сочетании).

4. Чтобы применить фильтр, нажмите на кнопку 

.



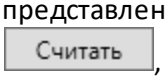
Если фильтр назначен, активируется кнопка 

в верхней панели инструментов. Используйте ее, чтобы сбросить все фильтры.

Для того чтобы найти сотрудника в БД:

1. Через иерархический список в левой навигационной панели раскройте список сотрудников (функция фильтрации доступна как в полном списке, так и в списках сотрудников внутри групп, интерфейс функции в обоих случаях одинаков).
2. Нажмите на кнопку 
.

Откроется окно ***Поиск сотрудников***.

3. Выберите один из трех параметров поиска ***ФИО***, ***Табельный номер*** или ***Ключи*** (одновременно может использоваться только один параметр):
   - фамилия, имя и отчество (возможен поиск только по фамилии, имени или отчеству, либо по полному имени);
   - табельный номер;
   - ключ (обратите внимание, что ввод ключа возможен в десятичном и шестнадцатеричном представлениях. Также, при выборе этого параметра активируется кнопка 

, позволяющая использовать устройство, считывающее данные карт.).
4. Введите искомое значение параметра.
5. Нажмите на кнопку ***Найти далее***.

Если искомый сотрудник найден, приложение выделит строку с его данными на вкладке ***Сотрудники*** в главном экране. Если искомый сотрудник не обнаружен в БД, отображается соответствующее сообщение.

Для того чтобы заблокировать учетную запись сотрудника/ов:

1. Найдите сотрудника (или сотрудников) в БД (например, используя функцию поиска141).
2. Выделите строку с данными о сотруднике на вкладке ***Сотрудники*** списка (доступна как через общий список сотрудников, так и при навигации через группы). Вы также можете выделить несколько строк, используя стандартные комбинации клавиш ОС Windows для выделения.
3. Нажмите на кнопку  в панели инструментов выбранной вкладки. Эта кнопка доступна только если выбранный сотрудник имеет статус `Активен` (обозначается пиктограммой ).

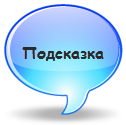
Система блокирует учетную запись (отображается окно, демонстрирующее выполнение процесса). Пиктограмма возле имени заблокированного сотрудника становится серой (), его статус меняется с `Активен` на `Заблокирован`.

Кроме того активируется кнопка  , которая позволяет выполнить обратную операцию.

Для того чтобы переместить сотрудника или сотрудников:

1. Найдите сотрудника (или сотрудников) в БД (например, используя функцию поиска141).
2. Выделите строку с данными о сотруднике на вкладке ***Сотрудники*** списка (доступна как через общий список сотрудников, так и при навигации через группы). Вы также можете выделить несколько строк, используя стандартные комбинации клавиш ОС Windows для выделения.
3. Нажмите на кнопку  ***Переместить сотрудников*** в верхней панели управления.

Отобразится окно выбора группы, в которую следует переместить выбранного сотрудника(ов) (см. рис. 42).



Если необходимо создать новую группу, а затем переместить в нее сотрудника(ов), вы можете выполнить оба действия в этом окне, используя кнопку Добавить группу сотрудников в нем.

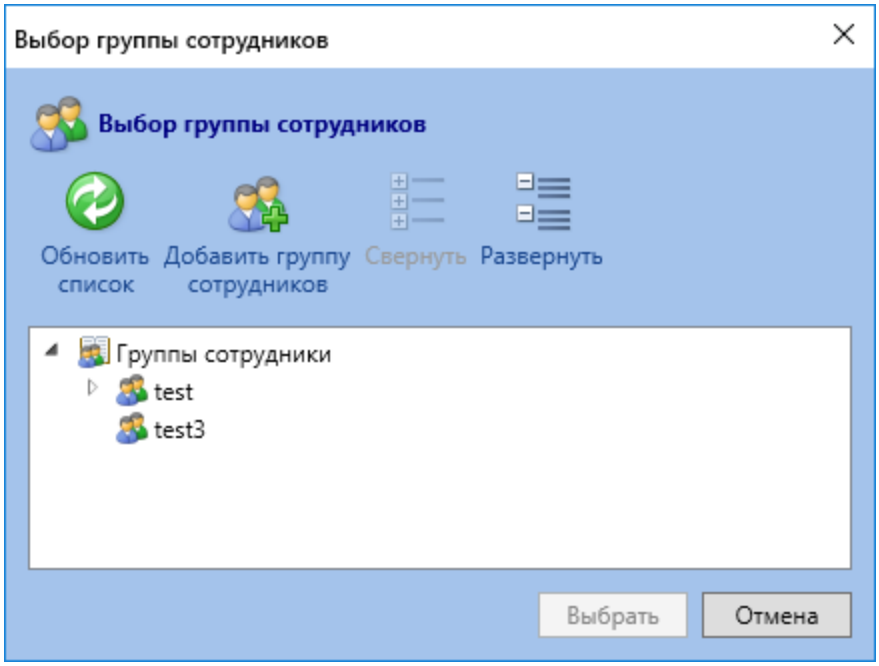


Рисунок 42 - APM RusGuard. Модуль Конфигурация СКУД. Диалог перемещения сотрудников

4. Выберите одну из существующих групп или создайте новую. Нажмите на кнопку Выбрать.
5. Подтвердите действие.

Система переместит выбранную учетную запись (или записи) в указанную группу.

Загрузка и распознавание документов

Используя вкладку ***Документы*** (см. рис. 43) карточки сотрудника, пользователь может:

- загружать отсканированные копии паспортов, водительских удостоверений и заграничных паспортов;
- редактировать графические файлы;
- распознавать данные отсканированных документов при помощи модуля ABBYY PassportReader SDK и использовать их для заполнения полей карточки (подробнее об ABBYY PassportReader SDK см. в разделе "Установка стороннего ПО" Руководства по установке).

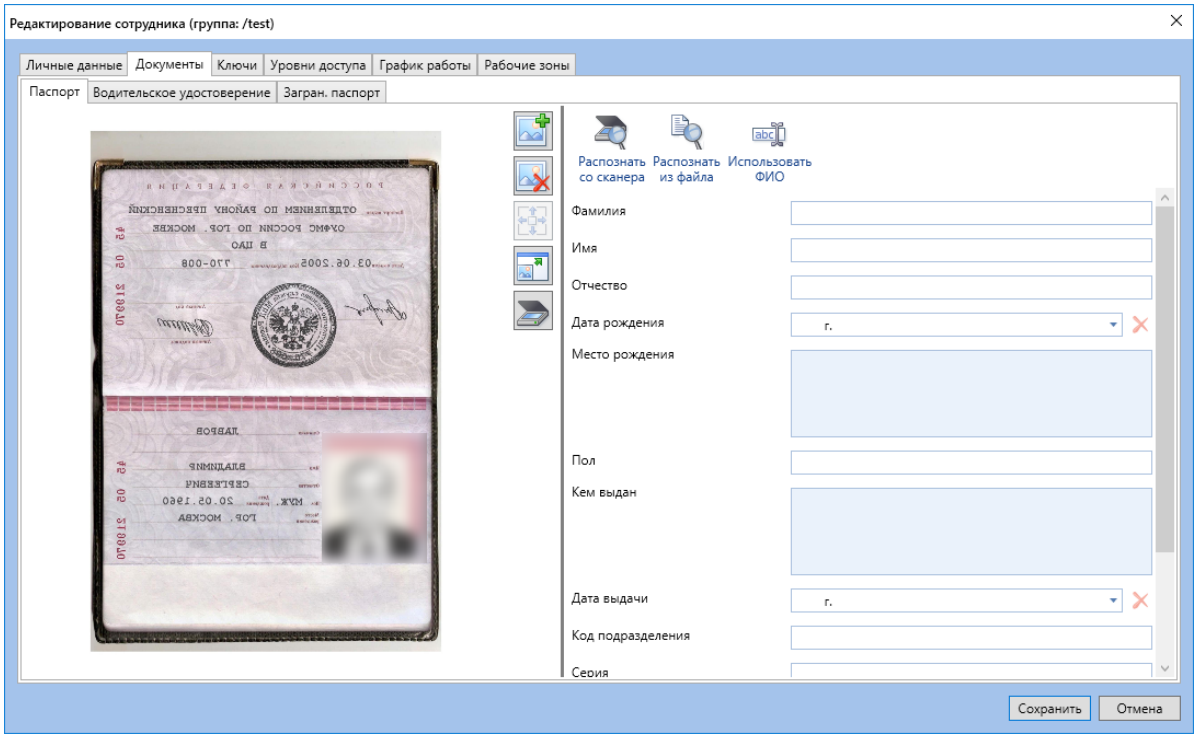


Рисунок 43 - АРМ RusGuard. Модуль Конфигурация СКУД. Карточка сотрудника. Вкладка Документы

Для того чтобы загрузить изображение в карточку:

1. Перейдите на вкладку ***Документы*** карточки нужного сотрудника.
2. Нажмите на кнопку  .

Откроется стандартный диалог выбора файла приложения Проводник ОС Windows.

3. Выберите графический файл для загрузки.

АРМ предложит отредактировать файл в новом окне (см. рис. 44).

4. Если это необходимо, отредактируйте файл и нажмите на кнопку  .

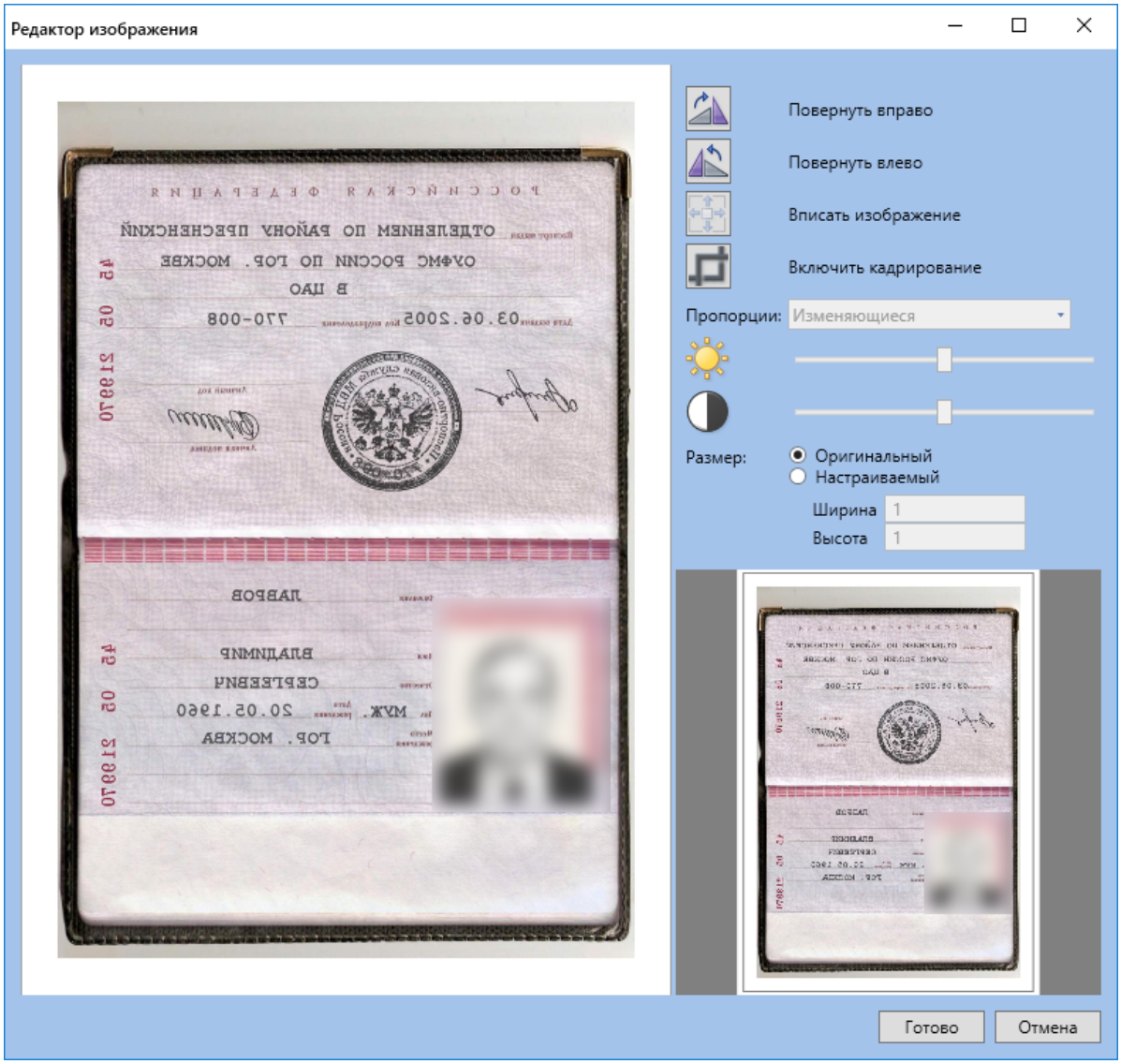


Рисунок 44 - APM RusGuard. Модуль Конфигурация СКУД. Карточка сотрудника. Вкладка Документы. Редактирование загружаемой копии паспорта

Изображение появится на вкладке ***Документы*** слева.

5. Нажмите на кнопку Сохранить, чтобы завершить процедуру.

Подсказка Обратите внимание на кнопку abc, с ее помощью вы можете переносить отсканированные фамилию, имя и отчество сотрудника из документа в соответствующие поля на вкладке ***Личные данные***.

Для того чтобы распознать данные с отсканированной копии документа:

1. Перейдите на вкладку ***Документы*** карточки нужного сотрудника.
2. Выполните одно из следующих действий:

- Нажмите на кнопку  ***Распознать со сканера***, если необходимо распознать сканируемый документ;
- Нажмите на кнопку  ***Распознать из файла***, если необходимо распознать уже готовую отсканированную копию из файла.

Внимание: Для использования функции должен быть установлен модуль ABBYY PassportReader SDK и USB-ключ лицензии к нему. Модуль не поддерживает распознавание документов с разрешением отличным от 300dpi, выполненных в цвете.

При распознавании заграничных паспортов возможны ошибки, так как эти паспорта содержат символы латинского алфавита.

(подробнее об ABBYY PassportReader SDK см. в разделе "Установка стороннего ПО" Руководства по установке).

Загрузится окно с результатом распознавания (см. рис. 45).

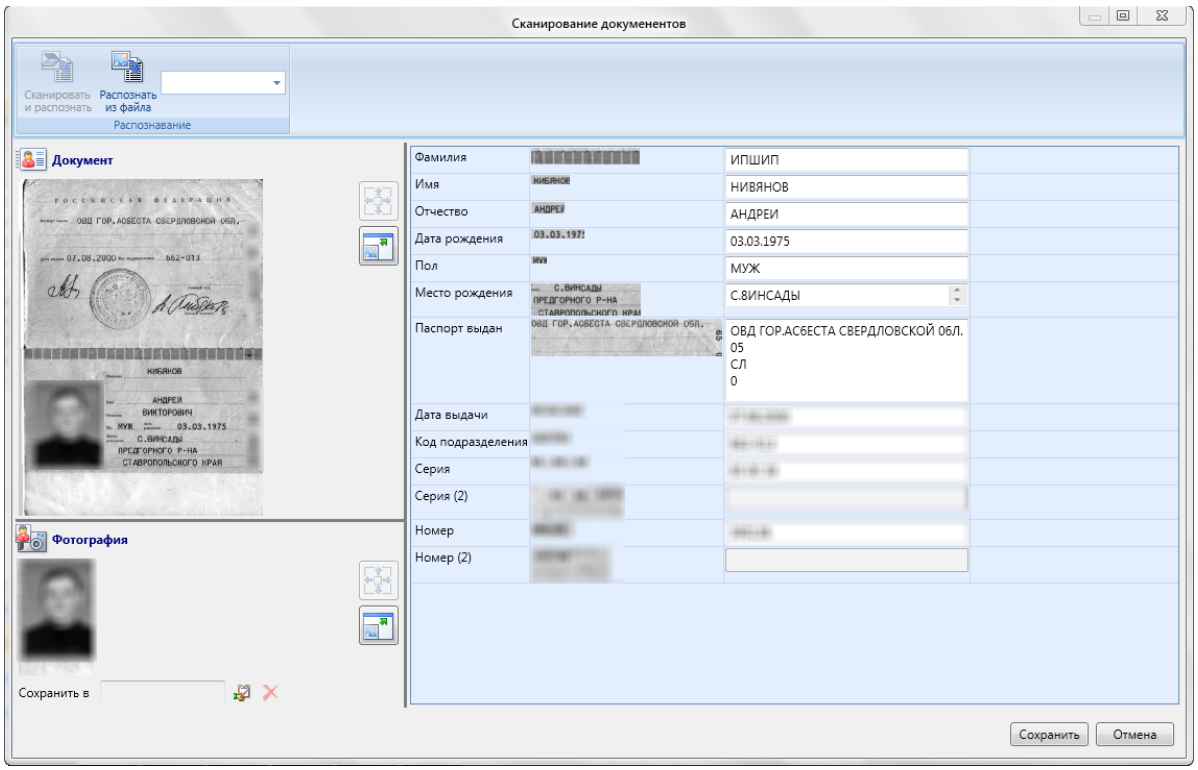


Рисунок 45 - АРМ RusGuard. Модуль Конфигурация СКУД. Карточка сотрудника. Вкладка Документы. Сканирование и распознавание паспорта

3. Исправьте возможные ошибки и нажмите на кнопку Сохранить.

Данные отобразятся на вкладке ***Документы*** справа.

4. Нажмите на кнопку Сохранить, чтобы завершить процедуру.

Ведение базы данных должностей

Создание должности

См. раздел Быстрый старт > Создание должности 69.

Управление расписаниями

APM RusGuard позволяет вести расписания рабочего времени на каждые сутки, определенный день (несколько дней), на неделю, а также производственный календарь на год.

В АРМ предусмотрено два типа суточных расписаний: *встроенный* и *пользовательский* (см. рис. 46). К первому типу относятся три расписания, созданные по умолчанию. Пользователь не может редактировать и удалять их. К пользовательским относятся все прочие расписания, создаваемые в АРМ пользователями.

Расписания на дни, недели и т.д., - только пользовательского типа.

Создаваемые расписания привязываются к точкам доступа в этом же модуле.

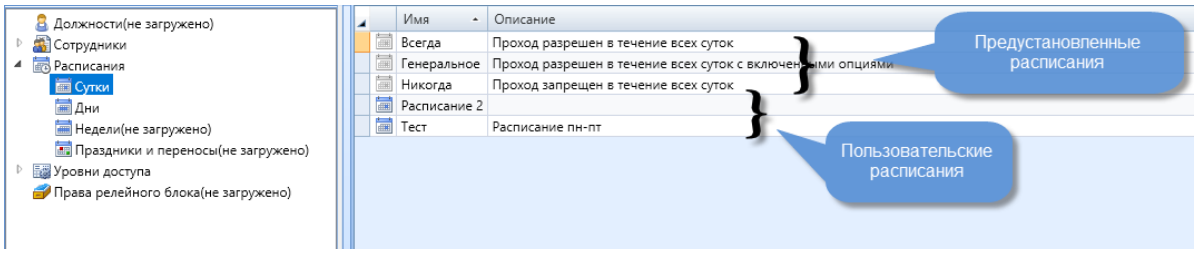


Рисунок 46 - APM RusGuard. Модуль Конфигурация СКУД. Список суточных расписаний

Для того чтобы создать суточное расписание:

1. Через иерархический список в левой навигационной панели раскройте список ***Расписания***. Зайдите в пункт ***Сутки***.

2. Нажмите на кнопку  ***Добавить расписание*** в верхней панели управления. Откроется окно ***Добавление расписания*** (см. рис. 47).

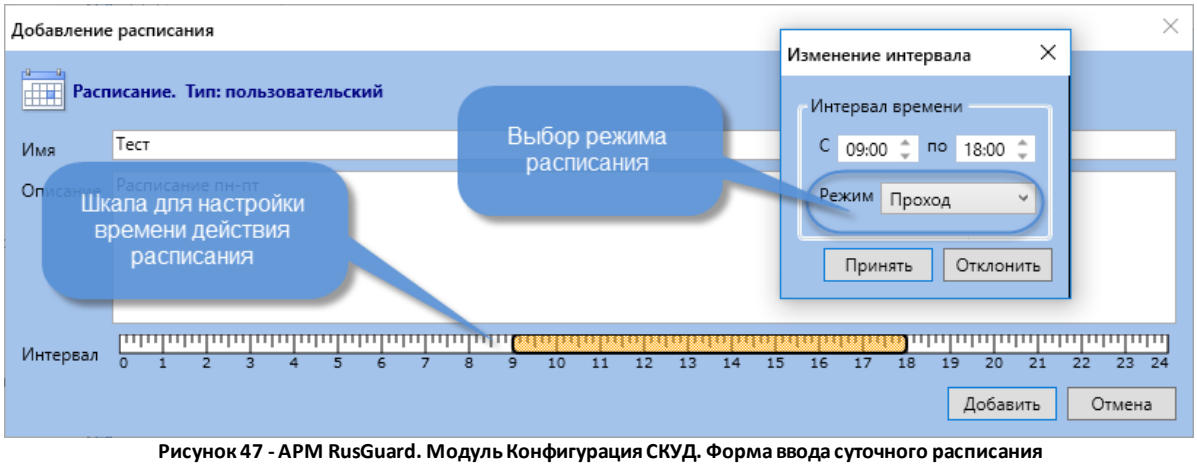


Рисунок 47 - APM RusGuard. Модуль Конфигурация СКУД. Форма ввода суточного расписания

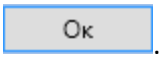
3. Заполните форму. Обязательные поля: ***Имя*** и ***Интервал***.

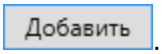
В поле ***Имя*** вводится название расписания, в поле (шкале) ***Интервал*** задается промежуток времени, когда возможен проход на объект, охраняемый СКУД, через ту точку доступа, к которой привязано расписание.

Чтобы задать интервал, щелкните левой кнопкой мыши на начальной или конечной точке желаемого интервала. Удерживая левую кнопку мыши, двигайте курсор влево или вправо, чтобы задать интервал в часах. При этом появляется дополнительное окно, позволяющее настраивать время с точностью до 5 минут.

В процессе установки времени действия расписания, система предлагает выбрать режим расписания:

- ***Проход*** (вход и выход)
- ***Вход*** (только вход)
- ***Выход*** (только вход)
- ***Сервис***

4. Выберите нужный режим из списка и нажмите на кнопку 

.
5. Задав все необходимые параметры, нажмите на кнопку 

.

Новое расписание появится в списке расписаний в главном экране. Расписание на сутки действует на соответствующей точке доступа все время после привязки. Также суточные расписания могут привязываться к недельным.

Для того чтобы создать расписание на несколько дней:

1. Через иерархический список в левой навигационной панели раскройте список ***Расписания***. Зайдите в пункт ***Дни***.
2. Нажмите на кнопку  ***Добавить расписание*** в верхней панели управления. Откроется окно ***Добавление расписания*** (см. рис. 48).

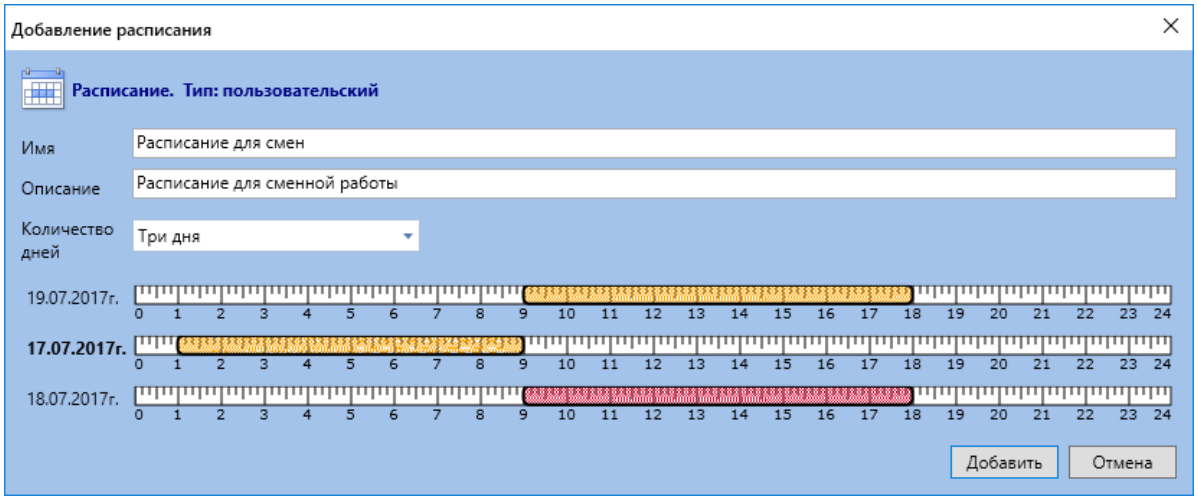


Рисунок 48 - АРМ RusGuard. Модуль Конфигурация СКУД. Форма ввода расписания на дату (даты)

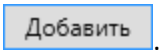
3. Заполните форму. Обязательные поля: ***Имя***, ***Количество дней*** (от 1 до 7 ближайших дней, начиная с текущей даты) и интервалы на каждый из дней.

В поле ***Имя*** вводится название расписания, в списке ***Количество дней*** выбирается необходимое количество дней (от 1 до 7 ближайших дней, начиная с текущей даты), для каждого дня устанавливается собственный интервал, т.е. промежуток времени, когда возможен проход на объект, охраняемый СКУД, через ту точку доступа, к которой привязывается расписание.

Чтобы задать интервал, щелкните левой кнопкой мыши на начальной или конечной точке желаемого интервала. Удерживая левую кнопку мыши, двигайте курсор влево или вправо, чтобы задать интервал в часах. При этом появляется дополнительное окно, позволяющее настраивать время с точностью до 5 минут.

Когда время установлено, система предлагает выбрать режим расписания для каждого интервала:

- ***Проход*** (вход и выход)
- ***Вход*** (только вход)
- ***Выход*** (только вход)
- ***Сервис*** (этот режим предусмотрен для прохода по правилу двух лиц. Если сотрудник с правом первого лица, для которого действительно это расписание, подносит карту к считывателю, дверь не открывается, устройство переходит в режим ожидания поднесения карты с правом или пометкой "Второе лицо")

5. Установите нужный режим для каждого из интервалов.
6. Задав необходимые параметры, нажмите на кнопку 

.

Новое расписание появится в списке расписаний в главном экране. После привязки к точке доступа расписание циклически действует в течение заданного интервала (1-7 дней).

Для того чтобы составить расписание на одну или несколько недель:

1. Через иерархический список в левой навигационной панели раскройте список ***Расписания***. Зайдите в пункт ***Недели***.
2. Нажмите на кнопку  ***Добавить расписание*** в верхней панели управления.

Откроется окно ***Добавление расписания*** (см. рис. 49).

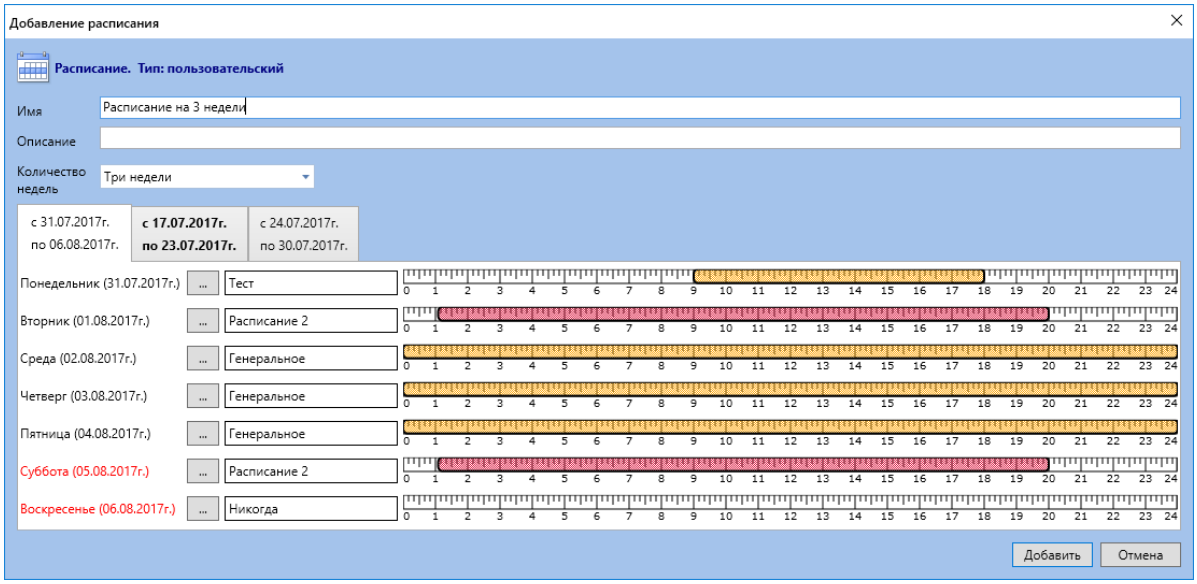


Рисунок 49 - АРМ RusGuard. Модуль Конфигурация СКУД. Установка расписания на неделю

В этом окне пользователь может составить расписание на одну или несколько недель (до 8 недель).

По умолчанию, первый день первой недели расписания - текущая дата.

Настройка недельного расписания составляется из имеющихся в АРМ суточных расписаний 147. По умолчанию для всех дней всех выбранных недель выбрано суточное расписание, запрещающее проход на объект всегда.

3. Заполните поля ***Имя***.
4. Настройте суточное расписание для каждого из дней каждой недели. Для этого нажимайте на кнопку ... возле каждой из дат, чтобы вызывать список доступных суточных расписаний. В списке выбирайте желаемый вариант.
5. Установив расписания для всех дней, нажмите на кнопку Добавить.

Созданное расписание отобразится в главном экране модуля. Расписание на одну или несколько недель привязывается к точке доступа в этом же модуле АРМ.

Для того чтобы добавить выходной или праздничный день в календарь:

1. Через иерархический список в левой навигационной панели раскройте список ***Расписания***. Зайдите в пункт ***Праздники и переносы***.

В главном экране отобразится календарь на текущий год (см. рис. 50).

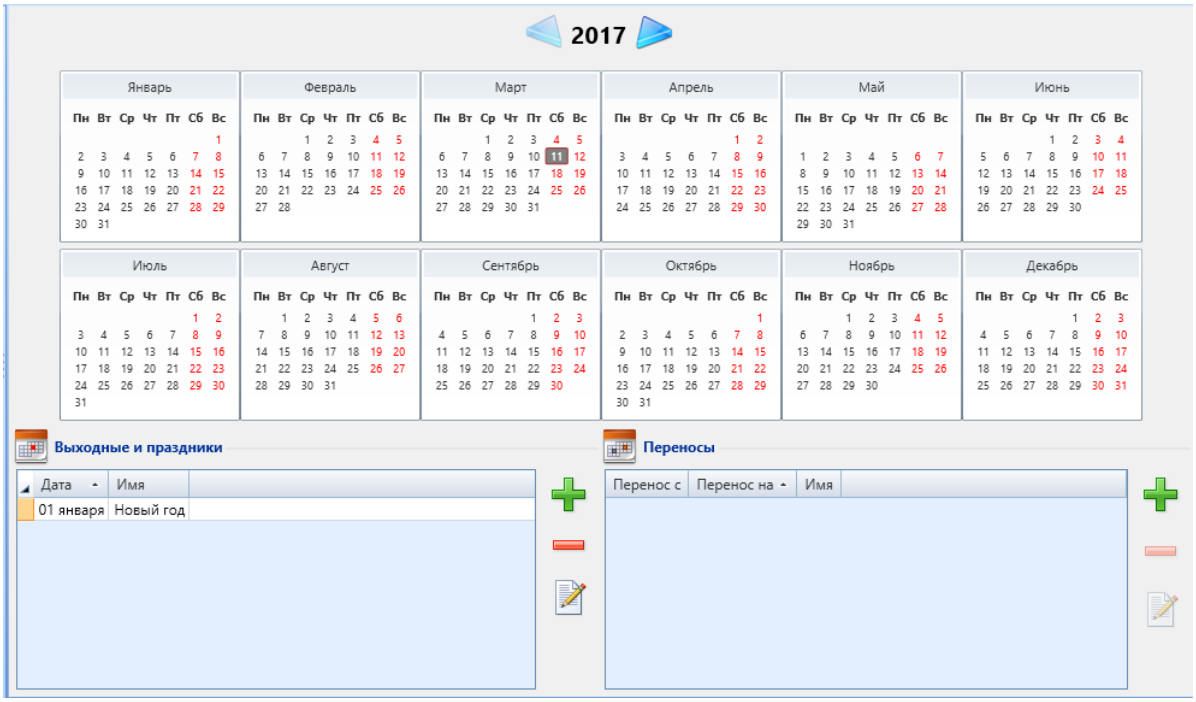
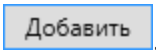
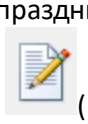


Рисунок 50 - APM RusGuard. Модуль Конфигурация СКУД. Настройка календаря выходных и праздничных дней

2. В области ***Выходные и праздники*** в левой нижней части экрана нажмите на кнопку  .

Откроется окно ***Добавление выходного***. По умолчанию в окне загружен календарь на текущий месяц, но пользователь может пролистать календарь вперед или назад, используя стрелки.

3. Введите название праздника в поле ***Имя***, выберите дату в календаре.
4. Нажмите на кнопку  .

Введенный выходной появится в списке выходных и праздников. При выделении строки в этом списке активируются кнопки  (удаление) и  (редактирование).

Список выходных дней и праздников может использоваться в настройках точек доступов.

Для того чтобы добавить перенос:

1. Через иерархический список в левой навигационной панели раскройте список ***Расписания***. Зайдите в пункт ***Праздники и переносы***.

В главном экране отобразится календарь на текущий год.

1. В области ***Переносы*** в левой нижней части экрана нажмите на кнопку  .

Откроется окно ***Добавление переноса***. По умолчанию в окне загружен календарь на текущий месяц для двух дат: исходной и целевой, но пользователь может пролистать

календарь вперед или назад, используя стрелки. При этом первая и вторая дата должны относиться к одному месяцу.

2. Введите название переноса в поле ***Имя***, выберите даты в календаре слева и справа.
3. Нажмите на кнопку Добавить.

Введенный перенос появится в списке. При выделении строки в этом списке активируются кнопки (удаление) и (редактирование).

Список переносов может использоваться в настройках точек доступов.

Управление уровнями и точками доступа

Как создать уровень и точку доступа, см. здесь 67. Для настройки необходимо перейти к соответствующему пункту навигационной панели модуля (см. рис. 51).

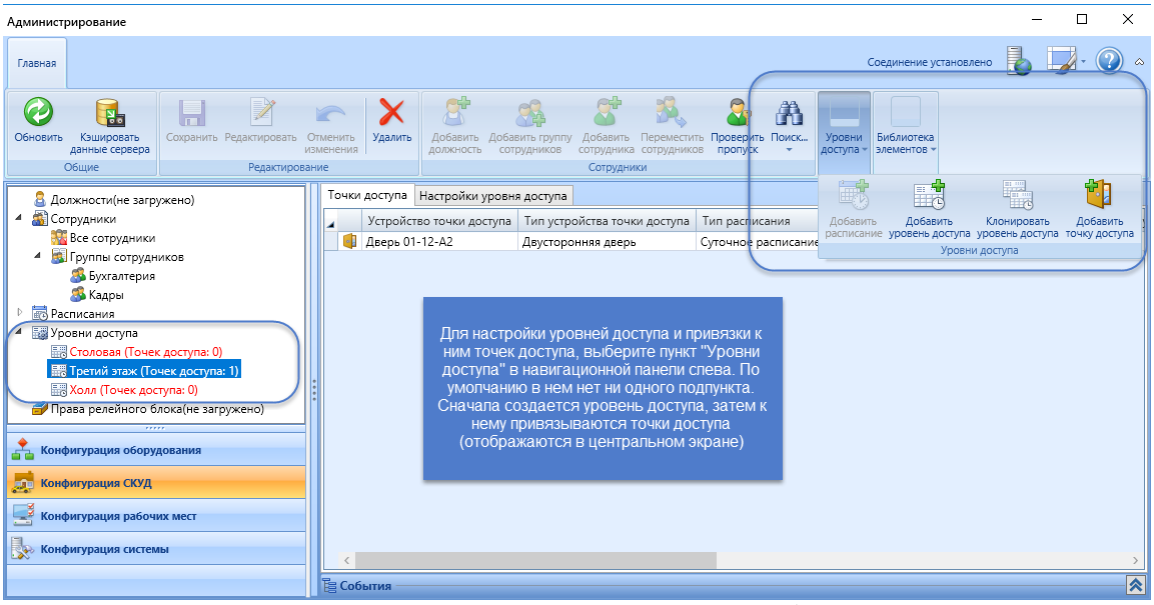


Рисунок 51 - АРМ RusGuard. Модуль Конфигурация СКУД. Порядок работы с уровнями доступа

Для того чтобы настроить точку доступа:

1. Создайте точку доступа.

Созданная точка доступа отображается в списке ***Точки доступа*** выбранного в левой панели уровня доступа.

2. Установите курсор на нужную точку доступа и нажмите на кнопку в верхней панели инструментов.

Откроется окно ***Редактирование точки доступа*** (см. рис. 52).

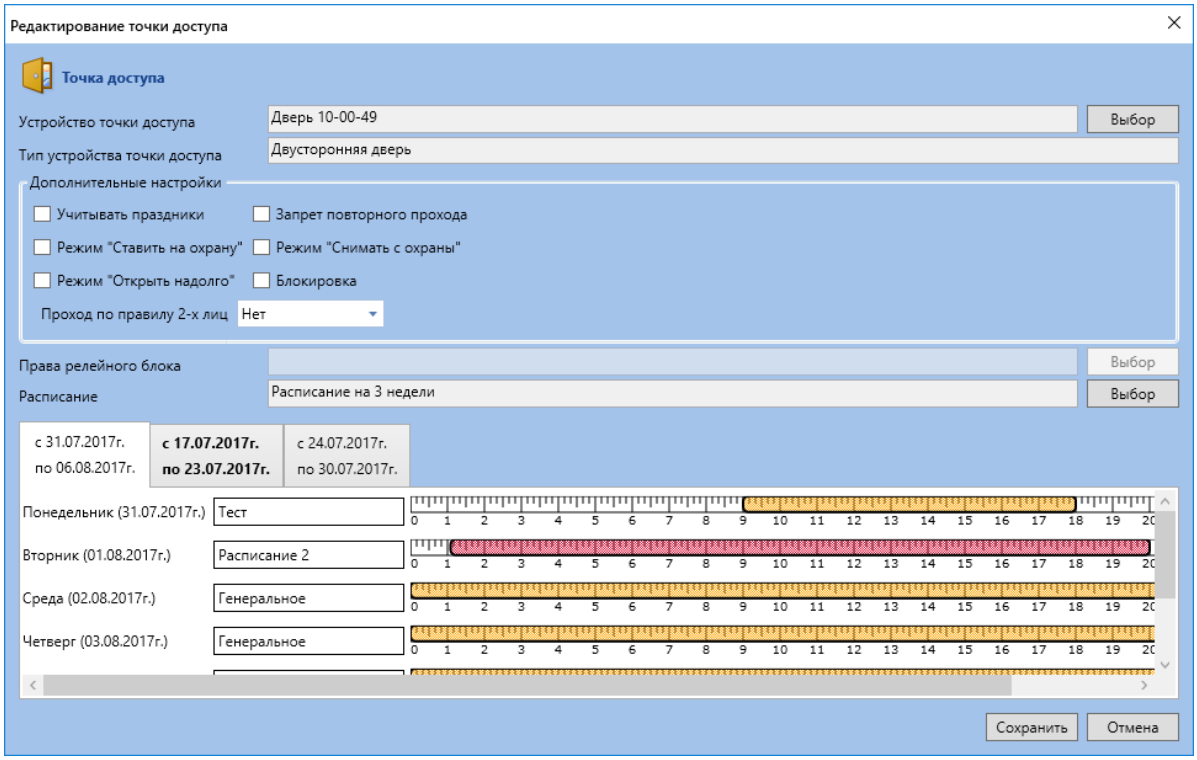


Рисунок 52 - АРМ RusGuard. Модуль Конфигурация СКУД. Редактирование параметров точки доступа

По умолчанию выбрано расписание, когда точка доступа доступна для прохода всегда, дополнительные настройки не применяются. Обратите внимание, что дополнительные настройки могут вводиться только после выбора расписания *пользовательского типа*.

3. Нажмите на кнопку Выбор напротив пункта ***Расписание***.

Загрузится список существующих в АРМ расписаний. Интерфейс этого окна позволяет не только выбрать одно из расписаний для привязки его к точке доступа, но и создать новое расписание любого типа.

4. Создайте или выберите расписание, нажмите на кнопку Выбрать.

Название выбранного расписание и шкала соответствующего интервала работы точки доступа отобразятся в окне ***Редактирование точки доступа***.

5. Если это необходимо, введите дополнительные настройки (используются при настройке режима повторного приложения ключа). Обратите внимание на правило ***Проход по правилу 2-х лиц***. Чтобы использовать правило, необходимо настроить хотя бы одно расписание с режимом прохода ***Сервис***. К нему привязывается настройка ***Первое лицо***, расписание привязывается к соответствующим карточкам сотрудников. Настройка ***Второе лицо*** привязывается к обычному расписанию, включающему интервал и точку доступа "сервисного", но пользователь с правами второго лица на точку доступа не сможет пройти на нее без первого лица.

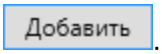
6. Нажмите на кнопку Сохранить, чтобы завершить процедуру.

Для того чтобы отредактировать уровень доступа (привязать к нему метки):

1. Откройте вкладку ***Настройки уровня доступа***.

2. В области ***Метки*** нажмите на пиктограмму  .

Загрузится общий список меток системы (кроме тех, которые были ранее привязаны к уровню доступа.)

3. Выберите нужную метку и нажмите на кнопку 

.

Добавленная метка отобразится в списке привязанных (см. рис. 53).

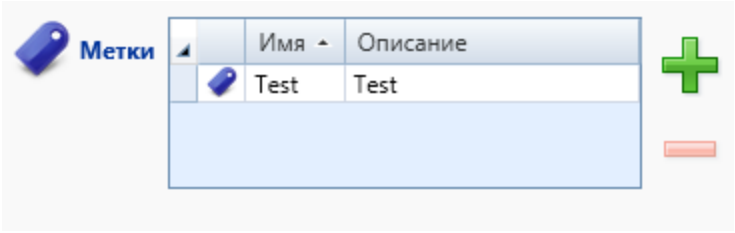


Рисунок 53 - АРМ RusGuard. Модуль Конфигурация СКУД
Привязка меток к уровню доступа

4. Сохраните изменения ().

Чтобы удалить метку из списка привязанных, выделите ее в списке и щелкните пиктограмму  .

Просмотр состояния точек доступа

В модуле Конфигурация СКУД АРМ RusGuard предусмотрена возможность мониторинга состояния точек доступа (см. рис. 54).

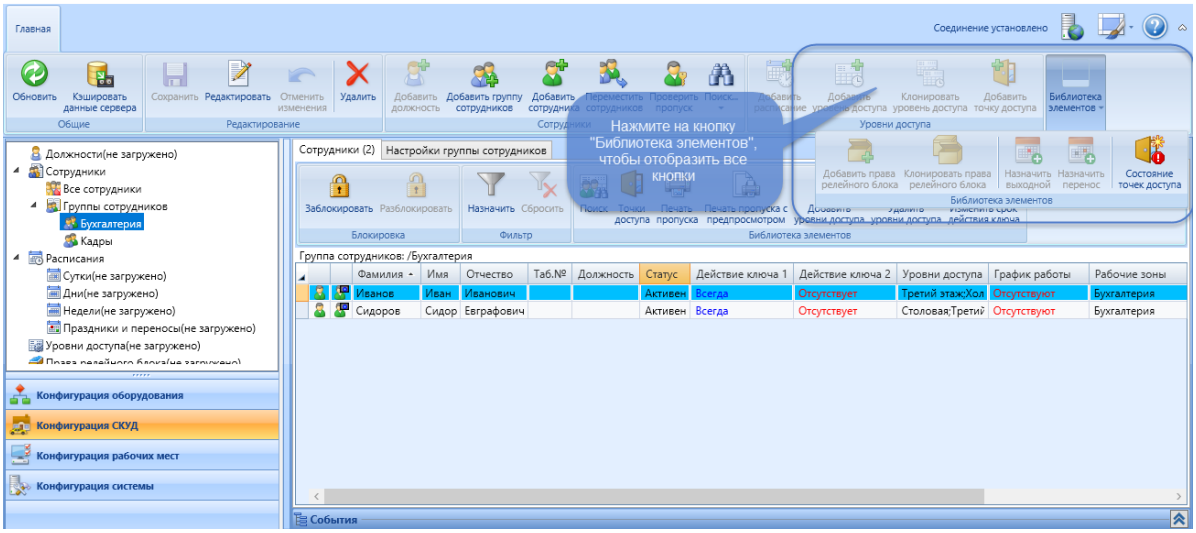


Рисунок 54 - АРМ RusGuard. Модуль "Конфигурация СКУД". Проверка состояния точек доступа

Для того чтобы просмотреть состояние точек доступа:

1. Нажмите на кнопку  ***Состояние точек доступа*** в панели управления модуля ***Конфигурация СКУД***.

Откроется окно ***Состояние точек доступа***.

В окне предусмотрен фильтр. По умолчанию, фильтр настроен на поиск настроенных точек доступа, в статусе которых есть какие-то ошибки. В случае отсутствия ошибок, окно отображается пустым, как на иллюстрации выше.

Если изменить настройки фильтра или если система выявляет ошибки в функционировании точки (точек) доступа, в окне выводится соответствующий список (см. рис. 55).

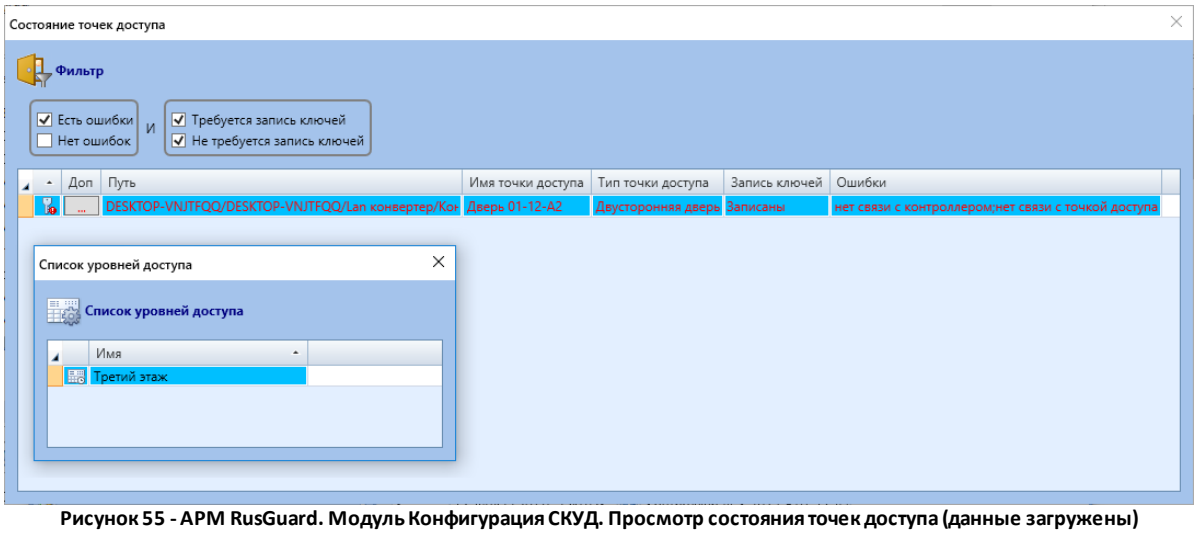


Рисунок 55 - АРМ RusGuard. Модуль Конфигурация СКУД. Просмотр состояния точек доступа (данные загружены)

В таблице приводится краткое описание параметров точки доступа, кнопка  (цвет кнопки зависит от статуса точки доступа) позволяет перейти к списку уровней доступа, привязанных к соответствующей точке доступа.

Модуль Конфигурация рабочих мест

В этом модуле создаются пользовательские рабочие места с набором модулей, которые требуются конкретному оператору АРМ для выполнения своих функций и решения задач.

Обратите внимание, что для выполнения различных функций разными группами пользователей могут создаваться разные рабочие места с одинаковым набором модулей.

По умолчанию в системе создано два рабочих места в группе "Системные рабочие места":

Администрирование, включает модули:

- Конфигурация оборудования
- Конфигурация СКУД
- Конфигурация рабочих мест
- Конфигурация системы

Планы и отчеты, включает модули:

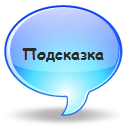
- Планы
- Отчеты

Удалить рабочие места из этой группы, а также саму группу невозможно. Если возможностей системных рабочих место достаточно, они могут использоваться для управления системой без создания дополнительных рабочих мест.

Модули Табло посетителей 255, Статистика 252 и Фотоидентификация 248 настраиваются дополнительно.

Также через этот модуль выполняется создание и настройка мобильных приложений 256.

Внимание: Оператор может использовать любое количество стационарных рабочих мест в АРМ, но, при настройке рабочих мест для работы с мобильными приложениями, к учетной записи пользователя должно быть привязано единственное рабочее место - мобильное.



Для рабочих мест предусмотрена функция автозапуска АРМ через ярлык на Рабочем столе. При ее использовании ввод пароля при каждом запуске не требуется. Подробнее см. здесь 260.

Создание пользовательских рабочих мест

Для того чтобы создать рабочее место:

1. Запустите АРМ RusGuard. Для создания рабочего места необходимо иметь доступ к модулю ***Конфигурация рабочих мест***.
2. Зайдите в модуль ***Конфигурация рабочих мест***.
3. В левой навигационной панели (см. рис. 56) раскройте верхний уровень списка и выберите в списке ***Рабочие места*** пункт ***Пользовательские***.

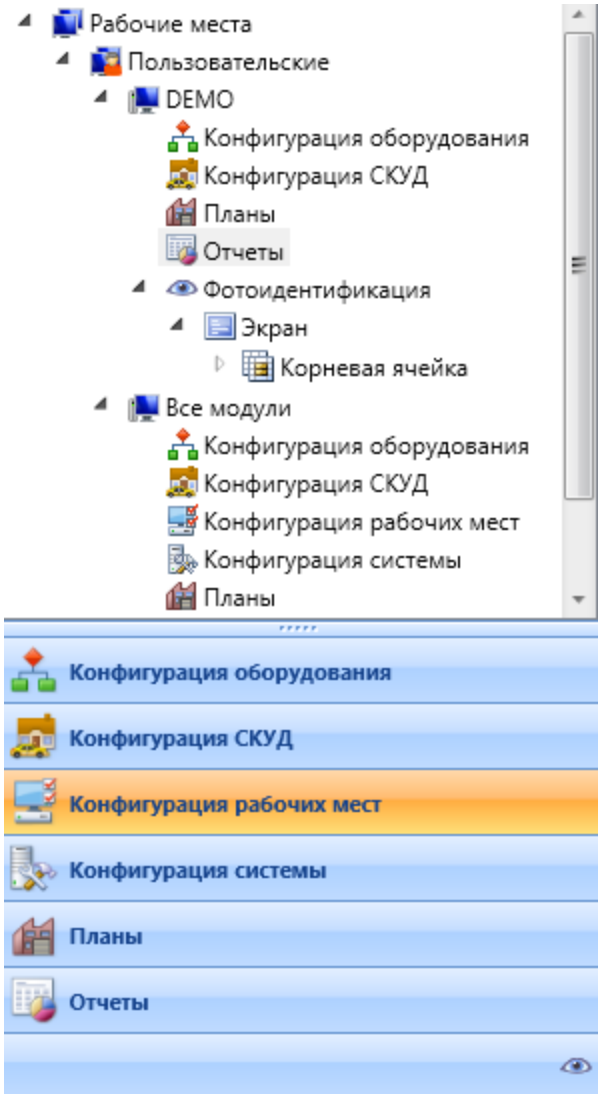


Рисунок 56 - АРМ RusGuard. Модуль Конфигурация рабочего места. Левая навигационная панель с раскрытым иерархическим списком

При этом в панели управления сверху активируется кнопка .

4. Нажмите на кнопку .

Откроется диалоговое окно.

5. Введите название создаваемого рабочего места (например, "Оператор", "Пользователь", "Планы и отчеты", "Test" и т.д.). Если необходимо, введите описание. Также в этом окне могут быть настроены некоторые параметры рабочего места. Эти параметры позднее будут доступны для редактирования (см. процедуру настройки параметров рабочего места 158).
6. Сохраните новое рабочее место.

Если рабочее место сохранено корректно, оно появится в списке настроенных рабочих мест, доступных данному пользователю, который отображается при запуске АРМ (см. рис.

57), а также в левой навигационной панели модуля ***Конфигурация рабочих мест*** внутри выбранной категории рабочих мест.

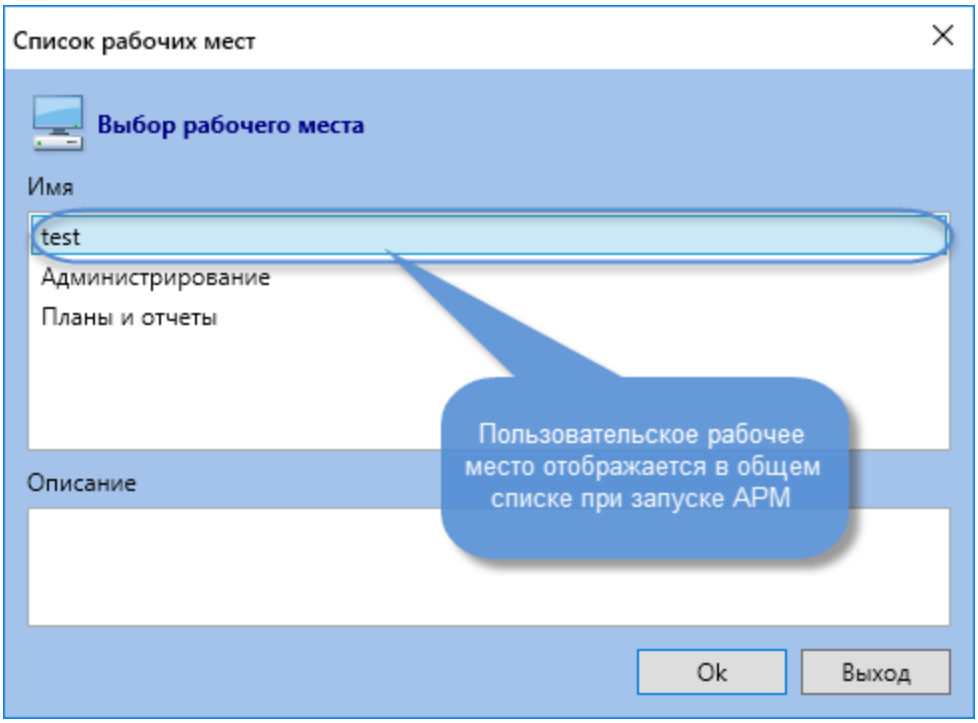


Рисунок 57 - АРМ RusGuard. Запуск. Выбор рабочего места.

7. Чтобы продолжить настройку рабочего места, зайдите в него через левую навигационную панель модуля.

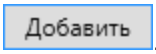
В главной панели управления активируется ряд кнопок.

8. Нажмите на кнопку  .

При этом раскроется меню с полным списком доступных системных модулей.

9. В зависимости от задач, выберите любой модуль.

Откроется диалоговое окно. Имя модуля уже введено по умолчанию. Вы можете ввести описание, если это необходимо.

10. Нажмите на кнопку 
.

Название модуля появится в списке в левой навигационной панели уровнем ниже созданного рабочего места.

Аналогично можно привязать к рабочему месту любое количество модулей.

Также вы можете изменить базовые настройки интерфейса и параметры функционирования рабочего места.

Для того чтобы настроить параметры рабочего места:

1. Зайдите в рабочее место (установите курсор мыши на его названии в навигационной панели).

В главном экране отобразятся вкладки для настройки параметров рабочего места. По умолчанию открывается вкладка ***Настройки*** (см. рис. 58).

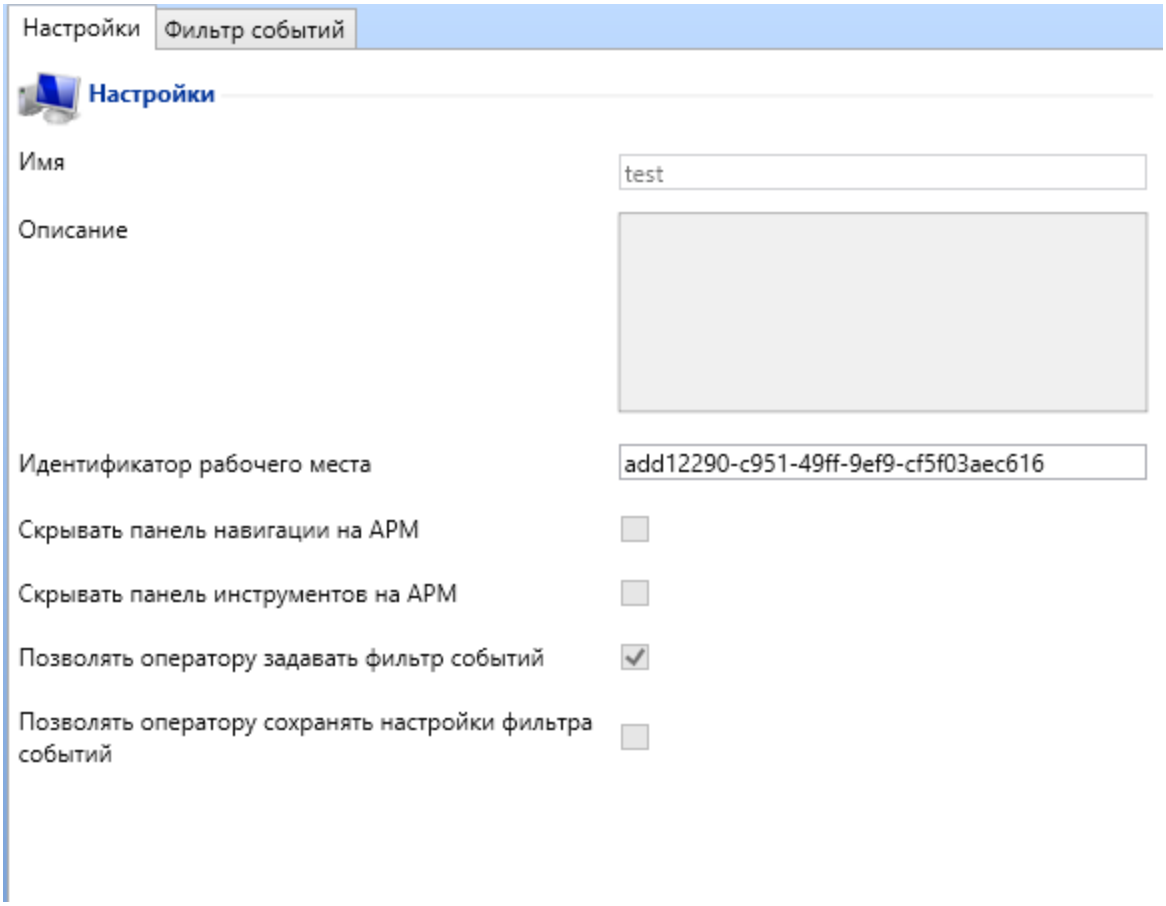


Рисунок 58 - АРМ RusGuard. Основные параметры рабочего места

2. Нажмите на кнопку  ***Редактировать***.
3. Внесите необходимые изменения. В частности, вы можете указать:
   - Скрывать ли панель навигации в АРМ при использовании рабочего места;
   - Скрывать ли панель инструментов в АРМ;
   - Разрешать ли оператору использовать фильтр событий самостоятельно (по умолчанию, флаг установлен);

Здесь также отображается идентификатор рабочего места, необходимый для настройки автозапуска 260.

4. Нажмите на кнопку  ***Сохранить***, чтобы применить настройки.
5. Перейдите на вкладку ***Фильтр событий***, чтобы настроить фильтр событий для рабочего места. То есть, вы можете указать, какие события (типы событий) от каких устройств отображаются для оператора редактируемого рабочего места (см. рис. 59). По умолчанию, установлены все флаги (т.е. все события ото всех подключенных устройств отображаются).

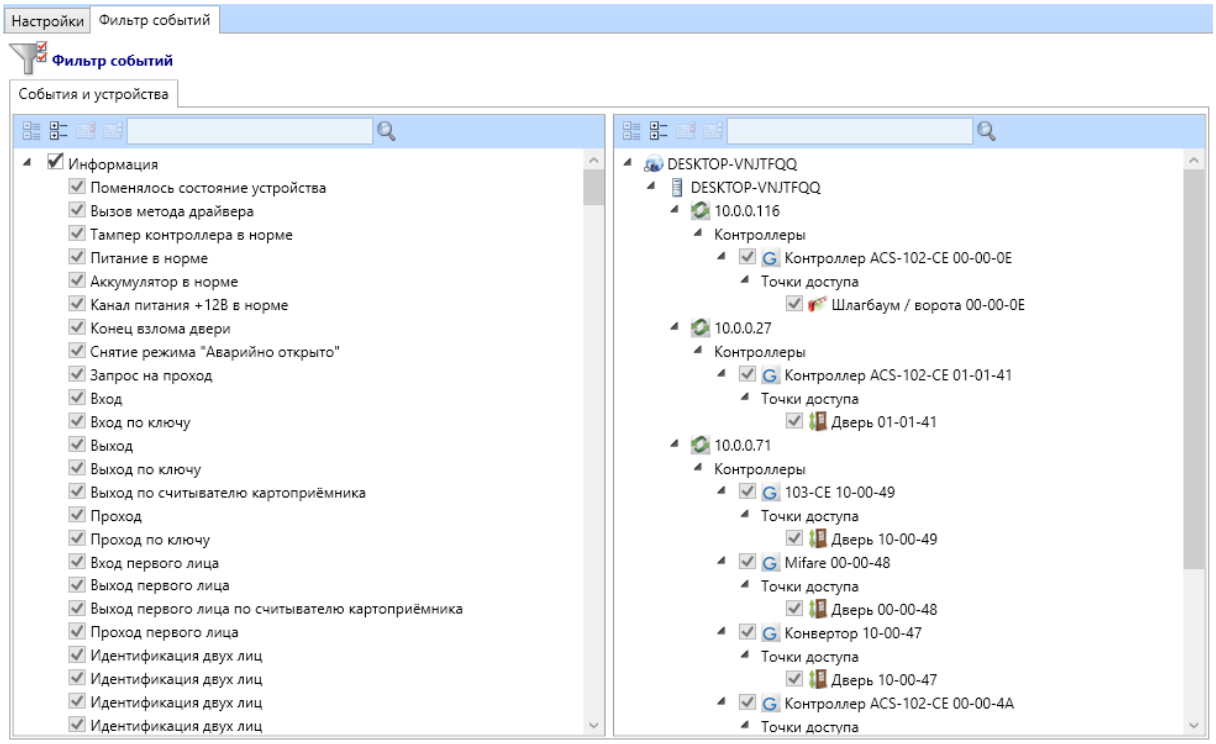


Рисунок 59 - АРМ RusGuard. Настройка фильтра событий

6. Установите желаемые настройки фильтрации, сохраните изменения ( ).

Настройка модуля Планы

Модуль ***Планы*** предназначен для создания визуальных планов-схем объектов с указанием на них точек размещения оборудования СКУД, камер и других элементов системы.

Для того чтобы настроить модуль Планы:

1. Добавьте модуль ***Планы*** к одному из рабочих мест.
2. Используя иерархический список в навигационной панели слева, зайдите в созданный модуль.
3. Нажмите на кнопку в панели инструментов.

Откроется окно ввода плана (см. рис. 60).

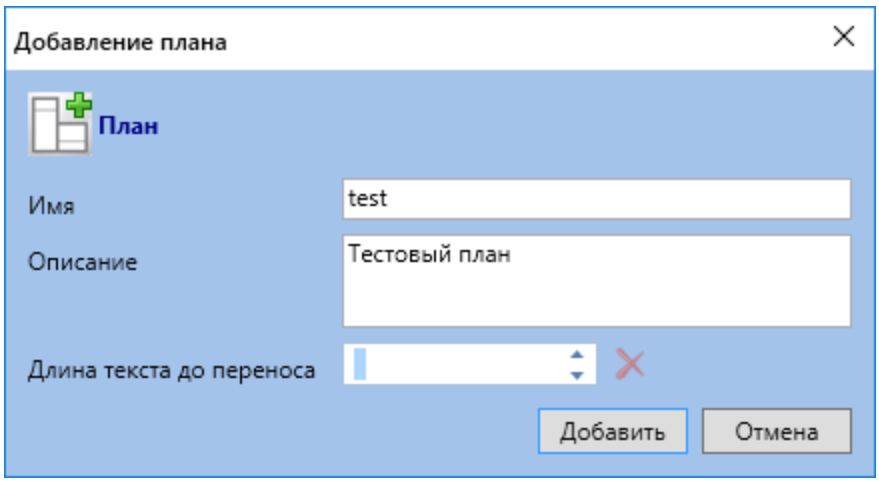
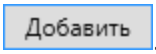


Рисунок 60 - APM RusGuard. Создание нового плана

4. Введите название плана (обязательно) и описание (если необходимо).

5. Нажмите на кнопку 

.

Внутри модуля ***Планы*** в иерархическом списке в левой навигационной панели появится новая строка для созданного плана (см. рис. 61).

Примечание: АРМ позволяет создавать любое количество планов в модуле, а также создавать иерархию планов с неограниченным количеством уровней вложенности.

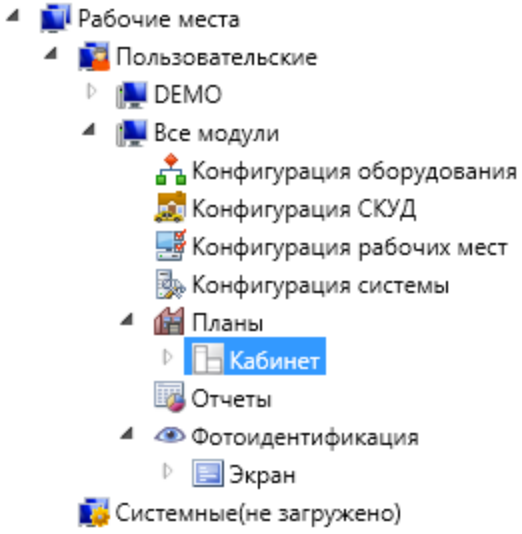


Рисунок 61. APM RusGuard. Создан новый план

6. Зайдите в новый план и нажмите на кнопку  ***Редактировать***.

В правой части экрана загрузится список настроенных в СКУД устройств, в панели управления активируются дополнительные кнопки.

7. Чтобы загрузить план объекта, нажмите на кнопку  .

Система предложит загрузить графический файл через стандартный диалог загрузки файла ОС Windows.

8. Выполните загрузку изображения.
9. Отметьте на плане точки размещения элементов системы (точек доступа, оборудования). Для этого перетаскивайте мышью пиктограммы нужных элементов или устройств из списка справа на схему (см. рис. 62). При установке пиктограммы ("драйвера") пользователь имеет возможность ввести его название (по умолчанию используется название точки доступа), а также выбрать, отображать ли название на схеме.

Рисунок 62 - АРМ RusGuard. Размещение пиктограм ("драйверов") устройств на плане

11. Разместив все нужные драйверы, сохраните план ( ).

План загружается в БД и может использоваться оператором модуля ***Планы*** через АРМ. Используя настроенные драйверы, оператор может выполнять мониторинг состояния устройств и управлять ими. Обратите внимание, что на план можно наносить и драйверы устройств сторонних систем (камер Ivideon).

Статусы планов в АРМ

Графический знак плана в АРМ может меняться в зависимости от статуса объекта (см. табл. 8).

Таблица 7 - Статусы планов	
Пиктограмма	Значение
	План заведен в системе и функционирует нормально

Таблица 7 - Статусы планов	
	Возникла ошибка в системе и/или чрезвычайная ситуация на одной из привязанных к плану точек доступ
	План удален

Настройка модуля Фотоидентификация

В модуле ***Конфигурация рабочих мест*** выполняются первоначальные настройки модуля ***Фотоидентификация***.

Для того чтобы настроить модуль Фотоидентификация:

1. Добавьте модуль ***Фотоидентификация*** к одному из рабочих мест.
2. Используя иерархический список в навигационной панели слева, зайдите в созданный модуль, где заданы первоначальные настройки (см. рис. 63).

Рисунок 63 - APM RusGuard. Настройки модуля Фотоидентификация по умолчанию

3. Зайдите в пункт ***Экран*** и задайте настройки отображения модуля (см. рис. 64).

   Нажмите на кнопку  в верхней навигационной панели, чтобы отредактировать параметры. Вы можете:

   - Изменить имя экрана модуля;
   - Выбрать, следует ли отображать имя в модуле;
   - Выбрать, отображать ли сетку в модуле (деление экрана на ячейки);
   - Отрегулировать формат и масштаб экрана в АРМ.

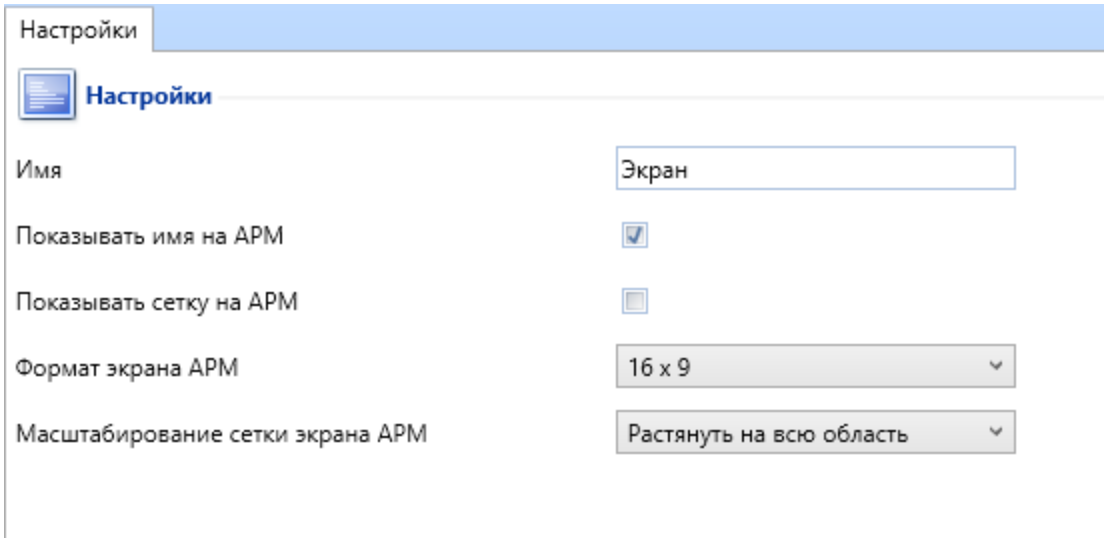


Рисунок 64 - АРМ RusGuard. Настройки модуля Фотоидентификация. Настройка вида экрана в модуле

4. Перейдите в уровень ***Корневая ячейка***. Нажмите на кнопку  в верхней навигационной панели.

Активируется кнопка  ***Редактировать ячейку экрана*** в верхней панели инструментов.

5. Нажмите на эту кнопку и, используя раскрывшуюся сетку, установите количество ячеек для экрана (см. рис. 65).

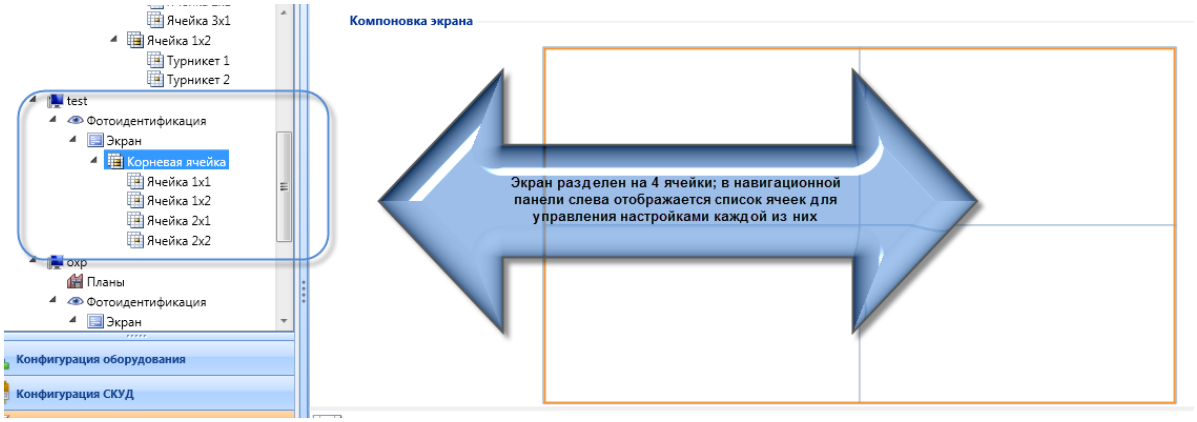


Рисунок 65 - АРМ RusGuard. Настройки модуля Фотоидентификация. Создание ячеек экрана

6. Для настройки параметров определенной ячейки, перейдите в нее через левую навигационную панель (иерархический список, на уровень ниже ***Корневой ячейки***). Либо выделите ее щелчком мыши непосредственно в центральном экране. Нажмите на кнопку  .

Внизу экрана появится область ***Настройки ячейки*** (см. рис. 66).

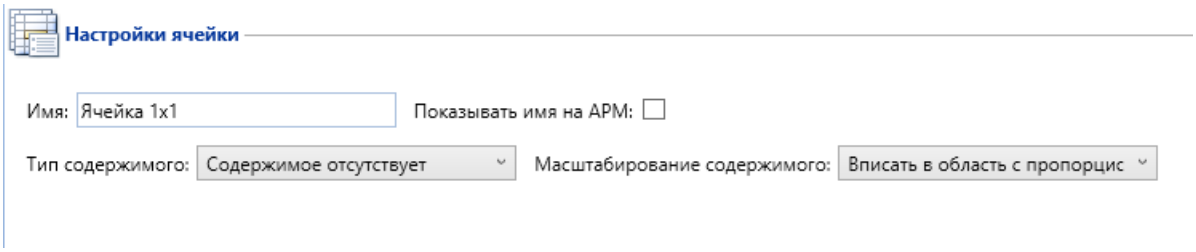


Рисунок 66 - APM RusGuard. Настройки модуля Фотоидентификация. Область настройки параметров ячейки. Вид по умолчанию

7. Если это необходимо, введите имя ячейки в поле ***Имя***.
8. Укажите тип содержимого (список ***Тип содержимого***). Система позволяет выводить в ячейке фото сотрудника, проходящего через точку доступа, либо изображение с камеры.

При выборе типа содержимого на экране отобразятся дополнительные элементы интерфейса, необходимые для его настройки.

9. Если выбран тип содержимого ***Камера*** выполните настройку камеры следующим образом:

   i. Нажмите на кнопку Выбор напротив поля ***Камера***.

   Отобразится список настроенных камер Ivideon.

   ii. Выберите камеру из списка (щелкните мышью по строке с названием нужной камеры).

   Название камеры отобразится в поле ***Камера***.

   iii. Чтобы завершить настройку, нажмите на кнопку  в главной панели инструментов сверху.

10. Если выбран тип содержимого ***Фотоидентификация***, выполните настройку идентификации следующим образом:

    i. Выберите точку доступа, данные о проходе через которую будут выводиться в ячейке. Для этого нажмите на кнопку Выбор напротив поля ***Имя*** в области ***Точка доступа*** (см. рис. 67).

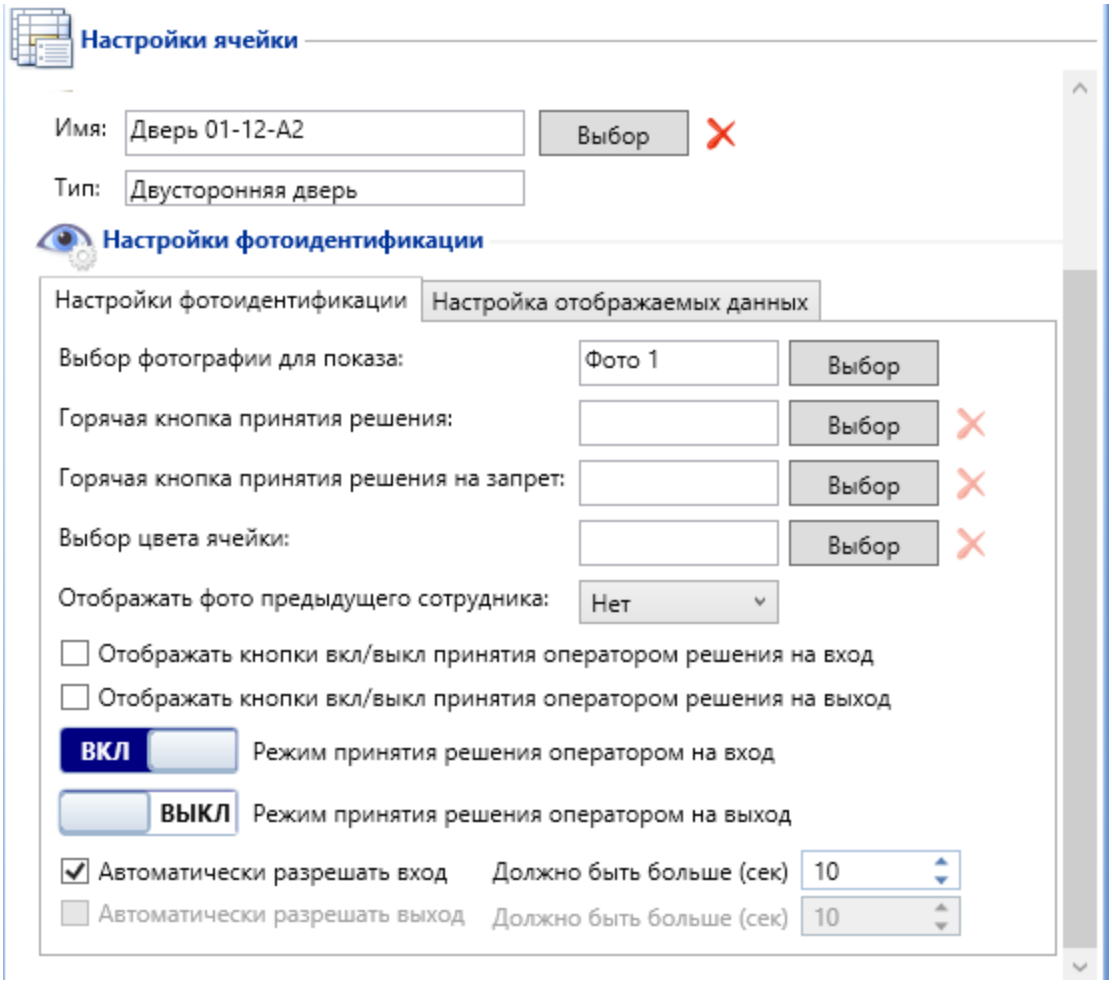
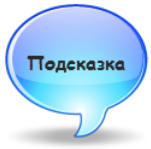


Рисунок 67 - АРМ RusGuard. Настройки модуля Фотоидентификация. Область настройки параметров ячейки. Тип содержимого: Фотоидентификация



Вы можете свернуть/развернуть содержимое нижней части экрана, перемещая мышью разделительную черту в середине.

Загрузится список доступных точек доступа.

ii. Выберите нужную точку доступа в списке (кнопка Выбор либо двойной щелчок мышью в строке с названием нужной точки доступа).

Данные о выбранной точке доступа (имя и тип) загрузятся на экран (см. рис. выше).

iii. По умолчанию к карточке сотрудника может быть привязано три фото (это число может быть изменено). Чтобы выбрать, какую из фотографий отображать при прохождении сотрудника через указанную точку доступа, нажмите на кнопку Выбор напротив поля ***Выбор фотографии для показа***.

Загрузится перечень фотографий, настроенный в АРМ.

iv. Выберите нужную фотографию ("позицию") списке (кнопка Назначить либо двойной щелчок мышью в строке с названием нужной точки доступа).

Название выбранной фотографии загрузится в поле ***Выбор фотографии для показа***.

v. Вы также можете назначить горячие клавиши принятия решения на разрешение и/или запрет прохода. Для этого нажмите на кнопку Выбор возле поля ***Горячая кнопка принятия решения*** и/или ***Горячая кнопка принятия решения на запрет***. Введите сочетание клавиш в открывшемся окне (см. рис. 68). Нажмите на кнопку Назначить.

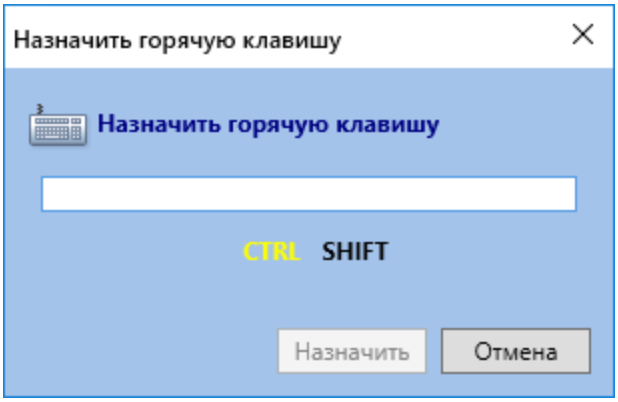


Рисунок 68 - АРМ RusGuard. Настройки модуля Фотоидентификация. Область настройки параметров ячейки. Тип содержимого: Фотоидентификация. Настройка горячих клавиш

Назначенное сочетание клавиш отобразится в поле.

vi. Поле ***Выбор цвета ячейки*** позволяет настроить выделение фотографии проходящего сотрудника цветом. Для того, чтобы использовать поле, необходимо предварительно настроить дополнительное поле сотрудника 313 типа "цвет" в модуле "Конфигурация системы" (если поле создано, вы можете настроить разные цвета для каждого сотрудника на вкладке ***Добавочные поля*** карточки). После этого созданное поле станет доступно в списке, загружаемом при щелчке по кнопке Выбор возле названия поля.

vii. По умолчанию режим принятия решения оператором отключен и на вход, и на выход. Чтобы включить его щелкните мышью по кнопке ***ВКЛ/ВЫКЛ*** возле поля ***Режим принятия решения оператором на вход*** и/или ***Режим принятия решения оператором на выход***.

Внимание: Для корректной работы функции необходимо также выполнить настройку информирования оператора о входе и/или выходе в модуле Конфигурация оборудования (настройка точки доступа) (см. рис. 69).

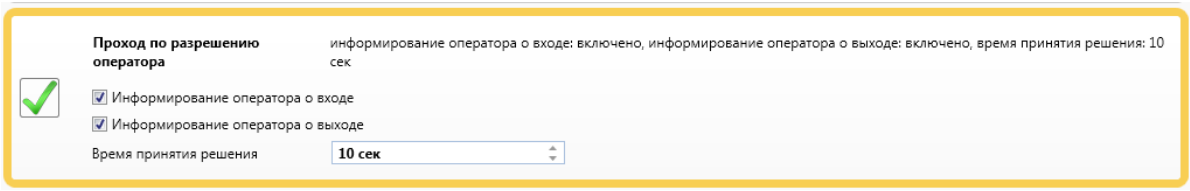


Рисунок 69 - АРМ RusGuard. Настройки модуля Фотоидентификация. Модуль Конфигурация оборудования. Вкладка точки доступа (в данном примере тип "Дверь"). Настройка уведомления оператора о проходе

viii. Чтобы в модуле ***Фотоидентификация*** отображались кнопки включения/отключения режима принятия решения на вход/выход оператором, установите соответствующие флаги (либо один из них, если такова конфигурация системы). Если эти кнопки отображаются, оператор модуля имеет возможность самостоятельно отключать/включать функцию принятия решения. В противном случае, либо постоянно используется автоматический режим, либо принятие решения оператором.

ix. Если необходимо, отфильтруйте отображаемые при проходе данные. Для этого перейдите на вкладку ***Настройка отображаемых данных*** (см. рис. 70). По умолчанию отображаются ФИО, должность сотрудника и группа. Вы можете как добавить ( )дополнительные поля для отображения вместе с фото, так и удалить все ( ), чтобы не отображать личные данные при приходе. Порядок отображения также регулируется стрелками.

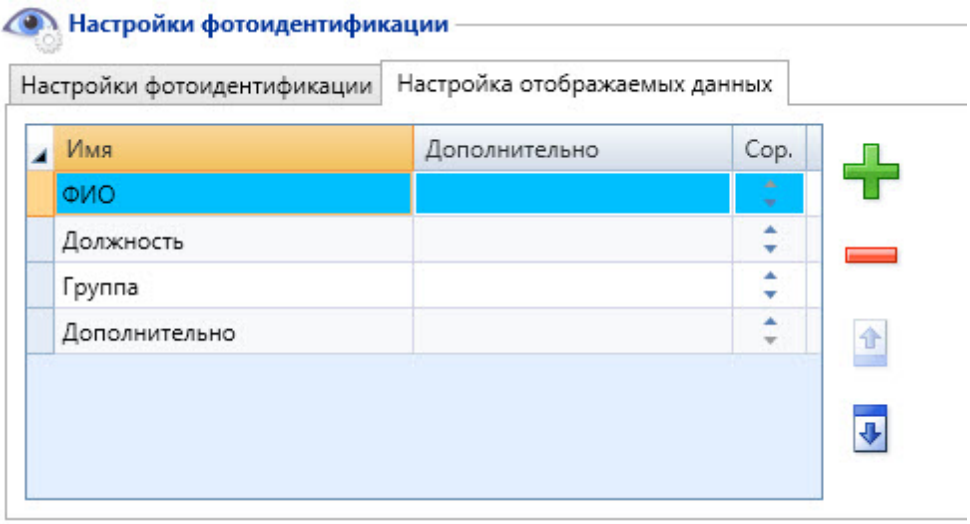


Рисунок 70 - АРМ RusGuard. Модуль Фотоидентификация. Флаг "Скрыть личные данные"

x. Чтобы завершить настройку, нажмите на кнопку в главной панели инструментов сверху.

Настройка режима распознавания документов для модуля Конфигурация СКУД

Используя модуль ***Конфигурация рабочих мест*** (см. рис. 71), пользователь АРМ может настроить использование распознанных 143 данных из документов сотрудника (вкладка ***Документы*** карточки сотрудника) на вкладке ***Личные данные*** карточки. В частности:

- Использовать ФИО из поддерживаемого документа (паспорта, водительского удостоверения или заграничного паспорта) для заполнения полей ***Фамилия***, ***Имя***, ***Отчество*** на вкладке ***Личные данные***.
- Использовать одну или несколько фотографий из документов пользователя на вкладке ***Личные данные***.

См. также раздел Управление данными системы RusGuard 313 и раздел ABBYY PassportReader SDK 390.

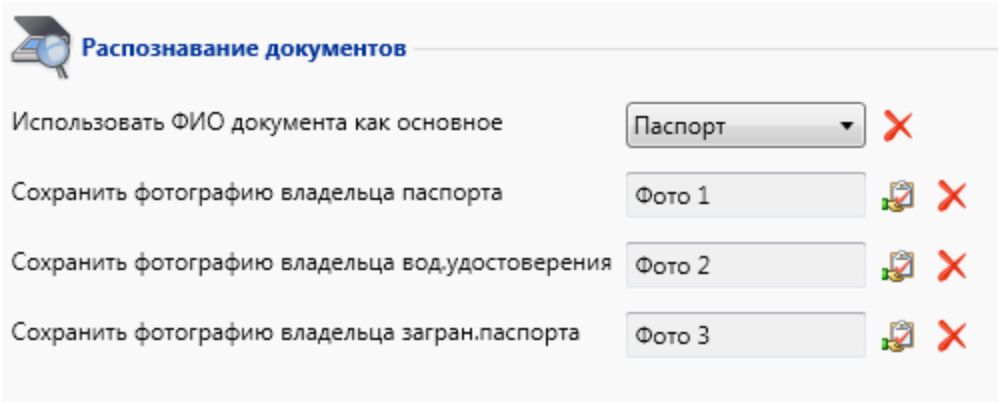


Рисунок 71 - АРМ RusGuard. Настройки модуля Конфигурация СКУД. Режим распознавания документов

Настройка мобильных приложений

Терминалы

Для того чтобы настроить мобильный терминал:

1. Перейдите в раздел ***Мобильные терминалы*** в левой навигационной панели модуля.
2. Нажмите на кнопку . Откроется диалоговое окно для ввода параметров рабочего места мобильного терминала (см. рис. 72).
3. Заполните параметры по аналогии с обычными рабочими местами АРМ. Сохраните данные (кнопка ***Добавить***). Созданный терминал отобразится на левой навигационной панели, в иерархическом списке.

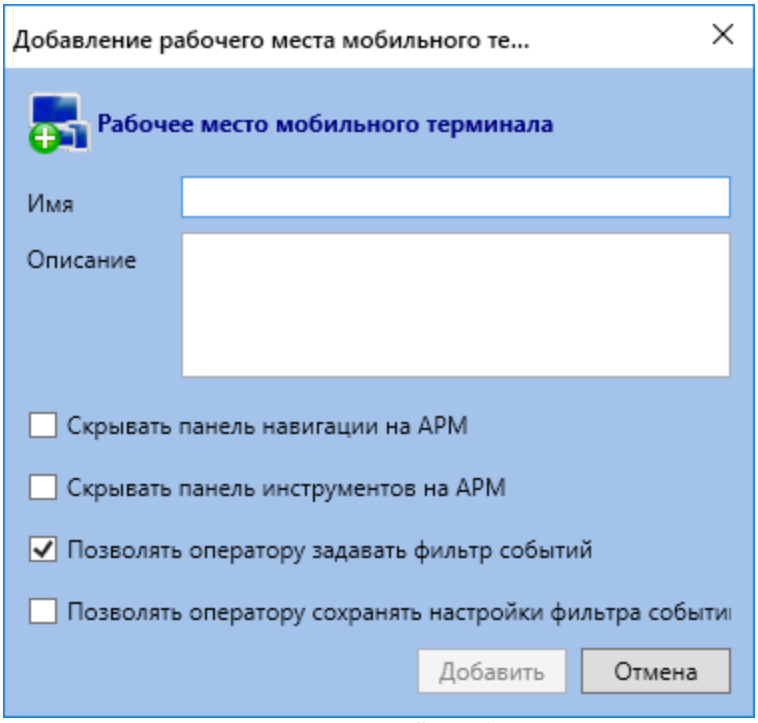


Рисунок 72 - АРМ RusGuard. Настройка мобильного терминала

4. Установите курсор на строке с названием созданного терминала. Активируется меню ***Добавить модуль***  .
5. Раскройте меню и выберите вариант ***Удаленный терминал***. Откроется диалог для создания записи терминала. Заполните поля, сохраните данные. Название нового терминала отобразится в иерархии слева.

ПО RusGuard позволяет создавать мобильные приложения (модули) нескольких типов для разных задач и аудиторий пользователей. Обратите внимание, что в каждом РМ может быть только по одному модулю (приложению) каждого типа. Если необходимо создать больше приложений с разными настройками, создайте несколько мобильных терминалов.

6. Установите курсор мыши на названии нового удаленного терминала в левой панели.
7. Нажмите на кнопку  верхней панели управления. Основной экран станет доступен для редактирования.

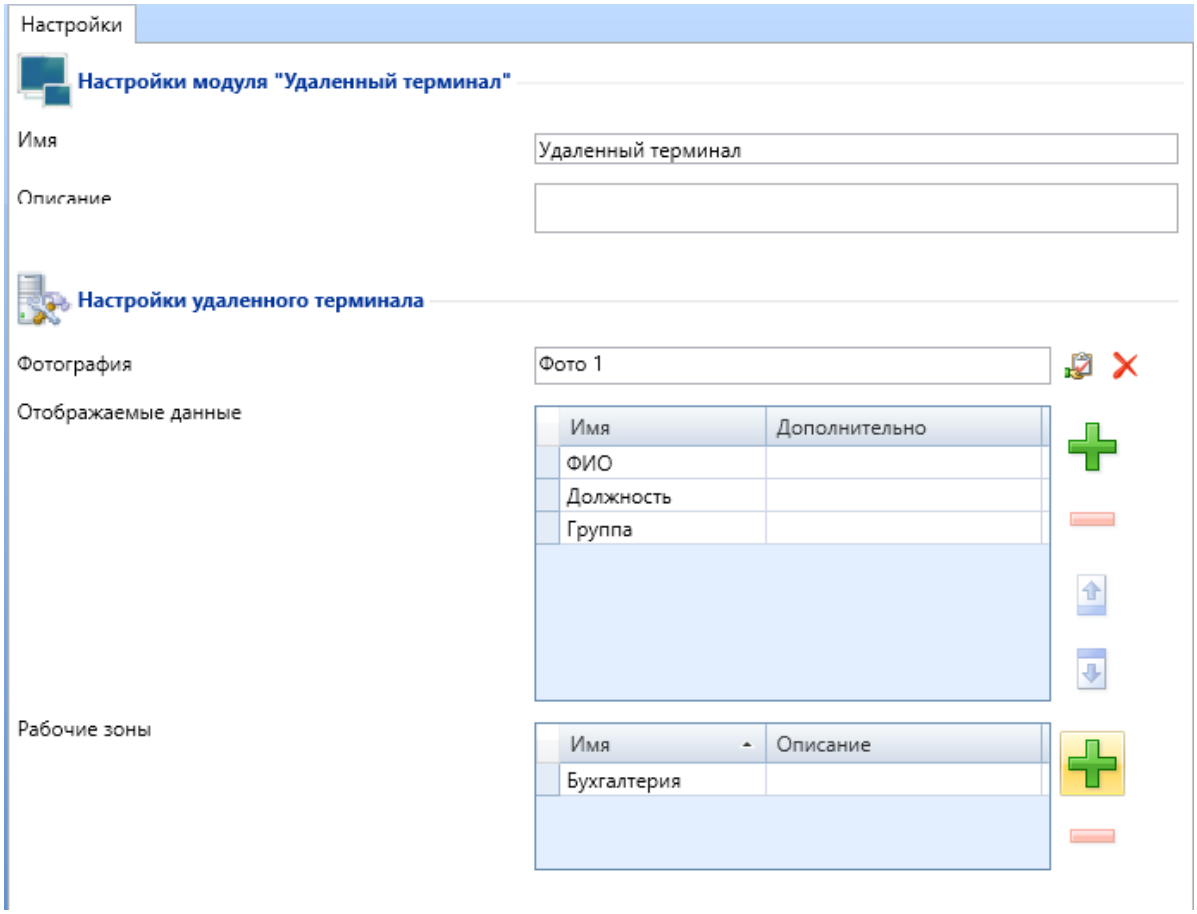


Рисунок 73 - APM RusGuard. Настройка параметров удаленного терминала

8. Используя пиктограммы  и  , выберите, какие поля из карточки сотрудника должны обрабатываться удаленным терминалом. Выберите рабочие зоны (необходимо настроить рабочие зоны, выполнить привязку к ним точек и уровней доступа). Для корректной работы приложения необходимо выбрать хотя бы одно фото и рабочую зону.

9. Щелкните пиктограмму  в верхней панели управления.

Модуль ***Администратор*** добавляется аналогичным образом, при этом никакие дополнительные настройки не требуются.

Модуль Конфигурация системы

Модуль предназначен для создания системных сущностей и управления ими:

- учетными записями сотрудников и пользователей;
- параметрами расписания (типы дней, графики работы, рабочие зоны);
- профилями карт Mifare
- и пр.

Также в модуле настраиваются реакции (то, как обрабатываются системные события), метки (дополнительный способ разграничения прав доступа), ряд дополнительных элементов, используемых при настройке СКУД.

Ведение базы данных пользователей

Создание группы пользователей

Для того чтобы создать группу пользователей:

1. Запустите АРМ RusGuard.

Для работы с базой данных пользователей АРМ необходимо иметь доступ к модулю ***Конфигурация системы***.

2. Зайдите в модуль ***Конфигурация системы***.
3. Раскройте иерархический список в левой навигационной панели и зайдите в пункт ***Группы*** (см. рис. 73).

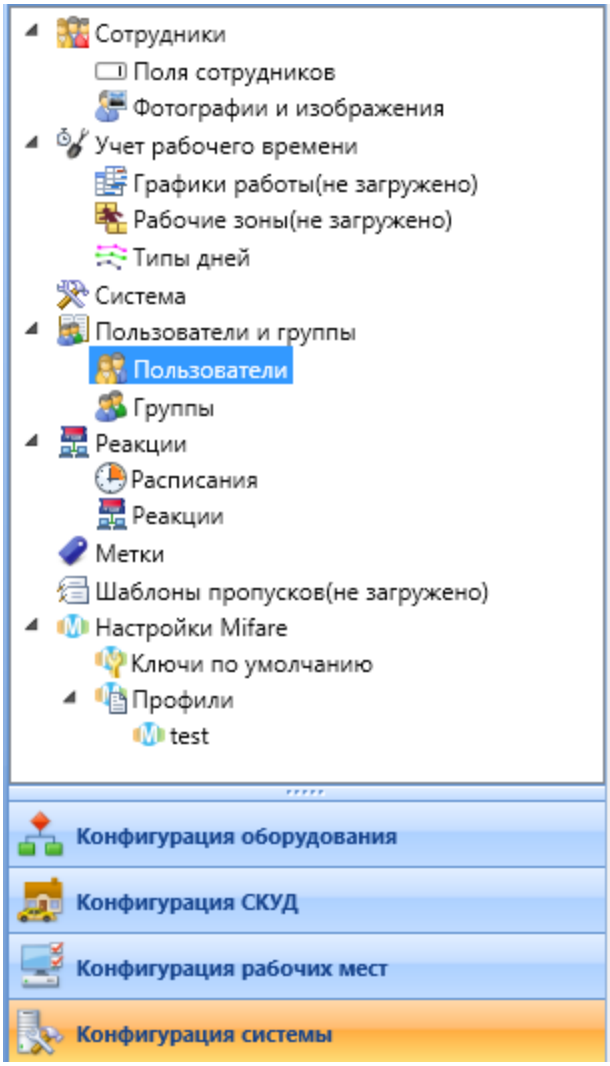


Рисунок 74 - АРМ RusGuard. Модуль Конфигурация системы. Левая навигационная панель с раскрытым иерархическим списком

По умолчанию в системе существует встроенная группа "Администраторы", где создана учетная запись пользователя "Admin" (учетная запись администратора системы). Удалить группу "Администраторы" невозможно, но в нее могут быть добавлены новые пользователи. Пользователи группы Администраторы всегда имеют доступ ко ВСЕМ АРМ, создаваемым в системе.

Удалить встроенную учетную запись администратора системы ("Admin") также невозможно, но можно изменить логин (по умолчанию "Admin") и пароль (по умолчанию отсутствует).

4. Нажмите на кнопку  ***Добавить группу***, которая активируется в панели инструментов сверху.

Откроется окно для ввода данных о группе (см. рис. 74). Тип уже задан согласно выбору пользователя в шаге 4.

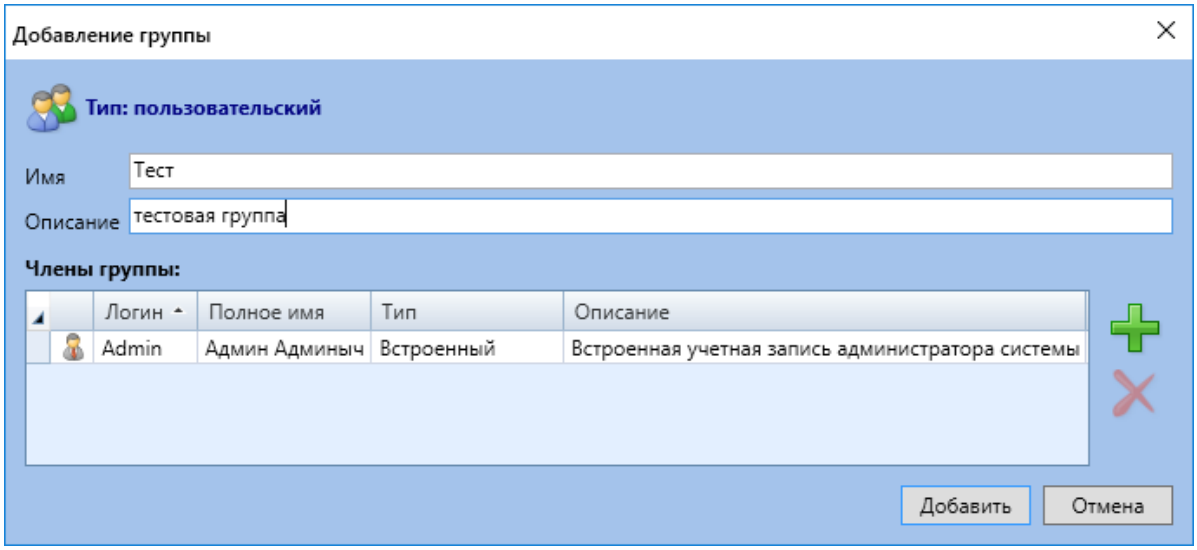


Рисунок 75 - АРМ RusGuard. Модуль Конфигурация системы. Окно ввода данных о группе

5. Введите название группы в поле ***Имя*** (обязательно). При необходимости добавьте описание. После ввода названия активируется кнопка Добавить. Нажмите на нее, чтобы создать пустую группу и закончить процедуру, или, не закрывая окна, добавьте в группу пользователей.

6. Чтобы добавить в группу пользователей, нажмите на кнопку  .

Откроется список учетных записей пользователей.

7. Выберите нужную учетную запись и добавьте ее в группу. В группе может быть любое количество пользователей. Как только к группе привязан хотя бы один пользователь, активируется кнопка  для удаления пользователя из группы.

8. Добавив желаемое количество пользователей, нажмите на кнопку Добавить, чтобы закончить процедуру.

Название новой группы пользователей появится в иерархическом списке в левой навигационной панели.

Для того чтобы отредактировать полномочия группы пользовательского типа:

1. Запустите АРМ RusGuard.

Для работы с базой данных пользователей АРМ необходимо иметь доступ к модулю ***Конфигурация системы***.

2. Зайдите в модуль ***Конфигурация системы***.
3. Раскройте иерархический список в левой навигационной панели и зайдите в пункт ***Группы***. Выберите нужную группу пользовательского типа.

4. Перейдите в центральный экран. Нажмите на кнопку ***Редактировать*** в нижней части экрана (область ***Полномочия***). Эта кнопка активна только для групп пользовательского типа.

По умолчанию активируется список рабочих мест (первая закладка слева). В списке приведены все настроенные в АРМ рабочие места. Флажками отмечены те, которые доступны группе в настоящее время (см. рис. 75).

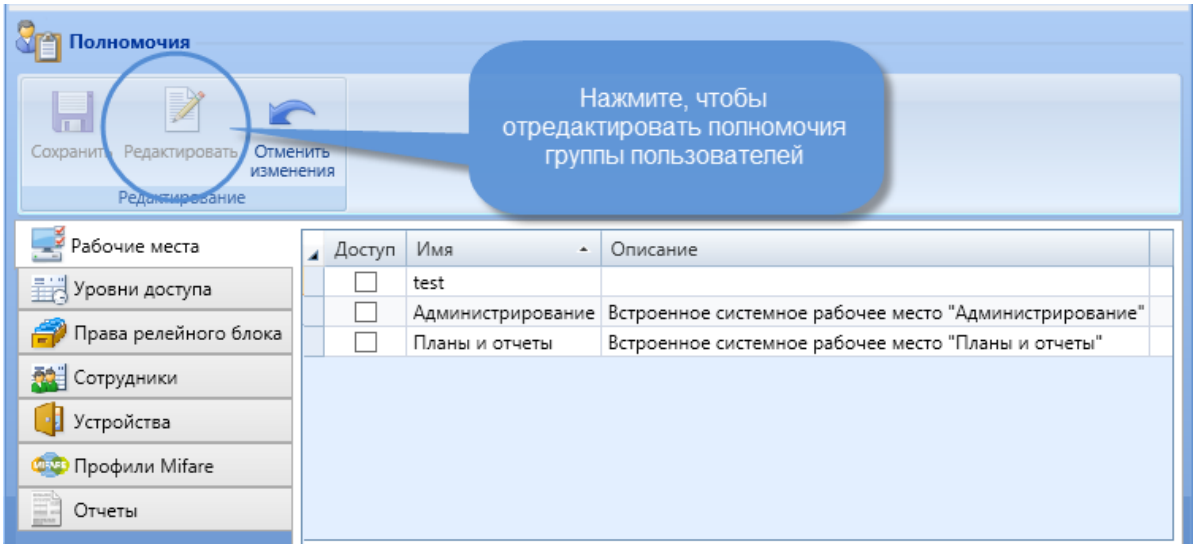


Рисунок 76 - АРМ RusGuard. Модуль Конфигурация системы. Полномочия группы пользователей (рабочие места)

5. Отредактируйте настройки, снимая/устанавливая флажки напротив названий рабочих мест, доступ группы к которым следует ограничить/добавить.

6. Сохраните настройки ( ).

7. Перейдите на закладку ***Уровни доступа*** (см. рис. 76).

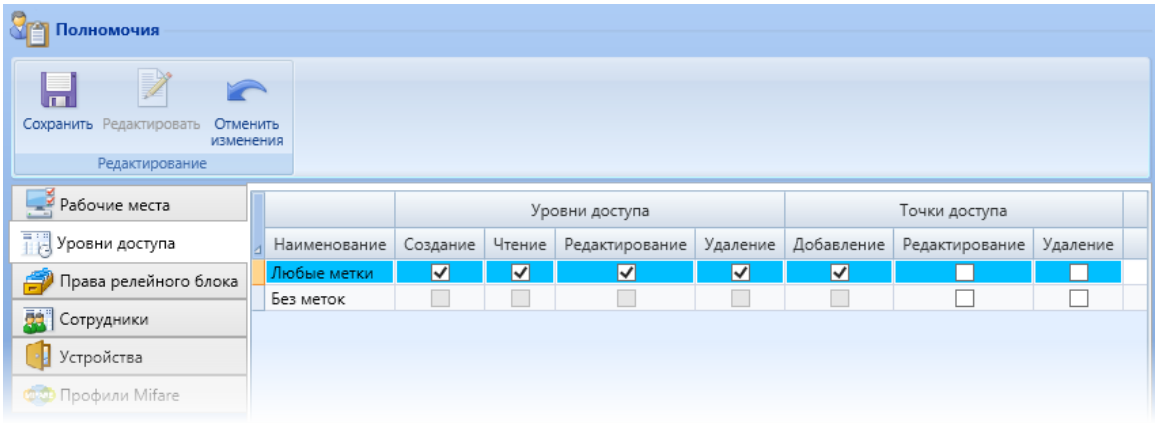


Рисунок 77 - АРМ RusGuard. Модуль Конфигурация системы. Полномочия группы пользователей (уровни доступа)

8. Нажмите на кнопку ***Редактировать*** в нижней части экрана (область ***Полномочия***).

9. Используя флаги, настройте доступ группы сотрудников к уровням доступа и точкам доступа. Доступ настраивается:
   i. с точки зрения применения меток (операция доступна либо для уровней и точек доступа со всеми метками, не имеющих меток, имеющих определенную метку 206 (метки);
   ii. с точки зрения доступных операций (члены группы могут создавать, просматривать, редактировать, и/или удалять уровень/точку доступа).
10. Сохраните настройки ().
11. Перейдите на закладку ***Сотрудники*** и выполните настройки доступа к управлению группами сотрудников и учетными записями сотрудников по аналогии с шагами 7-10.
12. Перейдите на закладку ***Устройства*** и выполните настройки доступа к информации об устройствах для членов группы по аналогии с шагами 7-10 (доступна только операция "Чтение", т.е. просмотр данных).
13. Перейдите на закладку ***Профили Mifare*** и выполните настройки доступа к управлению профилями Mifare 210 для членов группы по аналогии с шагами 7-10.
14. Перейдите на закладку ***Отчеты*** и выполните настройки доступа к управлению отчетами 214 для членов группы по аналогии с шагами 7-10.

Создание учетной записи пользователя

Для того чтобы создать учетную запись пользователя АРМ:

1. Запустите АРМ RusGuard.

Для работы с базой данных пользователей АРМ необходимо иметь доступ к модулю ***Конфигурация системы***.

2. Зайдите в модуль ***Конфигурация системы***.
3. Раскройте иерархический список в левой навигационной панели и зайдите в пункт ***Пользователи***.
4. Нажмите на кнопку  ***Добавить пользователя*** в верхней навигационной панели.

Откроется окно для ввода учетных данных пользователя (см. рис. 77).

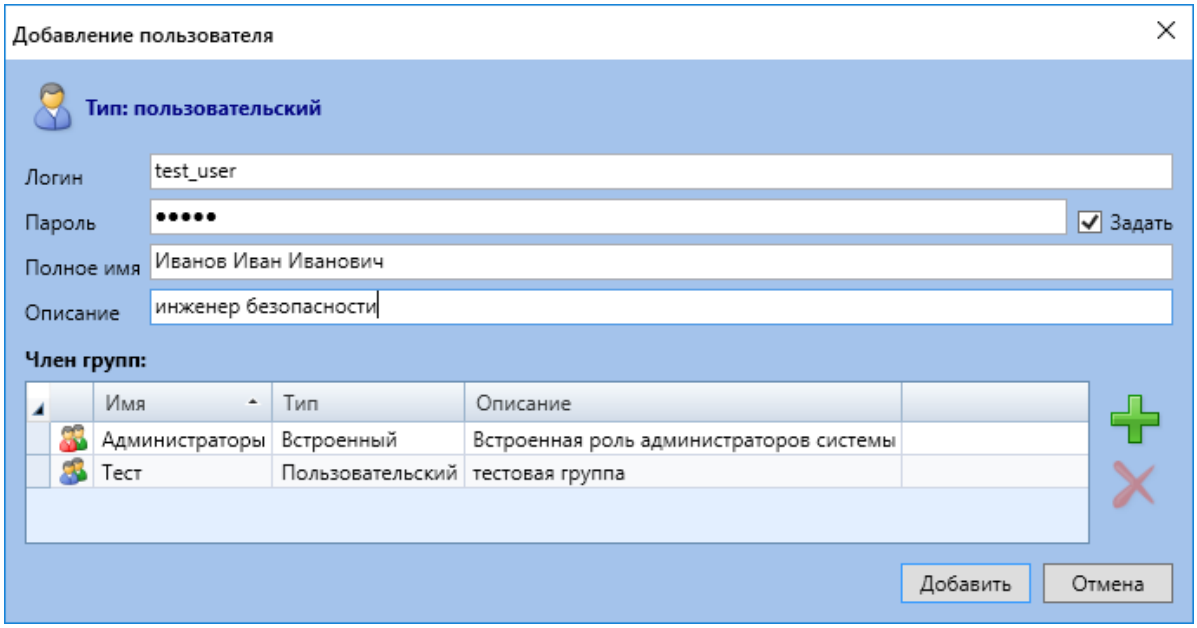


Рисунок 78 - APM RusGuard. Модуль Конфигурация системы. Окно ввода данных о пользователе

5. Заполните обязательные поля: ***Логин***, ***Пароль***, ***Полное имя***. При необходимости добавьте описание.

Снимите флаг ***Задать***, если не хотите использовать пароль в учетной записи пользователя.

Предупреждение: Для доступа к модулю ***Отчеты*** 214 учетная запись пользователя обязательно должна иметь пароль.

После ввода достаточных учетных данных активируется кнопка Добавить. Нажмите на нее, чтобы создать пользователя без привязки к группе и завершить процедуру, или, не закрывая окна, выполните привязку к группе.

6. Чтобы привязать пользователя к группе, нажмите на кнопку  .

Откроется список доступных групп.

7. Выберите нужную группу. Пользователь может быть членом нескольких групп. Как только выполнена привязка хотя бы к одной группе, активируется кнопка  для удаления группы из карточки пользователя.

8. Добавив желаемое количество групп, нажмите на кнопку Добавить, чтобы закончить процедуру.

Новая учетная запись пользователя появится в иерархическом списке в левой навигационной панели.

Настройка длины ключа

В модуле ***Конфигурация системы*** APM RusGuard предусмотрена возможность настройки максимальной отображаемой длины кода ключа, считываемого настольным считывающим устройством.

Например, если устройство считало с карты 6 байт, а в настройках указан максимум 3 - в системе отобразится только 3 байта.

Эта функция обеспечивает совместимость со считывателями различных моделей.

Поддерживаются значения от 1 до 6.

Для того чтобы задать длину кода ключа:

1. Запустите APM RusGuard.

   Для работы с базой данных пользователей APM необходимо иметь доступ к модулю ***Конфигурация системы***.

2. Зайдите в модуль ***Конфигурация системы***.
3. Выберите пункт ***Система*** в левой навигационной панели (см. рис. 78).

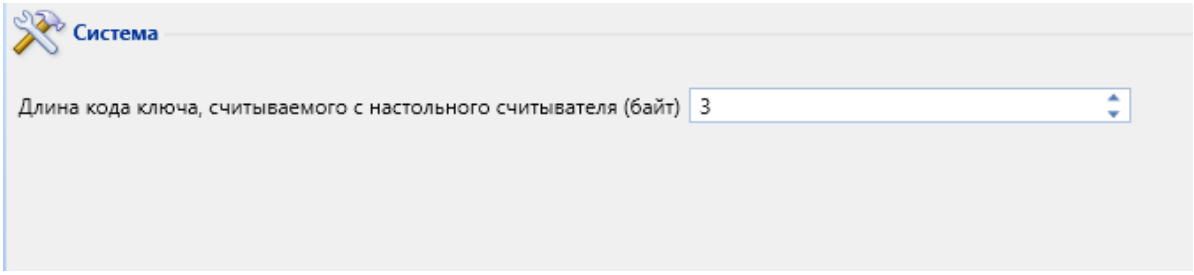


Рисунок 79 - APM RusGuard. Модуль Конфигурация системы. Настройка длины отображаемого кода

4. Нажмите на кнопку ***Редактировать*** в панели управления сверху.

   В главном экране активируется поле ввода.

5. Введите значение от 1 до 6 вручную или используя стрелочки.
6. Нажмите на кнопку ***Редактировать*** в панели управления сверху.

   Система применит настройки.

Типы дней

ПО RusGuard позволяет вести базу типов дней, в которой сохраняются настройки для различных типов дней, кроме будней и выходных, которые могут потребоваться для учета рабочего времени.

По умолчанию список содержит стандартный список вариантов, предусмотренных стандартным делопроизводством (отпуск по уход за ребенком, ежегодный оплаченный отпуск и т.д.).

Для того чтобы создать новый тип дня:

1. Зайдите в модуль конфигурация системы APM RusGuard.

2. Раскройте меню ***Учет рабочего времени*** навигационной панели слева. Установите курсор в подменю ***Типы дней*** (см. рис. 79).

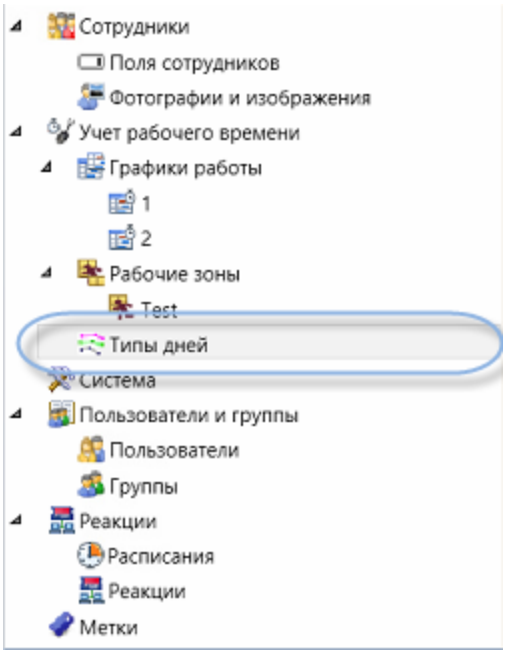
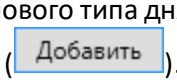


Рисунок 80 - APM RusGuard. Модуль Конфигурация системы. Меню боковой панели

3. Нажмите на кнопку 

в верхней панели управления, чтобы создать новый тип дня.
4. Введите основные параметры нового типа дня в диалоговом окне, которое откроется (см. рис. 80). Сохраните данные (

).

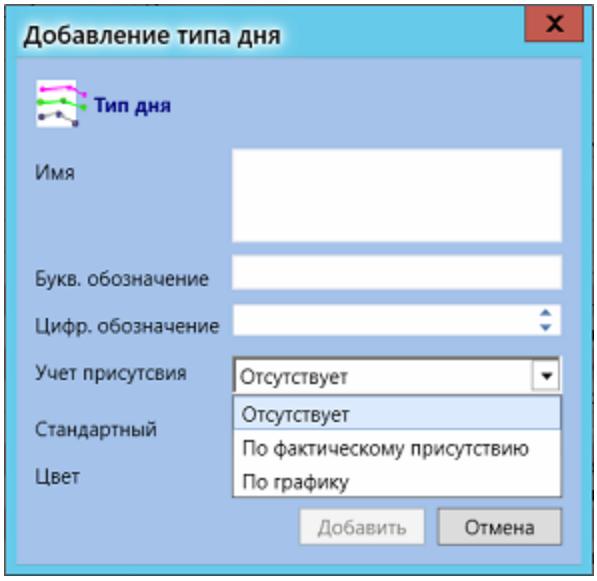
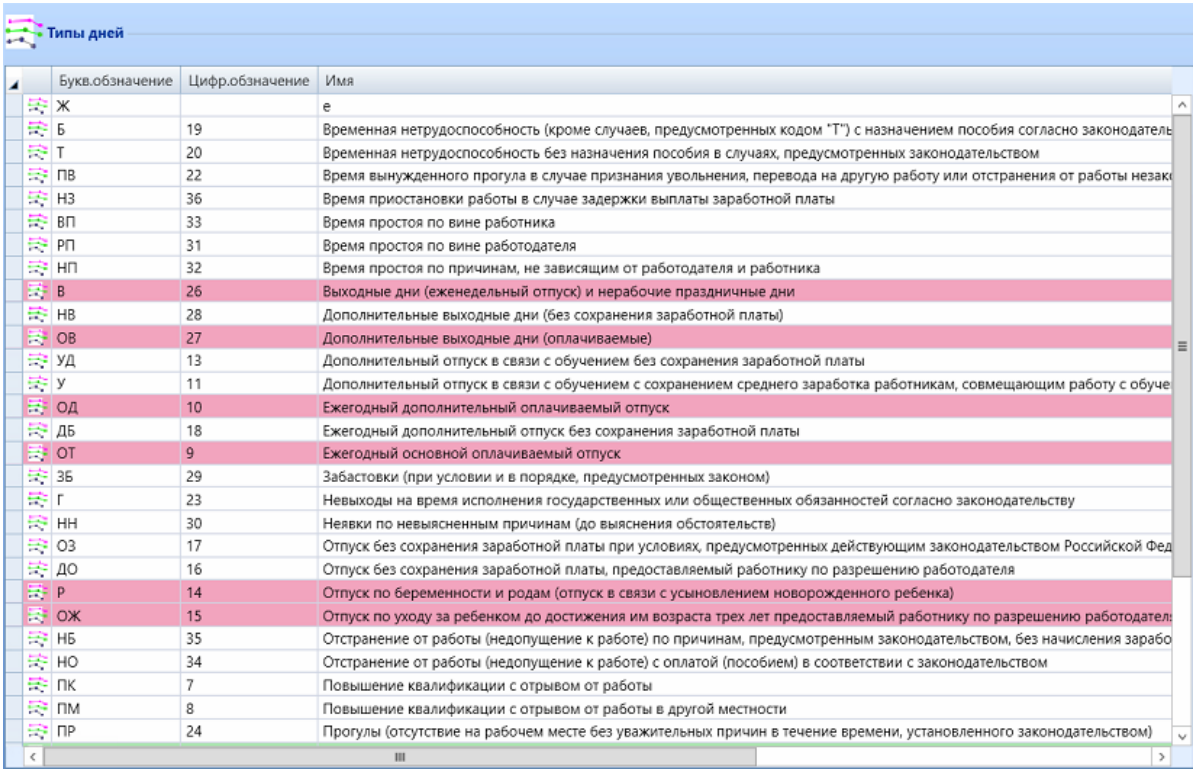


Рисунок 81 - АРМ RusGuard. Модуль Конфигурация системы. Ввод основных параметров типа дня

Созданный тип дня отобразится в общем списке (см. рис. 81).



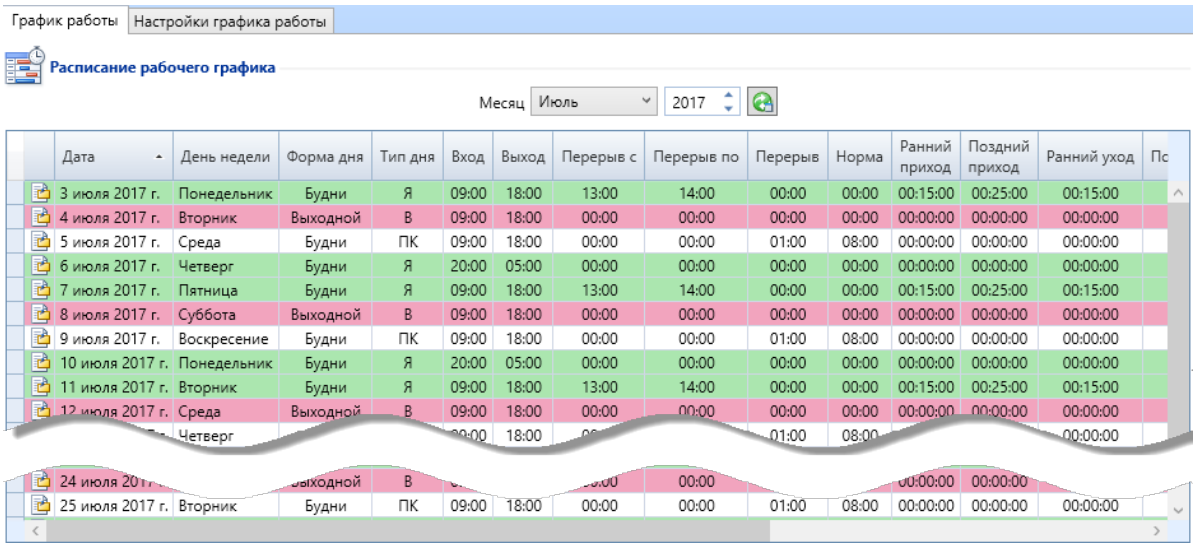
Букв.обзначение	Цифр.обзначение	Имя
Ж		е
Б	19	Временная нетрудоспособность (кроме случаев, предусмотренных кодом "Т") с назначением пособия согласно законодатель
Т	20	Временная нетрудоспособность без назначения пособия в случаях, предусмотренных законодательством
ПВ	22	Время вынужденного прогула в случае признания увольнения, перевода на другую работу или отстранения от работы незак
НЗ	36	Время приостановки работы в случае задержки выплаты заработной платы
ВП	33	Время простоя по вине работника
РП	31	Время простоя по вине работодателя
НП	32	Время простоя по причинам, не зависящим от работодателя и работника
В	26	Выходные дни (еженедельный отпуск) и нерабочие праздничные дни
НВ	28	Дополнительные выходные дни (без сохранения заработной платы)
ОВ	27	Дополнительные выходные дни (оплачиваемые)
УД	13	Дополнительный отпуск в связи с обучением без сохранения заработной платы
У	11	Дополнительный отпуск в связи с обучением с сохранением среднего заработка работникам, совмещающим работу с обуче
ОД	10	Ежегодный дополнительный оплачиваемый отпуск
ДБ	18	Ежегодный дополнительный отпуск без сохранения заработной платы
ОТ	9	Ежегодный основной оплачиваемый отпуск
ЗБ	29	Забастовки (при условии и в порядке, предусмотренных законом)
Г	23	Невыходы на время исполнения государственных или общественных обязанностей согласно законодательству
НН	30	Неявки по невыясненным причинам (до выяснения обстоятельств)
ОЗ	17	Отпуск без сохранения заработной платы при условиях, предусмотренных действующим законодательством Российской Фед
ДО	16	Отпуск без сохранения заработной платы, предоставляемый работнику по разрешению работодателя
Р	14	Отпуск по беременности и родам (отпуск в связи с усыновлением новорожденного ребенка)
ОЖ	15	Отпуск по уходу за ребенком до достижения им возраста трех лет предоставляемый работнику по разрешению работодател
НБ	35	Отстранение от работы (недопущение к работе) по причинам, предусмотренным законодательством, без начисления зарабо
НО	34	Отстранение от работы (недопущение к работе) с оплатой (пособием) в соответствии с законодательством
ПК	7	Повышение квалификации с отрывом от работы
ПМ	8	Повышение квалификации с отрывом от работы в другой местности
ПР	24	Прогулы (отсутствие на рабочем месте без уважительных причин в течение времени, установленного законодательством)

Рисунок 82 - АРМ RusGuard. Модуль Конфигурация системы. Список типов дней

5. Теперь вы можете использовать созданный тип дня для привязки к рабочим графикам[181] и исключениям рабочих графиков в карточке сотрудника[137].

Графики работы

ПО RusGuard позволяет настраивать графики на каждый день с учетом различных параметров (см. рис. 82). Графики работы необходимы для корректного построения отчетов 214 рабочего времени.



Дата	День недели	Форма дня	Тип дня	Вход	Выход	Перерыв с	Перерыв по	Перерыв	Норма	Ранний приход	Поздний приход	Ранний уход	Пс
3 июля 2017 г.	Понедельник	Будни	Я	09:00	18:00	13:00	14:00	00:00	00:00	00:15:00	00:25:00	00:15:00	
4 июля 2017 г.	Вторник	Выходной	В	09:00	18:00	00:00	00:00	00:00	00:00	00:00:00	00:00:00	00:00:00	
5 июля 2017 г.	Среда	Будни	ПК	09:00	18:00	00:00	00:00	01:00	08:00	00:00:00	00:00:00	00:00:00	
6 июля 2017 г.	Четверг	Будни	Я	20:00	05:00	00:00	00:00	00:00	00:00	00:00:00	00:00:00	00:00:00	
7 июля 2017 г.	Пятница	Будни	Я	09:00	18:00	13:00	14:00	00:00	00:00	00:15:00	00:25:00	00:15:00	
8 июля 2017 г.	Суббота	Выходной	В	09:00	18:00	00:00	00:00	00:00	00:00	00:00:00	00:00:00	00:00:00	
9 июля 2017 г.	Воскресение	Будни	ПК	09:00	18:00	00:00	00:00	01:00	08:00	00:00:00	00:00:00	00:00:00	
10 июля 2017 г.	Понедельник	Будни	Я	20:00	05:00	00:00	00:00	00:00	00:00	00:00:00	00:00:00	00:00:00	
11 июля 2017 г.	Вторник	Будни	Я	09:00	18:00	13:00	14:00	00:00	00:00	00:15:00	00:25:00	00:15:00	
12 июля 2017 г.	Среда	Выходной	В	09:00	18:00	00:00	00:00	00:00	00:00	00:00:00	00:00:00	00:00:00	
	Четверг			09:00	18:00			01:00	08:00			00:00:00	
24 июля 2017 г.		Выходной	В				00:00			00:00:00	00:00:00		
25 июля 2017 г.	Вторник	Будни	ПК	09:00	18:00	00:00	00:00	01:00	08:00	00:00:00	00:00:00	00:00:00	

Рисунок 83 - APM RusGuard. Модуль Конфигурация системы. Параметры рабочего графика

Функция настройки рабочих графиков тесно связана с ведением списка типов дней. В целом, процесс управления рабочими графиками включает следующие шаги:

- создание списка типов дней;
- создание рабочего графика;
- тиражирование рабочего графика на определенный период (если необходимо);
- привязка рабочего графика к сотруднику 137 или группе сотрудников;
- редактирование/удаление графиков.

Для того чтобы настроить график работы на период:

1. Зайдите в модуль конфигурация системы APM RusGuard.
2. Раскройте меню ***Учет рабочего времени*** навигационной панели слева. Установите курсор в подменю ***Графики работы*** (см. рис. 83).

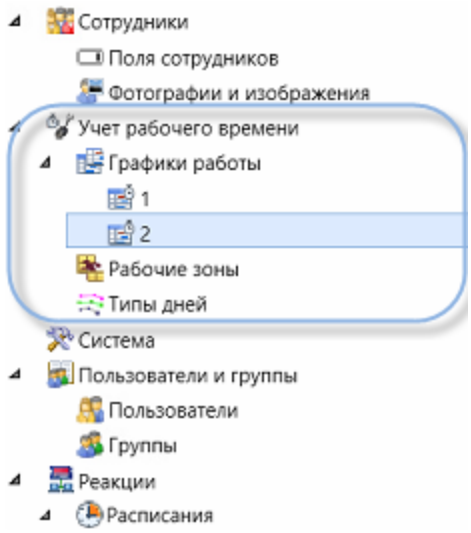
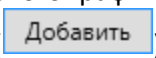


Рисунок 84 - АРМ RusGuard. Модуль Конфигурация системы. Создание рабочего графика

3. Нажмите на кнопку 

в верхней панели управления, чтобы создать новый график работы.
4. Введите основные параметры нового графика в диалоговом окне, которое откроется (см. рис. 84). Сохраните данные (

).

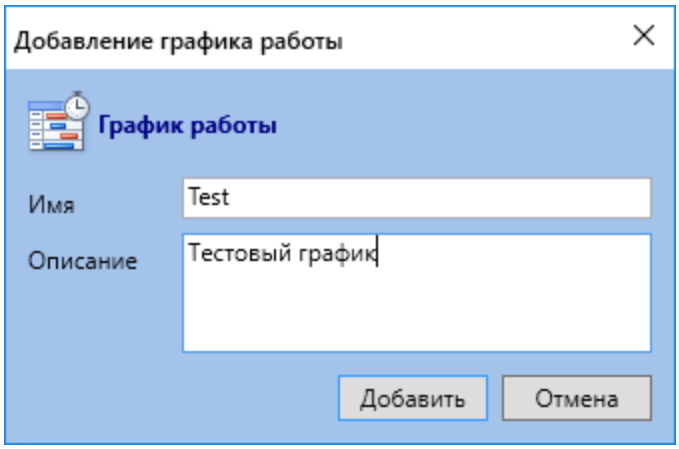


Рисунок 85 - АРМ RusGuard. Модуль Конфигурация системы. Ввод основных параметров нового графика

Откроется окно ***Список рабочего графика***, где вы сможете настроить произвольное количество графиков на день (см. рис. 85). По умолчанию список пуст. Как правило, заводится 7 строк: 5 для будних дней и 2 для выходных. Затем настройки тиражируются на определенный период.

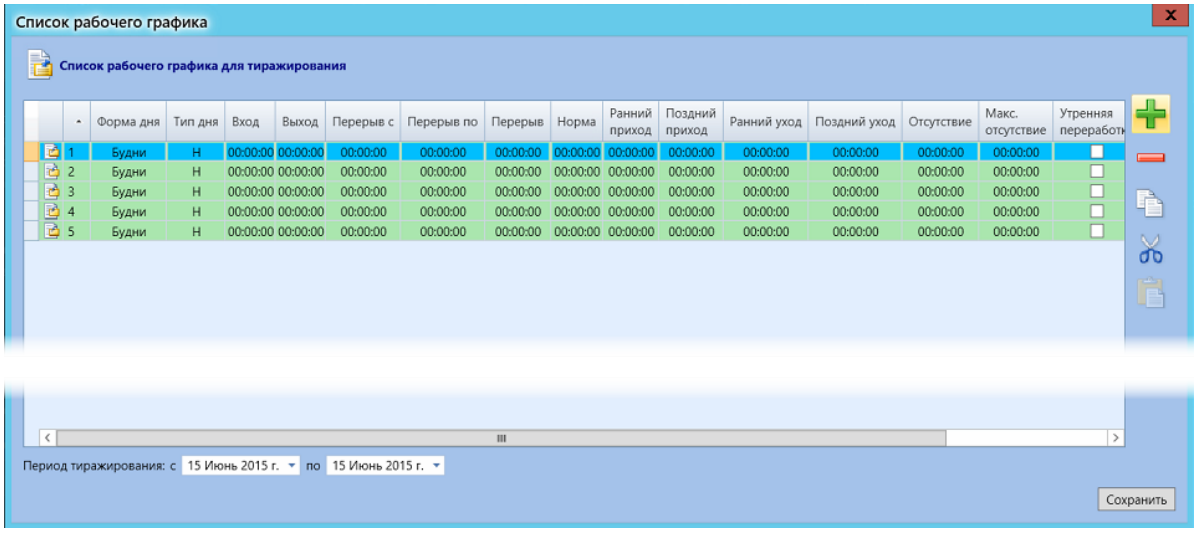


Рисунок 86 - APM RusGuard. Модуль Конфигурация системы. Формирование списка графиков

Чтобы добавить, скопировать, вставить, вырезать, удалить или отредактировать строку в списке, используйте пиктограммы в правой части окна. Таким образом, вы можете сначала настроить график для одного дня (например, буднего), затем создать еще четыре ее копии, либо настроить пять разных графиков для будних дней, если это необходимо.

5. Создайте пустую строку. По умолчанию значения полей нового графика ***Форма дня*** и ***Тип дня*** установлены на ***Будни*** и ***Н*** соответственно (наиболее распространенные варианты обычного рабочего дня). Все указатели времени обнулены, флаги неактивны.
6. Заполните поля в строке (см. табл. 9редактирование полей выполняется непосредственно в активной строке). Для ввода времени просто введите нужные цифры. Чтобы заполнить поля ***Форма дня*** и ***Тип дня***, щелкните в поле мышкой. Появится соответствующий список, из которого необходимо выбрать нужный вариант (см. рис. 86).

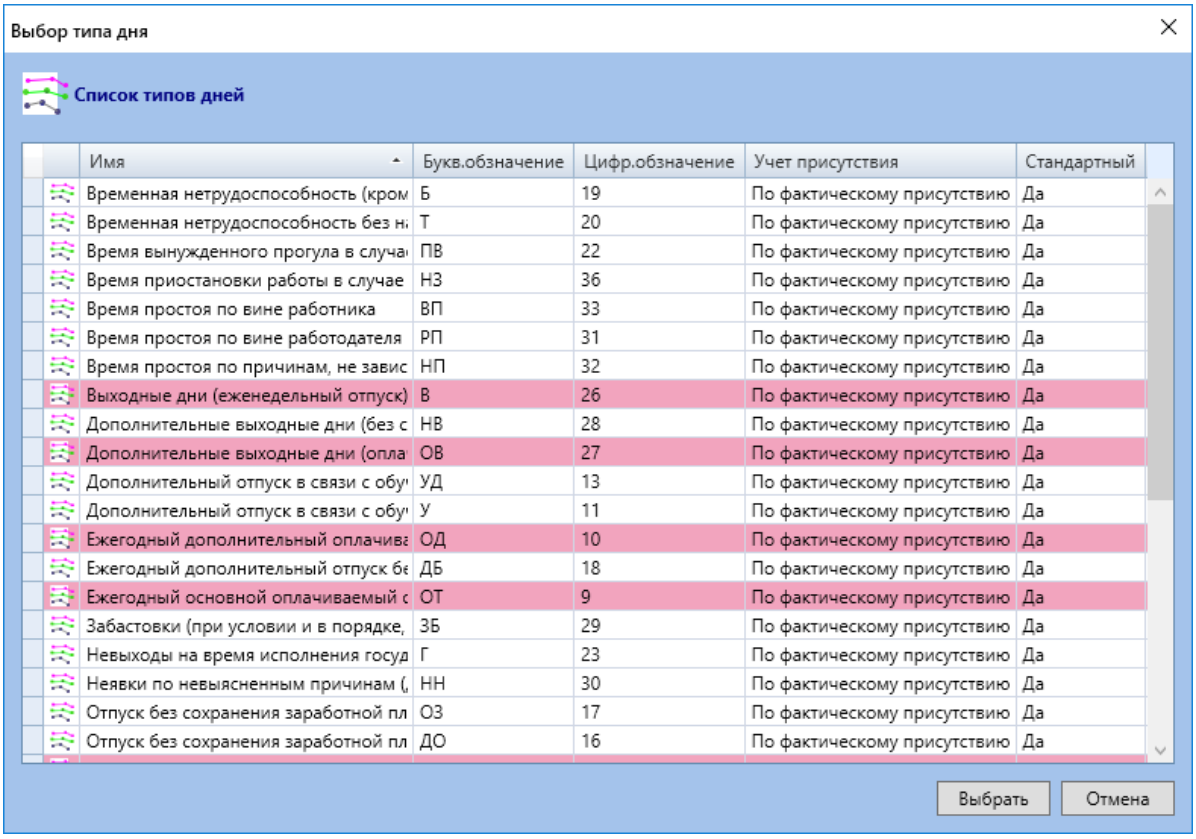


Рисунок 87 - АРМ RusGuard. Модуль Конфигурация системы. Окно выбора типа дня для вставки в соответствующее поле графика

Таблица 10 - Параметры настройки рабочих графиков	
Параметр	Описание
Форма дня	Возможные варианты: будний, выходной и праздник
Тип дня	Загружается список (соответствует списку в программах 1С) типов дней. Этот список может быть отредактирован, дополнен. Ведется отдельно 178.
Вход	Указывается время для контроля входа
Выход	Указывается время для контроля выхода
Перерыв с	Указывается время начала перерыва. Это поле и следующее используются вместе в том случае, если время перерыва жестко нормировано. При использовании полей вход и выход сотрудника на перерыв не учитываются как отлучка, а время перерыва автоматически вычитается из общего времени пребывания на работе.
Перерыв по	Указывается время начала перерыва. Это поле и предыдущее используются вместе в том случае, если время перерыва жестко нормировано. При использовании полей вход и выход сотрудника на перерыв не учитываются как отлучка, а время перерыва

Таблица 10 - Параметры настройки рабочих графиков	
	автоматически вычитается из общего времени пребывания на работе.
Перерыв	Указывается продолжительность перерыва, при этом два предыдущих поля остаются пустыми. Этот вариант используется для настройки "плавающего" перерыва, т.е. его время не имеет значения. Подразумевается, что сотрудник **не покидает рабочую зону и обедает на рабочем месте**. **Любые отлучки при этом типе настройки перерыва учитываются в системе как отлучки с рабочего места**.
Норма	В это поле вводится общая продолжительность рабочего времени для свободного графика посещения. При этом не заполняются поля времени входа, выхода, перерывы. Важно только соответствие общего количества часов пребывания сотрудника на рабочем месте указанной норме.
Ранний приход	В этом поле указывается **разница между необходимым временем прихода и точкой, от которой отсчитывается утренняя переработка**. То есть, если рабочий день начинается с 9 утра, а в это поле введено 30 минут, то приход в 8:30 утра не является переработкой.
Поздний приход	В этом поле указывается **разница между необходимым временем прихода и точкой, от которой отсчитывается опоздание**. То есть, если рабочий день начинается с 9 утра, а в это поле введено 30 минут, то приход в 9:30 утра не является опозданием.
Ранний уход	В этом поле указывается **разница между ожидаемым временем ухода и точкой, от которой ранний уход**. То есть, если рабочий день заканчивается в 18:00, а в это поле введено 30 минут, то уход в 17:30 не является ранним уходом.
Поздний уход	В этом поле указывается **разница между ожидаемым временем ухода и точкой, от которой отсчитывается вечерняя переработка**. То есть, если рабочий день заканчивается в 18:00, а в это поле введено 30 минут, то уход в 18:30 не является переработкой.
Отсутствие	В этом поле указывается продолжительность отсутствия на рабочем месте, которая считается отлучкой. Например, если в поле введено значение 15 минут, то отсутствие в течение 14 минут не составляет отлучки. При этом, каждая отлучка учитывается в системе, отлучки суммируются для использования в поле ниже.
Макс. отсутствие	В этом поле указывается суммарное допустимое отсутствие на рабочем месте. Например, если в этом поле указано значение 1 час, то 6 отлучек по 11 минут превысят это значение, что приведет к **вычету разницы из общего отработанного времени**.
Утренняя переработка	Флаг устанавливается для учета утренних переработок. Обратите внимание, что для его использования обязателен ввод значения в поле ***Вход***.

Таблица 10 - Параметры настройки рабочих графиков	
Вечерняя переработка	Флаг устанавливается для учета вечерних переработок. Обратите внимание, что для его использования обязателен ввод значения в поле ***Выход***.
Ночная смена	Флаг устанавливается для корректного учета рабочего времени при переходе через полночь.

7. Сформировав график, вы можете тиражировать его на определенный период (т.е. выбрать период, когда он будет циклично применяться (с первого дня до последнего), начиная с текущей даты). Введите нужные даты в нижней части списка графиков, в полях ***Период тиражирования с ...по...***. По умолчанию в обоих полях установлена текущая дата.
8. Сохраните созданный список (Сохранить).
9. Чтобы использовать график, привяжите его к группе сотрудников или сотруднику (через карточку сотрудника).

Обратите внимание, что для отдельных сотрудников возможно создание исключений графика (т.е. индивидуальных графиков). Настройка выполняется в карточке сотрудника.

Типовые примеры настройки графиков работы

Ранний приход/уход, поздний приход/уход

Настройка раннего и позднего прихода, раннего и позднего ухода, т.е. возможных отклонений от начала и конца рабочего дня, которые не составляют переработки, опоздания или раннего ухода (см. рис. 87).

В примере на иллюстрации (первая строка) установлены значения ***15*** и ***25*** минут в полях ***Ранний приход*** и ***Поздний приход***, то есть, приход в 08:50 или 09:10 не является переработкой или опозданием. В полях ***Ранний уход*** и ***Поздний уход*** установлены значения ***15*** минут и ***20*** минут, то есть уход в 17:50 или 18:10 - ранним уходом или переработкой соответственно.

Обратите внимание, что в поля ***Форма дня*** и 4 в примере введены значения ***Будни*** и ***Я***, то есть, это рабочий день.

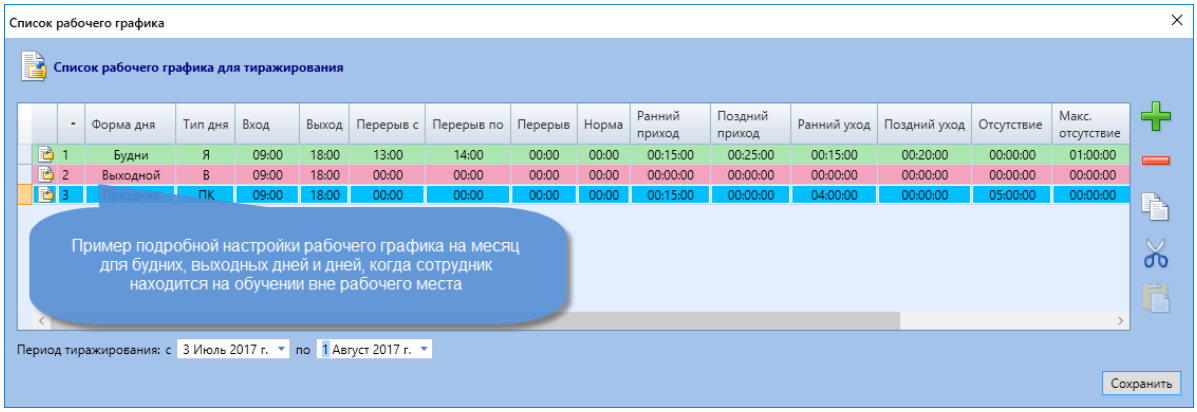


Рисунок 88 - APM RusGuard. Модуль Конфигурация системы. Пример настройки допустимого времени раннего прихода/ухода, позднего прихода/ухода

Настройка учета переработок

Для учета переработок необходимо установить флаги ***Утренняя переработка*** и ***Вечерняя переработка*** (см. рис. 88). При этом обязательно должно быть настроено фиксированное время входа и выхода. Может быть удобно также настроить поля раннего прихода/ухода, позднего прихода/ухода. При свободном графике (поле ***Норма***) эти флаги работать не будут.

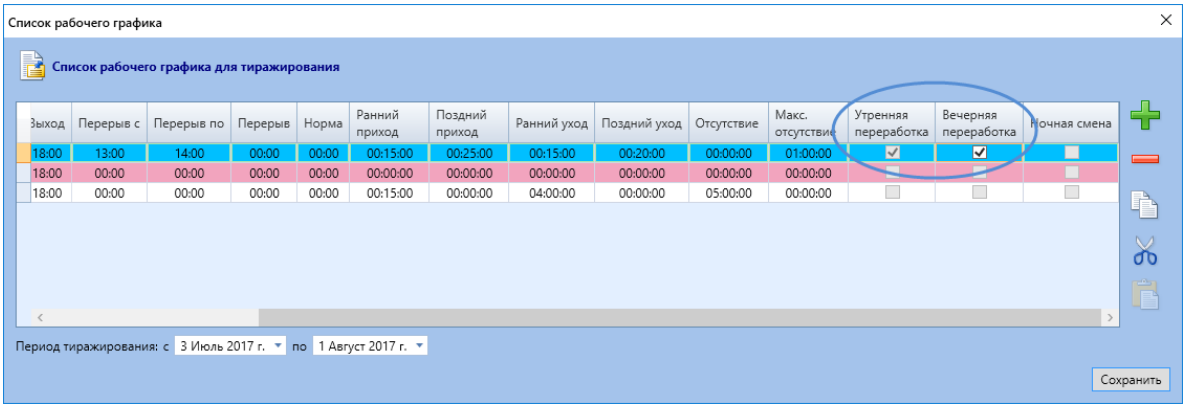


Рисунок 89 - APM RusGuard. Модуль Конфигурация системы. Пример настройки переработок

Настройка перерыва

Вы можете настроить время перерыва двумя способами:

- указав точный интервал в полях ***Перерыв с*** и ***Перерыв по***
- указав продолжительность перерыва в поле ***Перерыв***

Первый вариант позволяет сотрудникам покидать во время перерыва рабочие зоны, при этом выходы не учитываются как отлучки. Установленное время перерыва не учитывается в общем времени работы и не вычитается из него.

Второй вариант предназначен для тех случаев, когда сотрудники не покидают рабочую зону на время перерыва и сами определяют его время. В этом случае указанная продолжительность перерыва не учитывается в рабочем времени, но дополнительные выходы/входы не предусмотрены.

Ниже (см. рис. 89) показан пример фиксированного перерыва с 13:30 до 14:30.

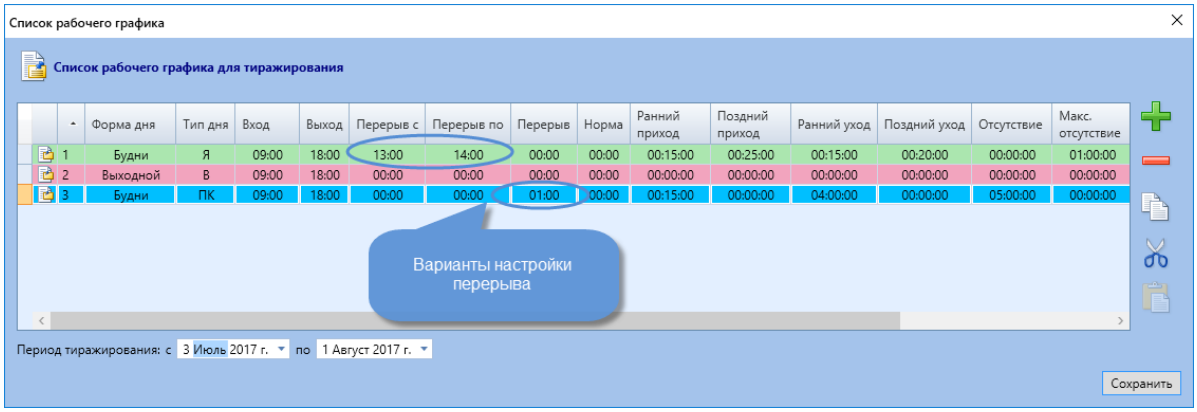


Рисунок 90 - АРМ RusGuard. Модуль Конфигурация системы. Пример настройки фиксированного перерыва

Настройка отлучек

Учет отлучек регулируется полями ***Отсутствие*** и ***Макс. отсутствие*** (см. рис. 90). В первом поле вводится продолжительность допустимой разовой отлучки. Во втором - общая допустимая отлучка за день. Например, если в поле ***Отсутствие*** указано значение 10 минут, а в поле ***Макс. отсутствие*** - 1 час, общая продолжительность отлучек не должна превышать одного часа, то есть, 6 отлучек по 11 минут превысят это значение, и разница будет учтена как отсутствие на рабочем месте. Также, 7 отлучек по 9 минут приведут к превышению максимума, несмотря на то, что каждая отлучка не превышает 10 минут.

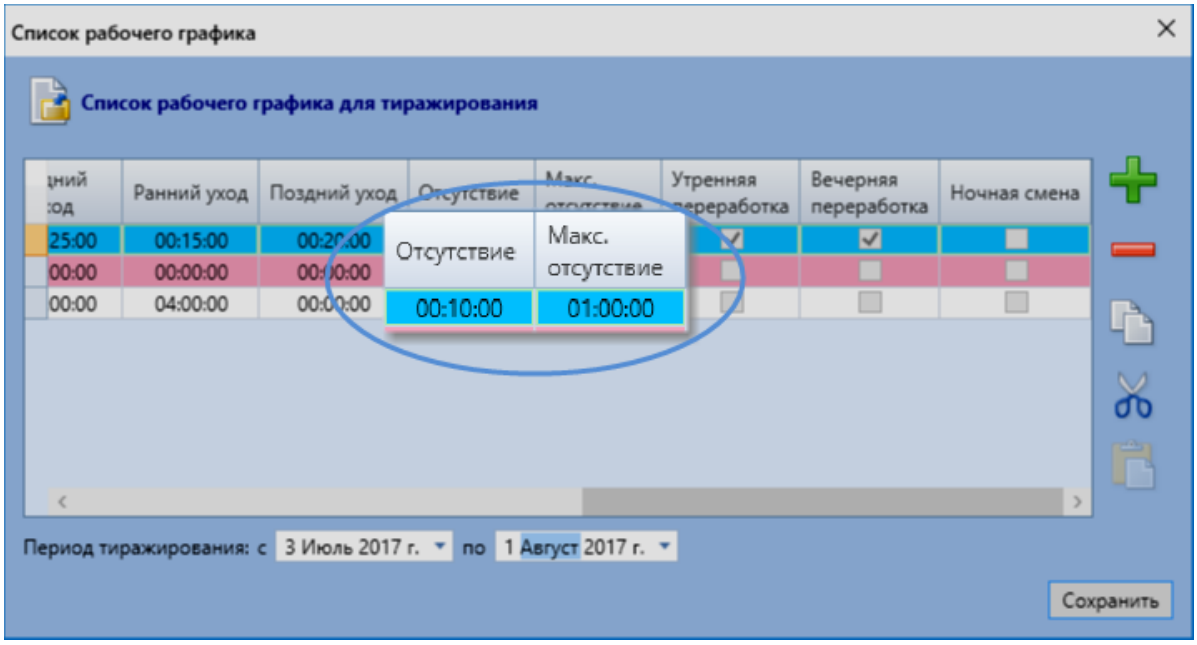


Рисунок 91 - АРМ RusGuard. Модуль Конфигурация системы. Пример настройки учета отлучек

Настройка свободного графика

Свободный график (без фиксированного времени прихода и ухода) настраивается при помощи поля ***Норма*** (см. рис. 91). В это поле вводится общая продолжительность рабочего времени (например, 8 часов), при этом отлучки, время прихода и ухода, отсутствие и пр.

параметры значения не имеют. Оценивается только соответствие общего времени пребывания в рабочей зоне норме.

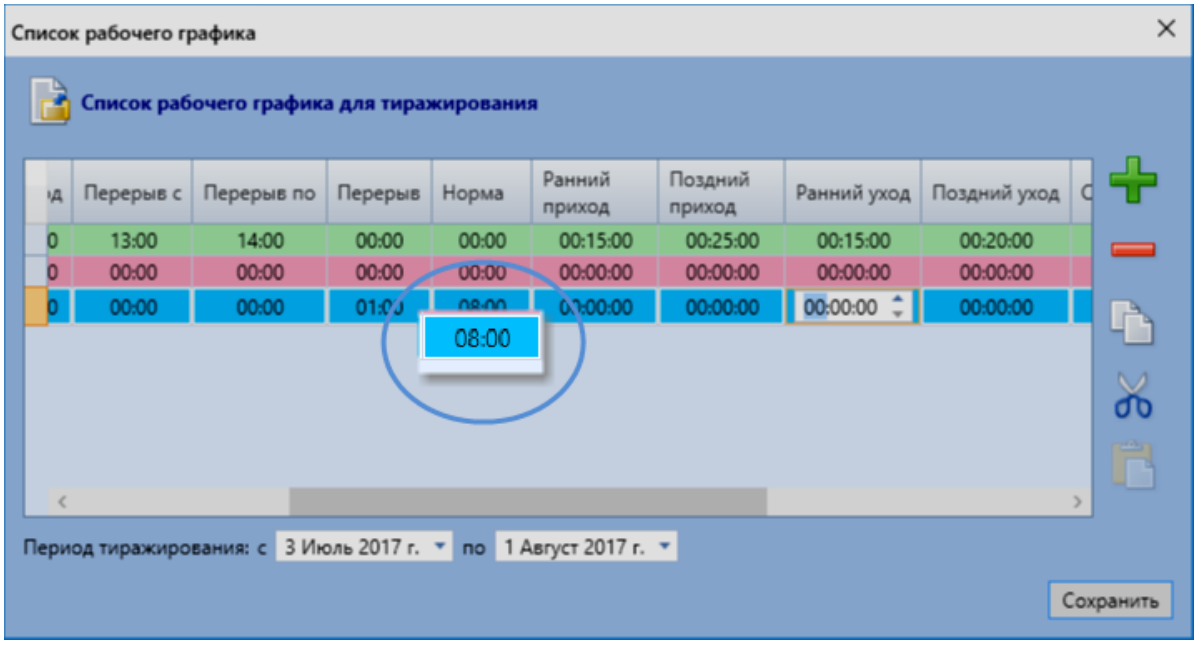


Рисунок 92 - APM RusGuard. Модуль Конфигурация системы. Пример настройки свободного графика

Настройка ночных смен

Флаг ***Ночная смена*** позволяет вести корректный учет рабочего времени при переходе через полночь (см. рис. 92).

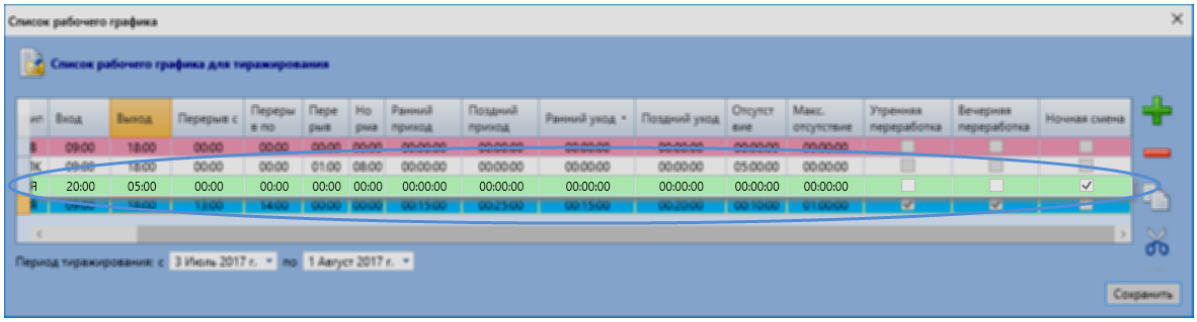


Рисунок 93 - APM RusGuard. Модуль Конфигурация системы. Пример настройки ночной смены с 20:00 до 05:00

Рабочие зоны

ПО RusGuard позволяет создавать рабочие зоны. Рабочие зоны содержат списки точек доступа (о точках доступа и уровнях доступа см. здесь 67) на вход и выход. При привязке к карточке сотрудника они позволяют ограничивать/контролировать его доступ внутри объекта.

Для того чтобы создать и настроить рабочую зону:

1. Зайдите в модуль конфигурация системы АРМ RusGuard.
2. Раскройте меню ***Учет рабочего времени*** навигационной панели слева. Установите курсор в подменю ***Рабочие зоны*** (см. рис. 93).

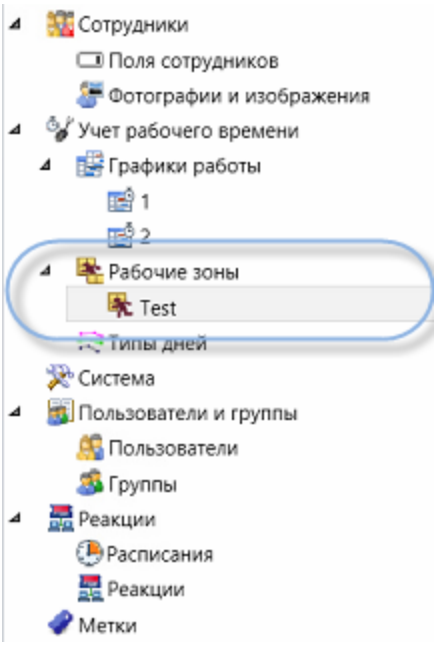
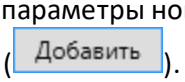


Рисунок 94 - АРМ RusGuard. Модуль Конфигурация системы. Меню боковой панели

3. Нажмите на кнопку 

в верхней панели управления, чтобы создать новую рабочую зону.
4. Введите основные параметры нового типа дня в диалоговом окне, которое откроется. Сохраните данные (

).

Новая рабочая зона появится в списке боковой панели слева (см. рис. 94). Чтобы завершить процедуру настройки рабочей зоны, необходимо привязать к ней точки доступа на выход и на вход.

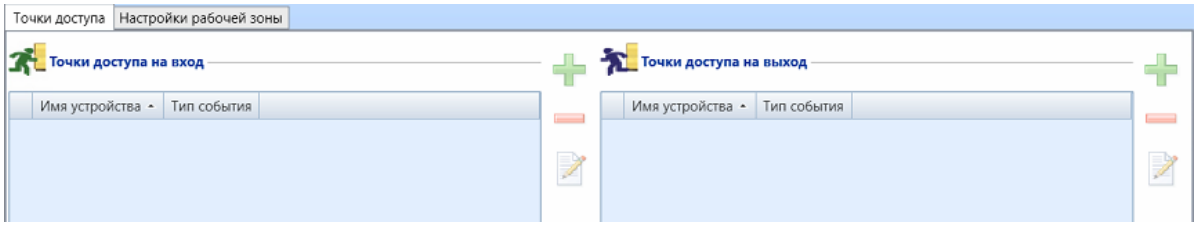


Рисунок 95 - APM RusGuard. Модуль Конфигурация системы. Рабочая зона (новая)

5. Нажмите на пиктограмму  в верхней панели инструментов, чтобы сделать возможным редактирование (настойку) созданной рабочей зоны.

6. Нажмите на кнопку  справа от области ***Точки доступа на вход***, чтобы добавить к настраиваемой рабочей зоне одну из точек доступа.

Откроется диалоговое окно настройки (см. рис. 95).

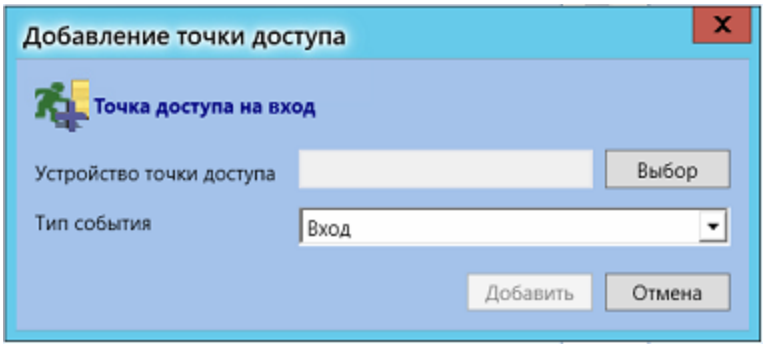


Рисунок 96 - APM RusGuard. Модуль Конфигурация системы. Привязка точки доступа к рабочей зоне

7. Выберите устройство точки доступа из списка (кнопка ***Выбор***) (см. рис. 96).

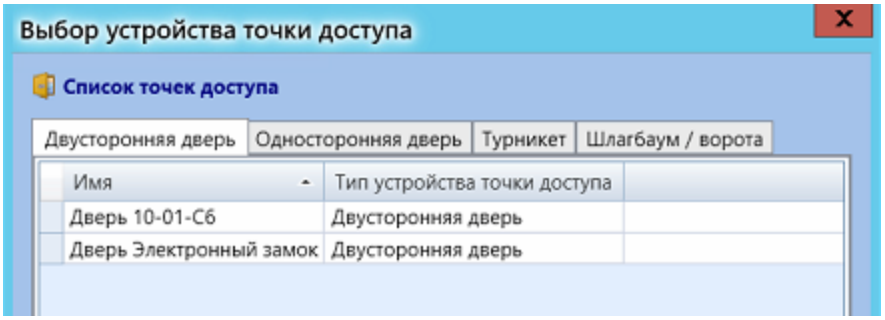
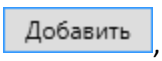


Рисунок 97 - APM RusGuard. Модуль Конфигурация системы. Привязка точки доступа к рабочей зоне (список устройств точек доступа)

8. Укажите тип события (по умолчанию выбран ***Вход***).

9. Нажмите на кнопку  , чтобы завершить настройку точки доступа на вход.

10. Аналогичным образом вы можете настроить другие точки доступа на вход и выход. Для редактирования и удаления точек доступа в списках рабочих зон используйте кнопки  и  .

Созданные рабочие зоны могут быть привязаны к карточкам сотрудников[137].

Реакции

Реакции настраиваются для обеспечения уведомления заинтересованных лиц (пользователей и администраторов ПО RusGuard, пользователей систем, обслуживаемых ПО, и т.д.) о событиях, связанных с функционированием оборудования (устройств), входящего в систему, которую обслуживает ПО. Каждая реакция представляет собой операцию, которая выполняется в ответ на одно или несколько событий по настроенному расписанию.

Например, ПО позволяет настроить рассылку уведомлений по электронной почте одному или нескольким лицам в случае осуществления прохода через определенную точку доступа.

Настройка Расписаний

Для того чтобы создать расписание реакции:

1. Загрузите модуль ***Конфигурация системы*** APM.
2. В навигационной панели слева выберите пункт ***Расписания***.
3. Нажмите на кнопку  ***Добавить расписание реакции***.

Загрузится форма ввода расписания (см. рис. 97).

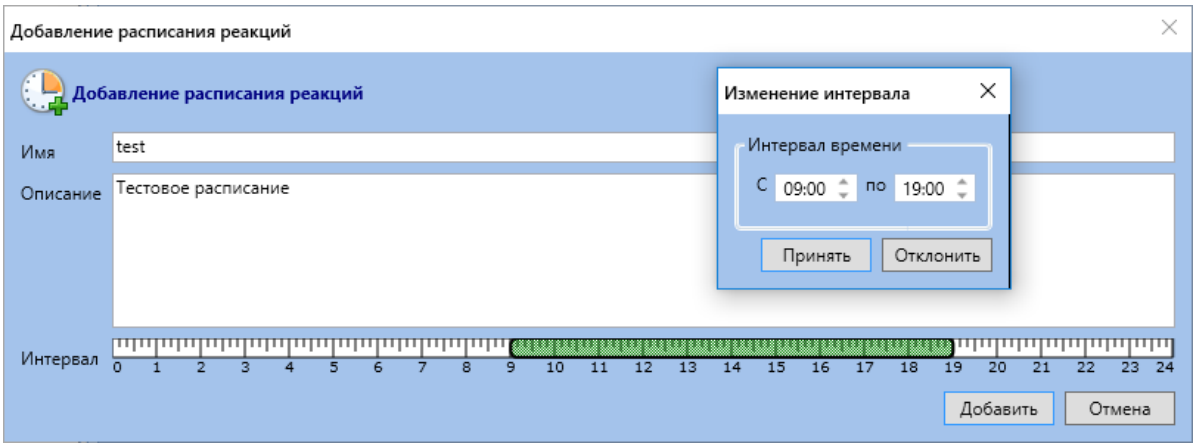


Рисунок 98 - APM RusGuard. Модуль Конфигурация системы. Ввод нового расписания реакции

4. Введите название расписания в поле ***Имя*** (обязательное поле, имена расписаний не могут совпадать). Установив курсор в начало желаемого временного интервала, нажмите левую кнопку и тащите курсор вправо, чтобы задать интервал действия расписания. Если поле ***Интервал*** не заполнено, расписание действует 24 часа.

Поле ***Описание*** может быть пустым.

5. Нажмите на кнопку  .

Система выполнит сохранение данных. Название расписания (поле ***Имя***) отобразится в иерархическом списке навигационной панели слева.

В дальнейшем расписание может быть отредактировано.

Настройка Реакций

Для того чтобы создать новую реакцию:

1. Загрузите модуль ***Конфигурация системы*** АРМ.
2. В навигационной панели слева выберите пункт ***Реакции***.
3. Нажмите на кнопку 

в панели управления сверху.

Загрузится форма ввода данных о реакции (см. рис. 98).

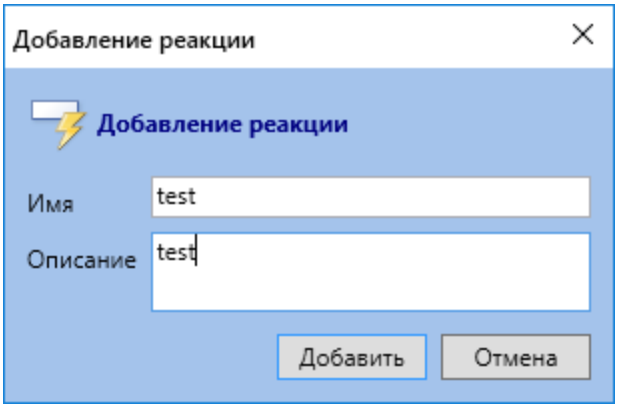


Рисунок 99 - АРМ RusGuard. Модуль Конфигурация системы. Ввод параметров новой реакции

4. Введите название реакции в поле ***Имя*** (обязательное поле). Нажмите на кнопку Добавить.

Система выполнит сохранение данных. Название реакции (поле ***Имя***) отобразится в иерархическом списке навигационной панели слева. У созданной реакции есть два подпункта: ***События*** и ***Действия*** (см. рис. 99).

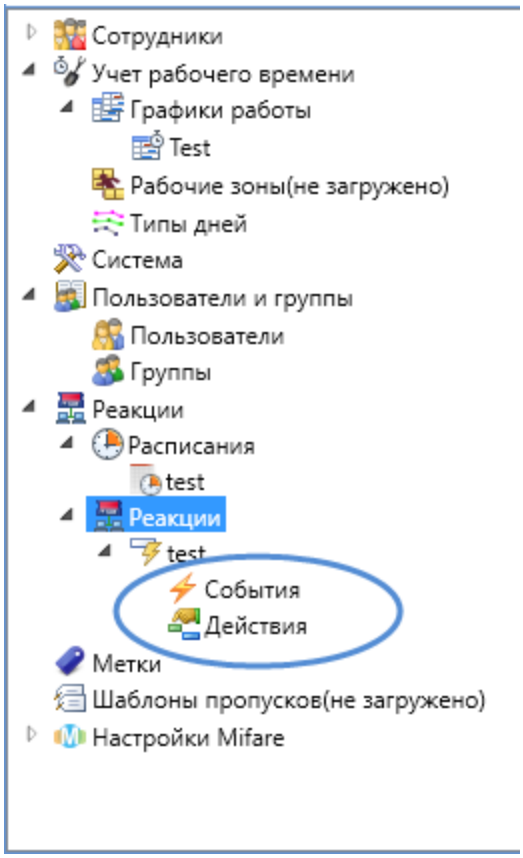


Рисунок 100 - APM RusGuard. Модуль Конфигурация системы. Созданная реакция в навигационной панели

Теперь вы можете настроить реакцию.

Для того чтобы настроить параметры реакции:

1. Выполните настройки события.
2. Выполните настройки действия.

Для того чтобы выполнить настройки события:

1. Найдите нужную реакцию в иерархическом списке навигационной панели слева.
2. Перейдите в подпункт ***События***.

По умолчанию, при первоначальной настройке событий в главном экране отобразится пустой список.

3. Нажмите на кнопку  Редактировать в верхней панели инструментов.

Активируется кнопка  справа от пустого списка. Если список редактируется не впервые, и в нем уже есть события, активируется также и кнопка  для удаления событий.

4. Чтобы добавить событие, нажмите на кнопку  .

Загрузится форма ввода событий (см. рис. 100).

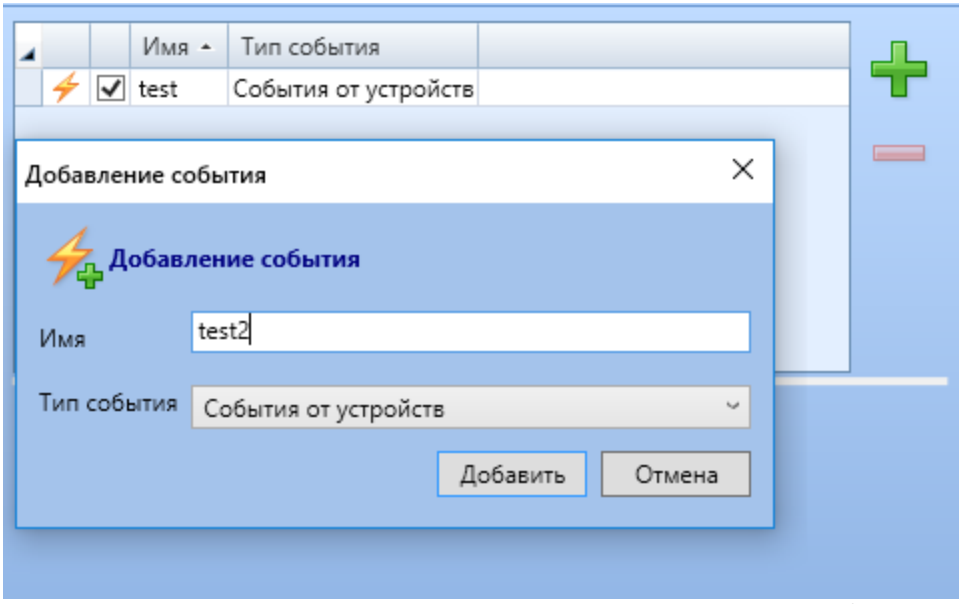
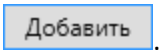


Рисунок 101 - АРМ RusGuard. Модуль Конфигурация системы. Создание нового события

5. Укажите тип события и введите его название. Нажмите на кнопку  .

Название события отобразится в таблице в верхней части экрана. В нижней части экрана отобразятся параметры текущего (выделенного) события. По умолчанию при загрузке экрана отображаются параметры первого события из списка. Первым в списке из нескольких событий отображается последнее добавленное событие. Параметры события настраиваются на двух вкладках: ***Общие*** и ***Сотрудники*** (см. рис. 101).

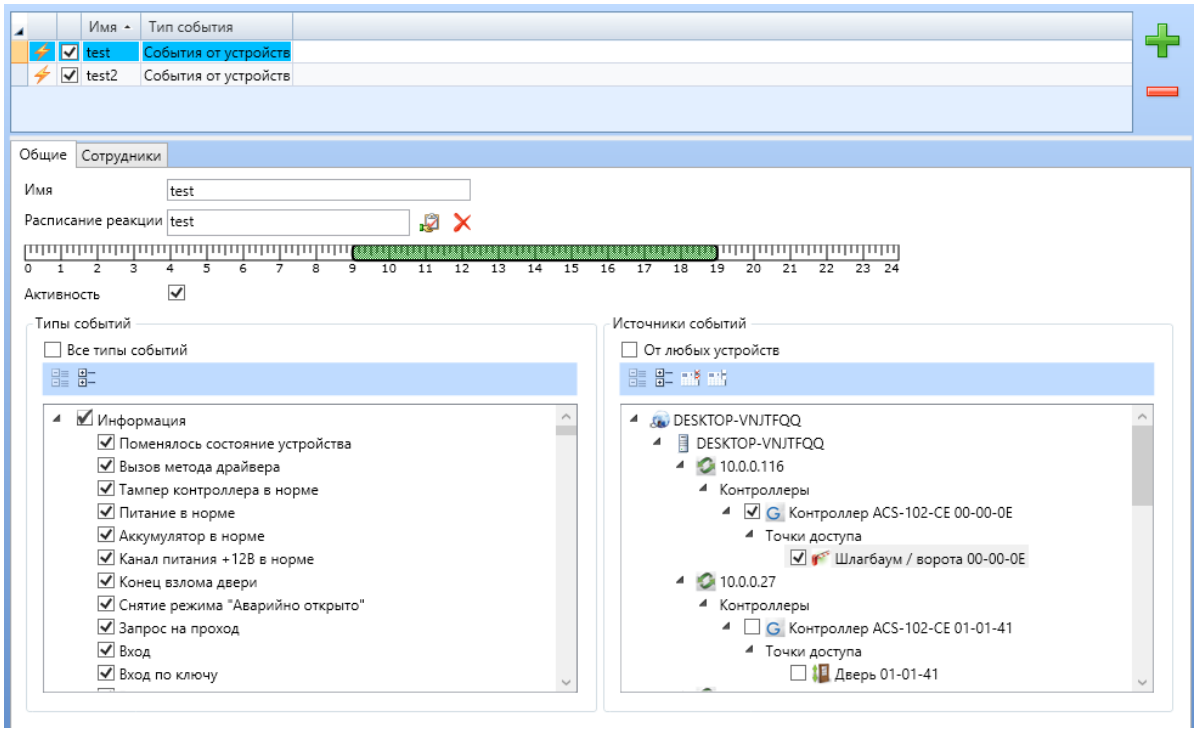
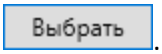


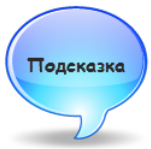
Рисунок 102 - АРМ RusGuard. Модуль Конфигурация системы. Событие в списке. Параметры события

6. Нажмите на кнопку  ***Редактировать*** в верхней панели инструментов, чтобы приступить к редактированию параметров события.
7. Привяжите к событию расписание. Для этого нажмите на кнопку  на вкладке ***Общие***.

Загрузится список созданных расписаний. Если список пуст, необходимо создать расписание 193.

8. Выберите расписание из списка, нажмите на кнопку  .

На вкладке ***Общие*** отобразится название расписания и соответствующая шкала.



Выбрав расписание в списке, вы можете отредактировать интервал, находясь в списке расписаний. Используете для этого шкалу, которая отображается в нижней части списка.

9. Чтобы сделать событие активным, установите флаг ***Активность***.
10. Привяжите к редактируемому событию реакции один или несколько типов системных событий. Для этого выполните следующие действия:

i. В области ***Типы событий*** установите флаг ***Все типы событий*** или выберите нужные типы и подтипы событий в списке ниже (см. рис. 102).

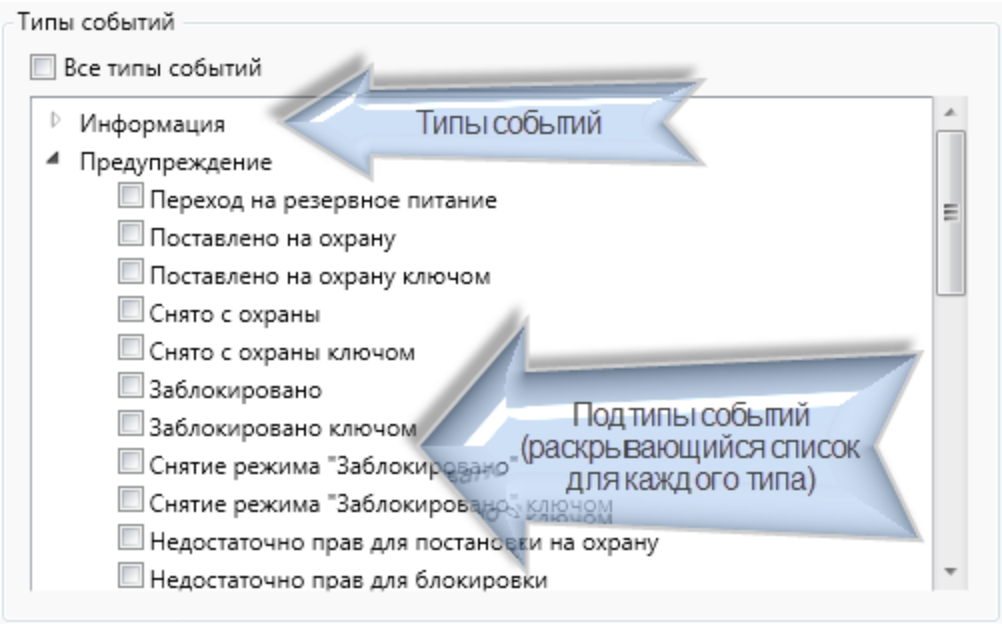


Рисунок 103 - АРМ RusGuard. Модуль Конфигурация системы. Типы системных событий. Настройка

ii. В области ***Источники событий*** установите флаг ***Все устройства***, либо установите флаг напротив названий нужных устройств в списке ниже (см. рис. 103).

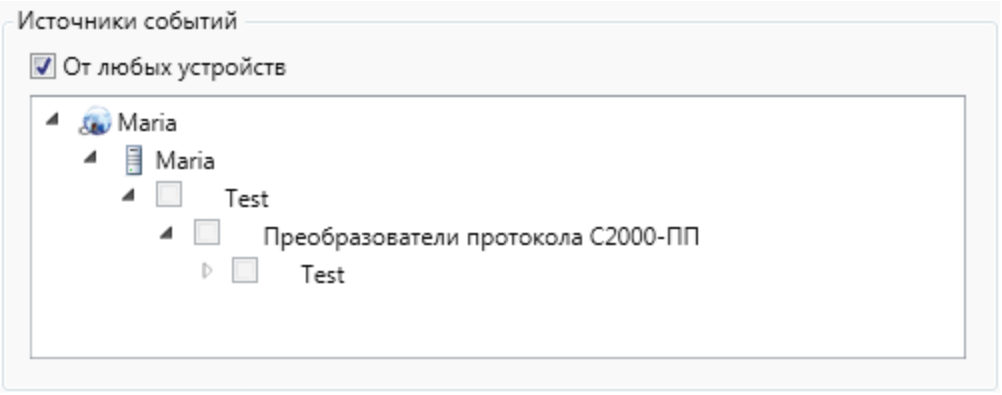


Рисунок 104 - АРМ RusGuard. Модуль Конфигурация системы. Источники событий. Установлен флаг "От любых устройств"

11. Перейдите на вкладку ***Сотрудники*** (см. рис. 104). Здесь пользователь АРМ может указать, с каким сотрудником/ами должны быть связаны действия, привязанные к реакции.

При переходе на вкладку загружается только левая часть экрана. Правая (список сотрудников с возможностью поиска) загружается после выбора группы сотрудников.

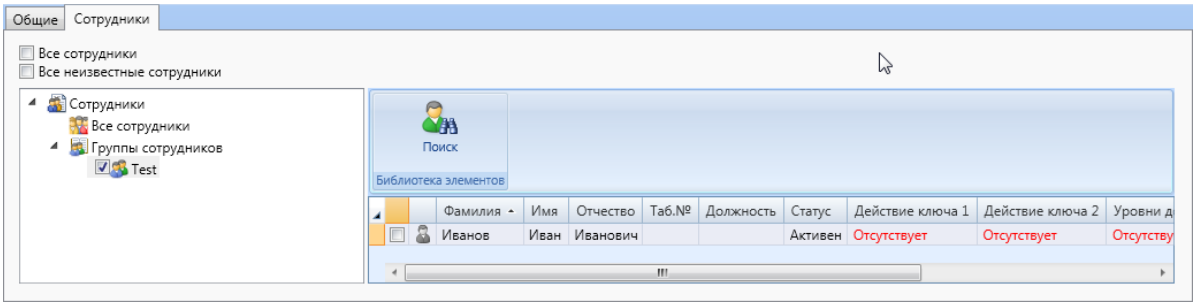


Рисунок 105 - АРМ RusGuard. Модуль Конфигурация системы. Настройка события. Вкладка "Сотрудники"

12. Выполните привязку сотрудников к событию. Для этого выполните одно из следующих действий:

   i. Установите флаг ***Все сотрудники***, чтобы в настраиваемом событии учитывались все сотрудники (например, проход через определенную точку доступа, выбранную в списке устройств).

   ii. Установите флаг ***Все неизвестные сотрудники***, чтобы учитывать действия не зарегистрированных в системе лиц.

   iii. Выполните выбор группы и/или отдельных сотрудников, используя дерево сотрудников в левой части экрана, а также список сотрудников справа (см. рис. выше).

13. Нажмите на кнопку  ***Сохранить*** в верхней панели управления, чтобы завершить настройки события.

Для того чтобы создать действие:

1. Найдите нужную реакцию в иерархическом списке навигационной панели слева.

2. Перейдите в подпункт ***Действия***.

По умолчанию, при первоначальной настройке действий в главном экране отобразится пустой список.

3. Нажмите на кнопку  ***Редактировать*** в верхней панели инструментов.

Активируется кнопка  справа от пустого списка. Если список редактируется не впервые, и в нем уже есть действия, активируется также и кнопка  для удаления действий.

4. Чтобы добавить действие, нажмите на кнопку  .

Загрузится форма ввода действий (см. рис. 105).

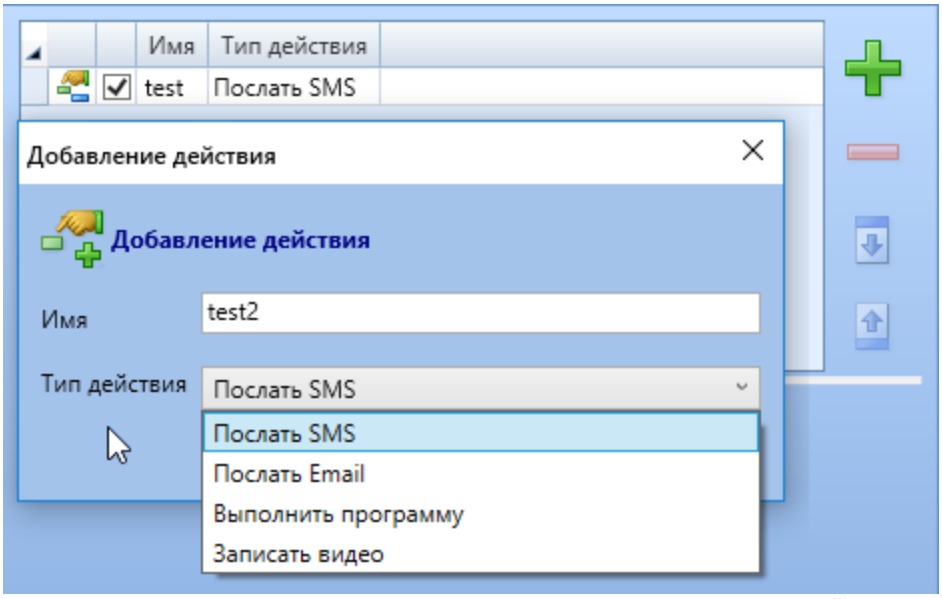
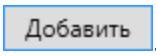


Рисунок 106 - АРМ RusGuard. Модуль Конфигурация системы. Создание нового действия

5. Укажите тип действия (выберите из списка ***Тип действия***) и введите его название (поле ***Имя***). Нажмите на кнопку 

.

Название действия отобразится в таблице в верхней части экрана. В нижней части экрана отобразятся параметры текущего (выделенного) действия, набор полей зависит от выбранного типа действия. По умолчанию при загрузке экрана отображаются параметры первого действия из списка. Первым в списке из нескольких действий отображается последнее добавленное событие. Параметры события настраиваются на двух вкладках: ***Общие*** и ***Сотрудники*** (см. рис. 106).

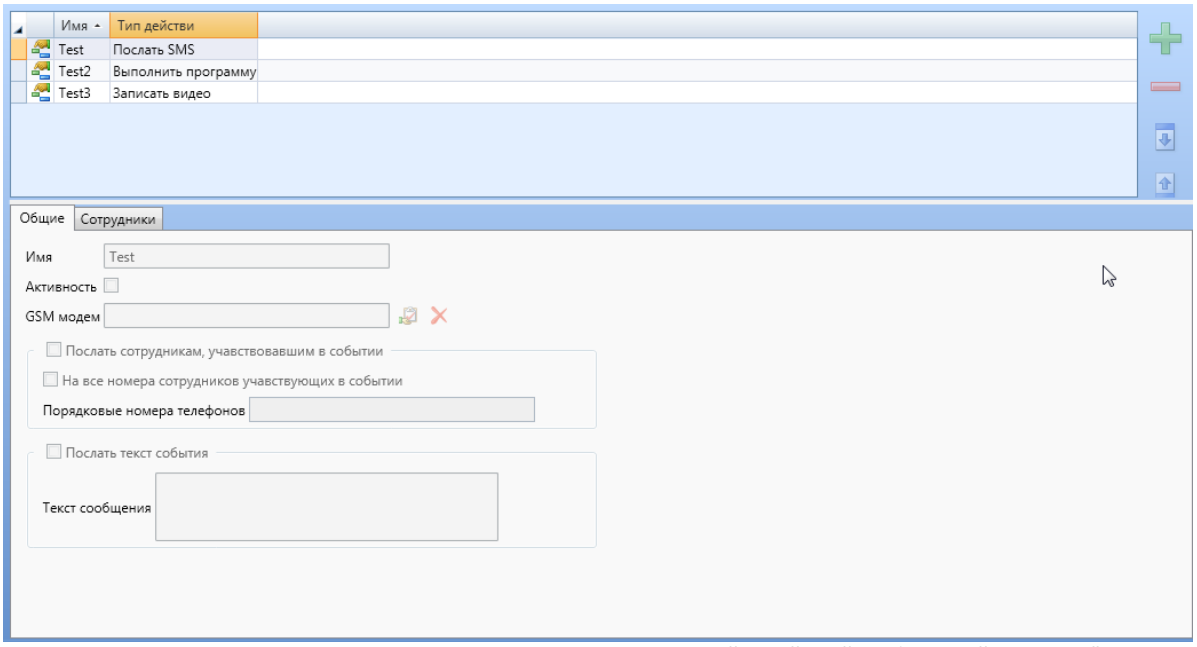


Рисунок 107 - АРМ RusGuard. Модуль Конфигурация системы. Окно настройки действий. Выбрано действие типа "Послать SMS"

6. Выполните настройки для выбранного типа действия.
   - ***Послать SMS*** 201
   - ***Послать Email*** 202
   - ***Записать видео*** 203
   - ***Выполнить программу*** 204
7. Нажмите на кнопку  ***Сохранить*** в верхней панели инструментов, чтобы завершить настройку действия.

Для того чтобы настроить отправку SMS:

1. Создайте действие 199 типа ***Послать SMS***.
2. Заполните поля на вкладке ***Общие*** (открывается по умолчанию) (см. рис. 107).

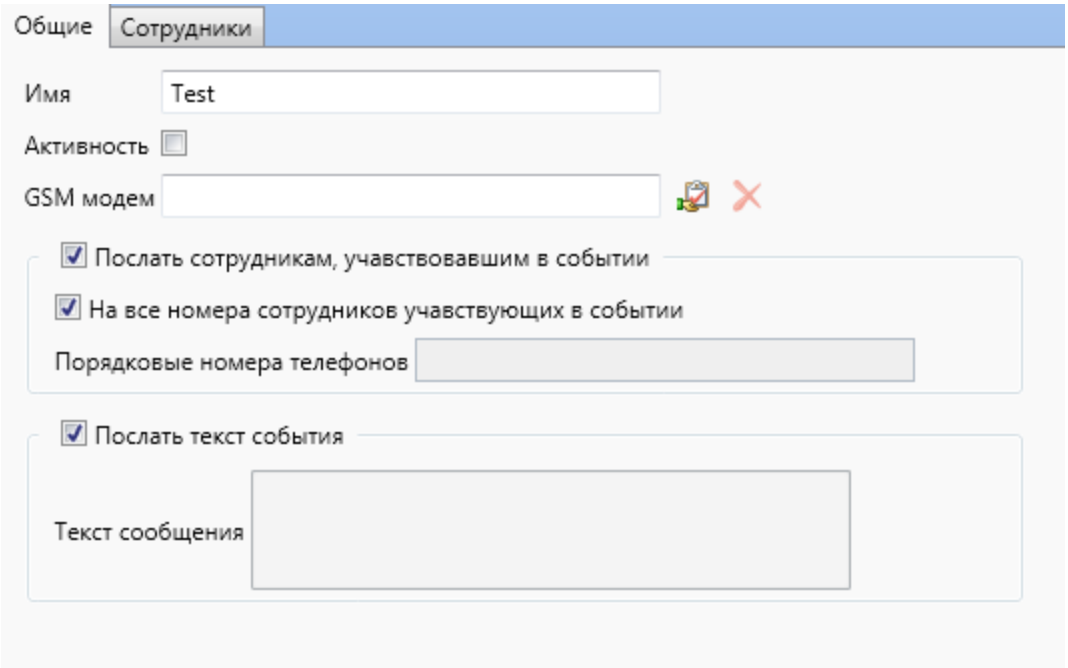


Рисунок 108 - APM RusGuard. Модуль Конфигурация системы. Настройка отправки SMS. Вкладка "Общие"

   i. Установите флаг ***Активность***, чтобы действие выполнялось при наступлении соответствующего события.
   ii. Выберите один из настроенных GSM-модемов 129 (кнопка  для вызова списка);
   iii. Установите флаг ***Послать сотрудникам, участвовавшим в событии***;
   iv. Установите флаг ***На все номера сотрудников, участвующих в событии*** или введите порядковые номера телефонов в соответствующее поле;
   v. Установите флаг ***Послать текст события***, если сообщения должны содержать системное описание события, или введите альтернативный текст в поле ***Текст сообщения***.
3. Перейдите на вкладку ***Сотрудники*** (см. рис. 108). Заполните форму следующим образом:

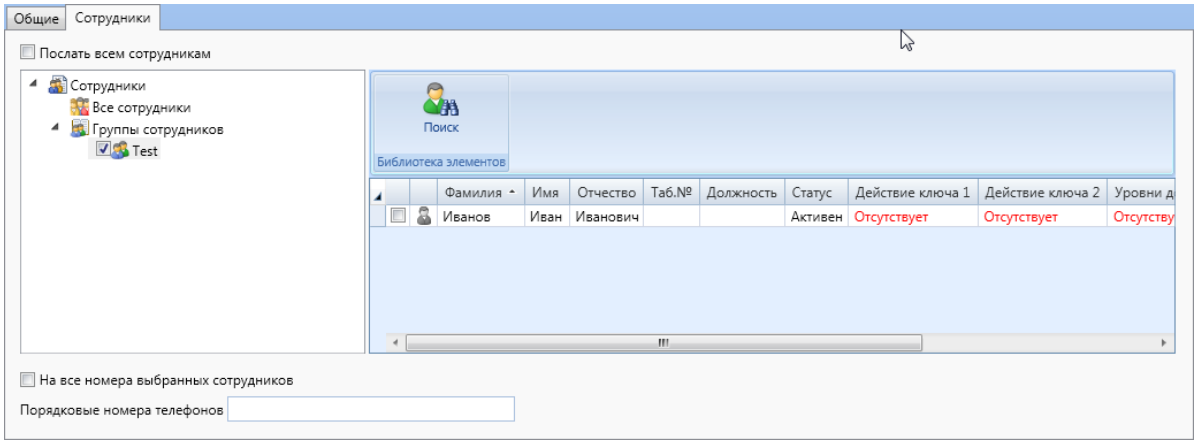


Рисунок 109 - АРМ RusGuard. Модуль Конфигурация системы. Настройка отправки SMS. Вкладка "Сотрудники"

i. Установите флаг ***Послать всем сотрудникам***, если сообщение должны получить все сотрудники. Если сообщение должно быть отправлено определенным лицам, выберите группу в списке ***Сотрудники*** слева, затем найдите нужных сотрудников в списке справа и установите флаги в соответствующих строках.

ii. Установите флаг ***На все номера выбранных сотрудников***, либо укажите порядковые номера телефонов.

4. Чтобы завершить настройку действия, нажмите на кнопку  ***Сохранить*** в панели управления сверху.

Для того чтобы настроить отправку Email:

1. Создайте действие 199 типа ***Послать Email***.

2. Заполните поля на вкладке ***Общие*** (открывается по умолчанию) (см. рис. 109).

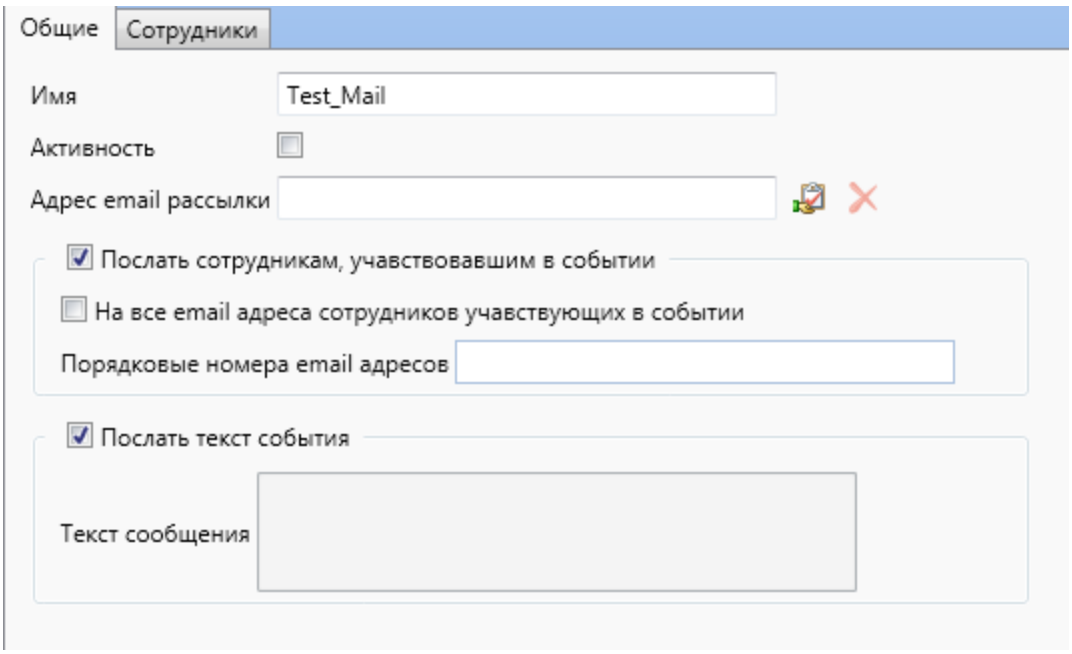


Рисунок 110 - АРМ RusGuard. Модуль Конфигурация системы. Настройка отправки Email. Вкладка "Общие"

i. Установите флаг ***Активность***, чтобы действие выполнялось при наступлении соответствующего события.

ii. Выберите настроенный email-адрес 125, если отправка должна выполняться только на один адрес (кнопка для вызова списка), либо

iii. Установите флаг ***Послать сотрудникам, участвовавшим в событии***;

iv. Установите флаг ***На все email-адреса сотрудников, участвующих в событии*** или введите порядковые адреса электронной почты в соответствующее поле;

v. Установите флаг ***Послать текст события***, если сообщения должны содержать системное описание события, или введите альтернативный текст в поле ***Текст сообщения***.

3. Перейдите на вкладку ***Сотрудники*** (см. рис. 110). Заполните форму следующим образом:

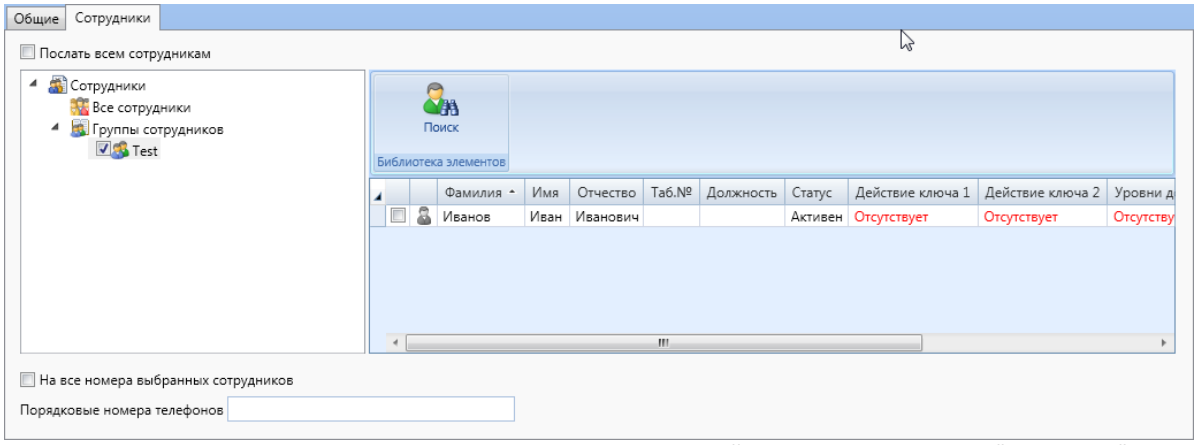


Рисунок 111 - APM RusGuard. Модуль Конфигурация системы. Настройка отправки Email. Вкладка "Сотрудники"

i. Установите флаг ***Послать всем сотрудникам***, если сообщение должны получить все сотрудники. Если сообщение должно быть отправлено определенным лицам, выберите группу в списке ***Сотрудники*** слева, затем найдите нужных сотрудников в списке справа и установите флаги в соответствующих строках.

ii. Установите флаг ***На все номера выбранных сотрудников***, либо укажите порядковые номера адресов.

4. Чтобы завершить настройку действия, нажмите на кнопку ***Сохранить*** в панели управления сверху.

Для того чтобы настроить запись видео:

1. Создайте действие 199 типа ***Записать видео***.

2. Выполните настройку параметров записи видео (см. рис. 111) следующим образом:

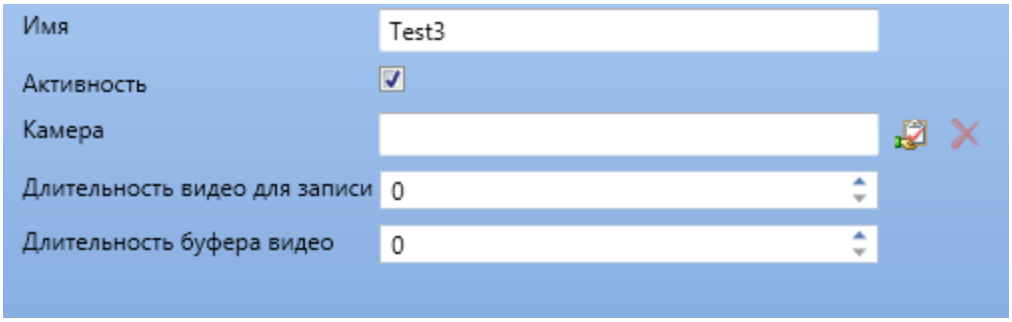


Рисунок 112 - АРМ RusGuard. Модуль Конфигурация системы. Настройка записи видео

i. Установите флаг ***Активность***, чтобы действие выполнялось при наступлении события;

ii. Выберите одну из настроенных в системе камер (кнопка для вызова списка устройств);

iii. Укажите длительность видео в минутах;

iv. Укажите длительность буфера в минутах (т.е. длительность записи с выбранной камеры периода до запуска реакции).

3. Чтобы завершить настройку действия, нажмите на кнопку ***Сохранить*** в панели управления сверху.

Перейдите по ссылке, чтобы подробнее узнать о настройке записи видео событий с камер Ivideon 285.

Для того чтобы настроить выполнение программы:

1. Создайте действие 199 типа ***Выполнить программу***.

2. Введите параметры запуска программы (см. рис. 112) следующим образом:

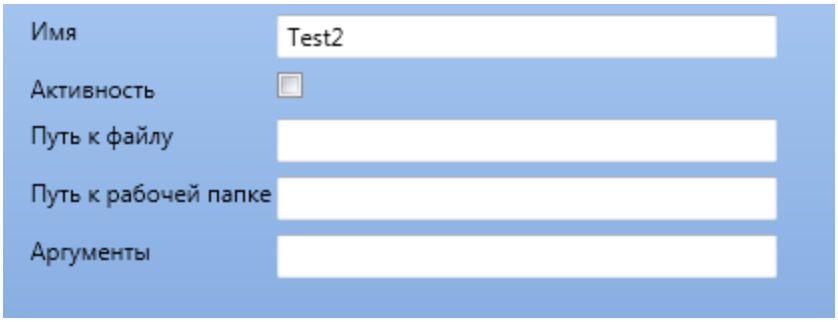


Рисунок 113 - АРМ RusGuard. Модуль Конфигурация системы. Настройка выполнения программы

i. Установите флаг ***Активность***, чтобы действие выполнялось при возникновении события;

ii. Укажите путь к файлу программы (пути указываются с точки зрения сервера).

iii. Укажите путь к рабочей папке с файлами.

iv. Введите аргументы.

3. Чтобы завершить настройку действия, нажмите на кнопку  ***Сохранить*** в панели управления сверху.

Метки

ПО RusGuard обеспечивает возможность гибкого управления правами доступа операторов (пользователей) при помощи меток, которые привязываются к различным сущностям системы .

Метки создаются в модуле ***Конфигурация системы***, а затем привязываются к:

- уровням доступа
- устройствам
- точкам доступа
- группам сотрудников 137
- профилям Mifare 210
- отчетам по УРВ 214

Обратите внимание, что метка не может быть привязана непосредственно к отдельному пользователю. Кроме того, система меток неприменима к Административной группе (встроенная группа). Эта группа не подлежит редактированию. По умолчанию ее члены имеют максимальный уровень доступа (с учетом всех создаваемых меток).

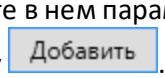
Для того чтобы создать метку:

1. Зайдите в модуль ***Конфигурация системы***.
2. Перейдите в пункт ***Метки*** навигационной панели слева.
3. Щелкните пиктограмму 

в верхней панели управления.

Откроется новое окно ***Добавление метки*** (см. рис. 113).

Рисунок 114 - АРМ RusGuard. Модуль Конфигурация системы. Добавление метки

4. Введите в нем параметры метки (название, описание -если требуется). Нажмите на кнопку 

.

Созданная метка отобразится в списке меток (см. рис. 114).

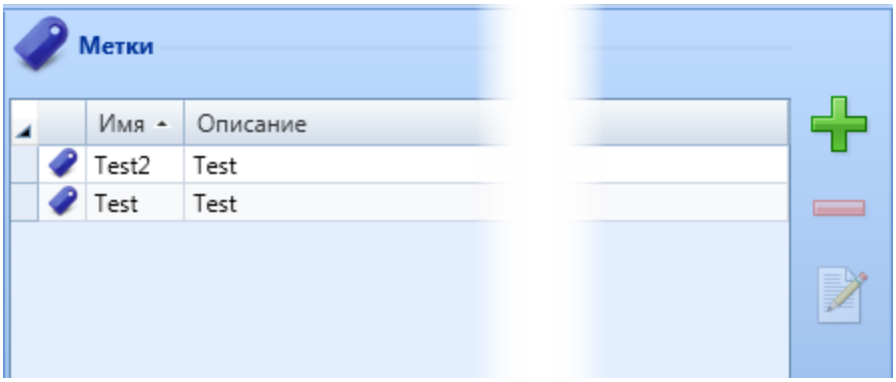


Рисунок 115 - APM RusGuard. Модуль Конфигурация системы. Список меток

В дальнейшем вы можете удалять метки ( ), редактировать их ( ) и добавлять новые ( ).

О привязке меток к элементам СКУД см. в соответствующих разделах инструкции:

- Привязка метки к устройству 90
- Привязка метки к точке доступа 113
- Привязка метки к уровню доступа см. здесь 69 (создание уровня доступа) и здесь 153 (редактирование, привязка меток).
- Привязка метки к отчету 224.
- Привязка метки к профилю Mifare 210.
- Привязка метки к группе сотрудников см. здесь 69 (создание группы) и здесь 135 (настройка меток для группы).
- Настройка полномочий группы с использованием меток 174.

Об использовании меток для разграничения доступа см. также здесь 262.

Шаблоны пропусков

APM "RusGuard" позволяет создавать макеты пропусков. Макет создается в модуле ***Конфигурация системы***, при этом к нему могут привязываться поля карточки сотрудника.

Готовый шаблон используется в модуле ***Конфигурация СКУД***, где, из базы данных сотрудников, могут быть распечатаны пропуска (один или несколько).

Количество шаблонов не ограничено возможностями ПО, однако зависит от условий лицензии. Ненужные или устаревшие шаблоны могут быть удалены в любой момент.

Для того чтобы создать шаблон пропуска:

1. Зайдите в модуль ***Конфигурация системы***.
2. Установите курсор на пункт ***Шаблоны пропусков*** навигационной панели слева.
3. Щелкните мышью пиктограмму 

в верхней панели управления.

4. Заполните поля формы для заведения нового шаблона и сохраните его.
Созданный шаблон отобразится в иерархическом списке левой навигационной панели.

5. Перейдите к созданному шаблону в навигационной панели слева.
Откроется редактор шаблона, где вы можете настроить его оформление (см. рис. 115).

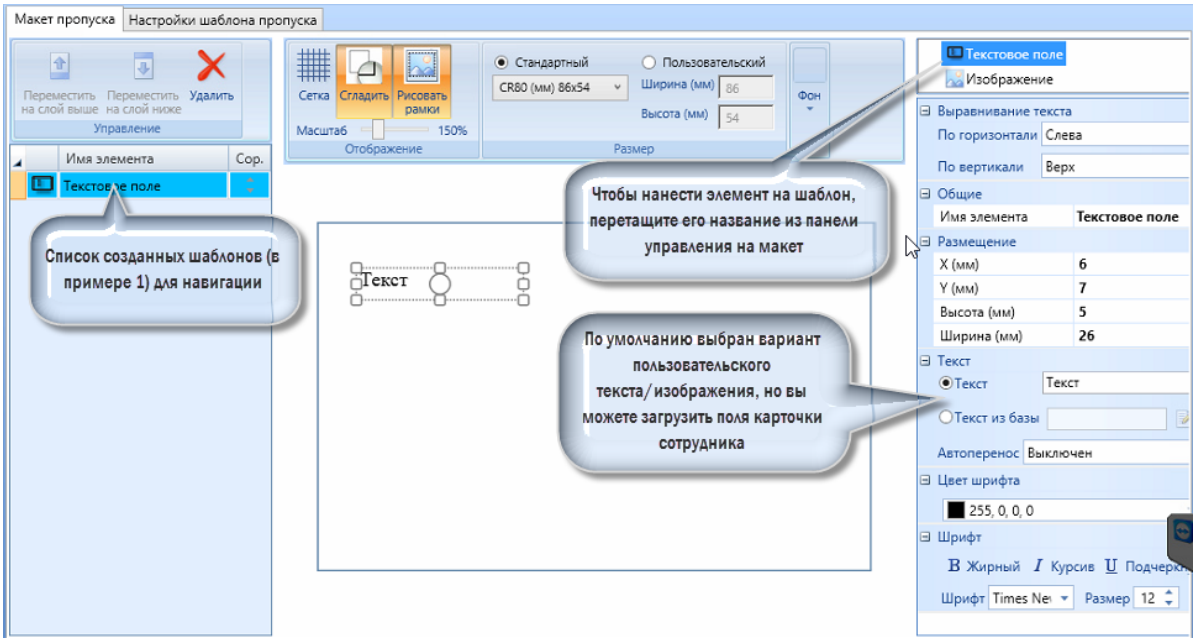


Рисунок 116 - АРМ RusGuard. Модуль Конфигурация системы. Редактор макета пропуска.

6. Сформируйте макет. Чтобы начать редактирование, необходимо щелкнуть пиктограмму () в верхней панели инструментов.

Обратите внимание на возможность привязки к макету полей карточки сотрудника. Они могут быть привязаны как к текстовому полю, так и к изображению. Чтобы использовать поля из карточки сотрудника:

a. Установите флаг ***Текст из базы*** или ***Изображение из базы***.

b. Щелкните пиктограмму справа от флага.

Загрузится список полей карточки сотрудника или фотографий. Обратите внимание, что загружаются не значения полей, а именно сами поля (см. рис. 116).

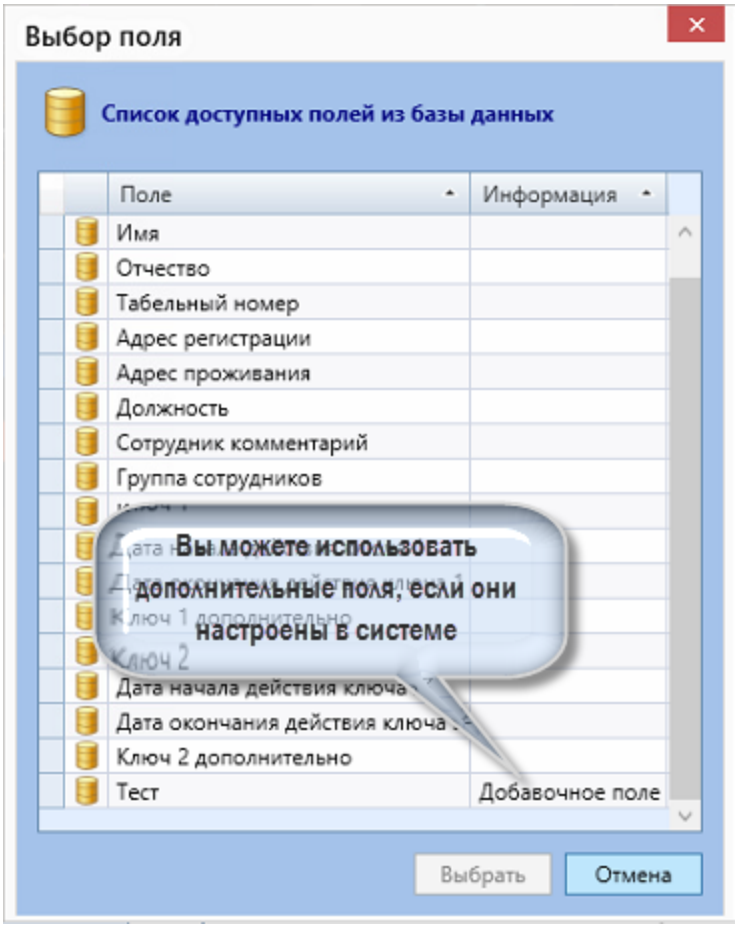


Рисунок 117 - APM RusGuard. Модуль Конфигурация системы. Выбор поля сотрудника

c. Выберите нужное поле/фото. Обратите внимание, что в список попадают и дополнительные поля, если они заведены в системе.

7. Закончив формировать макет, сохраните его ( ).

В дальнейшем вы можете использовать шаблон для печати пропусков из базы данных сотрудников модуля ***Конфигурация СКУД*** 135.

Настройка Mifare

Настройка профилей Mifare позволяет выполнять эмиссию карт Mifare Classic и Mifare Plus. Обратите внимание, что для работы с этим блоком пользователь АРМ должен обладать соответствующими правами 137.

Экран ***Ключи по умолчанию*** содержит исходные (как правило, заводские ключи). Редактировать ключи по умолчанию не следует, если используются новые карты. Для карт бывших в употреблении могут быть другие исходные настройки.

Экран ***Профили Mifare*** позволяет создавать так называемые "профили", то есть шаблоны настроек эмиссии. Для каждого профиля настраиваются и сохраняются следующие параметры:

- тип карты (Classic и/или Plus) и уровень защиты, если используется карта Plus;
- распределение прав между ключами А и Б карточки;
- режим эмиссии (запись на все секторы карты или на определенный, номер которого сохраняется в профиле);
- служебные ключи для карт Plus (рекомендуется использовать настройку по умолчанию);
- режим аутентификации;
- права доступа для ключей А и Б.

Система поддерживает неограниченное количество профилей, но по стандартной лицензии доступен только один.

Для того чтобы создать профиль Mifare:

1. Зайдите в модуль ***Конфигурация оборудования***.
2. В навигационной панели слева выберите Настройки ***Mifare*** > ***Профили Mifare***.
3. Щелкните пиктограмму 

. Откроется форма для создания карточки профиля (см. рис. 117).

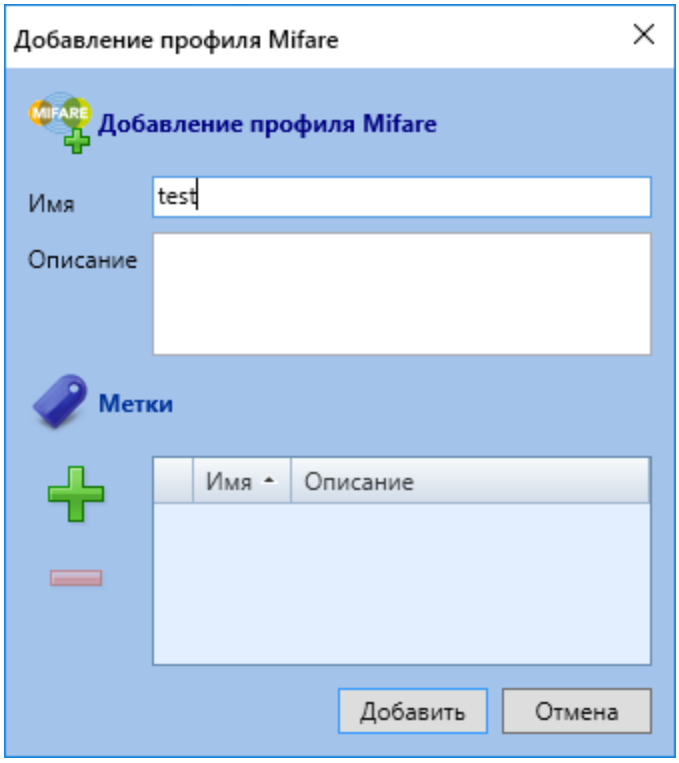


Рисунок 118 - APM RusGuard. Модуль Конфигурация системы. Создание нового профиля Mifare.

4. Введите название профиля. Если необходимо, введите описание. Нажмите на кнопку Добавить. Название нового профиля отобразится в навигационной панели слева.
5. Выберите созданный профиль. По умолчанию откроется вкладка ***Профиль***.
6. Щелкните пиктограмму в верхней панели управления, чтобы отредактировать параметры профиля 211.
7. Задайте параметры профиля. Обратите внимание, что в большинстве случаев рекомендуется минимально менять настройки по умолчанию.
8. Сохраните настройки профиля ( ).

Созданный профиль Mifare станет доступен для привязки к устройствам в модуле ***Конфигурация оборудования*** 79.

Особенности настройки профиля

В верхней части окна настройки профиля настраиваются ключи для выбранного типа карт (Classic/Plus) (см. рис. 118). Необходимо указать:

- Значение ключа A и B;

Вы можете указать значения вручную (щелкните чтобы отобразить текущее значение ключа) или сформировать автоматически ( ).

Прежде чем сгенерировать значение ключа автоматически, обязательно откройте его значение ( ), чтобы записать его.

- Полномочия каждого из ключей (ключ эмиссии (используемый для доступа), ключ контроллера);
- Режим эмиссии (все сектора или выбранный);
- Для карт Mifare Plus также настраиваются служебные ключи и уровень защиты (поддерживается SL1 (для переходных периодов)/SL3).

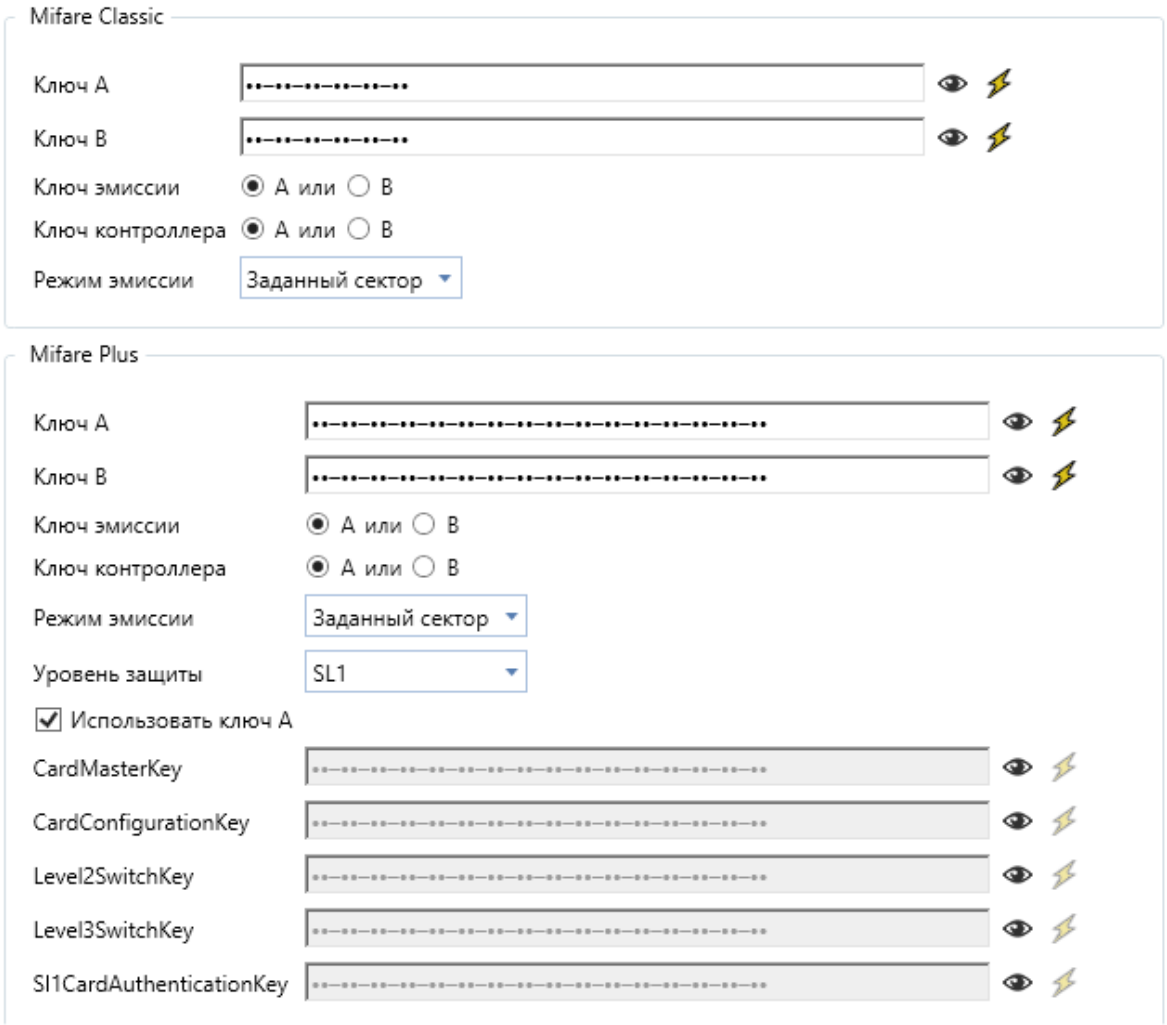


Рисунок 119 - АРМ RusGuard. Модуль Конфигурация системы. Настройка параметров эмиссии

В нижней части экрана (см. рис. 119) настраивается:

- сектор, куда записывается ключ;
- тип аутентификации (рекомендуется использовать режим по умолчанию, остальные режимы могут использоваться в рамках переходных периодов, но обеспечивают более низкий уровень защиты);

- в таблице ***Данные*** определяются права каждого из ключей для работы с данными карты;
- в таблице ***Ключи*** настраиваются права ключей на изменение самих ключей (не рекомендуется менять настройки по умолчанию).

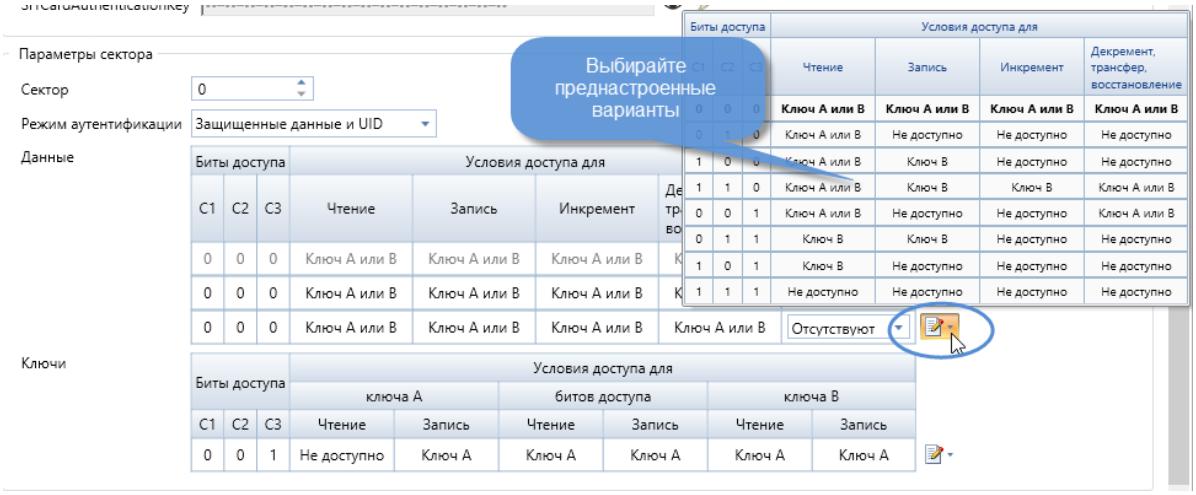


Рисунок 120 - APM RusGuard. Модуль Конфигурация системы. Настройка параметров безопасности

Отчеты

Доступ к отчетам может выполняться двумя способами:

- Через модуль ***Отчеты*** АРМ;
- Через веб-интерфейс, т.е. путем доступа непосредственно на Сервер отчетов.

Подробнее о настройке сервера отчетов см. в разделе *Установка сервера RusGuard* 31.

Функции модуля АРМ практически полностью совпадают с функциями Севера отчетов.

Внимание: для того чтобы в отчетах корректно отображались все данные Системы по учету рабочего времени, необходимо до начала работы с ними выполнить ряд предварительных настроек в других модулях АРМ (см. рис. 120).

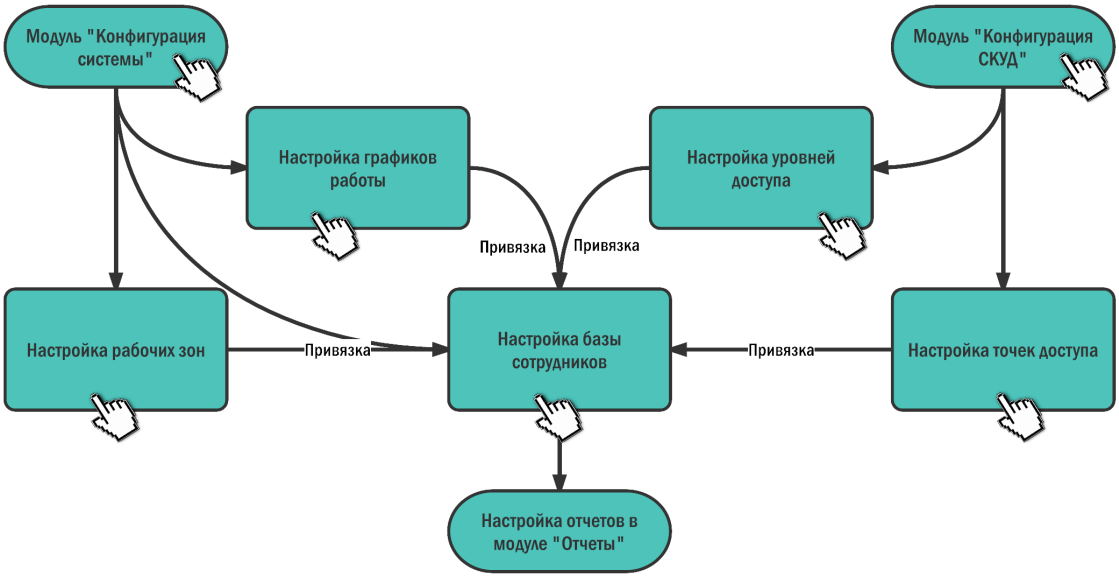


Рисунок 121 - Необходимые предварительные настройки (используйте ссылки для перехода в соответствующие разделы документа)

Типы отчетов

Модуль ***Отчеты*** АРМ RusGuard позволяет загружать отчеты о функционировании СКУД с сервера отчетов в интерфейс АРМ. Для удобства использования создается несколько типов отчетов (см. рис. 121):

- Аудит действий операторов
- Картотека сотрудников
- Контроль посещаемости
- Кто прописан в контроллер
- Статистика проходов
- Учет посещаемости 1
- Учет посещаемости 1, расширенный

- Учет посещаемости 2
- Опоздания
- Отработанное время
- Отработанно время, расширенный
- Системные события
- Табель 13
- Уход раньше времени

Часть из этих отчетов строится по стандартному шаблону и не предполагает возможности создания пользовательских вариантов (стандартные 217), однако ряд отчетов (настраиваемые 224) дают такую возможность.

В каждом отчете предусмотрены фильтры, кроме того, для некоторых отчетов могут быть сформированы и сохранены пользовательские настройки.

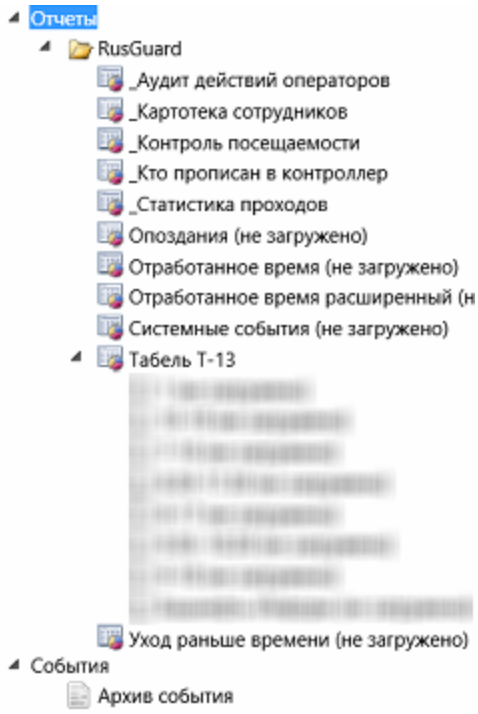
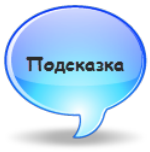


Рисунок 122 - Список отчетов в левой навигационной панели ПО



Если вы используете Сервер отчетов для доступа к отчетам ПО RusGuard, вы можете настроить параметры по умолчанию для каждого из отчетов. Для этого раскройте список отчетов на сервере, выделите нужный отчет (установите на него курсор, так, чтобы отобразилась стрелка, см. рис. 122), раскройте контекстное меню (щелчок по стрелке),

выберите пункт ***Управление параметрами (Manage)*** и установите режим использования параметров по умолчанию (см. рис. 123). Установленные параметры также будут применены в АРМ, если редактируется один из стандартных 217 отчетов.

Также панель настройки параметров отчета можно скрыть при его отображении в АРМ или на Сервере отчетов ( ).

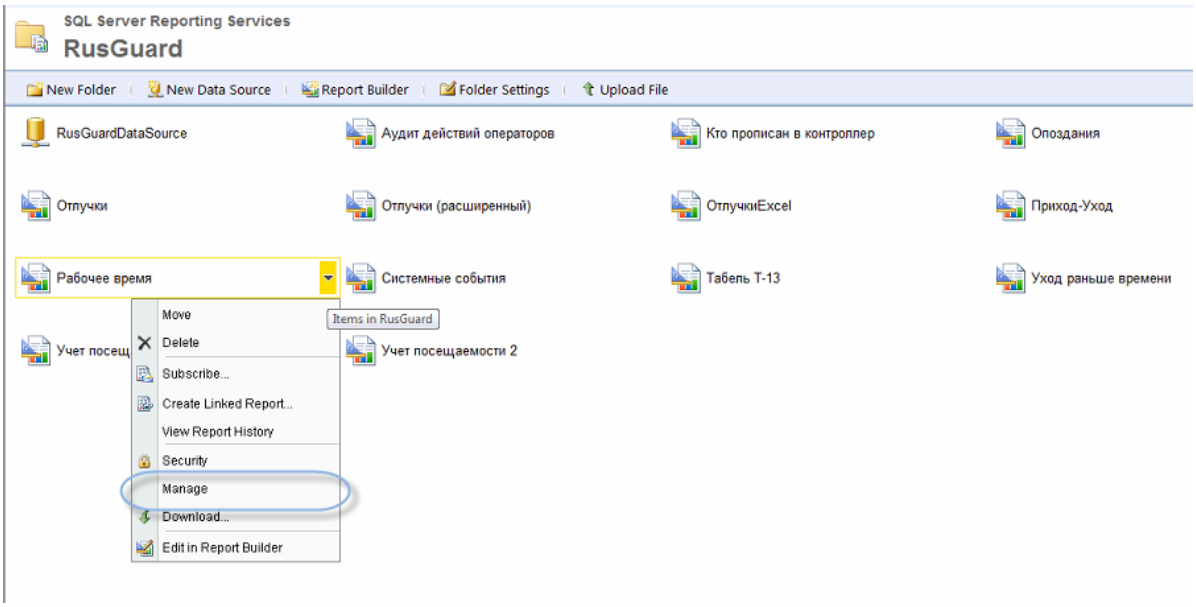


Рисунок 123 - Список отчетов на Сервере отчетов, раскрыто контекстное меню для управления параметрами

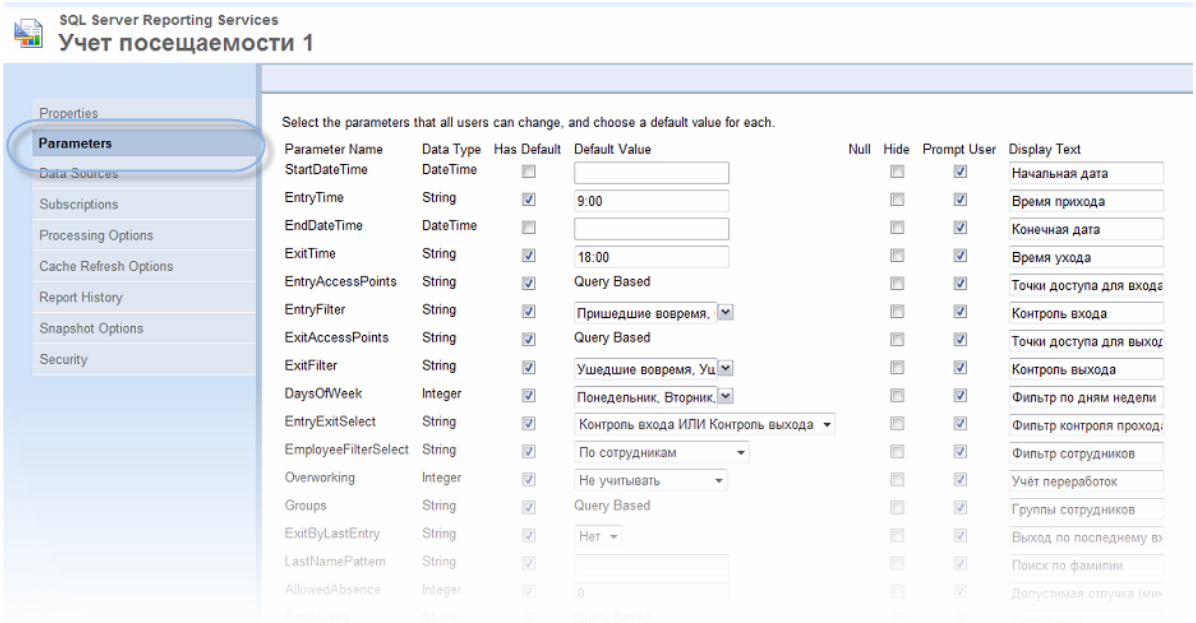


Рисунок 124 - Настройка значений полей по умолчанию на Сервере отчетов

Стандартные отчеты

Отчеты, описанные в подразделах ниже, формируются на основе системных шаблонов, однако к ним можно применить ряд фильтров. О возможностях применения фильтров для отчетов по учету рабочего времени (УРВ) см. здесь.

Кроме того, каждый из готовых отчетов может быть экспортирован на локальное устройство в нужном формате.

Выгрузка отчета

APM RusGuard позволяет выгружать готовые отчеты в следующих форматах:

- XML-файл с данными отчета;
- CSV (разделитель - запятая);
- PDF;
- MHTML;
- MS Excel (`.xls`);
- TIFF (графический файл);
- MS Word (`.doc`).

Для того чтобы выгрузить отчет:

1. Сформируйте отчет (примените фильтры, если это требуется).
2. Нажмите на кнопку  .
   Раскроется список доступных форматов.
3. Щелкните левой кнопкой мыши по нужному формату.
   Система начнет процесс подготовки выгрузки, затем предложит локально сохранить файл выбранного формата.
4. Выполните сохранение (стандартная процедура ОС Windows).

Аудит действий операторов

По умолчанию при загрузке отчета из левой панели навигации в главном экране отображаются все данные о действиях операторов за прошедшие сутки (см. рис. 124).

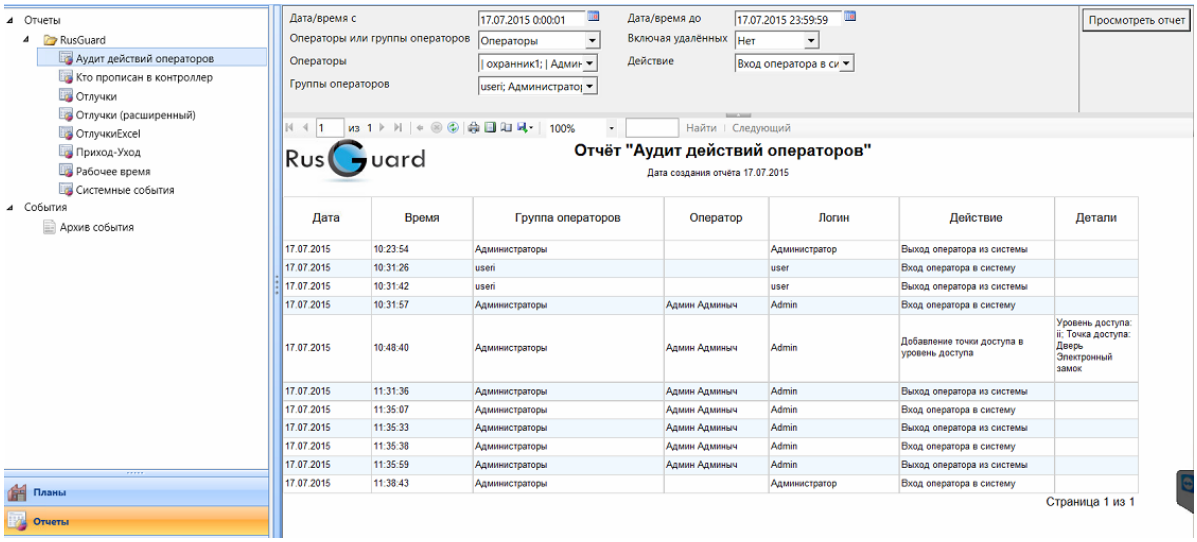


Рисунок 125 - АРМ RusGuard. Модуль Отчеты. Аудит действий операторов

Пользователь может:

- Отфильтровать статистику по одному или нескольким параметрам;
- Выгрузить отчет в одном из поддерживаемых форматов;
- Выполнить поиск.

Также интерфейс предусматривает ряд служебных функций (вывод на печать, настройка формата, обновление и т.д.).

Построение отчета

Для того чтобы построить и отфильтровать отчет:

1. Загрузите отчет.
2. Используя поля в верхней части главного экрана, отфильтруйте данные по одному или нескольким следующим параметрам:
   - Начальная и/или конечная дата
   - Оператор/группа операторов (вы можете включить данные об удаленных операторах)
   - Действие (см. рис. 125)

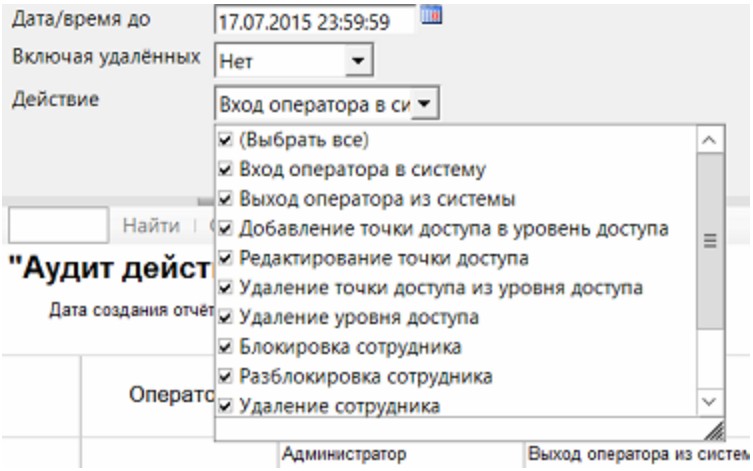


Рисунок 126 - APM RusGuard. Модуль Отчеты. Аудит действий операторов. Список действий, попадающих в отчет

3. Нажмите на кнопку Просмотреть отчет.

Подсказки:

Область ввода параметров фильтрации можно скрыть. Для этого щелкните мышью по кнопке на линии, разделяющей области центрального экрана.

Чтобы сбросить фильтр, выйдите из модуля и зайдите в него снова.

Картотека сотрудников

По умолчанию при загрузке отчета из левой панели навигации в главном экране отображается список сотрудников на текущую дату (см. рис. 126).

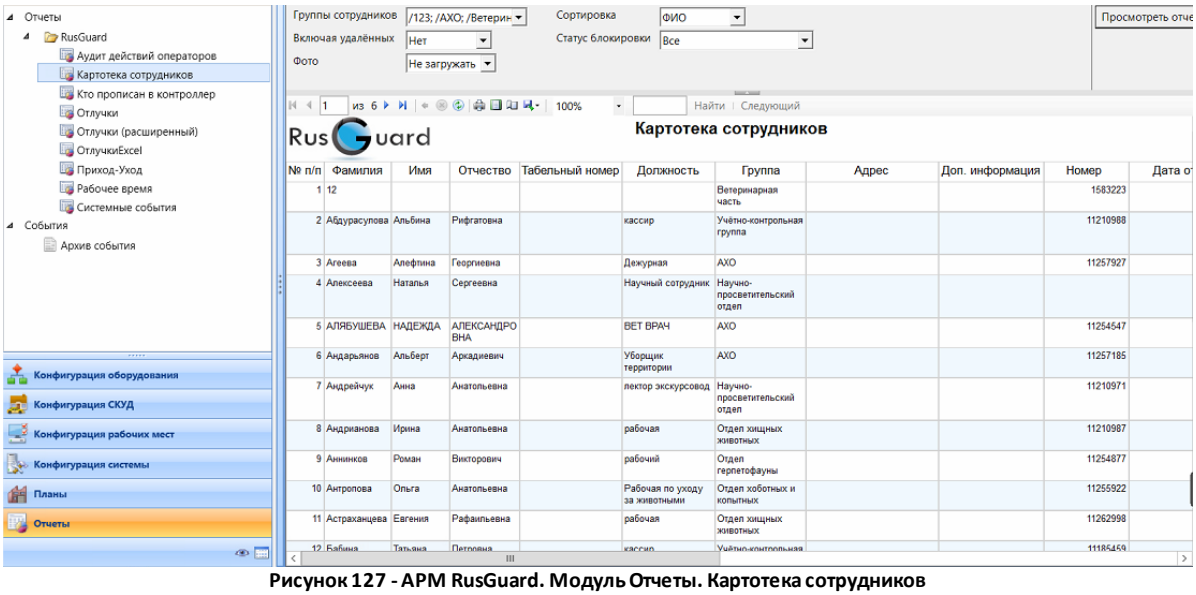


Рисунок 127 - APM RusGuard. Модуль Отчеты. Картотека сотрудников

Пользователь может:

- Отфильтровать отчет по одному или нескольким параметрам (принадлежность к группе, удален или нет, статус блокировки);
- Отсортировать отчет по одному из полей;
- Выгрузить отчет в одном из поддерживаемых форматов;
- Выполнить поиск.

Также интерфейс предусматривает ряд служебных функций (вывод на печать, настройка формата, обновление и т.д.).

Кто прописан в контроллер

По умолчанию при загрузке отчета из левой панели навигации в главном экране отображается список сотрудников, прописанных в выбранный контроллер (см. рис. 127).

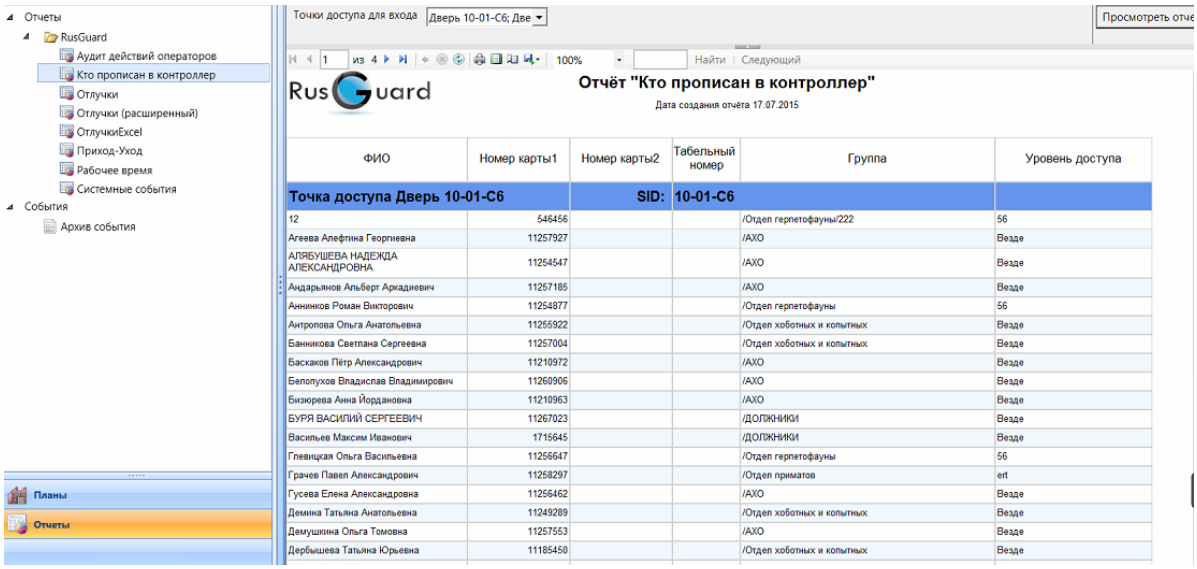


Рисунок 128 - АРМ RusGuard. Модуль Отчеты. Кто прописан в контроллер

Для настройки предусмотрен один фильтр: точка доступа

Также интерфейс предусматривает ряд служебных функций (вывод на печать, настройка формата, обновление и т.д.).

Построение отчета

Для того чтобы построить и отфильтровать:

1. Загрузите отчет.
2. Выберите точку доступа, используя список в верхней части экрана.
3. Нажмите на кнопку Просмотреть отчет.

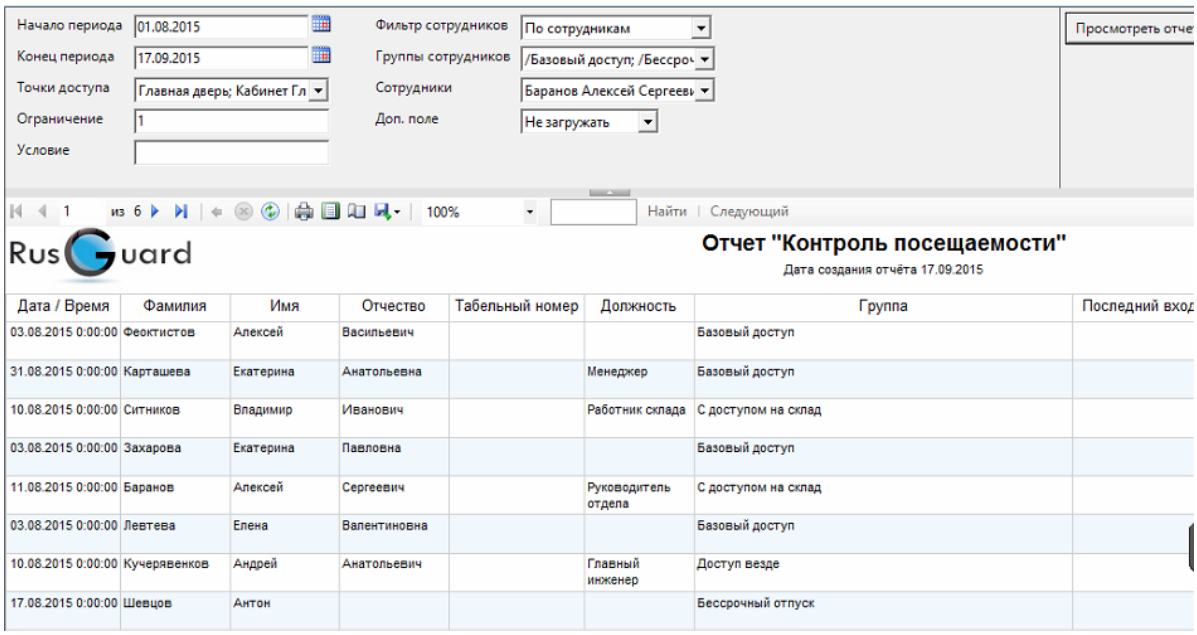
Подсказки:

Область ввода параметров фильтрации можно скрыть. Для этого щелкните мышью по кнопке на линии, разделяющей области центрального экрана.

Чтобы сбросить фильтр, выйдите из модуля и зайдите в него снова.

Контроль посещаемости

По умолчанию при загрузке отчета из левой панели навигации в главном экране отображаются все данные о посещаемости за указанный период (см. рис. 128). По умолчанию в обоих полях периода установлена текущая дата.



Дата / Время	Фамилия	Имя	Отчество	Табельный номер	Должность	Группа	Последний вход
03.08.2015 0:00:00	Феоктистов	Алексей	Васильевич			Базовый доступ	
31.08.2015 0:00:00	Карташева	Екатерина	Анатольевна		Менеджер	Базовый доступ	
10.08.2015 0:00:00	Ситников	Владимир	Иванович		Работник склада	С доступом на склад	
03.08.2015 0:00:00	Захарова	Екатерина	Павловна			Базовый доступ	
11.08.2015 0:00:00	Баранов	Алексей	Сергеевич		Руководитель отдела	С доступом на склад	
03.08.2015 0:00:00	Левтева	Елена	Валентиновна			Базовый доступ	
10.08.2015 0:00:00	Кучерявенков	Андрей	Анатольевич		Главный инженер	Доступ везде	
17.08.2015 0:00:00	Шевцов	Антон				Бессрочный отпуск	

Рисунок 129 - APM RusGuard. Модуль Отчеты. Контроль посещаемости

Пользователь может:

- Отфильтровать статистику по одному или нескольким параметрам;
- Выгрузить отчет в одном из поддерживаемых форматов;
- Выполнить поиск.

Также интерфейс предусматривает ряд служебных функций (вывод на печать, настройка формата, обновление и т.д.).

Построение отчета

Для того чтобы построить и отфильтровать отчет:

1. Загрузите отчет.
2. Используя поля в верхней части главного экрана, отфильтруйте данные по одному или нескольким следующим параметрам:
   - Начальная и/или конечная дата периода отчетности;
   - Сотрудники/группы сотрудников;
   - Точки доступа;
   - Интервал допустимого пропуска отметок (поле ***Ограничение***). Указывается в днях. Например, если ввести "2", в отчет попадают только те, кто не отмечался более 2-х дней. Обратите внимание, что поле не может быть пустым. По умолчанию введено значение "1";

- Дополнительные поля (Доп. поле) принимает значения из дополнительных полей карточки сотрудника;
- Условия позволяют накладывать дополнительные ограничения на выборку сотрудников/групп.

3. Нажмите на кнопку Просмотреть отчет.

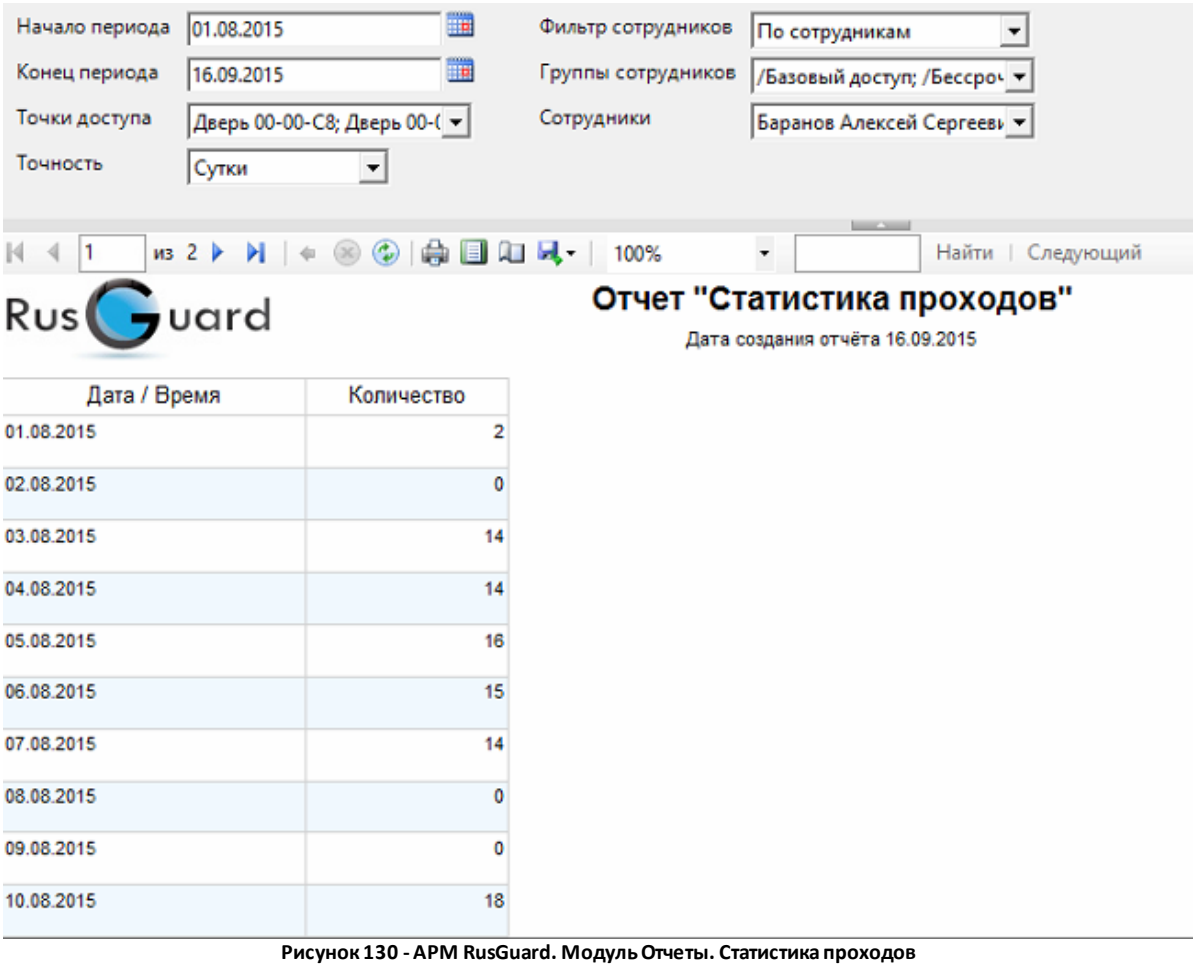
Подсказки:

Область ввода параметров фильтрации можно скрыть. Для этого щелкните мышью по кнопке на линии, разделяющей области центрального экрана.

Чтобы сбросить фильтр, выйдите из модуля и зайдите в него снова.

Статистика проходов

Отчет отображает количество проходов черз точки доступа на каждые сутки (по умолчанию) выбранного периода (см. рис. 129).



Дата / Время	Количество
01.08.2015	2
02.08.2015	0
03.08.2015	14
04.08.2015	14
05.08.2015	16
06.08.2015	15
07.08.2015	14
08.08.2015	0
09.08.2015	0
10.08.2015	18

Рисунок 130 - АРМ RusGuard. Модуль Отчеты. Статистика проходов

Пользователь может:

- Отфильтровать статистику по одному или нескольким параметрам;

- Выгрузить отчет в одном из поддерживаемых форматов;
- Выполнить поиск.

Также интерфейс предусматривает ряд служебных функций (вывод на печать, настройка формата, обновление и т.д.).

Обратите внимание, что в конце отчета, на последней странице, отображается его вариант в виде графика (см. рис. 130).

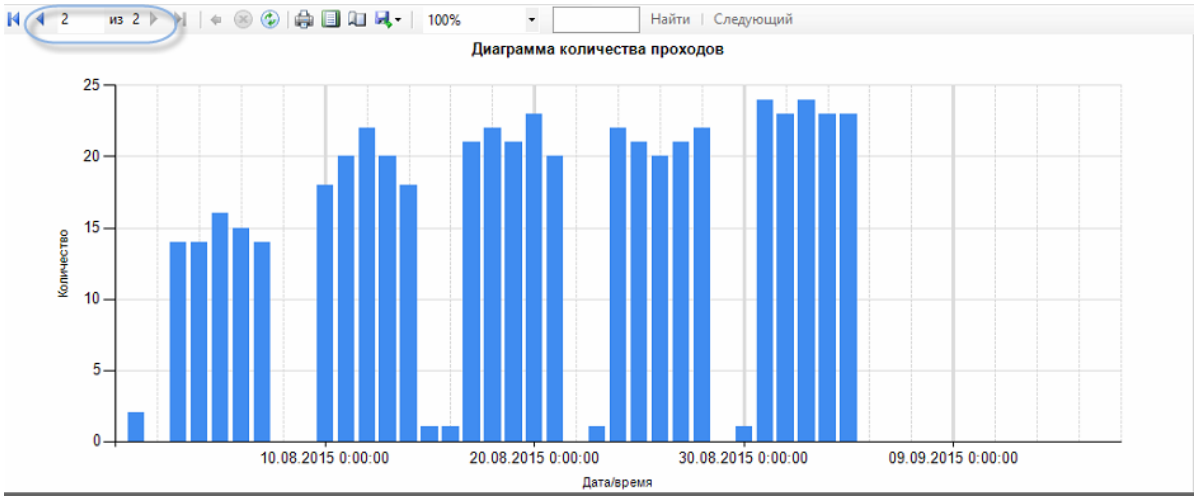


Рисунок 131 - APM RusGuard. Модуль Отчеты. Статистика проходов. График

Построение отчета

Для того чтобы построить и отфильтровать отчет:

1. Загрузите отчет.
2. Используя поля в верхней части главного экрана, отфильтруйте данные по одному или нескольким следующим параметрам:
   - Начальная и/или конечная дата
   - Сотрудники
   - Группы сотрудников
   - Точки доступа
   - Точность (по умолчанию, сутки)
3. Нажмите на кнопку Просмотреть отчет.

Подсказки:

Область ввода параметров фильтрации можно скрыть. Для этого щелкните мышью по кнопке на линии, разделяющей области центрального экрана.

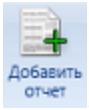
Чтобы сбросить фильтр, выйдите из модуля и зайдите в него снова.

Настраиваемые отчеты

Настраиваемые отчеты в ПО RusGuard имеют несколько иной интерфейс ("мастер настройки отчета"), который позволяет пользователю создавать и сохранять любое количество вариантов определенного отчета, управляя доступными параметрами.

Также для каждого из формируемых пользователем отчетов предусмотрен стандартный набор фильтров (см. здесь о возможностях фильтрации отчетов по УРВ), доступный после формирования самого отчета.

Начало процедуры создания версии отчета при помощи мастера настройки стандартное:

1. Перейдите к нужному типу отчета. Например, ***Системные события***.
2. Щелкните пиктограмму в верхней панели управления 

. Откроется диалоговое окно (см. рис. 131).

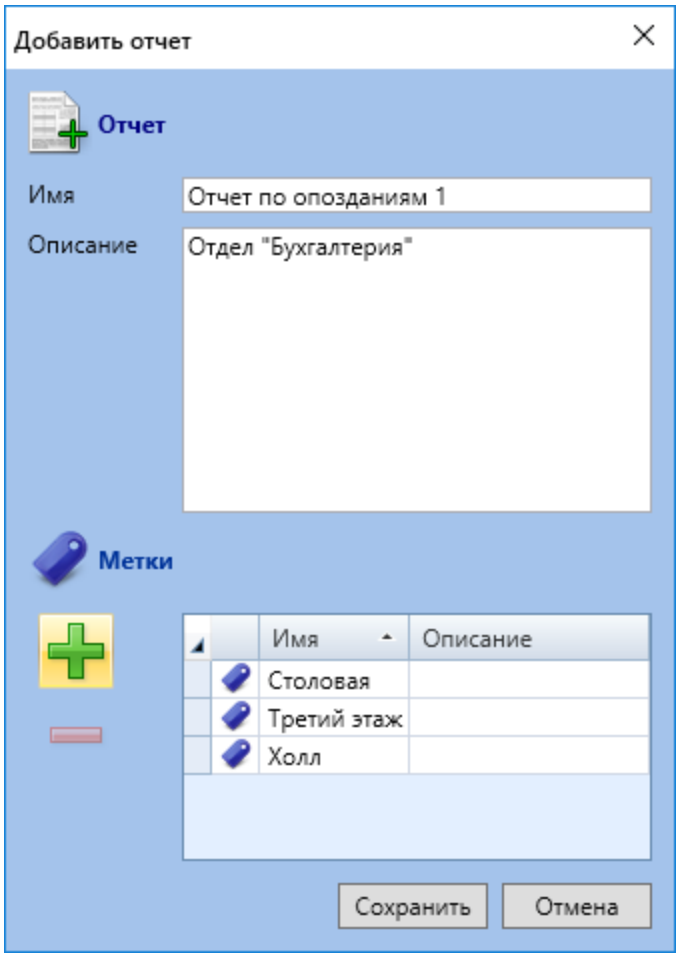


Рисунок 132 - Создание варианта отчета. Добавить отчет

3. Введите название и описание отчета в диалоговом окне. Обратите внимание, что для создания варианта отчета по УРВ доступны метки. В зависимости от привязанных к отчету меток определяются права доступа к отчету пользователей АРМ (см. рис. 132). В примере на иллюстрации показано, что пользователи редактируемой группы

имеют возможность создавать и читать отчеты без меток, создавать, читать, редактировать и удалять отчеты с меткой "Холл".

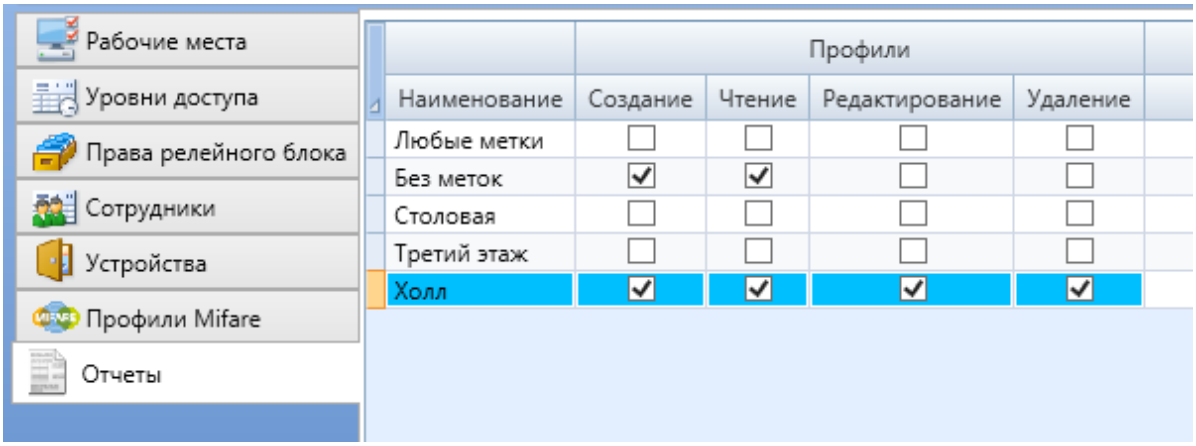


Рисунок 133 - Создание варианта отчета. Пример настройки прав пользователей к отчетам с использованием меток

4. Нажмите на кнопку Сохранить. В навигационной панели слева появится новый уровень с именем созданного отчета.

5. Перейдите к новому отчету. Щелкните пиктограмму в верхней панели управления, чтобы начать редактирование параметров.

6. Задайте стандартные параметры (поля в верхней части экрана, вкладка ***Параметры и настройки***): имя организации, подразделения, а также период отчета (см. рис. 133).

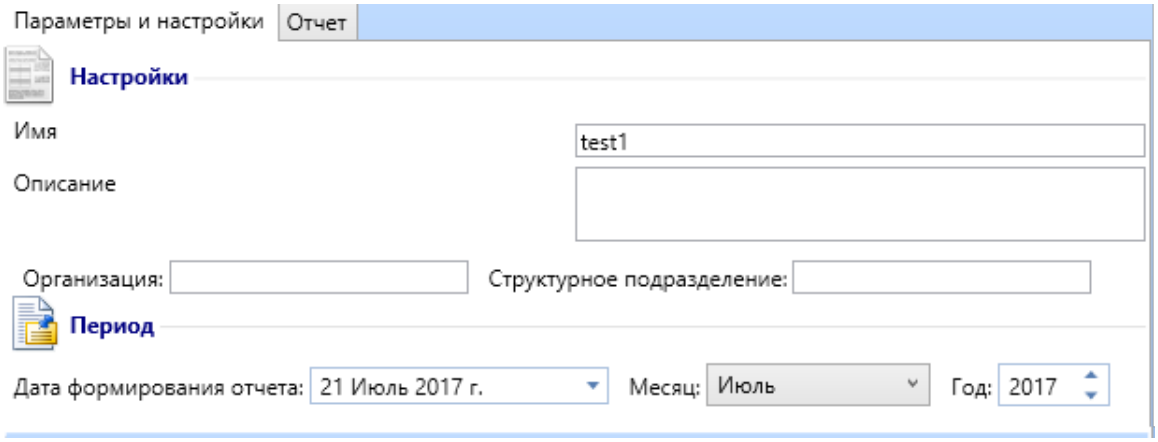


Рисунок 134 - Создание варианта отчета. Общие параметры

7. Выполните подробную настройку параметров в нижней части экрана (см. описания для каждого отчета).

8. Щелкните пиктограмму в верхней панели управления.

Готовый отчет с соответствующими настройками отобразится на вкладке ***Отчет***. Для каждого из настраиваемых отчетов доступен стандартный набор фильтров.

Каждый из готовых отчетов может быть экспортирован на локальное устройство в нужном формате.

Выгрузка отчета

APM RusGuard позволяет выгружать готовые отчеты в следующих форматах:

- XML-файл с данными отчета;
- CSV (разделитель - запятая);
- PDF;
- MHTML;
- MS Excel (`.xls`);
- TIFF (графический файл);
- MS Word (`.doc`).

Для того чтобы выгрузить отчет:

1. Сформируйте отчет (примените фильтры, если это требуется).
2. Нажмите на кнопку  .
   Раскроется список доступных форматов.
3. Щелкните левой кнопкой мыши по нужному формату.
   Система начнет процесс подготовки выгрузки, затем предложит локально сохранить файл выбранного формата.
4. Выполните сохранение (стандартная процедура ОС Windows).
   Для всех отчетов совпадает процедура настройки включения в отчет сведений о сотрудниках, для отчета ***Системные события*** также выполняется настройка параметров, связанных с устройствами. Подробные описания см. ниже.

Опоздания за месяц

Данный отчет выводит данные об опозданиях за указанный период.

Подготовка выборки данных сотрудников для отчета

Для того чтобы сформировать выборку данных о сотрудниках:

1. Создайте пустой бланк отчета 224.
2. Откройте вкладку ***Настройки и параметры*** (открыта по умолчанию), начните редактирование (см. рис. ниже).

Вы можете использовать настройки по умолчанию (все активные сотрудники), либо выбрать одну или несколько групп сотрудников. Обратите внимание на флаги ***Все сотрудники*** и ***Отображать удаленных***.

Если вы выбрали определенную группу сотрудников, ПО позволяет также выбрать определенных сотрудников внутри нее (список отображается в правой части формы, когда курсор установлен на нужной группе в списке слева). По умолчанию выбраны все сотрудники в группе (см. рис. 134).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

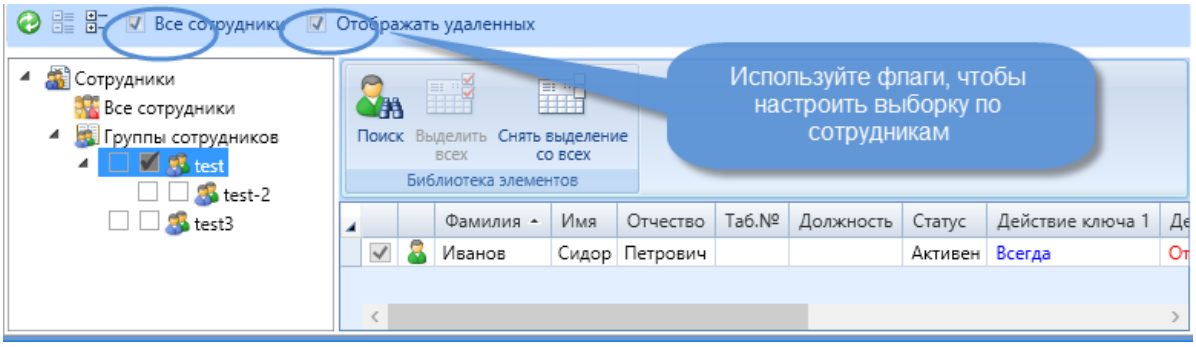


Рисунок 135 - Создание варианта отчета. Формирование выборки параметров сотрудников

3. Закончив редактирование, сохраните настройки отчета ( ).

По умолчанию при загрузке на вкладке ***Отчет*** в главном экране отображаются данные за текущий месяц, для примера выбран ноябрь 2015 года (см. рис. 135). Каждый столбец соответствует дню, строка - сотруднику.

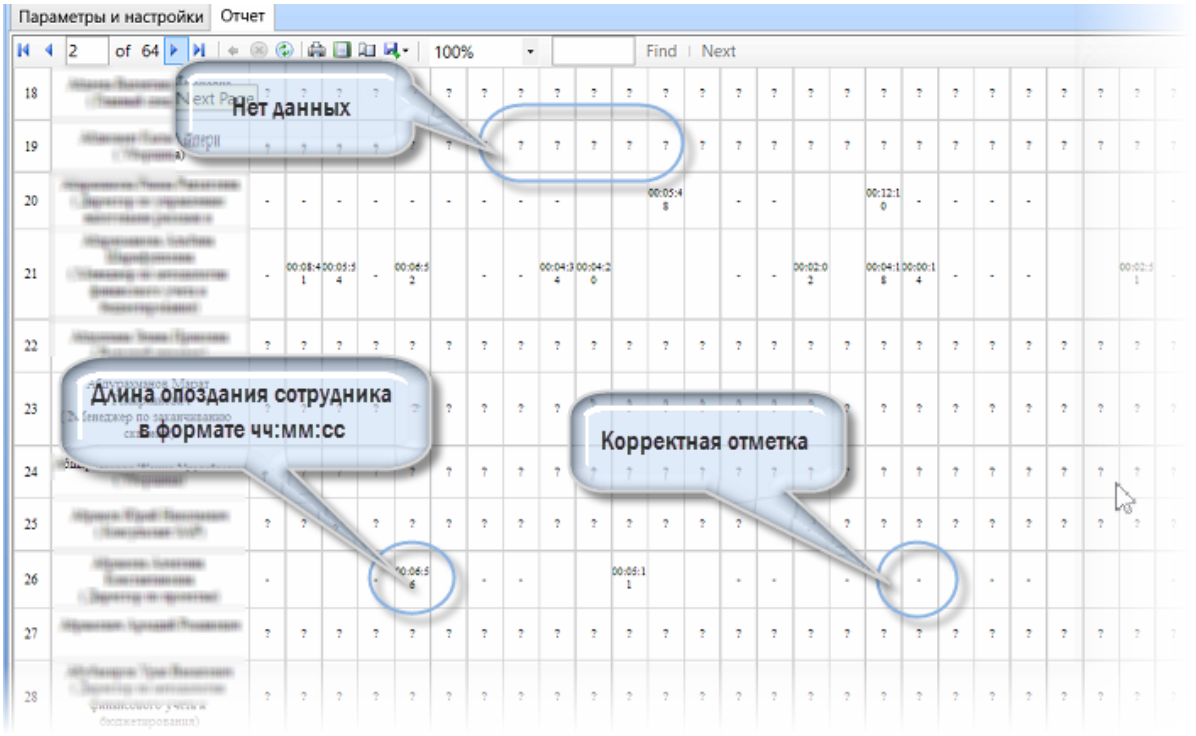


Рисунок 136 - Вывод отчета за период на экране. Опоздавшие

Отработанное время

Данный отчет отображает данные об отработанном сотрудником времени.

Подготовка выборки данных сотрудников для отчета

Для того чтобы сформировать выборку данных о сотрудниках:

1. Создайте пустой бланк отчета 224.
2. Откройте вкладку ***Настройки и параметры*** (открыта по умолчанию), начните редактирование (см. рис. ниже).

Вы можете использовать настройки по умолчанию (все активные сотрудники), либо выбрать одну или несколько групп сотрудников. Обратите внимание на флаги ***Все сотрудники*** и ***Отображать удаленных***.

Если вы выбрали определенную группу сотрудников, ПО позволяет также выбрать определенных сотрудников внутри нее (список отображается в правой части формы, когда курсор установлен на нужной группе в списке слева). По умолчанию выбраны все сотрудники в группе (см. рис. 136).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

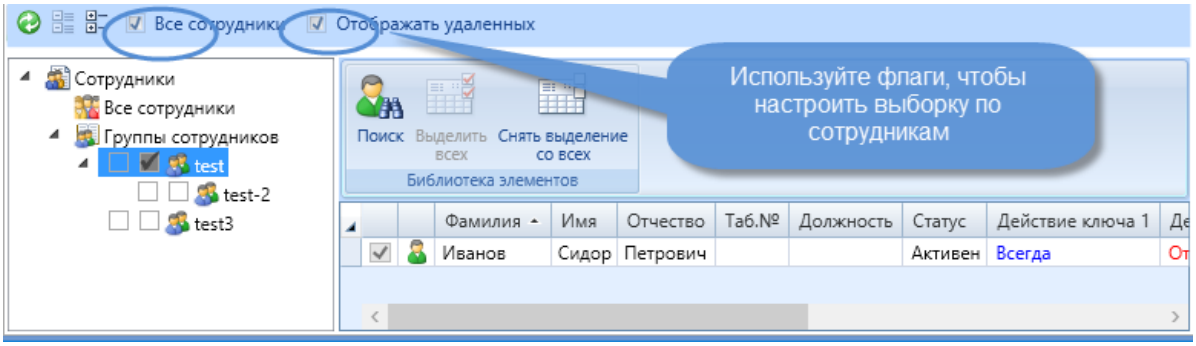


Рисунок 137 - Создание варианта отчета. Формирование выборки параметров сотрудников

3. Закончив редактирование, сохраните настройки отчета ( ).

По умолчанию при загрузке на вкладке ***Отчет*** в главном экране отображаются данные за текущий месяц.

В обычной версии отчета (см. рис. 137) содержится единая таблица, каждый столбец которой соответствует дню месяца, строка - сотруднику. В каждой ячейке отображается время прихода, ухода и отработанное время.

Рисунок 138 - Создание варианта отчета. Формирование отчета "Отработанное время"

Отработанное время (расширенный)

Данный отчет отображает данные об отработанном сотрудником времени за произвольный период (по умолчанию выводится текущая неделя), с дополнительными параметрами.

Подготовка выборки данных сотрудников для отчета

Для того чтобы сформировать выборку данных о сотрудниках:

1. Создайте пустой бланк отчета 224.
2. Откройте вкладку ***Настройки и параметры*** (открыта по умолчанию), начните редактирование (см. рис. ниже).

Вы можете использовать настройки по умолчанию (все активные сотрудники), либо выбрать одну или несколько групп сотрудников. Обратите внимание на флаги ***Все сотрудники*** и ***Отображать удаленных***.

Если вы выбрали определенную группу сотрудников, ПО позволяет также выбрать определенных сотрудников внутри нее (список отображается в правой части формы, когда курсор установлен на нужной группе в списке слева). По умолчанию выбраны все сотрудники в группе (см. рис. 138).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

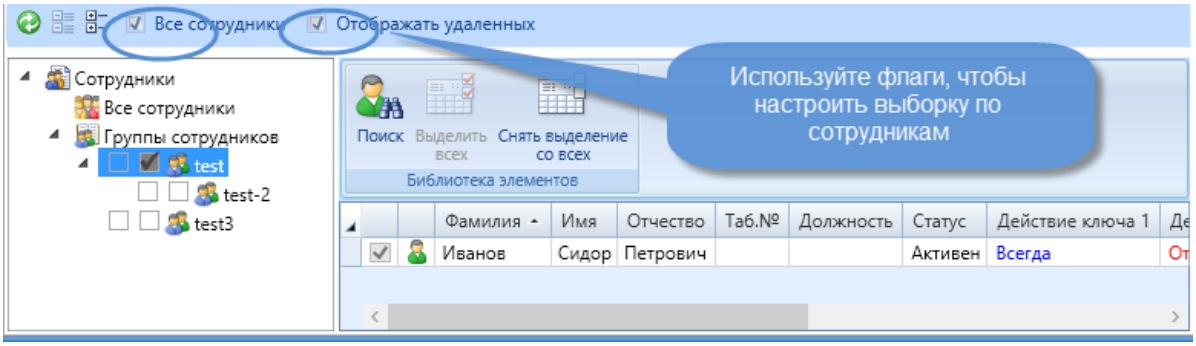
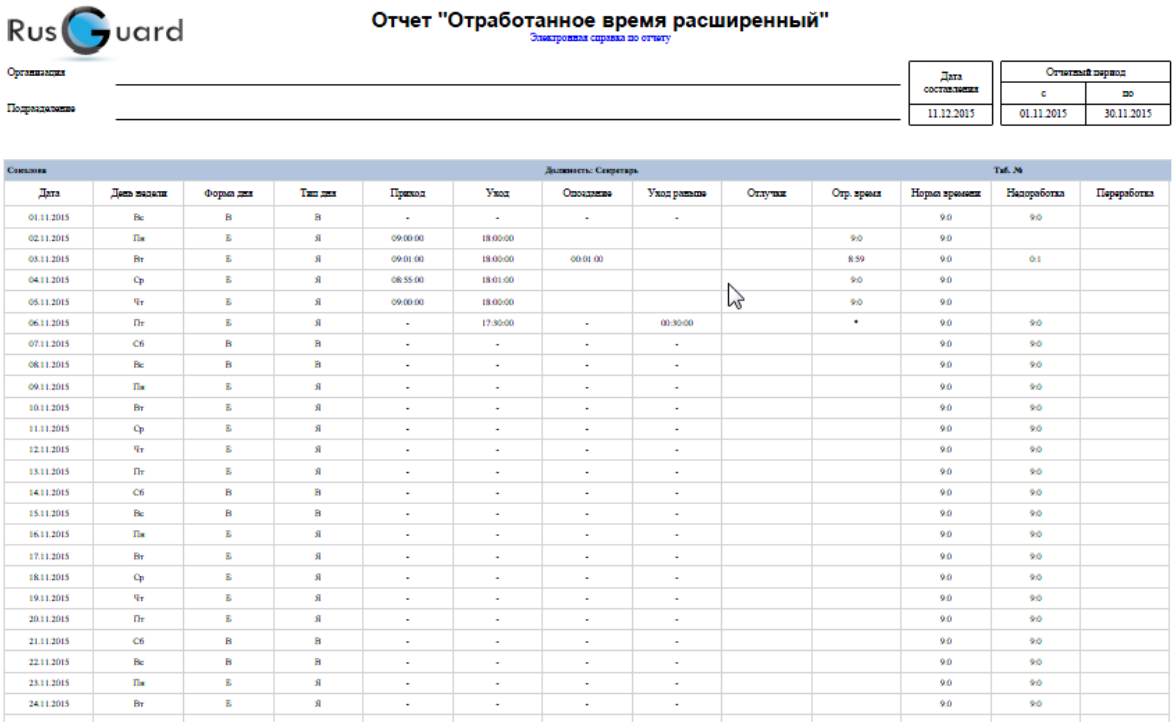


Рисунок 139 - Создание варианта отчета. Формирование выборки параметров сотрудников

3. Закончив редактирование, сохраните настройки отчета ( ).

В расширенной версии (см. рис. 139) отображаются отдельные таблицы для каждого из выбранных (или всех) сотрудников (могут использоваться ФИО, должность, инициалы и т.д.)

за выбранный период. В таблице отображается не только время прихода, ухода и отработанное время, но и сведения об опозданиях, ранних приходах/уходах, норме, недоработке/переработке, а также тип и форма дня.



Отчет "Отработанное время расширенный"

Электронная справка по отчету

Организация

Подразделение

Дата составления	Отчетный период	
	с	по
11.12.2015	01.11.2015	30.11.2015

Сотрудник — Должность: Секретарь — Таб. №

Дата	День недели	Форма дня	Тип дня	Приход	Уход	Опоздание	Уход раньше	Отлучки	Отр. время	Норма времени	Недоработка	Переработка
01.11.2015	Вс	В	В	-	-	-	-			9:0	9:0	
02.11.2015	Пн	Б	Я	09:00:00	18:00:00				9:0	9:0		
03.11.2015	Вт	Б	Я	09:01:00	18:00:00	00:01:00			8:59	9:0	0:1	
04.11.2015	Ср	Б	Я	08:55:00	18:01:00				9:0	9:0		
05.11.2015	Чт	Б	Я	09:00:00	18:00:00				9:0	9:0		
06.11.2015	Пт	Б	Я	-	17:30:00	-	00:30:00		*	9:0	9:0	
07.11.2015	Сб	В	В	-	-	-	-			9:0	9:0	
08.11.2015	Вс	В	В	-	-	-	-			9:0	9:0	
09.11.2015	Пн	Б	Я	-	-	-	-			9:0	9:0	
10.11.2015	Вт	Б	Я	-	-	-	-			9:0	9:0	
11.11.2015	Ср	Б	Я	-	-	-	-			9:0	9:0	
12.11.2015	Чт	Б	Я	-	-	-	-			9:0	9:0	
13.11.2015	Пт	Б	Я	-	-	-	-			9:0	9:0	
14.11.2015	Сб	В	В	-	-	-	-			9:0	9:0	
15.11.2015	Вс	В	В	-	-	-	-			9:0	9:0	
16.11.2015	Пн	Б	Я	-	-	-	-			9:0	9:0	
17.11.2015	Вт	Б	Я	-	-	-	-			9:0	9:0	
18.11.2015	Ср	Б	Я	-	-	-	-			9:0	9:0	
19.11.2015	Чт	Б	Я	-	-	-	-			9:0	9:0	
20.11.2015	Пт	Б	Я	-	-	-	-			9:0	9:0	
21.11.2015	Сб	В	В	-	-	-	-			9:0	9:0	
22.11.2015	Вс	В	В	-	-	-	-			9:0	9:0	
23.11.2015	Пн	Б	Я	-	-	-	-			9:0	9:0	
24.11.2015	Вт	Б	Я	-	-	-	-			9:0	9:0	

Рисунок 140 - Создание варианта отчета. Формирование отчета "Отработанное время, расширенный"

В отчете предусмотрены четыре дополнительных фильтра:

- ***Все*** - выводятся все данные;
- ***Опоздавшие***- выводятся только те строки статистики по сотруднику, где содержатся опоздания (если по сотруднику нет опозданий, он исключается из отчета). В строке ***ИТОГО*** выводится сумма по опозданиям;
- ***Ушедшие раньше*** - отображаются только те события ухода раньше по сотруднику. Если таких событий для сотрудника за период нет, данные по нему исключаются из отчета. В строке ***ИТОГО*** выводится суммарная статистика по уходам раньше;
- ***Опоздавшие и ушедшие раньше*** - в отчет включается статистика по обоим событиям для сотрудников. В строке ***ИТОГО*** выводится суммарное количество обоих событий.

Системные события

Данный отчет позволяет выводить данные обо всех или некоторых событиях в СКУД, обслуживаемой ПО. В отчет автоматически вносятся данные согласно настройкам рабочих графиков, расписаний и зон в системе.

Формирование выборки данных с устройств для отчета

Для того чтобы сформировать выборку данных с устройств:

1. Создайте пустой бланк отчета 224.
2. Раскройте вкладку ***События и устройства*** в нижней части экрана.

Вы можете использовать настройки по умолчанию (выбраны все события со всех устройств), либо сформировать выборку, устанавливая флаги, как показано на рисунке ниже (см. рис. 140).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

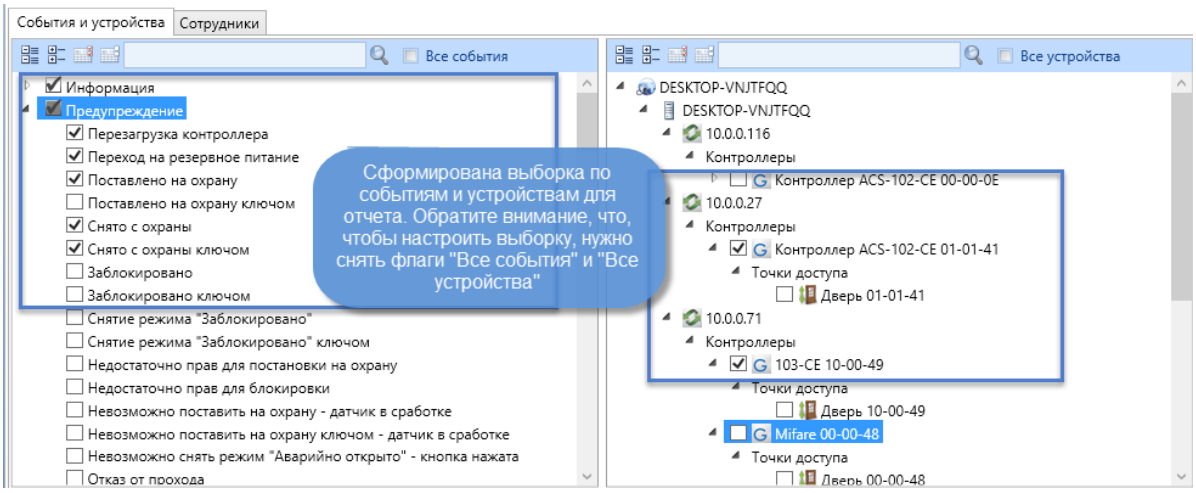


Рисунок 141 - Создание варианта отчета. Формирование выборки параметров устройств

3. Закончив редактирование, сохраните настройки отчета ( ).

Подготовка выборки данных сотрудников для отчета

Для того чтобы сформировать выборку данных о сотрудниках:

1. Создайте пустой бланк отчета 224.
2. Откройте вкладку ***Настройки и параметры*** (открыта по умолчанию), начните редактирование (см. рис. ниже).

Вы можете использовать настройки по умолчанию (все активные сотрудники), либо выбрать одну или несколько групп сотрудников. Обратите внимание на флаги ***Все сотрудники*** и ***Отображать удаленных***.

Если вы выбрали определенную группу сотрудников, ПО позволяет также выбрать определенных сотрудников внутри нее (список отображается в правой части формы, когда курсор установлен на нужной группе в списке слева). По умолчанию выбраны все сотрудники в группе (см. рис. 141).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

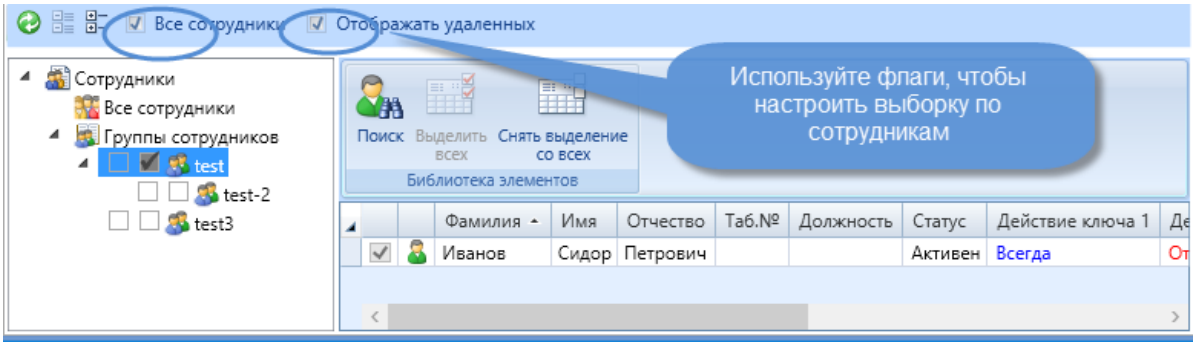


Рисунок 142 - Создание варианта отчета. Формирование выборки параметров сотрудников

3. Закончив редактирование, сохраните настройки отчета ( ).

По умолчанию при загрузке на вкладке ***Отчет*** в главном экране отображаются данные за текущую дату (см. рис. 142). Для формирования отчета необходимо выбрать тип события в фильтре.

Обратите внимание, что при загрузке отчета все поля фильтра должны быть заполнены, даже если никакой ограничивающий фильтр не применяется, и загружаются все доступные данные.

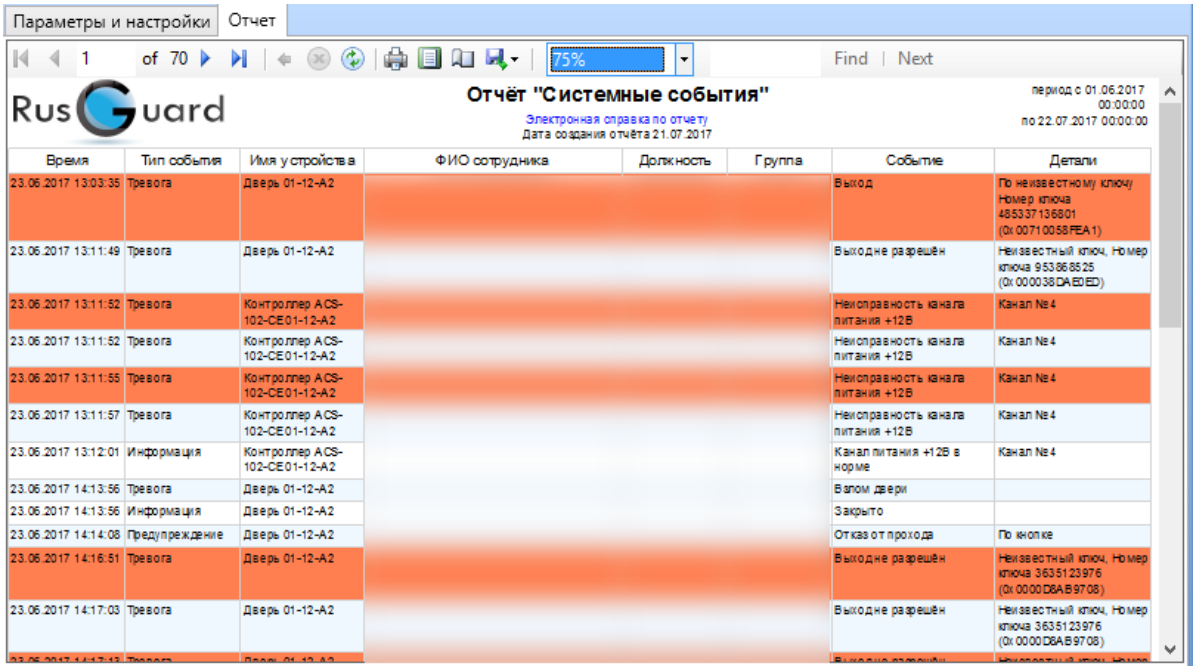


Рисунок 143 - АРМ RusGuard. Модуль Отчеты. Системные события

Пользователь может:

- Выгрузить отчет в одном из поддерживаемых форматов;
- Выполнить поиск;

Также интерфейс предусматривает ряд служебных функций (вывод на печать, настройка формата, обновление и т.д.).

Табель Т13

Данный отчет выводит данные об учете рабочего времени согласно стандартной форме Т-13. В отчет автоматически вносятся данные согласно настройкам рабочих графиков, расписаний и зон в системе.

Подготовка выборки данных сотрудников для отчета

Для того чтобы сформировать выборку данных о сотрудниках:

1. Создайте пустой бланк отчета [224].
2. Откройте вкладку ***Настройки и параметры*** (открыта по умолчанию), начните редактирование (см. рис. ниже).

Вы можете использовать настройки по умолчанию (все активные сотрудники), либо выбрать одну или несколько групп сотрудников. Обратите внимание на флаги ***Все сотрудники*** и ***Отображать удаленных***.

Если вы выбрали определенную группу сотрудников, ПО позволяет также выбрать определенных сотрудников внутри нее (список отображается в правой части формы, когда курсор установлен на нужной группе в списке слева). По умолчанию выбраны все сотрудники в группе (см. рис. 143).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

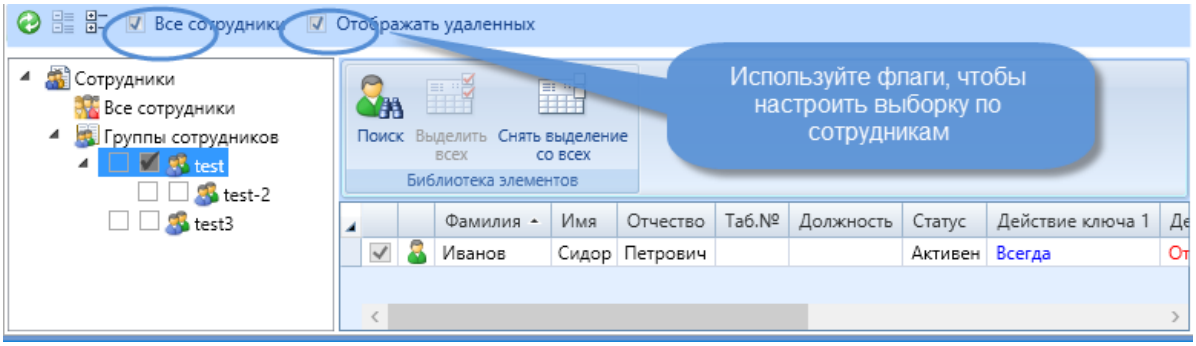
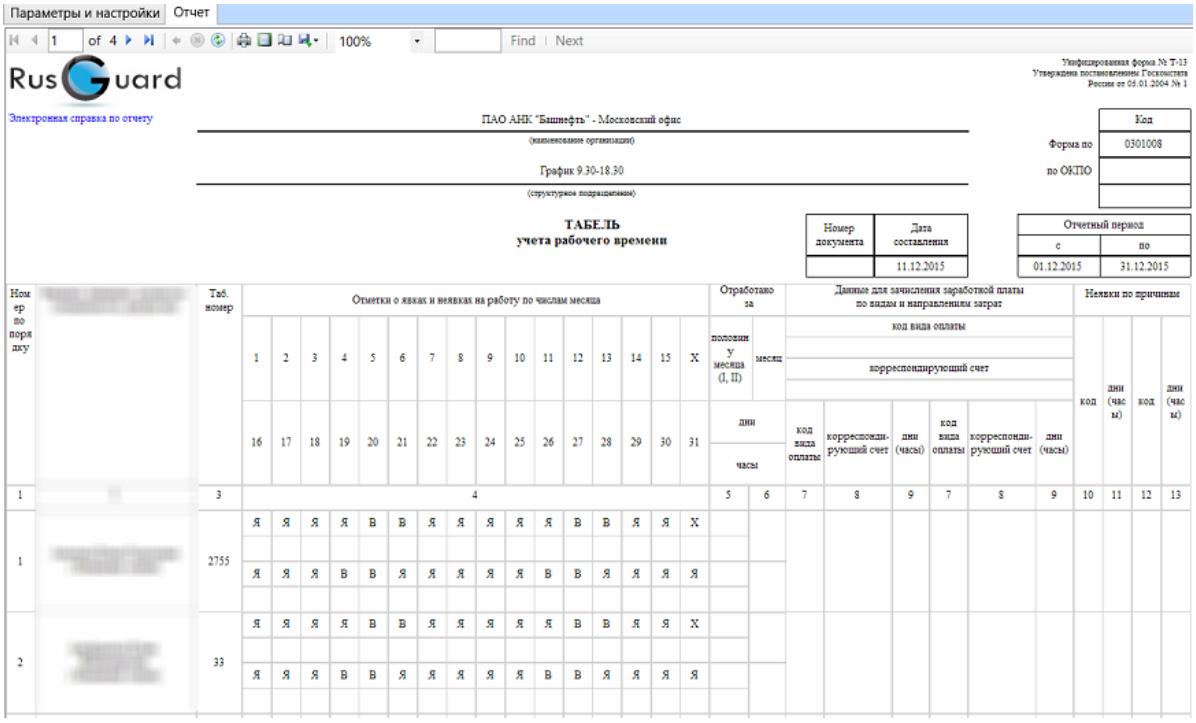


Рисунок 144 - Создание варианта отчета. Формирование выборки параметров сотрудников

3. Закончив редактирование, сохраните настройки отчета ( ).

По умолчанию при загрузке на вкладке ***Отчет*** в главном экране отображаются данные на текущую дату, для примера выбран ноябрь 2015 года (см. рис. 144). Каждый столбец соответствует дню, строка - сотруднику.



Параметры и настройки | Отчет

1 of 4 | 100% | Find | Next

RusGuard

Электронная справка по отчету

Унифицированная форма № Т-13
Утверждена постановлением Госкомстата России от 05.01.2004 № 1

ПАО АНК "Башнефть" - Московский офис
(наименование организации)

График 9.30-18.30
(структурное подразделение)

	Код
Форма по	0301008
по ОКПО	

ТАБЕЛЬ
учета рабочего времени

Номер документа	Дата составления
	11.12.2015

Отчетный период	
с	по
01.12.2015	31.12.2015

Номер по порядку	Таб. номер	Отметки о явках и неявках на работу по числам месяца															Отработано за		Данные для зачисления заработной платы по видам и направлениям затрат						Неявки по причинам			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	половину месяца (I, II)	месяц	код вида оплаты						код	дни (часы)	код	дни (часы)
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	дни / часы	код вида оплаты	корреспондирующий счет	дни (часы)	код вида оплаты	корреспондирующий счет	дни (часы)				
1		3	4															5	6	7	8	9	7	8	9	10	11	12	13
1		2755	Я	Я	Я	Я	В	В	Я	Я	Я	Я	Я	В	В	Я	Я	Х												
			Я	Я	Я	В	В	Я	Я	Я	Я	Я	В	В	Я	Я	Я	Я												
			Я	Я	Я	В	В	Я	Я	Я	Я	Я	В	В	Я	Я	Я	Я												
2		33	Я	Я	Я	Я	В	В	Я	Я	Я	Я	Я	В	В	Я	Я	Х												
			Я	Я	Я	В	В	Я	Я	Я	Я	Я	В	В	Я	Я	Я	Я												
			Я	Я	Я	В	В	Я	Я	Я	Я	Я	В	В	Я	Я	Я	Я												

Рисунок 145 - Создание варианта отчета. Формирование отчета "Табель Т13"

Уход раньше времени за месяц

Данный отчет выводит данные о сотрудниках, ушедших раньше времени. В отчет автоматически вносятся данные согласно настройкам рабочих графиков, расписаний и зон в системе.

Подготовка выборки данных сотрудников для отчета

Для того чтобы сформировать выборку данных о сотрудниках:

1. Создайте пустой бланк отчета 224.
2. Откройте вкладку ***Настройки и параметры*** (открыта по умолчанию), начните редактирование (см. рис. ниже).

Вы можете использовать настройки по умолчанию (все активные сотрудники), либо выбрать одну или несколько групп сотрудников. Обратите внимание на флаги ***Все сотрудники*** и ***Отображать удаленных***.

Если вы выбрали определенную группу сотрудников, ПО позволяет также выбрать определенных сотрудников внутри нее (список отображается в правой части формы, когда курсор установлен на нужной группе в списке слева). По умолчанию выбраны все сотрудники в группе (см. рис. 145).

После применения пользовательских настроек, отчет формируется автоматически на основании статистики по всем соответствующим системным сущностям (рабочие графики и зоны, реакции, устройства, точки и уровни доступа и т.д.).

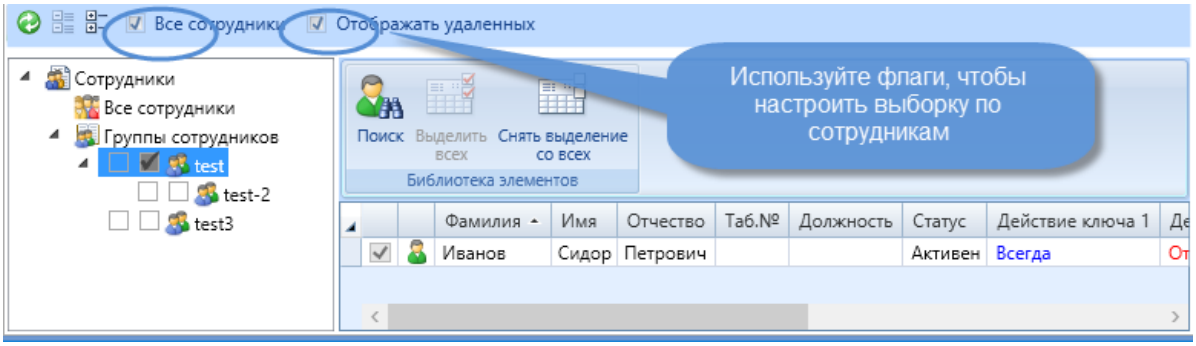


Рисунок 146 - Создание варианта отчета. Формирование выборки параметров сотрудников

3. Закончив редактирование, сохраните настройки отчета ( ).

По умолчанию при загрузке на вкладке ***Отчет*** в главном экране отображаются данные за выбранный период (см. рис. 146). По умолчанию выводятся данные за текущую дату.

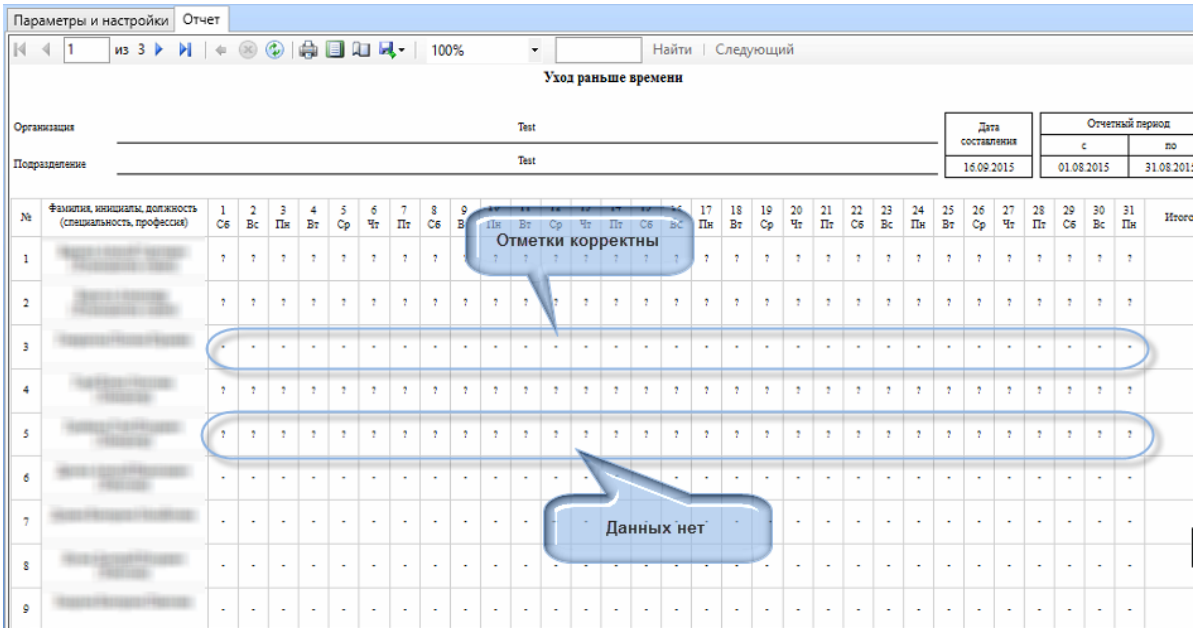


Рисунок 147 - Отображение отчета в АРМ

Управление шаблонами отчетов

Удаление устаревших шаблонов

Если необходимо удалить шаблон отчета с сервера или обновить его, выполняется операция удаления. Операция может быть выполнена только через сервер отчета (недоступна в модуле АРМ).

Для того чтобы удалить отчет с сервера:

1. Зайдите на Сервер отчетов 55.
2. Перейдите к списку отчетов.
3. Выделите нужный отчет.
4. В зависимости от настроек экрана, вызовите контекстное меню или воспользуйтесь верхней панелью управления (см. рис. 147). Найдите пункт ***Удалить***.

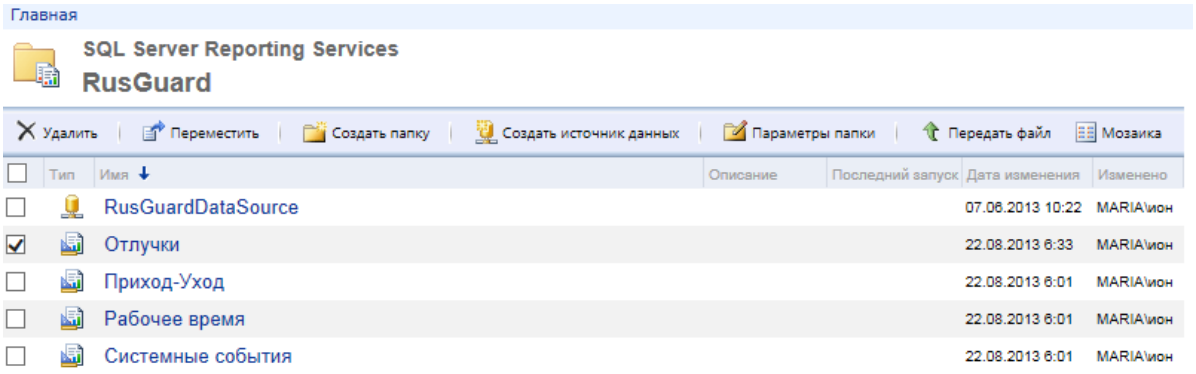


Рисунок 148 - Сервер Отчетов. Удаление шаблона отчета

Система попросит подтвердить или отменить действие.

5. Подтвердите действие.

Система удалит выбранный отчет.

Загрузка новых шаблонов

После того, как удален старый отчет (шаблон отчета), можно загрузить новый. Вы можете сделать это, используя веб-интерфейс, или через утилиту ***RusGuard Агент***.

Для того чтобы загрузить шаблон на сервер через веб-интерфейс:

1. Зайдите на сервер отчетов.
2. Перейдите к списку отчетов.
3. Нажмите на кнопку ***Передать файл*** в панели управления.
4. Найдите файл шаблона отчета (.rdl) на локальном ПК.
5. Выполните загрузку файла.

Для того чтобы загрузить шаблон через утилиту RusGuard Агент:

1. Сохраните новый шаблон отчета (`.rdl`) на локальном ПК рядом с другими шаблонами (по умолчанию, отчеты хранятся в папке `C:\Program Files\VVI Investment\RusGuard\Reports`) (см. рис. 148).

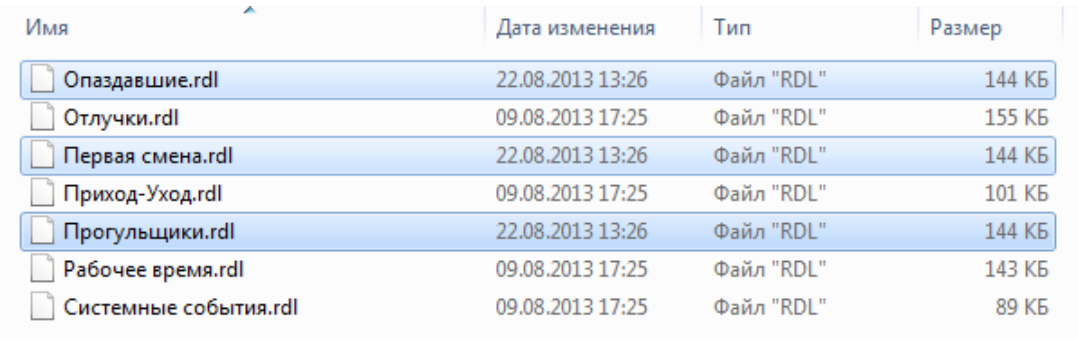


Рисунок 149 - Новые шаблоны отчетов в папке на локальном ПК

2. Запустите утилиту ***RusGuard Агент***.
3. Перейдите на вкладку ***Сервер Отчетов***. Если новые шаблоны отчетов были добавлены в папку, но отсутствуют на сервере, на вкладке отображается соответствующее сообщение, индикатор вкладки (флаг) становится красным (см. рис. 149).

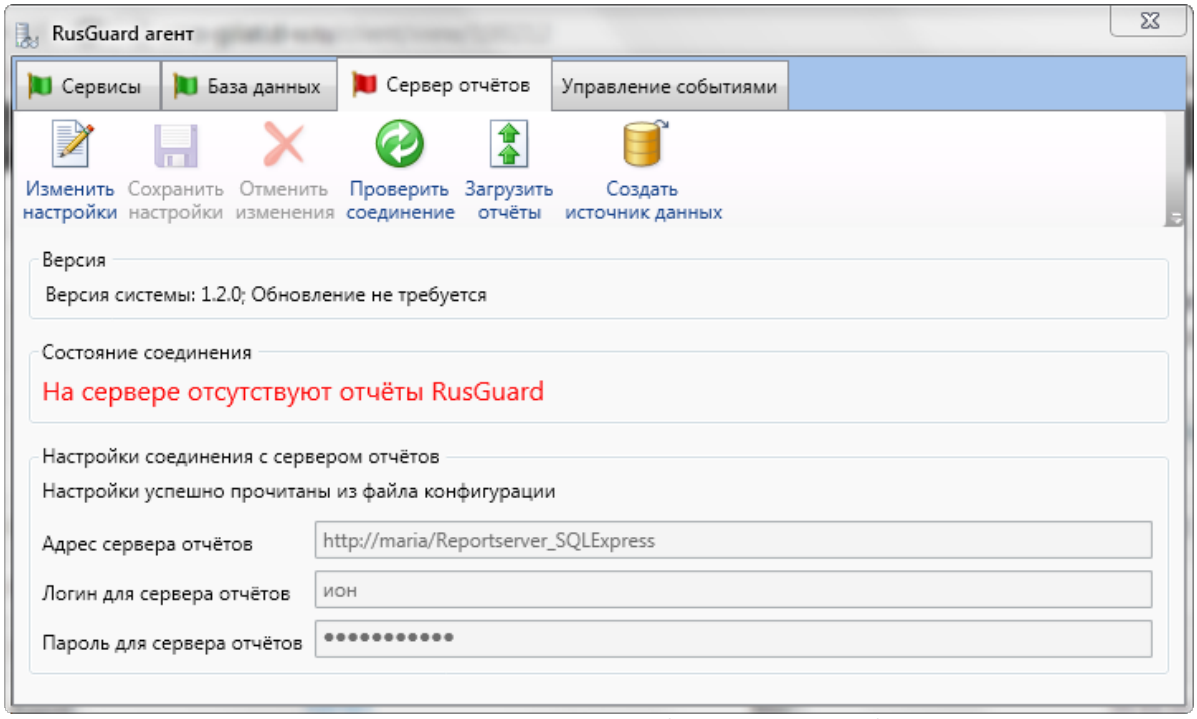


Рисунок 150 - Утилита RusGuard агент. Локально обнаружены новые шаблоны отчетов

4. Нажмите на кнопку ***Загрузить отчеты***. Кнопка активна, когда в папке ***Reports*** есть новые, не загруженные на сервер отчеты.

Система выполнит загрузку из папки автоматически. В случае успешной загрузки, отобразится соответствующее сообщение. Новые шаблоны появятся в списке на сервере (см. рис. 150). Индикатор на вкладке утилиты RusGuard агент окрашивается в зеленый цвет.

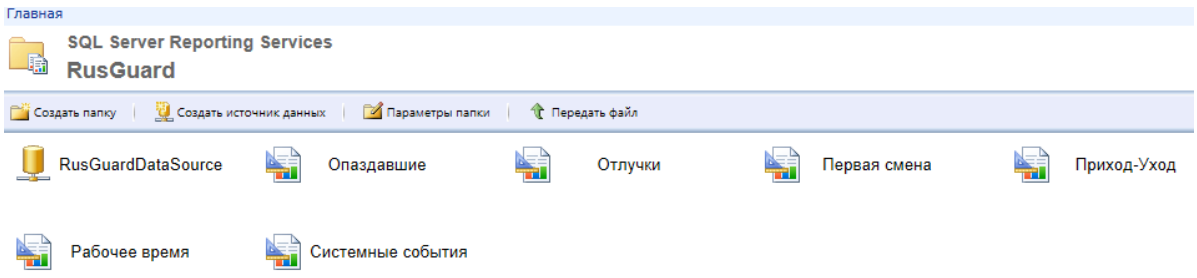


Рисунок 151 - Новые отчеты загружены на сервер

В случае возникновения затруднений при выполнении операции обновления/удаления шаблона, проверьте:

- Запущена ли служба RepotringServer.
- Верно ли введен адрес сервера отчетов в командную строку.

Модуль Планы

О первоначальной настройке модуля см. здесь 160.

Использование модуля Планы

Оператор АРМ использует модуль ***Планы*** для просмотра схем расположения оборудования СКУД на объекте, мониторинга состояния оборудования и управления устройствами.

Модуль позволяет выполнять следующие операции:

- Просматривать состояние точки доступа и устройства;
- Управлять точкой доступа (менять статус);
- Просматривать события в СКУД в реальном времени.

Для того чтобы просмотреть состояние точки доступа:

1. Запустите АРМ RusGuard, выбрав рабочее место, содержащее модуль ***Планы***.
2. Зайдите в модуль ***Планы***.
3. Обновите модуль ( ).
4. Раскройте нужный план в иерархическом списке в левой навигационной панели.

В главном экране отобразится план-схема объекта с драйверами расположенных на нем устройств (см. рис. 151).

Обратите внимание, что пиктограммы драйверов показывают статус устройства или статус точки доступа 246.

Рисунок 152 - АРМ RusGuard. Модуль Планы. Схема с размещенным на ней драйвером устройства "дверь"

5. Чтобы проверить состояние точки доступа, дважды щелкните левой кнопкой мыши по драйверу.

Откроется окно статуса. В верхнем перечне приведены характеристики точки доступа и их состояние, в нижнем - устройства (см. рис. 152). На приведенном примере все параметры устройства и точки доступа находятся в норме. При изменении параметров устройства и точки доступа их статус отображается **красным** шрифтом в этом окне.

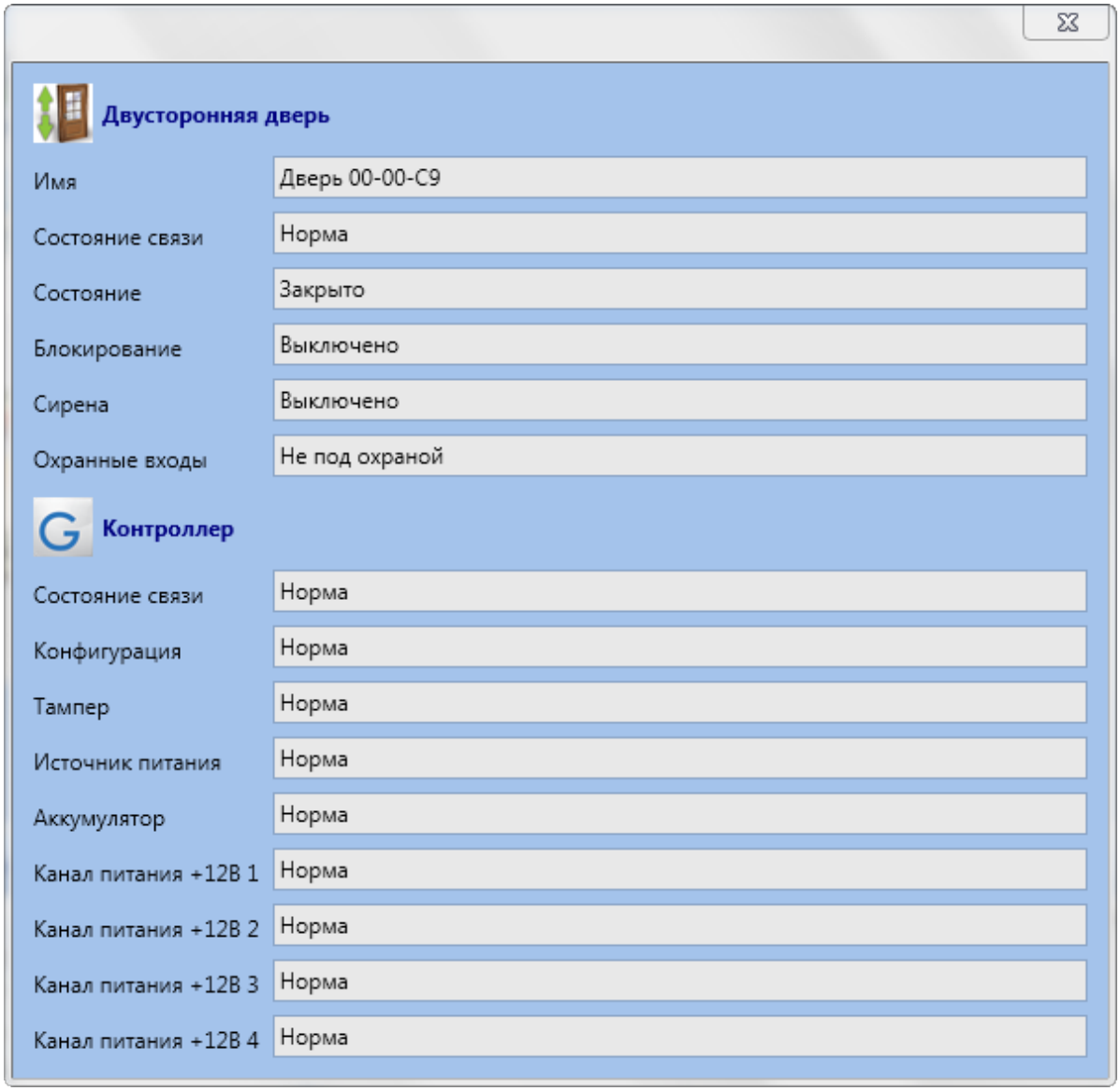


Рисунок 153 - АРМ RusGuard. Модуль Планы. Состояние точки доступа и соответствующего контроллера

Данное окно предназначено только для просмотра. Данные в нем нельзя отредактировать. Параметры редактируются в модуле ***Конфигурация оборудования*** 79.

В случае возникновения тревожного события на одной точке доступа или нескольких в верхней панели управления модуля Планы АРМ появляется пиктограмма "тревога", щелкнув которую пользователь может перейти к соответствующей точке доступа и принять меры (см. рис. 153 и 154).

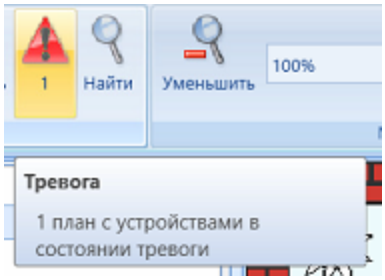


Рисунок 154 - APM RusGuard. Модуль Планы. Индикатор тревоги в панели управления

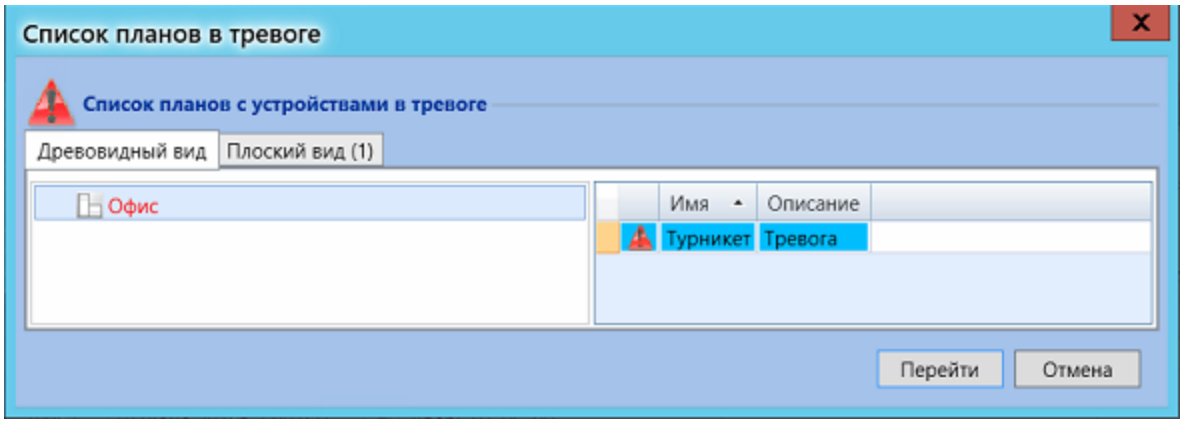


Рисунок 155 - APM RusGuard. Модуль Планы. Переход к точке доступа, где возникло тревожное событие

Для изменения состояния точки доступа:

1. Запустите APM RusGuard, выбрав рабочее место, содержащее модуль ***Планы***.
2. Зайдите в модуль ***Планы***.
3. Обновите модуль ( ).
4. Раскройте нужный план в иерархическом списке в левой навигационной панели.

В главном экране отобразится план-схема объекта с драйверами расположенных на нем устройств (см. рис. 155).

Обратите внимание, что пиктограммы драйверов показывают состояние устройства. Если пиктограмма окрашена в красный цвет - устройство работает некорректно, необходимо проверить состояние точки доступа. Зеленый цвет - устройство функционирует нормально, точка доступа контролируется.

Рисунок 156 - АРМ RusGuard. Модуль Планы. Схема с размещенным на ней драйвером устройства "дверь"

5. Чтобы изменить состояние точки доступа, щелкните правой кнопкой мыши по драйверу. Откроется контекстное меню (см. рис. 156).

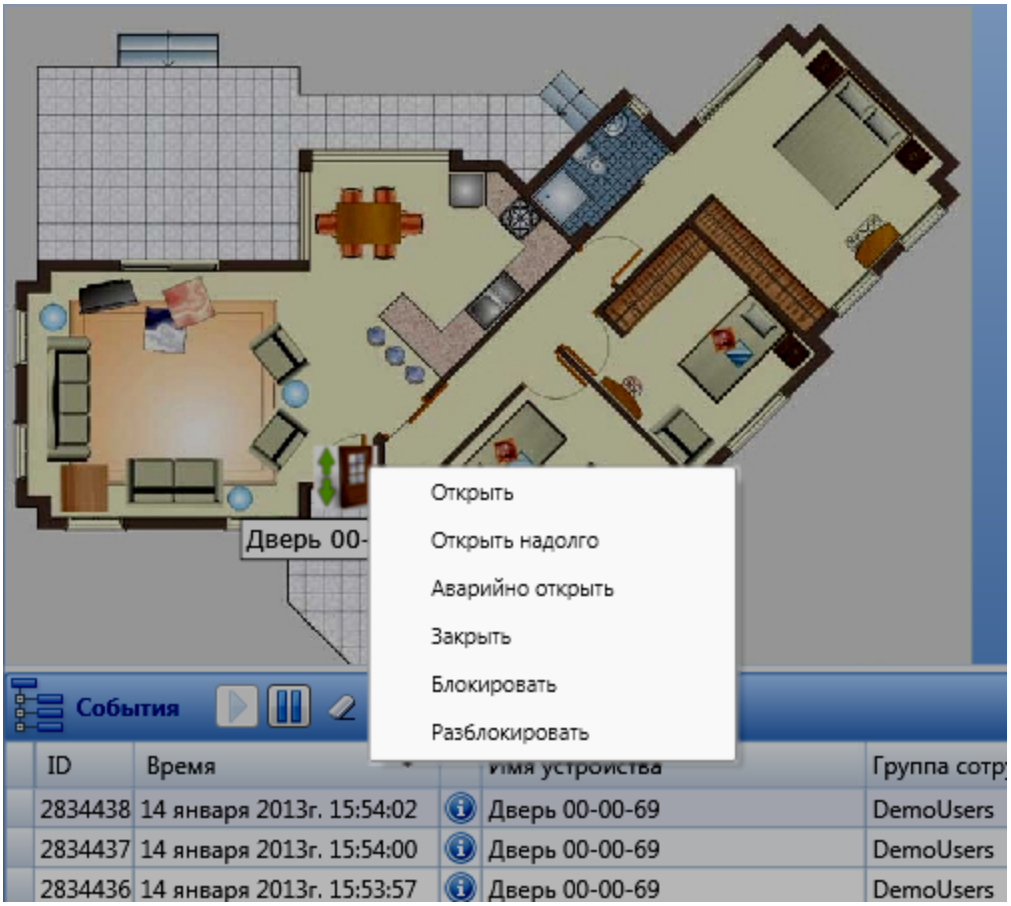


Рисунок 157 - АРМ RusGuard. Модуль Планы. Меню управления точкой доступа через драйвер

6. Выберите нужное действие в списке. Щелкните мышкой по строке.
Система выполнит указанное действие.

Начиная с версии 1.5.0 ПО RusGuard, вы также можете изменить состояние всех точек доступа на плане одновременно.

Для этого выделите нужный план в левой панели (в "дереве"), щелкните по нему правой кнопкой мыши и выберите нужное действие в контекстном меню, которое откроется (см. рис. 157).

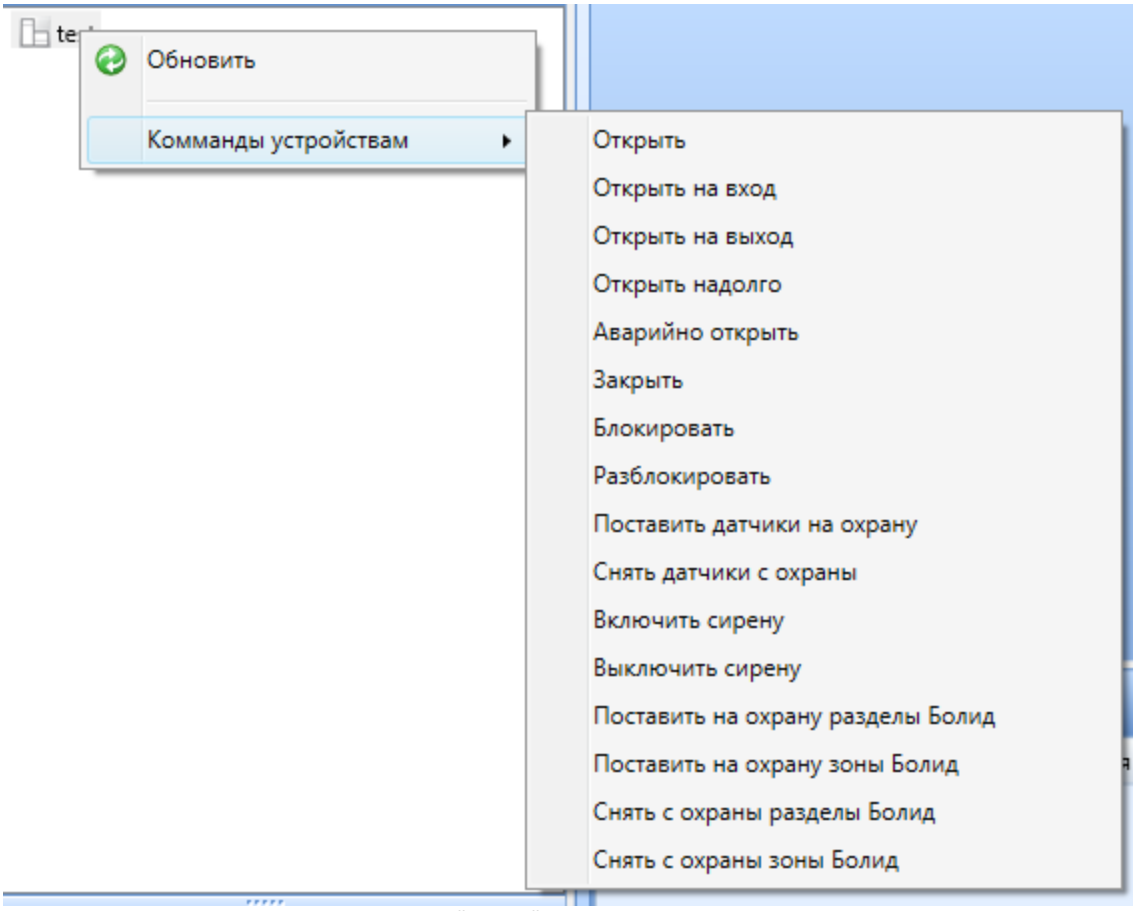
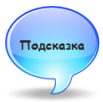


Рисунок 158 - АРМ RusGuard. Модуль "Планы". Изменение состояния всех точек доступа на плане.

Типы событий и их обозначение

Все системные события (в т.ч. изменения статуса устройств) отображаются в отчетах, а также в списке ***События*** (см. рис. 158), который отображается в нижней части окна нескольких модулей (см. табл. 10).



Щелкнув два раза по нужному событию в этом списке **в модуле *Планы***, вы можете перейти к нужному плану.

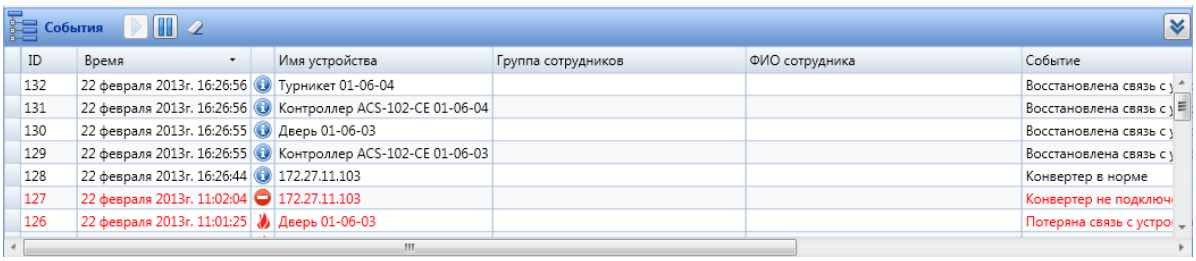


Рисунок 159 - АРМ RusGuard. Список событий раскрыт

Таблица 10 - События и их обозначения			
Тип события	Событие/Состояние	Пиктограмма	Описание
Предупреждение	Отказ от входа		
	Отказ от выхода		
	Нажата кнопка звонок		
Ошибка	Устройство (конвертер/контроллер) не подключено		От устройства не поступает сигнал. Необходимо проверить связь
Информационное сообщение	Восстановлена связь с контроллером		Связь с устройством восстановлена после отключения или сбоя. Также событие возникает при запуске АРМ, когда устройства вновь найдены. Сначала сообщается, что в норме конвертер, потом, что восстановлена связь с контроллером
	Конвертер в норме		Устройство работает нормально. Событие возникает в списке при запуске АРМ, когда устройство найдено и связь с ним установлена. При этом отображается IP-адрес найденного и распознанного устройства
	Вход		Выполнен вход по действующей карточке
	Выход		Выполнен выход по действующей карточке
	Закрыто		Точка доступа закрыта после успешного прохода сотрудника
	Снятие режима "Аварийно открыто"		Кнопка аварийного открытия была нажата повторно, проход закрыт
Тревога	Потеряна связь с устройством		Нарушена связь с конвертером. Необходимо проверить настройки и физическое состояние устройства
	Взлом двери/турникета/		Произошло принудительное открытие двери, турникета, шлагбаума и т.д.

Таблица 10 - События и их обозначения			
	шлагбаума		
	Аварийно открыто		Нажата кнопка аварийного открытия
	Оставлено открытым		Проход остается в режиме аварийного открытия

Статусы точек доступа

APM RusGuard отображает текущий статус точек доступа (см. табл. 11).

Таблица 11 - Графические обозначения статусов точек доступа на Планах				
Статус	Две двери	Дверь	Шлагбаум/ Ворота	Турникет
Работает нормально ("дежурный")				
Не совпадают настройки контроллера и сервера				
Нет сигнала от точки доступа				
Открыть				
Закрыть				
Заблокировать				
Нет связи с сервером ????				
Удален сервер				
Взлом				
Тревога охранного датчика				

Таблица 11 - Графические обозначения статусов точек доступа на Планах				
Аварийно открыть				
Нет опроса				
Открыть надолго				
Не отвечает				

Модуль Фотоидентификация

Модуль ***Фотоидентификация*** предназначен для:

- мониторинга прохождения сотрудников через точки доступа, привязанные к конкретному рабочему месту;
- видеонаблюдения через камеры, привязанные к конкретному рабочему месту;
- контроля прохода через точки доступа, привязанные к рабочему месту (в зависимости от настроек).

В зависимости от настроек, выполненных в модуле ***Конфигурация рабочих мест***, на экране модуля ***Фотоидентификация*** отображается одна или несколько ячеек, показывающих следующую информацию:

- Фотографии сотрудников, проходящих через одну или н Модуль Конфигурация рабочих мест 155 есколько точек доступа (зависит от количества ячеек);
- Видео с камер, установленных на одной или нескольких точках доступа (зависит от количества ячеек).

Также у оператора модуля может быть возможность контролировать проход через точку(точки) доступа вручную.

Пример 1. Фотоидентификация. Принятие решения оператором включено.

На иллюстрации ниже (см. рис. 159) приведен пример вида ячейки экрана модуля. Ячейка настроена на работу в режиме фотоидентификации. При этом при проходе сотрудника отображается:

- фото (согласно настройкам в модуле ***Конфигурация рабочих мест*** 155)
- имя
- номер ключа, по которому выполняется проход
- должность (если указана в карточке сотрудника)
- группа, к которой привязан сотрудник
- тип прохода (вход или выход)

Отображаются кнопки принятия оператором решения на вход и на выход. Кнопки находятся в режиме "включено", то есть, при каждом проходе перед фотографией отображаются кнопки ***Разрешить*** и ***Запретить***. Оператор принимает решение по каждому проходящему сотруднику, используя мышь или настроенные в модуле Конфигурация рабочих мест горячие клавиши.

Поскольку в данном примере кнопки принятия решения отображаются непосредственно в модуле ***Фотоидентфикация***, оператор может отключить режим принятия решения. В этом случае разрешение или запрет прохода выполняются автоматически, без запроса оператору.

В верхней части ячейки также отображается драйвер точки доступа, привязанной к ячейке. Пиктограмма драйвера 246 может меняться, показывая изменения статуса точки доступа. Двойным щелчком мыши по драйверу можно вызвать окно с более подробными данными о

состоянии точки доступа и соответствующего контроллера. Однако никаких возможностей для управления точкой доступа или контроллером в данном модуле не предусмотрено.

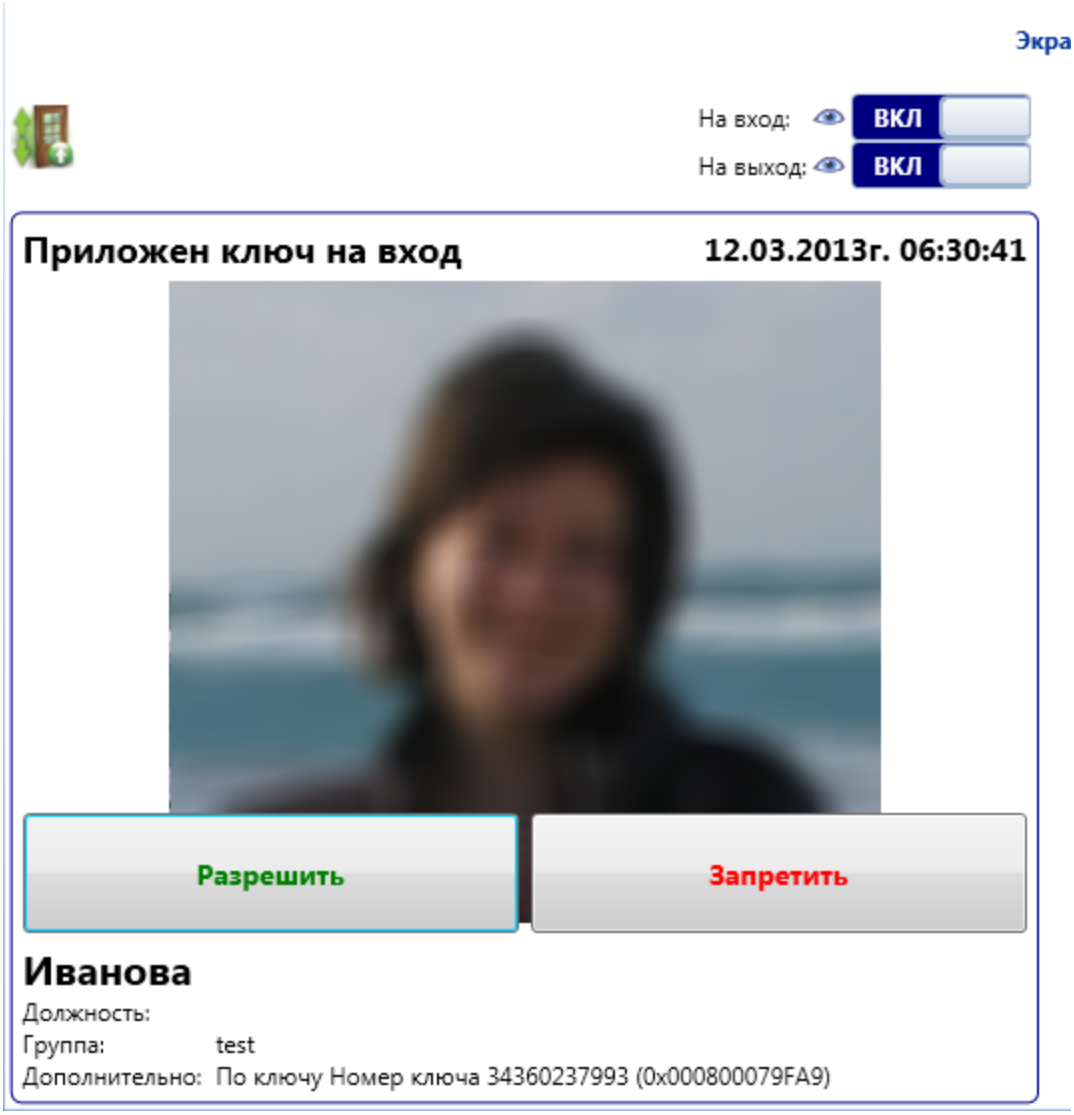


Рисунок 160 - APM RusGuard. Модуль Фотоидентификация. Пример ячейки экрана 1

Обратите внимание, что личные данные сотрудника не отображаются при проходе, если во время настройки модуля установлен флаг ***Скрыть личные данные***.

Пример 2. Фотоидентификация. Принятие решения оператором отключено

На иллюстрации ниже (см. рис. 160) показан пример настройки ячейки экрана, когда оператор не имеет возможности включить режим принятия решения по каждому сотруднику. Решение принимается автоматически, без участия оператора. В случае отказа в нижней части экрана отображается причина.

В верхней части ячейки также отображается драйвер точки доступа, привязанной к ячейке. Пиктограмма драйвера 246 может меняться, показывая изменения статуса точки доступа. Двойным щелчком мыши по драйверу можно вызвать окно с более подробными данными о

состоянии точки доступа и соответствующего контроллера. Однако никаких возможностей для управления точкой доступа или контроллером в данном модуле не предусмотрено.

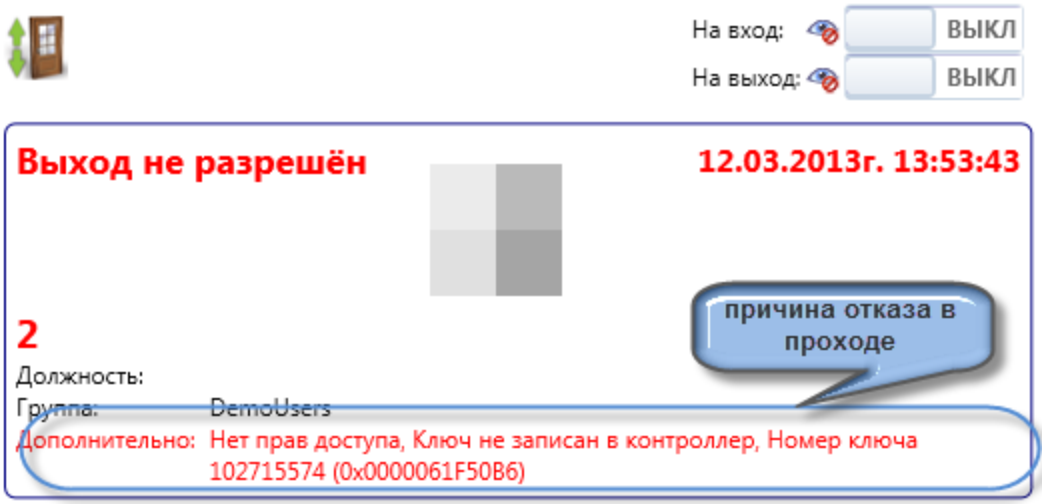


Рисунок 161 - АРМ RusGuard. Модуль Фотоидентификация. Пример ячейки экрана 2

Пример 3. Фотоидентификация. Отображение фото с двух точек доступа. Отображение фото предыдущего сотрудника

На иллюстрации ниже (см. рис. 161) приведен пример настройки экрана из двух ячеек.

Каждая ячейка соответствует одной точке доступа.

В левой ячейке отображается только фотография сотрудника, проходящего в настоящий момент. Принятие решения оператором возможно, но отключено, то есть решение принимает система в автоматическом режиме.

В правой ячейке сверху отображается фотография сотрудника, который проходит через точку доступа в настоящий момент. Принятие решения оператором включено, необходимо разрешить или запретить вход. Ниже отображается фотография лица, прошедшего (пытавшегося пройти) через точку доступа до этого. Также указан результат операции. В данном случае, отказ по решению оператора.

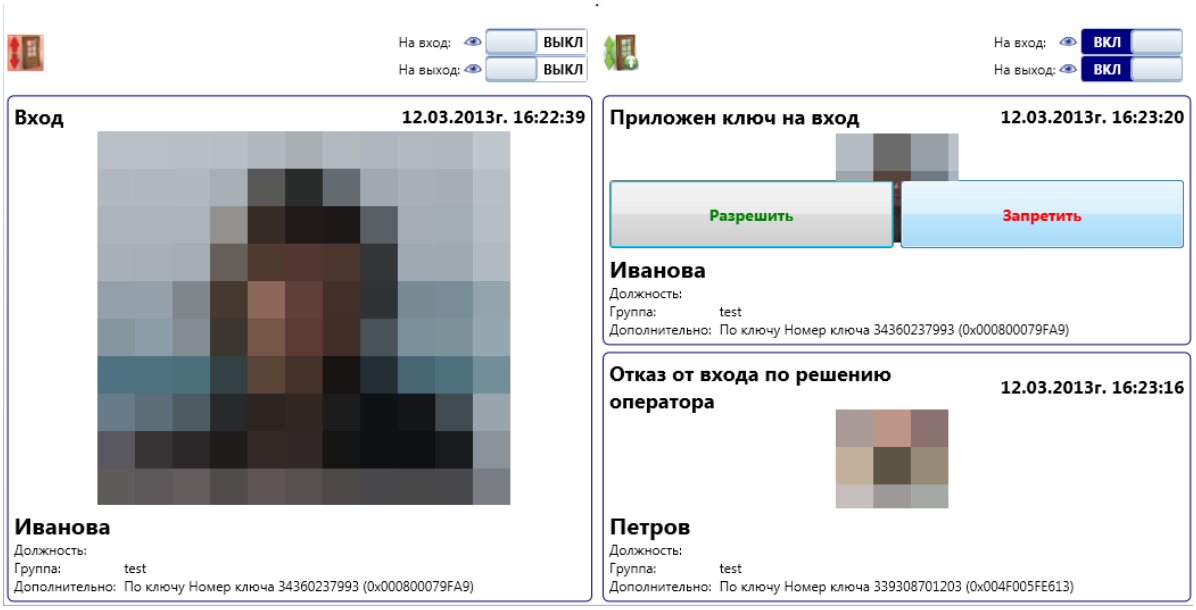


Рисунок 162 - APM RusGuard. Модуль Фотоидентификация. Пример экрана 3

Пример 4. Видеонаблюдение

На иллюстрации ниже (см. рис. 162) приведен пример настройки экрана из четырех ячеек.

Две нижние ячейки соответствуют двум точкам доступа. В двух верхних (выделены на иллюстрации) отображается видео с камер Ivideon.

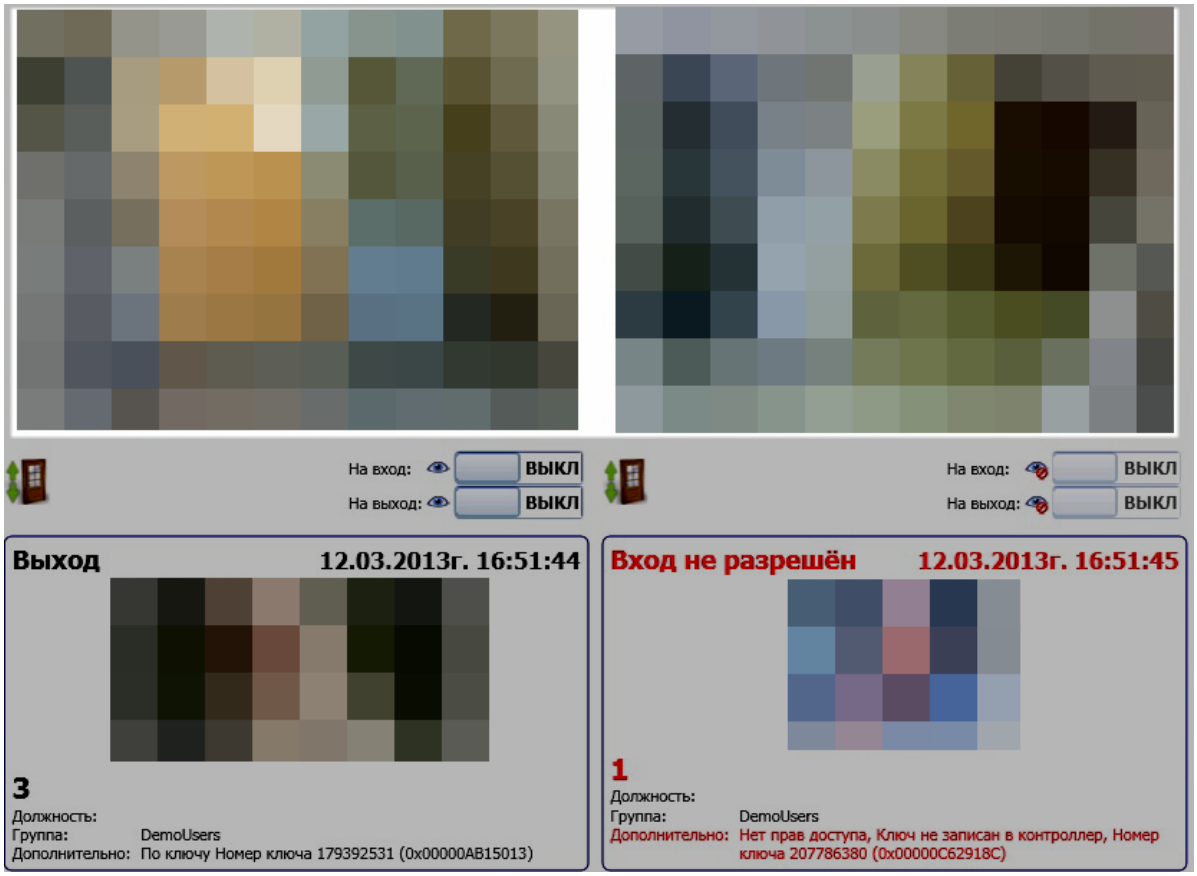


Рисунок 163 - АРМ RusGuard. Модуль Фотоидентификация. Пример экрана 4

Модуль Статистика

Модуль ***Статистика*** АРМ показывает сводную статистику по точкам доступа и/или устройствам СКУД (см. рис. 163). Модуль настраивается для рабочего места по стандартной процедуре 156.

В верхней части экрана выводится краткая информация в разрезе состояний точек доступа и устройств, в нижней - подробная таблица с детализацией для каждого устройства и/или точки доступа.

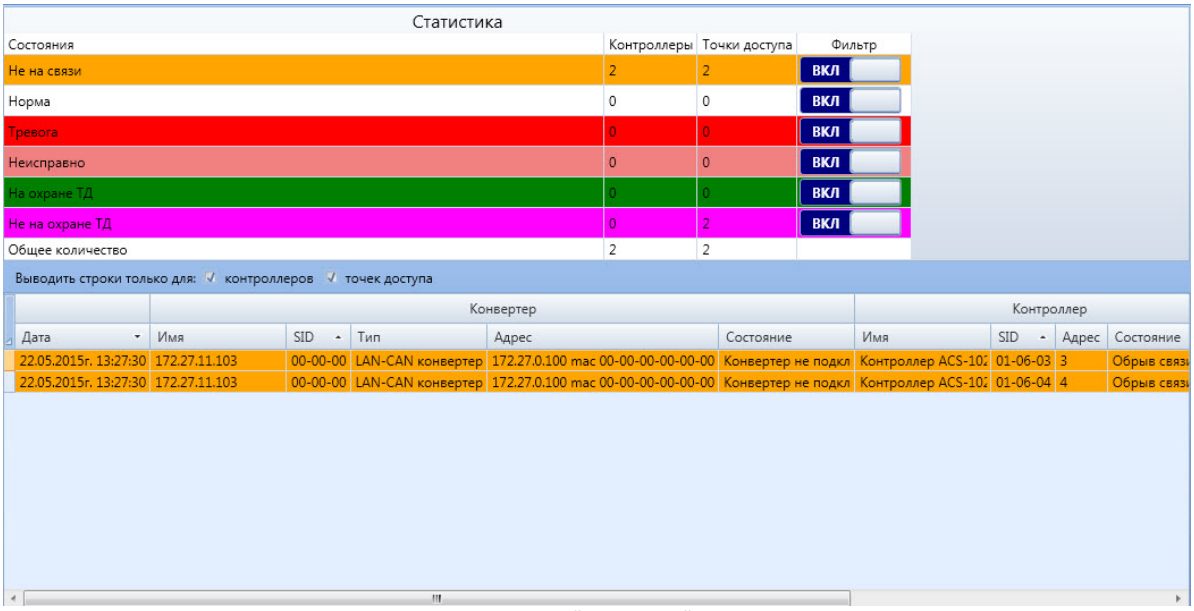


Рисунок 164 - Модуль "Статистика". Главное окно

Пользователь может:

- Выбрать режим отображения таблицы:
  - устройства и точки доступа;
  - только точки доступа;
  - только устройства.
- Настроить поля детализации (по умолчанию выводятся все доступные поля);
- Скопировать данные из таблицы.

Для того чтобы выбрать режим отображения таблицы воспользуйтесь флагами над ней (***Выводить только для:***).

Для того чтобы настроить поля таблицы:

1. Щелкните правой кнопкой мыши по значку  в верхнем левом углу таблицы.

   Откроется контекстное меню (см. рис. 164).

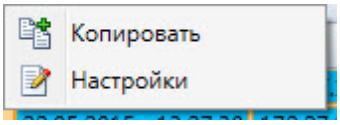


Рисунок 165 - Контекстное меню модуля "Статистика"

2. Выберите пункт ***Настройки***.

Пункт меню ***Копировать*** активен, если выделены поля таблицы. Он позволяет скопировать данные из таблицы в текстовом формате и перенести, например, в программу MS Excel (с сохранением разбиения на столбцы).

В новом окне откроется список полей таблицы (см. рис. 165). Все они активны по умолчанию. Снимая/устанавливая флаги возле названий полей, вы можете менять набор полей таблицы.

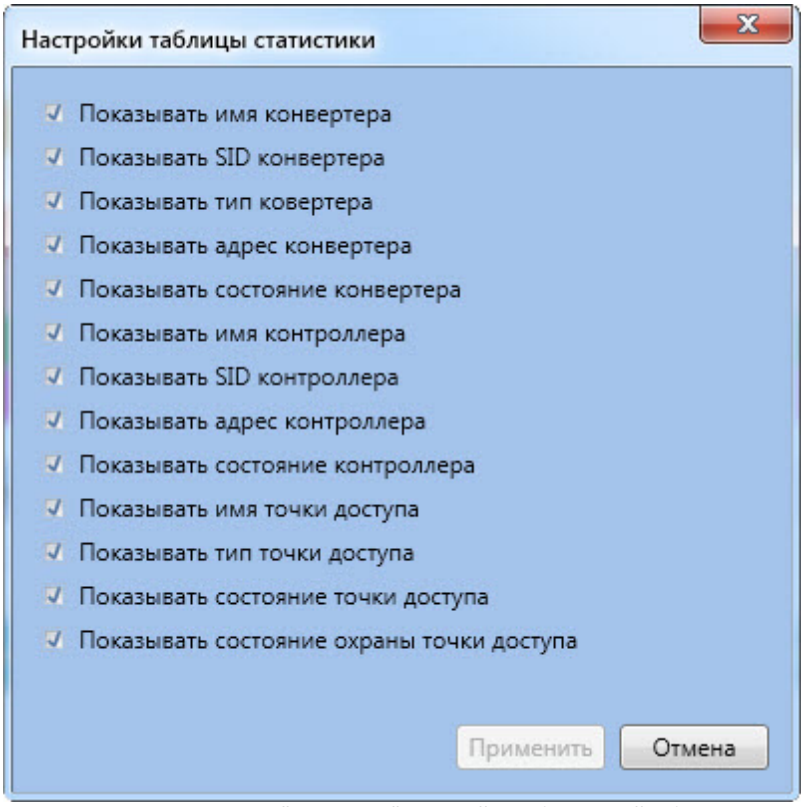


Рисунок 166 - Модуль "Статистика". Настройка набора полей таблицы

3. Настройте поля нужным образом. Нажмите на кнопку ***Применить***.

Система применит настройки.

Обратите внимание, что, используя пиктограммы внизу экрана, можно развернуть/свернуть список событий, отображаемый в реальном времени.

Модуль "Табло посетителей"

Модуль позволяет отслеживать:

- сколько человек находится в настоящее время в рабочей зоне;
- сколько гостей находится в рабочей зоне;
- сколько сотрудников находится в рабочей зоне.

Для того чтобы использовать модуль, необходимо предварительно настроить хотя бы одну рабочую зону в рамках СКУД.

Для того чтобы настроить модуль:

1. Добавьте модуль ***Табло посетителей*** в одно из пользовательских рабочих мест. Созданный модуль отобразится в списке модулей редактируемого рабочего места.
2. Перейдите в строку с названием нового модуля для настройки его параметров.

   Нажмите на кнопку  в верхней панели управления. Откроется главное окно модуля (см. рис. 166).

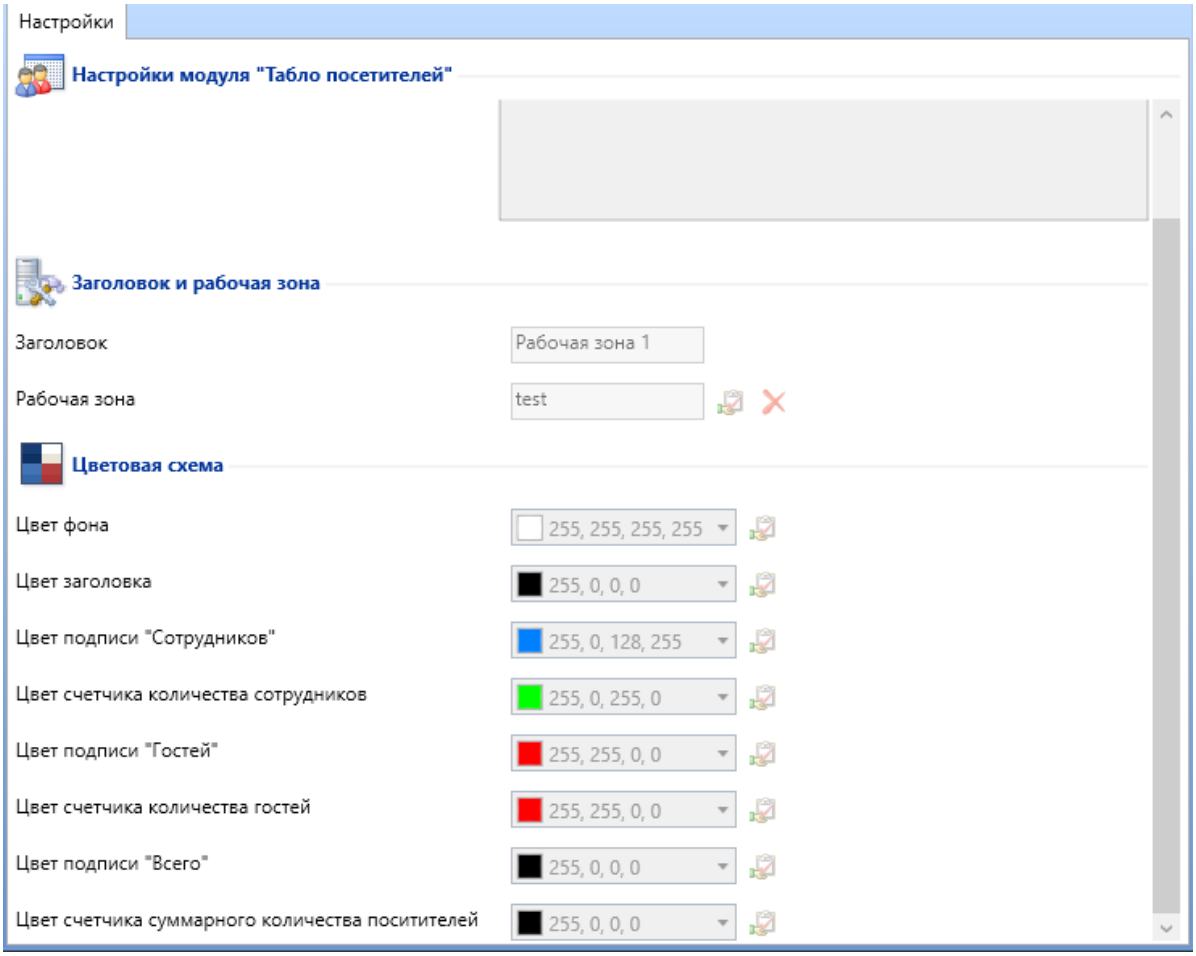


Рисунок 167 - Модуль "Табло посетителей". Главное окно

3. Задайте рабочую зону, мониторинг которой необходимо осуществлять при помощи модуля. Для этого в области экрана ***Заголовок и рабочая зона*** нажмите на кнопку  в поле ***Рабочая зона*** и выберите нужную зону из списка, который загрузится.
4. В поле заголовок введите название для табло, которое будет отображаться непосредственно в модуле.
5. В блоке полей ***Цветовая схема*** выберите, цвет фона и шрифта для заголовка, статистики по количеству сотрудников в зоне, гостей и по общему количеству лиц.
6. Сохраните настройки ().

Данные на табло могут отображаться некорректно, если лицо покидает зону или входит в нее по карте другого лица (например, одновременно с ним). Скорректировать отображение можно только приложив к контроллеру карту лица, чьи данные отображаются некорректно.

Мобильные приложения

Благодаря мобильному приложению, ПО RusGuard может использоваться на мобильных устройствах на базе ОС Android и iOS. В приложении предусмотрены компоненты, решающие задачи разных групп пользователей:

- удаленные терминалы для сотрудников службы охраны
- удаленый администратор для руководителей

Удаленный терминал превращает любое мобильное устройство в портативное устройство для считывания карт при контроле на объект. Настройка приложения выполняется в АРМ RusGuard (модуль Конфигурация рабочих мест 169). Функционал модуля позволяет считать код сотрудника с карты Mifare посредством NFC (только для платформы Android) или с любых штрих-кодов и QR-кодов бумажных пропусков. После считывания кода выводится информация о сотруднике. Набор выводимых полей настраивается на сервере. Модуль можно использовать как для проверки пропуска сотрудника, так и для регистрации его входа или выхода внутри любой рабочей зоны. Часто используемая рабочая зона может быть сохранена как шаблон для быстрого доступа.

Простая процедура позволяет настроить проверяемые при проходе параметры (фото, ключ, ФИО). По принципу работы приложение похоже на модуль Фотоидентификация. При считывании ключа отображаются данные о сотруднике (если найдены в базе данных) и запрос действия.

Приложение для администраторов обеспечивает удаленный контроль режимом работы дверей, ворот и пр. участков СКУД.

Для корректной работы терминала в АРМ 76 должны быть настроены:

- рабочие зоны 190
- точки доступа 87
- уровни доступа 67
- карточки сотрудников с фото 70

Кроме того, в АРМ должны быть настроены связи между указанными элементами.

При настройке мобильного терминала убедитесь, что это единственное рабочее место, привязанное к учетной записи пользователя (настройка выполняется через группу пользователей).

Общий порядок настройки приложения

1. Убедитесь, что выполнены предварительные условия (настроены рабочие зоны, точки доступа, уровни доступа, карточки сотрудников.
2. Перейдите в модуль ***Конфигурация рабочих мест***. Выполните настройку рабочего места типа мобильный терминал 169.
3. Перейдите в модуль ***Конфигурация системы***. Создайте группу пользователей мобильного приложения и убедитесь, что в правах доступа к рабочим местам 174 у этой группы выбран **только** настроенный ранее мобильный терминал.
4. Скачайте и установите мобильное приложение на устройства (о том, где можно скачать дистрибутивы, см. на нашем сайте).
5. Выполните настройку параметров подключения (выполняется для всего приложения, независимо от того, используется ли только удаленный терминал, администратор или оба компонента). О процедуре настройки см. раздел Удаленный терминал.
6. Убедитесь, что перед началом использования выполнена синхронизация.

Типовые операции

SQL не устанавливается автоматически

Если при установке ПО RusGuard не выполняется автоматическая установка компонентов SQL-сервера из дистрибутивного комплекта, рекомендуется проверить, установлен ли NetFramework 3.5 29.

Установка выполняется либо автоматически в процессе развертывания ПО, либо, если по каким-то причинам установка не была выполнена, через сайт Microsoft.

Настройка подписок сервера Отчетов

Обратите внимание, что настройка подписки для сервера Отчетов (т.е. для скачивания отчетов на локальный ПК) поддерживается только версией SQL Server версии Standart или выше.

Для того чтобы настроить подписку:

1. Запустите службу Агент SQL для редактируемого экземпляра Сервера RusGuard (***Панель управления*** > ***Администрирование*** > ***Службы***). Тип запуска - ***Автоматически*** (см. рис. 1).

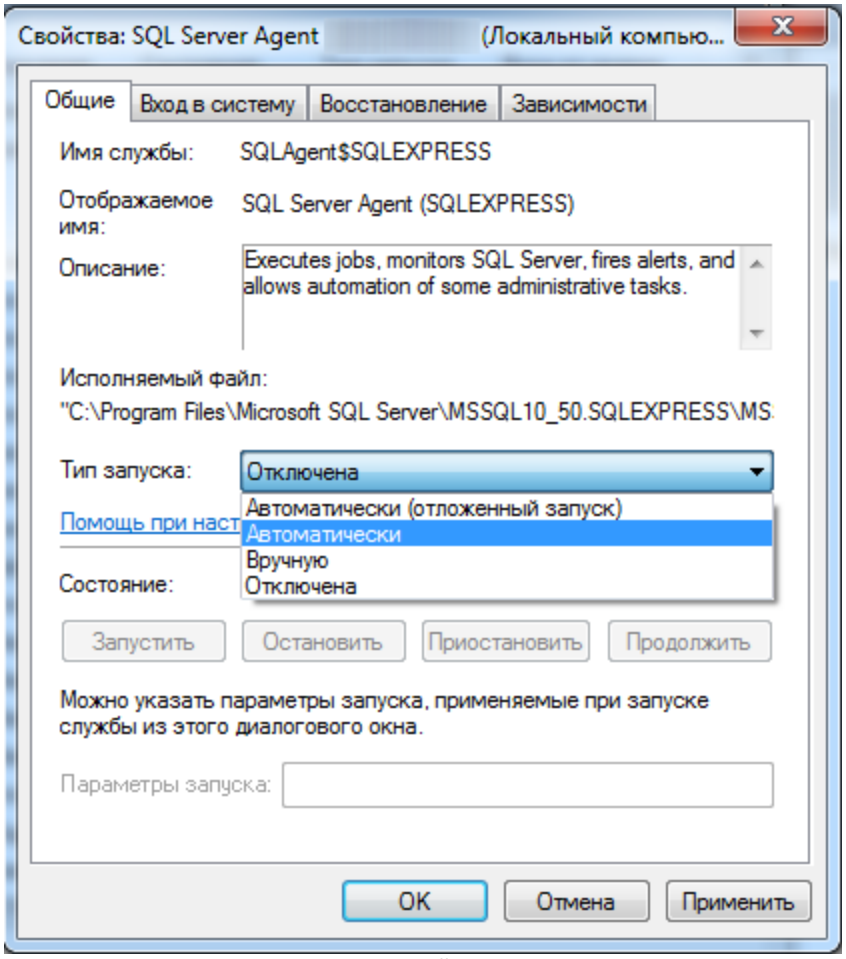


Рисунок 1 - APM RusGuard. Настройка подписок Сервера Отчетов

2. Создайте папку для отчетов на сервере или ином ресурсе в сети. Дайте определенному пользователю максимальный доступ к ней.
3. Зайдите в WEB-интерфейс Сервера отчетов (о работе с интерфейсом Сервера отчетов см. здесь 55).
4. Перейдите в отчет, для которого необходимо создать подписку. Раскройте контекстное меню и выберите пункт ***Подписка***.
5. В качестве способа доставки выберите ***Общая папка Windows***.
6. Укажите полный сетевой путь к папке сохранения отчетов (например: `\\Server\Reports`).
7. Укажите имя пользователя и пароль доступа к папке.
8. Укажите формат сохраняемого файла отчета (.xls, .pdf, .doc).
9. Настройте расписание автоматического построения отчета (при переходе на страницу расписаний стирается пароль пользователя для доступа к сетевой папке).
10. Укажите необходимые параметры отчета.
11. Завершите процедуру.

Посмотреть текущий статус или изменить свойства подписки можно через меню ***Мои подписки***.

Для того чтобы создать подписку с отправкой на электронную почту:

1. Запустите утилиту SQL ***Reporting Services Configuration Manager***.
2. На вкладке ***Настройка электронной почты*** (***E-mail Settings***) введите адрес SMTP сервера (127.0.0.1 если локальный) и имя пользователя, зарегистрированного на SMTP сервере (см. рис. 2).

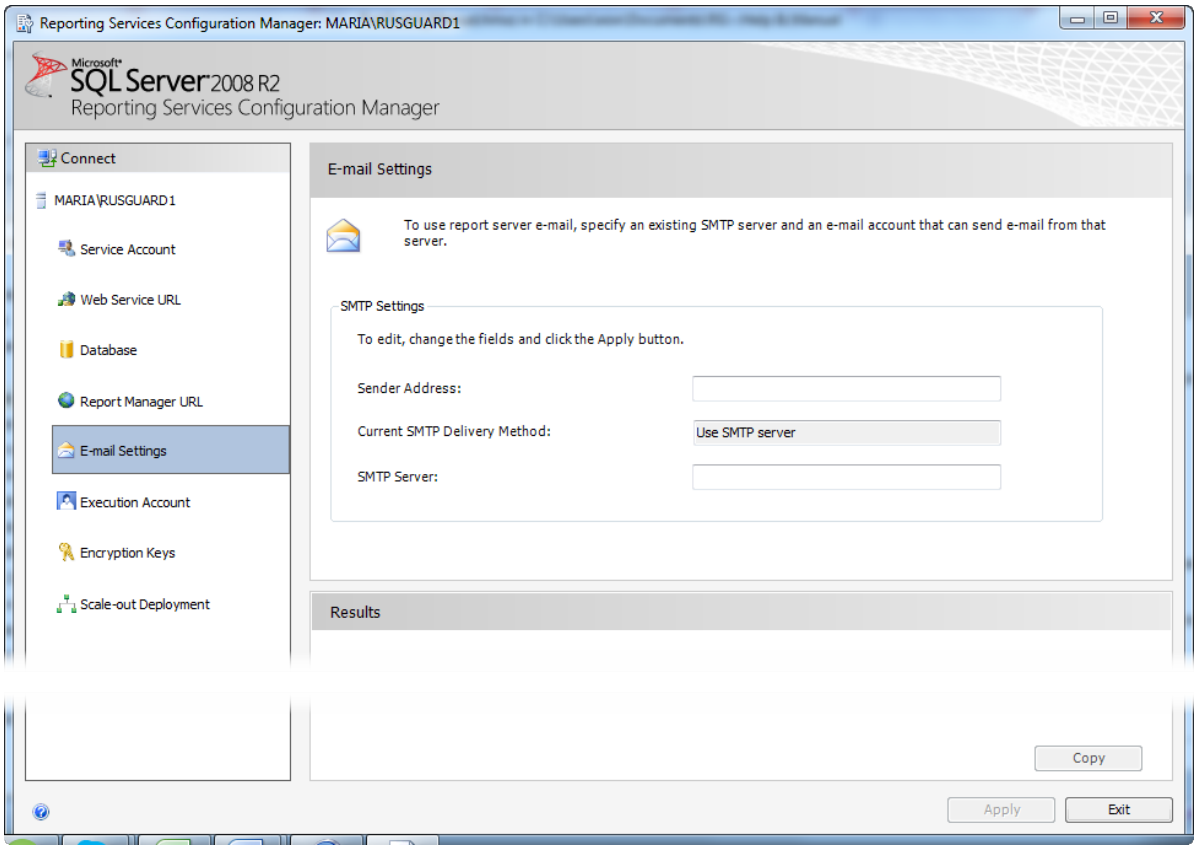


Рисунок 2 - АРМ RusGuard. Настройка подписок Сервера Отчетов через электронную почту

Обратите внимание, что настроеный SMTP-сервер может уже существовать в организации. Необходимо знать его адрес и зарегистрированного пользователя. Сервер должен поддерживать режим ***без аутентификации***.

Также его можно настроить на сервере RusGuard, включив соответствующие компоненты в Windows (см. https://msdn.microsoft.com/library), либо использовать в качестве SMTP-сервера стороннюю программу (одна из возможных бесплатных - Courier Mail Server).

3. Зайдите в WEB-интерфейс сервера отчетов.
4. Откройте контекстное меню и выберите пункт ***Подписка.***
5. Выполните процедуру аналогично предыдущей. При этом в качестве способа доставки выберите вариант Электронная почта, укажите данные получателя и желаемый формат письма с отчетом.

Настройка Courier Mail Server

1. Выполните настройку параметров Сервисов:

- порт 25, автоматический запуск

- вкладка Доступ, Разрешить
- Дополнительно, Разрешить отправку внешней почты группе Local

2. Выполните настройку параметров Пользователей:
   - Ввести имя пользователя (Email), от которого осуществляется отправка. Любой. Должен совпадать с тем, который указали в менеджере RepServ. Пароль любой.
   - Установите флаг Внешний адрес.
   - Укажите аккаунт внешнего SMTP сервера, с которого осуществляется отправка
3. Выполните настройку параметров Планировщика/Расписания:
   - Удалить
4. Выполните настройку параметров Отправки/SMTP-сервера: выберите имеющуюся запись и укажите верные параметры внешнего SMTP-сервера

Настройка автозапуска

Вы можете настроить автозапуск АРМ RusGuard через ярлык на Рабочем столе без ввода пароля. То есть, пароль задается в настройках ярлыка, после чего его не требуется вводить при каждом запуске АРМ.

Для того чтобы настроить автозапуск:

1. Если необходимо, создайте новое рабочее место 156.
2. Создайте ярлык АРМ RusGuard на рабочем столе. Для это щелкните правой кнопкой мыши по рабочему столу, выберите ***Создать*** > ***Ярлык***. Используя навигацию по дереву каталогов своего ПК, найдите папку, где установлено ПО RusGuard и установите ссылку на файл `VVIWorkstation.exe` (см. рис. 3). Ссылка отобразится в окне ***Укажите расположение объекта***. Ссылка заключена в кавычки.

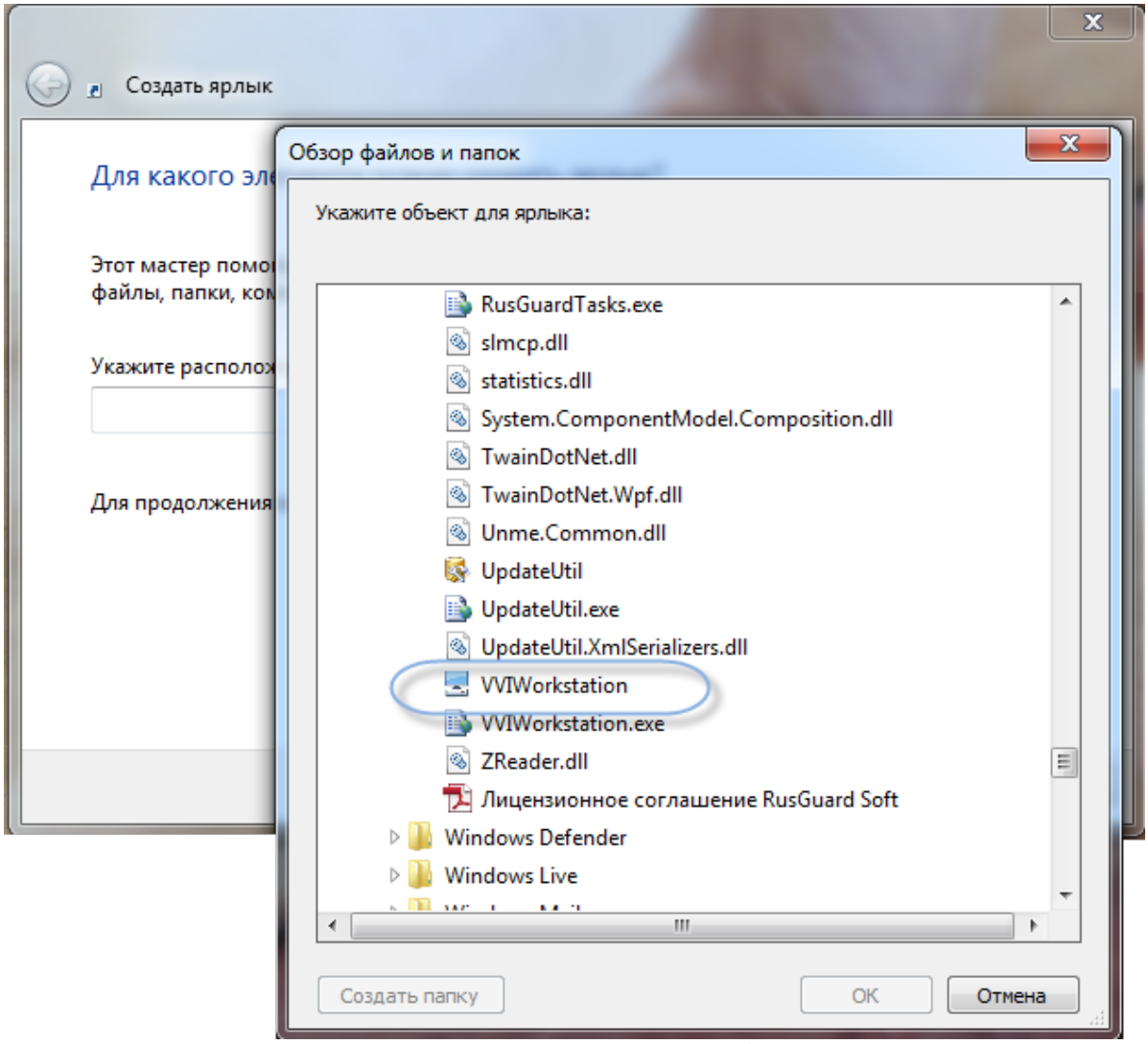


Рисунок 3 - АРМ RusGuard. Создание ярлыка на Рабочем столе.

3. **После кавычек и одного пробела** введите параметры своего АРМ в формате Login Password WorkplaceID. Если пароль не используется, то не вводится никакое значение. Workplace ID - Идентификатор рабочего места, который присваивается создаваемому рабочему месту автоматически. Чтобы узнать его, перейдите в модуль ***Конфигурация рабочих мест***, откройте нужное рабочее место, перейдите на вкладку ***Настройки*** (см. рис. 4).

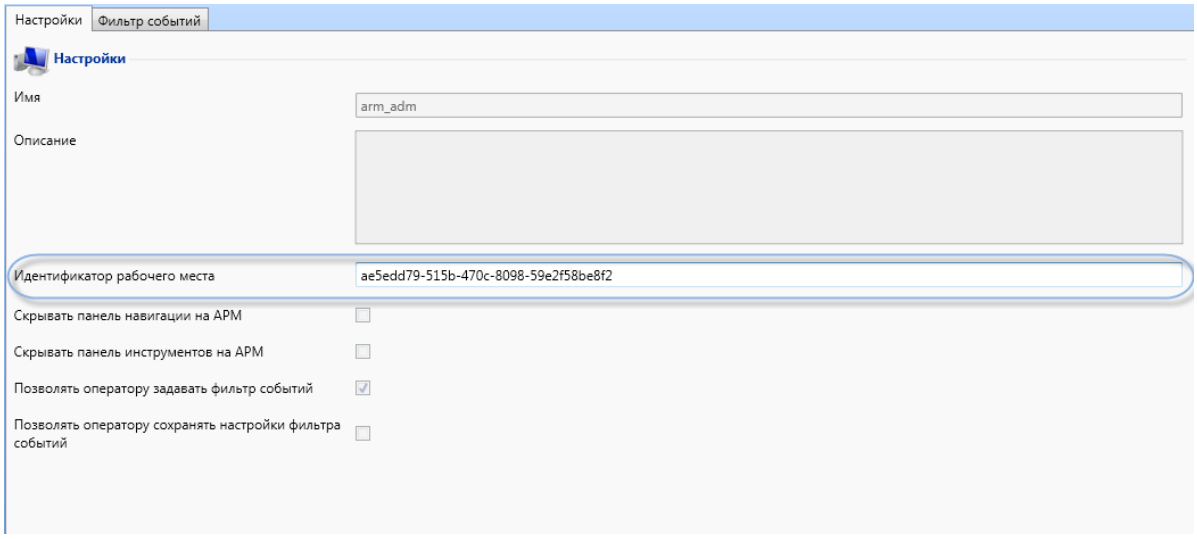


Рисунок 4 - АРМ RusGuard. Модуль Конфигурация рабочих мест. Идентификатор рабочего места.

- Например, если пароль используется, строка может иметь следующий вид: `"C:\Program Files (x86)\VVI Investment\RusGuard\VVIWorkstation.exe" 127.0.0.1 admin 12345 eee1c1e1-dbcd-4978-be9c-e71f52938c5c`
- Если пароль не используется: `"C:\Program Files (x86)\VVI Investment\RusGuard\VVIWorkstation.exe" 127.0.0.1 admin empty eee1c1e1-dbcd-4978-be9c-e71f52938c5c`

4. Завершите процесс создания ярлыка.
5. Проверьте функцию: при запуске АРМ через ярлык шаг ввода учетных данных пропускается, оператор попадает непосредственно в свое рабочее место.

Если изменено имя компьютера

Если изменено имя компьютера, на котором установлено ПО RusGuard, необходимо также изменить настройки сервера отчетов. Для этого выполните процедуру аналогичную, приведенной здесь 286.

Настройка полномочий операторов при помощи меток

Предварительные условия

Пользователь, отвечающий за настройку прав доступа операторов, должен обладать доступом к модулям ***Конфигурация оборудования*** 79 и ***Конфигурация системы*** 172 АРМ и ***Конфигурация СКУД*** 135 с соответствующими правами, (см. рис. 5).

Задача и последовательность действий

`Задача: Разграничение прав доступа операторов в разрезе сущностей СКУД (групп сотрудников, уровней доступа, точек доступа, устройств).`

Для того чтобы иметь возможность настраивать доступ с использованием меток, необходимо выполнить следующие действия:

1. Создать группу 172 пользователей в модуле ***Конфигурация системы***. Добавить в нее пользователей, для которых планируется настроить доступ.
2. Создать метку/и 206 в модуле ***Конфигурация системы***.
3. Привязать метку/метки к различным сущностям системы (в зависимости от поставленных задач):
   i. Привязка метки к устройству 90
   ii. Привязка метки к точке доступа 113
   iii. Привязка метки к уровню доступа см. здесь 69 (создание уровня доступа) и здесь 153 (редактирование, привязка меток).
   iv. Привязка метки к группе сотрудников см. здесь 69 (создание группы) и здесь 135 (настройка меток для группы).
   v. Настройка полномочий группы с использованием меток 174.
4. Выполнить настройку доступа группы операторов с использованием меток 174 в модуле ***Конфигурация системы***.

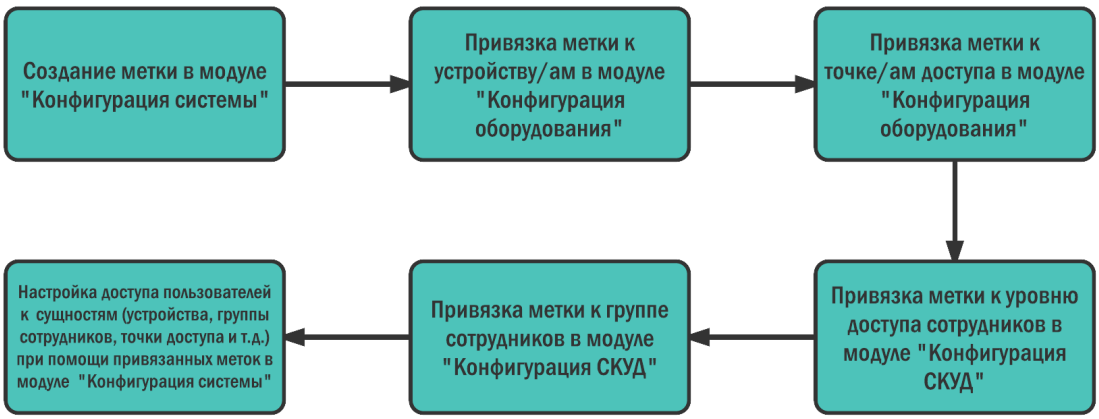


Рисунок 5 - Схема процесса управления доступом через метки

Используя данный алгоритм вы можете создать несколько групп операторов с разным доступом в системе.

Создание учетной записи оператора АРМ

Как правило, оператор АРМ имеет доступ к одному или нескольким следующим модулям:

- ***Фотоидентификация***
- ***Планы***
- ***Отчеты***

В его обязанности могут входить все или некоторые задачи, перечисленные ниже:

- Мониторинг прихода и ухода сотрудников;
- Управление устройствами точек доступа;
- Формирование и просмотр отчетов системы.

Создание учетной записи оператора АРМ (Мониторинг)

Предварительные условия

Пользователь, создающий учетную запись (записи) оператора, должен обладать доступом к модулям ***Конфигурация рабочих мест*** 155 и ***Конфигурация системы*** 172 АРМ и ***Конфигурация СКУД*** 135 с соответствующими правами.

Задача и последовательность действий

Задача: Создание учетной записи оператора АРМ для мониторинга прохода сотрудников и гостей объекта через точку доступа "А", а также видеонаблюдение через камеру, установленную возле точки доступа (см. рис. 6).

Для того чтобы создать учетную запись оператора с указанными задачами, необходимо выполнить следующие действия:

1. Создать рабочее место 156 "Оператор мониторинга" (название произвольно, используется для примера) в модуле ***Конфигурация рабочих мест***.
2. Настроить в рабочем месте модуль 163 ***Фотоидентификация*** 163 с привязанным к нему драйвером точки доступа "А" и драйвером соответствующей камеры или камер (т.е. не менее двух ячеек в экране модуля).
3. Настроить в рабочем месте модуль 160 ***Планы*** 160. К модулю должна быть привязана схема соответствующего участка с установленными на ней драйверами точки доступа "А" и соответствующей камеры (камер).
4. Создать группу пользователей 172 в модуле ***Конфигурация системы*** (если группа еще не создана).
5. Предоставить созданной группе полномочия 174 на доступ к рабочему месту "Оператор мониторинга".
6. Создать учетную запись пользователя 176 в модуле ***Конфигурация системы***, привязать ее к созданной группе.
7. Пользователь автоматически получит доступ к рабочему месту "Оператор мониторинга", поскольку система автоматически присваивает создаваемым пользователям права родительской группы. Вы также можете отредактировать права конкретного пользователя, если его служебные обязанности изменятся.

Рисунок 6 - Общая процедура создания учетной записи оператора АРМ и с определенным уровнем доступа (оператор мониторинга).

Используя данный алгоритм вы можете создать несколько рабочих мест с одинаковым набором модулей, для обслуживания разных точек доступа (допустим, Оператор мониторинга: 1-й этаж, Оператор мониторинга: 2-й этаж и т.д.).

См. также:

- ***Модуль Планы*** 239
- ***Модуль Фотоидентификация*** 248

Создание учетной записи оператора АРМ_2

Предварительные условия

Пользователь, создающий учетную запись (записи) оператора, должен обладать доступом к модулям ***Конфигурация рабочих мест*** 155 и ***Конфигурация системы*** 172 АРМ и ***Конфигурация СКУД*** 135 с соответствующими правами (см. рис. 7).

Задача и последовательность действий

`Задача: Создание учетной записи оператора АРМ для мониторинга прохода и выгрузки отчетов системы.`

Для того чтобы создать учетную запись оператора с указанными задачами, необходимо выполнить следующие действия:

1. Создать рабочее место 156 "Менеджер отчетов" (название произвольно, используется для примера) в модуле ***Конфигурация рабочих мест***.
2. Настроить в рабочем месте модуль 214 ***Отчеты*** 214.
3. Создать группу пользователей 172 в модуле ***Конфигурация системы*** (если группа еще не создана).
4. Предоставить созданной группе полномочия 174 на доступ к рабочему месту "Менеджер отчетов".
5. Создать учетную запись пользователя 176 в модуле ***Конфигурация системы***, привязать ее к созданной группе.

6. Пользователь автоматически получит доступ к рабочему месту "Менеджер отчетов", поскольку система автоматически присваивает создаваемым пользователям права родительской группы. Вы также можете отредактировать права конкретного пользователя, если его служебные обязанности изменятся.

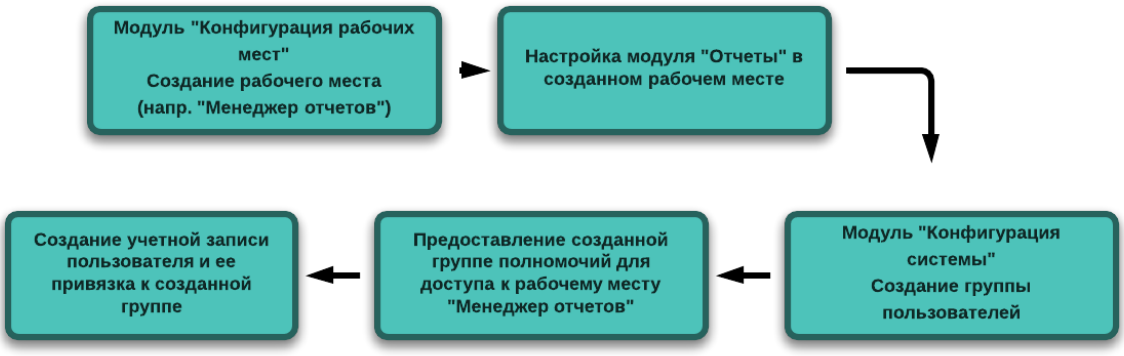


Рисунок 7 - Общая процедура создания учетной записи оператора АРМ и с определенным уровнем доступа (менеджер отчетов).

Примечание: Вы также можете настроить доступ к модулю ***Отчеты*** без установки АРМ RusGuard. Для этого необходимо создать учетную запись пользователя с правом доступа к отчетам непосредственно на сервере отчетов.

Подробнее о настройке сервера отчетов см. в разделе Установка сервера RusGuard 31.

Создание учетной записи сотрудника

Предварительные условия

Пользователь, создающий учетную запись (записи) сотрудника, должен обладать доступом к модулю ***Конфигурация СКУД*** 135 с соответствующими правами (см. рис. 8).

Кроме того, для корректного ввода копий документов сотрудника и присвоения ему карточки доступа, необходимо установить модуль ABBYY Passport Reader SDK, а также подключить к компьютеру считывающее устройство (либо иметь доступ к считывающему устройству контроллера, подключенного к системе).

Задача и последовательность действий

Задача: создание учетной записи сотрудника для осуществления доступа на объект, контролируемый системой.

Для того чтобы создать учетную запись сотрудника с указанными задачами, необходимо выполнить следующие действия:

1. Создайте новый уровень доступа 67 в модуле ***Конфигурация СКУД*** (если это необходимо).
2. Привяжите к уровню доступа одну или несколько точек доступа 67.
3. Если это необходимо, создайте расписания для точек доступа 147.
4. Привяжите созданные расписания к соответствующим уровням доступа 152.
5. Создайте должность 69 в модуле ***Конфигурация СКУД*** (если это необходимо).
6. Создайте группу сотрудников 69 в модуле ***Конфигурация СКУД*** (если это необходимо).
7. Присвойте созданной группе сотрудников нужный уровень доступа 69.
8. Создайте учетную запись сотрудника в требуемой группе 70.
9. Заполните карточку сотрудника, в том числе:
   i. Внесите данные о документах сотрудника 145;
   ii. Оформите электронный пропуск 71 (карточку).
10. По умолчанию сотруднику присваивается уровень доступа родительской группы. Если это необходимо, присвойте сотруднику другой/дополнительный уровень доступа 137.

Рисунок 8 - Общая процедура создания учетной записи сотрудника

Подключение устройств

ПО RusGuard предусматривает несколько вариантов подключения устройств и их привязки к уровням доступа:

- Подключение устройства с использованием существующего уровня доступа 269:
  - С использованием АРМ;
  - С использованием утилиты Сервисный конфигуратор оборудования 321 и АРМ 76.
- Подключение устройства и создание нового уровня доступа 271:
  - С использованием АРМ
  - С использованием утилиты Сервисный конфигуратор оборудования 321 и АРМ 76.

Подключение устройств (существующий уровень доступа)

Последовательность действий

С использованием АРМ

Пользователь, подключающий устройства, должен обладать доступом к модулям Конфигурация оборудования 79 и Конфигурация СКУД 135 с соответствующими правами (см. рис. 9).

Для того чтобы подключить устройство к системе:

1. Подключите устройство физически через CAN-LAN/USB-CAN конвертер (см. также раздел Периферийные устройства 269).
2. Зайдите в модуль ***Конфигурация оборудования***. Выполните поиск и синхронизацию устройств 86.
3. В модуле ***Конфигурация оборудования*** выполните настройку точки доступа 92, контролируемой устройством.
4. Зайдите в модуль ***Конфигурация СКУД*** и привяжите к нужному уровню доступа одну или несколько точек доступа 67 (в зависимости от количества подключаемых устройств).
5. Оставаясь в модуле ***Конфигурация СКУД***, выполните настройку расписания для точки доступа 147, если это необходимо.
6. Оставаясь в модуле ***Конфигурация СКУД***, привяжите расписание к точке доступа 152.

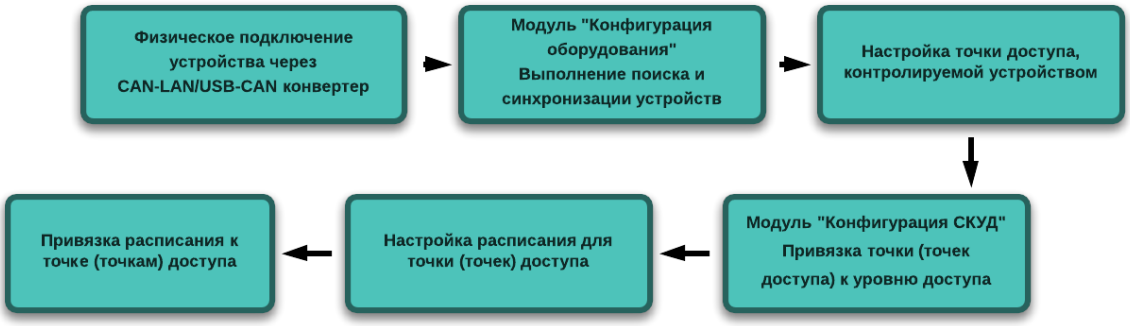


Рисунок 9 - Подключение устройств через АРМ

С использованием утилиты Сервисный конфигуратор оборудования

Для того чтобы подключить устройство к системе:

1. Подключите устройство физически через CAN-LAN/USB-CAN конвертер 413.
2. Запустите утилиту ***Сервисный конфигуратор оборудования*** 321 (см. рис. 10).
3. Выполните настройку устройства, в том числе, ключей 326. Сохраните данные в самом устройстве.
4. Зайдите в модуль ***Конфигурация оборудования***. Выполните поиск и синхронизацию устройств 86.
5. В модуле ***Конфигурация оборудования*** выполните настройку точки доступа, контролируемой устройством.
6. Зайдите в модуль ***Конфигурация СКУД*** и привяжите к созданному уровню доступа одну или несколько точек доступа (в зависимости от количества подключаемых устройств).
7. Оставаясь в модуле ***Конфигурация СКУД***, выполните настройку расписания для точки доступа, если это необходимо.
8. Оставаясь в модуле ***Конфигурация СКУД***, привяжите расписание к точке доступа.

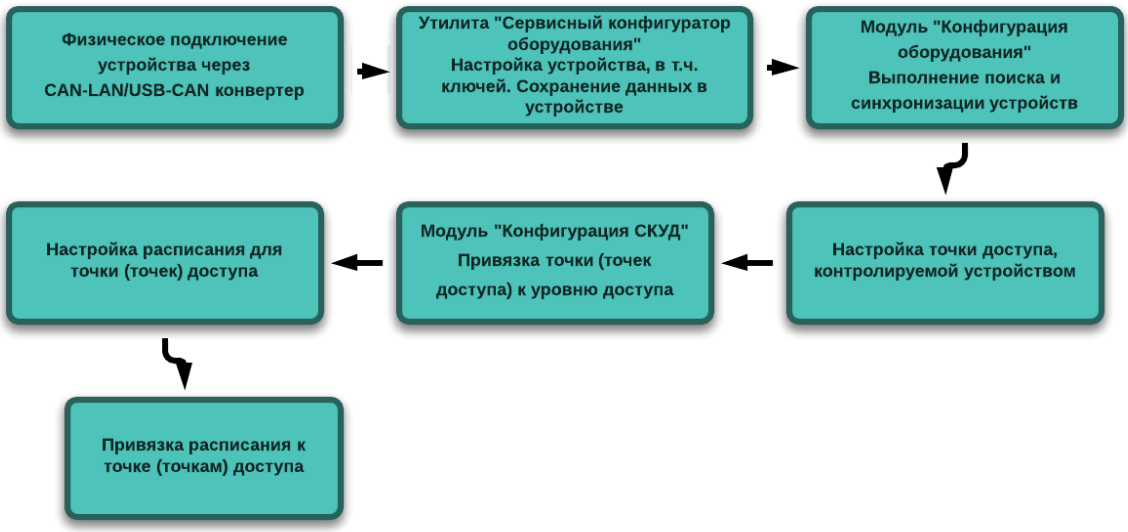


Рисунок 10 - Подключение устройств через утилиту "Сервисный конфигуратор оборудования" и АРМ

За более подробной информацией об использовании APM RusGuard 76 обратитесь к соответствующему руководству.

Подключение устройств (новый уровень доступа)

Последовательность действий

С использованием АРМ

Пользователь, подключающий устройства, должен обладать доступом к модулям ***Конфигурация оборудования*** 79 и ***Конфигурация СКУД*** 135 с соответствующими правами (см. рис. 11).

Для того чтобы подключить устройство к системе:

1. Подключите устройство физически через CAN-LAN/USB-CAN конвертер (см. также раздел Периферийные устройства 269).
2. Зайдите в модуль ***Конфигурация оборудования***. Выполните поиск и синхронизацию устройств 86.
3. В модуле ***Конфигурация оборудования*** выполните настройку точки доступа 92, контролируемой устройством.
4. Зайдите в модуль ***Конфигурация СКУД*** и создайте новый уровень доступа 67.
5. Привяжите к созданному уровню доступа одну или несколько точек доступа 67 (в зависимости от количества подключаемых устройств).
6. Оставаясь в модуле ***Конфигурация СКУД***, выполните настройку расписания для точки доступа 147, если это необходимо.
7. Оставаясь в модуле ***Конфигурация СКУД***, привяжите расписание к точке доступа 152.

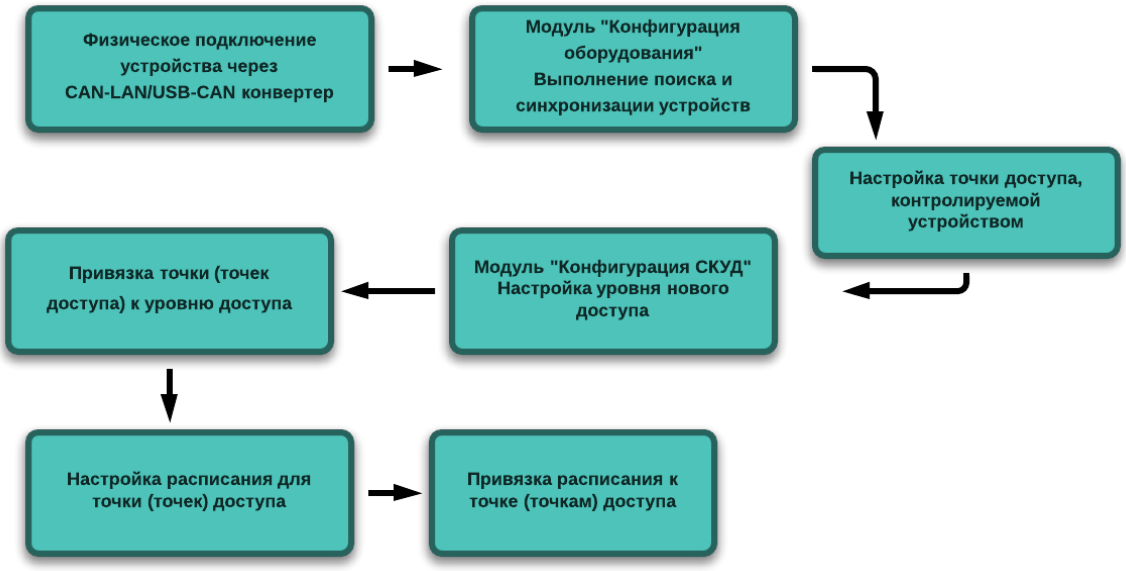


Рисунок 11 - Подключение устройств через и АРМ

С использованием утилиты Сервисный конфигуратор оборудования

Для того чтобы подключить устройство к системе:

1. Подключите устройство физически через CAN-LAN/USB-CAN конвертер 413.
2. Запустите утилиту ***Сервисный конфигуратор оборудования*** 321 (см. рис. 12).
3. Выполните настройку устройства, в том числе, ключей 326. Сохраните данные в самом устройстве.
4. Зайдите в модуль ***Конфигурация оборудования***. Выполните поиск и синхронизацию устройств.
5. В модуле ***Конфигурация оборудования*** выполните настройку точки доступа, контролируемой устройством.
6. Зайдите в модуль ***Конфигурация СКУД*** и создайте новый уровень доступа.
7. Привяжите к созданному уровню доступа одну или несколько точек доступа (в зависимости от количества подключаемых устройств).
8. Оставаясь в модуле ***Конфигурация СКУД***, выполните настройку расписания для точки доступа, если это необходимо.
9. Оставаясь в модуле ***Конфигурация СКУД***, привяжите расписание к точке доступа.

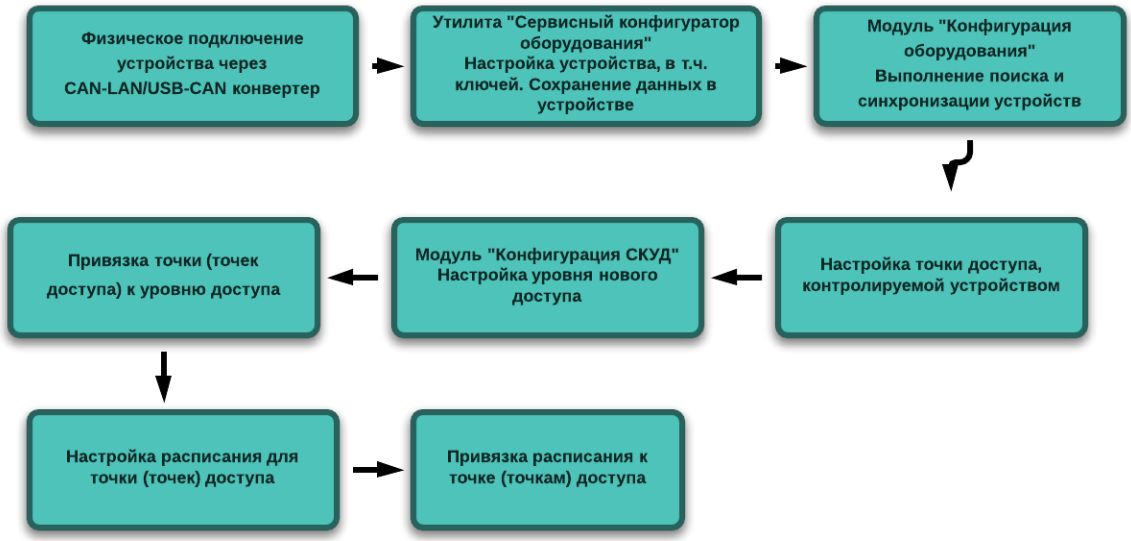


Рисунок 12 - Подключение устройств через утилиту "Сервисный конфигуратор оборудования" и АРМ

За более подробной информацией об использовании АРМ RusGuard обратитесь к соответствующему разделу руководства 76.

Настройка режима Запрета повторного входа

Предварительные условия

Пользователь, настраивающий режим Запрета повторного входа (Antipassback, АПБ), должен обладать доступом к модулям ***Конфигурация оборудования*** 79 и ***Конфигурация СКУД*** 135 с соответствующими правами.

Кроме того, для корректного ввода копий документов сотрудника и присвоения ему карточки доступа, необходимо установить модуль ABBYY Passport Reader SDK 390, а также подключить к компьютеру считывающее устройство (либо иметь доступ к считывающему устройству контроллера, подключенного к системе).

Задача и последовательность действий

Задача: настройка режима запрета повторного входа (АПБ), т.е. запрет возможности выполнить вход по одной и той же карточке не выходя из зоны, контролируемой системой (см. рис. 13).

Для того чтобы настроить режим АПБ:

1. Зайдите в модуль ***Конфигурация оборудования*** 79.
2. Выполните поиск устройств/а, для которых/ого будет настроен режим. Также, если необходимо, выполните подключение устройств 269.
3. Перейдите к настройкам контроллера и точки доступа 92 и установите флаг ***Запрет повторного входа*** в конфигурации "геркона" точки доступа.
4. Выберите режим:
   - *Локальный* для единственного контроллера;
   - *Глобальный* для нескольких контроллеров. Обратите внимание, что настройки глобального режима следует установить на всех контроллерах, для которых настраивается АПБ.
5. Пронумеруйте внешнюю и внутреннюю зоны. По умолчанию установлены значения 0 и 1. Максимальное значение - 250.
6. Перейдите в модуль ***Конфигурация СКУД*** 135.
7. Создайте расписание 147 для АПБ. Обратите внимание, что использование АПБ невозможно со встроенными расписаниями.
8. Привяжите к точке доступа пользовательское расписание для АПБ 152. Установите флаг ***Запрет повторного входа*** в дополнительных настройках точки доступа.
9. Создайте нужный уровень доступа 67, либо зайдите в настройки существующего. Привяжите точку/и доступа, для которой/ых настраивается АПБ, к уровню доступа 67.
10. Выполните привязку уровня доступа к учетным записям сотрудников, которые будут осуществлять доступ на объект через точки доступа, где настроен АПБ.

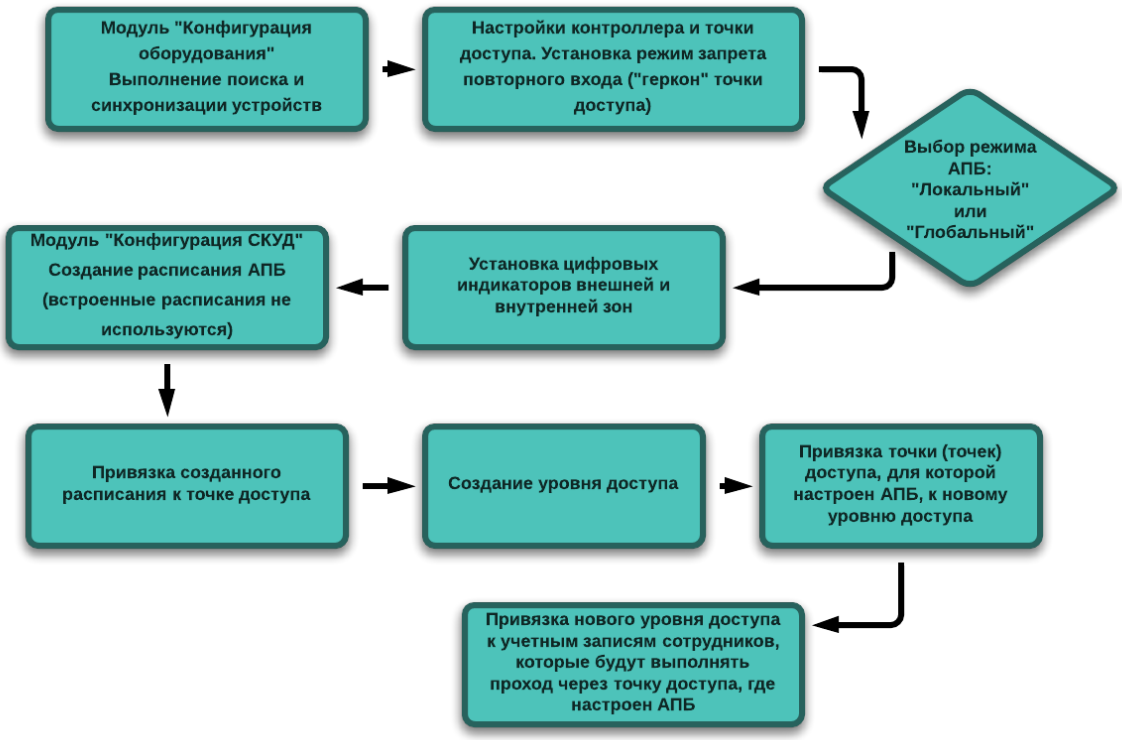


Рисунок 13 - Настройка режима запрета повторного прохода (АПБ)

Настройка доступа к отчетам через web-интерфейс

При необходимости возможно использование модуля ***Отчеты*** 214 без установки АРМ RusGuard. Для этого необходимо обеспечить оператору, использующему отчеты доступ к серверу отчетов через стандартный веб-интерфейс (создать на нем учетную запись).

См. также раздел ***Установка SQL-Сервера и настройка сервера отчетов*** 48

Предварительные условия

Пользователь, создающий учетные записи на сервере отчетов, должен обладать правами администратора на ПК, с которого выполняется настройка.

Задача и последовательность действий

`Задача: доступ к серверу отчетов через веб-интерфейс.`

Для того чтобы создать учетную запись оператора на сервере отчетов:

1. Откройте окно браузера с разрешением ***Запуск от имени администратора*** (меню ***Пуск*** > ***Все программы*** > ***Internet Explorer*** > ***Запуск от имени администратора***).

Откроется окно с требованием подтвердить или отменить действие.

2. Чтобы продолжить, нажмите на кнопку ***Да***.
3. Добавьте в список URL-адресов адрес диспетчера отчетов.

i. Выберите меню ***Сервис***.
ii. Выберите пункт ***Свойства браузера***.
iii. Перейдите на вкладку ***Безопасность***.
iv. Выберите ***Надежные сайты***.
v. Нажмите на кнопку ***Сайты***.
vi. Добавьте адрес сервера отчетов ***http://<имя-сервера>***.

Примечание: Если для сайта по умолчанию не используется HTTPS, снимите флажок ***Для всех сайтов этой зоны требуется проверка серверов (https:)***.

4. Нажмите на кнопку ***Добавить***.
5. Нажмите на кнопку ***ОК***.
6. На домашней странице диспетчера отчетов щелкните ссылку ***Параметры папки***.
7. На странице настроек папки щелкните пункт ***Безопасность*** (см. рис. 14).

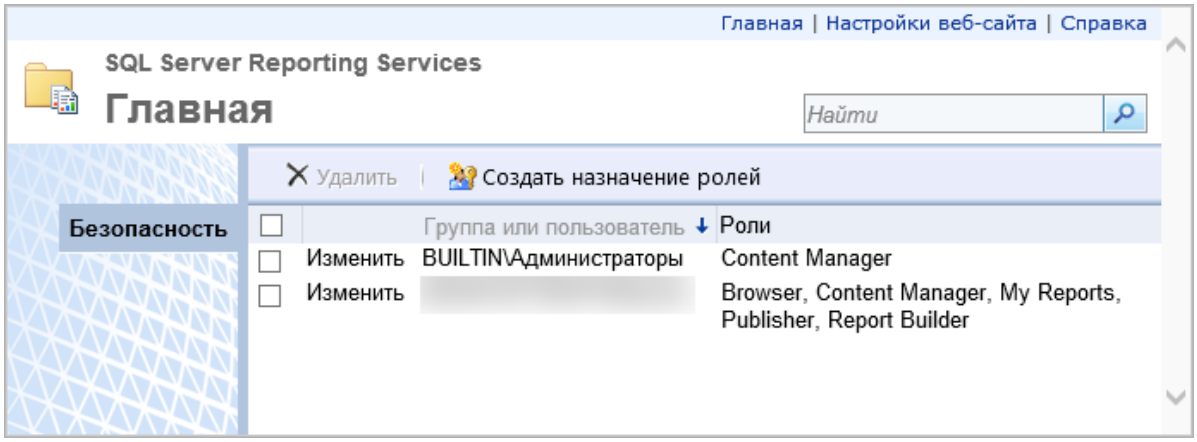


Рисунок 14 - Настройка сервера отчетов. Настройка доступа к папке

8. Нажмите на кнопку ***Создать назначения ролей***.
9. Введите имя учетной записи Windows пользователя, которому предоставляется доступ, в формате: `<домен>\<пользователь>`.
10. Выберите ***Диспетчер содержимого***.
11. Нажмите кнопку ***ОК***.
12. В верхнем углу домашней страницы нажмите на кнопку ***Настройки веб-сайта*** (см. рис. 15).

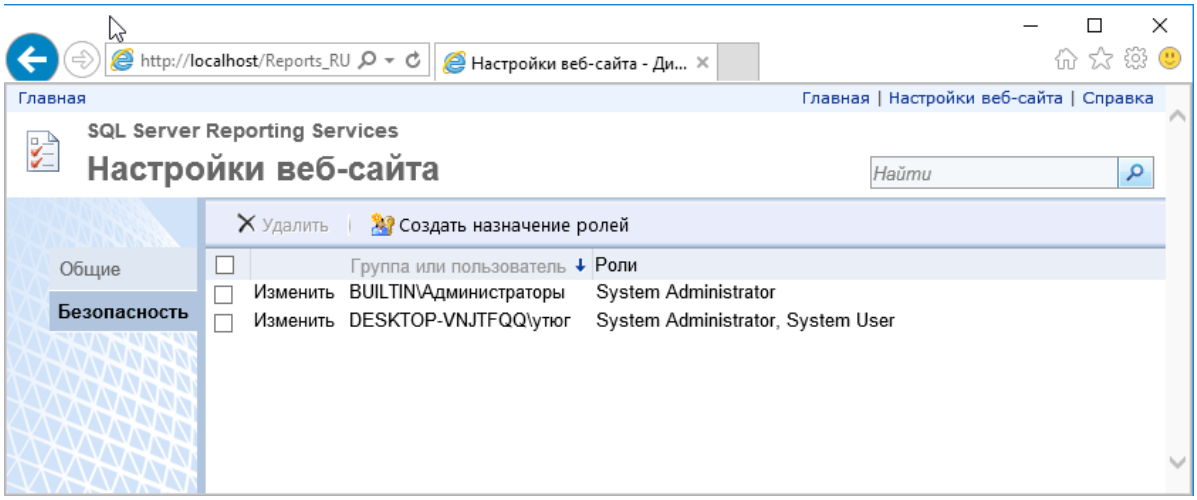


Рисунок 15 - Настройка сервера отчетов. Настройка сайта

13. Щелкните мышью пункт ***Безопасность***.
14. Нажмите на кнопку ***Создать назначения ролей***.
15. Введите имя учетной записи Windows пользователя, для которого создается доступ, в формате: `<домен>\<пользователь>`.
16. Выберите уровень доступа, соответствующий обязанностям пользователя (например, *Системный пользователь*).
17. Нажмите на кнопку ***ОК***.
18. Закройте окно диспетчера отчетов в браузере.
19. Повторно откройте диспетчер отчетов в Internet Explorer без использования режима ***Запуск от имени администратора***.

Использование режима повторного приложения карточки

ПО RusGuard Soft позволяет настраивать режим повторного приложения карточки, то есть при повторном приложении карточки-пропуска к считывающему устройству выполняется определенная операция (см. рис. 16).

Режим не может быть настроен для точек доступа типа турникет и шлагбаум (не имеет смысла).

Предварительные условия

Пользователь (администратор), обладающий доступом к модулям ***Конфигурация оборудования*** 79 и ***Конфигурация СКУД*** 135.

Задача и последовательность действий

`Задача: настройка режима повторного приложения карточки.`

Для того чтобы настроить режим повторного приложения карточки:

1. Зайдите в модуль ***Конфигурация оборудования*** 79.
2. Выполните поиск устройств/а, для которых/ого настраивается режим.
3. Перейдите к настройкам определенного устройства, затем перейдите на вкладку точки доступа 92 (например, двери).
4. Убедитесь, что "геркон" включен. Установите один или несколько режимов второго приложения ключа.

Обратите внимание, что набор режимов может отличаться для разных типов точек доступа.

5. Перейдите в модуль Конфигурация СКУД 135.
6. Создайте уровень доступа 67 для использования с режимом повторного приложения карточки на той точке (точках) доступа, которая (которые) были настроены ранее, либо отредактируйте существующий уровень доступа соответствующим образом. Необходимо выполнить следующие действия:
   i. зайти в список точек доступа, выбрать в нем нужную.

См. также ***Привязка точки доступа к уровню доступа*** 67.

   ii. привязать к точке доступа любое подходящее расписание 152, кроме ***Генерального***.

См. также ***Управление расписаниями*** 147.

   iii. в области ***Дополнительные настройки*** установить флаги для действий, выполняемых при повторном приложении карточки (см. табл. 1).

7. Привяжите созданный/настроенный уровень доступа к группе пользователей 69 (или конкретному пользователю 137).

Рисунок 16 - Настройка режима повторого приложения ключа

Описание операций при повторном приложении карточки-ключа

Таблица 1 - Повторное приложение карточки. Операции и действия		
Операция	Дверь	Две двери
Открыть надолго Уровень доступа с расписанием 147 ***Всегда*** не может открывать надолго	1. Приложить идентификатор (карточку-ключ) к считывателю ***Вход или Выход***. 2. Открыть дверь. 3. Приложить идентификатор к считывателю ***Вход или Выход***.	1. Приложить идентификатор к считывателю ***Вход***. 2. Открыть дверь. 3. Приложить идентификатор к считывателю ***Вход***.
Снять режим Открыть надолго Уровень доступа с расписанием ***Всегда*** не сможет закрыть дверь, если она находится в режиме ***Открыть надолго***	1. Приложить идентификатор к считывателю ***Вход или Выход***. 2. Открыть дверь. 3. Приложить идентификатор к считывателю ***Вход или Выход***. 4. Закрыть дверь.	1. Приложить идентификатор к считывателю ***Вход***. 2. Открыть дверь. 3. Приложить идентификатор к считывателю ***Вход***. 4. Закрыть дверь.
Включить режим Блокировать Если точка доступа заблокирована, то при использовании расписания ***Всегда*** проход невозможен	1. Приложить идентификатор к считывателю ***Выход***. 2. Приложить идентификатор к считывателю ***Выход*** повторно.	

Таблица 1 - Повторное приложение карточки. Операции и действия		
	3. Открыть и закрыть дверь (для электромеханического замка).	
Снять режим Блокировать С расписанием ***Всегда*** снять режим блокировки нельзя	1. Приложить идентификатор к считывателю ***Выход***. 2. Приложить идентификатор к считывателю ***Выход*** повторно. 3. Открыть и закрыть дверь (для электромеханического замка).	
Поставить на охрану Если точка доступа под охраной, то при использовании расписания ***Всегда*** возможен вход, но не выход	1. Приложить идентификатор к считывателю ***Вход***. 2. Приложить идентификатор к считывателю ***Вход*** повторно. 3. Открыть и закрыть дверь (для электромеханического замка).	1. Приложить идентификатор к считывателю ***Вход***. 2. Приложить идентификатор к считывателю ***Вход*** повторно. 3. Открыть и закрыть дверь (для электромеханического замка).
Снятие с охраны С расписанием ***Всегда*** снятие с охраны невозможно	1. Приложить идентификатор к считывателю ***Вход***. 2. Открыть и закрыть дверь (для электромеханического замка).	1. Приложить идентификатор к считывателю ***Вход***. 2. Открыть и закрыть дверь (для электромеханического замка).

Создание шаблонов пропусков и вывод на печать

ПО RusGuard Soft позволяет создавать макеты пропусков и привязывать поля в них к полям карточки сотрудников (см. рис. 17).

Количество шаблонов не ограничено возможностями ПО, но зависит от лицензий.

Предварительные условия

Пользователь (администратор), обладающий доступом к модулям ***Конфигурация системы*** 172 и ***Конфигурация СКУД*** 135.

Задача и последовательность действий

Задача: настройка шаблона и вывод на печать пропусков.

Для того чтобы создать шаблон и применить его:

1. Создайте шаблон пропуска 207 в модуле ***Конфигурация системы*** 172.
2. Перейдите в модуль ***Конфигурация СКУД*** 135 и выполните распечатку пропусков из списка сотрудников.

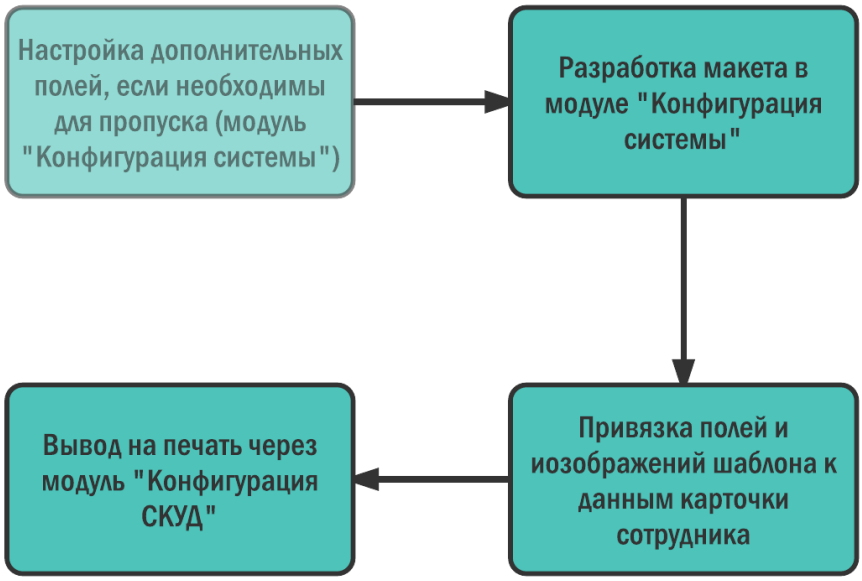


Рисунок 17 - Настройка шаблонов пропусков

Проход по решению оператора

Настройка режима прохода по решению оператора

Предварительные условия

Пользователь, настраивающий режим прохода по решению оператора, должен обладать доступом к модулю ***Конфигурация рабочих мест*** 155.

Задача и последовательность действий

Задача: настройка режима прохода по решению оператора.

Для того чтобы настроить режим прохода по решению оператора:

1. Зайдите в модуль ***Конфигурация рабочих мест*** 155.
2. Создайте новое рабочее место 156, содержащее модуль ***Фотоидентификация***, или используйте существующее.

Убедитесь, что режим прохода по решению оператора включен и доступен для оператора.

Использование режима прохода по решению оператора

Оператор модуля ***Фотоидентификация*** 248 АРМ RusGuard может использовать функцию разрешения/запрещения прохода, если эта функция настроена через модуль ***Конфигурация рабочих мест*** 155.

Для того чтобы использовать режим прохода по решению оператора:

1. Убедитесь, что режим настроен 282 в модуле ***Конфигурация рабочих мест*** 155 АРМ.
2. Зайдите в модуль ***Фотоидентификация*** 248. Убедитесь, что режим прохода по решению оператора активен в модуле (см. Модуль ***Фотоидентификация***, Пример 1 248 и Пример 2 249).

Автоматическое распознавание документов

Настройка автоматического распознавания

Предварительные условия

Пользователь, настраивающий функцию автоматического распознавания, должен обладать правами администратора на ПК, где выполняется настройка, и иметь доступ к модулю ***Конфигурация рабочих мест*** 155.

Задача и последовательность действий

Задача: установка ПО ABBYY PassportReader SDK и соответствующих драйверов.

Для того чтобы настроить функцию автоматического распознавания документов:

1. Выполните установку ПО ABBYY PassportReader SDK 390.
2. Установите драйверы для usb-лицензии ПО ABBYY PassportReader SDK 391.
3. Зайдите в модуль ***Конфигурация рабочих мест*** 155.
4. Создайте рабочее место, содержащее модуль ***Конфигурация СКУД*** 135 (либо перейдите к редактированию существующего).
5. Настройте режим отображения фотографий из распознаваемых документов 168, если это необходимо.

Использование автоматического распознавания

Предварительные условия

Пользователь, работающий с функцией автоматического распознавания, должен обладать доступом к модулю ***Конфигурация СКУД*** 135 APM RusGuard.

Для корректной работы функции должно быть установлено ПО ABBYY PassportReader SDK 390 и подключена USB-лицензия.

Также необходимо убедиться, что к компьютеру подключен сканер.

Задача и последовательность действий

Задача: использование функции автоматического распознавания документов через ABBYY PassportReader SDK.

Для того чтобы использовать функцию автоматического распознавания документов:

1. Запустите модуль ***Конфигурация СКУД*** 135 APM RusGuard.
2. Создайте новую учетную запись пользователя 70 (см. также раздел Быстрый старт 65) или найдите существующую 141.
3. Перейдите на вкладку ***Документы*** карточки сотрудника.

4. В зависимости от задач, выполните загрузку 144 или распознавание 145 документа.
5. Установите драйверы для usb-лицензии ПО ABBYY PassportReader SDK 391.

Настройка реакции: запись видео на камеру Ivideon

Для того чтобы настроить запись событий на видео:

1. Выполните настройку сервера и камер/ы Ivideon 378.
2. В настройках сервера Ivideon необходимо отредактировать настройки для **каждой из камер**, которые планируется использовать при настройке реакции. На вкладке ***Запись*** в настройках камера выберите режим ***Отключена*** (см. рис. 18).

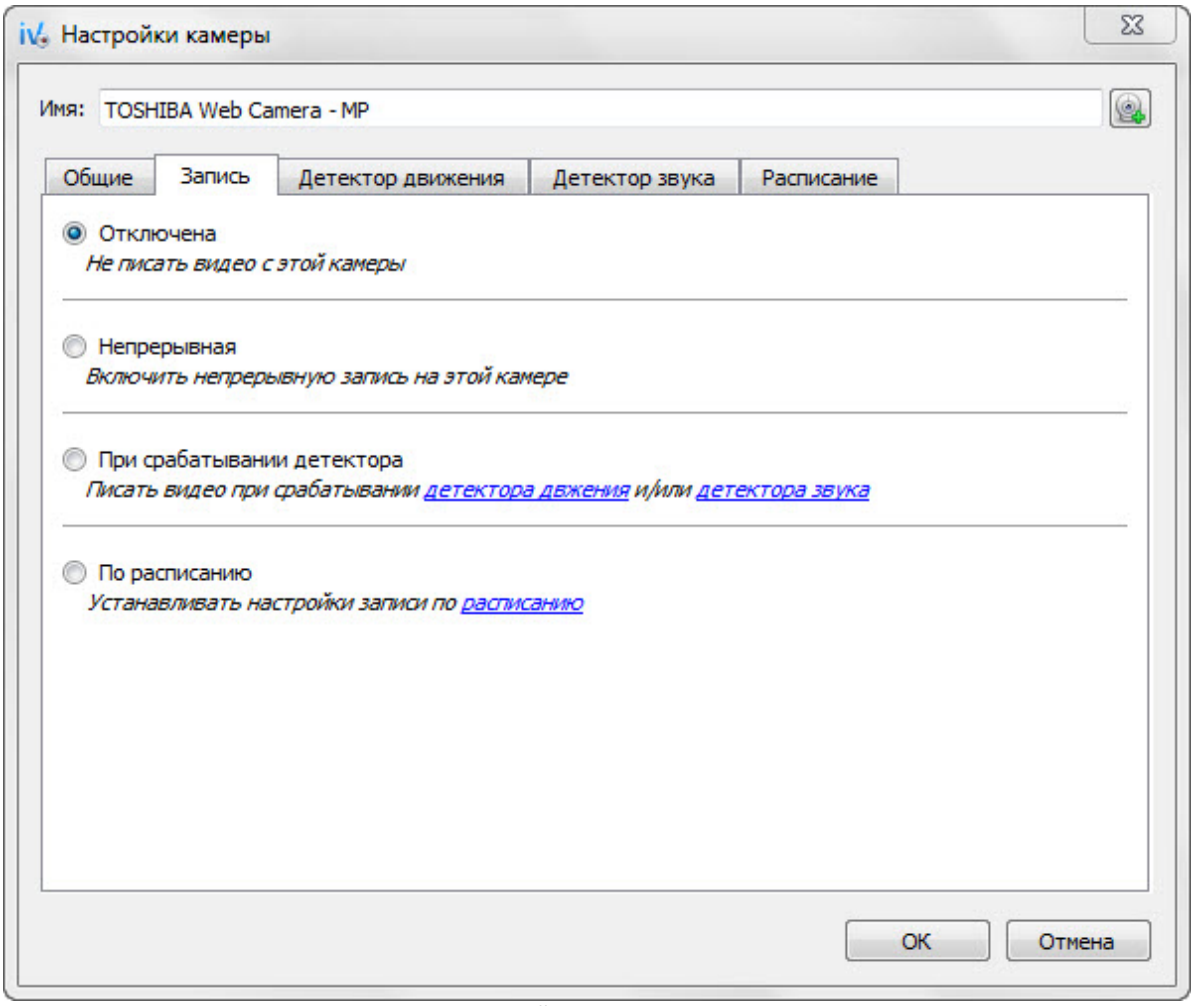


Рисунок 18 - Настройка режима записи для камеры

3. Выполните настройку реакции 193 стандартным образом.

При этом при настройке ***Действий***, выполняемых системой при наступлении настроенных ***Событий***, в списке ***Тип Действия*** выберите вариант ***Записать видео*** (см. рис. 19).

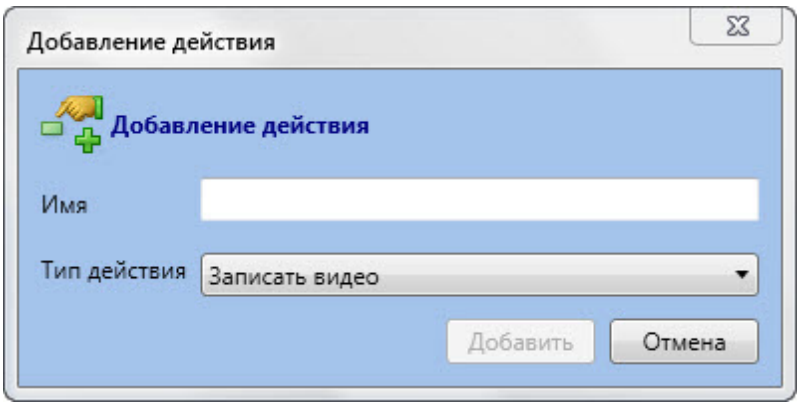


Рисунок 19 - Выбор типа действия: запись видео

4. В настройках действия выполните привязку одной из настроенных в системе камер Ivideon к ***Действию***. Кроме того, необходимо установить длительность буфера видео не менее заданного по умолчанию (см. рис. 20).

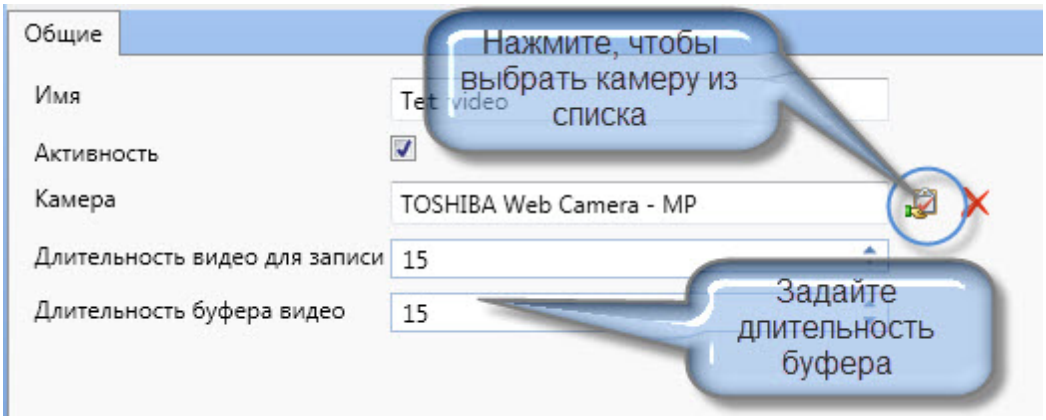


Рисунок 20 - Настройка параметров действия: привязка камеры

5. Сохраните настройки.

Типичные ошибки и их исправление

Имя ПК задано кириллическими символами

Локализация ошибки

Службы сервера отчетов, все версии ПО RusGuard.

Ознакомьтесь также с обязательными требованиями к установке 29

Описание и устранене ошибки

Если в процессе установки оказалось, что ПК имеет имя, заданное кириллическими символами, после смены имени и перезагрузки ПК необходимо также изменить настройки конфигурации БД сервера отчетов через утилиту Reporting Services Configuration Manager.

В противном случае, при попытках установки ПО RusGuard Soft система будет обращаться к серверу отчетов, используя прежние учетные данные.

Для того чтобы изменить настройки конфигурации БД сервера отчетов:

1. Запустите утилиту Reporting Services Configuration Manager (меню ***Пуск >*** папка ***Microsoft SQL Server 2008 R2 >*** подпапка ***Configuration Tools > Reporting Services Configuration Manager***).

Для запуска утилиты потребуется ввести имя ПК (сервера), где требуется изменить конфигурацию, и выбрать инстанс сервера отчетов (см. рис. 1).

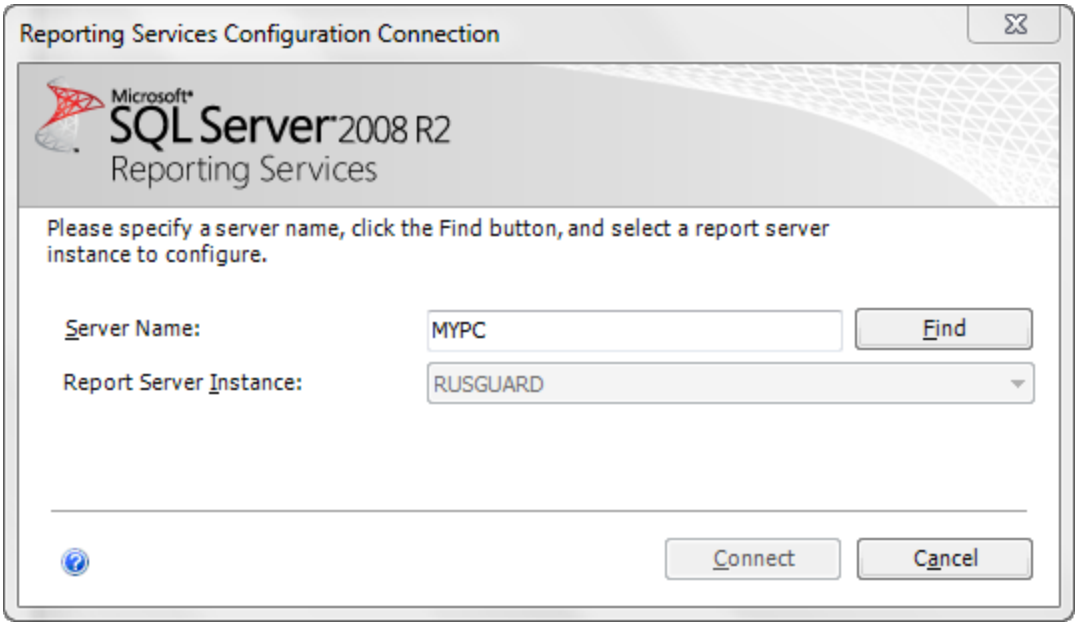


Рисунок 1 - Выбор ПК (сервера) и инстанса сервера отчетов

2. Введите учетные данные.
3. В навигационной панели слева выберите пункт ***Database*** (см. рис. 2).

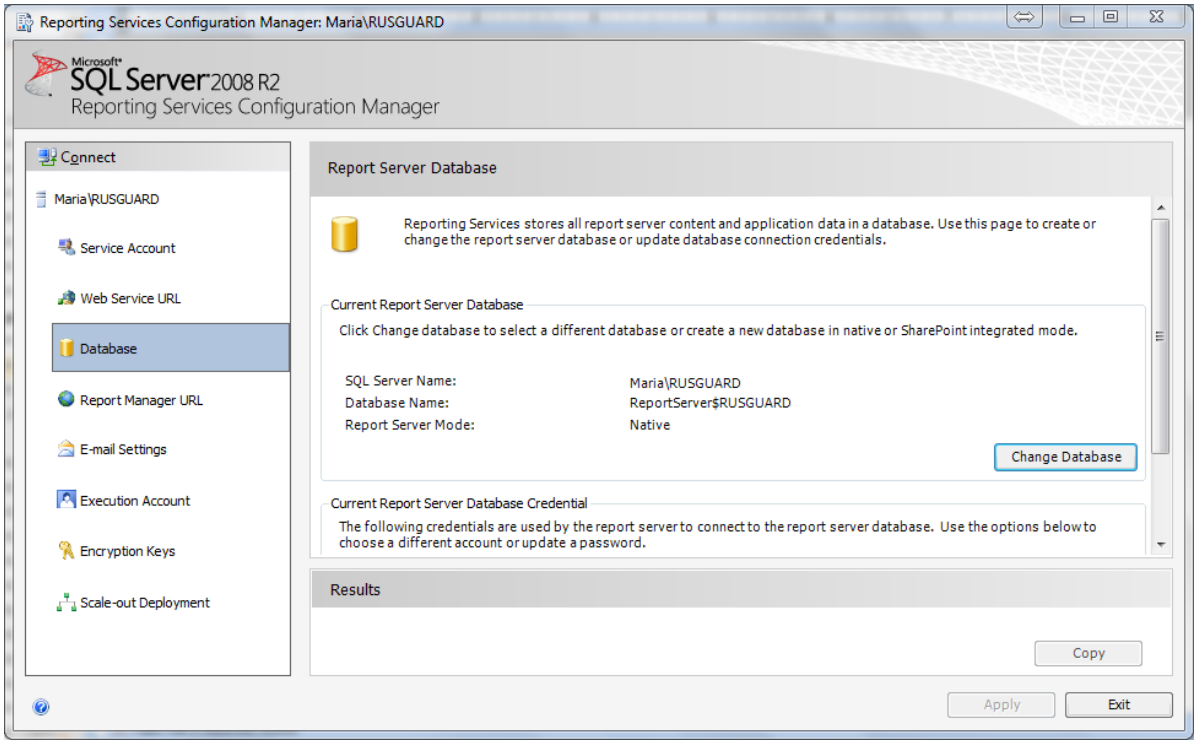


Рисунок 2 - Переход к настройкам БД

4. Нажмите на кнопку Change Database.
5. В открывшемся диалоге выберите второй пункт (существующий сервер БД сервера отчетов) (см. рис. 3). Нажмите на кнопку Next.

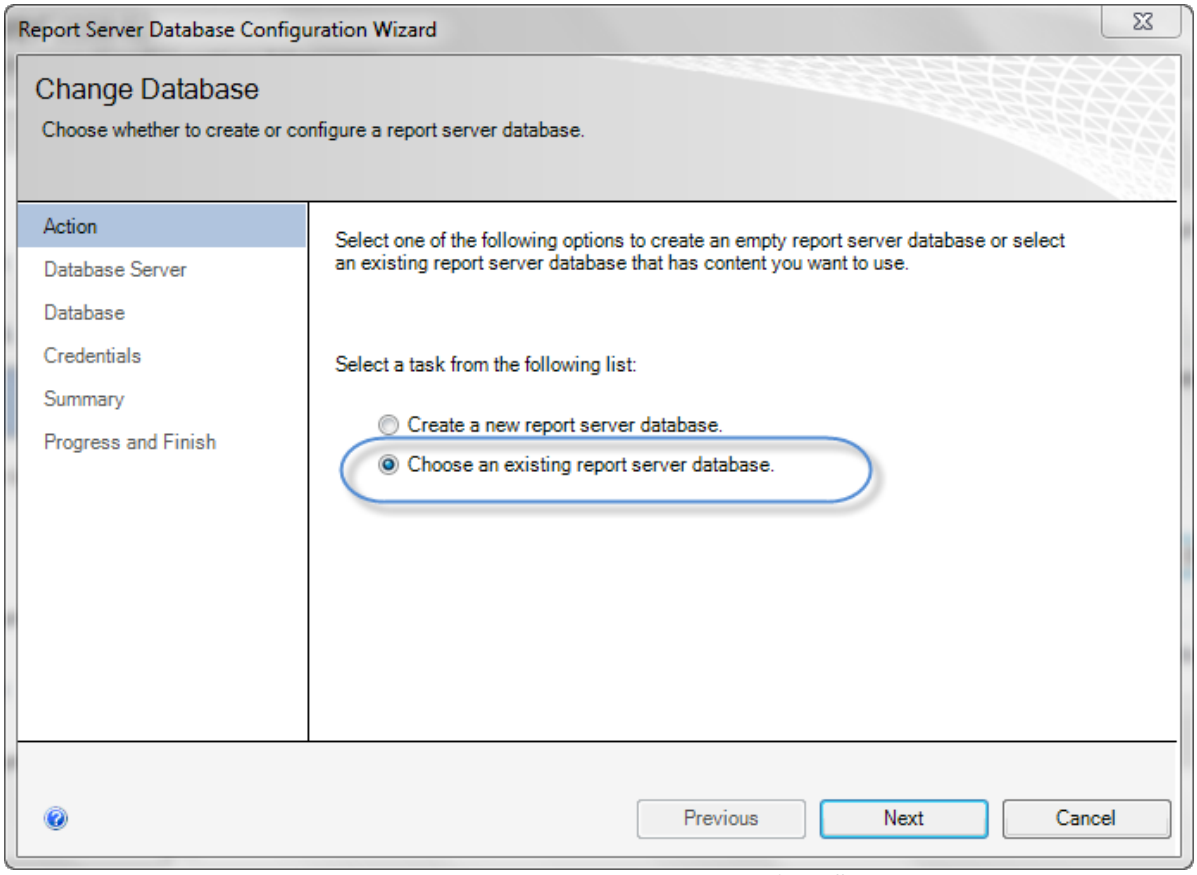


Рисунок 3 - Конфигурация БД сервера отчетов. Выбор действия

6. В следующем окне внесите необходимые изменения: введите новое имя компьютера (заданное латинским шрифтом) (см. рис. 4). Нажмите на кнопку Test Connection, чтобы проверить устанавливается ли соединение.

Чтобы перейти к следующему шагу, нажмите на кнопку Next.

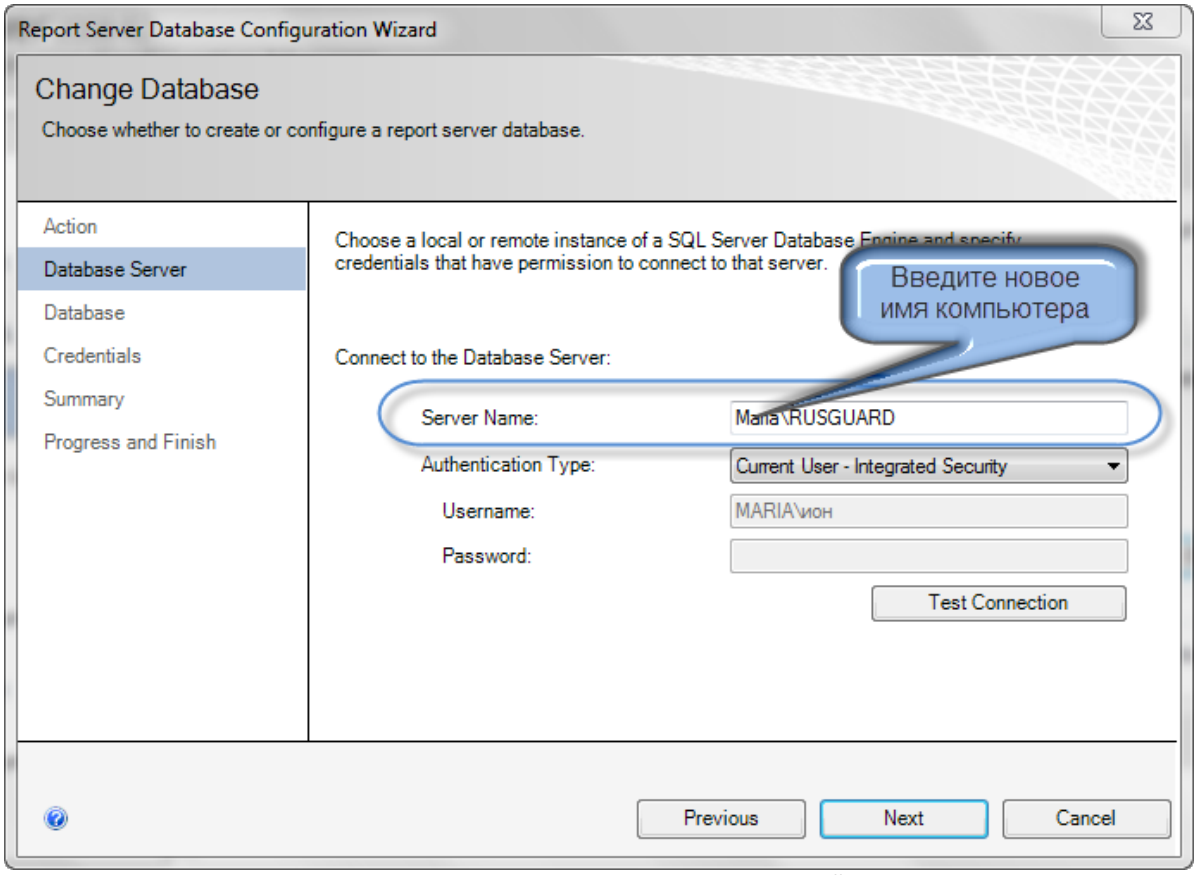


Рисунок 4 - Конфигурация БД сервера отчетов. Внесение изменений в конфигурацию

7. В следующем окне выберите имя базы данных сервера отчетов (см. рис. 5). Чтобы перейти к следующему шагу, нажмите на кнопку Next.

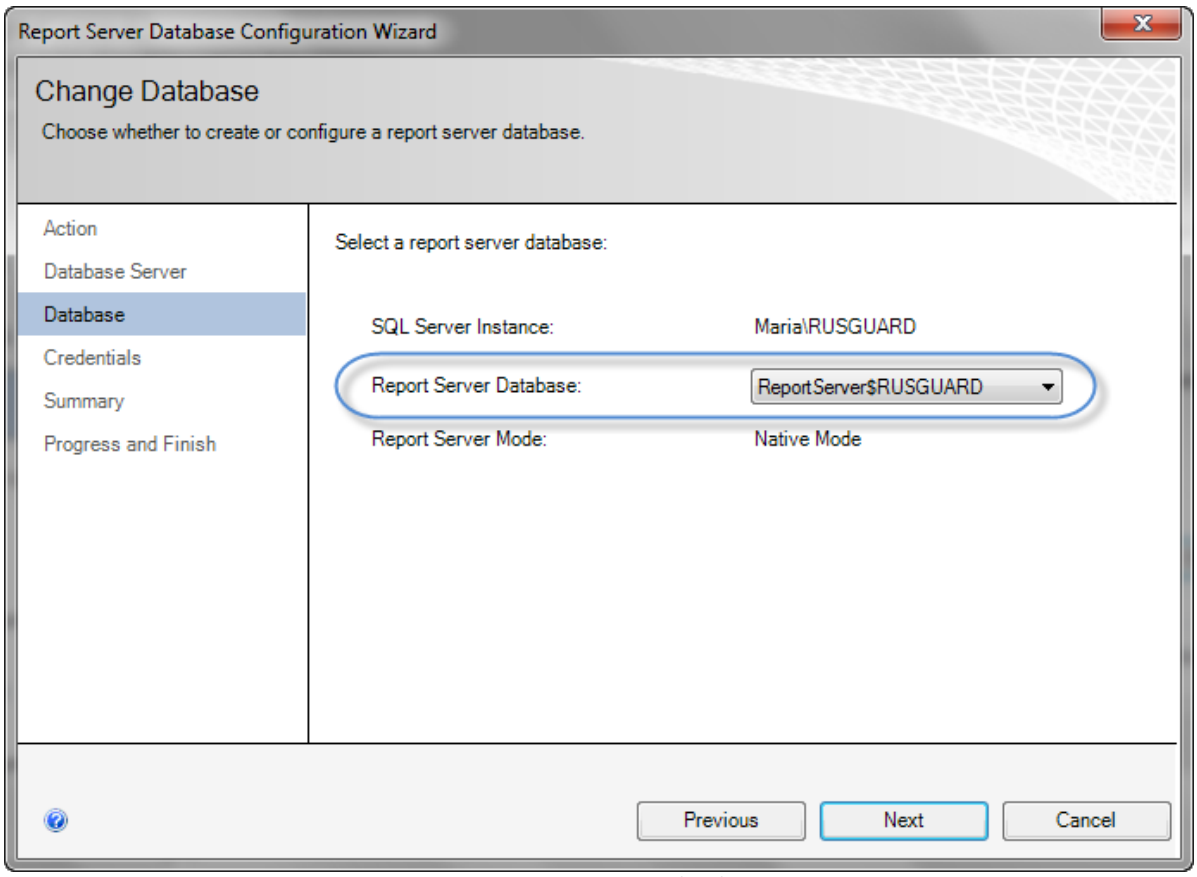


Рисунок 5 - Конфигурация БД сервера отчетов. Выбор базы данных сервера отчетов

8. Завершите процедуру, нажимая на кнопку Next в оставшихся окнах. Настройки в остальных окнах следует оставить без изменений, используя значения по умолчанию.

В последнем шаге система сообщит об успешном выполнении конфигурации БД сервера отчетов.

9. Нажмите на кнопку Finish, чтобы завершить процедуру.

Теперь вы можете перейти к установке ПО RusGuard Soft.

Сервер недоступен

Локализация ошибки. Компоненты

APM RusGuard (распределенный вариант установки), все версии ПО

Описание причин и исправление

При попытке запуска APM 76 сервер может быть недоступен (см. рис. 6).

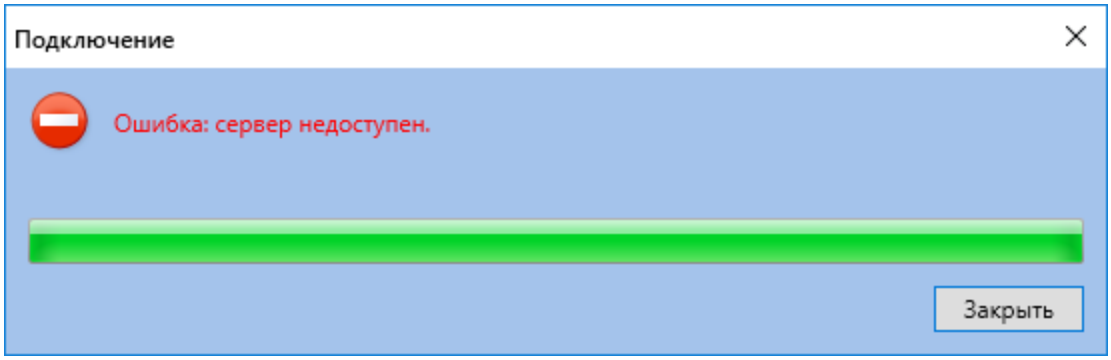


Рисунок 6 - Ошибка при невозможности доступа к серверу

Возможные причины:

1. Сервер выключен. Необходимо запустить сервер.
2. Нет доступа к Интернету. Необходимо проверить соединение.
3. На сервере включен брандмауэр, запущены антивирусы с функциями брандмауэра.

Необходимо выполнить одно из следующих действий:

i. Настроить доступ к серверу по протоколам HTTPS и HTTP;

ii. Отключить брандмауэр/антивирусное ПО/функции брандмауэра антивирусного ПО.

Не удается запустить ПО

Локализация ошибки. Компоненты

АРМ (распределенный вариант установки) и сервер RusGuard. Все версии ПО.

Описание причин и устранение ошибки

Если время и дата настроены некорректно, возможно возникновение ошибки при запуске ПО (см. рис. 7). Для исправления ошибки необходимо привести локальные настройки времени и даты в соответствие с сервером. Допустимое расхождение: +/- 5 минут.

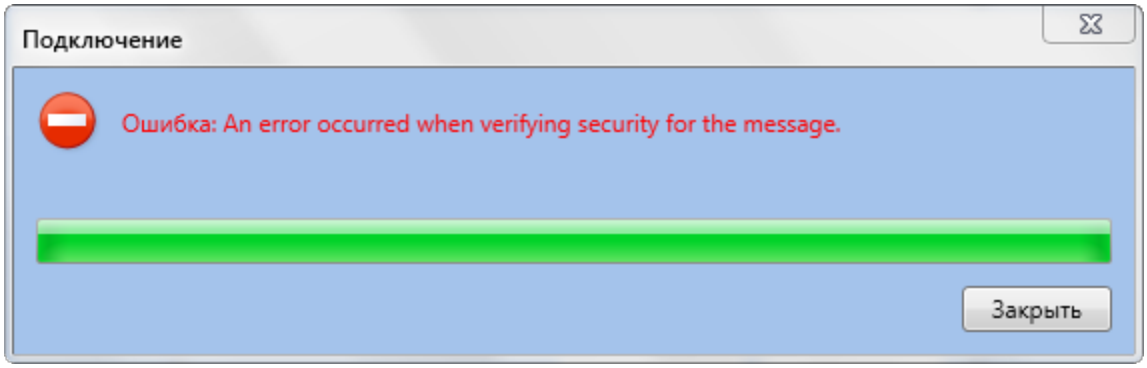


Рисунок 7 - Ошибка при запуске ПО. Некорректно выставлено время и дата на локальном ПК

Пример

Корректная настройка

В таблице ниже приведены примеры корректной настройки времени/даты (см. табл. 1).

Таблица 1 - Пример правильной настройки времени/даты	
Сервер	АРМ
Время 16.50 (часовой пояс +4)	Время 16.50 (часовой пояс +4)
Время 16.50 (часовой пояс +4)	Время 15.50 (часовой пояс +3)
Время 16.50 (часовой пояс +4)	Время 17.50 (часовой пояс +5)

Некорректная настройка

В таблице ниже (см. табл. 2) приведены примеры некорректной настройки времени/даты:

- одинаковое время при разных часовых поясах;
- разное время в одном часовом поясе.

Таблица 2 - Пример неправильной настройки времени/даты	
Сервер	АРМ
Время 16.50 (часовой пояс +4)	Время 16.40 (часовой пояс +4)
Время 16.50 (часовой пояс +4)	Время 16.50 (часовой пояс +3)
Время 16.50 (часовой пояс +4)	Время 16.50 (часовой пояс +5)

Не удается загрузить модуль Отчеты

Локализация ошибки. Компоненты

SQL-сервер, сервер отчетов. Все версии ПО.

Описание причин и устранение ошибки

Если не удается загрузить модуль ***Отчеты*** 214 (см. рис. 8).

Возможные причины:

- Нет доступа к серверу отчетов по протоколу HTTP. На сервере отчетов включен брадмауэр (фаервол), либо включено антивирусное ПО с функциями фаервола. Необходимо отключить указанное ПО или настроить его;
- Некорректная настройка/отсутствие настройки учетной записи на локальном ПК и на сервере отчетов. Для корректной работы модуля необходимо настроить учетную запись Windows с именем пользователя и паролем как локально, так и на сервере отчетов.

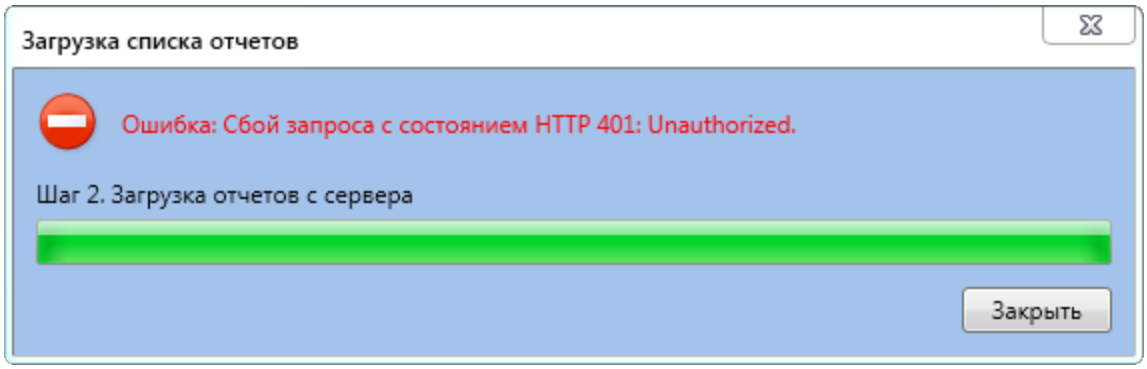


Рисунок 8 - Ошибка при попытке загрузки модуля Отчеты. Некорректно настроены/не настроены учетные записи пользователя

См. также раздел Установка SQL-сервера и настройка сервера отчетов 48

Не удается зайти на сервер отчетов

Локализация ошибки. Компоненты

Все компоненты и версии ПО.

Описание причин и устранение ошибки

Если вы не можете зайти на сервер отчетов через браузер и получаете сообщение об ошибке в связи с отсутствием прав доступа, необходимо добавить адрес сервера отчетов в местную интрасеть.

Для того чтобы добавить адрес сервера отчетов в местную интрасеть:

1. Зайдите в ***Свойства браузера***.
2. Перейдите на вкладку ***Безопасность*** (см. рис. 9).

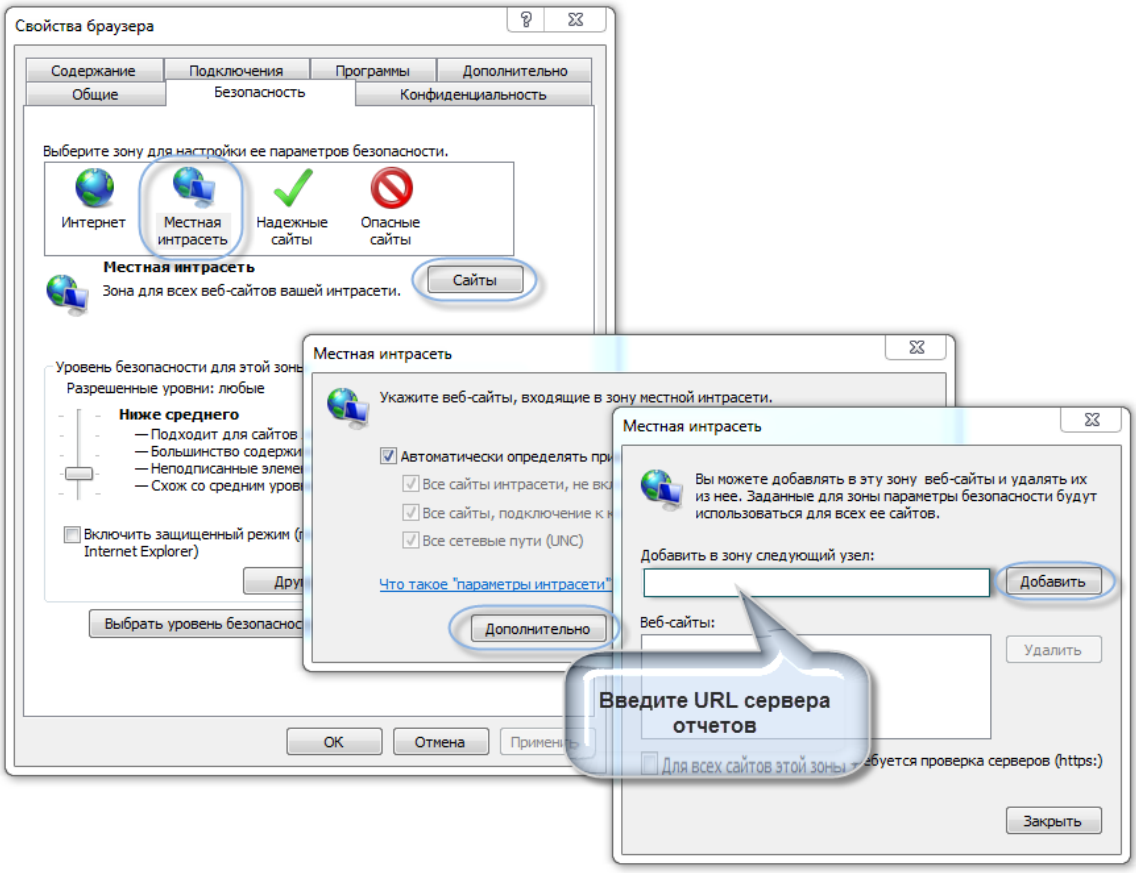


Рисунок 9 - Как добавить адрес сервера Отчетов в местную интрасеть.

3. Выберите пункт ***Местная интрасеть***.
4. Нажмите на кнопку ***Сайты***.

Откроется окно ***Местная интрасеть***.

5. Нажмите на кнопку ***Дополнительно***.

Откроется окно ***Местная интрасеть*** (2).

6. Введите адрес сервера отчетов в поле ввода ***Добавить в зону следующий узел***.

7. Нажмите на кнопку ***Добавить***.
8. Нажмите на кнопку ***Закрыть*** в этом окне и кнопку ***ОК*** следующем.
9. Закройте окно свойств браузера.

Некорректное отображение отработанного времени

Локализация ошибки. Компоненты

APM RusGuard. Все версии ПО.

Описание причин и устранение ошибки

Если в отчете вместо отработаного времени не отображаются значения (отображаются знаки вопросов), значит не созданы рабочие графики 181 и/или рабочие зоны 190.

Ошибка репозитория типов драйверов

Локализация ошибки. Компоненты

Ошибка возникает в АРМ (на сервере или удаленно) на любых ОС, актуальна для версий ПО от 1.8.

Описание и устранение

Ошибка возникает после установки ПО при запуске АРМ (см. рис. 10).

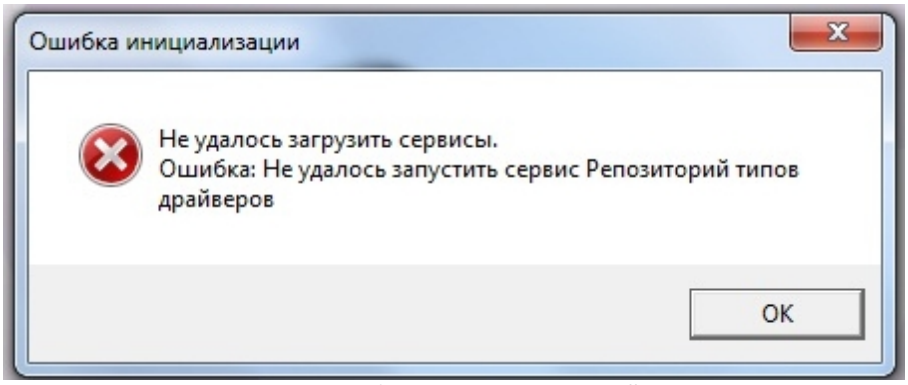


Рисунок 10 - Ошибка репозитория типов драйверов

Для того чтобы устранить ошибку:

1. Выполните обновление ОС. После установки обновлений необходимо перезагрузить ПК и повторно запустить поиск обновлений (актуально и для сервера, и для удаленного АРМ).
2. Выполните подключение компонента сервера Возможности рабочего стола 42 (актуально только для АРМ на самом сервере под управление ОС Windows Server 2008 R2, Windows Server 2012).

Если ошибка связана с частичной несовместимостью ПО с "N"-версиями Windows 10, необходимо скачать вручную и установить Media Feature Pack.

Ошибка серверных служб

Локализация ошибки. Компоненты

Ошибка возможна в серверной части на любых ОС для версий от 1.8.

Описание и устранение

После установки сервера RusGuard не запускаются службы базы данных, сервера отчетов, управления событиями, управления лицензиями. Работа служб останавливается после принудительного запуска.

Для устранения ошибки необходимо устранить ошибку репозитория типов драйверов 298.

Ошибки при восстановлении резервной копии

1. Если восстановление резервной копии невозможно по причине отказа в доступе к файлу .bak, переместите файл в папку, где в настоящее время сохранено ПО RusGuard (по умолчанию C:\Program Files (x86)\VVI Investment).
2. После восстановления резервной копии, созданной на другом ПК, может возникнуть ошибка при запуске АРМ. Необходимо повторно установить соединение с БД через утилиту RusGuard Agent. Перезапустить все службы.

Служебные программы и утилиты

Утилита RusGuard агент

Для мониторинга работоспособности ПО RusGuard Soft используется утилита RusGuard агент. Утилита устанавливается автоматически вместе с сервером RusGuard. RusGuard агент обеспечивает:

- контроль работоспособности серверных процессов (служб), соединений с сервером БД и сервером отчетов;
- оперативное оповещение пользователя о смене состояния контролируемых процессов;
- возможность изменения настроек соединения с сервером БД и сервером отчетов;
- проверку работоспособности соединения с сервером БД и сервером отчетов;
- возможность изменения настроек соединения с сервером БД и сервером отчетов;
- возможность настройки ручной или автоматической (по заданному расписанию) чистки БД (удаление событий до определенной даты).
- отображение информации о лицензиях и состоянии соответствующего ПО.
- регистрацию сервера в сервисе RusGuard Cloud.

После установки серверной части программного комплекса RusGuard Soft, утилита запускается из меню ***Пуск*** ОС Windows и в дальнейшем всегда доступна в области уведомлений (системном трее) (см. рис. 1).

RusGuard агент не будет отображаться в системном трее в случае смены текущего пользователя Windows на ПК.

Запустить RusGuard агент можно вручную: ***Пуск > Все программы > папка RusGuard > RusGuard агент***. Для автоматического запуска поместите ярлык RusGuard агент в меню ***Автозагрузка***.

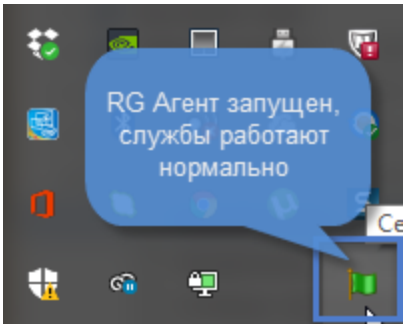


Рисунок 1 -
Утилита RusGuard агент
в системном трее

Пиктограмма в системном трее может менять цвет в зависимости от текущего состояния (настроек) системы (подсистем) (см. табл. 1).

Таблица 1 - Цветовые обозначения утилиты RusGuard агент. Общий случай (системный трей)	
Цвет пиктограммы	Значение
	Система (подсистемы) работает нормально
	Система (одна или несколько подсистем) отключены пользователем (не запущены), но работоспособны (т.е. настройки корректны и связанные с ними компоненты функционируют нормально)
	Состояние системы (одной или нескольких подсистем) неизвестно, или подсистема не установлена
	Ошибка в работе системы (одной или нескольких подсистем)

Цвет пиктограммы в системном трее меняется на желтый, серый или красный при изменении состоянии хотя бы одной из подсистем. Вызвав RusGuard агент, пользователь может определить, где именно произошла смена состояния, ошибка или отключение.

Интерфейс утилиты RusGuard агент состоит из набора вкладок, на каждой из которых отображается информация о состоянии основных подсистем программного комплекса и их отдельных компонентов. Для отображения состояния подсистем и компонентов используется та же цветовая схема, что и для оповещения пользователя в системном трее.

Также в каждой вкладке предусмотрен набор инструментов для базовой отладки компонентов.

Вкладка Сервисы

На этой вкладке (см. рис. 2) отображается состояние серверных процессов и служб (см. табл. 2 и 3).

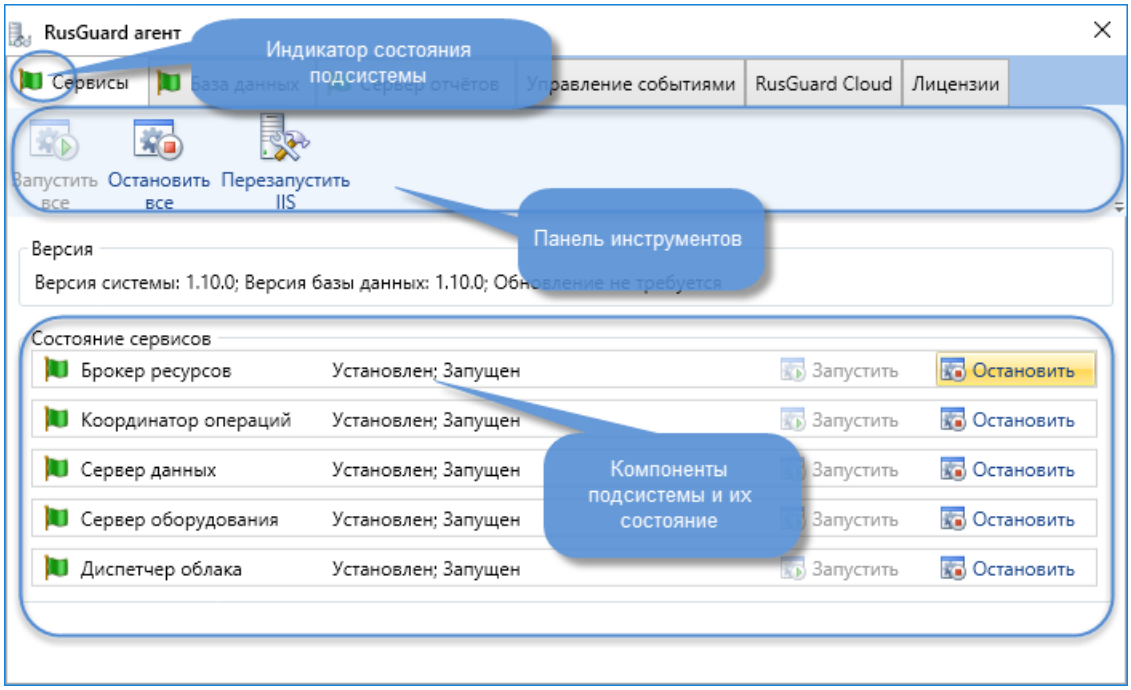


Рисунок 2 - Утилита RusGuard агент. Вкладка Сервисы

Таблица 2 - Цветовые обозначения утилиты RusGuard агент. Вкладка Сервисы	
Цвет пиктограммы	Значение
	Все сервисы работают нормально
	Один или несколько сервисов не запущены
	Сервис не установлен либо недоступен
	Ошибка при запуске одного или нескольких сервисов

Таблица 3 - Управление работой сервисов	
Кнопка	Значение
	Запуск всех сервисов
	Остановка всех сервисов

Таблица 3 - Управление работой сервисов	
	Перезапуск IIS. Может потребоваться после редактирования параметров доступ к серверу БД и серверу отчетов (см. ниже), а также при различных сбоях работы АРМ
	Остановка того сервиса, напротив названия которого расположена кнопка
	Запуск того сервиса, напротив названия которого расположена кнопка

Вкладка База данных

На этой вкладке отображается состояние БД.

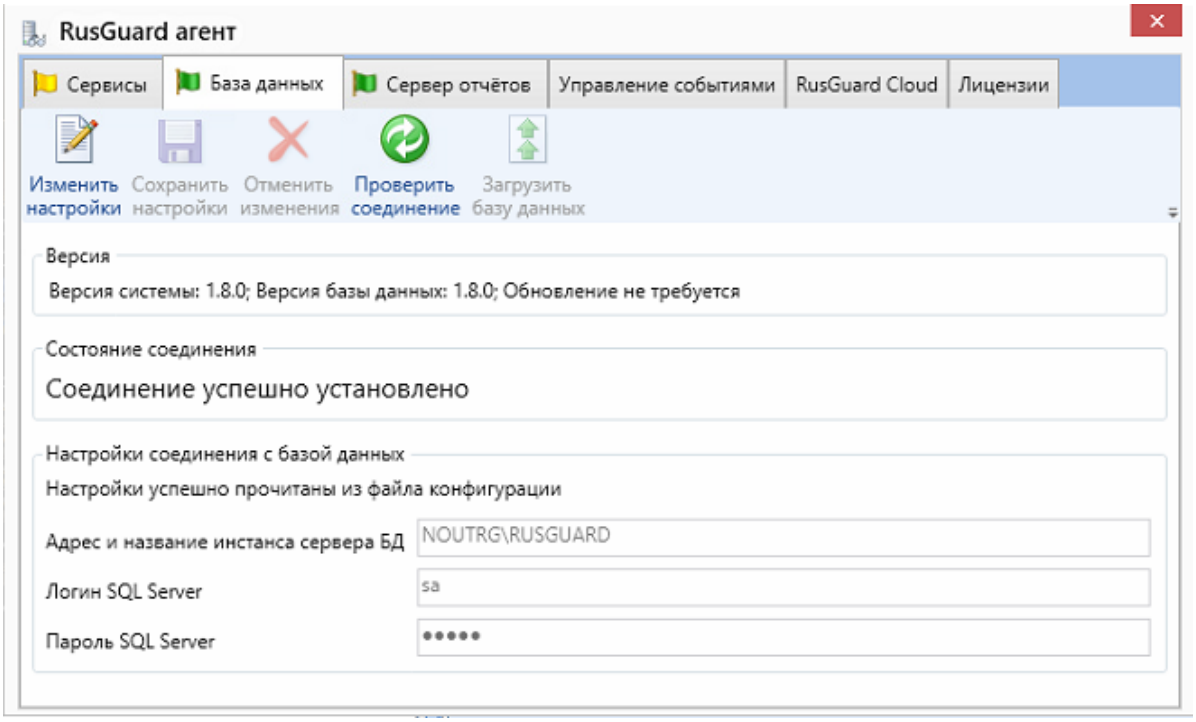


Рисунок 3 - Утилита RusGuard агент. Вкладка База данных

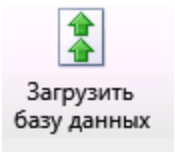
На вкладке ***База данных*** отображается текущее состояние соединения с сервером БД (см. рис. 3), для уведомления пользователя об изменениях состояния используется стандартная цветовая схема утилиты (см. табл. 4).

Таблица 4 - Цветовые обозначения утилиты RusGuard агент. Вкладка База данных	
Цвет пиктограммы	Значение
	Соединение установлено
	Не прочитан файл конфигурации, но соединение работает

Таблица 4 - Цветовые обозначения утилиты RusGuard агент. Вкладка База данных	
	Идет проверка соединения
	Ошибка соединения с БД

Используя панель инструментов на вкладке (см. табл. 5), пользователь может:

- Отредактировать параметры соединения с сервером БД 305
- Проверить соединение с БД
- Загрузить базу данных

Таблица 5 - Базовые настройки соединения с БД. Мониторинг БД	
Кнопка	Значение
	Позволяет активировать поля ввода настроек соединения с сервером БД в нижней части вкладки (область ***Настройки соединения с базой данных***) для их редактирования 305
	Кнопка становится активна после изменения настроек. Позволяет сохранить новые параметры соединения с БД
	Кнопка становится активна после изменения настроек соединения. Позволяет отменить новые параметры соединения с БД и вернуть прежние
	Проверка соединения с БД
	Создание новой базы данных на сервере БД. Используется в тех случаях, когда прежнюю БД потребовалось по той или иной причине удалить. Кнопка активна, когда база данных отсутствует. При этом отображается соответствующее сообщение

Для того чтобы изменить настройки соединения с БД:

1. Нажмите на кнопку  .
2. Введите новые параметры в поля области ***Настройки соединения с базой данных*** (см. табл. 6).

Таблица 6 - Поля формы для настройки соединения с БД	
Поле	Значение и требования к заполнению

Таблица 6 - Поля формы для настройки соединения с БД	

Адрес и название инстанса сервера БД	Адрес сервера БД, формируемый по следующему правилу (см. табл. 7):
	`[Имя компьютера]\[Название экземпляра]`
	Если сервер RusGuard и сервер БД развертываются на одном компьютере, адрес примет вид:
	`.\[Название экземпляра]`
	Значение параметра "Название экземпляра" зависит от типа экземпляра SQL Server ("Экземпляр по умолчанию", "Именованный экземпляр", выбранного при его установке.

Логин SQL сервер	sa (от "super administrator")
Пароль SQL сервер	Пароль, заданный при установке сервера RusGuard (если устанавливался одновременно с SQL-сервером), либо при установке SQL-сервера (если конфигурация подразумевает его самостоятельную установку).

3. Выполните проверку соединения  .
4. Если настройки корректны, нажмите на кнопку  . В противном случае отмените изменения и введите корректные данные.
5. Перезапустите все сервисы. Для этого:
   i. Перейдите на вкладку ***Сервисы***.
   ii. Нажмите на кнопку  и дождитесь остановки всех сервисов.
   iii. Нажмите на кнопку  .
   iv. Нажмите на кнопку  .

Таблица 7 - Вид адреса инстанса сервера БД. В зависимости от типа конфигурации	
Тип конфигурации	Вид адресной строки
Сервер RusGuard сервер БД установлены на одном компьютере	Если установка SQL-сервера выполнялась одновременно с установкой сервера RusGuard 36, экземпляр SQL-сервера получит имя *RUSGUARD*, и адрес будет выглядеть следующим образом: `.\RUSGUARD`
	Если SQL-сервер был установлен ранее в режиме наименования "*Экземпляр по умолчанию*", то адрес сервера БД будет состоять только из точки (.)
	Если SQL-сервер был установлен раньше в режиме наименования "*Именованный экземпляр*" с именем *SQLExpress* (возможно и другое), то адрес сервера БД примет вид: `.\SQLExpress`

Таблица 7 - Вид адреса инстанса сервера БД. В зависимости от типа конфигурации	
Сервер RusGuard сервер БД установлены на разных компьютерах	Если при установке SQL-сервера выбран режим наименования "*Именованный экземпляр*" с именем *SQLExpress* (возможно и другое, например, MyServer), то адрес примет вид: `[hostname]\SQLExpress`

Подсказка

Один из распространенных сбоев базы данных связан с остановкой SQL-сервера. Для устранения сбоя необходимо перезапустить SQL-сервер, используя SQL Server Configuration Manager (см. рис. 4).

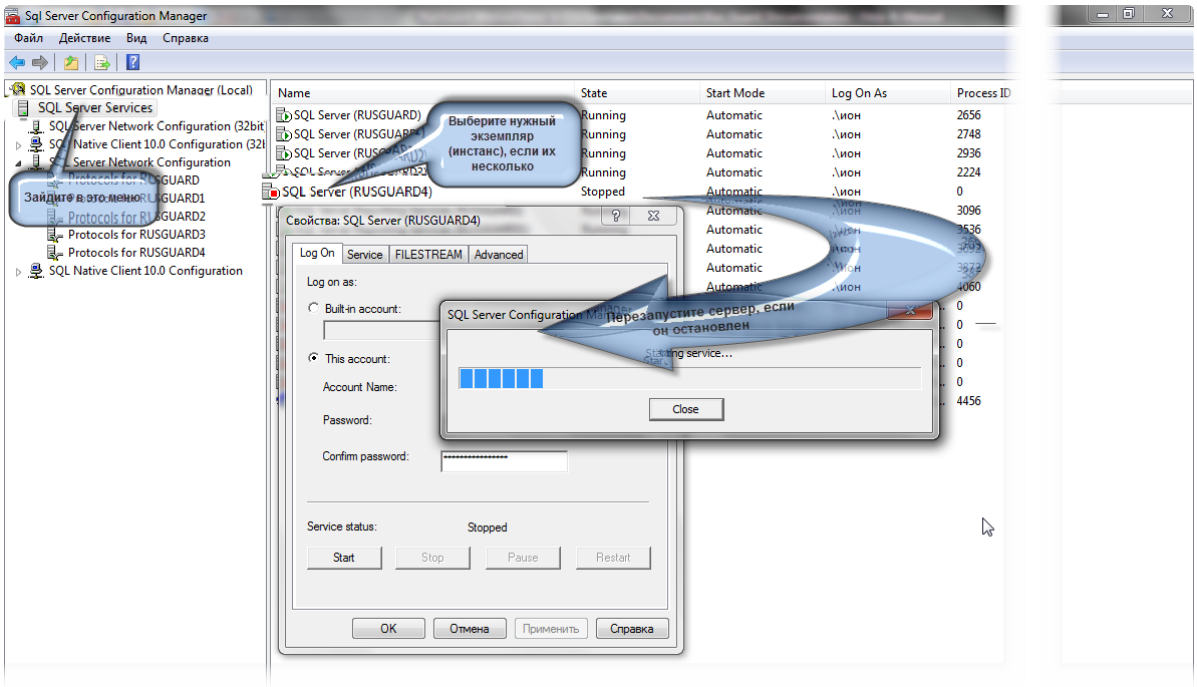


Рисунок 4 - Перезапуск экземпляра SQL-сервера

Вкладка Сервер отчетов

На этой вкладке (см. рис. 5) выполняется настройка соединения с сервером отчетов.

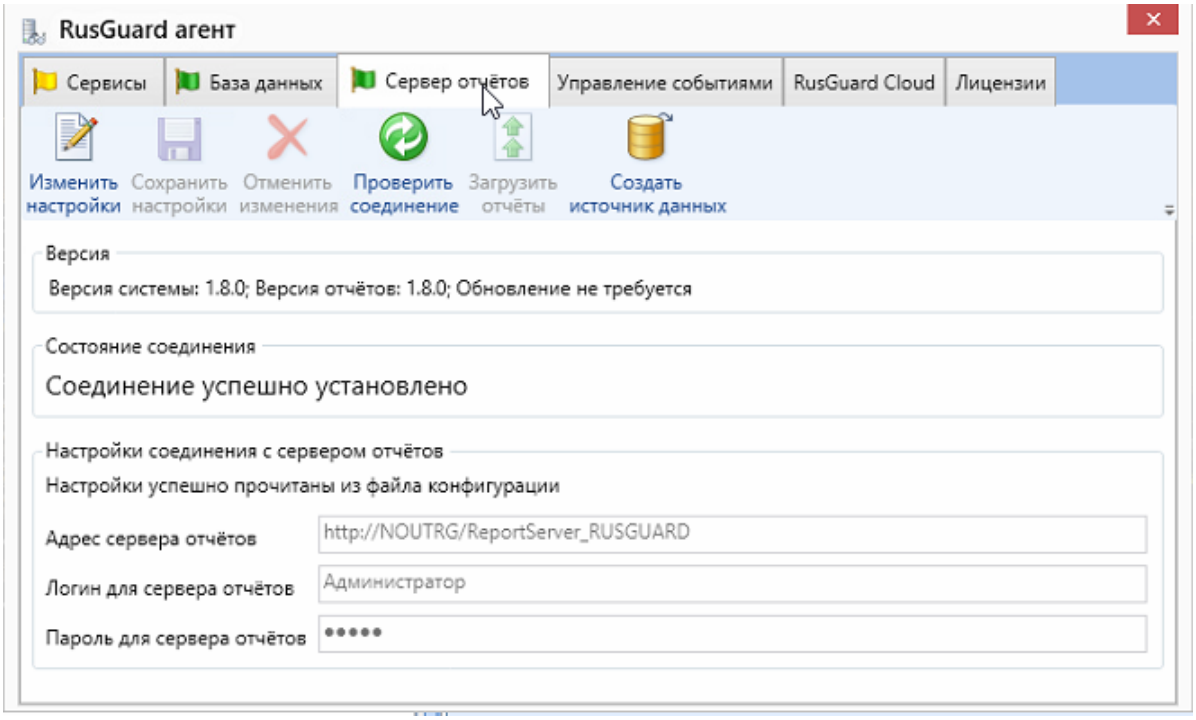


Рисунок 5 - Утилита RusGuard агент. Вкладка Сервер отчетов

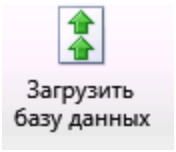
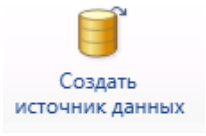
На вкладке отображается текущее состояние соединения с сервером отчетов, для уведомления пользователя об изменениях состояния используется стандартная цветовая схема утилиты (см. табл. 8).

Таблица 8 - Цветовые обозначения утилиты RusGuard агент. Вкладка База данных	
Цвет пиктограммы	Значение
	Соединение установлено
	Не прочитан файл конфигурации, но соединение работает
	Идет проверка соединения
	Ошибка соединения с сервером отчетов

Используя панель инструментов на вкладке (см. табл. 9), пользователь может:

- редактировать параметры соединения с сервером отчетов;
- проверять состояние соединения;
- загружать отчеты на сервер.

Таблица 9 Базовые настройки соединения с сервером отчетов	
Кнопка	Значение

Таблица 9 Базовые настройки соединения с сервером отчетов	
	Позволяет активировать поля ввода настроек соединения с сервером БД в нижней части вкладки (область ***Настройки соединения с сервером отчетов***) для их редактирования
	Кнопка становится активна после изменения настроек. Позволяет сохранить новые параметры соединения с сервером отчетов
	Кнопка становится активна после изменения настроек соединения. Позволяет отменить новые параметры соединения с сервером отчетов и вернуть прежние
	Проверка соединения с сервером отчетов
	Создание чистой базы данных на сервере отчетов
	Создание источника данных на сервере

Для того чтобы изменить настройки соединения с сервером отчетов:

1. Нажмите на кнопку  .
2. Введите новые параметры в поля области ***Настройки соединения с сервером отчетов***. Используйте учетные данные, введенные при установке сервера RusGuard (или SQL-сервера, если он был установлен отдельно) (см. табл. 10).

Таблица 10 - Формат ввода адреса сервера отчетов	
Поле	Формат заполнения
Сервер отчетов	`http://Имя сервера отчетов/ReportServer_Имя инстанса_SQ` **Примеры**: `http://ServerSQL /ReportServer_SqlExpress` – подключение серверу отчетов (ServerSQL) с именем инстанса SqlExpress `http://ServerSQL/ReportServer` – подключение к серверу отчетов (ServerSQL) с пустым именем инстанса

Таблица 10 - Формат ввода адреса сервера отчетов	
	Предупреждение: Недопустимо использование в строке подключения адресов типа `127.0.0.1` и `localhost`.

3. Выполните проверку соединения  .
4. Если настройки корректны, нажмите на кнопку  . В противном случае отмените изменения и введите корректные данные.
5. Перезапустите все сервисы. Для этого:
   I. Перейдите на вкладку ***Сервисы***.
   II. Нажмите на кнопку  и дождитесь остановки всех сервисов.
   III. Нажмите на кнопку  .
   IV. Нажмите на кнопку  .

Вкладка Управление событиями

На вкладке ***Управление событиями*** (см. рис. 6) пользователь может:

- Вручную удалить события до выбранной даты (включительно);
- Настроить автоматическое удаление событий.

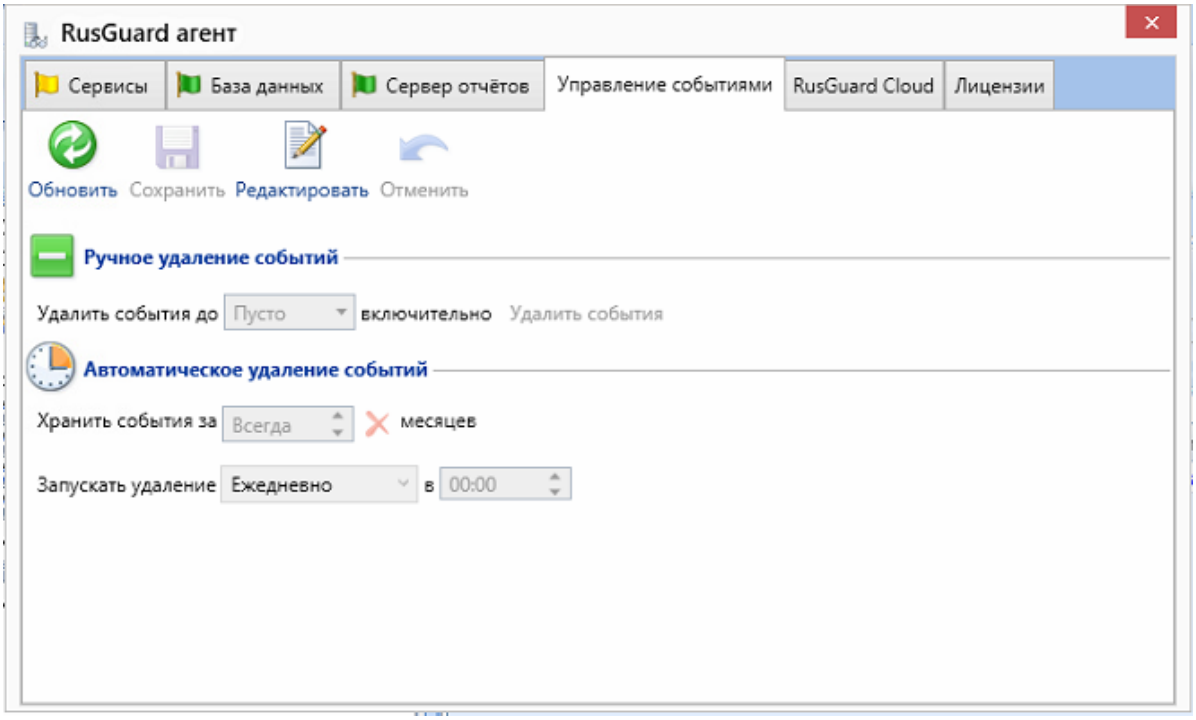


Рисунок 6 - Утилита RusGuard агент. Вкладка Управление событиями

Для того чтобы удалить события вручную:

1. Нажмите на кнопку  .

Активируются все поля ввода дат на вкладке.

2. В поле ***Удалить события до дд.мм.гггг включительно*** области ***Ручное удаление событий*** введите дату.

Дата вводится при помощи календаря, который всплывает при щелчке мышью внутри поля.

После ввода даты активируется кнопка ***Удалить события***.

3. Нажмите на кнопку ***Удалить события***.

Система начинает процесс удаления. Ход процесса отображается во всплывающем окне.

Для того чтобы настроить автоматическое удаление:

1. Нажмите на кнопку  .

Активируются все поля ввода на вкладке.

2. Введите период хранения событий в поле ***Хранить события за _x_ месяцев*** области ***Автоматическое удаление событий***.
3. В поле ***Запускать удаление _чч:мм_ в*** выберите частоту и время очистки базы данных событий (см. рис. 7).

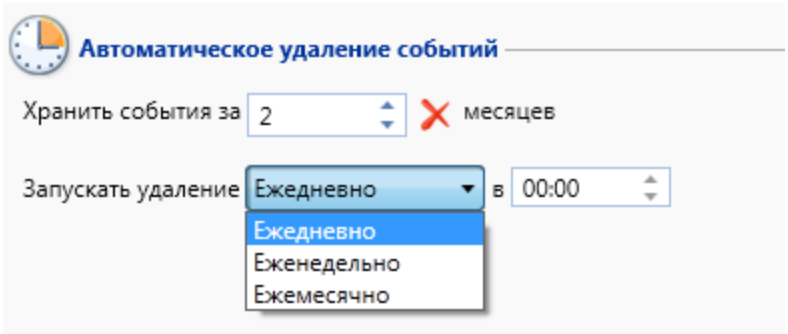


Рисунок 7 - Утилита RusGuard агент. Вкладка Управление событиями. Настройка автоматического удаления

После ввода даты активируется кнопка  . Также активируется кнопка  , которая позволяет сбросить введенные данные.

4. Нажмите на кнопку  .

Система применит настройки.

Вкладка Лицензии

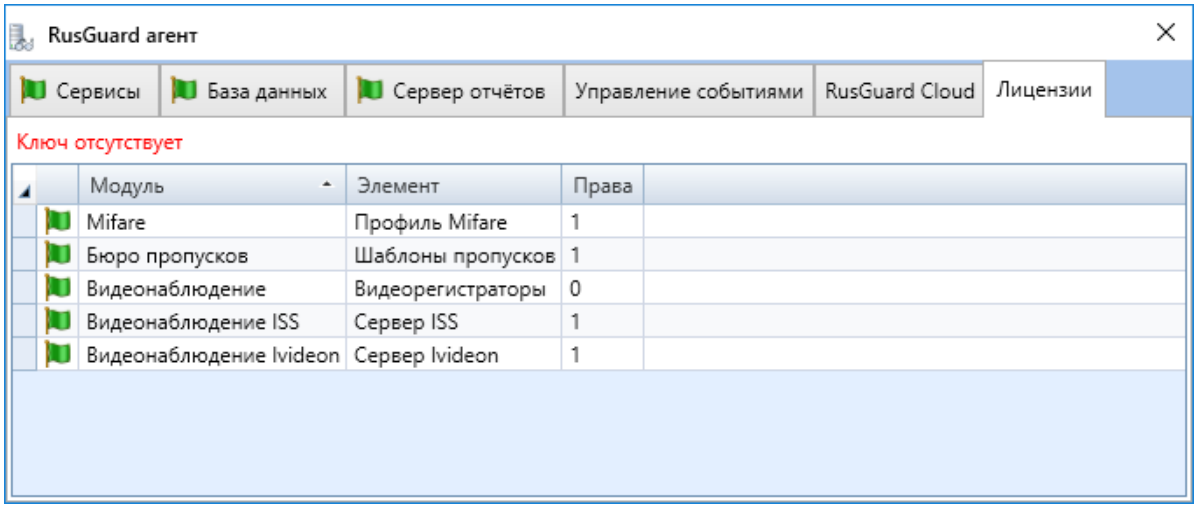


Рисунок 8 - Утилита RusGuard агент. Вкладка Лицензии

На вкладке ***Лицензии*** (см. рис. 8) отображается список подключенных лицензий и состояние связанного с ними ПО (например, драйверов).

Управление данными системы RusGuard

Утилита ***Управление данными системы RusGuard*** предназначена для выполнения следующих операций:

- Резервное копирование и восстановление 348;
- Обновление версии данных 286 (т.е. приведение данных на сервере в соответствие с новой версией ПО RusGuard, если это необходимо);
- Редактирование набора полей карточки сотрудника;
- Настройка набора фотографий в карточке сотрудника;
- Проверка соединений с БД и сервером отчетов.

Утилита запускается через меню ***Пуск*** ОС Windows **>** папка ***RusGuard***.

Обратите внимание, что функции редактирования полей карточки сотрудника и управления фотографиями также реализованы и доступны в модуле Конфигурация системы. Для единообразия работы рекомендуется использовать эти функции там.

Редактирование набора полей карточки сотрудника

Для того чтобы отредактировать набор полей карточки сотрудника:

1. Запустите утилиту ***Управление данными системы RusGuard***.
2. Перейдите на вкладку ***Редактор полей данных сотрудника***.
3. Нажмите на кнопку  , затем на кнопку  .

В нижней части экрана появится строка для ввода параметров поля (см. рис. 9).

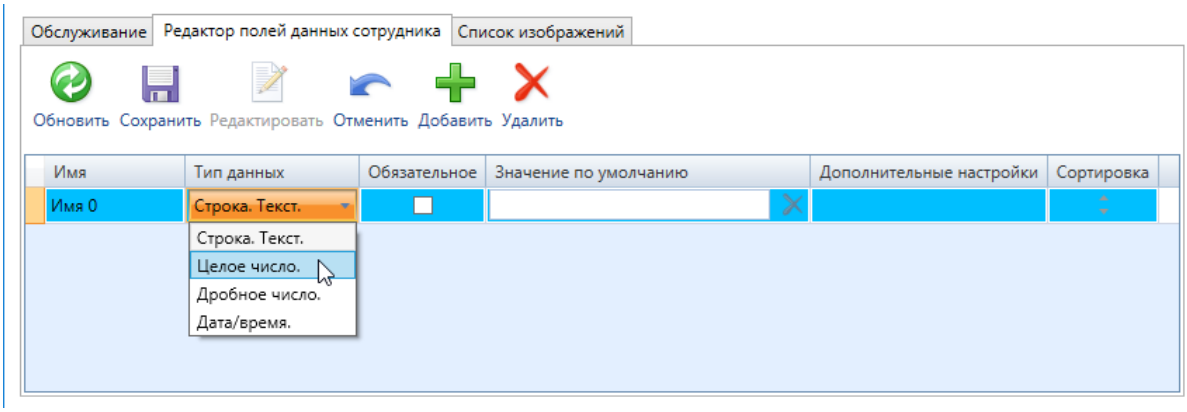


Рисунок 9 - Редактирование полей данных сотрудника

4. Введите параметры поля:
   - Имя;
   - Тип данных (выберите из списка);
   - Установите флаг ***Обязательное***, если создаваемое поле должно заполняться обязательно;
   - Введите значение по умолчанию, если требуется.

Пункт ***Дополнительные параметры*** доступен, если выбран тип данных ***Дата/время***. В нем вводится формат отображения информации. Если создано несколько дополнительных полей, активируется возможность их сортировки.

5. Нажмите на кнопку  .

Система обновит параметры карточки сотрудника.

Примечание: вы можете отменить последнее действие (), пока не было выполнено следующее в этой же вкладке, или не была закрыта утилита.

Настройка набора фотографий

Для того чтобы отредактировать набор фотографий:

1. Запустите утилиту ***Управление данными системы RusGuard***.
2. Перейдите на вкладку ***Редактор изображений***. По умолчанию предусмотрена возможность загрузки трех фотографий в карточку (см. рис. 10).

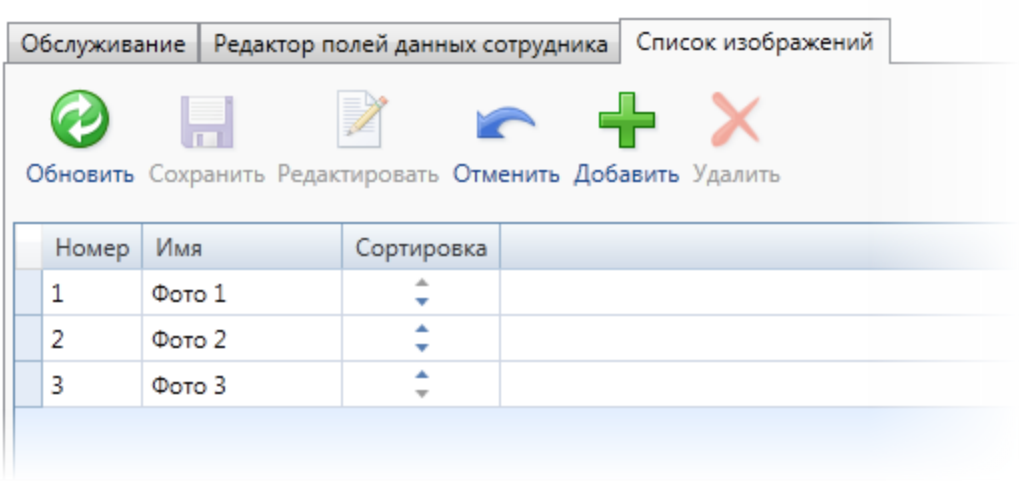


Рисунок 10 - Редактор изображений. Вид по умолчанию (три фото)

3. Нажмите на кнопку  (список фотографий станет активным), затем на кнопку  .

В нижней части экрана появится пустая строка.

4. В поле ***Имя*** введите имя фото, нажмите на кнопку  . Воспользуйтесь функцией сортировки порядка отображения фотографий, если это необходимо.

Для того чтобы уменьшить количество фотографий:

1. Запустите утилиту ***Управление данными системы RusGuard***.
2. Перейдите на вкладку ***Редактор изображений***. По умолчанию предусмотрена возможность загрузки трех фотографий в карточку.
3. Нажмите на кнопку  (список фотографий станет активным).
4. Выделите мышью строку с названием фотографии, которую требуется удалить.

5. Нажмите на кнопку  .
Выделенная строка будет удалена.

6. Нажмите на кнопку  .

Примечание: вы можете отменить последнее действие (), пока не было выполнено следующее в этой же вкладке, или не была закрыта утилита.

Проверка соединений

Функция проверки соединений утилиты дублирует аналогичную функцию утилиты RusGuard Агент 301.

Сетевые настройки контроллеров

Утилита (см. рис. 11) позволяет менять сетевые настройки контроллеров и не требует обязательной установки остальных компонентов ПО RusGuard Soft (сервера, АРМ). Утилита может потребоваться при установке и пуско-наладке оборудования.

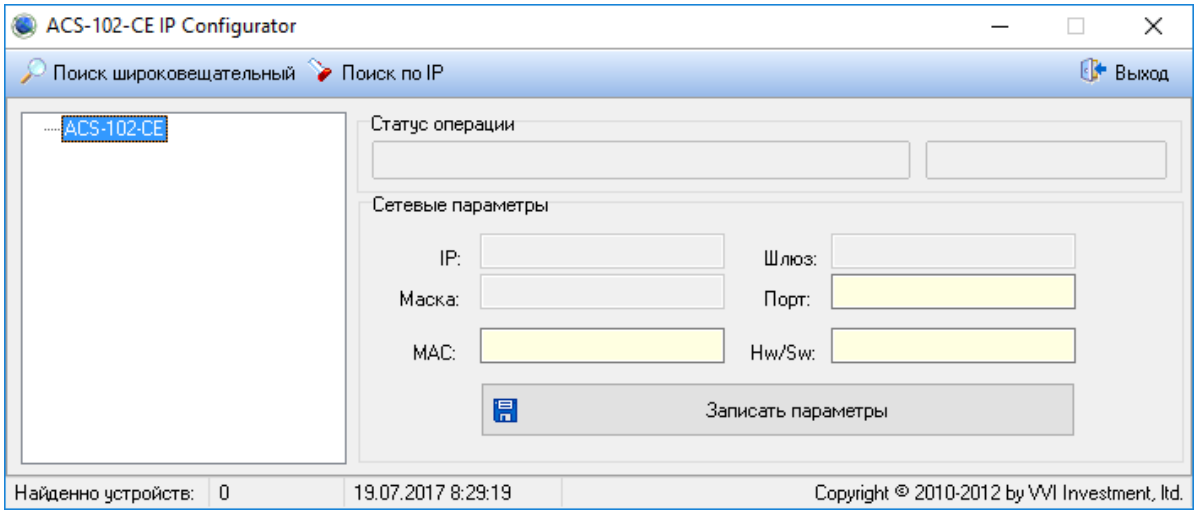


Рисунок 11 - Сетевые настройки контроллеров. Вид окна по умолчанию

Для того чтобы изменить настройки контроллера:

1. Выполните поиск нужного контроллера.

В утилите предусмотрено два варианта поиска:

- Широковещательный поиск автоматически находит все контроллеры, подключенные к системе внутри локальной сети.
- Поиск по IP позволяет находить по IP-адресу те контроллеры, которые находятся за пределами локальной сети, отделены шлюзами и т.д. (см. рис. 12).

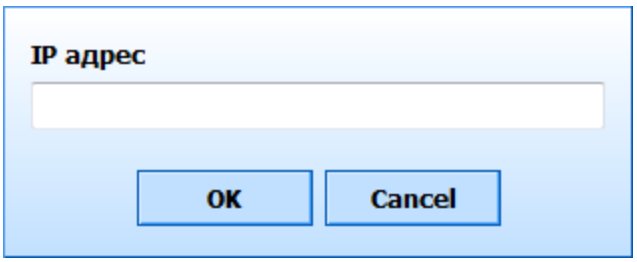


Рисунок 12 -
Сетевые настройки контроллеров.
Поиск по IP-адресу

После завершения поиска в левой навигационной панели отображается найденный контроллер (список контроллеров).

2. Если найдено несколько устройств (широковещательный поиск), перейдите к нужному устройству в списке.

В главном экране утилиты отобразятся сетевые параметры выбранного контроллера (см. рис. 13).

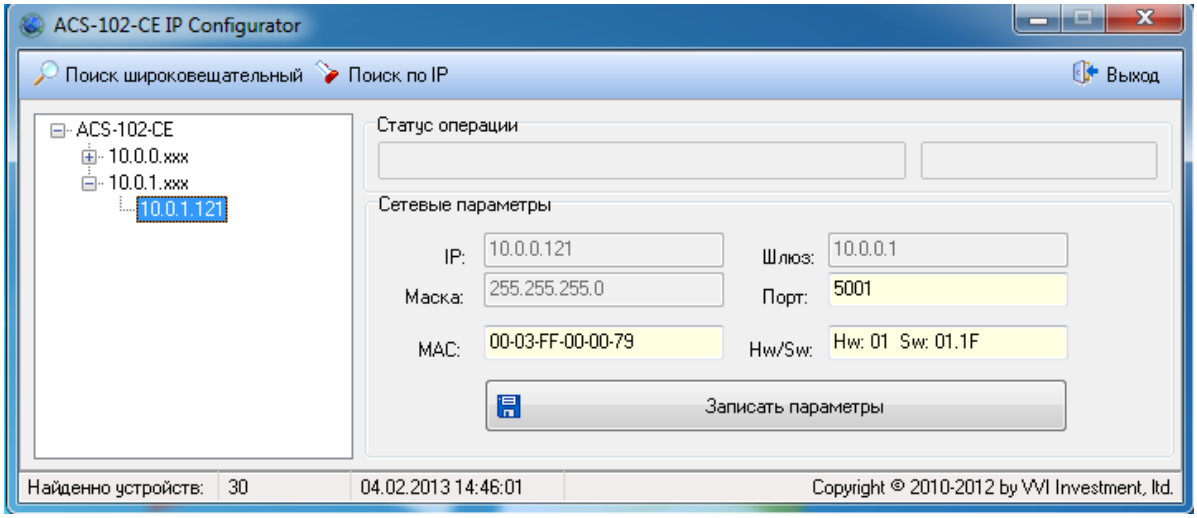
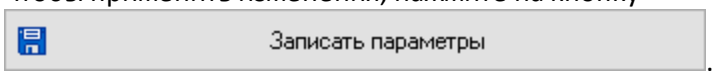


Рисунок 13 - Сетевые настройки контроллеров. Отображаются параметры контроллера

Предупреждение: MAC-адрес и порт устройства недоступны для редактирования.

Примечание: Последние 6 цифр MAC-адреса контроллера - это его SID (уникальный идентификатор контроллера, который программируется при выпуске изделия и изменить его нельзя).

3. Измените нужные параметры.
4. Чтобы применить изменения, нажмите на кнопку



.

Расширенные сетевые настройки контроллеров

Новая утилита "Расширенные сетевые настройки контроллеров" позволяет не только редактировать сетевые настройки контроллеров на этапе пусконаладки СКУД (без установки остальных компонентов ПО), но и настраивать дополнительные IP-адреса для доступа к контроллеру (до 4 штук).

Внимание! Если задан пароль доступа к настройкам, он не может быть изменен в других компонентах ПО RusGuard. В случае утери пароля, восстановление его НЕВОЗМОЖНО! Необходимо сбросить настройки устройства на заводские.

Настройка дополнительных IP-адресов

Для того чтобы настроить дополнительные IP-адреса:

1. Выполните поиск устройств в сети или по IP (воспользуйтесь одной из соответствующих кнопок в левой части экрана утилиты). По умолчанию при запуске утилиты список пуст (см. рис. 14).

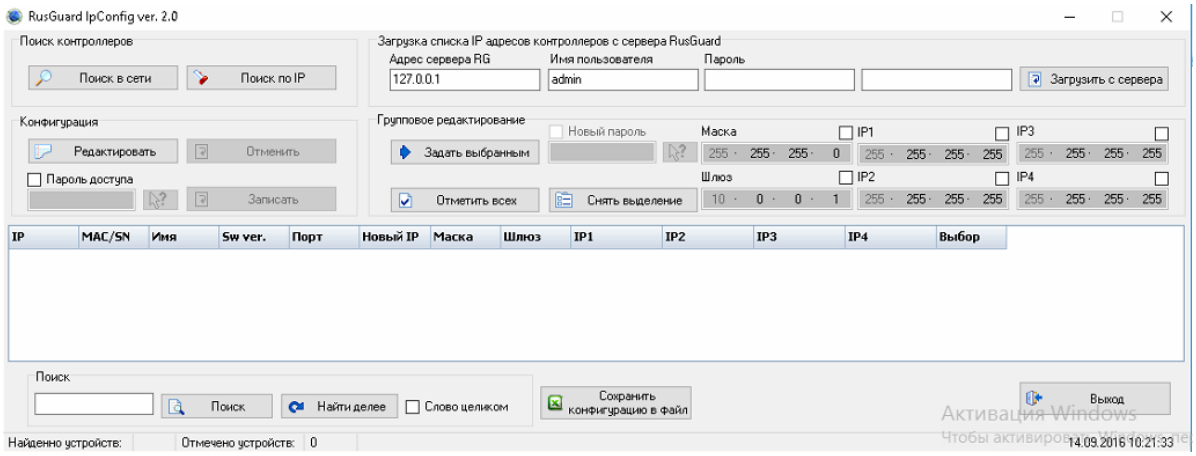


Рисунок 14 - Утилита "Сетевые настройки контроллеров"

2. Выберите нужное устройство в списке найденных, установив флаг в столбце ***Выбор***. Вы также можете выполнить групповую настройку, отметив все контроллеры в списке найденных (***Отметить всех***). Кроме того, вы можете редактировать параметры непосредственно в ячейках списка.
3. Нажмите на кнопку ***Редактировать***.
4. Если это необходимо, введите пароль в поле ввода ***Пароль доступа*** и нажмите на кнопку ***Записать*** (см. также ниже).

Обратите внимание, что, если данные защищены паролем, текущие настройки отображаются только после ввода пароля и щелчка мышью в нужной строке списка (см. рис. 15). Если пароль введен неверно, вы не сможете ни просмотреть, ни отредактировать параметры устройств. Обратите также, что для разных устройств в системе могут быть заданы разные пароли.

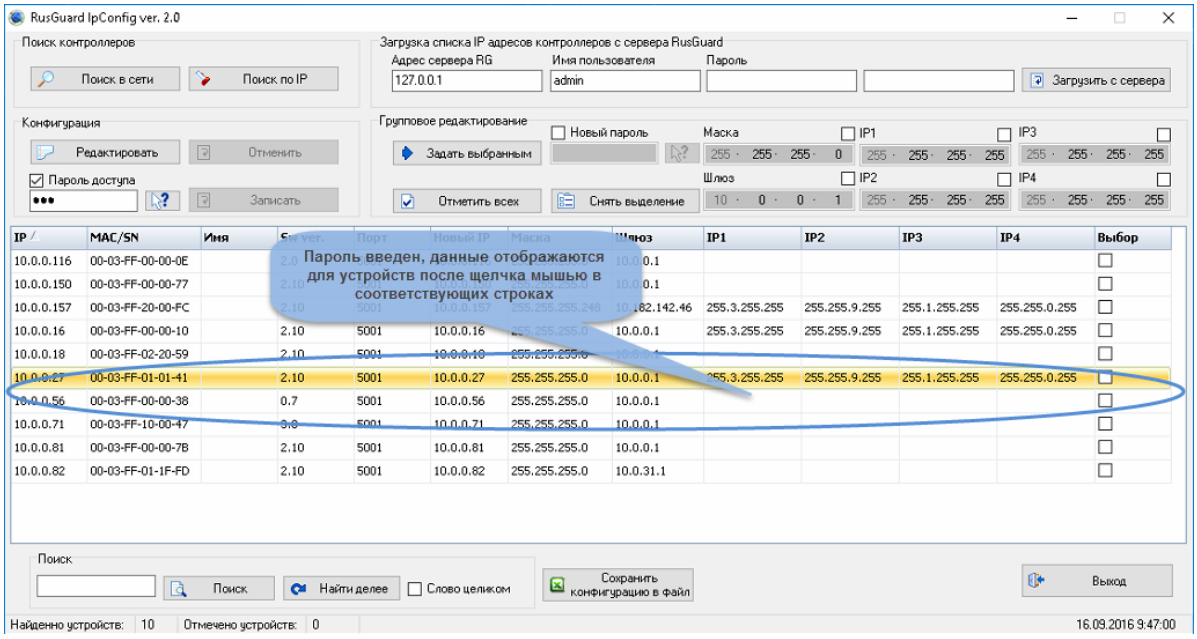


Рисунок 15 - Утилита "Сетевые настройки контроллеров". Отображение данных после ввода пароля и активации строк в списке

5. Введите дополнительные IP-адреса для выбранных контроллеров одним из указанных способов: либо непосредственно в ячейках списка, либо используя поля IP1-IP4 в верхней части формы. Если параметры должны применяться к нескольким устройствам, нажмите на кнопку ***Задать выбранным*** (предварительно установите флаги возле нужных устройств в списке, как указано выше).
6. Изменения применяются автоматически.

Обратите внимание, что после каждого действия (смены настроек) поля для редактирования становятся неактивными. Чтобы внести дополнительные изменения, необходимо снова нажать на кнопку ***Редактировать*** и ввести пароль.

Использование пароля

Вы можете задать пароль доступа к параметрам контроллеров.

В этом случае, после ввода дополнительных IP-адресов просмотреть и снова отредактировать их можно будет только после ввода пароля (см. рис. 16). Если вы не хотите использовать пароль, снимите флаг возле поля ***Пароль доступа***.

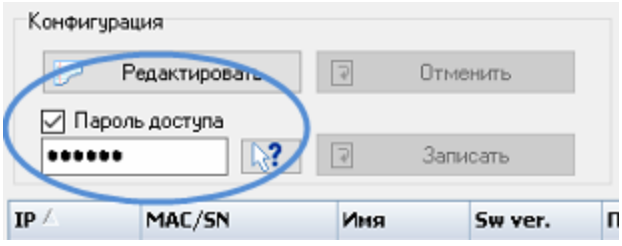


Рисунок 16 - Утилита "Сетевые настройки контроллеров". Ввод пароля

Обратите внимание, что смена пароля выполняется только в данной утилите, а процедура его восстановления не предусмотрена. В случае утери пароля, необходимо сбросить настройки контроллера на заводские.

Чтобы отобразить символы пароля в явном виде, щелкните на пиктограмму  .

Для создания/смены пароля воспользуйтесь полем ввода ***Новый пароль***. Вы можете сменить пароль к одному или нескольким устройствам.

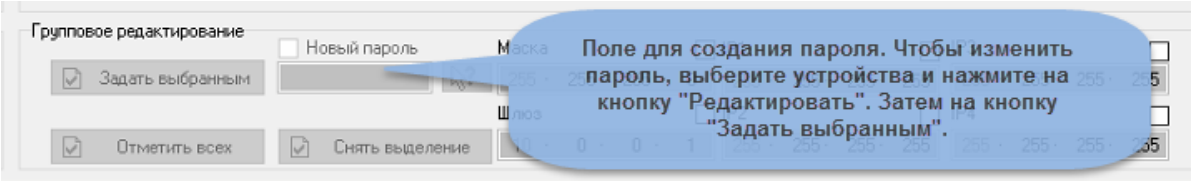


Рисунок 17 - Утилита "Сетевые настройки контроллеров". Создание нового пароля

Утилита также позволяет выгружать настройки в локальный файл формата `.xls`. Поддерживается текстовый поиск (окно в нижней части экрана).

Работая с утилитой, вы можете использовать контекстное меню (правая кнопка мыши).

Сервисный конфигуратор оборудования

Сервисный конфигуратор оборудования (см. рис. 17) предназначен для специалистов, выполняющих установку и пуско-наладку системного оборудования для первичного конфигурирования до установки и настройки Сервера RusGuard, сервера БД и др. программных компонентов.

В отличие от АРМ, Конфигуратор работает в режиме "офлайн".

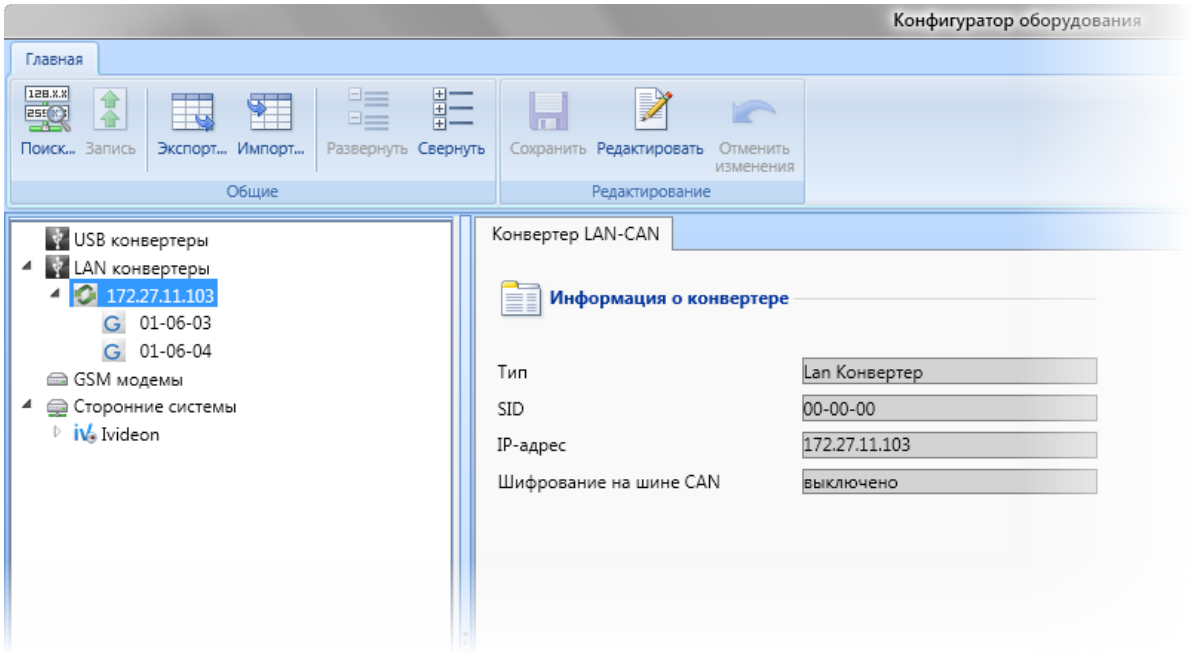


Рисунок 18 - Утилита Сервисный конфигуратор устройств

Утилита позволяет:

- находить подключенные контроллеры;
- редактировать CAN-адреса контроллеров;
- настраивать режимы работы и настройки;
- выполнять первичный мониторинг работоспособности системы (получение событий от контроллера, подача команд управления и т.д.).

Все настройки контроллеров, заданные через Сервисный конфигуратор, в дальнейшем считываются ПО и сохраняются в БД при первичной загрузке данных контроллеров на сервер RusGuard.

Выполнение поиска

ПО RusGuard поддерживает два типа подключения устройств:

- CAN-USB
- CAN-LAN

Соответственно, предусмотрено два режима поиска для каждого типа подключений.

Также, для CAN-LAN устройств, помимо широковещательного поиска, предусмотрена функция поиска по IP-адресу, она позволяет находить устройства, находящиеся за пределами локальной сети (отделенные шлюзами, и т.д.).

Для того чтобы выполнить поиск CAN-USB устройства:

1. Загрузите модуль Конфигурация оборудования.
2. Нажмите на кнопку  в верхней панели управления.

Откроется окно ***Поиск устройств*** (при первом запуске окно пустое) (см. рис. 18).

Примечание: При повторном запуске поиска система предложит сначала очистить окно.

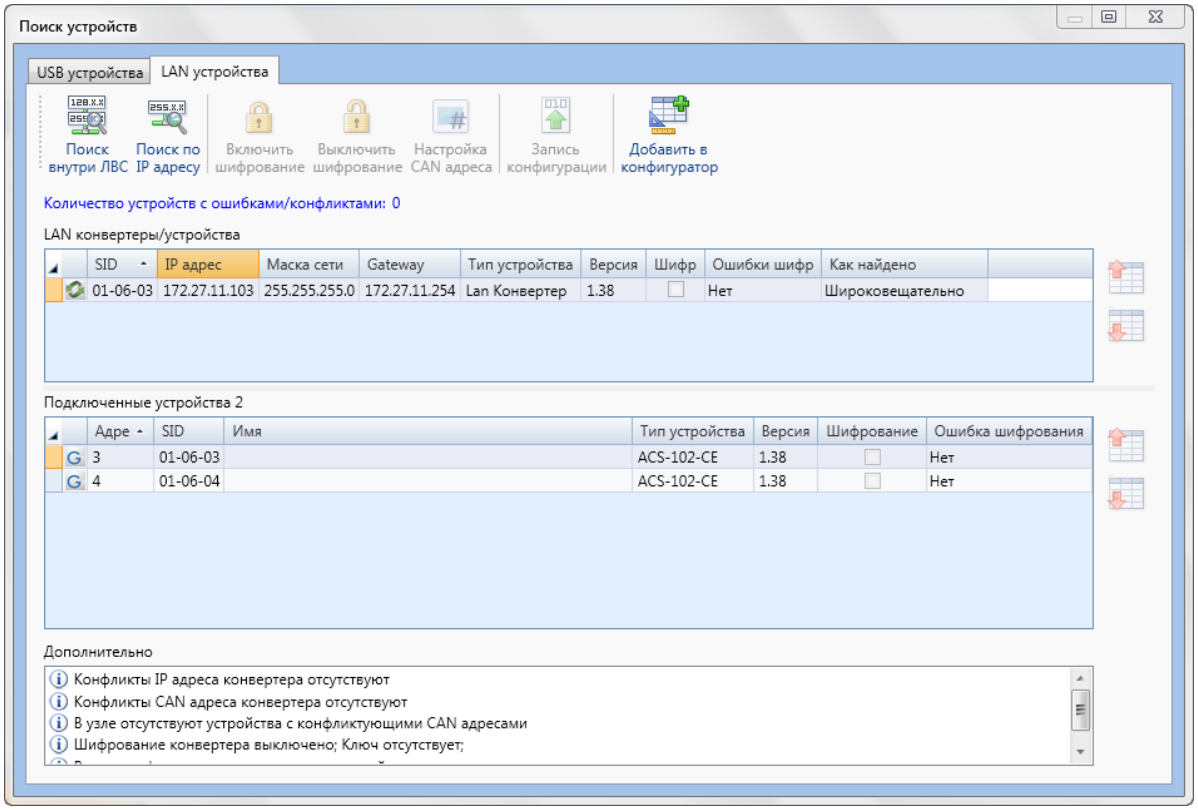


Рисунок 19 - Утилита Сервисный конфигуратор оборудования. Окно поиска

3. Оставаясь в текущей вкладке ***USB устройства***, нажмите на кнопку  в панели управления.

Загрузится список серверов оборудования.

4. Выберите тот сервер, на котором требуется выполнить поиск. Нажмите на кнопку Ок.

Примечание: Поиск может быть выполнен с любого сервера, находящегося в системе, обслуживаемой ПО RusGuard.

Система выполнит поиск и отобразит его результаты (см. рис. 19).

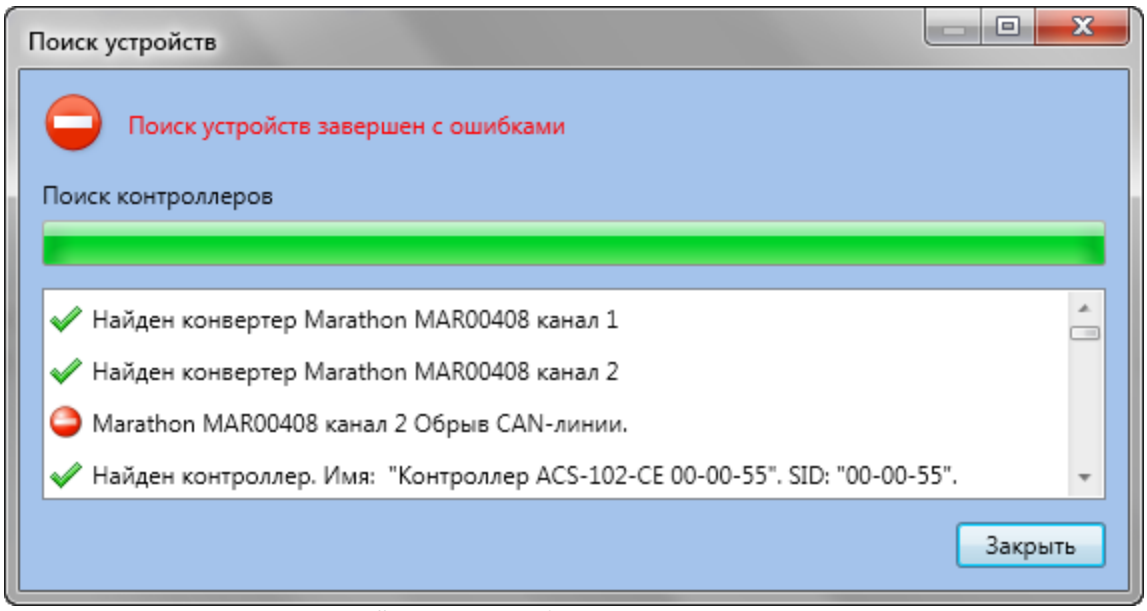


Рисунок 20 - Утилита Сервисный конфигуратор оборудования. Результаты широковещательного поиска

5. Нажмите на кнопку 

.

Данные о найденных устройства загрузятся в основное окно поиска. Сначала в верхней части окна (список ***USB-конвертеры***) отобразится список найденных USB-конвертеров и краткая информация о них, включая статус подключения.

6. Щелкните мышью по нужному устройству, чтобы загрузить ниже список подключенных к нему контроллеров.

В списке ***Подключенные устройства*** загрузится список контроллеров и краткая информация о каждом из них, включая текущий статус подключения. Ниже, в области ***Дополнительно***, отображается подробная информация по выделенному в списке контроллеру.

Для того чтобы найти CAN-LAN устройства (широковещательный поиск):

1. Загрузите модуль ***Конфигурация оборудования***.
2. Нажмите на кнопку 

в верхней панели управления.
Откроется окно ***Поиск устройств***
3. Перейдите на вкладку ***LAN устройства***.
4. Нажмите на кнопку 

.

Система выполнит поиск, сообщая о процессе в отдельном окне. Затем загрузится список найденных конвертеров. При щелчке мыши в строке с информацией об определенном конвертере ниже загружается список подключенных через него контроллеров (см. рис. 20).

Обратите внимание, что при поиске LAN устройств в списке результатов также указывается способ выполнения поиска.

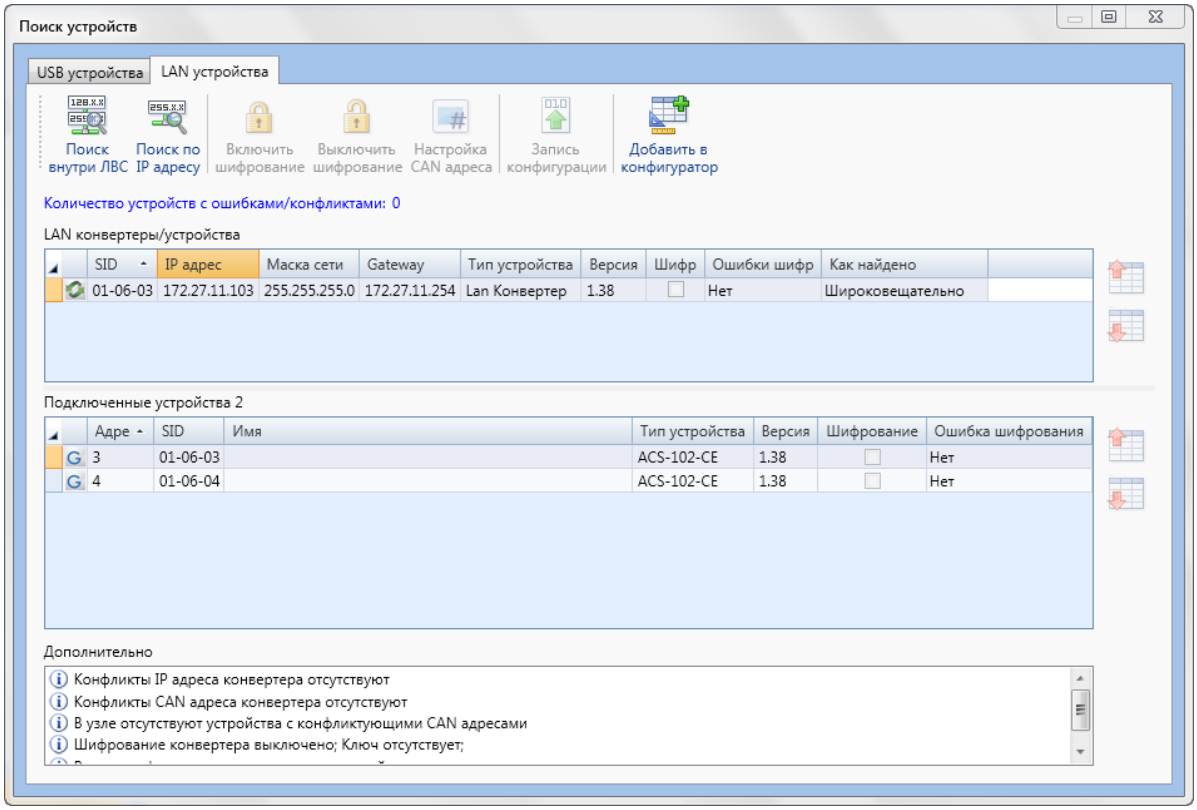


Рисунок 21 - Утилита Сервисный конфигуратор устройств. Функция поиска

Для того чтобы найти устройство по IP-адресу:

1. Загрузите модуль ***Конфигурация оборудования***.
2. Нажмите на кнопку  в верхней панели управления.

Откроется окно ***Поиск устройств***

3. Перейдите на вкладку ***LAN устройства***.
4. Нажмите на кнопку 

.

Откроется окно для ввода IP-адреса (см. рис. 21).

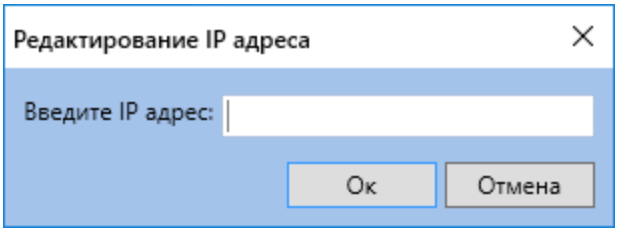


Рисунок 22 - Окно ввода IP-адреса для поиска

5. Введите IP-адрес и нажмите на кнопку 

.

Отобразится окно для выбора сервера.

6. Выберите нужный сервер и нажмите на кнопку Ок.

Система приступит к поиску. В случае успешного результата, данные об устройстве будут выведены в окне результатов.

Редактирование CAN-адреса

CAN-адреса присваиваются устройствам в интервале от 1 до 255. В редких случаях адреса устройств, установленные по умолчанию, совпадают. В таком случае необходимо изменить CAN-адрес одного из них.

Для того чтобы отредактировать CAN-адрес:

1. Выполните поиск USB или LAN устройства. В списке результатов выделите нужный контроллер в списке ***Подключенные устройства*** окна ***Поиск устройств***.
2. Щелкните по строке с данными о контроллере дважды правой кнопкой мыши, либо нажмите на кнопку # в верхней панели экрана.

Откроется окно, со списком доступных номеров CAN (от 1 до 255, минус уже занятые адреса) (см. рис. 22).

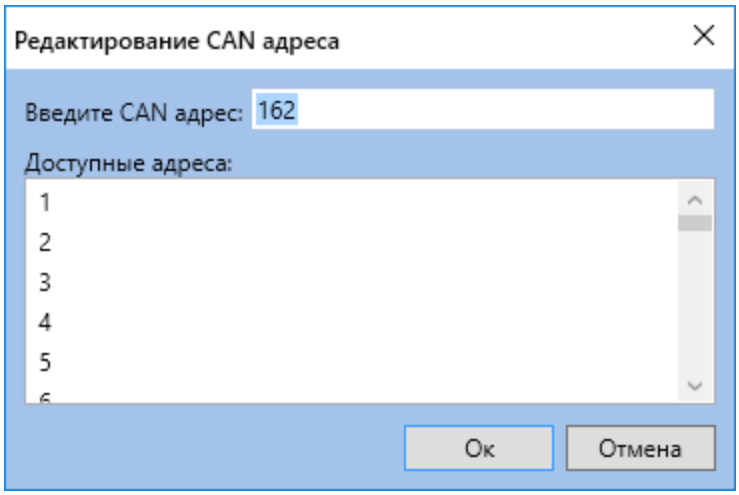


Рисунок 23 - Редактирование CAN-адреса в Сервисном конфигураторе оборудования

3. Выберите нужный номер в списке ***Доступные адреса*** и выделите его в списке.
4. Номер отобразится в поле ***Введите CAN адрес*** вместо текущего.
5. Нажмите на кнопку Ок.

Система применит требуемые изменения.

Синхронизация данных

Данные об устройствах, найденных при помощи поиска, а также об изменениях конфигурации устройств можно занести в конфигуратор для последующей синхронизации с БД.

Для того чтобы занести данные об устройствах в утилиту:

1. Выполните поиск USB или LAN устройства. В списке результатов выделите нужный контроллер в списке ***Подключенные устройства*** окна ***Поиск устройств***.
2. Нажмите на кнопку  ***Добавить в конфигуратор***.

Если устройство найдено впервые, данные о нем автоматически загружаются в утилиту и отображаются в левой навигационной панели в виде списка. Если конфигурация устройства уже заносилась в утилиту ранее, а затем была отредактирована, система потребует подтверждения перезаписи конфигурации (см. рис. 23).

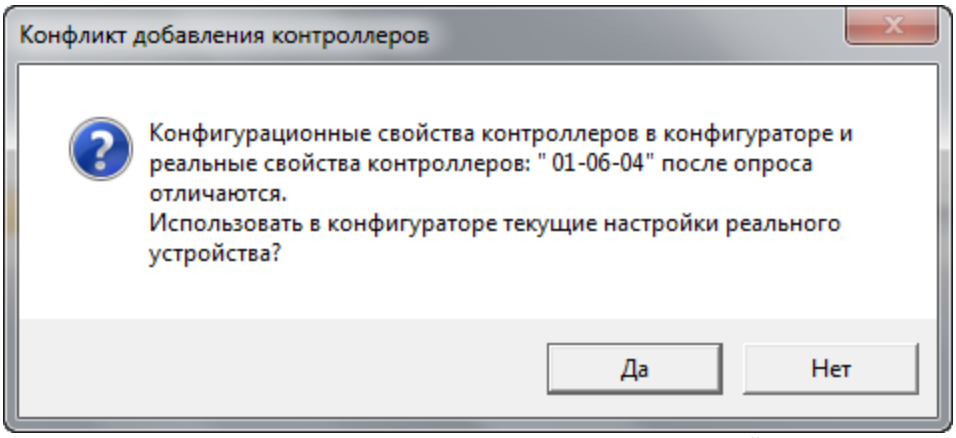


Рисунок 24 - Запрос на подтверждение перезаписи конфигурации устройства в утилите

3. Подтвердите действие.
4. Система выполнит перезапись настроек.

Управление ключами

Утилита ***Сервисный конфигуратор оборудования*** позволяет управлять ключами доступа, прописанными в контроллер. Ключи считываются либо с настольного считывателя, либо со считывателя подключенного к контроллеру. Данная функция используется для проверки работоспособности системы при её монтаже.

Чтобы запретить доступ по заведенным ключам, необходимо выбрать данный контроллер и нажать кнопку ***Синхронизировать*** в модуле Конфигурирования оборудования на сервере.

Чтобы оставить заведенные ключи в работе, необходимо добавить их в БД сервера (модуль Конфигурирование СКУД).

Для того чтобы приступить к управлению ключами:

1. Найдите устройство/а и добавьте его в конфигуратор.
2. Выберите нужное устройство в левой навигационной панели, перейдите на вкладку ***Сервисные функции*** на экране справа. Перейдите на вкладку с названием типа точки доступа (допустим, "Дверь") (см. рис. 24).

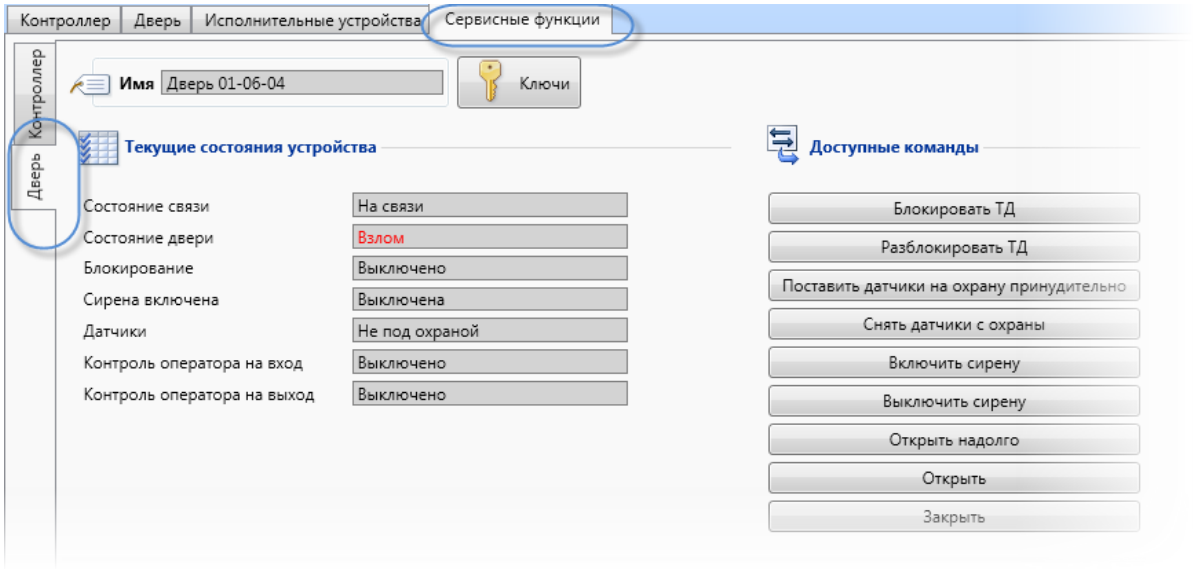


Рисунок 25 - Навигация к функции Управление ключами

3. Нажмите на кнопку 

.

Откроется окно ***Управление ключами*** (см. рис. 25).

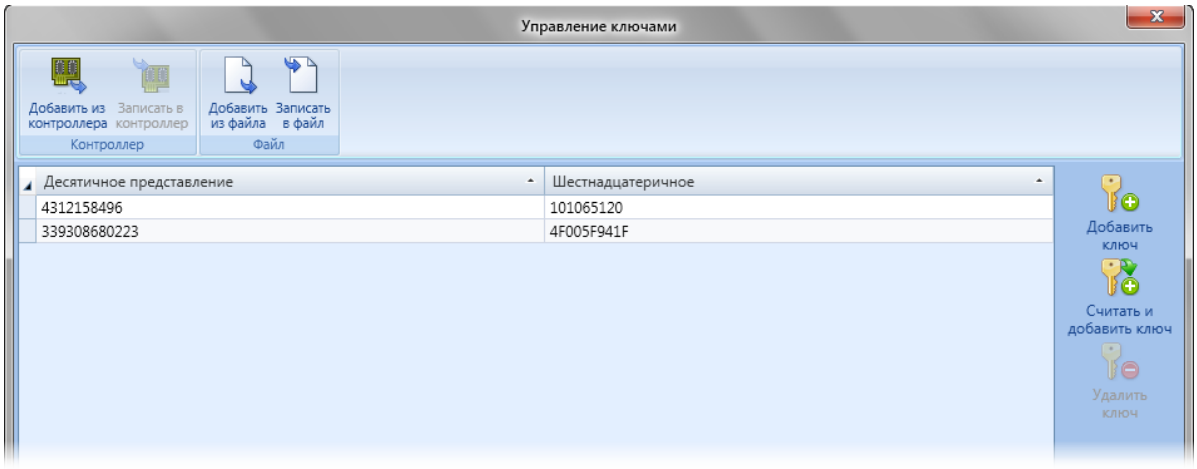


Рисунок 26 - Окно Управление ключами. Загружены ключи из контроллера. По умолчанию список в окне пустой

Вы можете приступить к управлению ключами.

Для того чтобы загрузить ключи из контроллера:

1. Запустите функцию 326 ***Управление ключами*** 326 утилиты для нужного устройства.

2. Нажмите на кнопку  ***Добавить из контроллера***.

Система загрузит ключи, привязанные к контроллеру.

Вы можете экспортировать полученные ключи в файл. Для этого нажмите на кнопку  ***Записать в файл***. Выполните процедуру сохранения файла (формат `.rgkeys`) через Проводник Windows.

Для того чтобы добавить ключи в контроллер из файла:

1. Запустите функцию ***Управление ключами*** утилиты для нужного устройства.
2. Нажмите на кнопку  ***Добавить из файла***.

Откроется окно приложения Проводник Windows.

3. Найдите файл с ключами (формат `.rgkeys`) и раскройте его.

Загрузится список ключей.

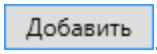
4. Нажмите на кнопку  ***Записать в контроллер***.

Система выполнит запись.

Для того чтобы вручную ввести ключ в контроллер:

1. Запустите функцию ***Управление ключами*** утилиты для нужного устройства.
2. Нажмите на кнопку  ***Добавить ключ***.

Откроется окно ***Добавить ключ***.

3. Введите ключ в шестнадцатеричном или десятеричном представлении. Нажмите на кнопку 

.

Система выполнит привязку ключа к контроллеру.

Для того чтобы считать ключ:

1. Запустите функцию ***Управление ключами*** утилиты для нужного устройства.
2. Нажмите на кнопку  ***Считать и добавить ключ***.

Откроется окно ***Считать и добавить ключ*** (см. рис. 26 и 27).

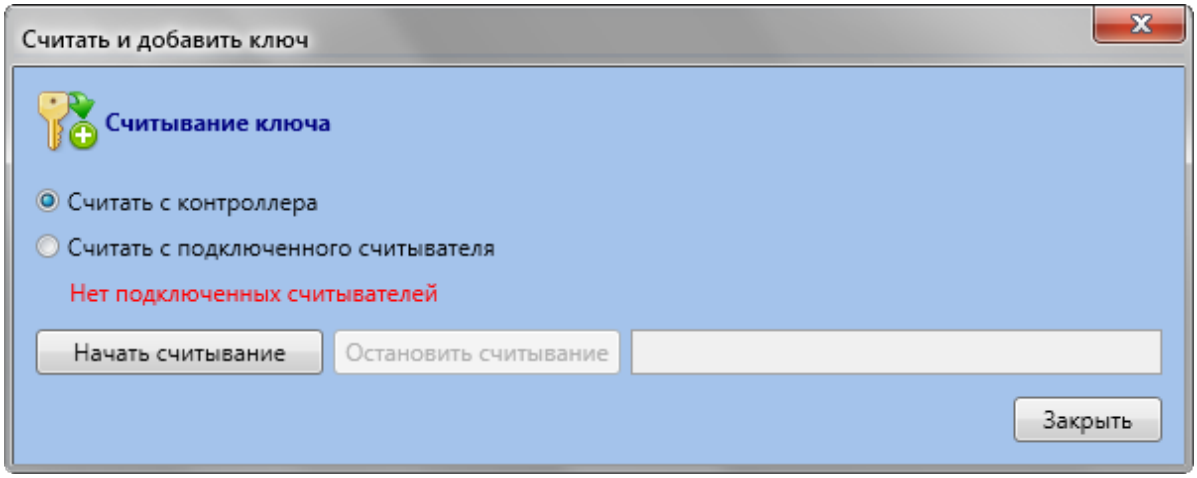


Рисунок 27 - Окно Считать и добавить ключ утилиты. Считывающее устройство не подключено. Возможно считывание с контроллера

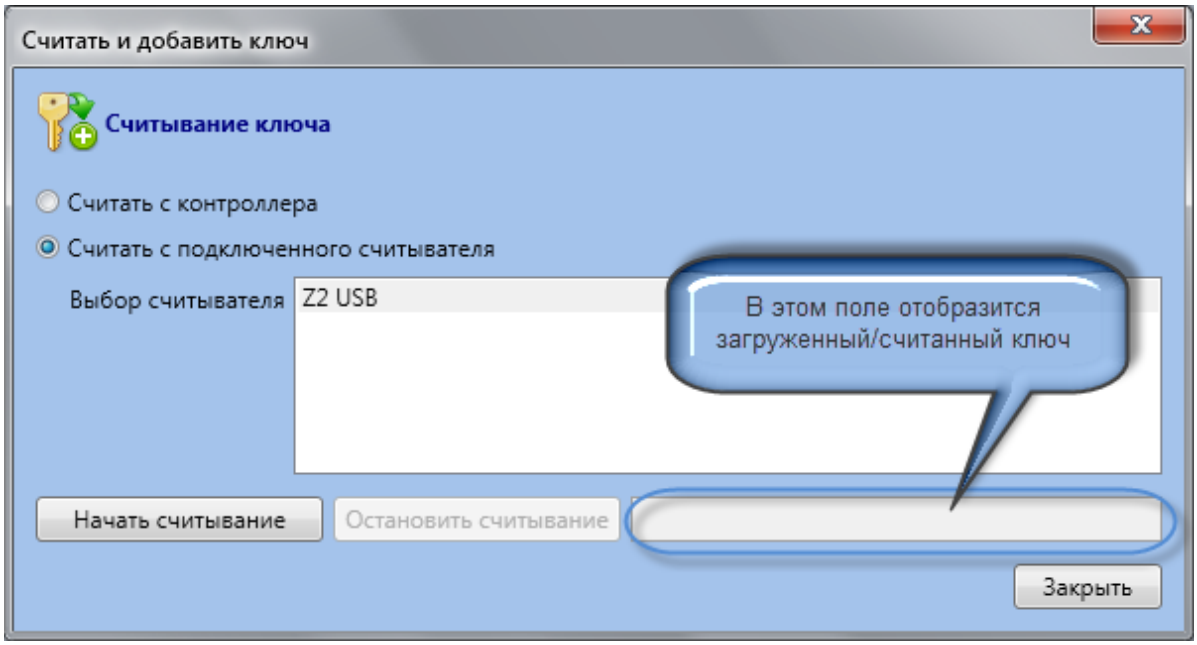


Рисунок 28 - Окно Считать и добавить ключ утилиты. Подключено считывающее устройство

3. Нажмите на кнопку 

. Приложите карточку к считывающему устройству.

Если считывание выполнено успешно, в пустом поле отобразится считанный ключ. Также ключ появится в окне ***Управление ключами***.

4. Вернитесь в окно ***Управление ключами***. Нажмите на кнопку  ***Записать в контроллер***.

Система запишет ключ в контроллер.

Для того чтобы удалить ключ:

1. Запустите функцию *Управление ключами* утилиты для нужного устройства.
2. Выделите в списке ключ, который следует удалить.

Активируется кнопка ***Удалить ключ***.

3. Нажмите на кнопку ***Удалить ключ***.
4. Подтвердите действие.

Система удалит выбранный ключ.

Предупреждения:

Ключи, добавленные через Сервисный конфигуратор не переносятся на сервер при первичном добавлении контроллера в БД.

Если утилита запущена в среде, где установлены другие элементы ПО RusGuard Soft, в т.ч. серверная часть, сервер следует отключить.

Также утилита позволяет выгружать конфигурации устройств в файлы и загружать их из файла. Для этого предназначены кнопки ***Экспорт...*** и ***Импорт...*** в главной панели инструментов утилиты. Процедуры экспорта/импорта выполняются через стандартный диалог сохранения/открытия файла Проводника Windows.

Внимание: Утилита не записывает данные об изменениях в контроллер по умолчанию.

Чтобы отредактированные данные были сохранены, нажмите на кнопку ***Запись*** в главной панели управления.

Обновление прошивки контроллера

Обновление прошивки контроллеров серий ACS-102, 103 и 105 осуществляется с помощью утилиты ***RusGuard_BootLoader_ACS_102_103_105_ver_15*** (файл `.exe`). Скачать актуальную версию утилиты ***RusGuard_BootLoader_ACS_102_103_105_ver_15*** можно бесплатно с сайта компании.

Для того чтобы обновить прошивку:

1. Скачайте с сайта компании нужный `.zip` - архив и распакуйте его на локальном ПК.

В архиве находятся: утилита для установки прошивки и файл с актуальной прошивкой для контроллеров серий CE.

2. Запустите утилиту `RusGuard_BootLoader_ACS_102_103_105_ver_15.exe`. Откроется окно утилиты (см. рис. 28).

Обратите внимание, что при первоначальном запуске утилиты список устройств в списке ***Ethernet*** пуст. При запуске утилиты параметры сервера (адрес и логин) загружаются автоматически.

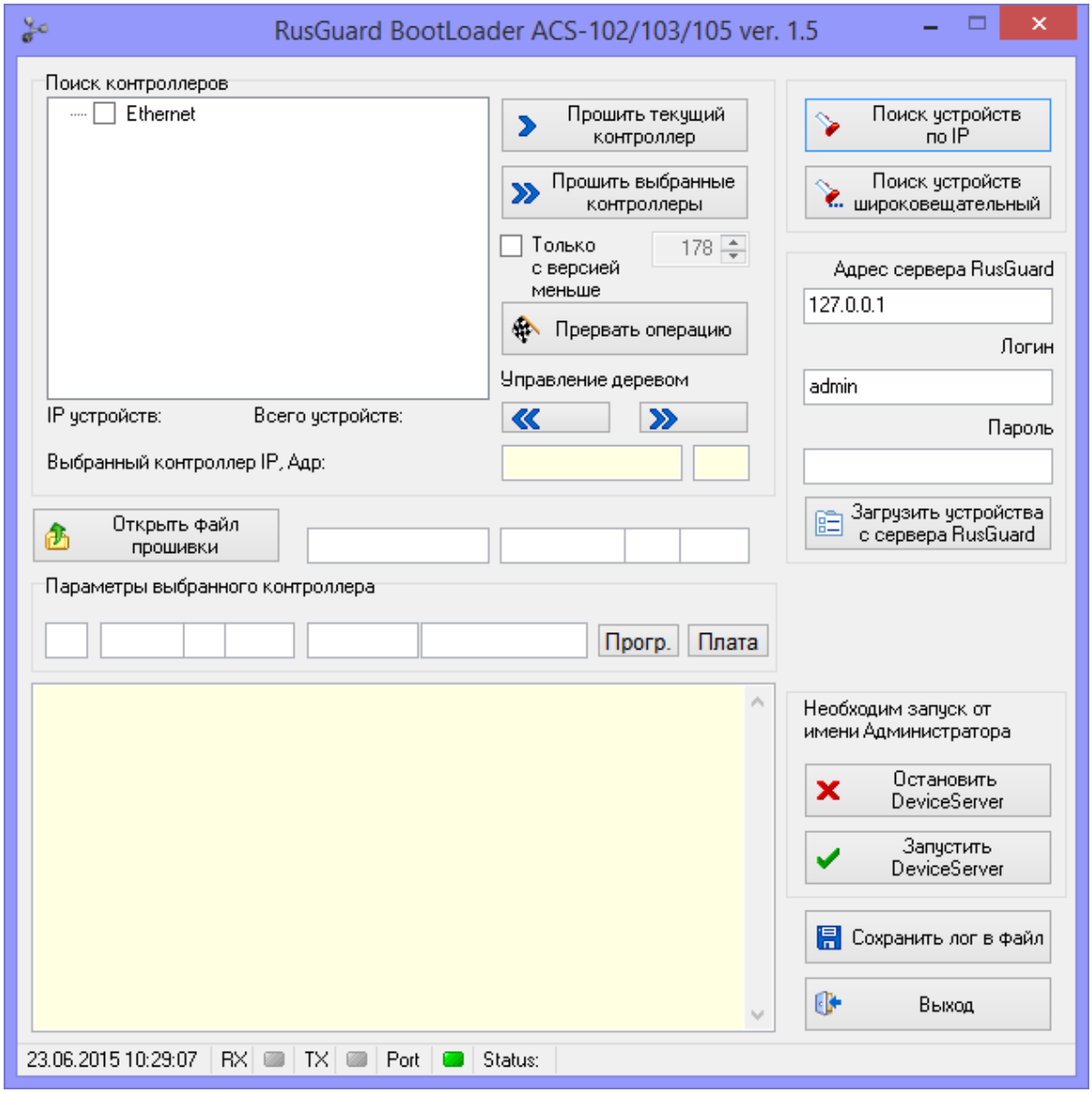
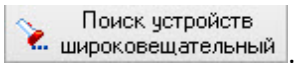
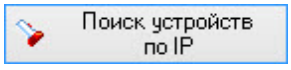


Рисунок 29. Окно утилиты

3. Чтобы найти устройства, выполните одно из следующих действий:

   i. Для поиска внутри ЛВС, нажмите на кнопку 

.

   ii. Чтобы найти системные устройства вне ЛВС, нажмите на кнопку 

, введите IP-адрес искомого устройства и нажмите на кнопку ***OK*** (см. рис. 29).

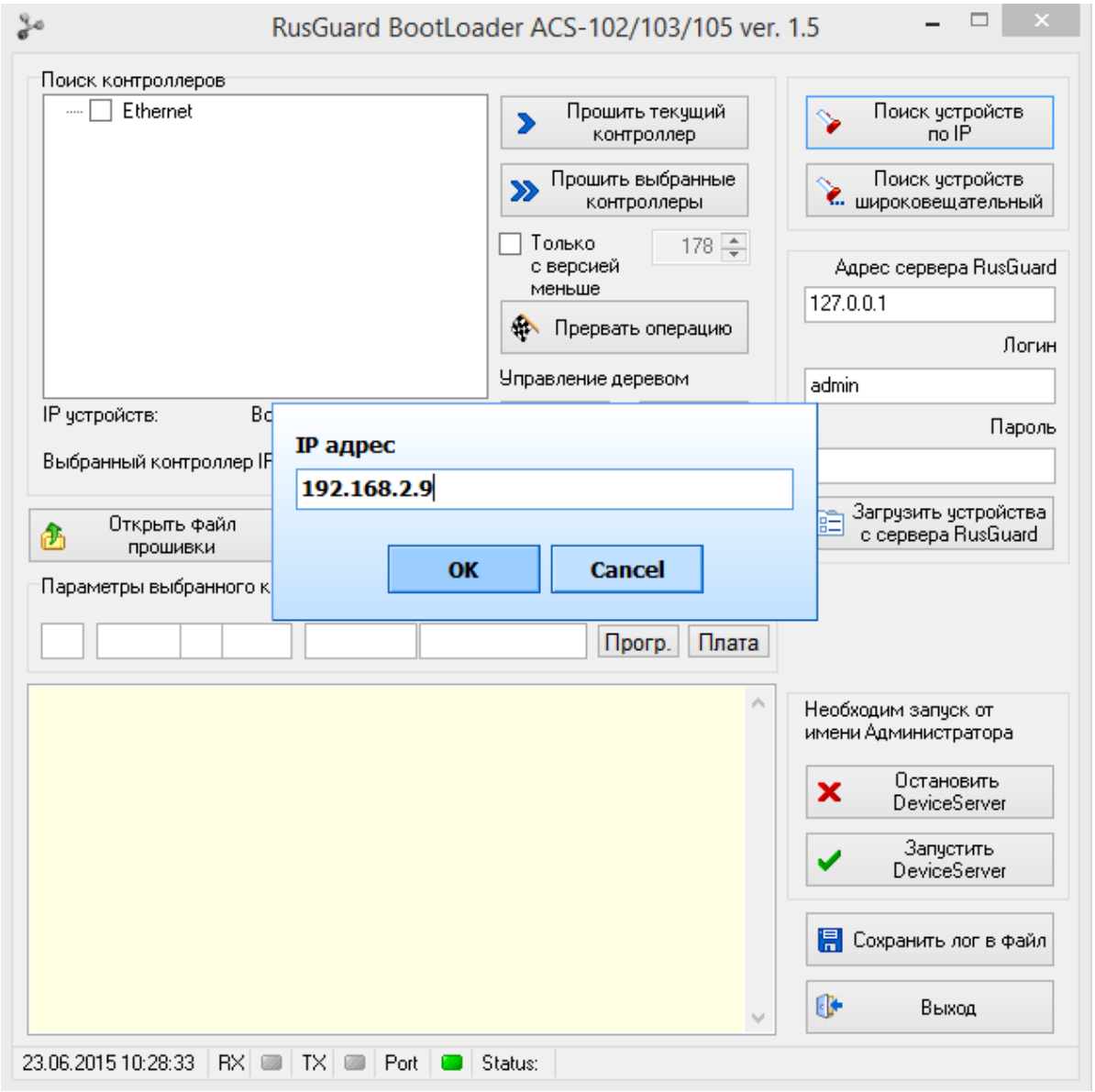
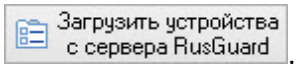


Рисунок 30. Поиск по IP

iii. Чтобы загрузить устройства с сервера RusGuard, нажмите на кнопку 

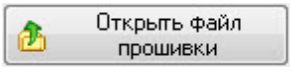
.

Список найденных устройств с указанием IP-адресов и MAC-адресов отобразится в списке ***Ethernet***.

4. Остановите сервер устройств. Для этого нажмите на кнопку 

от имени локального Администратора, либо используйте утилиту RusGuard агент 301.

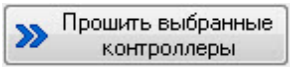
Остановка сервера требуется для предотвращения конфликтов между процессами сервера оборудования и перепрошивкой, которые замедляют процесс.

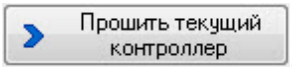
5. Нажмите на кнопку 

и выберите файл прошивки контроллера (`.bin`) в папке на локальном ПК, где был сохранен и распакован исходный архив. Откройте файл.

   Имя файла и его параметры отобразятся в окне утилиты.

6. Установите флаг/и в строке с физическим адресом устройства (устройств), на котором (которых) требуется обновить прошивку.

7. Нажмите на кнопку 

. Чтобы обновить прошивку одного устройства, выделите его в списке и нажмите на кнопку 

.

Обратите внимание, что параметры текущего (выделенного в списке) контроллера, отображаются в окне утилиты справа от списка в области ***Выбранный контроллер***.

Система выполнит установку. Ход процесса отображается в нижней части экрана утилиты (см. рис. 30).

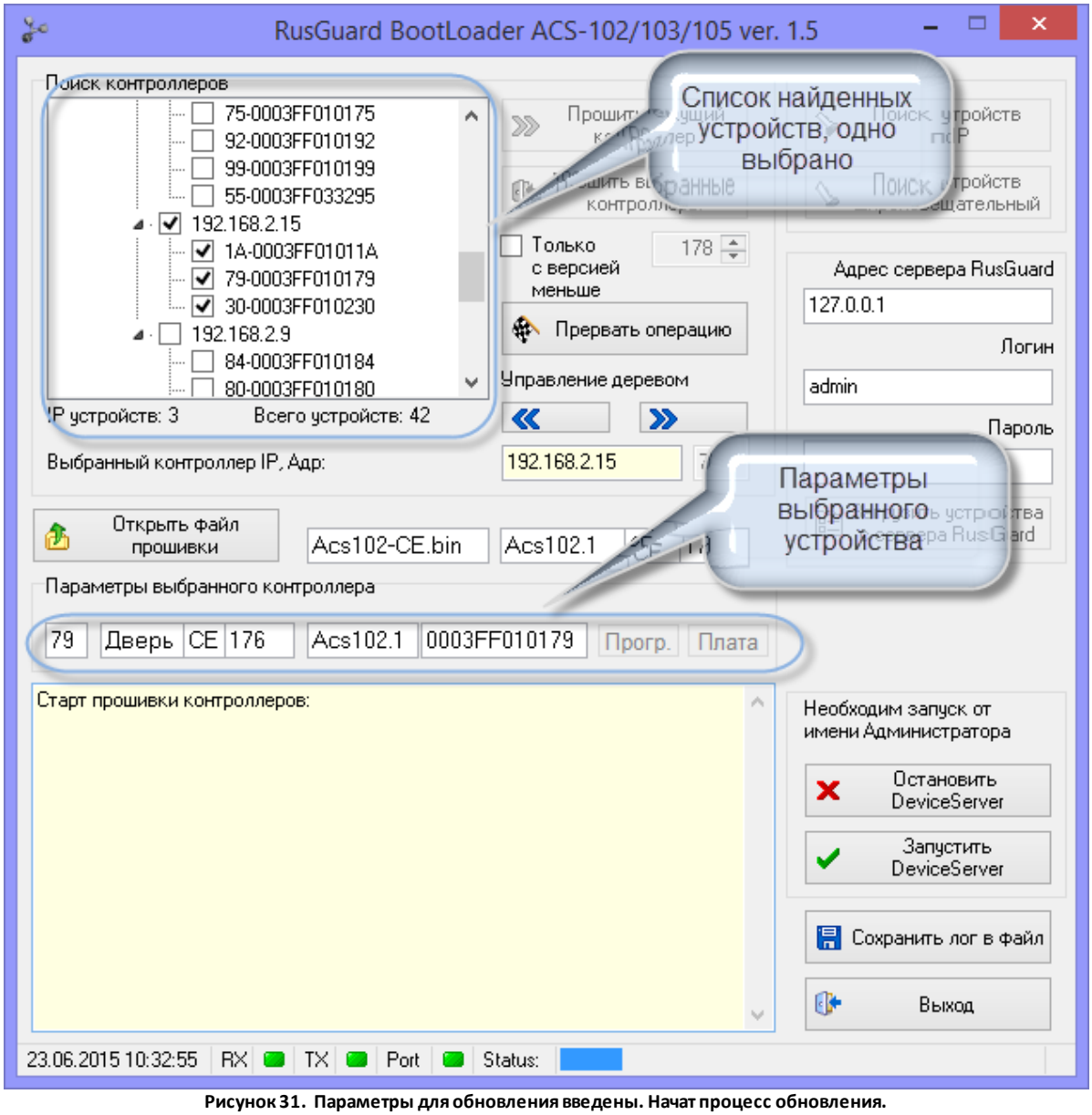


Рисунок 31. Параметры для обновления введены. Начат процесс обновления.

После завершения установки отображается соответствующее сообщение (см. рис. 31).

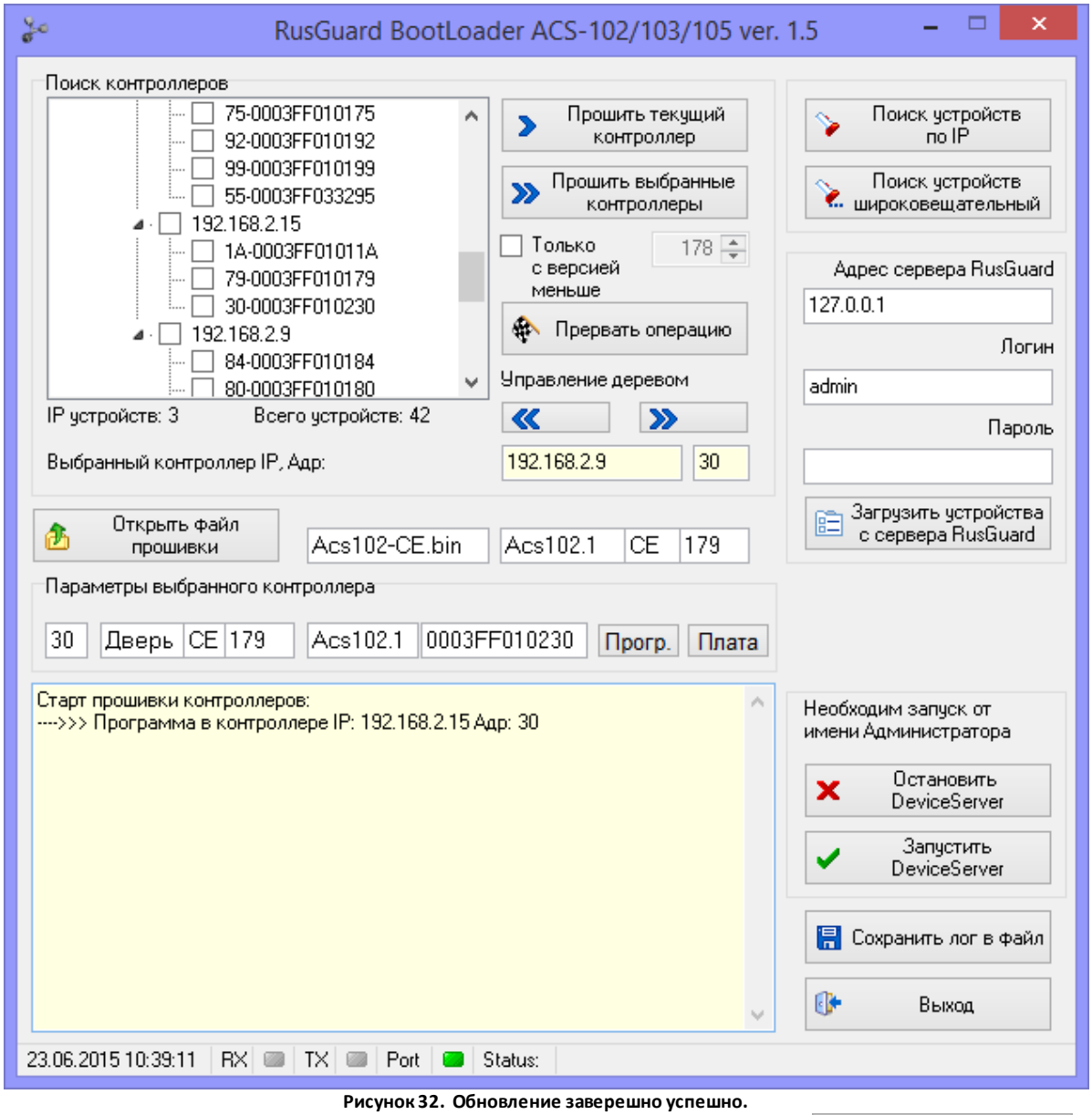


Рисунок 32. Обновление заверешно успешно.

8. Запустите сервер устройств от имени Администратора (кнопка 

либо через утилиту RusGuard агент).
9. Выполните синхронизацию устройств 86 в модуле АРМ Конфигурация оборудования 79.

Информация о системе

Утилита Информация о системе (см. рис. 32) выполняет сбор информации о статусе системы, компонентов и т.д. При штатном функционировании ПО она не требуется.

Утилита позволяет формировать отчет о статусе системы.

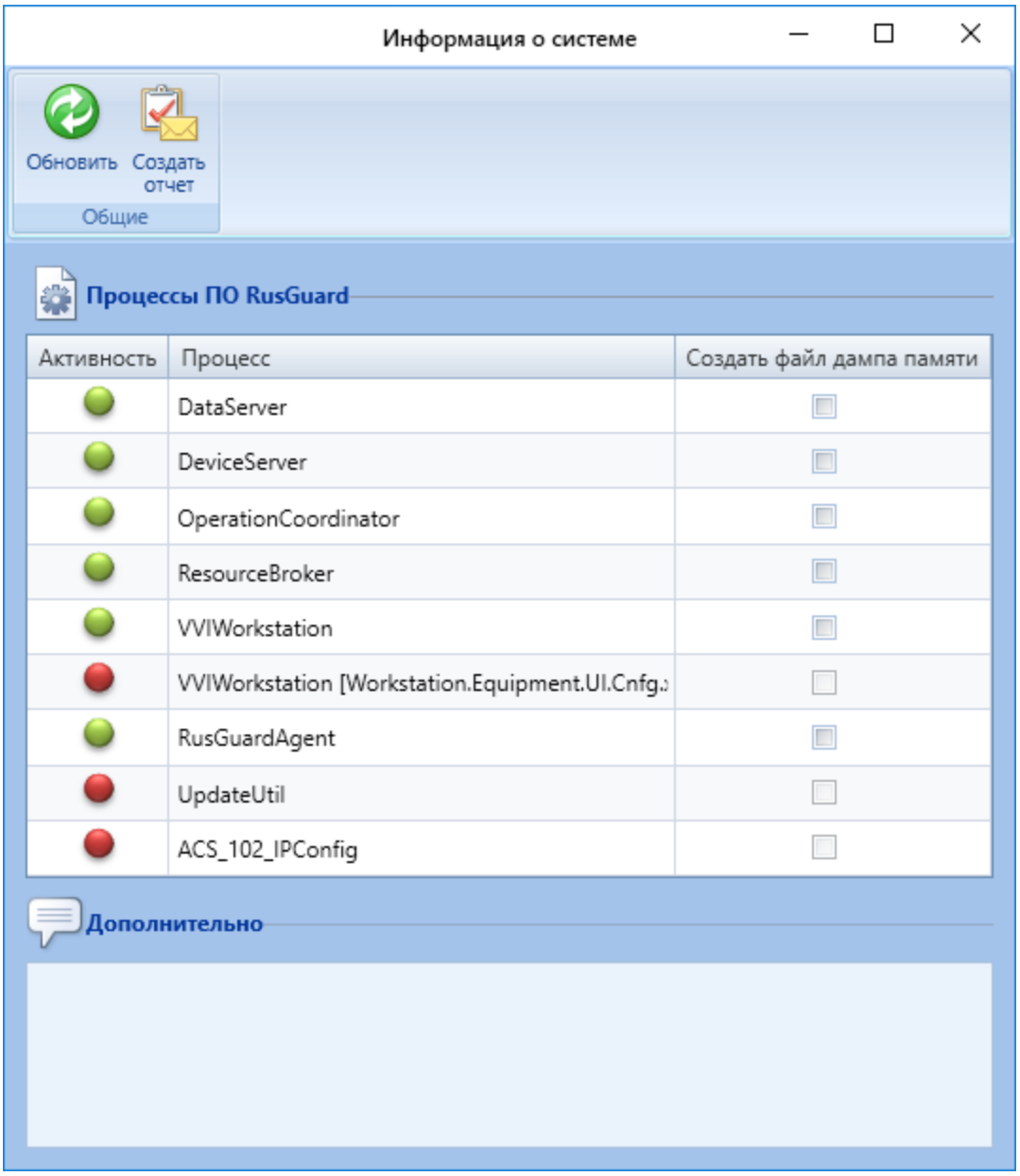


Рисунок 33 - Утилита "Информация о системе"

Для того чтобы сформировать отчет:

1. В случае возникновения ошибок и сбоев в работе ПО RusGuard Soft (выводе окон с сообщениями об ошибках, "зависании" окон и других нештатных ситуациях), запустите утилиту, не закрывая активный компонент ПО RusGuard Soft и сообщения об ошибках.

2. Установите флажки напротив названий доступных компонентов (зеленый индикатор в столбце ***Активность***).
3. Нажмите на кнопку ***Создать отчет***.
4. Сохраните созданный отчет через Проводник Windows.

При обращении в Службу технической поддержки RusGuard 361, опишите в письме условия при которых возникла та или иная нештатная ситуация в работе ПО и вложите созданный утилитой отчет (ZIP архив).

Универсальный импорт из файлов (утилита)

Утилита "Универсальнй импорт из файлов" предоставляется бесплатно. Вы можете скачать ее на сайте компании. Утилита позволяет импортировать списки сотрудников при миграции с других СКУД. Поддерживаются форматы:

- xls/xlsx (на ПК должен быть установлен Microsoft Excel)
- xml
- csv

Утилита не требует установки. Чтобы использовать ее, просто вызовите файл .exe из дистрибутива. Загрузится главное окно (см. рис. 33).

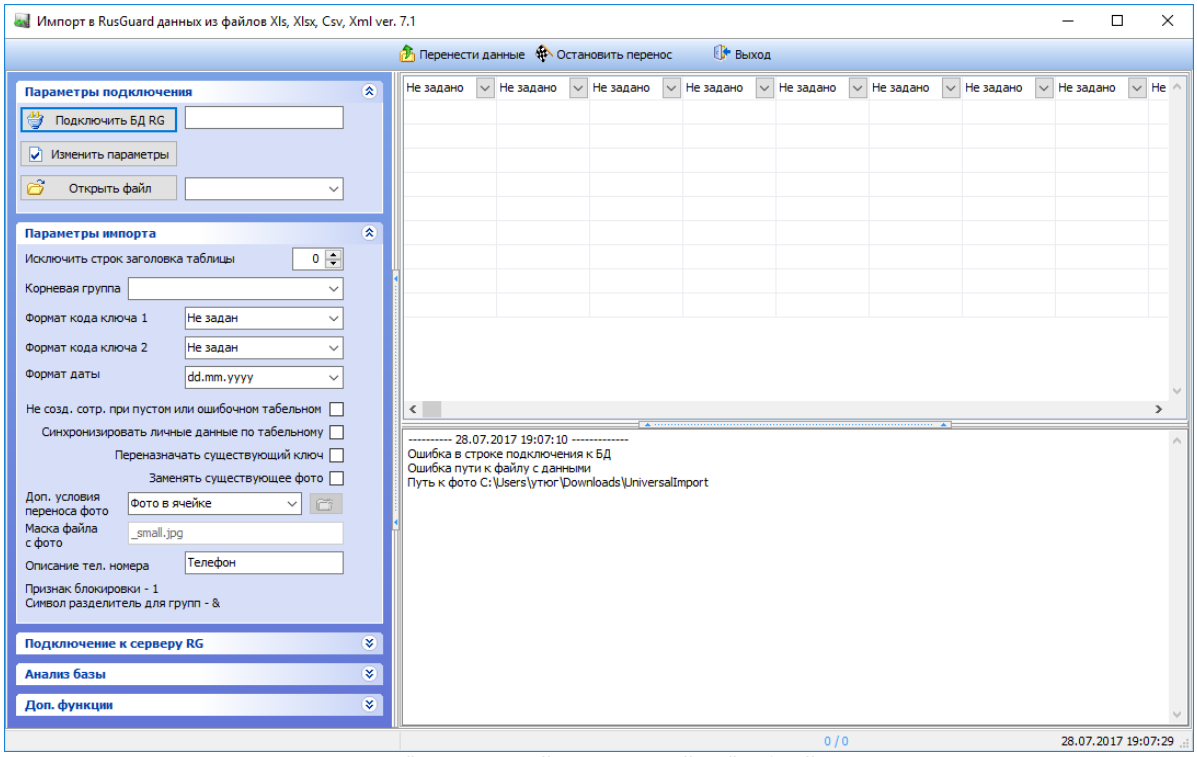


Рисунок 34 - Утилита "Универсальнй импорт из файлов". Общий вид главного окна

Для того чтобы выполнить импорт, необходимо:

- Настроить параметры подключения
- Настроить параметры импорта

Остальные функции утилиты - вспомогательные.

Для того чтобы настроить параметры подключения:

1. Нажмите на кнопу ***Подключить БД RG*** в блоке ***Параметры импорта***. Откроется диалоговое окно (см. рис. 34).

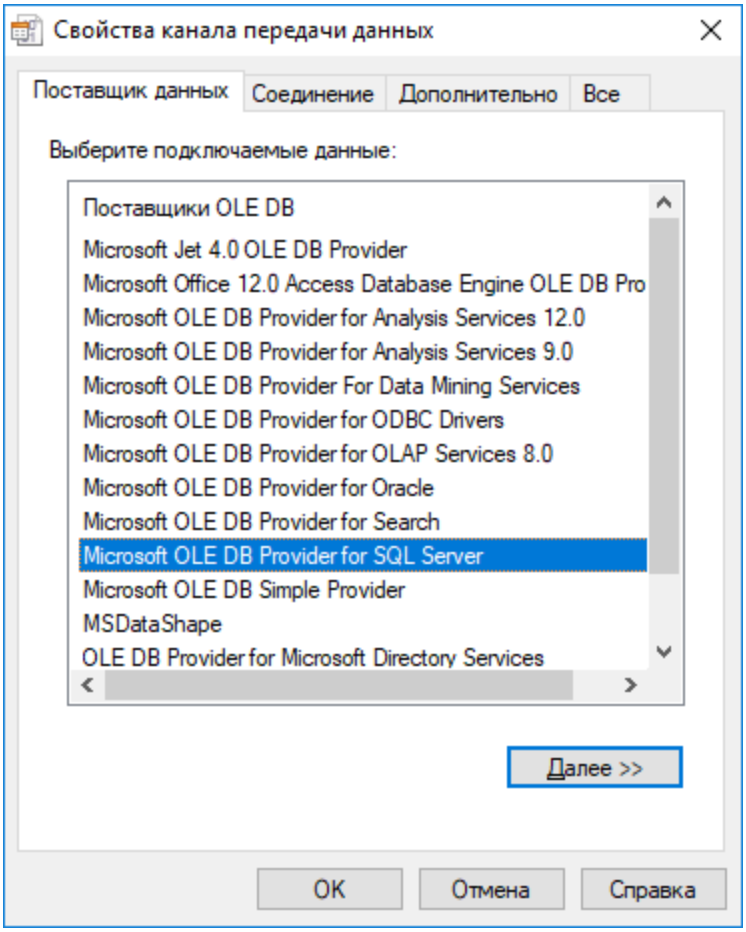


Рисунок 35 - Утилита "Универсальнй импорт из файлов". Настройка подключения к БД

2. На вкладке Поставщик данных выберите вариант Mircrosoft ***OLE DB Provider for ODBC Drivers***. Нажмите на кнопку ***Далее***. Загрузится вкладка ***Соединение*** (см. рис. 35).

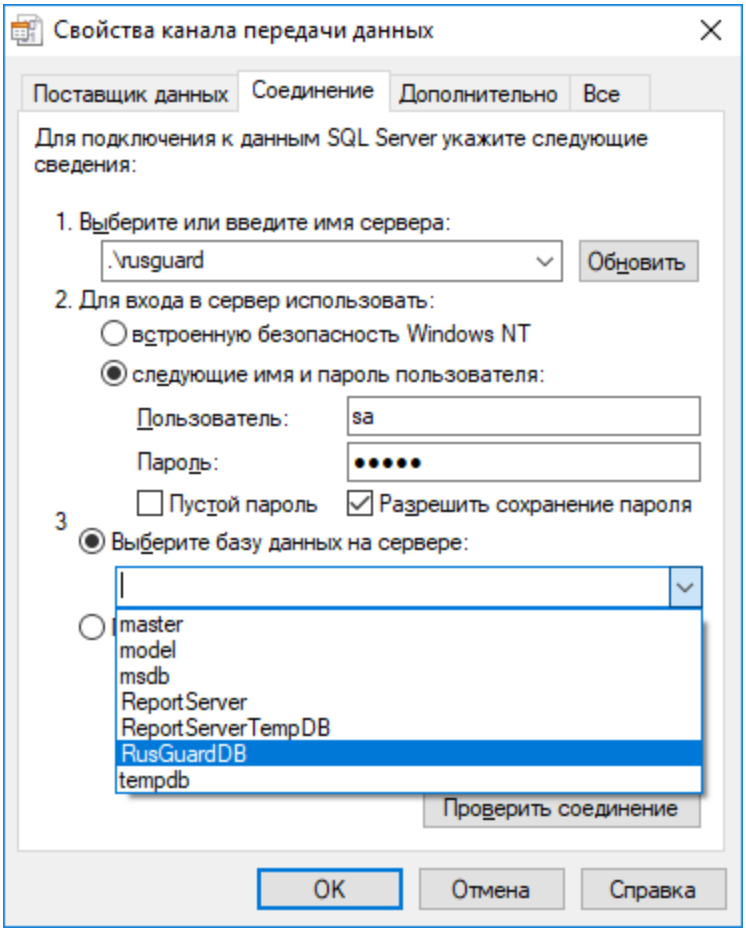


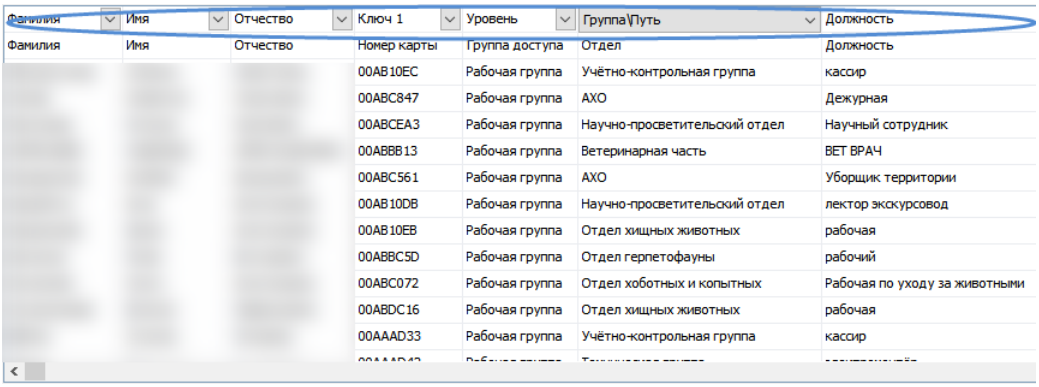
Рисунок 36 - Утилита "Универсальнй импорт из файлов". Настройка подключения к БД. Продолжение

3. Заполните поля как показано на иллюстрации выше (укажите имя сервера РусГард, введите пароль администратора, выберите имя экземпляра БД из списка).
4. Выполните проверку соединения и сохраните данные.

В дальнейшем, для редактирования этих параметров потребуется нажать на кнопку ***Изменить параметры***.

Для того чтобы настроить параметры импорта:

1. Убедитесь, что настроена связь с БД.
2. Нажмите на кнопку ***Открыть файл*** и выберите импортируемый файл на локальном ПК. Данные отобразятся в центральном экране (см. рис. 36).



Фамилия	Имя	Отчество	Ключ 1	Уровень	Группа\Путь	Должность
Фамилия	Имя	Отчество	Номер карты	Группа доступа	Отдел	Должность
			00AB10EC	Рабочая группа	Учётно-контрольная группа	кассир
			00ABC847	Рабочая группа	АХО	Дежурная
			00ABCEA3	Рабочая группа	Научно-просветительский отдел	Научный сотрудник
			00ABBB13	Рабочая группа	Ветеринарная часть	ВЕТ ВРАЧ
			00ABC561	Рабочая группа	АХО	Уборщик территории
			00AB10DB	Рабочая группа	Научно-просветительский отдел	лектор экскурсовод
			00AB10EB	Рабочая группа	Отдел хищных животных	рабочая
			00ABBC5D	Рабочая группа	Отдел герпетофауны	рабочий
			00ABC072	Рабочая группа	Отдел хоботных и копытных	Рабочая по уходу за животными
			00ABDC16	Рабочая группа	Отдел хищных животных	рабочая
			00AAAD33	Рабочая группа	Учётно-контрольная группа	кассир

Рисунок 37 - Утилита "Универсальнй импорт из файлов". Выбран файл, данные отображаются в центральном экране. Выбраны названия столбцов

3. В центральном экране задайте названия столбцов в соответствие с порядком столбцов исходного файла.
4. В блоке ***Параметры импорта*** (см. рис. 37) настройте следующие параметры:
   a. ***Исключить строк заголовка таблицы*** - укажите, сколько строк в начале импортируемой таблицы следует пропустить (по умолчанию, 0);
   b. ***Корневая группа*** - если в файле импорта настроена корневая группа пользователей, ее можно выбрать из списка. Также можно выбрать вариант ***Создать новую*** для автоматического включения импортируемых записей в новую группу. По умолчанию группа не создается.
   c. Выберите форматы кодов ключей 1 и 2 из карточки из списка (в список включены поддерживаемые форматы).
   d. Выберите подходящий формат даты.
   e. В следующих четырех полях установите флаги, если необходимо:
      i. отказаться от импорта записи при отсутствии табельного номера (ошибке в номере);
      ii. синхронизировать данные с текущей базой;
      iii. изменить ключ;
      iv. заменить фото (в этом случае также заполните следующие поля).

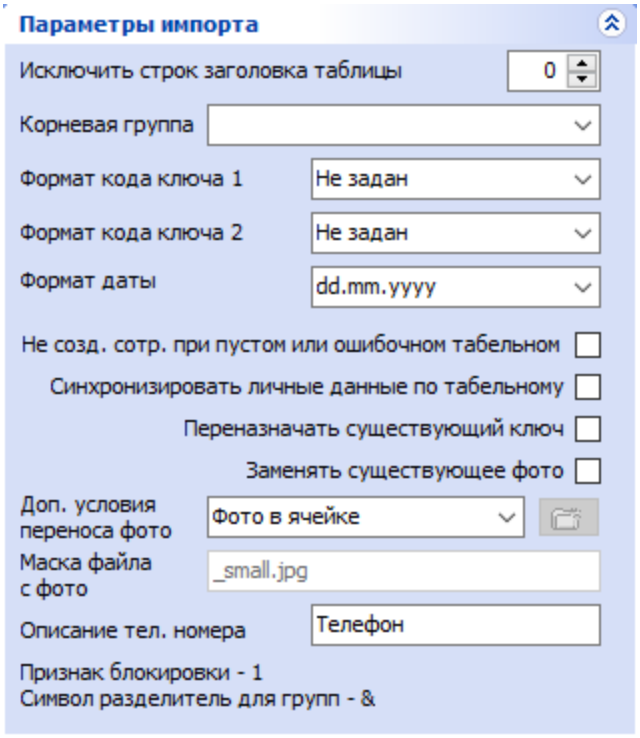


Рисунок 38 - Утилита "Универсальнй импорт из файлов". Настройка параметров импорта

5. Нажмите на кнопку ***Перенести данные***. Система начнет операцию.

Рассылка отчетов (утилита)

Утилита Рассылка отчетов использует стандартные функции ОС Windows для настройки графика рассылки настраиваемых отчетов 224 по УРВ. Обратите внимание, что настройка возможна только если отчеты созданы в АРМ.

Утилита не требует установки, запускается непосредственно из исполняемого файла.

Для того чтобы создать график рассылки, необходимо:

- Настроить параметры отправки
- Создать шаблон рассылки (или несколько шаблонов)
- Создать график рассылки

Для того чтобы настроить параметры отправки:

1. Заполните поля в блоке ***Параметры отправки почты по SMTP*** (см. рис. 38). Значения полей зависят от требований и параметров сервера исходящей почты. Настройки для серверов отправки основных служб приведены в подразделе Ведение базы адресов электронной почты 125.
2. Настроив хотя бы один шаблон, выполните проверку (кнопка ***Отправить тест***).

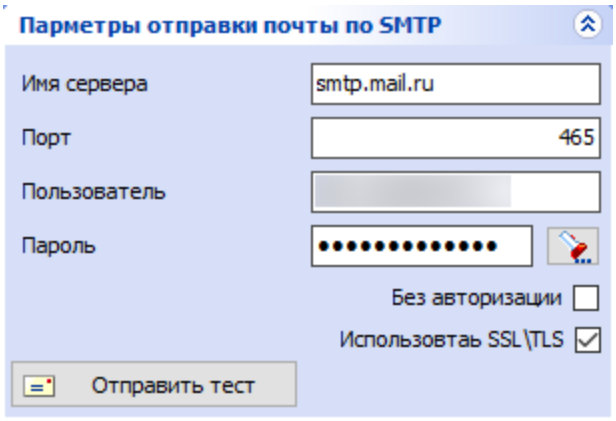


Рисунок 39 - Утилита для рассылки отчетов. Настройка параметров отправки

Для того чтобы создать шаблон рассылки:

1. Запустите утилиту и нажмите на кнопку ***Подключиться*** в блоке ***Параметры подключения*** (данные для подключения к серверу RusGuard подгружаются автоматически) (см. рис. 39). Данные об успешном подключении отображаются в нижней части основного экрана.

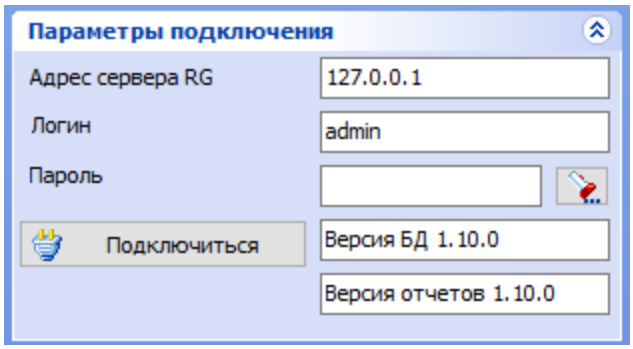


Рисунок 40 - Утилита для рассылки отчетов. Настройка подключения к серверу БД

2. Перейдите на вкладку ***Шаблоны рассылки*** утилиты. Нажмите на кнопку ***Добавить*** под списком шаблонов (по умолчанию пустой). Откроется диалоговое окно для ввода названия нового шаблона (см. рис. 40).

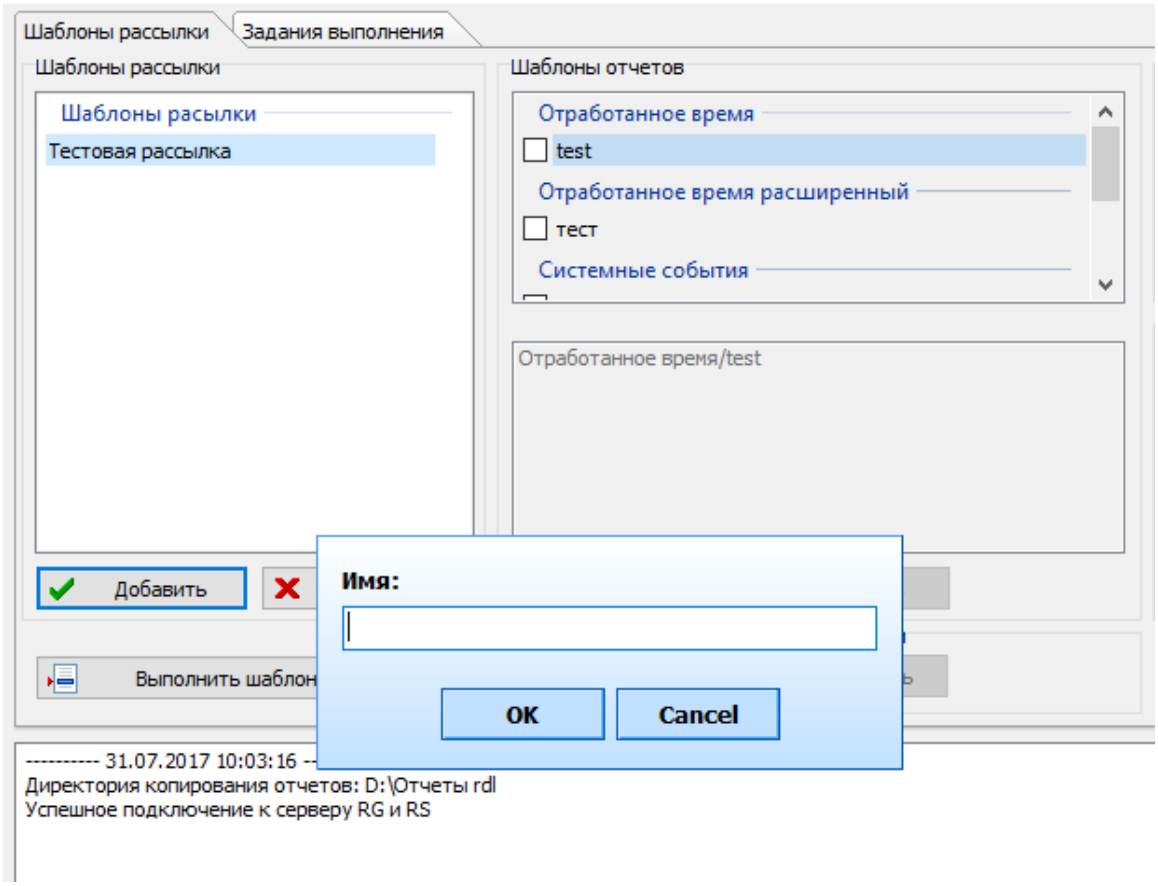


Рисунок 41 - Утилита для рассылки отчетов. Создание нового шаблона. Ввод названия

3. Введите название шаблона и сохраните его. Название нового шаблона отобразится в списке.
4. Установите курсор на названии нового шаблона. Нажмите на кнопку ***Редактировать*** в блоке ***Шаблоны отчетов*** справа. В верхней части окна отобразится список доступных для рассылки отчетов (41).

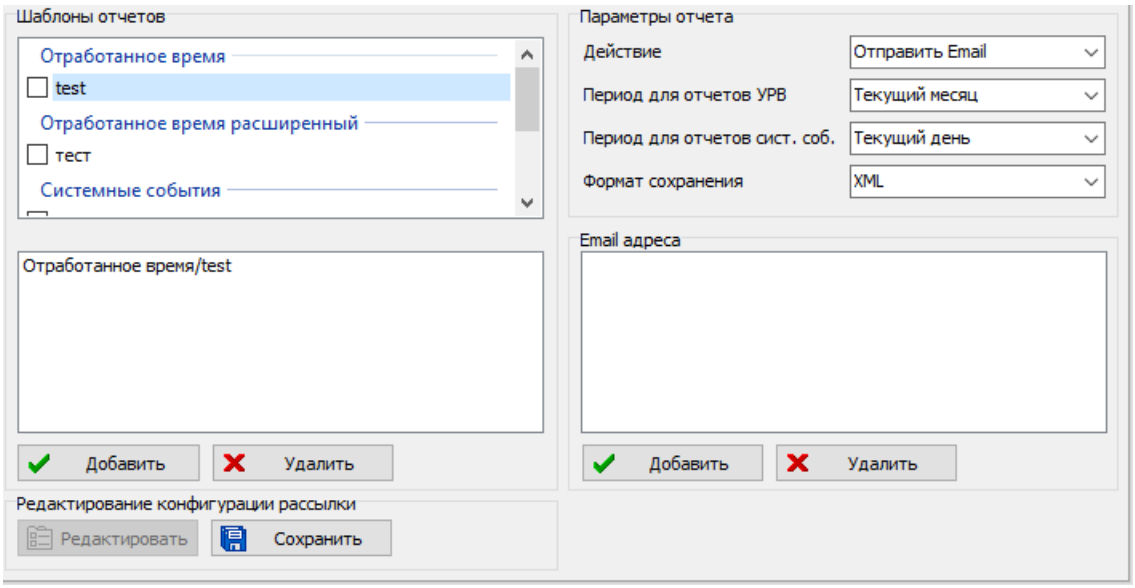


Рисунок 42 - Утилита для рассылки отчетов. Создание нового шаблона. Настройка параметров

5. Выберите один отчет, установите флаг возле его названия (рекомендуется в каждый шаблон добавлять только один отчет). Нажмите на кнопку ***Добавить*** под блоком ***Шаблоны отчетов***. Выбранный отчет отобразится в списке выбранных.
6. В блоке ***Параметры отчета*** сформируйте список адресов, на которые должна выполняться рассылка. Для этого:
   a. Нажмите на кнопку ***Добавить*** под блоком. Откроется диалоговое окно.
   b. Введите адрес электронной почты адресата в диалоговое окно и сохраните данные.
   c. Повторите процедуру для каждого адреса.
7. Настройте параметры рассылки:
   a. В поле Действие выберите вариант ***Отправить Email*** или ***Отправить Email и сохранить файл***, чтобы сохранить локальную копию отчета.
   b. Установите периоды отчетов для отчетов о системных событиях и отчетов по УРВ.
   c. Выберите формат сохранения файла, если планируется сохранять локальную копию.
8. Нажмите на кнопку ***Сохранить***.

Для того чтобы настроить график рассылки:

1. Выполните настройку шаблона, как показано выше.
2. Убедитесь, что в блоке ***Дополнительные настройки*** слева введены учетные данные администратора локального ПК (см. рис. 42).

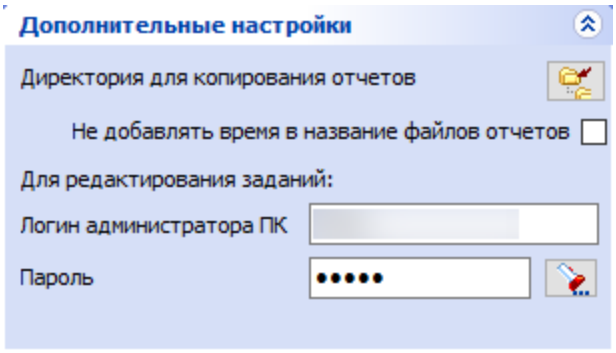


Рисунок 43 - Утилита для рассылки отчетов. Проверка прав локального пользователя

3. Перейдите на вкладку ***Задания выполнения***.
4. Заполните параметры рассылки: выберите шаблон, частоту рассылки (ежедневно, еженедельно, разово) и время рассылки. Для еженедельных рассылок доступны флаги выбора дней недели, вы можете выбрать один или несколько дней.

Только настроив график рассылки следует переходит к следующему пункту процедуры. Обратите внимание, что созданную и настроенную задачу невозможно отредактировать.

5. Нажмите на кнопку ***Создать задачу***. Откроется диалоговое окно (см. рис. 43).

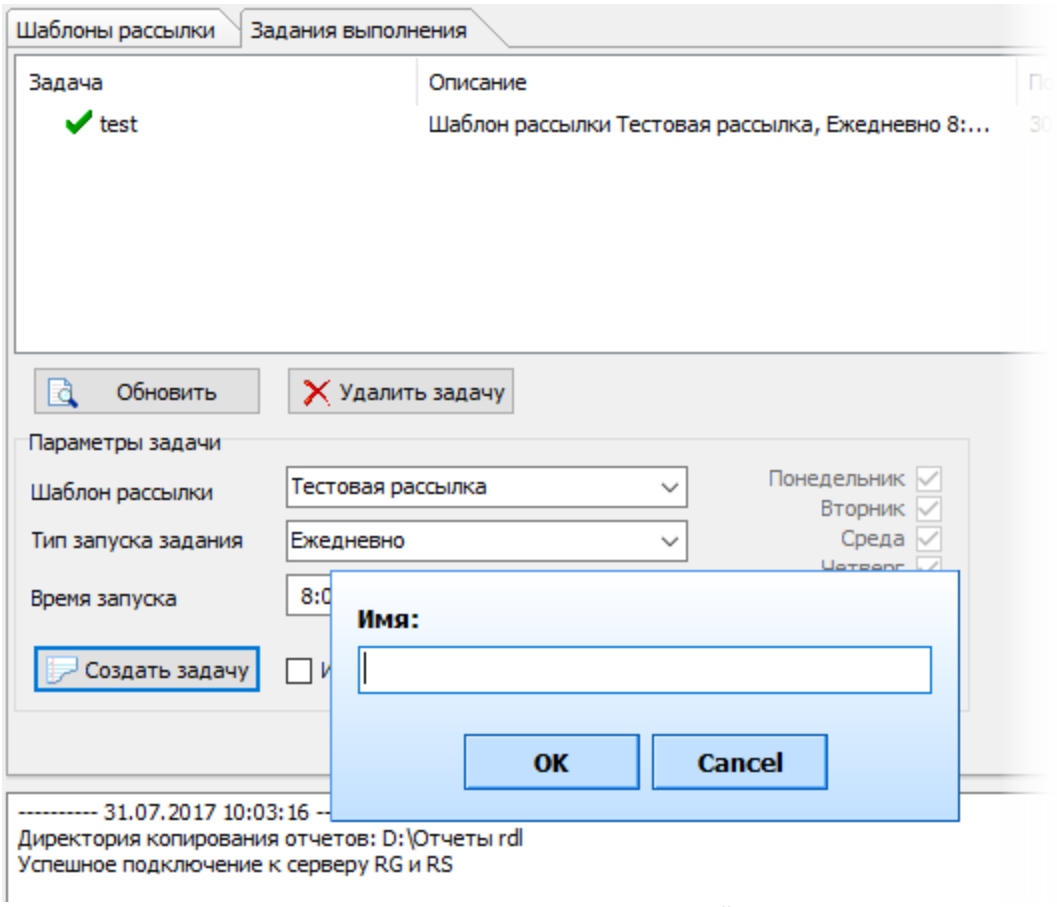


Рисунок 44 - Утилита для рассылки отчетов. Настройка задачи

6. Введите название новой задачи. Сохраните данные. Система сообщит об успешном создании задачи (выполняется проверка прав локального пользователя, см. шаг 2). Название новой задачи отобразится в списке в верхней части основного экрана.

Как правило, утилита работает в фоновом режиме. Флаг ***Интерактивный режим*** позволяет использовать утилиту на ПК, если ОС не поддерживает/блокирует фоновую работу утилиты.

Обслуживание ПО RusGuard Soft

Резервное копирование и восстановление БД

Резервная копия может быть создана как средствами ПО, так и через SQL Server Management Studio.

Использование средств ПО RusGuard

Для того чтобы создать резервную копию БД:

1. Запустите утилиту ***Управление данными системы RusGuard*** 313 (меню ***Пуск*** ОС Windows **>** список ***Все программы >*** папка ***RusGuard***).

Загрузится окно утилиты. По умолчанию открыта вкладка ***Обслуживание*** (см. рис. 1).

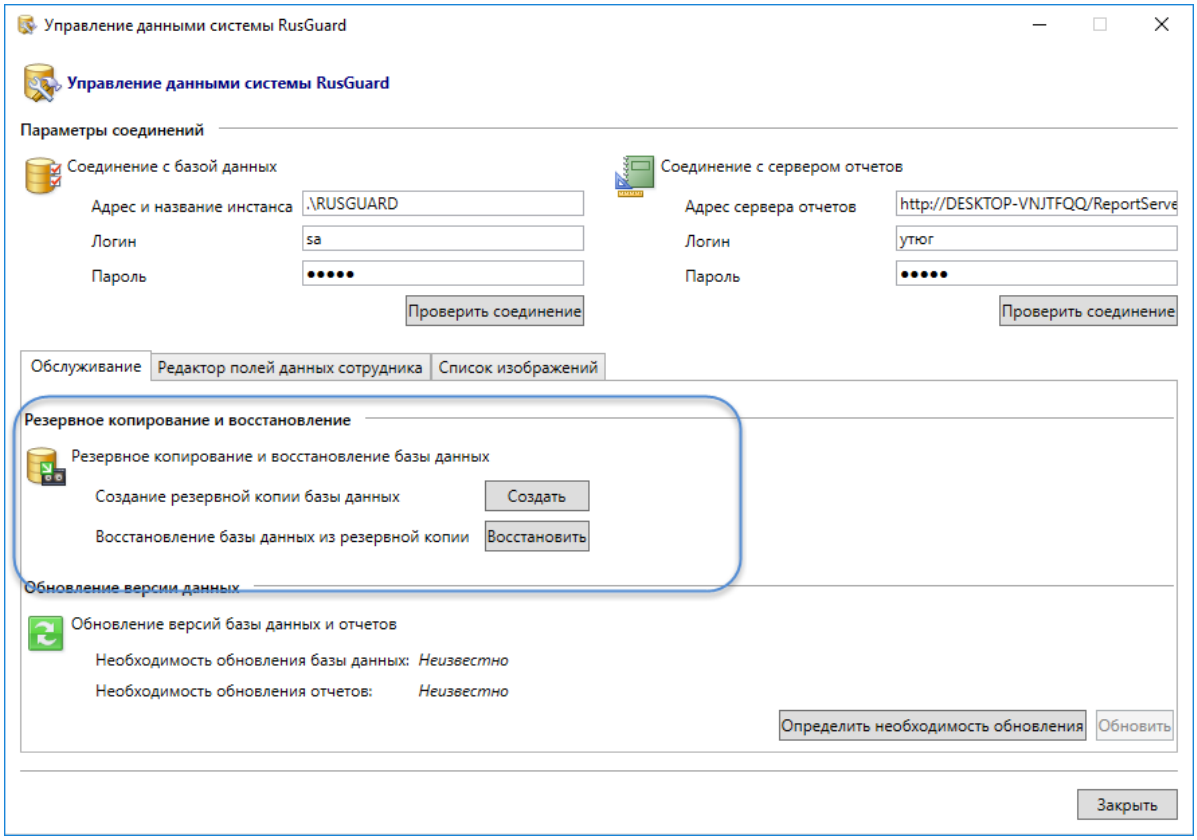
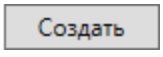


Рисунок 1 - Окно Утилиты "Управление данными системы RusGuard"

2. Нажмите на кнопку  в области ***Резервное копирование и восстановление***.

Откроется стандартный диалог Windows для сохранения файла резервной копии в формате `.bak`.

3. Введите имя файла, укажите, где он должен быть сохранен, подтвердите сохранение.

Система обратится к БД и выполнит резервное копирование.

Для того чтобы восстановить резервную копию:

1. Запустите утилиту ***Управление данными системы RusGuard*** 313 (меню ***Пуск*** ОС Windows **>** в список ***Все программы >*** папка ***RusGuard***).

Загрузится окно. По умолчанию открыта вкладка ***Обслуживание***.

2. Нажмите на кнопку Восстановить в области ***Резервное копирование и восстановление***.
3. Выберите нужный файл резервной копии и откройте его.
4. После восстановления **обязательно** проверьте совместимость с версией БД 356 (кнопка Определить необходимость обновления). Запустите процесс обновления в случае положительного ответа (кнопка Обновить).

Использование SQL Server Management Studio

Если необходимо выполнить восстановление резервной копии на ПК с другой конфигурацией, используйте утилиту Microsoft SQL Server Management Studio (доступна через меню ***Пуск***).

Для того чтобы создать резервную копию БД:

1. Запустите SQL Server Management Studio.
2. Перейдите к пункту ***Базы данных*** > ***База данных RusGuard*** (т.е. установите курсор на папку с базой данных СКУД).
3. Вызовите контекстное меню и выберите пункты ***Задачи*** > ***Создать резервную копию*** (см. рис. 2).

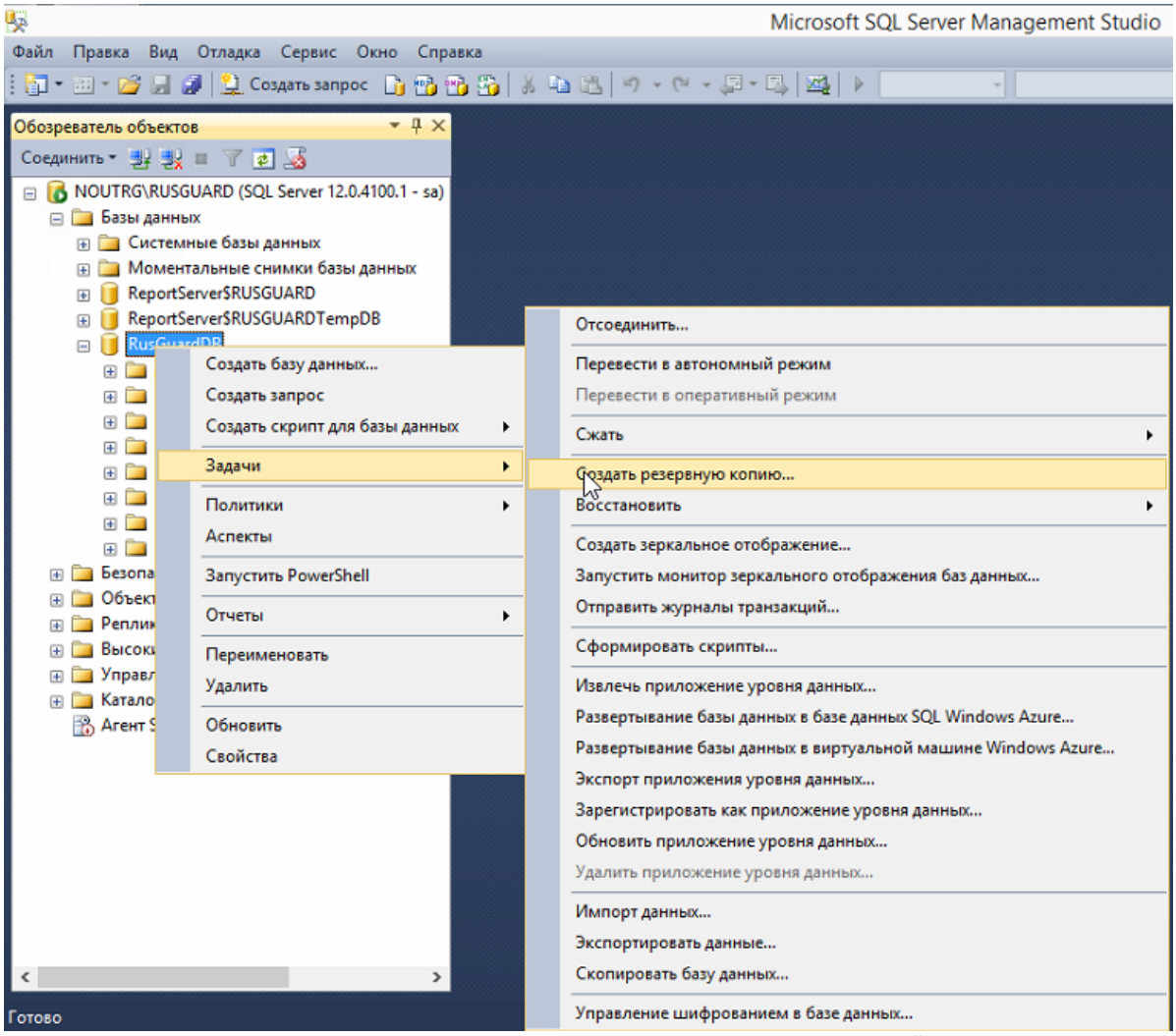


Рисунок 2 - Окно Утилиты SQL Server Management Studio. Создание резервной копии

4. Укажите путь для создания резервной копии.

Предупреждения:

- В файле резервной копии содержатся данные об имени ПК, имени экземпляра SQL-сервера и пути к файлам базы данных того ПК, на котором была сформирована данная копия. Поэтому корректное восстановление возможно только на этом же ПК, или на ПК имеющем абсолютно идентичную конфигурацию.

- Не сохраняйте резервные копии на Рабочем столе или в корневом каталоге ПК.

Для того чтобы восстановить резервную копию БД:

5. Запустите SQL Server Management Studio.
6. Перейдите к пункту ***Базы данных***.
7. Вызовите контекстное меню и выберите пункты ***Задачи*** > ***Восстановить***.

8. Выберите файл с резервной копией и установите настройки как показано ниже (см. рис. 3, 4, 5 и 6). Нажмите на кнопку ***ОК***.

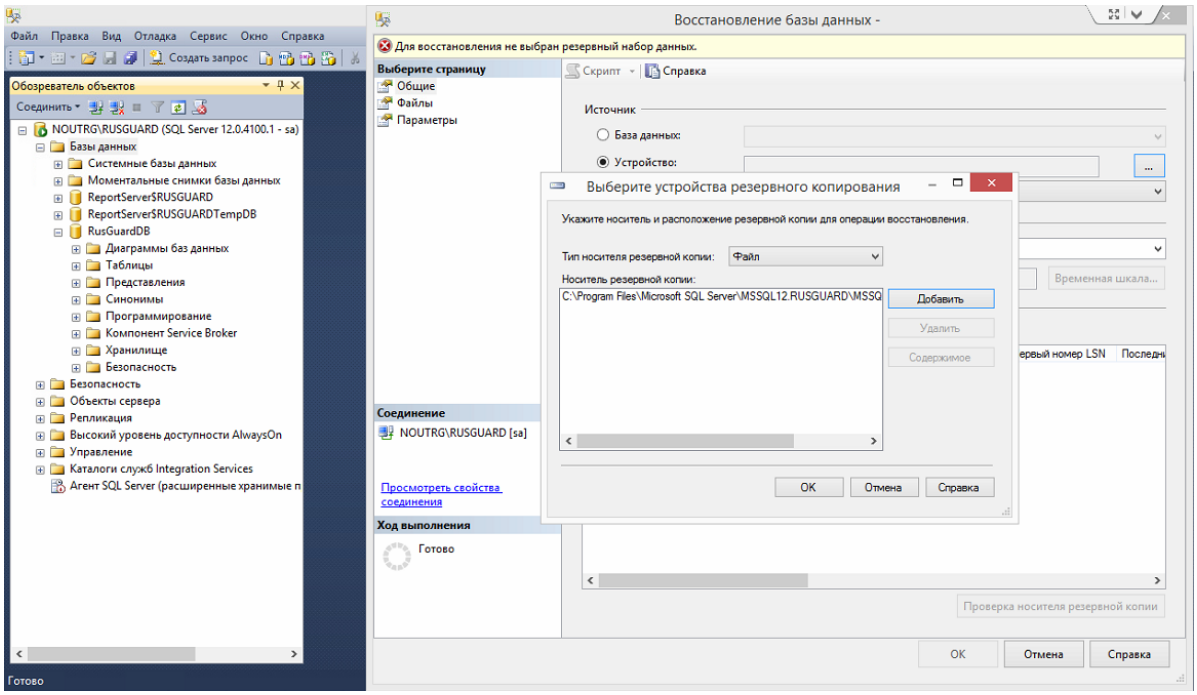


Рисунок 3 - Окно Утилиты SQL Server Management Studio. Восстановление резервной копии

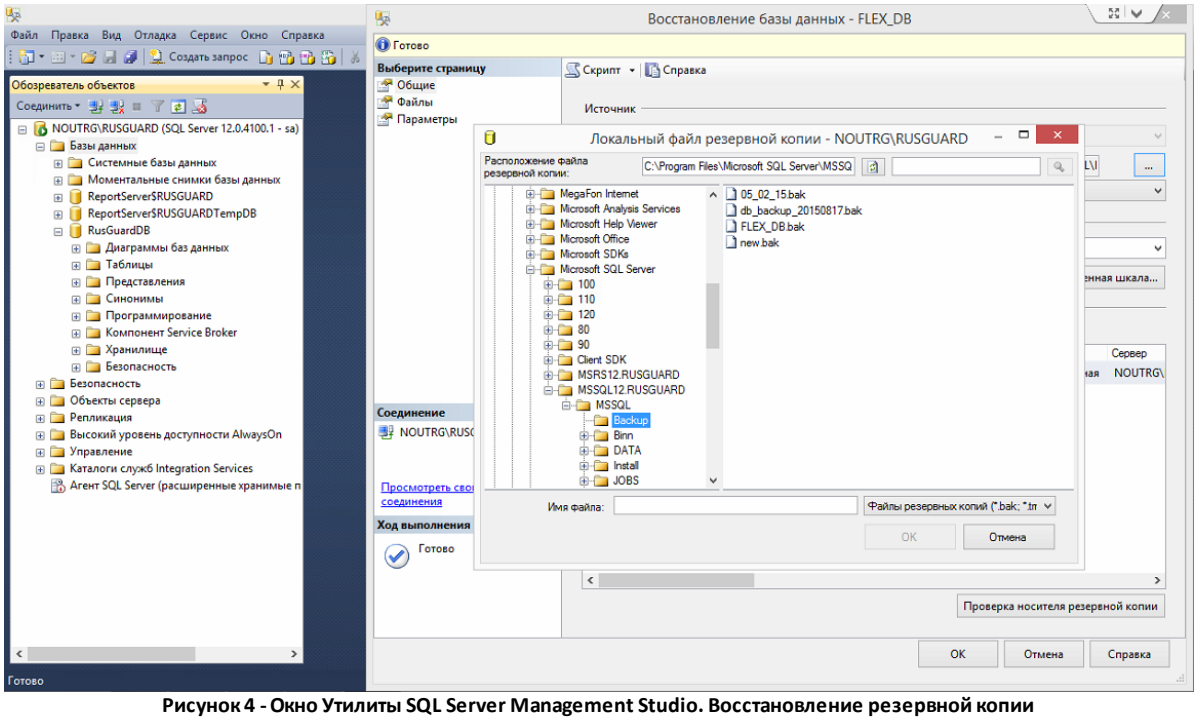


Рисунок 4 - Окно Утилиты SQL Server Management Studio. Восстановление резервной копии

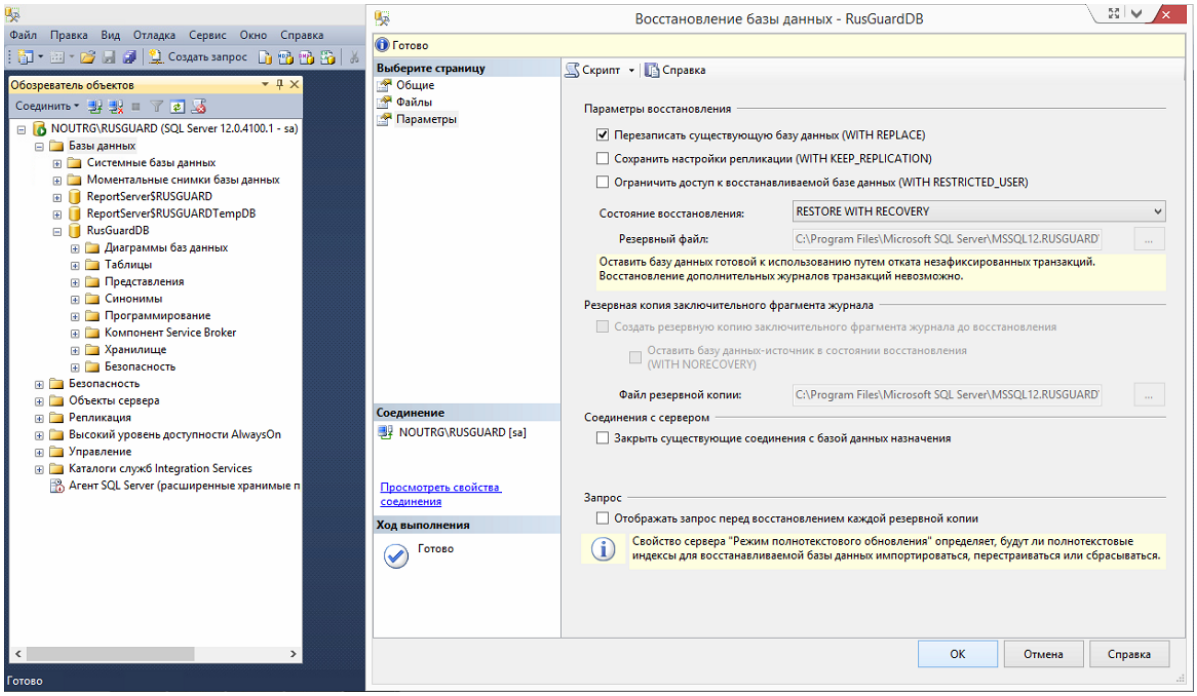


Рисунок 5 - Окно Утилиты SQL Server Management Studio. Восстановление резервной копии

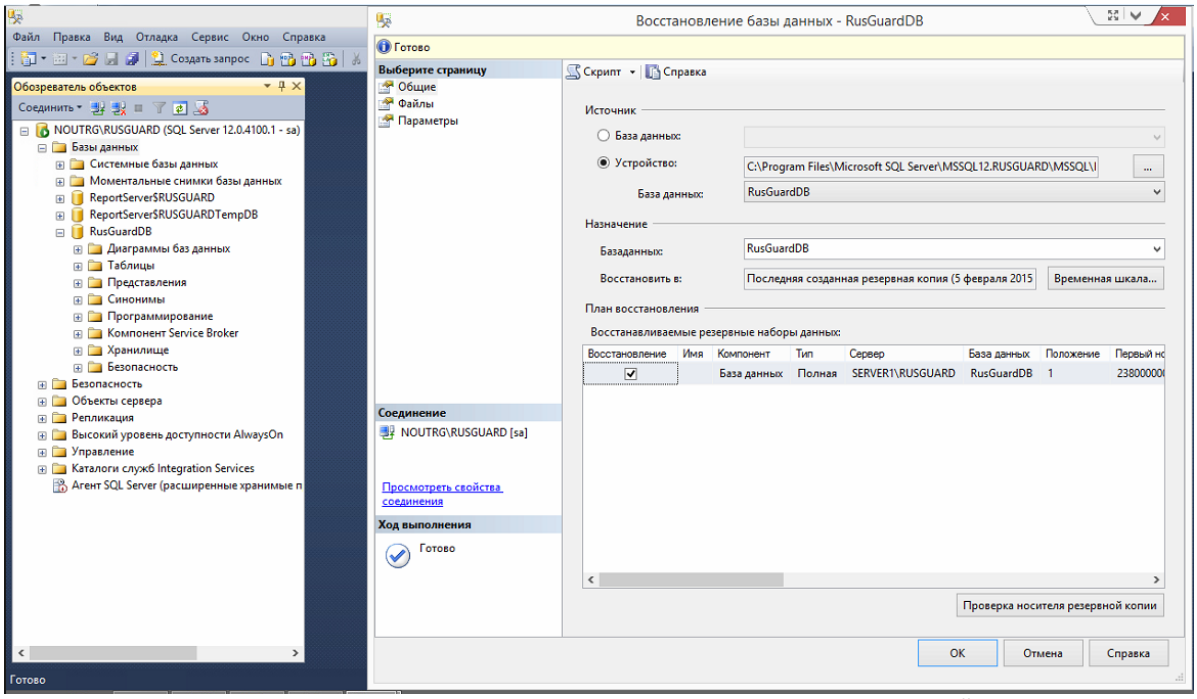


Рисунок 6 - Окно Утилиты SQL Server Management Studio. Восстановление резервной копии

Обратите внимание, что резервную копию нельзя восстановить с сетевого диска. Она должна находиться на локальном компьютере.

См. также раздел о возможных ошибках 300.

Удаление ПО RusGuard Soft

Для удаления ПО RusGuard Soft применяется стандартная процедура удаления ПО в ОС Windows, либо соответствующая функция установщика (см. рис. 7).

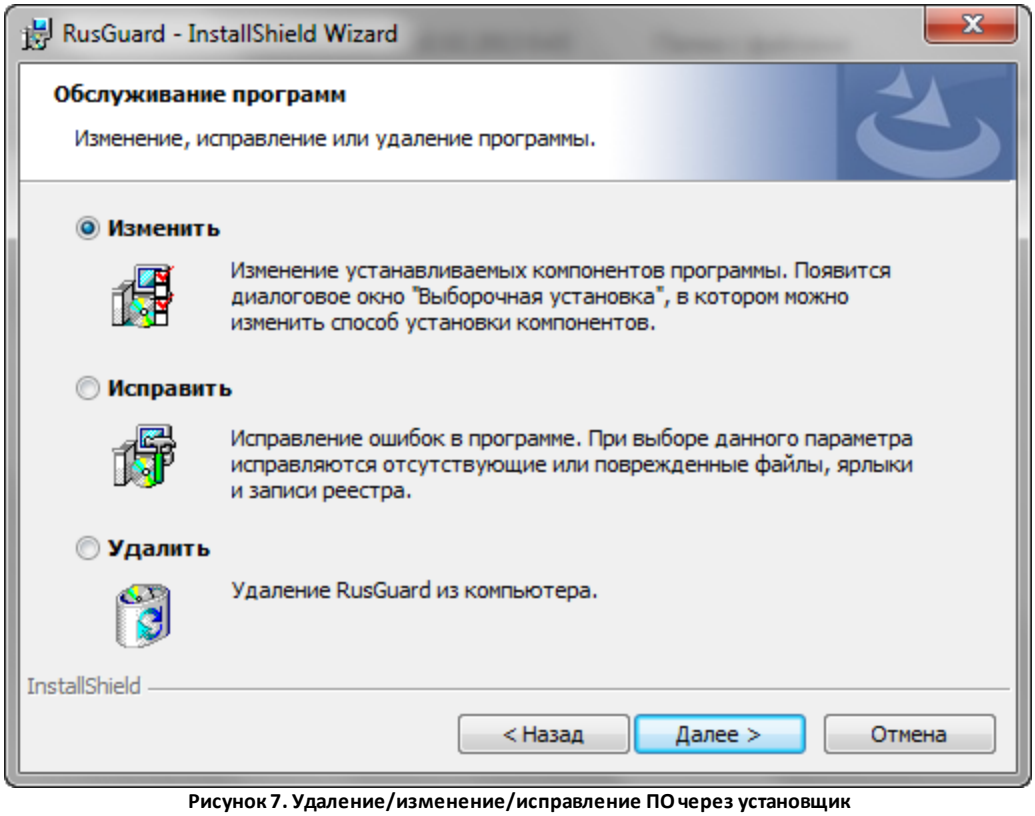


Рисунок 7. Удаление/изменение/исправление ПО через установщик

Для того чтобы удалить ПО RusGuard:

1. Откройте утилиту ***RusGuard агент*** 301.
2. На вкладке ***Сервисы*** 302 остановите все процессы (нажмите на кнопку  ***Остановить все***).
3. Завершите работу утилиты RusGuard агент (щелкните правой кнопкой мыши по значку утилиты в трее, выберите пункт ***Выход*** в раскрывшемся контекстном меню).
4. Закройте запущенные локальные АРМ.
5. В списке установленных программ (меню ***Пуск > Панель инструментов > Программы и компоненты***) выберите RusGuard, нажмите ***Удалить***.

Примечание: Процедура удаления не удаляет созданную БД системы, которая может потребоваться при установке новой версии ПО RusGuard Soft.

Предупреждение: После удаления БД восстановить прежнюю конфигурацию системы без резервной копии будет невозможно.

Для полного удаления БД RusGuard:

1. Запустите ***Microsoft SQL Server Management Studio*** (меню ***Пуск > все программы > Microsoft SQL Server 2008***).
2. Введите учетные данные для управления SQL сервером (как правило, данные уже сохранены при установке SQL-сервера).
3. Раскройте список ***Databases*** (базы данных) в навигационной панели слева (см. рис. 8).

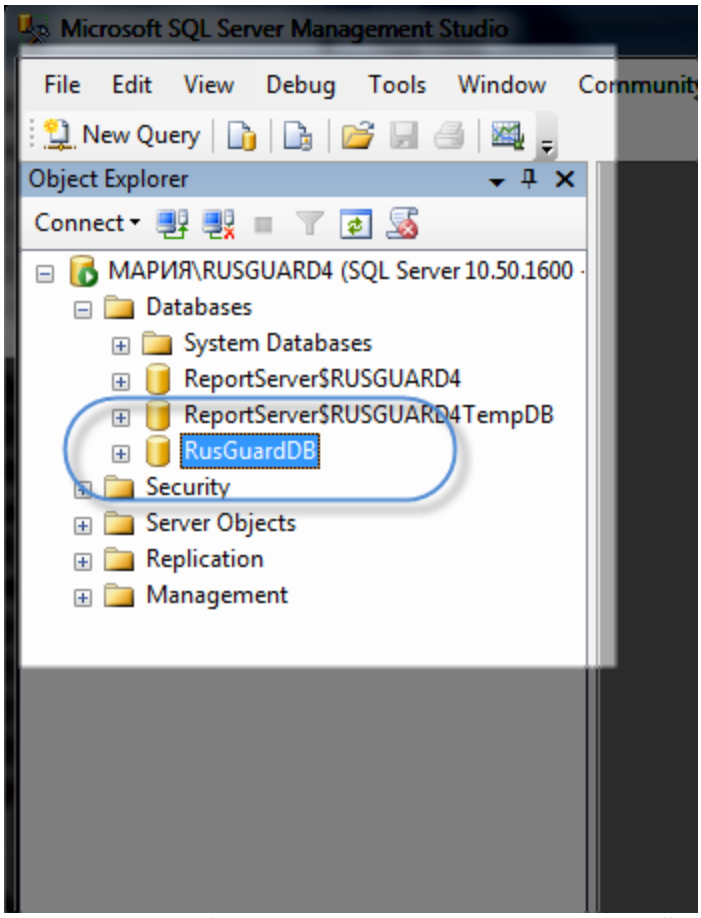


Рисунок 8. Microsoft SQL Server Management Studio. Иерархический список в навигационной панели

4. Найдите нужный экземпляр базы данных в списке.
5. Установите курсор мыши на строку с названием данного экземпляра.
6. В главном меню выберите ***Edit > Del*** (либо вызовите контекстное меню щелчком мыши).
7. В появившемся окне установите флаг ***Закрыть существующие соединения*** и нажмите на кнопку ***ОК***.

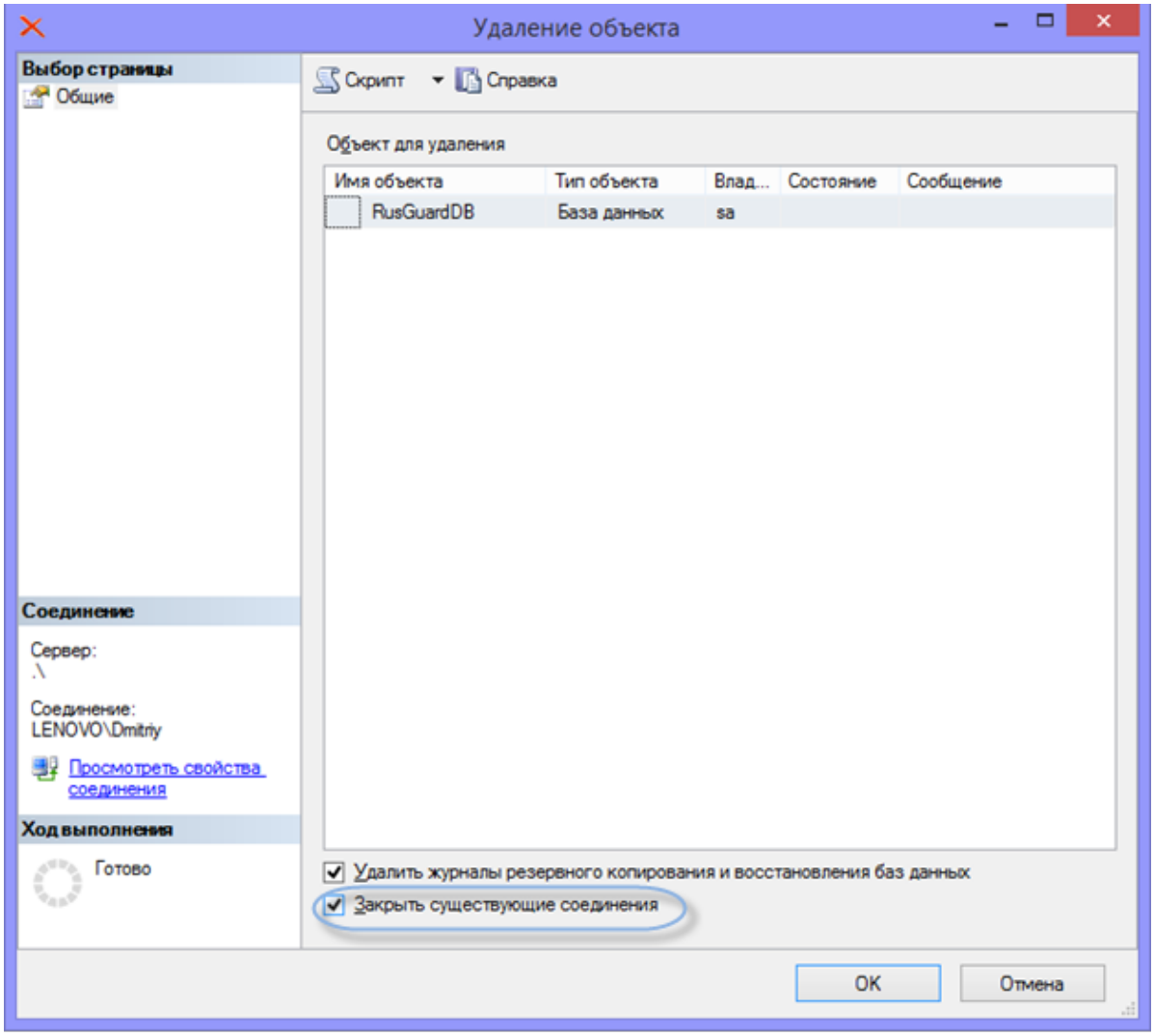


Рисунок 9. Удаление объекта

8. Удалите базу данных.

Обновление ПО RusGuard Soft

Для того чтобы обновить ПО RusGuard Soft:

1. Выполните резервное копирование БД 348.
2. Удалите текущую версию ПО с компьютера 353.

Примечание: После удаления ПО все использованные ранее учетные данные сохранятся в конфигурационном файле и автоматически загрузятся в формы ввода при установке новой версии.

3. Установите новую версию (см. разделы Установка сервера RusGuard 31 и Установка АРМ и утилит RusGuard 61) .
4. Обновите все АРМ, используемые в системе.

Примечание: Возможно, но крайне не рекомендуется, использование АРМ предыдущих версий с более новой версией сервера. Новые функции серверной части не будут доступны в сочетании с АРМ более ранних версий.

5. При установке новой версии может потребоваться обновление версии базы данных. Выполните обновление 356, если это необходимо.

Необходимость обновления версии БД при установке новой версии ПО

При установке новой версии ПО RusGuard может быть выявлен конфликт версий базы данных и ПО.

В этом случае перед завершением инсталляции отобразится соответствующее сообщение (см. рис. 9).

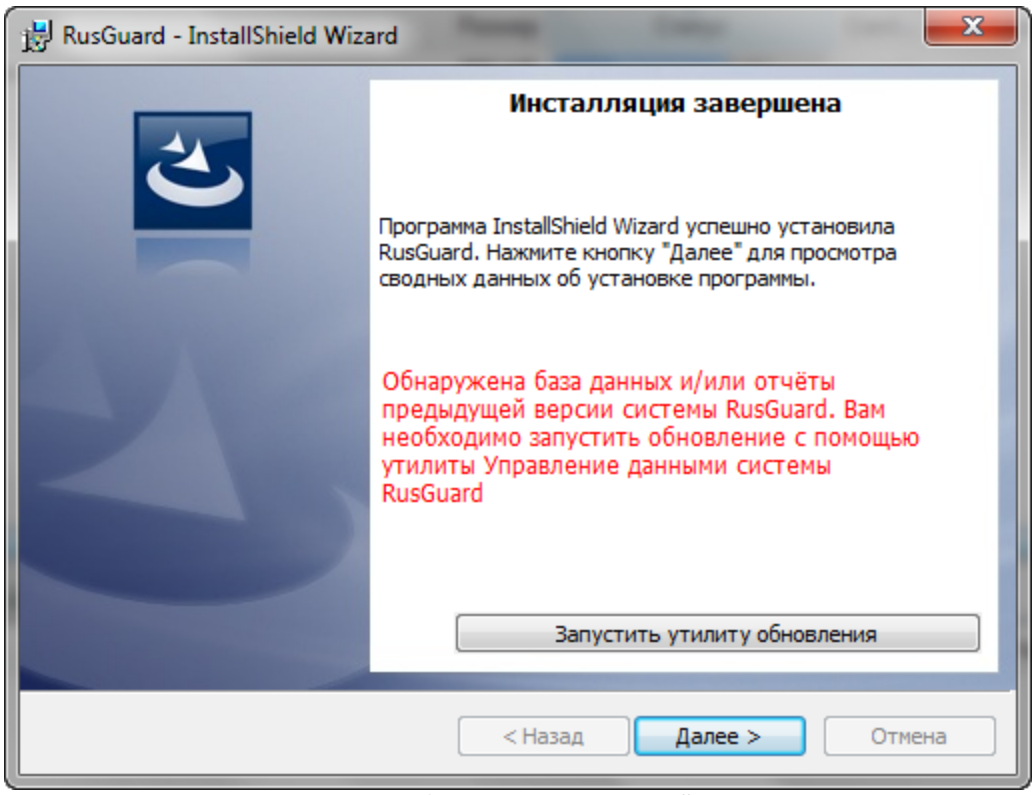


Рисунок 10 - Сообщение о конфликте версий ПО и БД

В этом случае необходимо обновить версию БД.

Для того чтобы выполнить обновление версии БД:

1. Нажмите на кнопку ***Запустить утилиту обновления***.

Запустится утилита Управление данными системы RusGuard 313 (также доступна из папки ***RusGuard*** в списке программ меню ***Пуск*** ОС Windows, либо соответствующий ярлык на рабочем столе, если он создан) (см. рис. 10). По умолчанию открыта вкладка ***Обслуживание***.

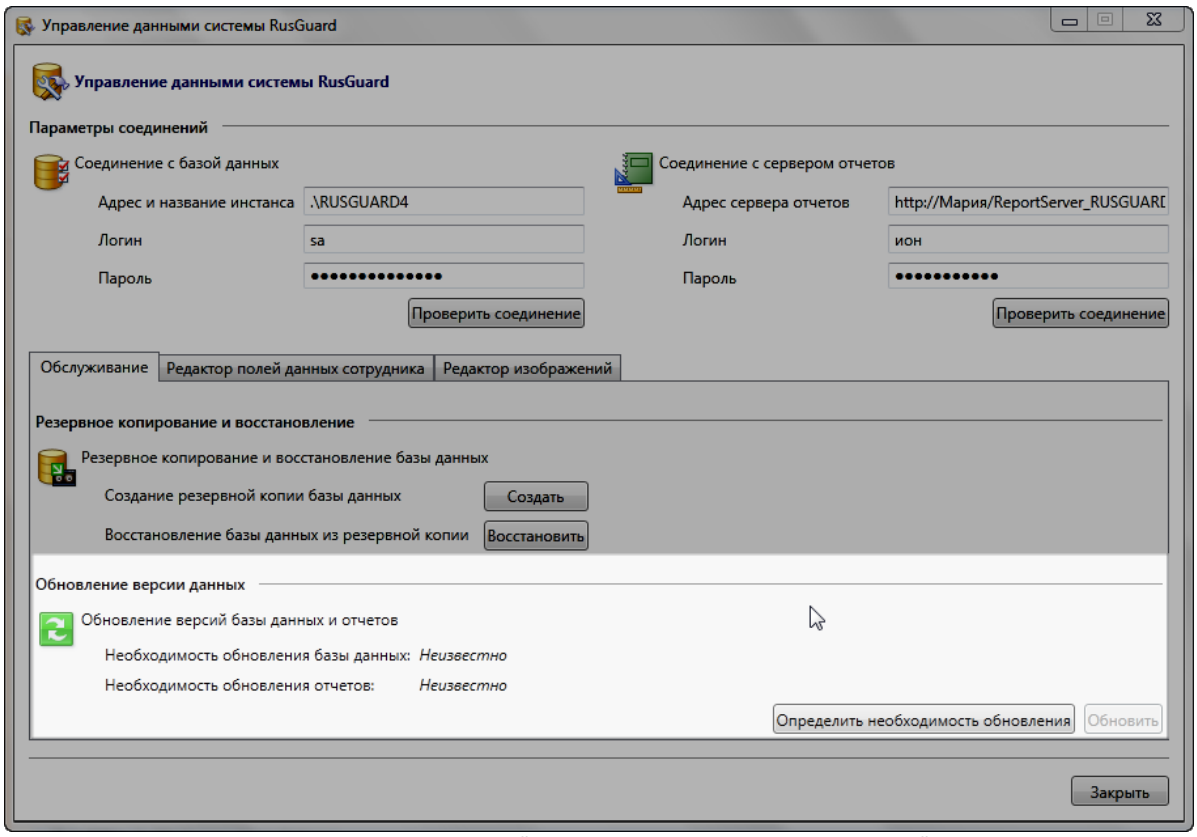


Рисунок 11 - Окно утилиты "Управление данными системы RusGuard"

Вы также можете отложить обновление и вернуться к завершению установки ПО RusGuard.

2. Чтобы определить необходимость обновления, нажмите на кнопку Определить необходимость обновления.

Система выполняет проверку и сообщает результат (см. рис. 11).

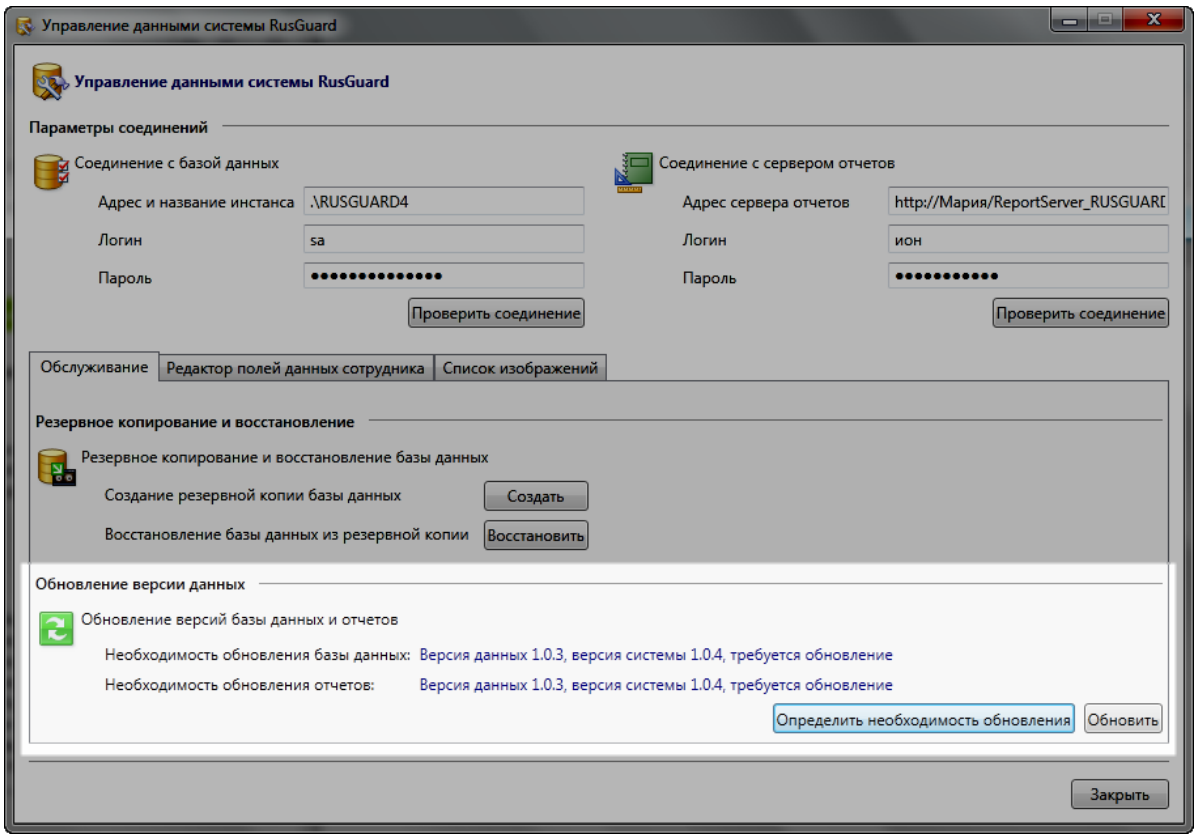


Рисунок 12 - Сообщение о конфликте версий ПО и БД

3. Если результат положительный (т.е. выявлен конфликт версий и необходимо обновление), нажмите на кнопку Обновить.

Откроется диалог с предупреждением (см. рис. 12).

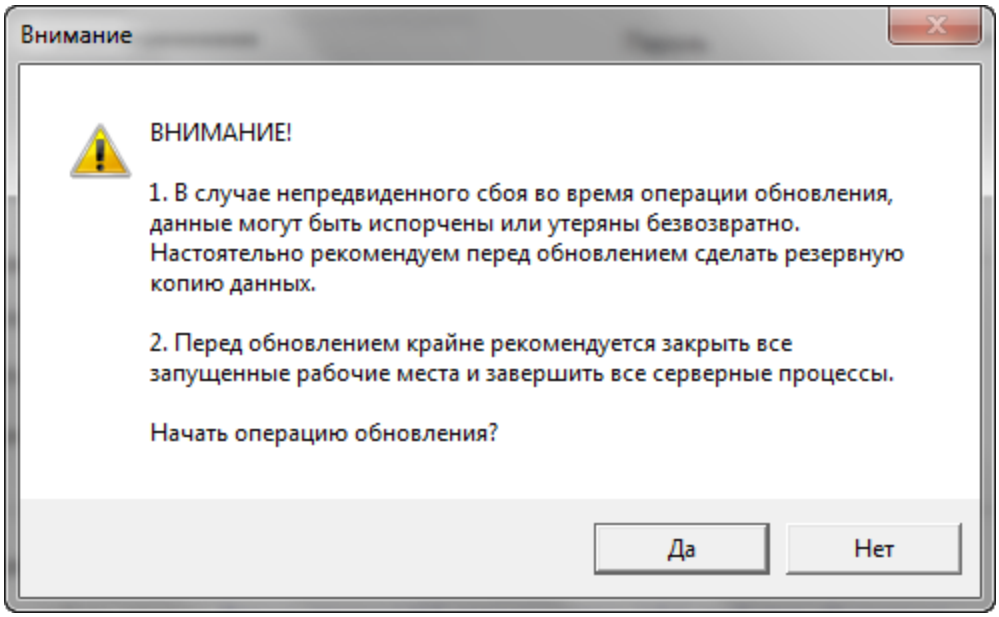


Рисунок 13 - Предупреждение о возможных ошибках

4. Чтобы выполнить обновление немедленно, нажмите на кнопку Да. Вы можете отложить обновление и вернуться к завершению установки ПО RusGuard.

Начнется процесс обновления. После его завершения вы можете вернуться к установке ПО и закончить ее.

Если процедура обновления была отложена, либо завершилась с ошибками, работа с установленным ПО невозможна.

Утилита ***RusGuard агент*** 301 в этом случае сообщает о наличии неполадок (статус ). При запуске утилиты на ее вкладках также отображается сообщение о необходимости обновить версию БД.

Обновление может быть выполнено в любой момент из утилиты ***Управление данными системы RusGuard*** 313 .

Настройка цветовой схемы

Версии ПО RusGuard от 10.0.0 позволяют настраивать цветовую схему (цветовое оформление) пользовательского интерфейса.

Для того чтобы настроить цветовую схему:

1. Запустите АРМ RusGuard.
2. Щелкните пиктограмму  в верхнем правом углу активного экрана. Раскроется меню, содержащее преднастроенные варианты цветовых схем (см. рис. 13). По умолчанию используется голубой цвет.
3. Выберите один из вариантов (установите флаг возле его названия).

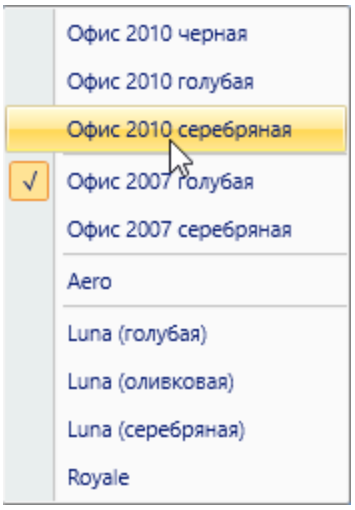


Рисунок 14 - Список доступных цветовых схем

4. Система загрузит желаемую схему.

Обращение в службу поддержки RusGuard

В случае возникновения неустранимой ошибки в работе ПО RusGuard Soft может потребоваться вмешательство службы технической поддержки.

Для того чтобы оперативно и качественно решить проблему, служба поддержки должна получить максимум информации о ней, поэтому мы просим пользователей при обращении в службу поддержки выполнять следующую процедуру:

1. Сделайте скриншот (клавиша **PRTSC**) сообщения об ошибке.

Скриншот должен включать весь экран (или ту его часть, в которой отображается ПО RusGuardSoft).

Сообщение об ошибке на скриншоте должно быть раскрыто, если в нем предусмотрена возможность просмотра подробной информации.

2. Сформируйте отчет о состоянии системы утилиты Информация о системе 337.
3. Подробно опишите в обращении ситуацию, при которой возникла ошибка.

4. Направьте обращение в службу поддержки, приложив скриншот и отчет.

Контакты службы поддержки:

Тел: 8-495-683-96-96, доб. 1

Email: Support@rgsec.ru

ICQ: 644-398-293

Skype: RusGuardSecurity_Support

Интеграции и установка стороннего ПО

Оборудование ИСО "Орион" (НВП Bolid)

Настройка интеграции в ПО "Болид"

Модуль интеграции системы контроля и управления доступом RusGuard с системой Bolid позволяет организовать единую комплексную систему безопасности на базе интегрированного ПО RusGuard Soft (см. рис. 1).

Для интеграции оборудования ИСО Орион в систему RusGuard не требуется установка ПО «Орион Про», «Орион» и другого серверного ПО «Болид».

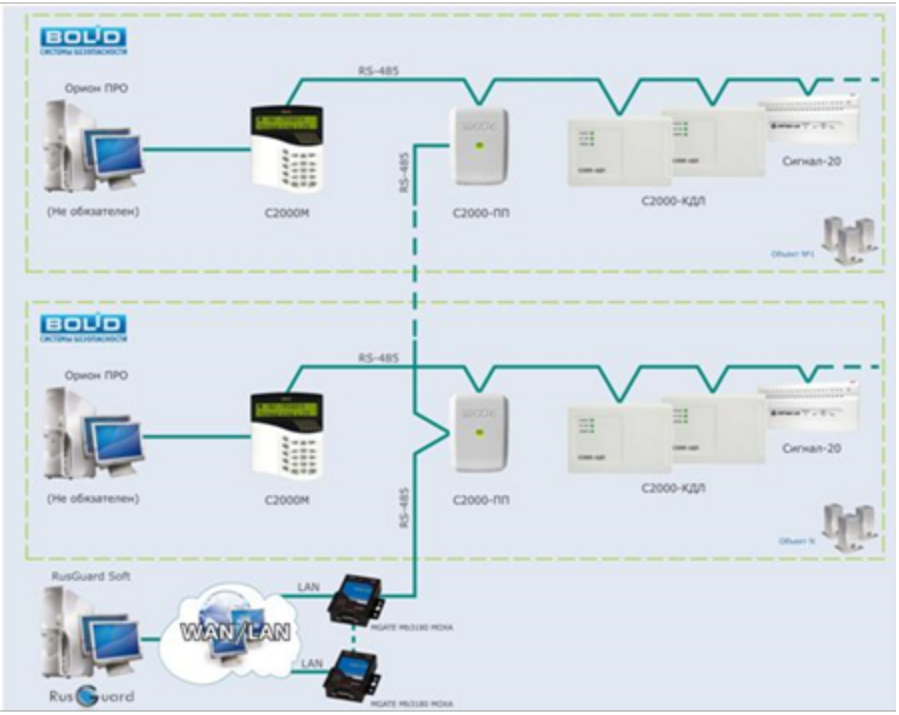


Рисунок 1 - Структурная схема интеграции

Для настройки интеграции оборудования ИСО “Орион” (НВП Болид) в ПО RusGuard Soft понадобятся две утилиты: PProg и Uprog. Утилиты предоставляются компанией "Болид" бесплатно, дистрибутивы и документацию можно скачать на сайте компании.

Настройка пульта С2000-М утилитой PProg

PProg - утилита, обеспечивающая настройку пульта С2000-М.

При интеграции с ПО RusGuard Soft настройка пульта выполняется следующим образом (пример настройки):

1. Запустите утилиту, переведите пульт в режим программирования и выполните поиск приборов на линии интерфейса RS-485.

2. Добавьте найденные приборы в дерево оборудования под пульт (см. рис. 2).

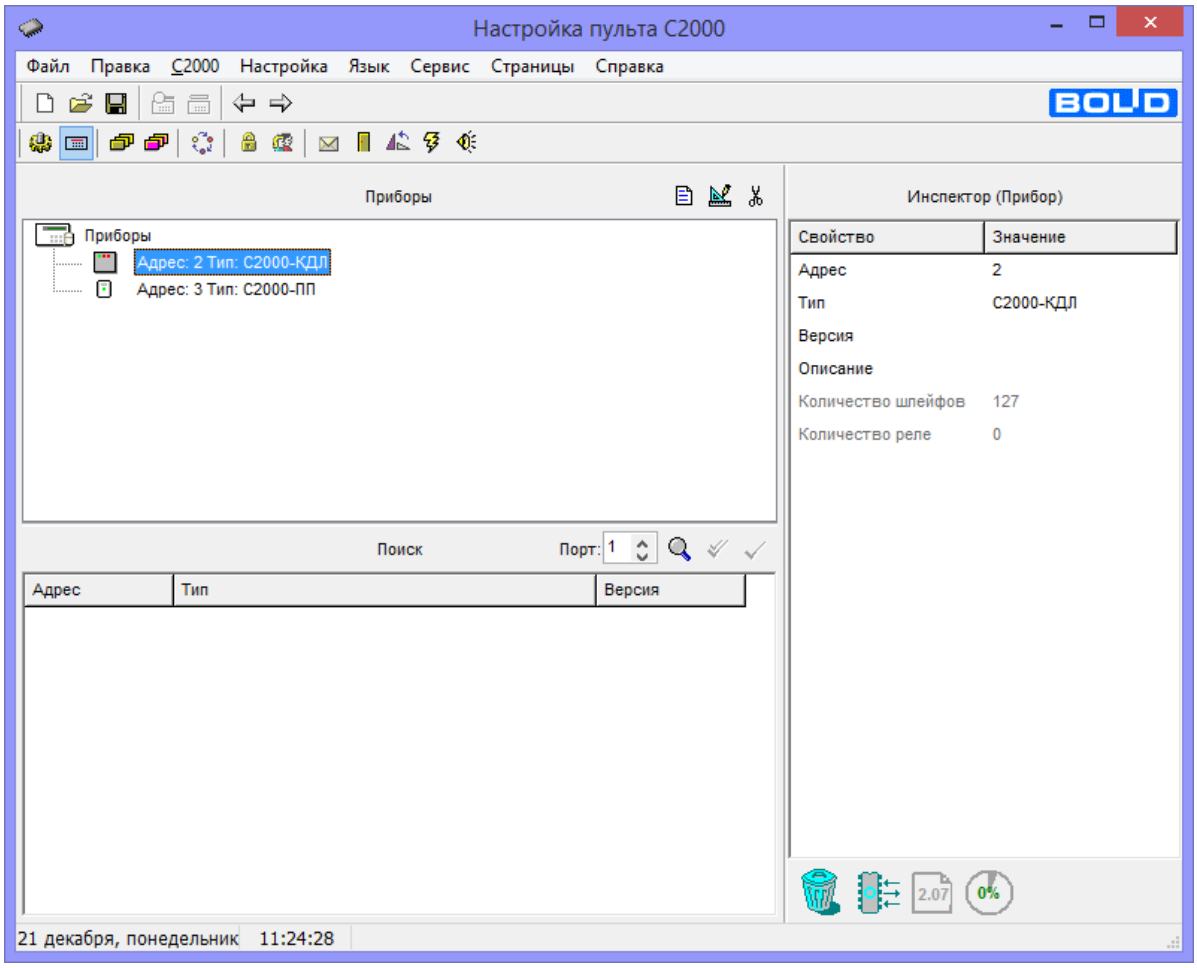


Рисунок 2 - Привязка С2000-ПП к пульту С2000

3. Создайте разделы и привяжите к ним шлейфы (см. рис. 3).

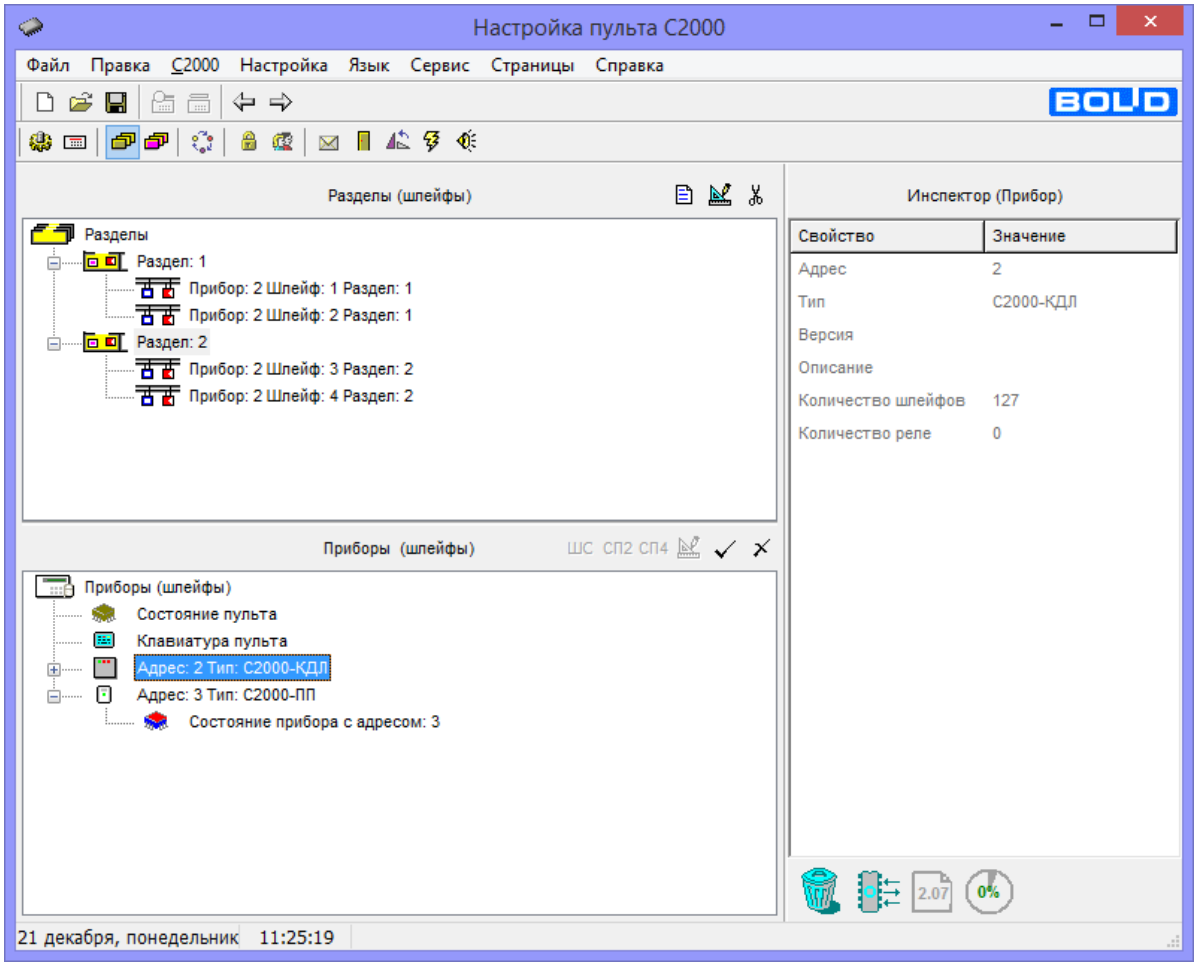


Рисунок 3 - Создание разделов

4. При необходимости создайте новый уровень доступа и пароль для быстрого управления созданными разделами (см. рис. 4 и 5).

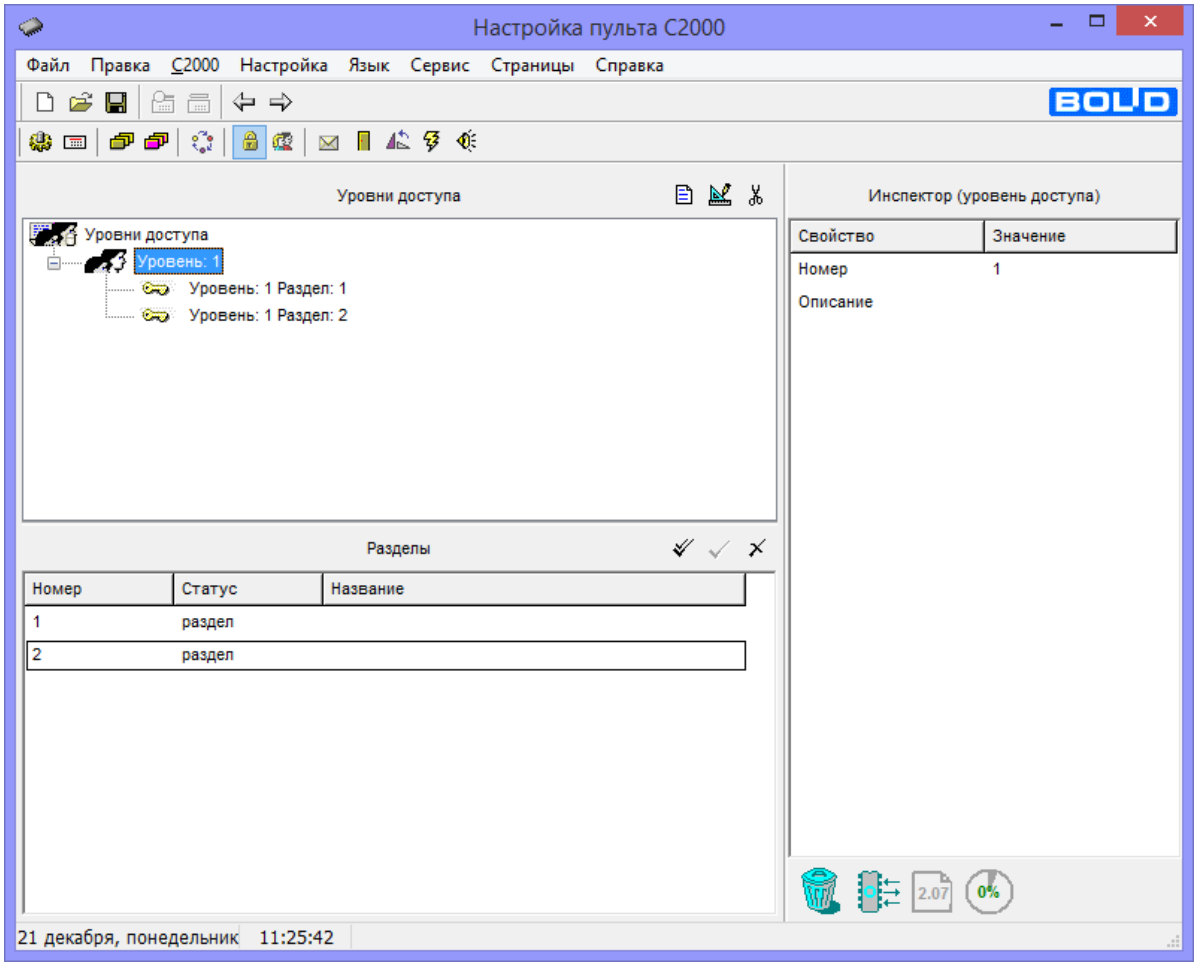


Рисунок 4 - Создание уровней доступа

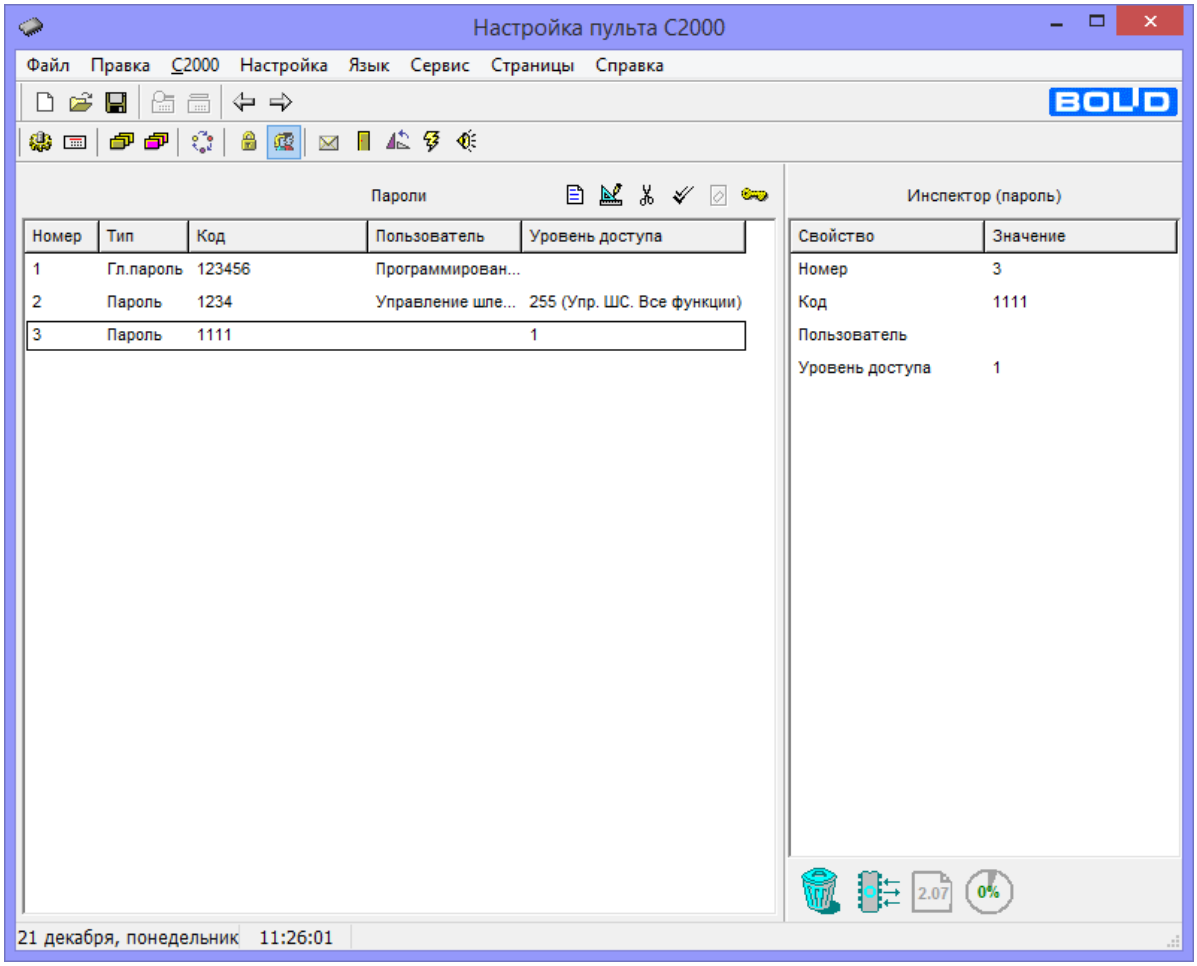


Рисунок 5 - Создание паролей доступа

5. В меню ***Трансляция событий*** добавьте С2000-ПП под пульт и отметьте события, которые требуется транслировать (см. рис. 6).

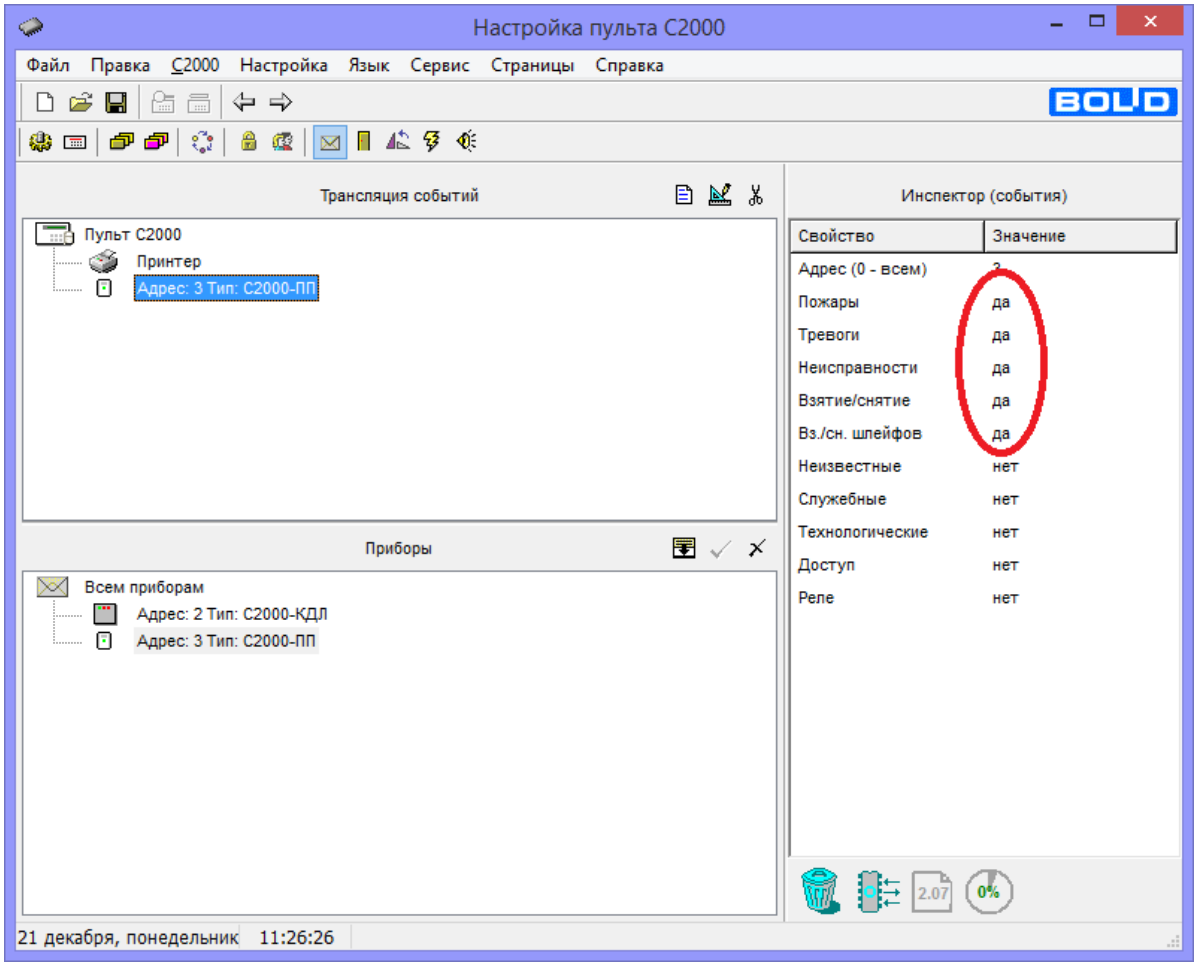


Рисунок 6 - Настройка трансляции событий

6. Привяжите управление созданных разделов к пульту (см. рис. 7).

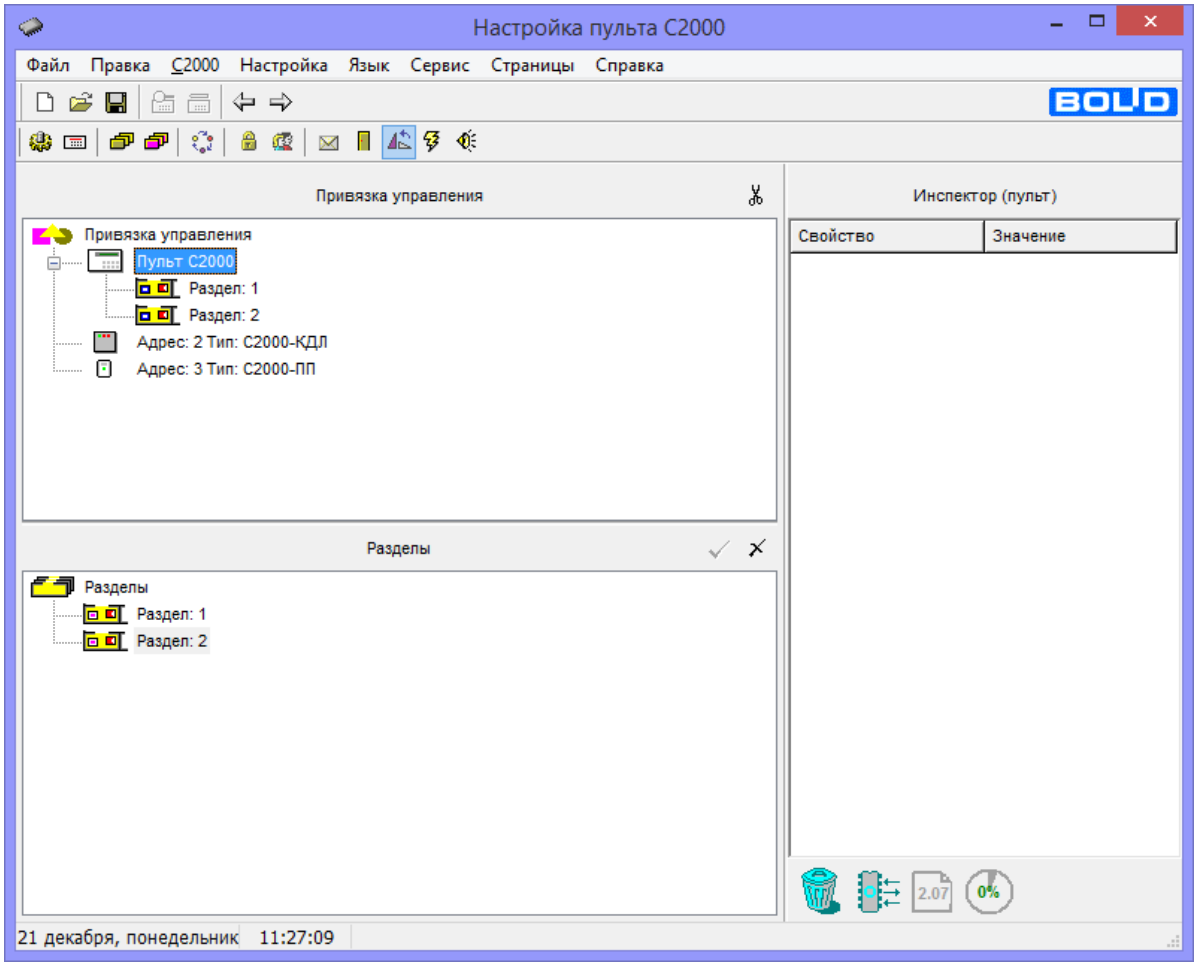
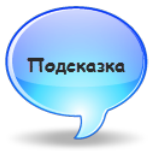


Рисунок 7 - Настройка трансляции событий

7. Сохраните созданную конфигурацию в пульт, выйдите из режима программирования



Рекомендуется выписать все адреса настраиваемых приборов, номера разделов, реле и т.д. Эти данные потребуются при настройке прибора С2000-ПП.

Настройка прибора С2000-ПП утилитой UProg

После настройки утилиты PProg, перейдите к настройке прибора С2000-ПП утилитой UProg (подробная инструкция доступна на сайте компании "Болид").

Внимание: перед настройкой прибора С2000-ПП при отключенном питании снимите все перемычки с платы прибора.

Для того чтобы настроить конфигурацию:

1. Запустите утилиту, переведите пульт в режим программирования и выполните поиск приборов на линии интерфейса RS-485.
2. Выберите прибор С2000-ПП и считайте с него конфигурацию.

3. Настройте основные параметры на вкладке ***Прибор*** (см. рис. 8).

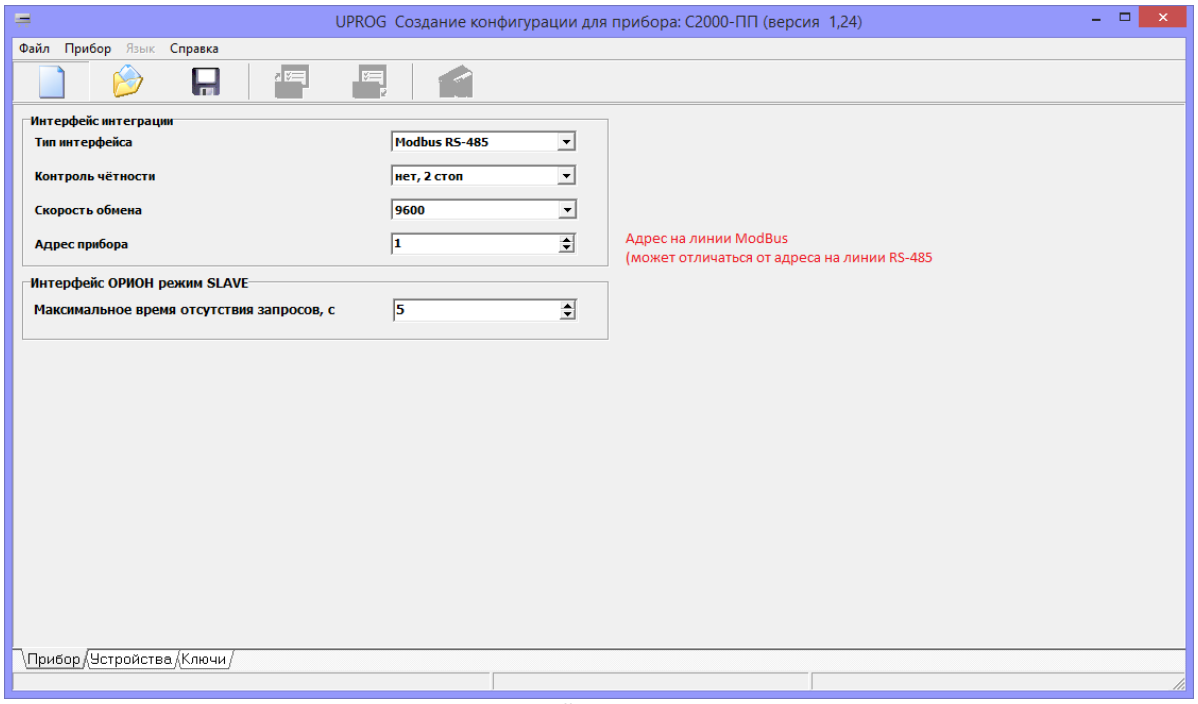


Рисунок 8 - Настройка основных параметров

4. Перейдите на вкладку ***Устройства***. Заполните конфигурационные таблички в соответствии с настройками пульта С2000. Для предотвращения путаницы при эксплуатации, рекомендуется дерево соответствия Зон и Разделов Modbus делать в полном соответствии дерева разделов в пульте С2000 (см. рис. 9).

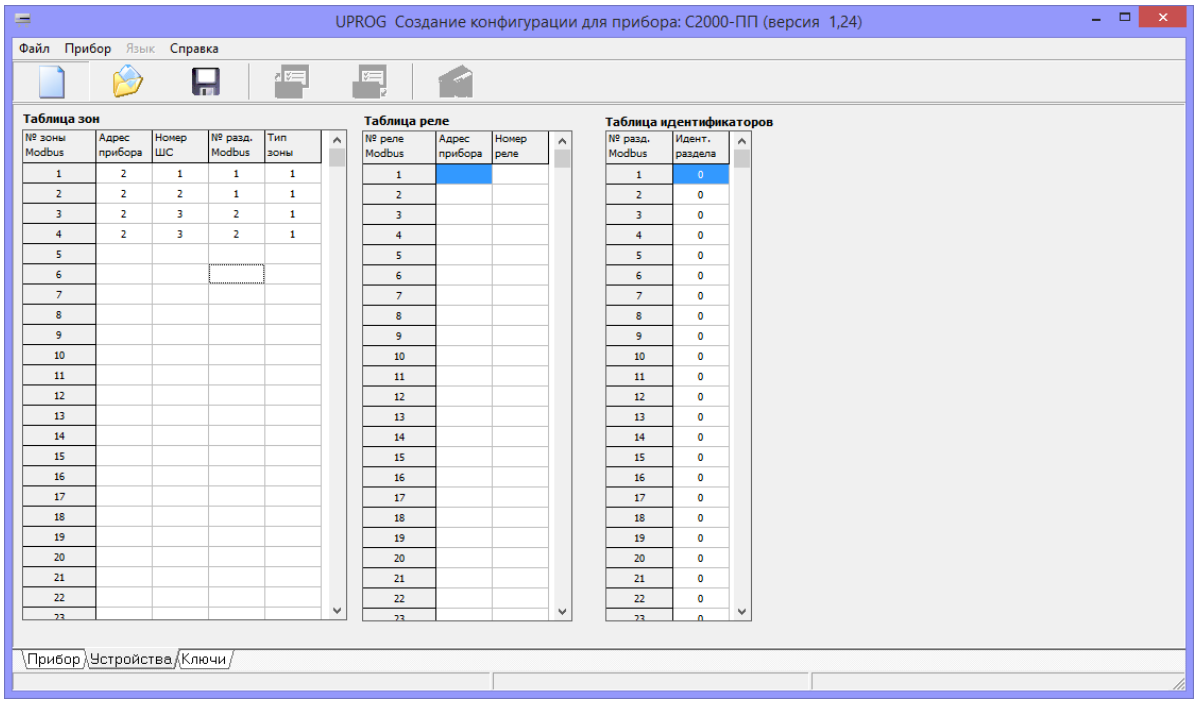


Рисунок 9 - Ввод параметров прибора

5. Сохраните конфигурацию и выйдете из режима настройки пульта.

Настройка интеграции в RusGuard Soft

ПО RusGuard Soft позволяет осуществлять интеграцию с оборудованием интегрированной системы охраны "Орион" (НВП Bolid). Пример настроенной конфигурации приведен ниже (см. рис. 10).

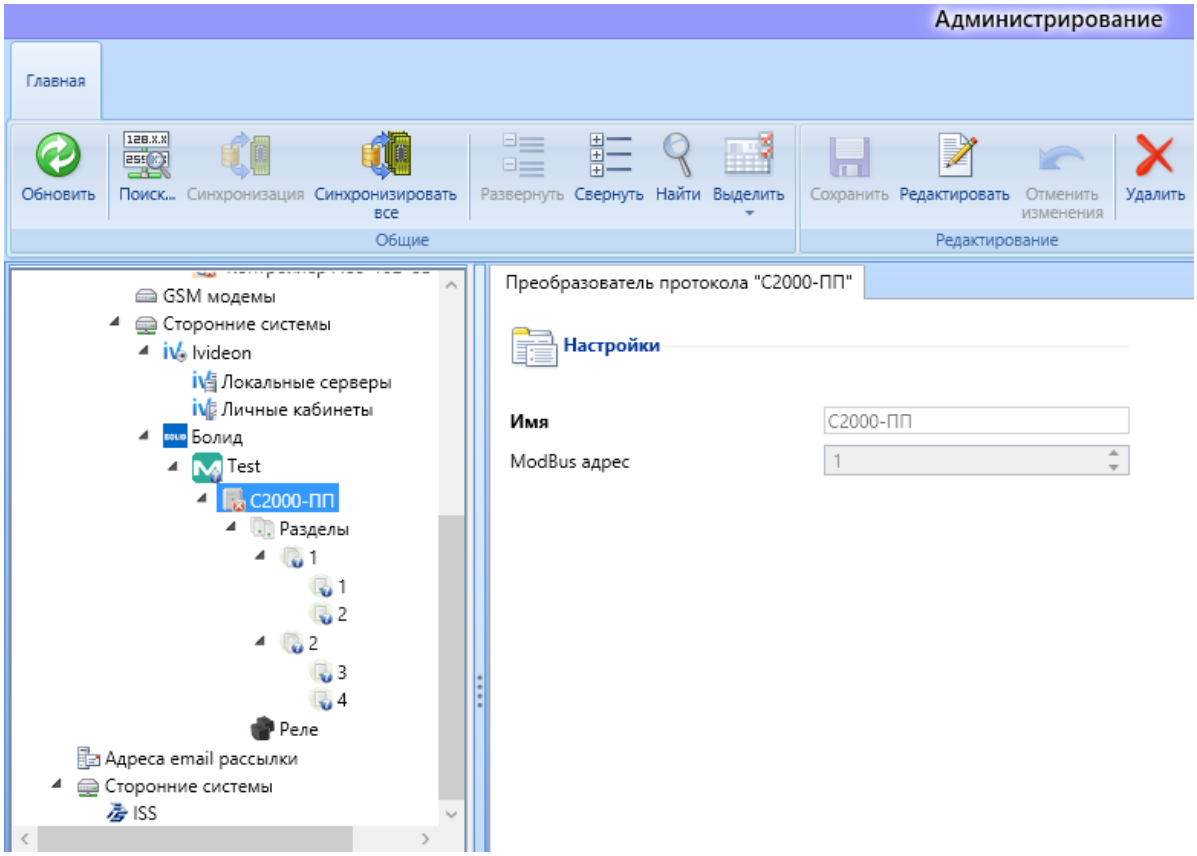


Рисунок 10 - Пример конфигурации

Внимание: перед настройкой ПО RusGuard Soft необходимо выполнить подключение и настройку шлюза Moxa Mgate 3180, см. подраздел Периферийные устройства > Подключение шлюза MOXA MGate MB3180 420.

Для того чтобы выполнить интеграцию с приборами ИСО "Орион":

1. Зайдите в модуль ***Конфигурация оборудования*** 79 АРМ.
2. В левой навигационной панели раскройте список ***Сторонние системы***, выберите пункт ***Болид***. Установите на нем курсор.
3. В панели управления перейдите к пункту ***Сторонние системы***. Выберите пункт ***Болид***.

Раскроется следующий уровень меню, где перечислены элементы ИСО "Орион", интегрируемые с ПО RusGuard для сбора корректного данных.

4. Выберите верхний пункт меню (см. рис. 11) ***Добавить преобразователь Modbus-RTU в Modbus/TCP*** (этот пункт единственный активный при начале конфигурации).

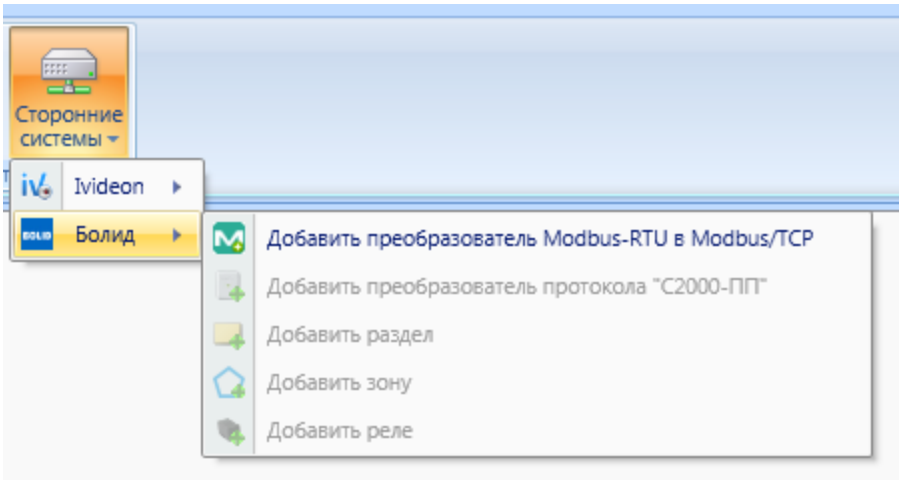


Рисунок 11 - Начало конфигурации ИСО "Орион"

Система загрузит окно выбора сервера оборудования (см. рис. 12).

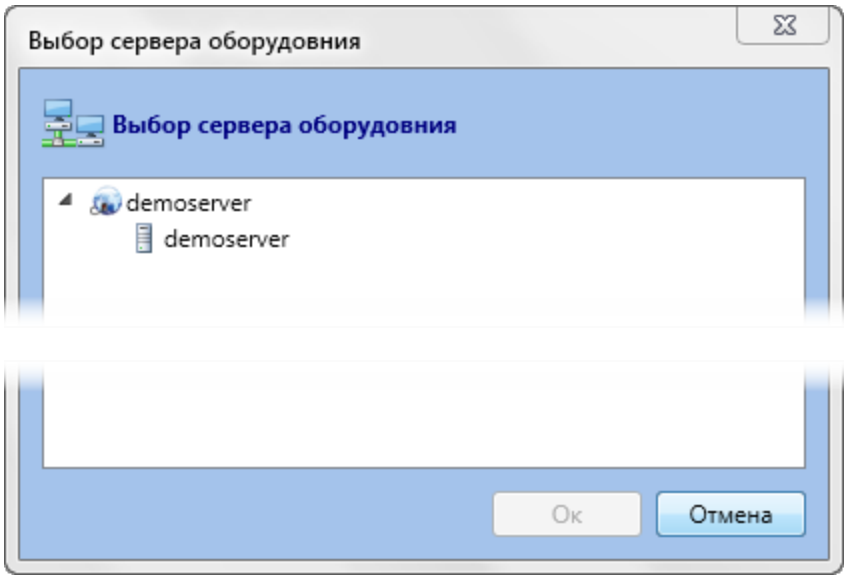


Рисунок 12 - Ввод сервера оборудования, где предстоит выполнить интеграцию

5. Выберите нужный сервер.

Откроется окно ***Добавить преобразователь Modbus-RTU в Modbus/TCP***.

6. Введите параметры преобразователя (см. рис. 13). Нажмите на кнопку Добавить. Кнопка становится активна только после ввода всех параметров.

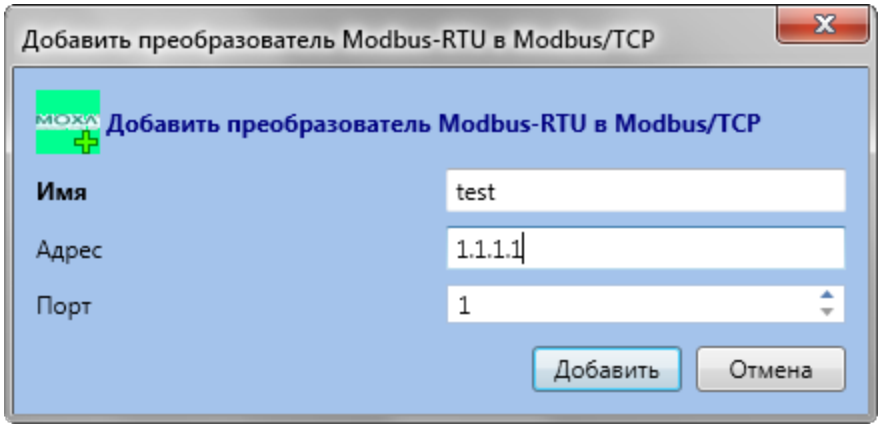


Рисунок 13 - Ввод параметров преобразователя Modbus RTU в Modbust TCP

Система выполнит сохранение устройства. Название созданного в системе преобразователя Modbus отобразится в иерархическом списке навигационной панели слева.

После того, как преобразователь Modbus подключен к системе под управлением ПО RusGuard, активируется следующий пункт меню конфигурации ИСО "Орион" в панели управления: ***Добавить преобразователь протокола "С2000-ПП"***. Пункт меню активен, когда курсор установлен на строке преобразователя Modbus в навигационной панели слева.

7. Оставаясь в стоке сконфигурированного преобразователя Modbus, выберите в панели управления ***Сторонние системы*** > ***Болид*** > ***Добавить преобразователь протокола "С2000-ПП"***.

Откроется окно ввода параметров преобразователя протокола (см. рис. 14).

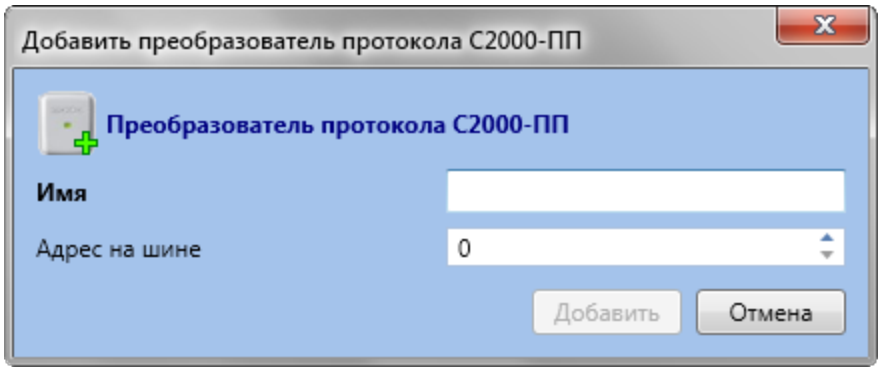
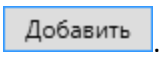


Рисунок 14 - Ввод параметров преобразователя протокола "С2000-ПП"

8. Введите параметры преобразователя протокола, нажмите на кнопку 

.

Система сохранит параметры преобразователя, соответствующая пиктограмма с именем преобразователя появится в навигационной панели слева. Кроме того, уровнем ниже преобразователя появятся пункты ***Разделы*** и ***Реле***. Соответственно, в каждом из них пользователь сможет создать так называемый "раздел" или выполнить конфигурацию реле (при переходе в каждый из подразделов в подменю ***Сторонние системы*** > ***Болид*** активируются соответствующие подпункты: ***Добавить раздел*** и ***Добавить реле***).

Разделы и реле могут наноситься на планы в виде маркеров. Оператор АРМ может осуществлять управление ими в модуле ***Планы*** 239 (или в модуле ***Конфигурация***

оборудования, если это необходимо). Разделы, в свою очередь, состоят из так называемых "зон", которые также могут отображаться на планах. При настройке "зоны" (см. ниже) задается тип датчика, которому она соответствует. Разделу также присваивается тип датчика, но он выбирается исходя из удобства визуализации раздела на плане.

Всего в системе может быть создано 64 раздела, 512 зон и 255 реле.

Примечание: Параметры (имя, номер, и т.д.) разделов и реле внутри одного преобразователя не могут совпадать. Если разделы и реле относятся к разным преобразователям, они могут иметь одинаковые параметры.

9. Чтобы создать раздел, перейдите в список ***Разделы*** левой навигационной панели. В панели инструментов сверху выберите ***Сторонние системы*** > ***Болид*** > ***Добавить раздел.***

Откроется окно ввода данных о разделе (см. рис. 15).

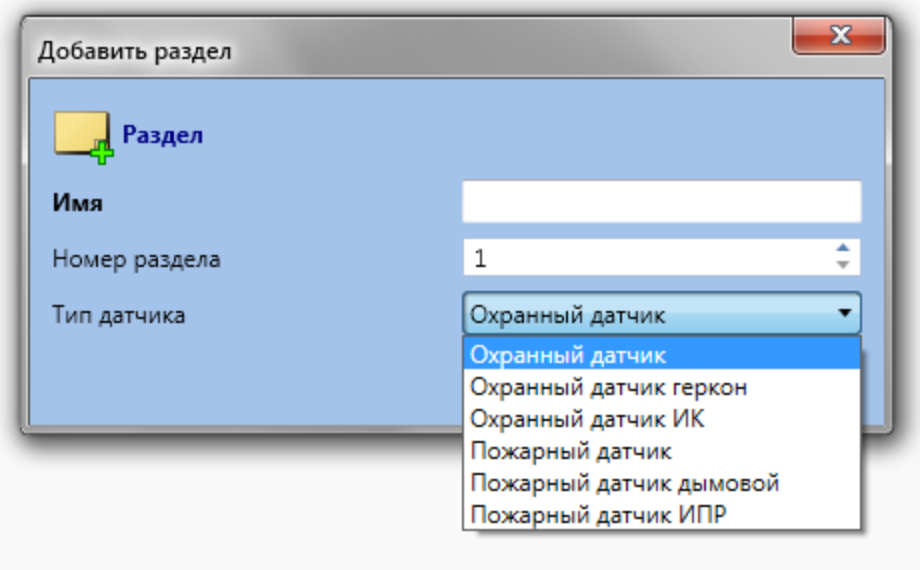


Рисунок 15 - Ввод параметров раздела

10. Введите параметры раздела: имя, номер и тип датчика (выбирается из списка). После ввода всех необходимых параметров нажмите на кнопку.

Созданный раздел отобразится в иерархическом списке. Зайдя в него, вы можете:

- создать внутри раздела "зоны" (активируется подпункт меню ***Сторонние системы*** > ***Болид*** > ***Добавить зону***;
- редактировать настройки раздела (вкладка ***Раздел***, область ***Настройки***);
- управлять разделом (вкладка ***Сервисные функции***) (см. рис. 16).

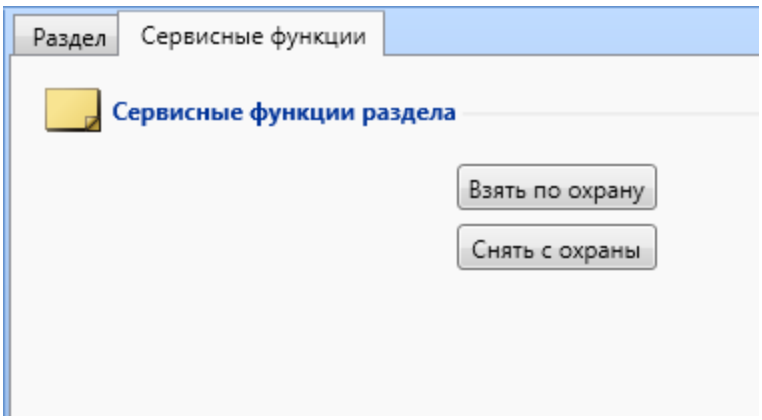


Рисунок 16 - Раздел. Вкладка "Сервисные функции"

11. Чтобы добавить зону внутри раздела, зайдите в нужный раздел через навигационную панель слева и выберите в панели управления сверху ***Сторонние системы*** > ***Болид*** > ***Добавить зону.***

Откроется окно ввода параметров зоны (см. рис. 17).

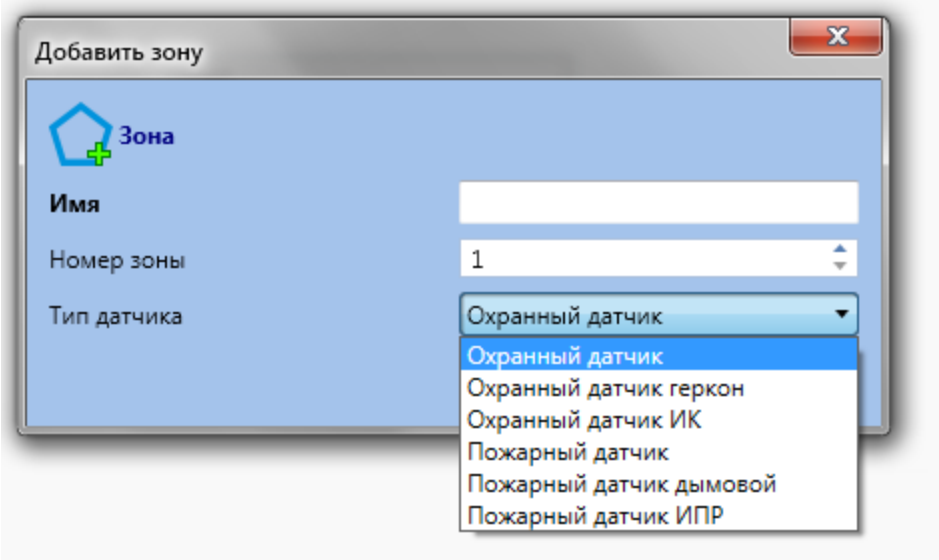
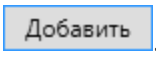


Рисунок 17 - Ввод параметров зоны

12. Заполните форму и нажмите на кнопку 

.

Название созданной зоны отобразится в иерархическом списке навигационной панели слева. В дальнейшем вы можете:

- редактировать параметры зоны (вкладка ***Зона***, область ***Настройки***);
- управлять зоной (вкладка ***Сервисные функции***) (см. рис. 18).

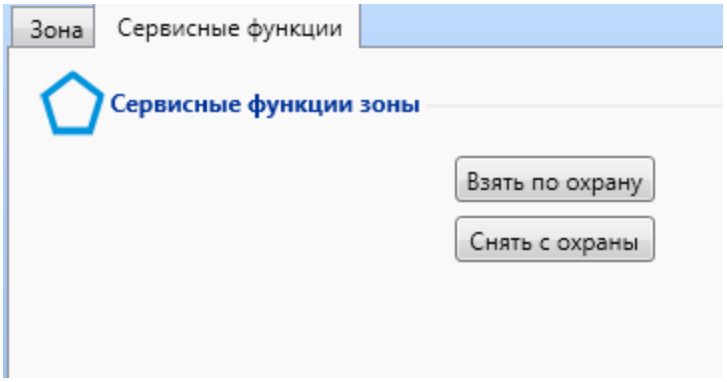


Рисунок 18 - Зона. Вкладка "Сервинсые функции"

13. Чтобы создать реле, перейдите в список ***Реле*** левой навигационной панели. В панели инструментов сверху выберите ***Сторонние системы*** > ***Болид*** > ***Добавить реле.***

Откроется окно ввода данных о реле (см. рис. 19).

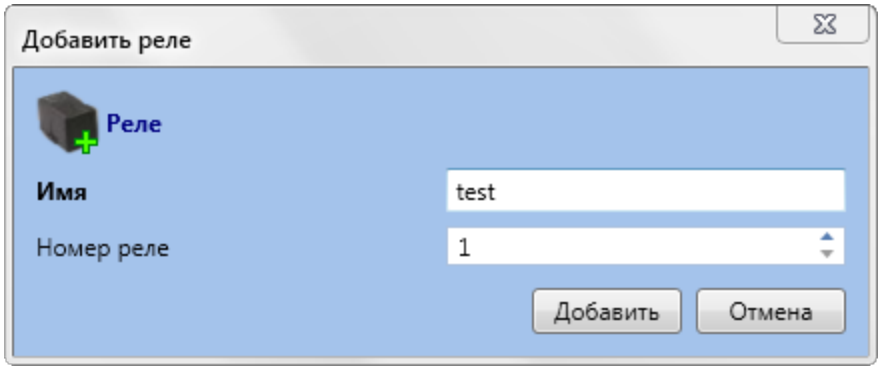
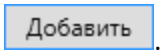


Рисунок 19 - Ввод параметров реле

14. Заполните форму, нажмите на кнопку 

.

Созданное реле отобразится в иерархическом списке. В дальнейшем вы можете:

- редактировать параметры реле (вкладка ***Реле***, область ***Настройки***);
- управлять реле (вкладка ***Сервисные функции***) (см. рис. 20).

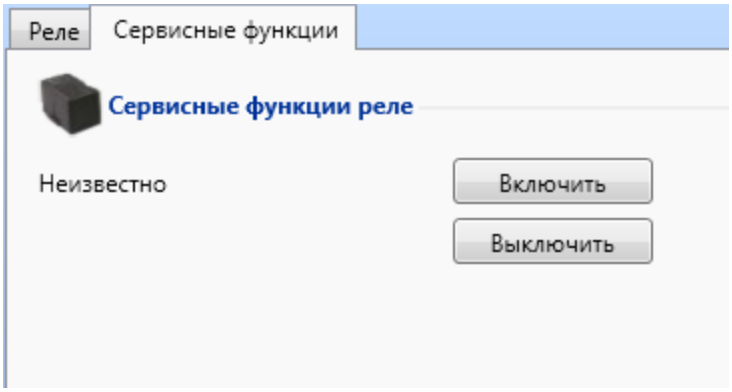


Рисунок 20 - Реле. Вкладка "Сервинсые функции"

Работа с элементами ИСО "Орион" через ПО RusGuard

Интегрированные элементы (устройства) ИСО "Орион" могут наноситься на планы 160 через модуль ***Конфигурация рабочих мест*** 155 АРМ. После этого оператор АРМ, использующий модуль ***Планы***, может выполнять управление ими.

Аналогичные функции управления элементами ИСО "Орион" доступны в модуле ***Конфигурация оборудования*** 79, на вкладке ***Сервисные функции*** каждого устройства.

Ivideon Video

Видеоподсистема Ivideon позволяет:

- создавать как локальные, так и распределенные системы видеонаблюдения на базе облачных сервисов Ivideon;
- интегрировать в систему любые IP камеры, Web-камеры и некоторые модели видеорегистраторов через локальные видеосерверы (ПО Ivideon Server);
- интегрировать в систему IP-камеры с предустановленным сервисом Ivideon, подключая их напрямую в сеть Интернет;
- организовывать локальные архивы с разными режимами записи (напр., Всегда, По расписанию, По детектору движения, По детектору звука);
- организовывать независимые удаленные архивы в облаке;
- организовывать в облаке дублирующие локальные архивы;
- пользоваться средствами локального просмотра и поиска по локальному архиву через ПО Ivideon Client;
- используя учетную запись личного кабинета удаленно (с любых устройств: ПК, ноутбуков, смартфонов iOS, mac, Android), просматривать видео с интегрированных в систему камер, просматривать архивы, как локальные, хранящиеся на удаленном ПК, так и облачные.

Примечание: Для более подробного ознакомления с функциями системы Ivideon и ее техническими характеристиками, а также для создания личного кабинета перейдите на сайт http://ru.ivideon.com.

Интеграция системы Ivideon в ПО RusGuard обеспечивает:

- создание полноценной системы видеонаблюдения в ПО RusGuard Soft;
- интеграцию локальных видеосерверов в RusGuard Soft (IP-, Web-камеры, видеорегистраторы, контролируемые локальными серверами Ivideon);
- интеграцию в RusGuard Soft всех устройств, привязанных к личным кабинетам Ivideon (устройства, подключенные через локальные серверы, а также IP-камеры, выведенные напрямую в облачные сервисы);
- возможность просмотра онлайн-видео с интегрированных устройств в модулях Фотоидентификация и Планы.

Примечание: Локальные видеосерверы интегрируются напрямую. Для интеграции личного кабинета Ivideon необходимо сначала завести его на сайте http://ru.ivideon.com.

Установка серверной части ПО Ivideon

Дистрибутив серверной части ПО Indiveon входит в комплект поставки ПО RusGuard. Установочные файлы находятся в папке Redistributables.

Для того чтобы выполнить установку серверной части:

1. Зайдите в дистрибутив RusGuard Soft, запустите файл `IvideonServer_3.4.0_win32_setup.exe` (`\Redistributables\Ivideon Video`).

2. Выполните пошаговую установку (рекомендуется использовать установки мастера по умолчанию).
3. После завершения процесса установки пользователю предлагается создать новую учетную запись Ivideon или ввести данные существующей (см. рис. 21).

Если вы планируете использовать функции личного кабинета и облачные сервисы, создайте учетную запись на этом этапе.

Если же необходимы только локальные функции, выберите пункт ***Я самостоятельно настрою регистрацию в системе Ivideon позже***.

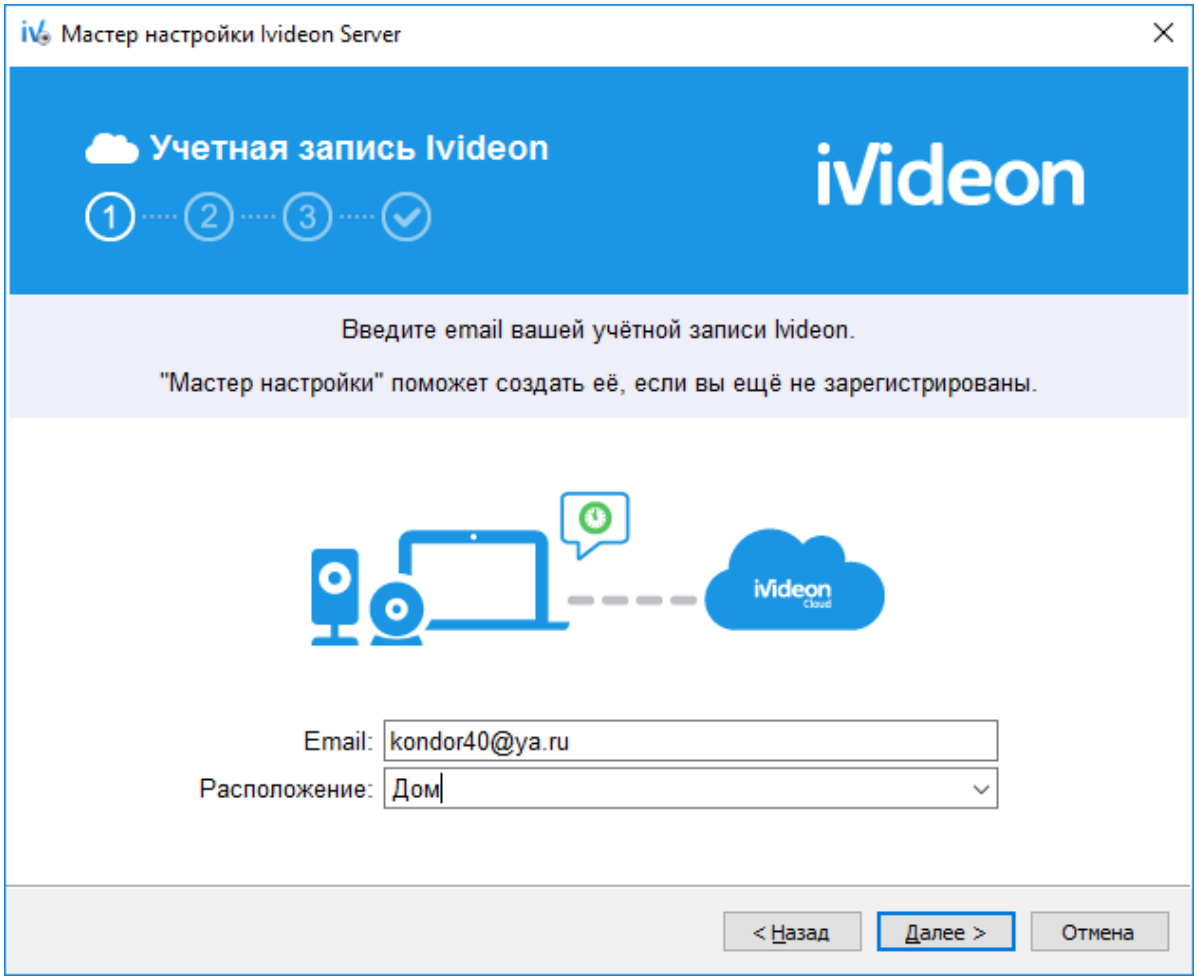


Рисунок 21 - Регистрация в системе Ivideon

4. Чтобы создать учетную запись Ivideon, в следующем окне введите действительный адрес электронной почты, пароль и название сервера.

Если данные введены корректно, пользователю предлагается подключить камеры (см. рис. 22).

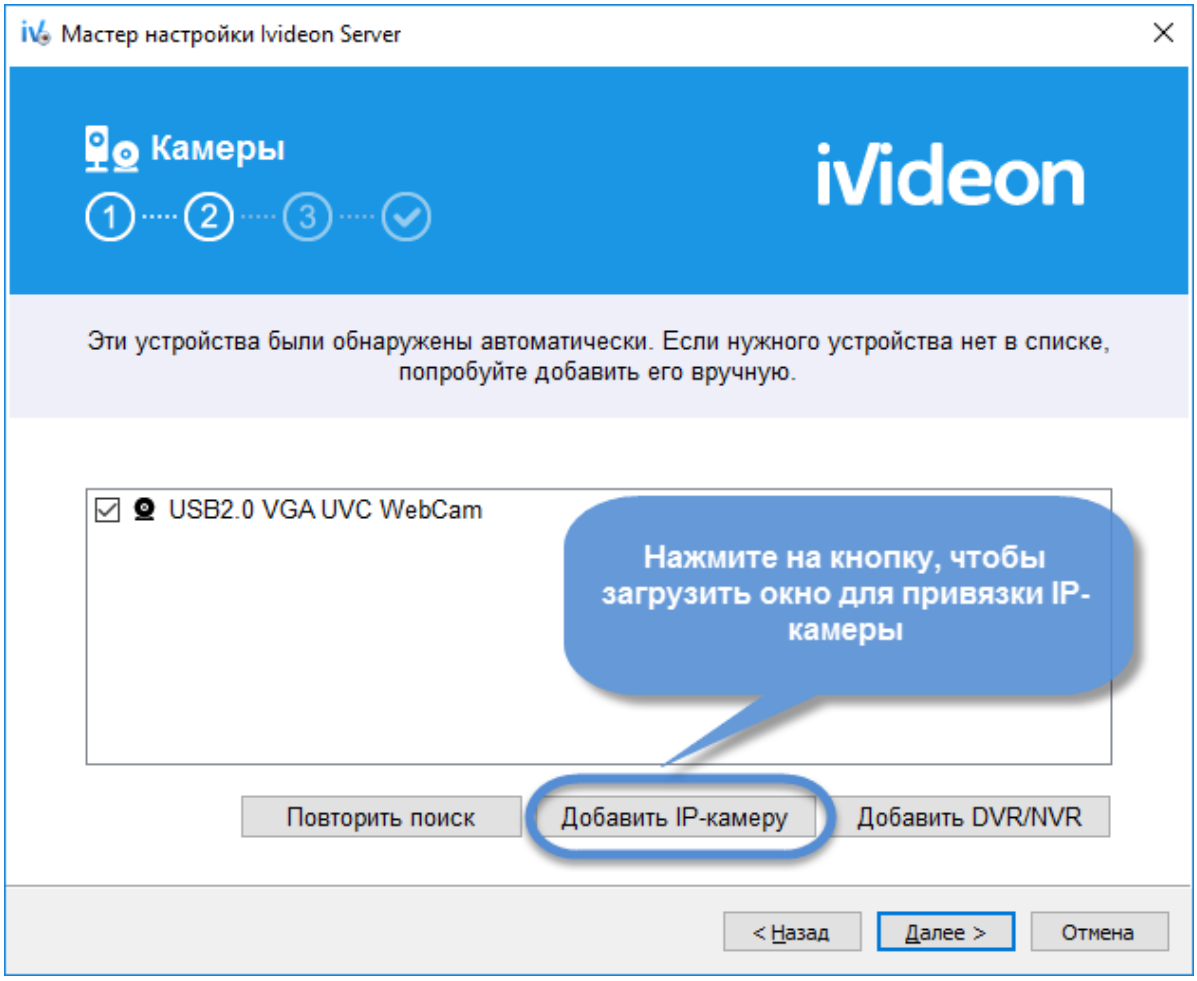


Рисунок 22 - Подключение камер к системе Ivideon

Обнаружение web-камер выполняется автоматически, для поиска IP-камер необходимо ввести параметры камер, соответствующие IP-адреса, учетные данные пользователя (см. рис. 23).

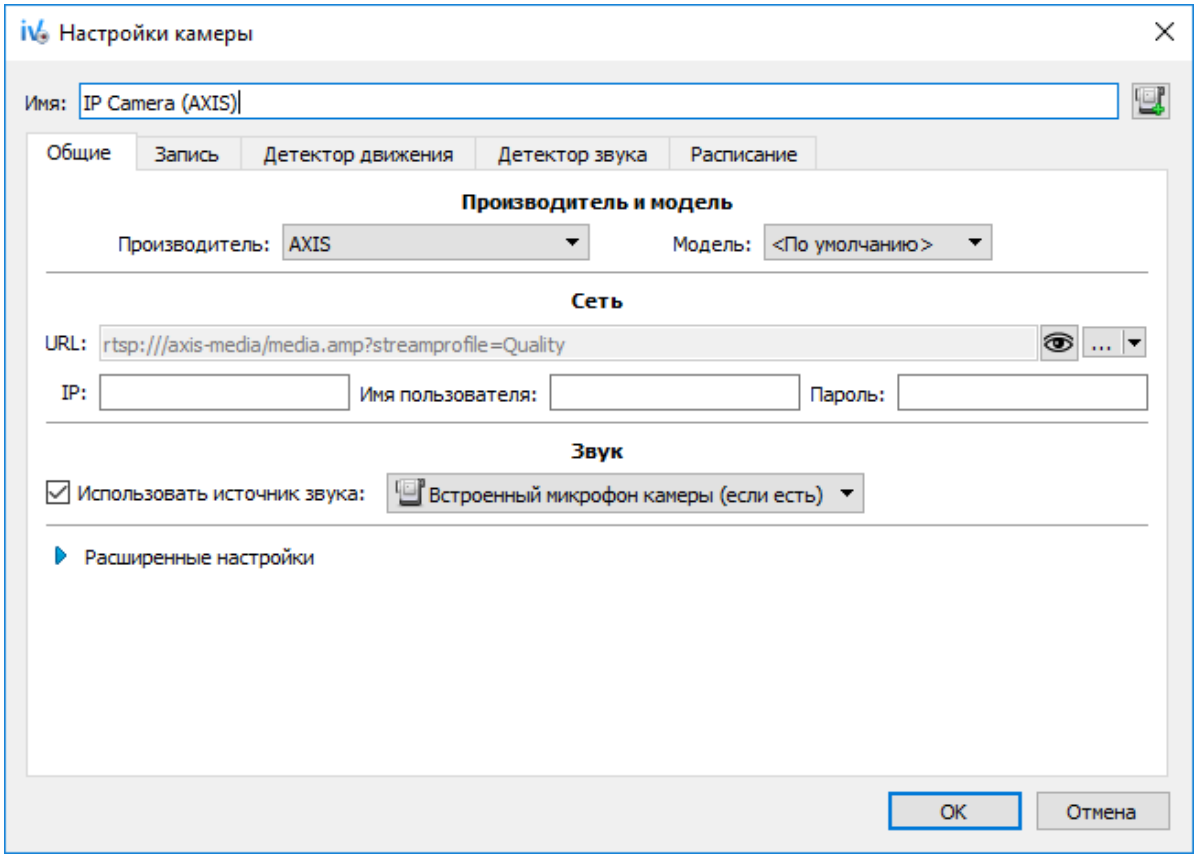


Рисунок 23 - Настройка IP-камеры в системе Ivideon

5. На следующем этапе настраиваются параметры видеоархива. По умолчанию используется та же папка, в которой установлена сама программа. Размер архива по умолчанию - 5Гб.
6. После настройки видеоархива вводятся параметры запуска сервера Ivideon (см. рис. 24).

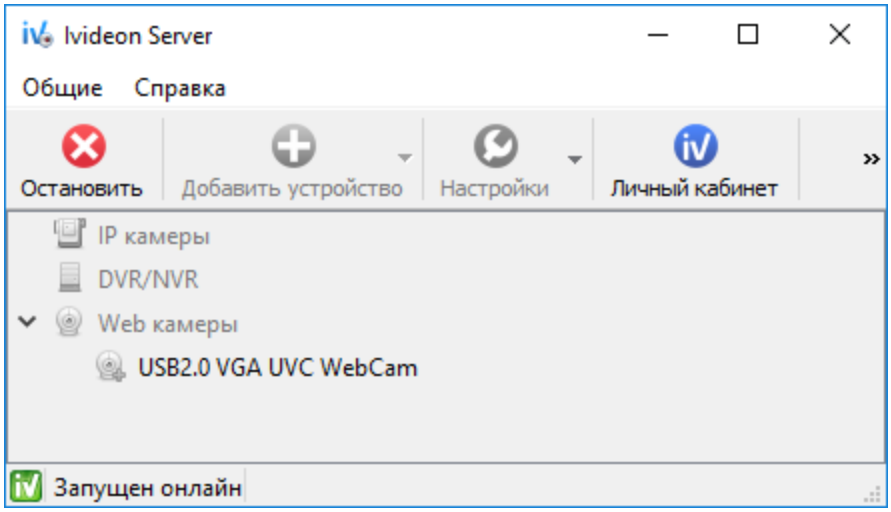


Рисунок 24 - Сервер Ivideon запущен локально. Обратите внимание, настойки не доступны, когда сервер включен

Внимание: Чтобы камеры, настроенные через сервер Ivideon были доступны для интеграции с ПО RusGuard, необходимо активировать и настроить режим "локальный просмотр". Кроме того, сервер Ivideon должен быть включен.

Для того чтобы подключить локальный доступ:

1. Откройте приложение Ivideon Server.
2. Не запуская сервер, перейдите в меню ***Настройки*** **>** вкладка ***Локальный просмотр*** (см. рис. 25).

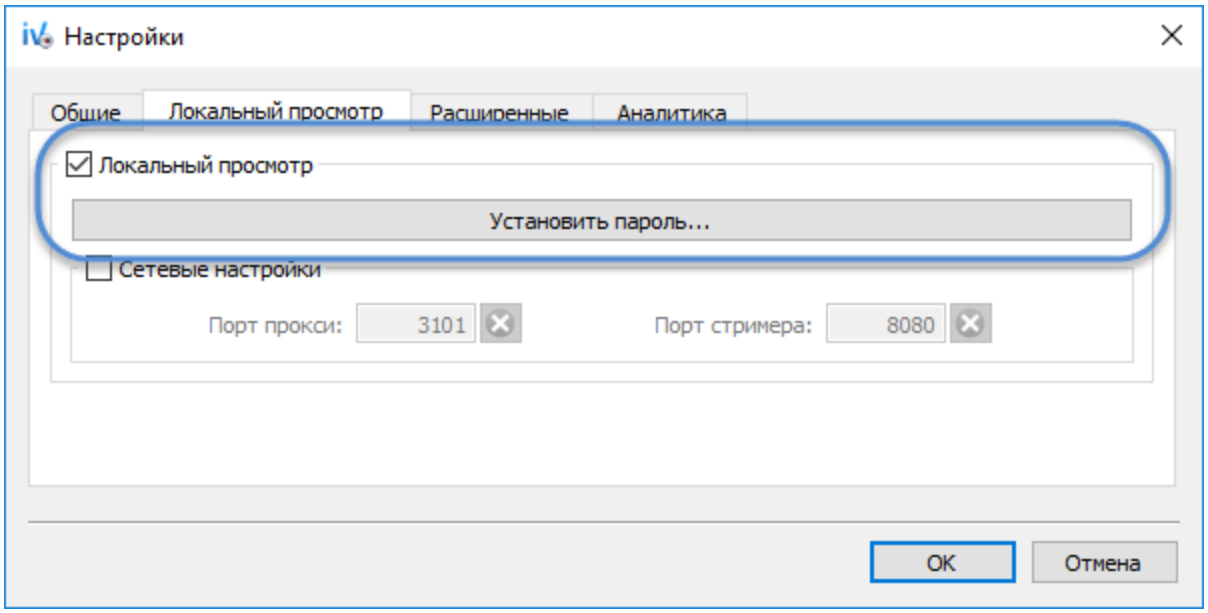
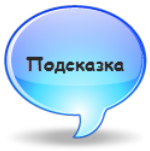


Рисунок 25 - Сервер Ivideon. Настройки. Установка режима локального просмотра

3. Установите флаг ***Локальный просмотр*** (по умолчанию флаг не активен, локальный доступ к серверу невозможен).
4. Задайте пароль доступа к серверу.
5. Сохраните настройки.



Чтобы сервер Ivideon всегда был включен, вы можете установить флаг Запускать Ivideon Server при старте ОС на вкладке ***Общие*** меню ***Настройки*** сервера (см. рис. 26). Также вы можете подключить этот режим работы в процессе установки.

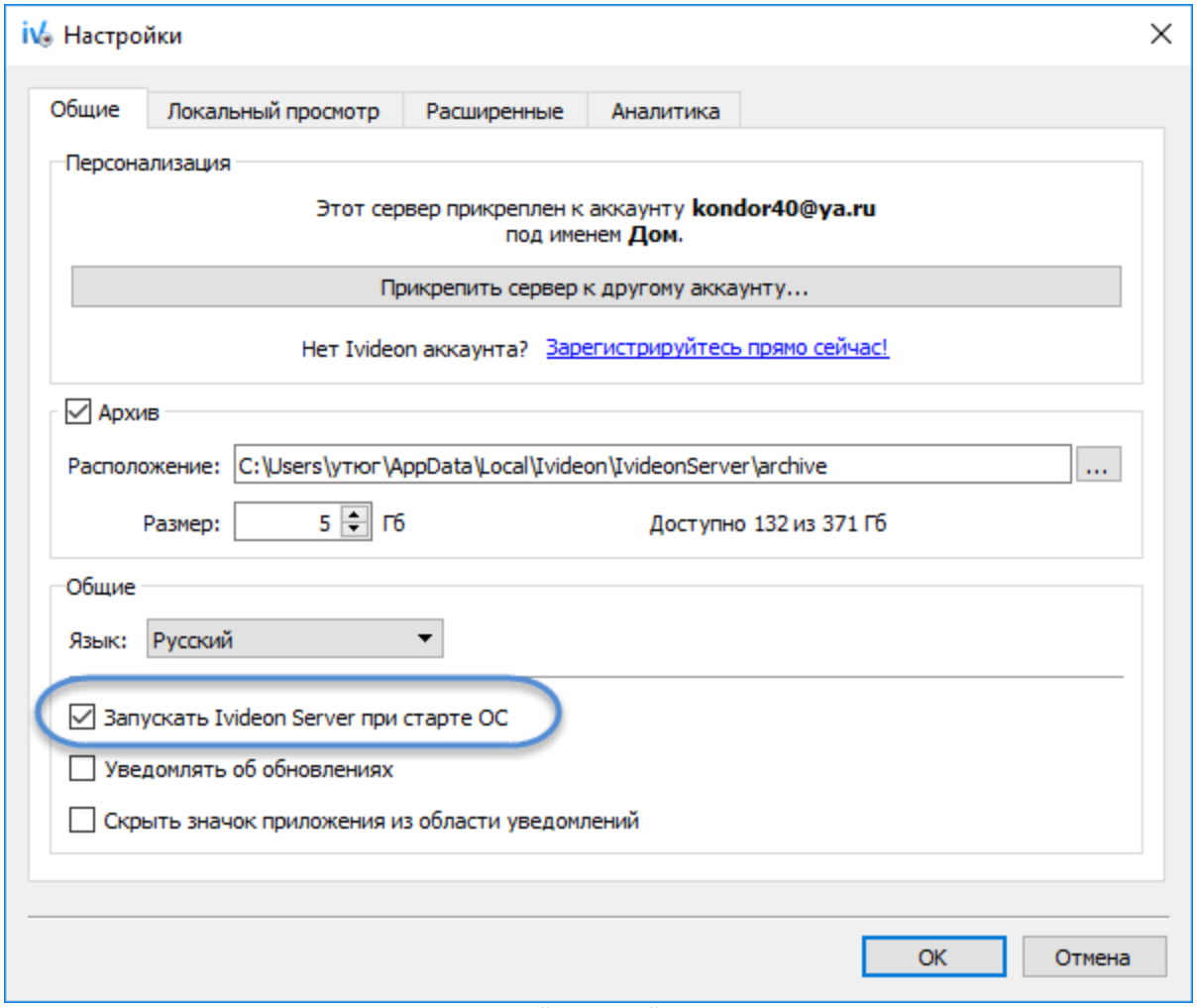


Рисунок 26 - Сервер Ivideon. Настройки. Настройка запуска приложения вместе с ОС

Установка клиента Ivideon

Для того чтобы выполнить установку клиента:

1. Зайдите в дистрибутив RusGuard Soft, запустите файл `IvideonClient_5.6.0_win32_setup.exe` (`\Redistributables\Ivideon Video`).
2. Выполните пошаговую установку (рекомендуется использовать установки мастера по умолчанию).
3. После завершения процесса установки пользователю предлагается зайти в систему, используя учетные данные системы Ivideon (см. рис. 27).

Используются либо учетные данные личного кабинета, либо IP-адрес/имя локального сервера[382] и соответствующий пароль.

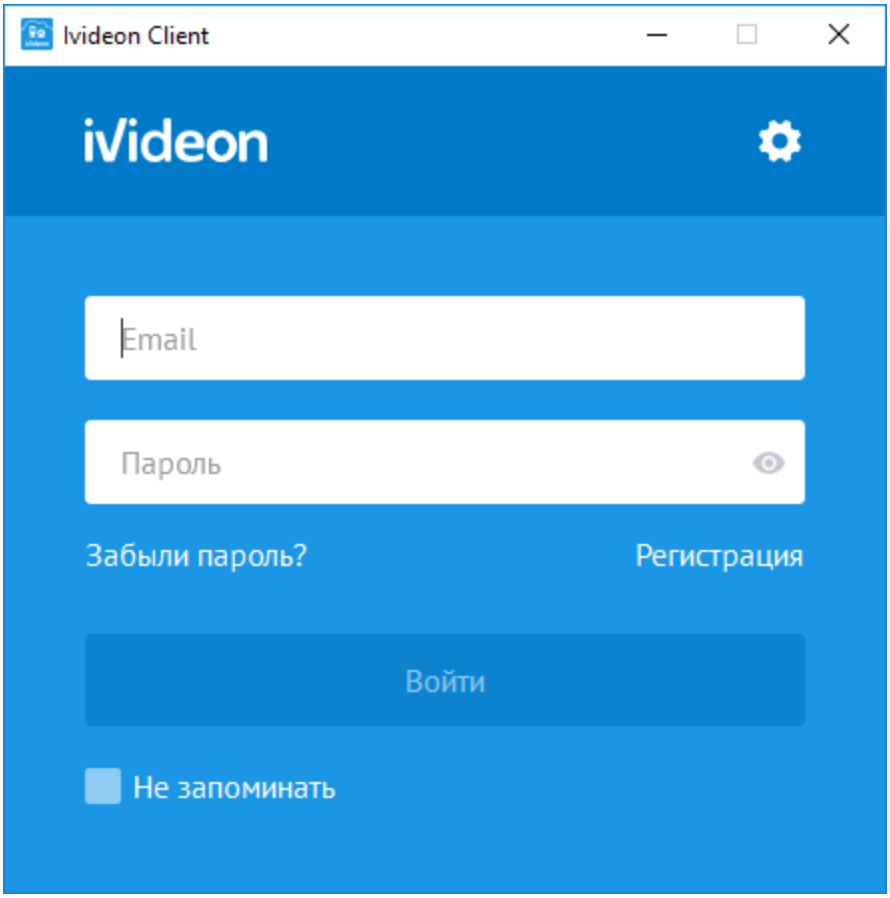


Рисунок 27 - Запуск клиента Ivideon

Если у вас еще нет учетной записи Ivideon, создайте ее, используя ссылку ***Регистрация*** в этом же окне.

Внимание: Доступ к видео возможен только если соответствующий сервер Ivideon включен.

Более подробная информация представлена в документации к ПО Ivideon.

Интеграция видеоподсистемы Ivideon в АРМ RusGuard

Если у вас есть учетная запись в системе Ivideon и камеры видеонаблюдения, подключенные через Ivideon, вы можете интегрировать их через модуль ***Конфигурация оборудования*** АРМ RusGuard.

Для того чтобы интегрировать сервер Ivideon в АРМ RusGuard:

1. Зайдите в модуль ***Конфигурация оборудования*** 79.
2. В иерархическом списке слева перейдите к пункту ***Сторонние системы***. Выберите ***Ivideon > Локальные сервера***.

   В верхней панели инструментов активируется кнопка  ***Сторонние системы***.
3. Нажмите на кнопку  ***Сторонние системы***.

   Раскроется меню.

4. Выберите ***Ivideon > Добавить локальный сервер*** (только этот пункт будет активен).

Откроется окно для ввода учетных данных (см. рис. 28).

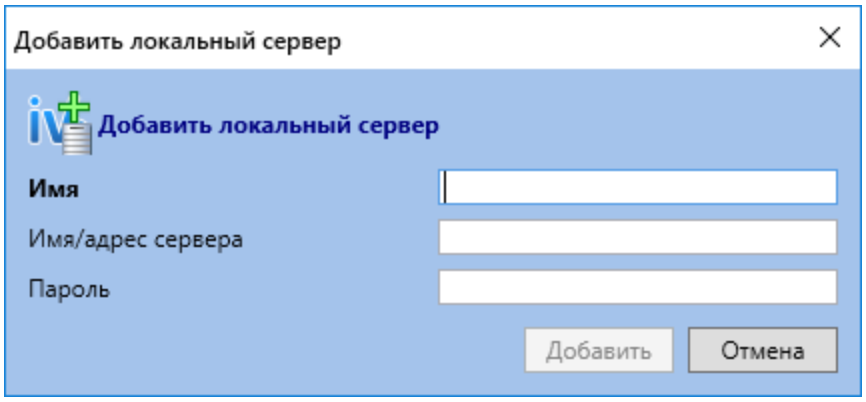
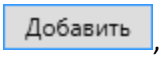


Рисунок 28 - Ввод учетных данных для интеграции сервера Ivideon в АРМ

5. Введите данные, использованные при создании учетной записи Ivideon и исходного сервера:
   - В поле ***Имя*** вводится имя сервера Ivideon (заполняется произвольно и служит для обозначения сервера в ПО RusGuard)
   - В поле ***Имя/адрес сервера*** вводится IP-адрес/имя сервера, где установлен и запущен сервер Ivideon (имя компьютера, на котором установлен сервер)
   - В поле ***Пароль*** вводится пароль доступа на сервер Ivideon

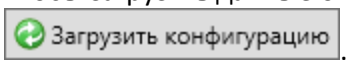
Предупреждение: если сервер Ivideon установлен на одном ПК с сервером RusGuard, в поле ***Имя/адрес сервера*** запрещено вводить значения `127.0.0.1` или `localhost`. Необходимо ввести действительный IP-адрес данного сервера в сети либо его имя.

6. Нажмите на кнопку 

, которая станет активна после ввода всех необходимых данных.

Внимание: Убедитесь, что локальный сервер включен и что на нем разрешен локальный просмотр 382.

Данные загрузятся в АРМ, вновь созданный сервер появится в списке.

7. Чтобы загрузить данные о камерах, подключенных к серверу, нажмите на кнопку 

.

Система загрузит данные о камерах, которые также появятся в иерархическом списке слева (см. рис. 29).

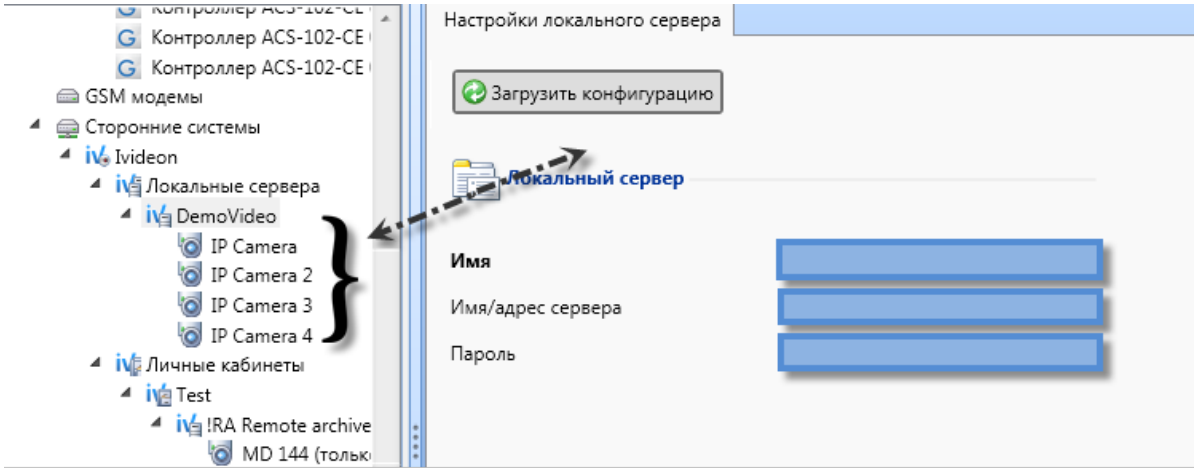


Рисунок 29 - Сервер Ivideon интегрирован в АРМ. Загружены конфигурации IP-камер

Для того чтобы интегрировать личный кабинет Ivideon в АРМ RusGuard:

1. Зайдите в модуль ***Конфигурация оборудования*** 79.
2. В иерархическом списке слева перейдите к пункту ***Сторонние системы***. Выберите ***Ivideon > Личные кабинеты***.

   В верхней панели инструментов активируется кнопка  ***Сторонние системы***.

3. Нажмите на кнопку  ***Сторонние системы***.

   Раскроется меню.

4. Выберите ***Ivideon > Добавить личный кабинет*** (только этот пункт будет активен).

Откроется окно для ввода учетных данных (см. рис. 30).

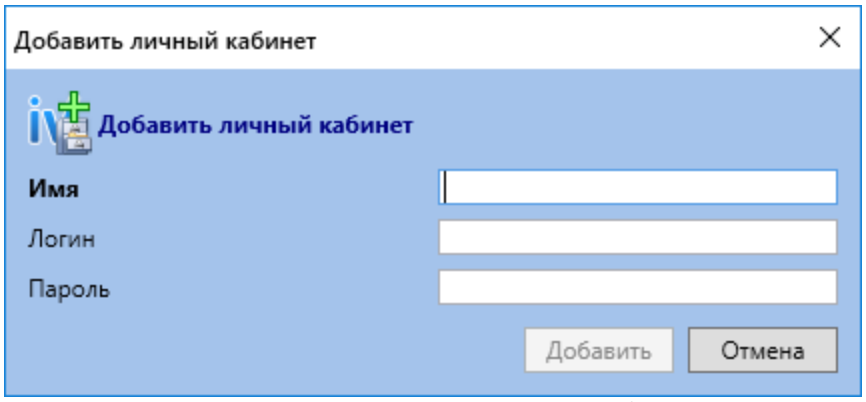


Рисунок 30 - Ввод учетных данных для интеграции личного кабинета Ivideon в АРМ

5. Введите данные, использованные при создании учетной записи Ivideon:

- В поле Имя вводится имя сервера Ivideon (вводится произвольно, используется для идентификации личного кабинета в системе RusGuard);
- В поле Логин - адрес электронной почты, использованный при создании учетной записи Ivideon;

- В поле Пароль вводится пароль доступа к учетной записи (личному кабинету) Ivideon.

6. Нажмите на кнопку Добавить, которая станет активна после ввода всех необходимых данных.

Данные загрузятся в АРМ, интегрированный личный кабинет появится в иерархическом списке (см. рис. 31).

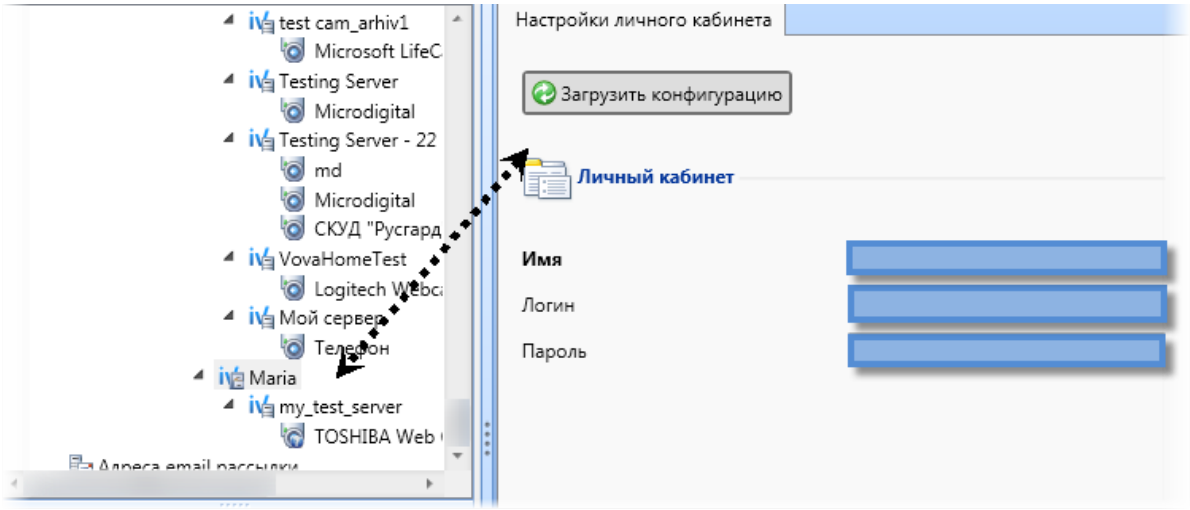


Рисунок 31 - Личный кабинет Ivideon Интегрирован в АРМ

7. Чтобы загрузить данные о камерах, подключенных к личному кабинету, нажмите на кнопку Загрузить конфигурацию.

Система выполнит загрузку, после чего изображение с камер, подключенных к учетной записи, станет доступно в АРМ, а сами камеры также появятся в списке.

Камеры Ivideon, интегрированные в АРМ RusGuard через серверы или личные кабинеты, используются и управляются как и остальные системные устройства. В частности, они могут размещаться на планах в виде "драйверов" (см. рис. 32).

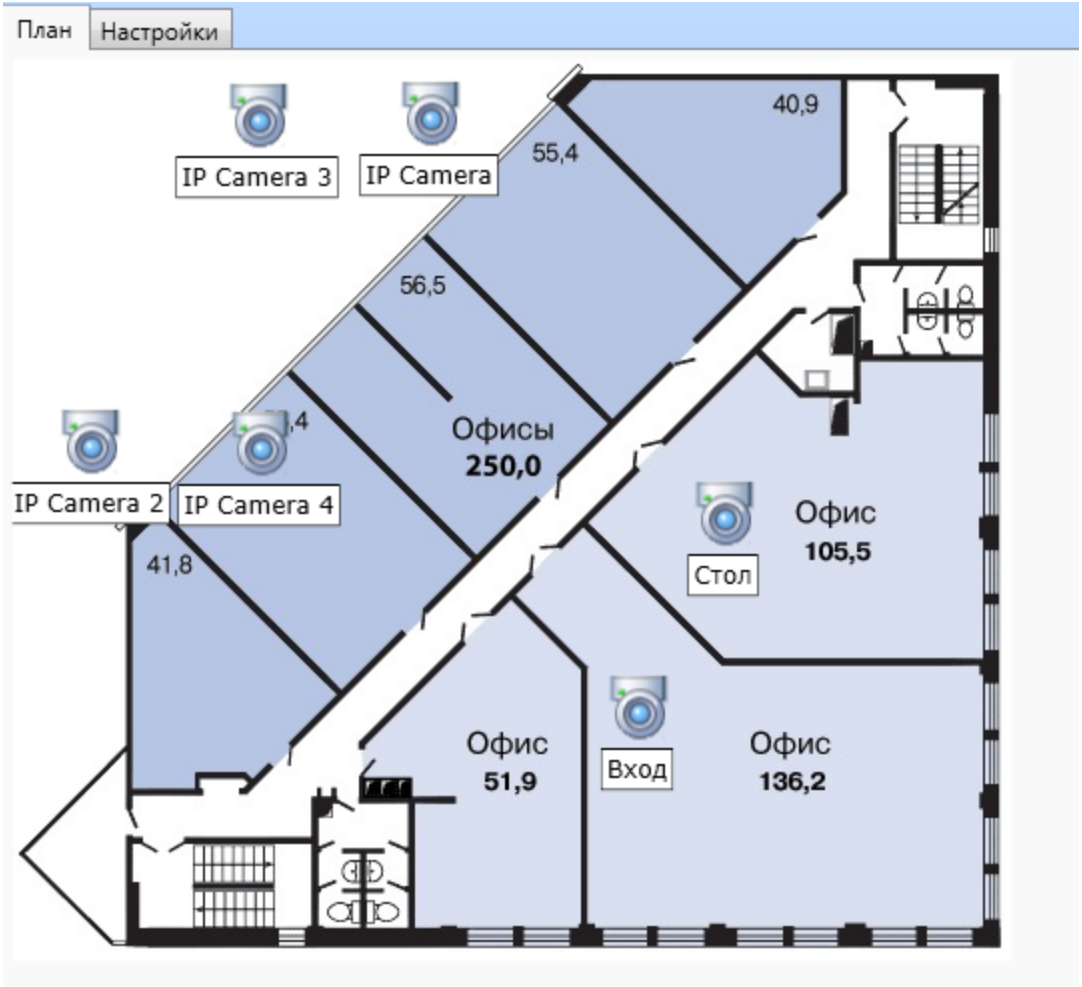


Рисунок 32 - Драйверы камер Ivideon на плане

Также изображение с камер Ivideon может выводиться в режиме реального времени через модуль ***Фотоидентификация*** 248. Камеры Ivideon могут использоваться для записи видео событий 285 при настройки ***Реакций*** 193.

Интеграция с видеорегистраторами Panasonic

Корпорация Panasonic - один из ведущих мировых производителей техники. Сфера деятельности компании Panasonic охватывает широчайший ассортимент электроники и высокотехнологичных приоборов. Традиционно компания специализировалась на аудио и видео технике, бытовой технике.

В рамках интеграции ПО RusGuard взаимодействует с IP NVR Panasonic и подключенными к ним IP камерами.

Процесс настройки сходен с настройкой камер Ivideon 384 и выполняется в модуле ***Конфигурация оборудования***. Настроенные камеры отображаются на схемах в модуле ***Планы***.

Обратите внимание, что использование сервиса подлежит платному лицензированию. При приобретении лицензии пользователь получает USB-ключ и файл License.txt. Файл нужно скопировать на ПК, где установлен **сервер** RusGuard, в установочную директорию (например, C:\\Program Files (x86)\VVI Investment\RusGuard\). И на этом же ПК (**сервер**) следует использовать USB-ключ.

ABBYY PassportReader SDK

Установка и активация модуля ABBYY PassportReader

Для корректной работы ABBYY PassportReader SDK необходимо установить:

- Само приложение ABBYY PassportReader SDK;
- Драйверы USB-ключа.

Для того чтобы установить и активировать приложение:

1. Запустите файл `ABBYY PassportReader SDK.msi` в папке `E:\Redistributables\ABBYY PassportReader`.
2. Выполните пошаговую процедуру установки. Рекомендуется использовать параметры по умолчанию.

Внимание: В окне ***Выбор папки установки*** необходимо установить флаг ***Использовать аппаратный ключ защиты*** (см. рис. 33).

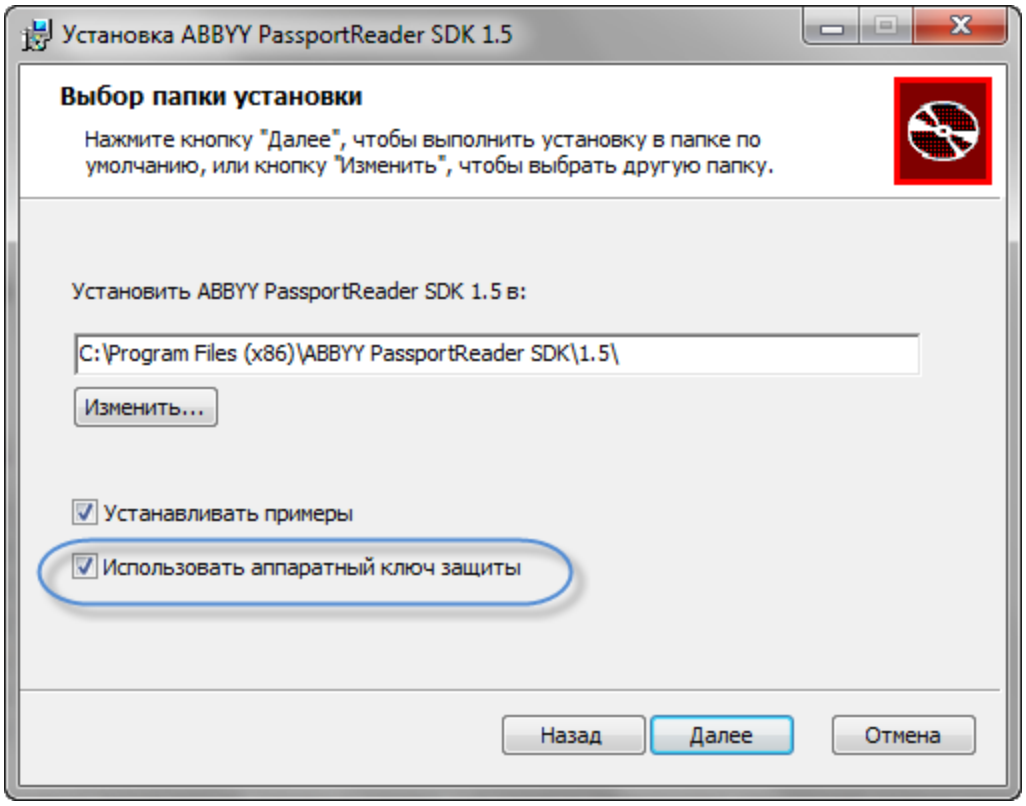


Рисунок 33 - Установка ABBYY PassportReader SDK

3. В конце процесса установки открывается окно Менеджера лицензий. Если USB-ключ подключен и драйверы корректно установлены, ввод лицензионного ключа выполняется автоматически (см. рис. 34).

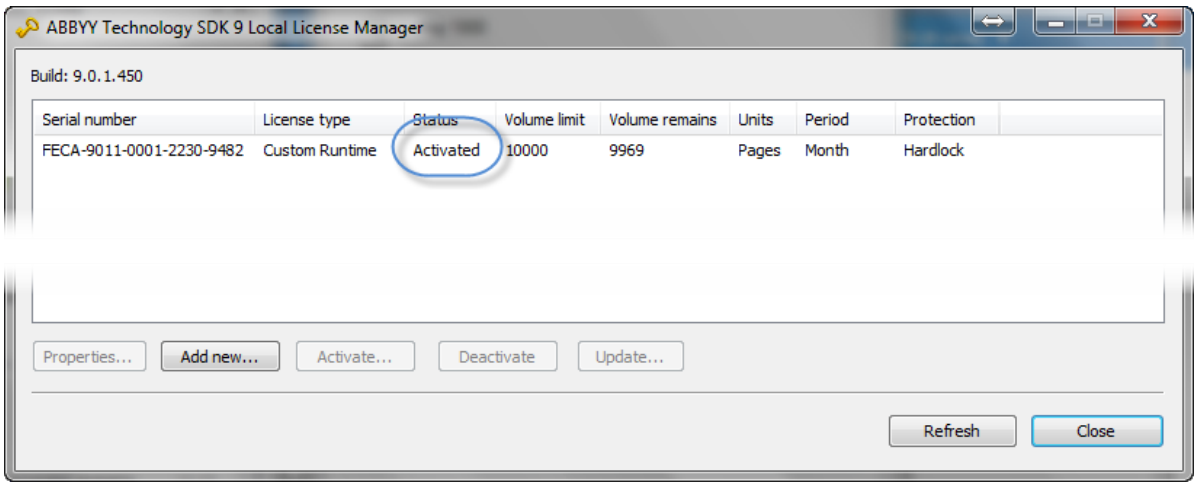


Рисунок 34 - Установка ABBYY PassportReader SDK. Код лицензии загружен с USB-ключа

Вы также можете завершить установку без активации лицензии. Чтобы активировать лицензию позднее, необходимо установить USB-ключ в разъем и запустить Менеджер лицензий ABBYY (см. рис. 35). Убедитесь, что драйверы для USB-ключа установлены. Приложение автоматически получит лицензионные данные от USB-ключа и отобразит статус ***Activated***.

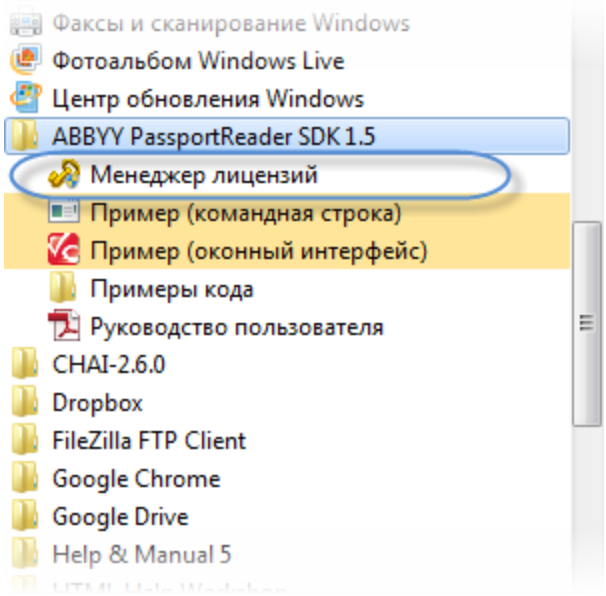


Рисунок 35 - Вызов приложения Менеджер Лицензий

Для того чтобы установить и настроить драйверы USB-ключа:

1. Запустите файл `iKeyDrvr64.exe` (для 64-х разрядных ОС) или `IKEYDRVR.exe` (для 32-х разрядных ОС) в папке `\Redistributables\ABBYY PassportReader\USB Drivers`.
2. Выполните установку, следуя указаниям системы.
3. Вставьте USB-ключ в разъем.

Система сообщит об отсутствии нужных драйверов устройства.

4. Запустите Диспетчер устройств ОС Windows (***Пуск > Панель управления > Диспетчер устройств***).
5. Найдите устройство в списке, выделите его и щелчком правой кнопки мыши раскройте контекстное меню. Выберите пункт ***Обновить драйверы***...
6. В раскрывшемся окне выберите ***Выполнить поиск драйверов на этом компьютере***.
7. Укажите путь к папке с установленными драйверами (по умолчанию драйверы устанавливаются на `C:\Program Files\SafeNet\iKey Driver`).
8. Выполните установку драйвера, следуя процедуре (отклоняйте системные предупреждения, продолжайте установку).

Интеграция с 1С "БИТ"

Предупреждение: при функционировании сервера RusGuard под управлением ОС Windows Server 2012 возможна некорректная работа модуля интеграции. Перед покупкой проконсультируйтесь со службой технической поддержки.

Модуль работы с системой на базе оборудования RusGuard доступен в разделе системы ***БИТ: Управление доступом (СКУД) 8*** (см. рис. 36).

Модуль позволяет использовать элементы системы RusGuard (базу данных сотрудников, устройств) в решениях на базе 1С. При этом для синхронизации не требуется установка ПО RusGuard на локальном ПК. Достаточно подключения к серверу RusGuard.

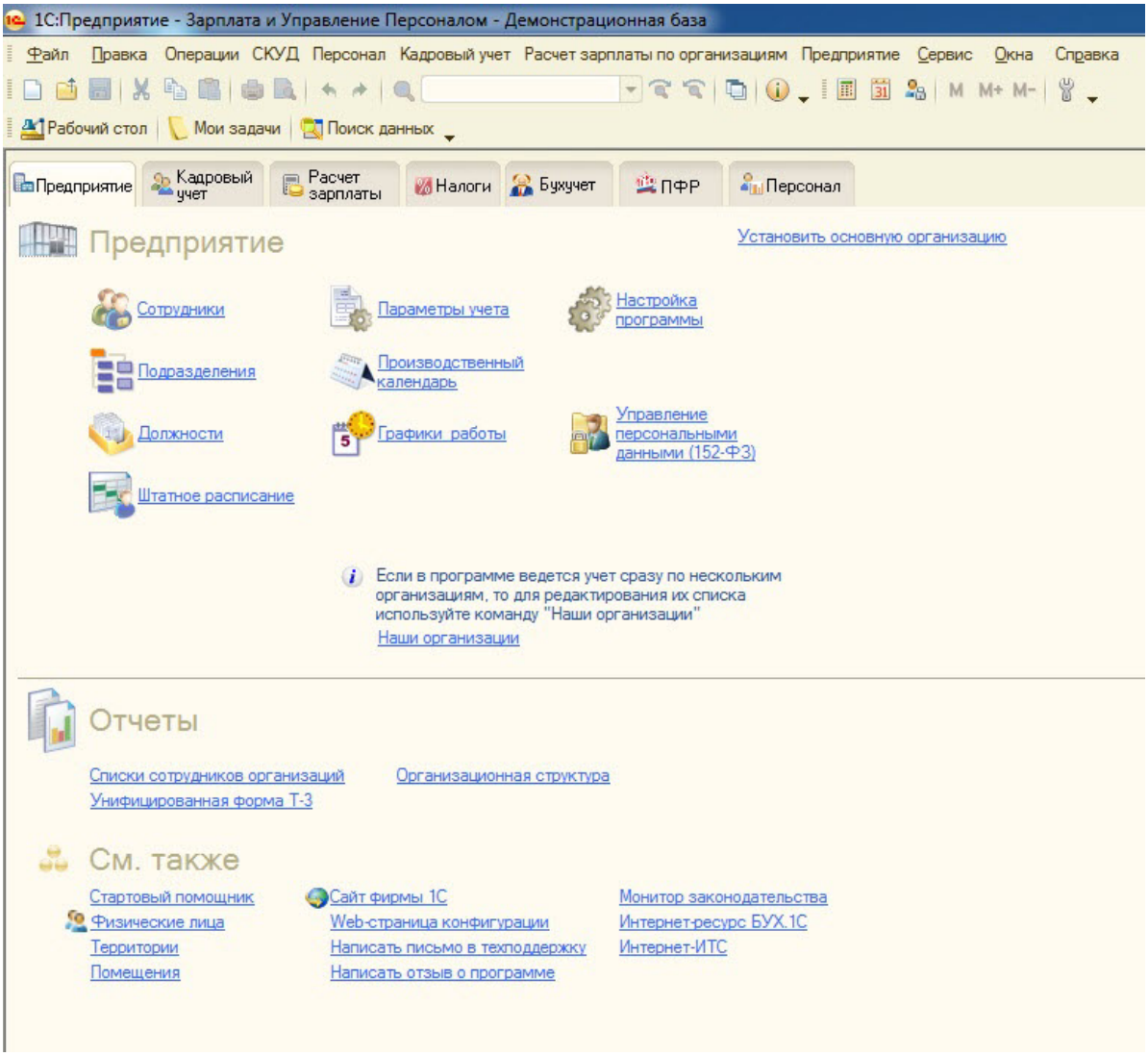


Рисунок 36 - Модуль 1С: Предприятие - Зарплата и управление персоналом

Обратите внимание, что модуль RusGuard доступен в модуле ***БИТ: Управление доступом (СКУД) 8*** при наличии дополнительной библиотеки AddIn.RusGuard.dll.

Для того чтобы настроить параметры подключения «БИТ: Управление доступом (СКУД) 8» к БД RusGuard:

1. Зайдите в конфигурацию ***БИТ: Управление доступом (СКУД) 8*** (см. рис. 37).

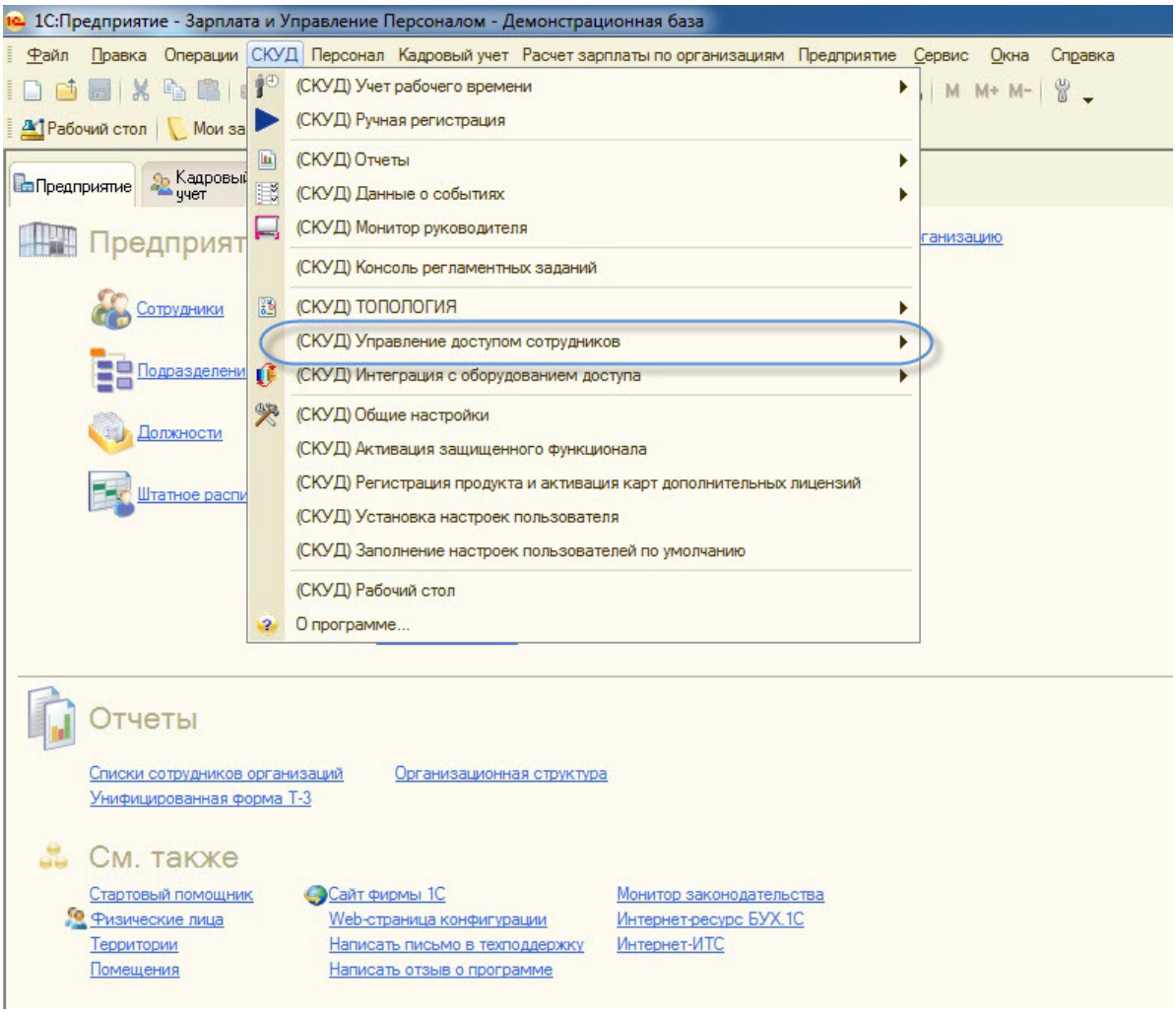


Рисунок 37 - Решение 1С. Переход к настройкам СКУД

2. Откройте форму настройки СКУД: ***(СКУД) Настройки***.
3. Перейдите на закладку настройки обмена данными: ***Обмен данными с внешними БД > RusGuard***
4. Введите параметры подключения, укажите настройки по умолчанию для новых физических лиц (***Установить назначение свойств и категорий***) (см. рис. 38).

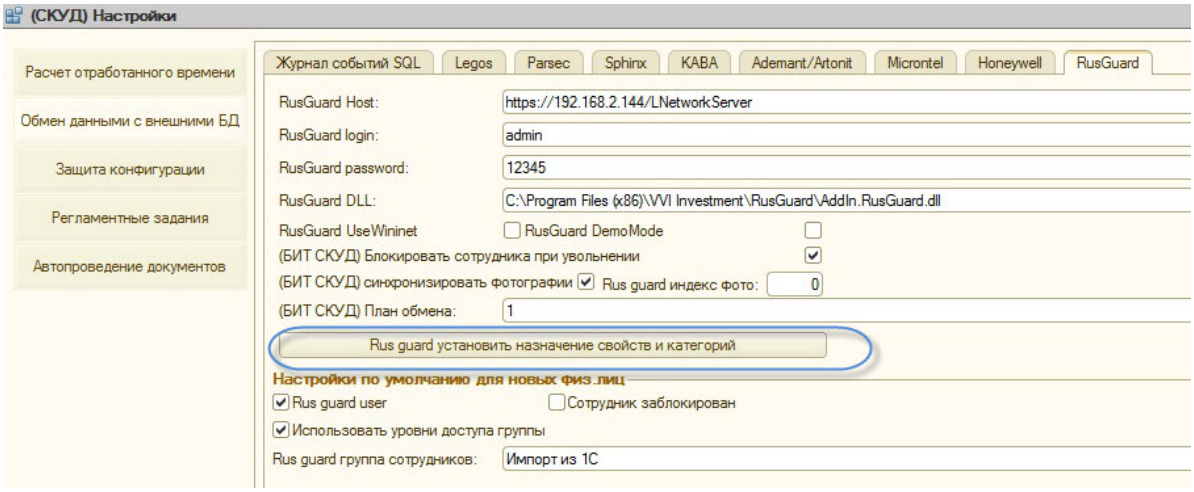


Рисунок 38 - Решение 1С. Переход к настройкам СКУД. Настройки для новых физических лиц

5. Сохраните настройки.

Для того чтобы выполнить синхронизацию данных RusGuard/1С:

1. Зайдите в конфигурацию ***БИТ: Управление доступом (СКУД) 8***.
2. Откройте форму настройки синхронизации СКУД: ***(СКУД) Интеграция с оборудованием доступа*** > ***(СКУД) Синхронизация RusGuard***.
3. Удостоверьтесь, что приоритет синхронизации установлен верно на всех вкладках (для импорта данных из RusGuard должно быть выбрано значение ***Внешний***).
4. Выполните синхронизацию БД сотрудников:
   i. Перейдите на вкладку ***Синхронизация сотрудников***.
   ii. Нажмите на кнопку ***Заполнить***.
   iii. Установите флаги напротив строк (записей), подлежащих синхронизации. По умолчанию, флаги установлены напротив строк с данными о сотрудниках, где отличаются ключевые поля учетных записей (ФИО, группа сотрудника **RusGuard**, карта), или которые присутствуют только в одной из БД (см. рис. 39).

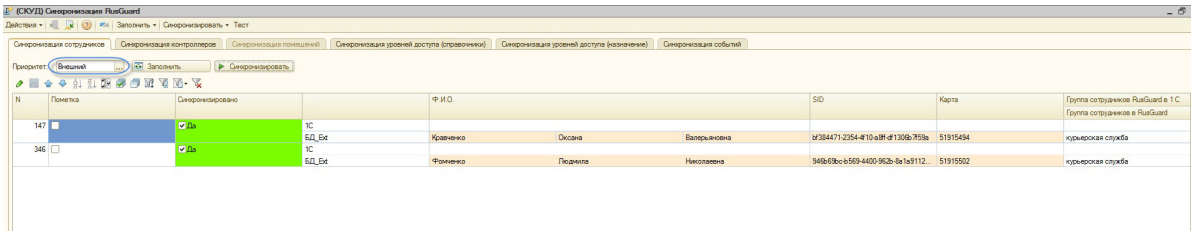


Рисунок 39 - Модуль 1С: Предприятие - Зарплата и управление персоналом. Синхронизация сотрудников

Если установлен ***Внешний*** приоритет синхронизации, и физическое лицо уже зарегистрировано в БД ***БИТ: Управление доступом (СКУД) 8***, его можно выбрать в соответствующем поле. Если физическое лицо еще не зарегистрировано, запись будет создана при синхронизации.

Если установлен ***Внутренний*** приоритет синхронизации, обновляются поля БД RusGuard, либо в этой БД создается новая учетная запись.

iv. Нажмите на кнопку ***Синхронизировать***.

Система создает элементы справочника ***Физические лица***, если в строке не выбран существующий элемент (см. рис. 40), либо существующий элемент отмечается как элемент подсистемы **RusGuard**.

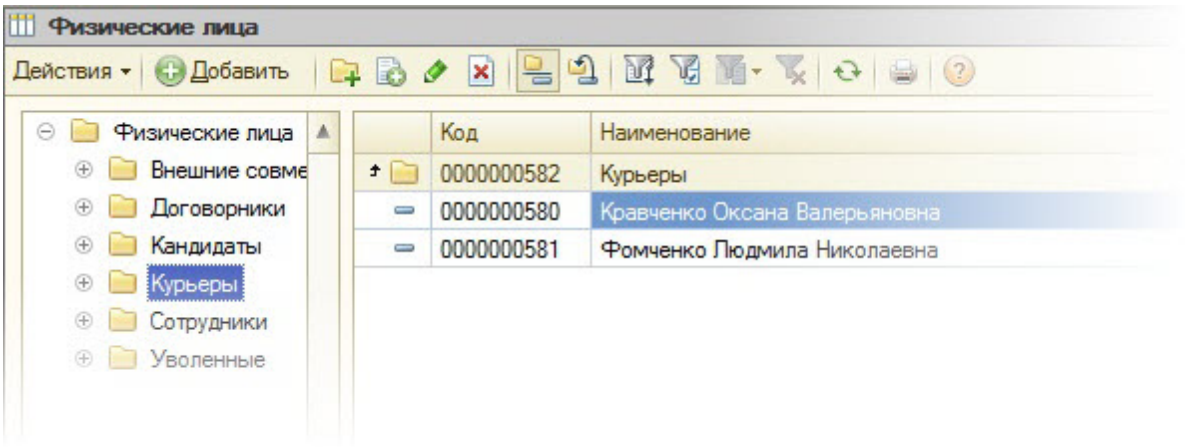


Рисунок 40 - Модуль 1С: Предприятие - Зарплата и управление персоналом. Справочник физических лиц

Помимо ФИО синхронизируются следующие элементы:

- Группа сотрудников **RusGuard**
- Уровни доступа группы **RusGuard**
- Блокировка сотрудника, **RusGuard**
- Паспортные данные
- Фотография
- Адреса
- Комментарий

v. В случае изменения карты доступа документы Движение карт создаются автоматически

5. Выполните синхронизацию контроллеров:

i. Перейдите на вкладку ***Синхронизация контроллеров***.

ii. Нажмите на кнопку ***Заполнить***.

Система извлекает все зарегистрированные в системе RusGuard контроллеры, заполняется таблица синхронизации (см. рис. 41).

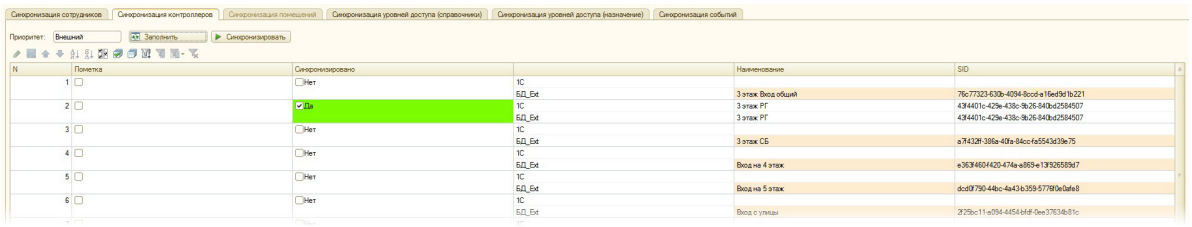


Рисунок 41 - Модуль 1С: Предприятие - Зарплата и управление персоналом. Синхронизация контроллеров

Если контроллер уже зарегистрирован в БД ***БИТ: Управление доступом (СКУД) 8***, его можно выбрать в соответствующем поле. Если нет, запись будет создана при синхронизации.

iii. Нажмите на кнопку ***Синхронизировать***.

Система создает элементы справочника ***Контроллеры***, если в строке не выбран существующий элемент, либо существующий элемент отмечается как элемент подсистемы **RusGuard**.

Примечание: Синхронизация контроллеров происходит только в режиме импорта.

6. Выполните синхронизацию помещений:
   i. Из-за различий между ПО RusGuard и ***БИТ: Управление доступом (СКУД) 8***, справочник помещений и регистр сведений ***Контрольные точки*** необходимо настроить вручную.
7. Выполните синхронизацию уровней доступа:
   i. Перейдите на вкладку ***Синхронизация уровней доступа (справочники)***.
   ii. Нажмите на кнопку ***Заполнить***.

Система извлекает все зарегистрированные в системе RusGuard уровни доступа, заполняется таблица синхронизации.

Если уровень уже зарегистрирован в БД ***БИТ: Управление доступом (СКУД) 8***, его можно выбрать в соответствующем поле. Если нет, запись будет создана при синхронизации.

iii. Нажмите на кнопку ***Синхронизировать***.

Система создает элементы справочника уровней доступа, если в строке не выбран существующий элемент, либо существующий элемент отмечается как элемент подсистемы **RusGuard**.

iv. Перейдите на вкладку ***Синхронизация уровней доступа (назначения)***.

v. Установите приоритет (***Внешний***, чтобы использовать данные БД RusGuard, или ***Внутренний***, чтобы использовать данные БД 1С).

vi. Нажмите на кнопку ***Заполнить***.

Система извлекает все зарегистрированные в системе RusGuard назначения уровней доступа, заполняется таблица синхронизации.

Если уровень уже зарегистрирован в БД ***БИТ: Управление доступом (СКУД) 8***, его можно выбрать в соответствующем поле. Если нет, запись будет создана при синхронизации.

vii. Нажмите на кнопку ***Синхронизировать***.

Создаются документы ***БИТ СКУД назначение уровней доступа***. Если сотрудники совпали по ФИО, но имеют разные уровни доступа, формируется два документа: один отменяет прежний уровень доступа, другой - присваивает новый. Если совпадений нет, создается один документ о присвоении уровня доступа сотруднику.

8. Выполните синхронизацию событий:
   i. Перейдите на вкладку ***Синхронизация событий*** (см. рис. 42).

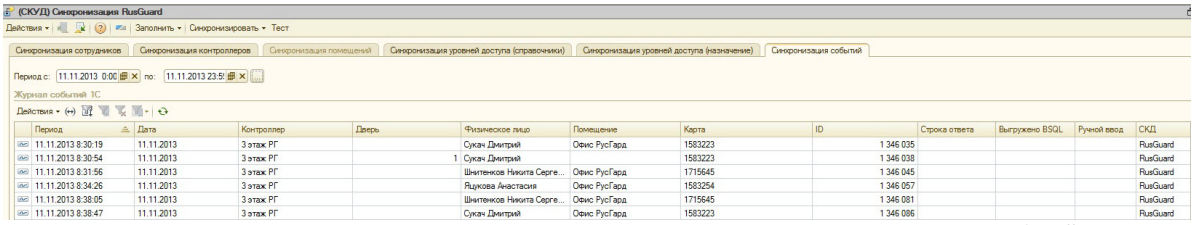


Рисунок 42 - Модуль 1С: Предприятие - Зарплата и управление персоналом. Синхронизация событий

ii. Задайте условия отбора событий (период, с которого должна быть выполнена выборка событий из БД RusGuard).

iii. Нажмите на кнопку ***Обновить*** для табличного поля ***Загружаемые события***.

Если в БД RusGuard обнаружены события, отвечающие условиям поиска, они заносятся в поле ***Загружаемые события***.

Обратите внимание, что выборка выполняется только по зарегистрированным сотрудникам БД ***БИТ: Управление доступом (СКУД) 8***, которым выданы карты. Если на момент синхронизации ни одному сотруднику не выдана карта, события не считываются.

Все неидентифицированные события загружаются в журнал ошибок.

iv. Нажмите на кнопку ***Сохранить в 1С***. чтобы сохранить выборку событий в ***БИТ: Управление доступом (СКУД) 8***.

В случае успешного выполнения операции, данные отображаются в верхнем табличном поле.

Решение также позволяет настраивать расписание синхронизаций, или выполнения "регламентных заданий".

Для того чтобы настроить регламентные задания:

1. Зайдите в конфигурацию ***БИТ: Управление доступом (СКУД) 8***.
2. Откройте форму настройки заданий: ***(СКУД) Консоль регламентных заданий***. Обратите внимание, что предварительно необходимо указать для файлового варианта работы БД учетную запись, под которой будут выполняться задания, интервал для опроса в константах ***БИТ: Управление доступом (СКУД) 8*** (см. рис. 43).

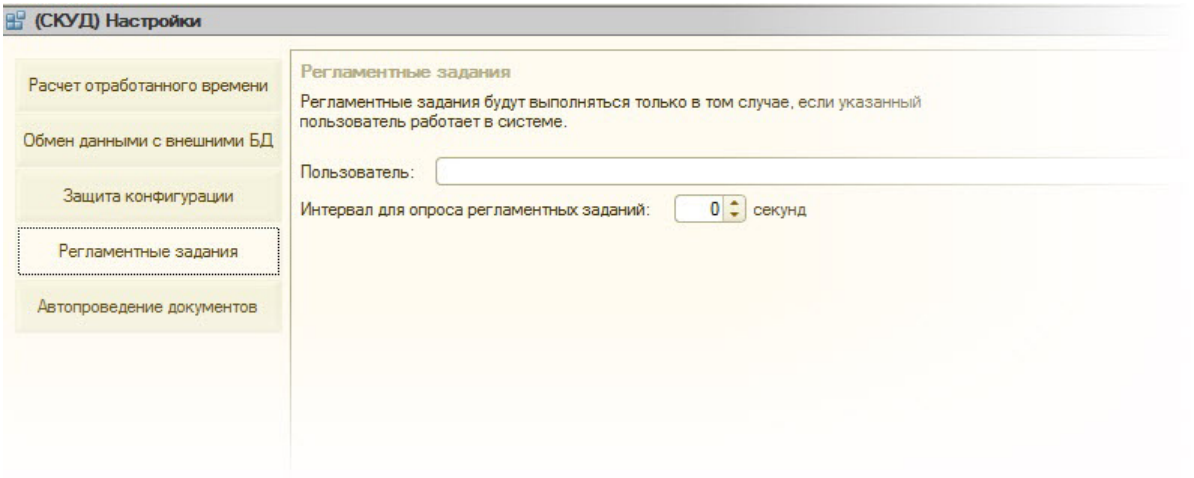
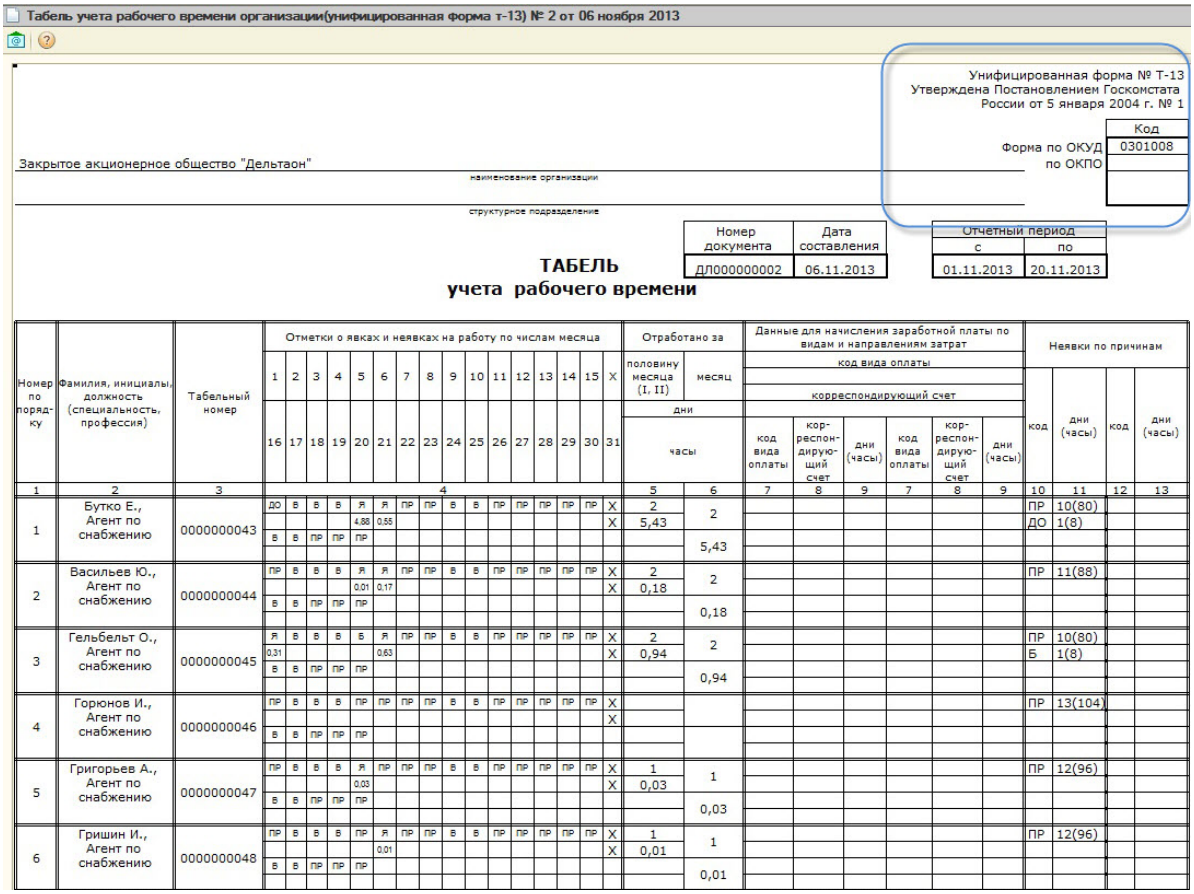


Рисунок 43 - Модуль 1С: Предприятие - Зарплата и управление персоналом. Настройка регламентных заданий: ввод учетной записи для опроса

3. Для выполнения загрузок необходимо создать задания:
   - (СКУД) Синхронизация сотрудников RusGuard
   - (СКУД) Синхронизация контроллеров RusGuard
   - (СКУД) Синхронизация помещений RusGuard
   - (СКУД) Импорт событий RusGuard
4. Настройте расписание выполнения указанных заданий.
5. Введите параметры подключения, укажите настройки по умолчанию для новых физических лиц (***Установить назначение свойств и категорий***).

Данные, импортируемые из БД RusGuard, используются для формирования табеля рабочего времени установленного образца (см. рис. 44) и анализа рабочего времени в решении 1С в различных форматах (см. рис. 45).



Табель учета рабочего времени организации(унифицированная форма т-13) № 2 от 06 ноября 2013

Унифицированная форма № Т-13
Утверждена Постановлением Госкомстата России от 5 января 2004 г. № 1

	Код
Форма по ОКУД	0301008
по ОКПО	

Закрытое акционерное общество "Дельтаон"
наименование организации

структурное подразделение

Номер документа	Дата составления	Отчетный период с	Отчетный период по
ДЛ000000002	06.11.2013	01.11.2013	20.11.2013

ТАБЕЛЬ учета рабочего времени

Номер по порядку	Фамилия, инициалы, должность (специальность, профессия)	Табельный номер	Отметки о явках и неявках на работу по числам месяца: 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	X	Отработано за: половину месяца (I, II) дни	Отработано за: месяц дни	Отработано за: месяц часы	Данные для начисления заработной платы по видам и направлениям затрат: код вида оплаты	корреспондирующий счет: код вида оплаты	корреспондирующий счет: корреспондирующий счет	корреспондирующий счет: дни (часы)	код вида оплаты	корреспондирующий счет: корреспондирующий счет	корреспондирующий счет: дни (часы)	Неявки по причинам: код	дни (часы)	код	дни (часы)
			16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31														
1	2	3	4																5	6		7	8	9	7	8	9	10	11	12	13
1	Бутко Е., Агент по снабжению	0000000043	ДО	В	В	В	Я	Я	ПР	ПР	В	В	ПР	ПР	ПР	ПР	ПР	X	2	2								ПР	10(80)		
							4,68	0,55										X	5,43									ДО	1(8)		
			В	В	ПР	ПР	ПР													5,43												
2	Васильев Ю., Агент по снабжению	0000000044	ПР	В	В	В	Я	Я	ПР	ПР	В	В	ПР	ПР	ПР	ПР	ПР	X	2	2								ПР	11(88)		
							0,01	0,17										X	0,18												
			В	В	ПР	ПР	ПР													0,18												
3	Гельбельт О., Агент по снабжению	0000000045	Я	В	В	В	Б	Я	ПР	ПР	В	В	ПР	ПР	ПР	ПР	ПР	X	2	2								ПР	10(80)		
			0,31					0,63										X	0,94									Б	1(8)		
			В	В	ПР	ПР	ПР													0,94												
4	Горюнов И., Агент по снабжению	0000000046	ПР	В	В	В	ПР	ПР	ПР	ПР	В	В	ПР	ПР	ПР	ПР	ПР	X										ПР	13(104)		
																		X													
			В	В	ПР	ПР	ПР																									
5	Григорьев А., Агент по снабжению	0000000047	ПР	В	В	В	Я	ПР	ПР	ПР	В	В	ПР	ПР	ПР	ПР	ПР	X	1	1								ПР	12(96)		
							0,03											X	0,03												
			В	В	ПР	ПР	ПР													0,03												
6	Гришин И., Агент по снабжению	0000000048	ПР	В	В	В	ПР	Я	ПР	ПР	В	В	ПР	ПР	ПР	ПР	ПР	X	1	1								ПР	12(96)		
								0,01										X	0,01												
			В	В	ПР	ПР	ПР													0,01												

Рисунок 44 -Модуль 1С: Предприятие - Зарплата и управление персоналом. Формирование табеля рабочего времени

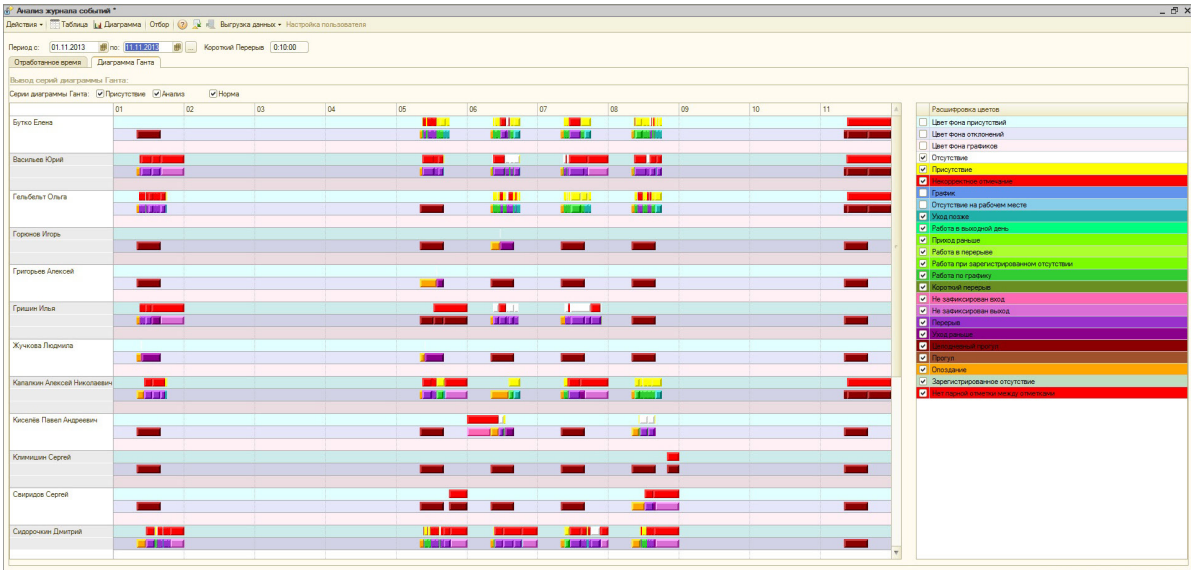


Рисунок 45 -Модуль 1С: Предприятие - Зарплата и управление персоналом. Анализ событий. Диаграмма Ганта

Более подробная информация представлена в руководстве пользователя к модулю ***БИТ: Управление доступом (СКУД) 8***.

Модуль Формула для учета рабочего времени

Модуль представляет собой внешнюю обработку для 1С: Предприятие 8.2 или 8.3 (файл с расширением `epf`). Для использования модуля необходимо установить 1С: Предприятие 8.2 или 8.3 совместимой с модулем конфигурации.

Модуль работоспособен в конфигурациях:

- Зарплата и Управление персоналом 2.5 (далее - ЗУП);
- Управление производственным предприятием 1.3;
- Комплексная автоматизация;
- и иных с аналогичным ЗУП функционалом кадрового учета и расчета заработной платы.

Разработчик гарантирует работу заявленных функций только в актуальных релизах типовых конфигураций закрытых для внесения изменений.

Актуальные релизы типовых конфигураций приведены здесь. Использование модуля не требует доработок имеющейся конфигурации. Алгоритмы закрыты для редактирования.

Запуск модуля

Для того чтобы запустить модуль:

1. В меню Файл 1С: Предприятие 8.2 в пункте меню "Файл" выполните команду "Открыть" и укажите файл модуля в диалоговом окне, которое открывается по команде.

Подробное руководство по использованию модуля представлено в его справке.

Установка внешней компоненты

Для СКУД RusGuard требуется установка библиотек взаимодействия модуля с ПО СКУД. Для СКУД RusGuard это файл `AddIn.RusGuard.dll`, который необходимо разместить в каталог BIN используемого релиза платформы 1С на ***КАЖДОМ*** компьютере, де будет запускаться модуль учета рабочего времени.

Порядок получения лицензии

Модуль имеет встроенную систему лицензирования. Без лицензирования модуль работает в демонстрационном режиме со следующими ограничениями:

- Возможность загрузить не более 200 событий входа-выхода;
- Возможность обработать не более 5 сотрудников в каждом документе "Регламентированный табель учета рабочего времени".

Порядок лицензирования

Выполните следующие действия:

1. Отсканируйте заполненную регистрационную анкету.
2. Получите в диалоговом окне модуля первую часть ключа.
3. Вышлите отсканированную анкету и первую часть ключа по адресу info@timeaccount.ru. Ждите получения второй части ключа.
4. Введите вторую часть ключа в соответствующее диалоговое окно модуля.

Интеграция с ISS

Интеграция с ISS позволяет строить внутри системы ISS (решение SecurOS) дерево устройств, импортируемое из ПО RusGuard, передавать все соответствующие события, а также отображать метки точек доступа системы RusGuard ("драйверы") на планах системы ISS.

Для работы модуля интеграции в ISS необходима лицензия на интерфейс IIDK и точку интеграции.

Поддерживаемые SecurOS:

- Enterprise
- Premium

Возможны два варианта настройки интеграции:

- На одном сервере (т.е. обе системы развертываются на одном физическом сервере)
- На разных серверах (т.е. используются разные физические машины).

Первый вариант следует использовать только для небольших конфигураций и/или на мощных серверах.

Настройка интеграции на одном сервере

Предварительные условия

- На сервере должно быть настроено ПО RusGuard версии 10 не ниже 1.4.0.
- Развернутое решение SecureOS (в данном случае считается, что все элементы архитектуры установлены на одном сервере).

Процедура настройки

Для того чтобы выполнить интеграцию:

1. Скачайте модуль интеграции с сайта RusGuard: http://www.rgsec.ru/files/ftp/Other-systems/ISSIntegration.zip.
2. Запустите ПО SecurOS на компьютере (запуск всегда следует выполнять, используя права Администратора). Логин и пароль: root, securos.
3. Распакуйте архив и скопируйте файлы в установочную директорию SecurOS (выполняется для каждого экземпляра, в случае распределенной системы).
4. Закройте программу. Используя права Администратора, запустите утилиту **idb.exe** и, не меняя ничего, нажмите на кнопку ***Обновить***.

Данная утилита находится в директории установки SecurOS (по умолчанию: C:\Program files (x86)\ISS\SecurOS).

Внимание: Этот шаг обязательно выполнить до всех последующих. Иначе SecurOS не сможет обновить конфигурацию на части видеосерверов и система на какое-то время перестанет быть конфигурируемой.

5. Снова запустите SecurOS.
6. Зайдите в панель управления SecurOS (***Выполнить*** > ***Конфигурирование***).

7. Если в системе отсутствует объект "***Компьютер***", создайте его.
8. Перейдите в созданный объект "Компьютер" и создайте интеграцию RusGuard (см. рис. 46).

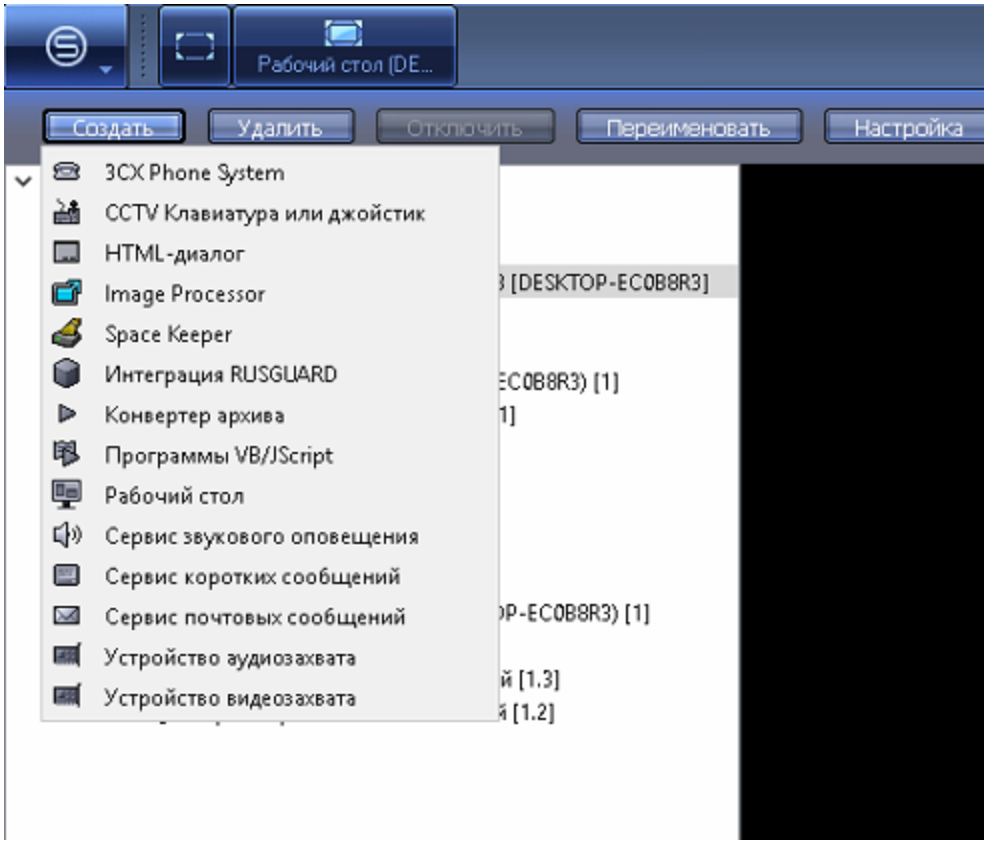


Рисунок 46 - SecurOS, интеграция с ISS (создание интеграции с RG)

9. Введите параметры интеграции (см. рис. 47).

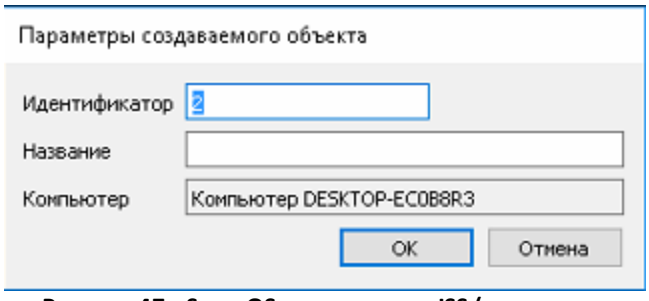


Рисунок 47 - SecurOS, интеграция с ISS (параметры интеграции)

10. Зайдите в АРМ RusGuard, модуль ***Конфигурация оборудования*** 79.
11. Нажмите на кнопку ***Сторонние системы*** в верхней панели управления. Выберите пункт ***ISS*** > ***Добавить ISS IIDK*** (см. рис. 48).

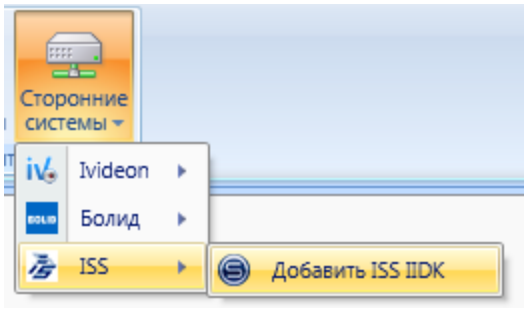


Рисунок 48 - АРМ RusGuard, интеграция с ISS

Откроется диалоговое окно для ввода параметров сервера RusGuard в системе SecurOS.

12. Введите ID интерфейса IIDK (номер объекта, присвоенный в панели управления SecurOS), имя сервера и IP адрес (см. рис. 49). Сохраните данные.

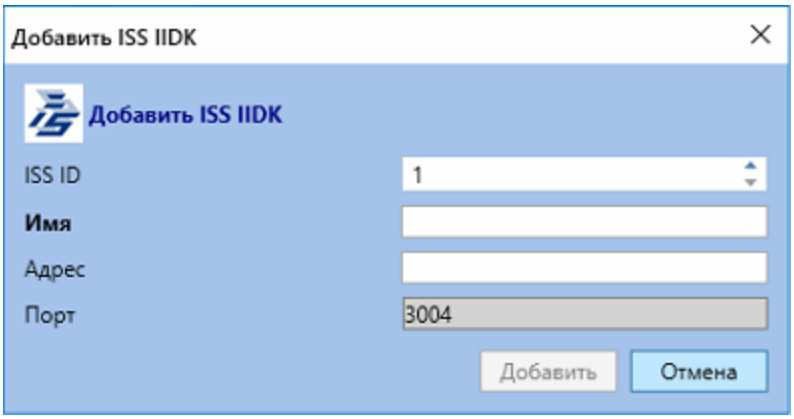


Рисунок 49 - Модуль "Конфигурация оборудования" ПО RusGuard, создание интеграции с ISS

13. На следующем экране АРМ нажмите на кнопку ***Считать конфигурацию*** (см. рис. 50). В систему SecurOS импортируются данные о дереве устройств и точек доступа RusGuard, а также настроенных для них событий.

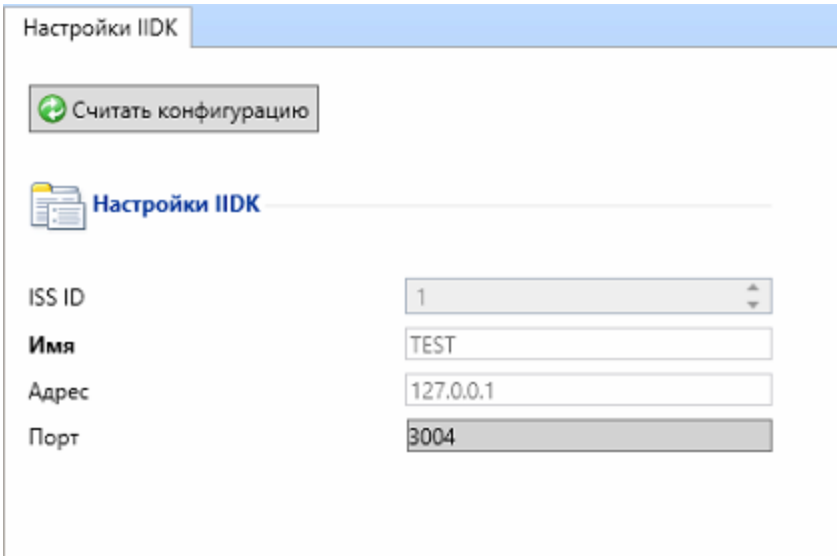


Рисунок 50 - Модуль "Конфигурация оборудования" ПО RusGuard, считывание конфигурации

14. В левой навигационной панели появится структура точки интеграции. Перейдите к нужной интеграции, чтобы выполнить привязку точек доступа. (см. рис. 51).

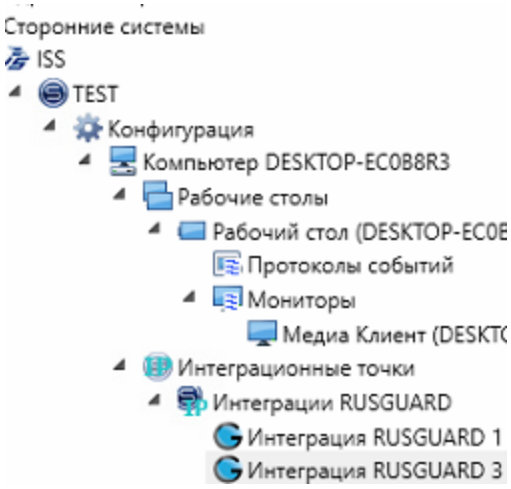


Рисунок 51 - APM RusGuard, навигационная панель

15. Перейдите на вкладку ***Драйверы*** в главном окне.

16. Нажмите на кнопку  в верхней половине экрана, чтобы добавить точку доступа.

17. Выберите одну или несколько точек доступа из списка, который откроется в новом окне, примените выбор. Точки доступа отобразятся в главном окне (см. рис. 52).

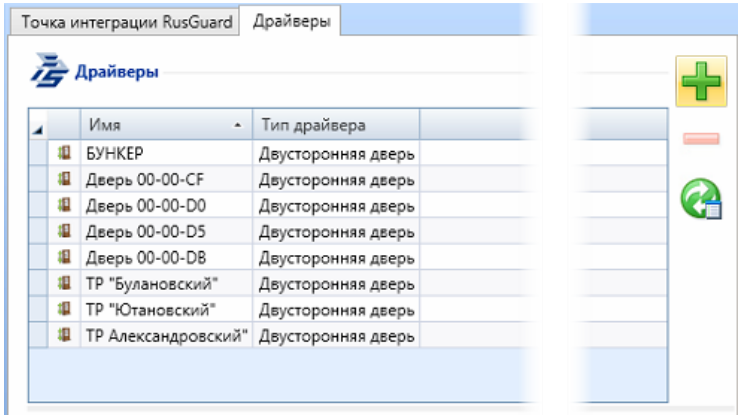


Рисунок 52 - APM RusGuard, список точек доступа

18. Аналогичным образом, используя кнопку  в нижней части экрана, выполните привязку камер и протоколов событий к каждой точке доступа (см. рис. 53).

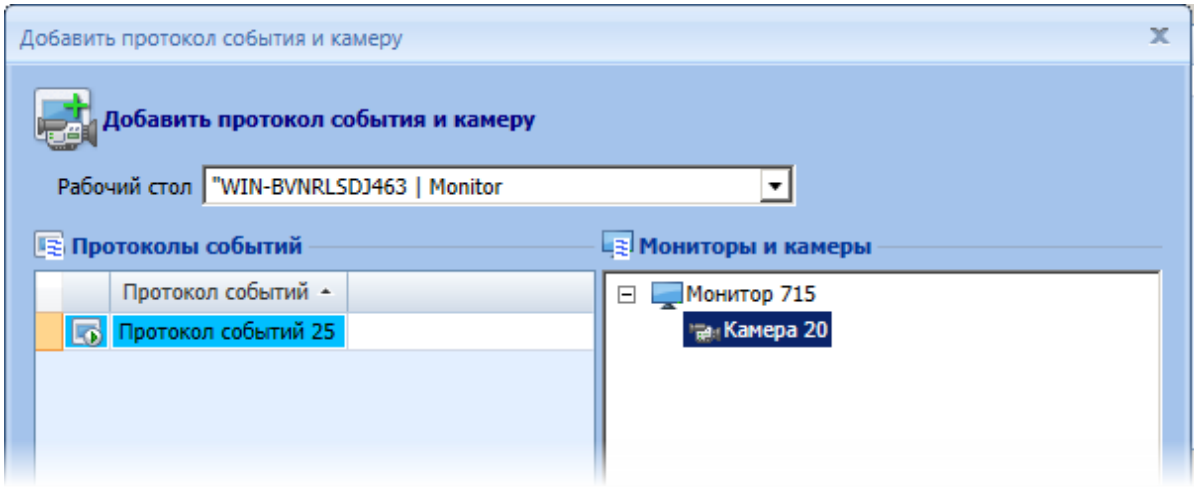


Рисунок 53 - АРМ RusGuard, добавление протокола событий и камеры

19. Щелкните пиктограмму  возле списка точек доступа, чтобы обновить данные о драйверах.
20. Вернитесь в панель управления SecurOS. Перейдите к настраиваемой интеграции с RusGuard.
21. Нажмите на кнопку ***Настройка*** в верхней панели управления.
22. Откроется диалоговое окно настройки интеграции. Обновите конфигурацию. Система выполнит импорт данных о точках доступа, камерах и драйверах из ПО RusGuard в систему SecurOS.

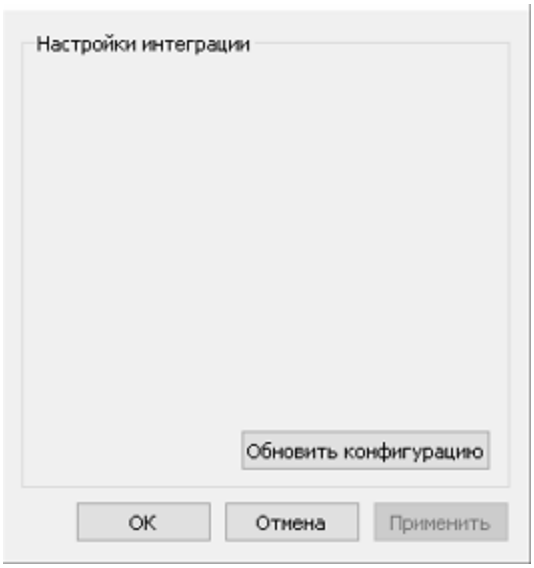


Рисунок 54 - SecurOS, интеграция с ISS (обновление конфигурации)

Периферийные устройства

Подключение считывателя Z-2 USB/USB MF

Установка драйверов Z-2 USB и Z-2 USB MF

Для заполнения карточки сотрудника 70 система RusGuard поддерживает настольные считыватели для эмиссии карт Z-2 USB (см. рис. 1) и Z-2 USB MF (для смарт-карт Mifare).

Считыватель подключается к компьютеру, на котором установлен Сервисный конфигуратор оборудования 321 или АРМ RusGuard. Процедура установки драйверов для обеих модификаций сходна.

Рисунок 1 -
Считывающее устройство Z2-USB

Для того чтобы самостоятельно установить драйверы:

1. Подключите считыватель к ПК через USB-кабель.

   Windows попытается установить драйверы для него, но не сможет (см. рис. 2 и 3).

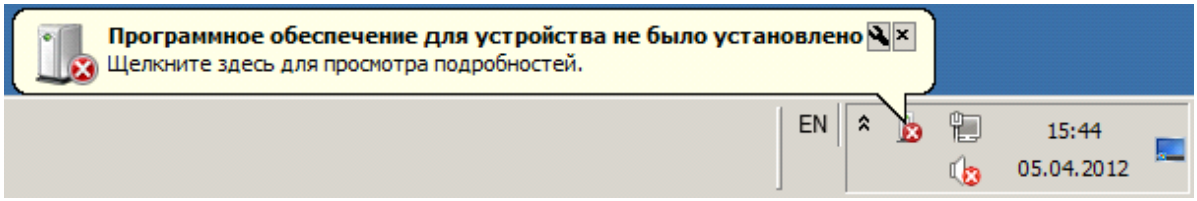


Рисунок 2 - Попытка установки драйверов для устройства

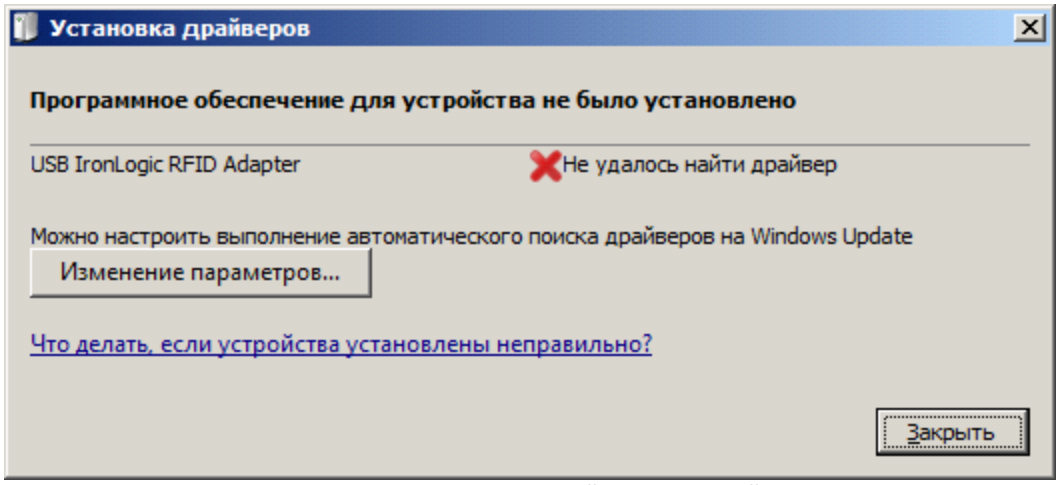


Рисунок 3 - Попытка установки драйверов для устройства

2. Выберите меню ***Пуск > Панель управления > Диспетчер устройств***.

В ***Диспетчере устройств*** появится неизвестное устройство под названием ***USB IronLogic RFID Adpater*** (см. рис. 4).

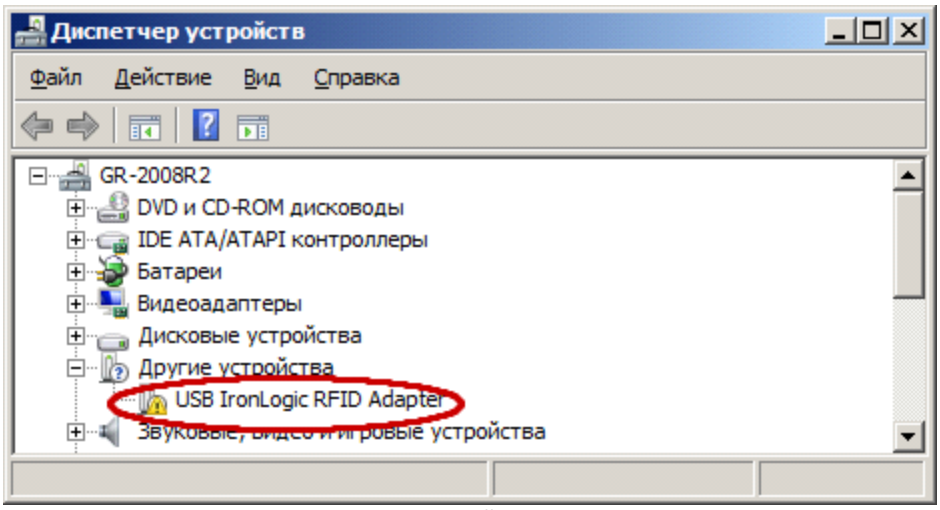


Рисунок 4 - Устройство в списке

Примечание: В ОС Windows 7 Home Premium для вызова ***Диспетчера устройств*** необходимо сначала выбрать в ***Панели инструментов*** пункт ***Оборудование и звук***, в открывшемся окне найдите ***Диспетчер устройств*** в разделе ***Устройства и принтеры*** (см. рис. 5).

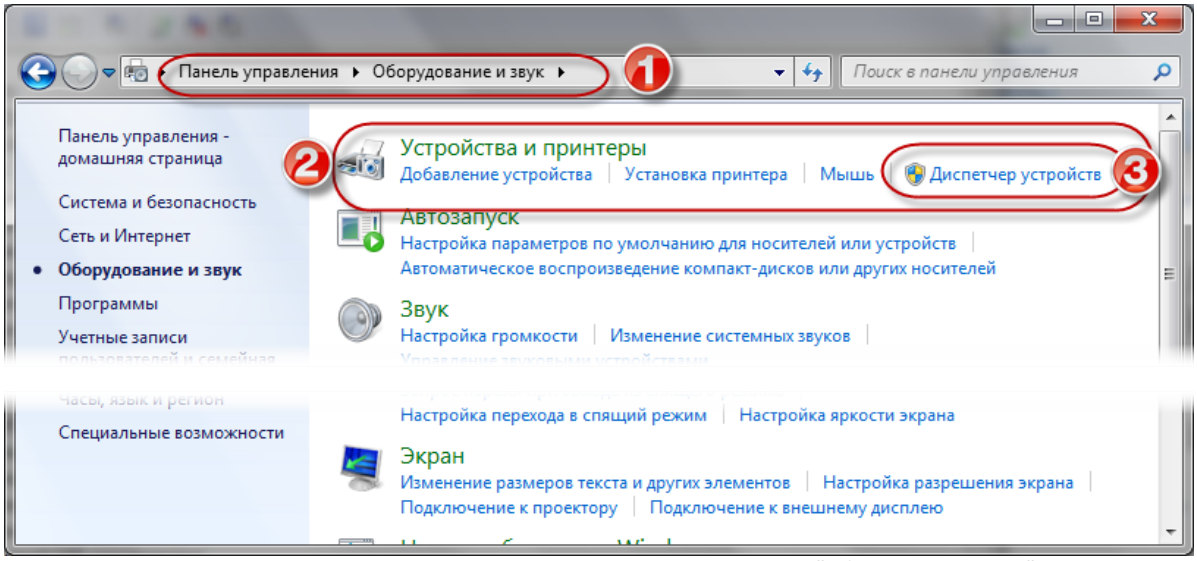


Рисунок 5 - Панель инструментов ОС Windows Home Premium. Пункт "Оборудование и звук"

3. Щелкните по названию устройства правой кнопкой мыши и выберите пункт меню ***Обновить драйверы…*** в контекстном меню.
4. В появившемся окне выберите пункт ***Выполнить поиск драйверов на этом компьютере*** (см. рис. 6).

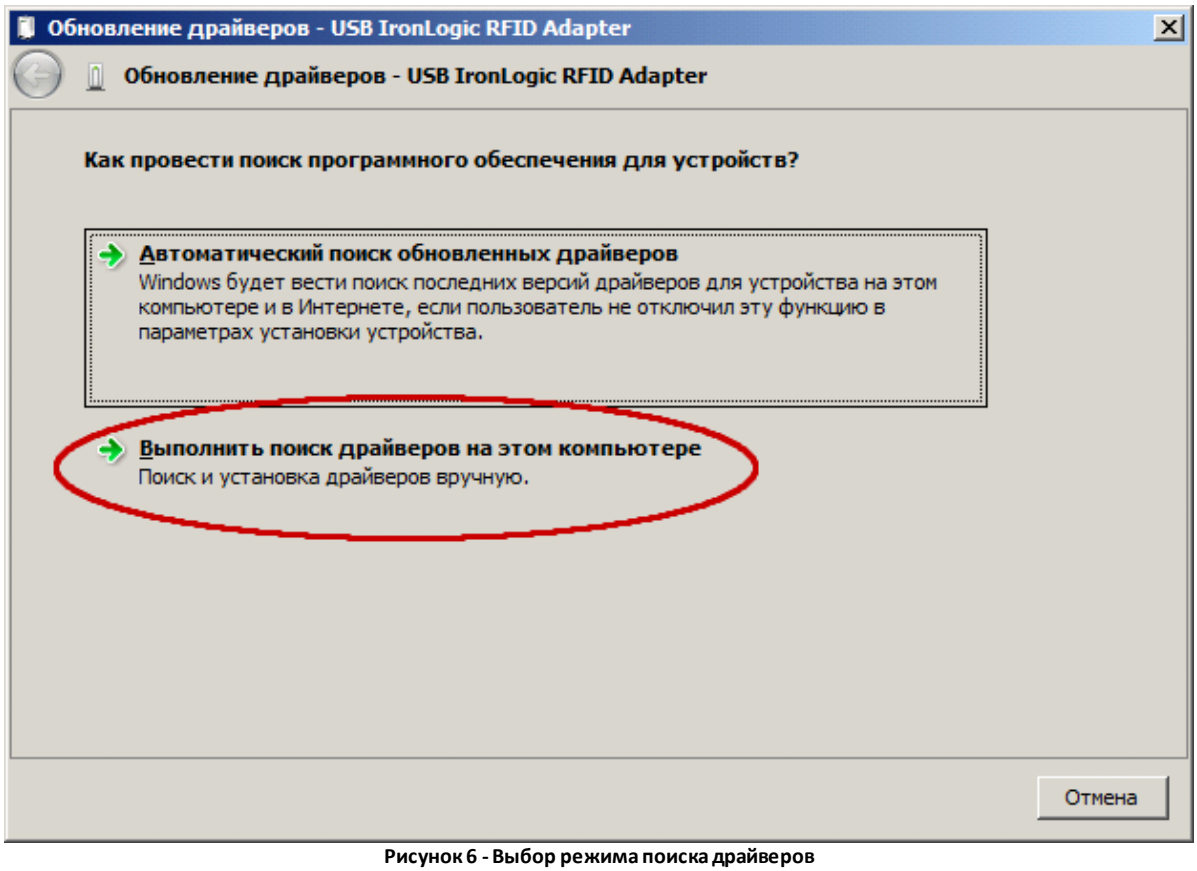


Рисунок 6 - Выбор режима поиска драйверов

5. Нажмите на кнопку Обзор и выберите папку, в которой лежат драйверы Z-2 Usb.

В дистрибутиве ПО RusGuard они находятся в папке `\Components\Z-2 Usb`.

6. Убедитесь, что флаг ***Включая вложенные папки*** установлен , и нажмите на кнопку Далее > (см. рис. 7).

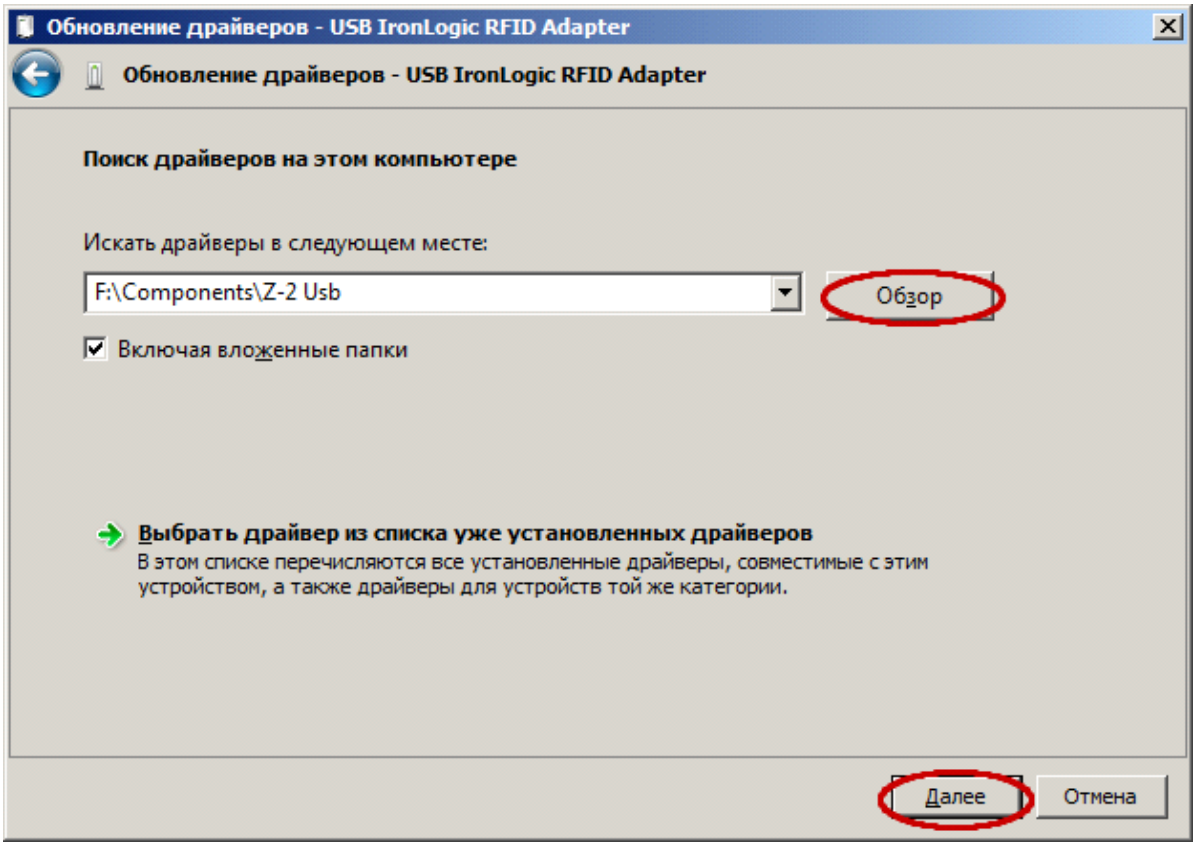


Рисунок 7 - Настройка поиска драйверов

При установке драйвера отобразится предупреждение.

7. Выберите вариант ***Всё равно установить этот драйвер*** (см. рис. 8).

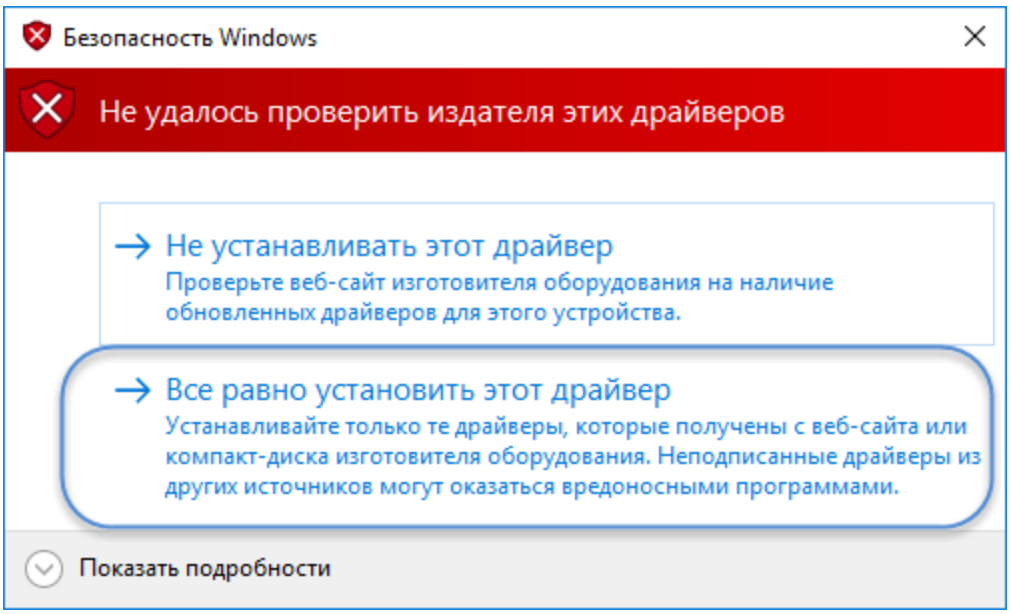


Рисунок 8 - Предупреждение системы

8. Убедитесь, что установка завершена успешно, и нажмите на кнопку Закрыть.

В диспетчере устройств должно появиться устройство USB IronLogic RFID Reader в разделе Контроллеры USB (см. рис. 9).

Не обращайте внимания на неизвестное устройство USB Serial Port в списке.

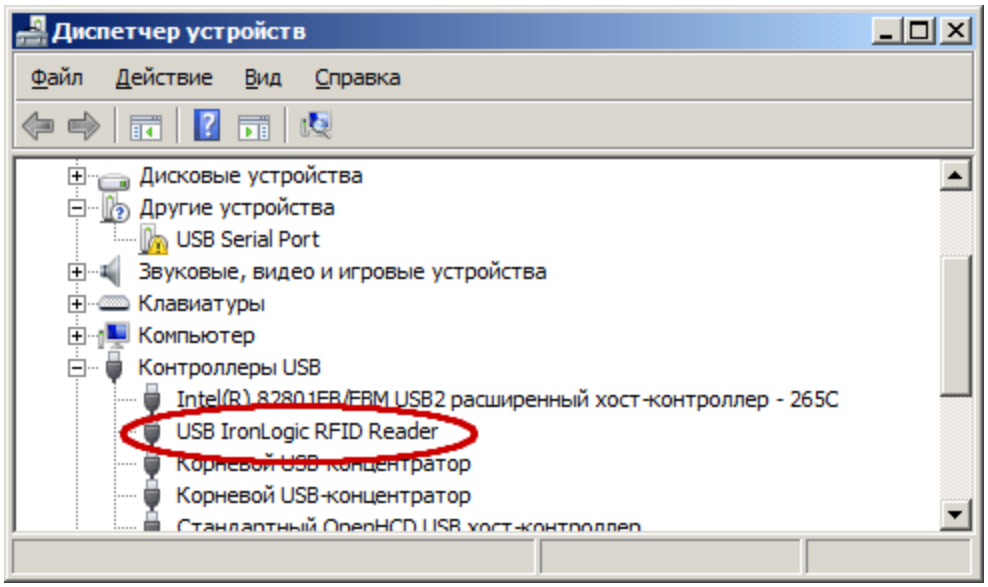


Рисунок 9 - Устройство в списке. Драйверы установлены

Внимание: Для ОС Windows 8, 8.1, Windows 10, а также Windows 2012 Server необходимо до начала установки драйверов отключить обязательную проверку подлинности драйверов.

Для того чтобы отключить обязательную проверку подлинности:

1. Отключите считыватель.

2. Откройте боковую панель системы (щелчок мышью в правом верхнем углу экрана) (см. рис. 10).

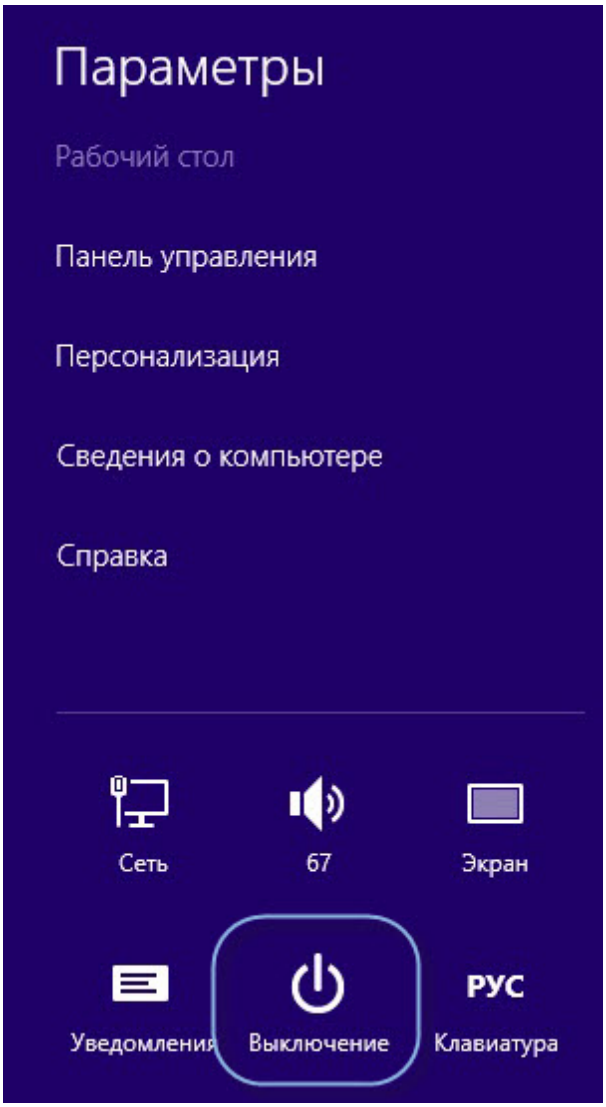


Рисунок 10 - Отключение обязательной проверки подлинности

3. Выберите ***Параметры > Выключение***.

Откроется контекстное меню.

4. Удерживая левую клавишу ***Shift***, выполните перезагрузку (пункт ***Обновить и перезагрузить***).
5. После вывода на экран сервисного меню перейдите в раздел: ***Диагностика*** > ***Дополнительные параметры***> ***Параметры загрузки*** и нажмите кнопку ***Перезагрузить***.
6. Во время загрузки на экран будет выведено меню с возможными опциями загрузки. Нажмите клавишу ***F7***, чтобы выбрать пункт ***Отключить обязательную проверку подписи драйверов*** (см. рис. 11).

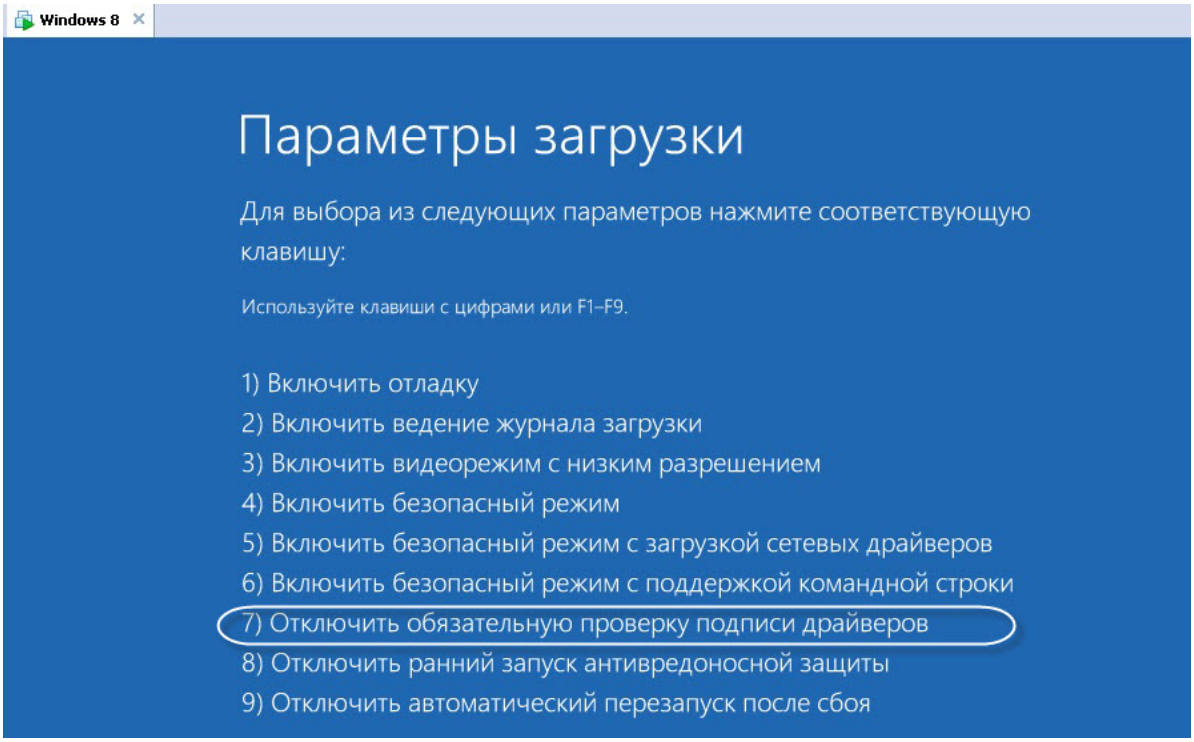


Рисунок 11 - Отключение обязательной проверки подлинности

7. Подключите считыватель. Дождитесь, когда система его найдет. Далее выполняйте процедуру выше 407 от шага 5.

Подключение конвертера CAN-USB CAN-bus-USBnp Marathon

Установка драйверов Marathon

Драйверы для конвертера CAN-USB CAN-bus-USBnp Marathon (см. рис. 12) необходимо установить на компьютере, где развернут сервер RusGuard, а также на компьютере, где будет выполняться конфигурация оборудования RusGuard.

Рисунок 12 - Конвертер CAN-USB CAN-bus-USBnp Marathon

Для того чтобы установить драйверы для конвертера USB-CAN Marathon:

1. Запустите файл `chai-2.6.0-XP-Vista-Win7.exe` и следуйте инструкциям установщика (англ.).
2. Ознакомьтесь с лицензионным соглашением и подтвердите свое с ним согласие (I Agree).
3. При выборе компонентов для установки (см. рис. 13) сохраните настойки по умолчанию и нажмите Next > .

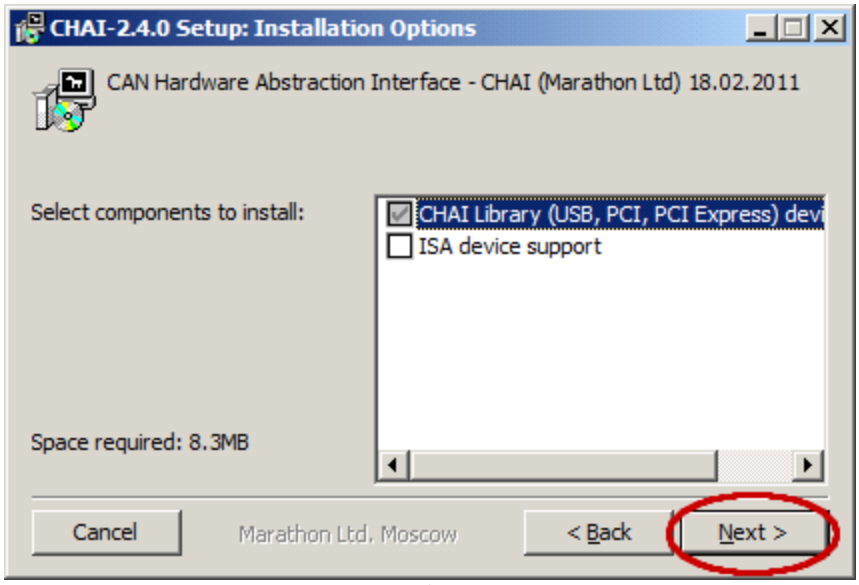


Рисунок 13 - Выбор компонентов

4. Выберите директорию для установки и нажмите на кнопку Install.
5. По окончании установки нажмите на кнопку Close.

Программа установки предложит перезапустить систему.

6. Чтобы согласиться, нажмите на кнопку Да (см. рис. 14).

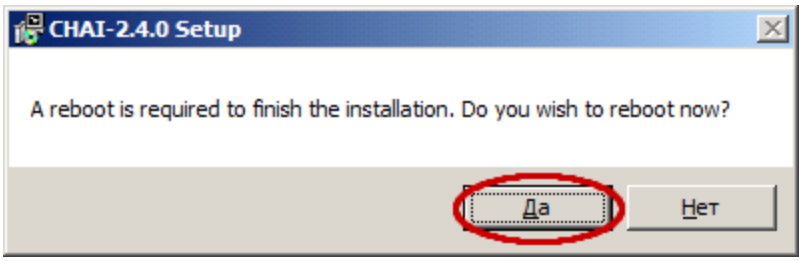


Рисунок 14 - Система предлагает выполнить перезагрузку

7. После перезагрузки системы подключите конвертер Marathon к компьютеру через USB-кабель.

Windows попытается установить драйверы для него, но не сможет (см. рис. 15 и 16).

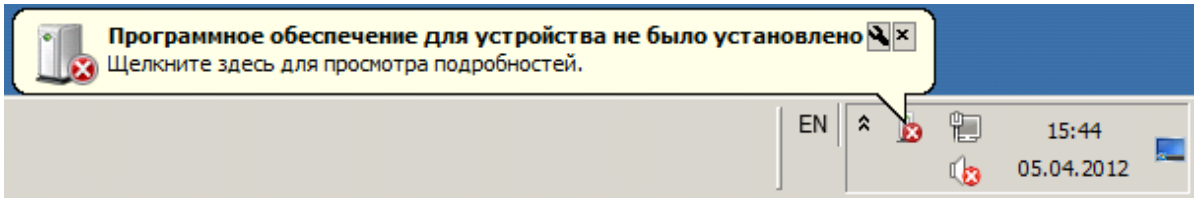


Рисунок 15 - Попытка установки драйверов

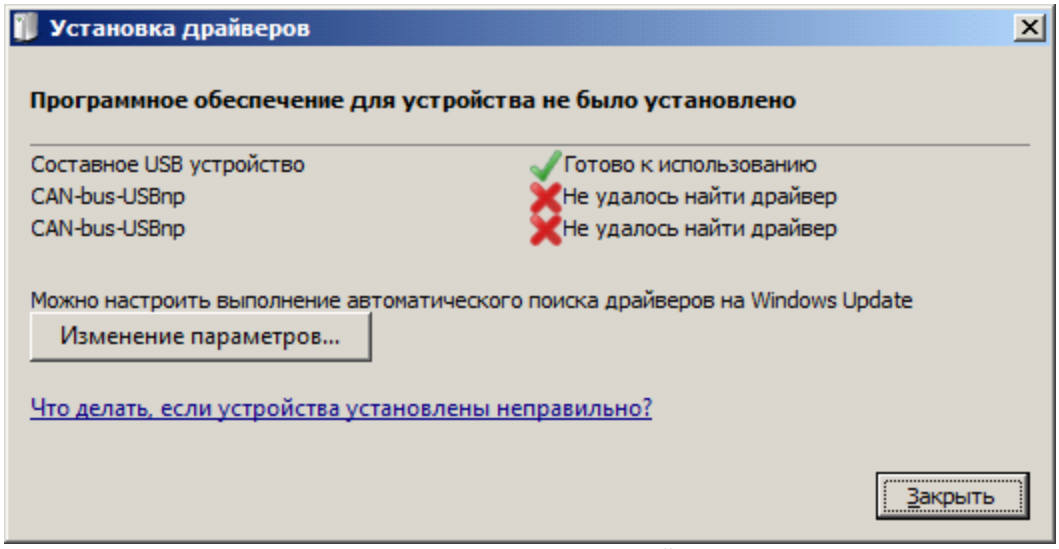


Рисунок 16 - Попытка установки драйверов

8. Выберите меню ***Пуск > Панель управления > Диспетчер устройств***.

В списке ***Диспетчера устройств*** отображаются 2 неизвестных устройства под названием ***CAN-bus-USBnp*** (см. рис. 17).

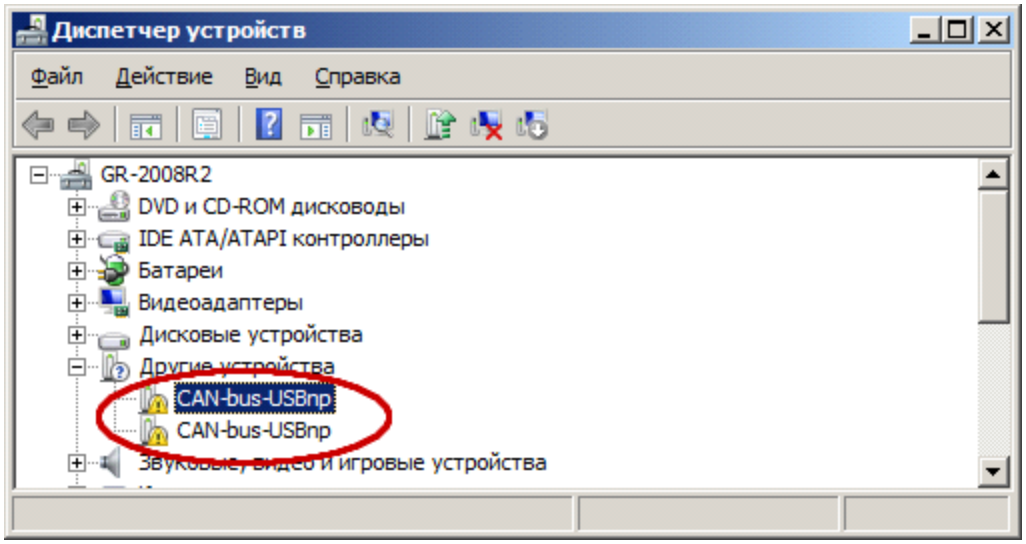


Рисунок 17 - Список устройств

Примечание: В ОС Windows 7 Home Premium для вызова ***Диспетчера устройств*** необходимо сначала выбрать в ***Панели инструментов*** пункт ***Оборудование и звук***, в открывшемся окне найдите ***Диспетчер устройств*** в разделе ***Устройства и принтеры*** (см. рис. 18).

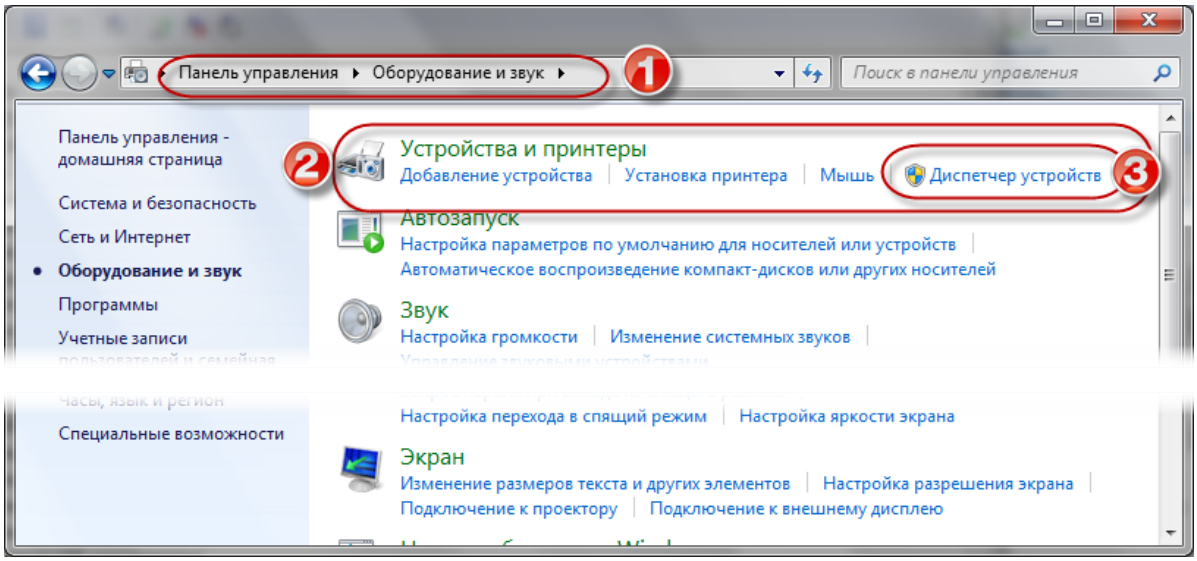


Рисунок 18 - Панель инструментов ОС Windows Home Premium. Пункт "Оборудование и звук"

9. Щелкните по названию одного из этих устройств правой кнопкой мыши и выберите пункт меню ***Обновить драйверы...*** в контекстном меню (см. рис. 19).

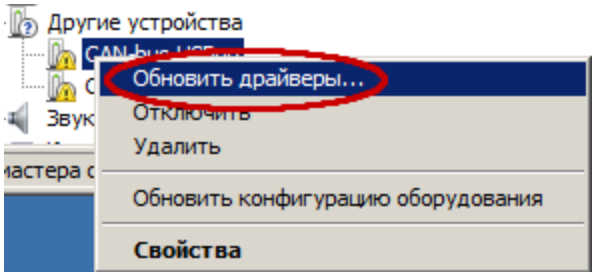


Рисунок 19 - Контекстное меню устройства

10. Выберите пункт ***Выполнить поиск драйверов на этом компьютере*** в открывшемся диалоге (см. рис. 20).

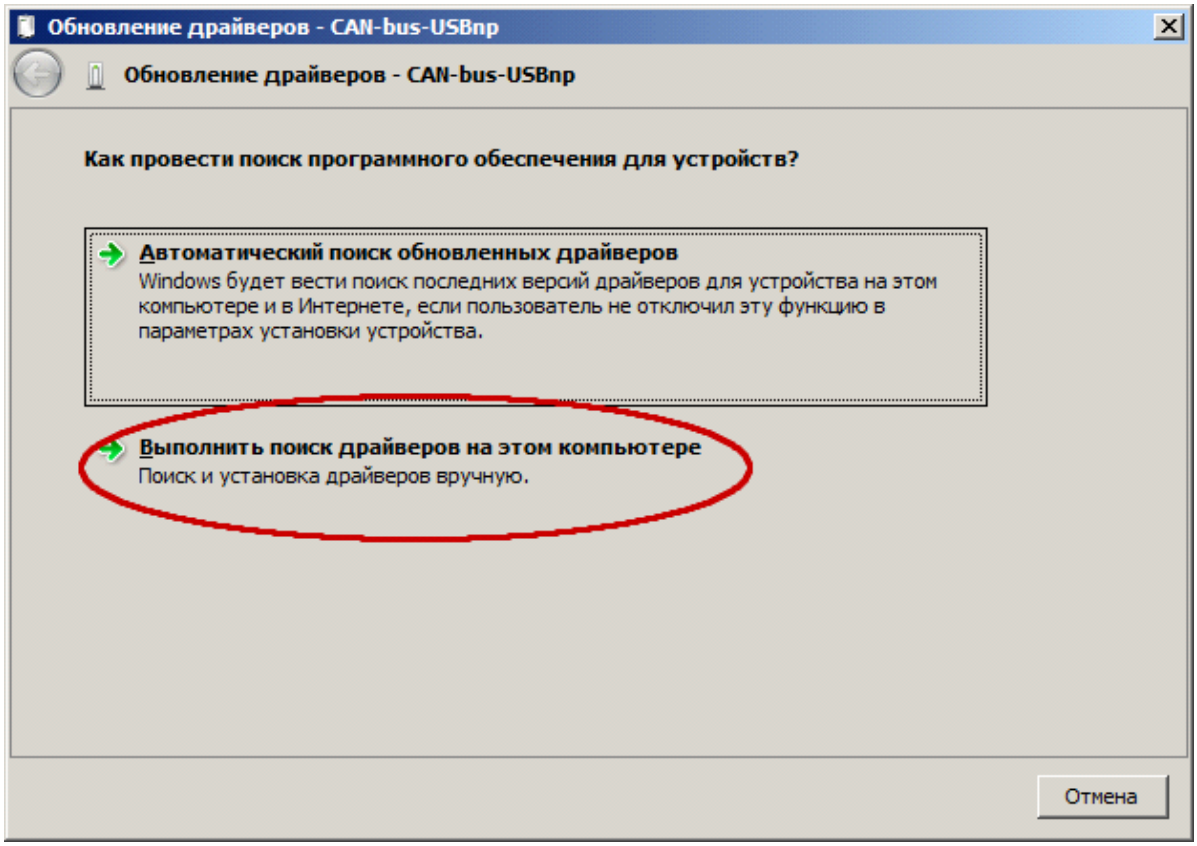


Рисунок 20 - Выбор способа обновления драйверов

11. Нажмите кнопку Обзор и выберите папку, в которую вы установили ПО Marathon (см. рис. 21).

По умолчанию это `C:\Program Files (x86)\CHAI-2.6.0`.

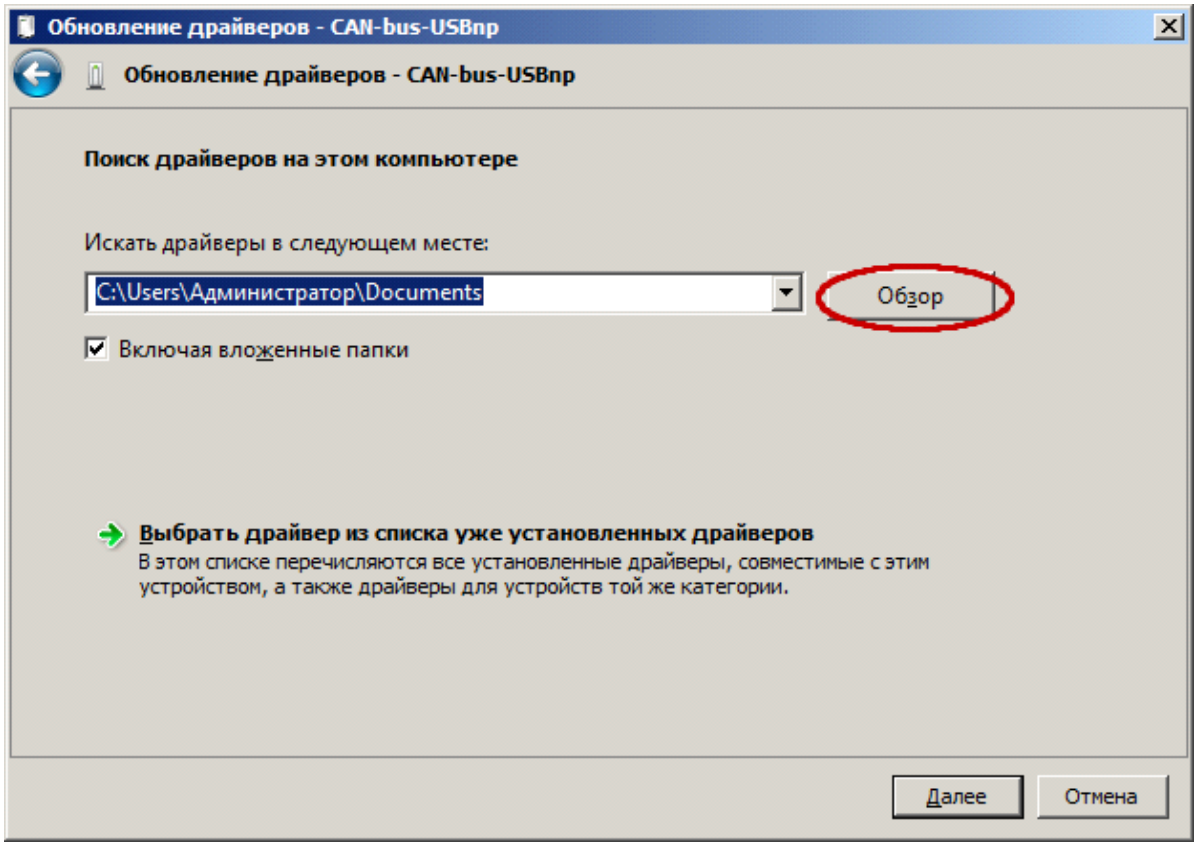


Рисунок 21 - Поиск драйверов

12. Убедитесь, что флаг ***Включая вложенные папки*** установлен, и нажмите на кнопку Далее >.

При установке драйвера отобразится предупреждение.

13. Выберите вариант ***Всё равно установить этот драйвер*** (см. рис. 22).

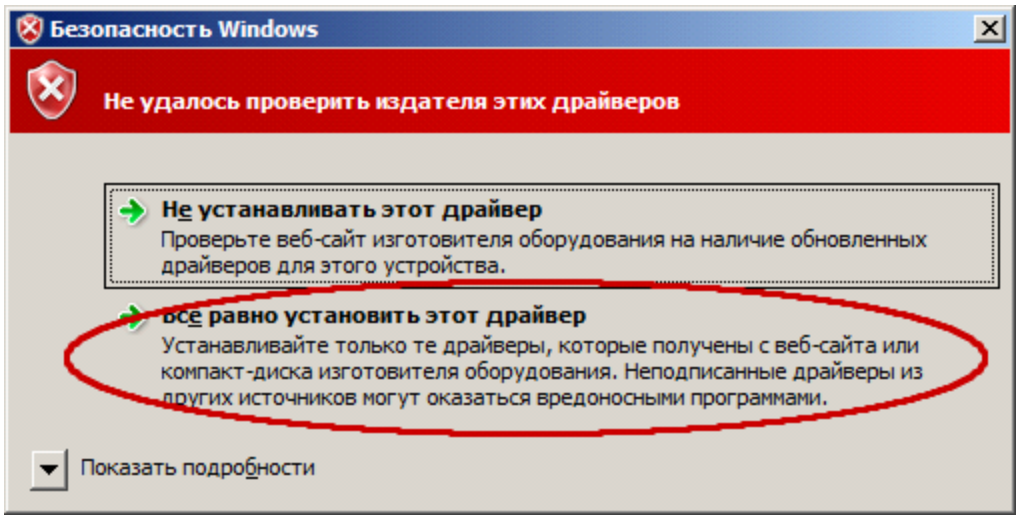


Рисунок 22 - Предупреждение системы

14. Убедитесь, что установка завершена успешно и нажмите на кнопку Закрыть.

В диспетчере устройств должно появиться устройство ***CAN-bus-USBnp interface*** в разделе ***Контроллеры USB*** (см. рис. 23). Теперь повторите шаги 9-14 для второго неизвестного устройства.

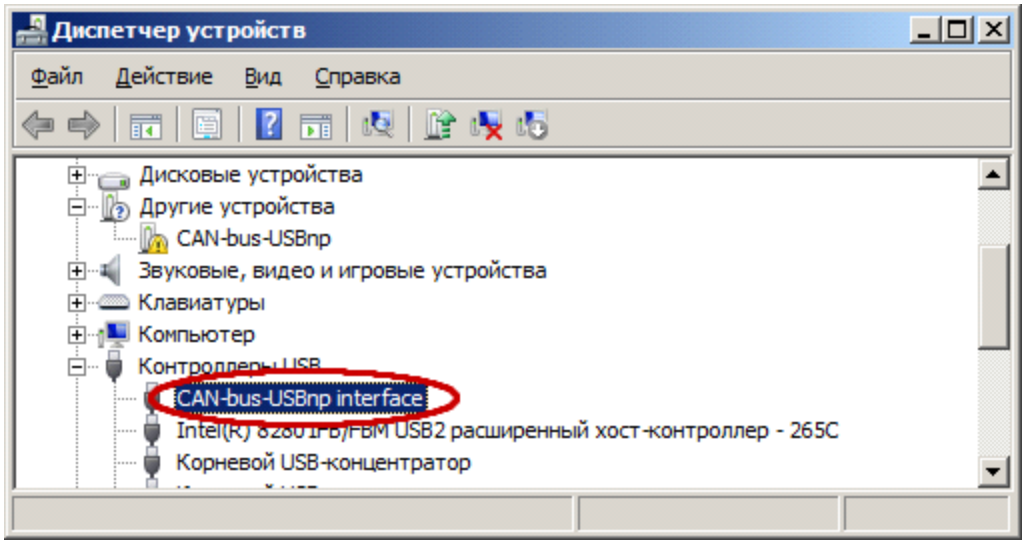


Рисунок 23 - Устройство в списке

Внимание: Для ОС Windows 8, 8.1, Windows 10, а также Windows 2012 Server необходимо до начала установки драйверов отключить обязательную проверку подлинности драйверов. Об отключении проверки подлинности см. здесь 411.

Подключение и настройка шлюза MOXA MGate MB3180

Для того чтобы подключить шлюз:

1. Выполните физическое подключение устройства.
2. Установите ПО для управления устройством. Для этого:
   i. Скачайте дистрибутив программы MGate Manager.
   ii. Разархивируйте дистрибутив и выполните установку ПО.
   iii. Запустите MGate Manager (см. рис. 24) и выполните настройку ПО.

Внимание: перед использованием, рекомендуется обновить прошивку шлюза до последней версии, для чего скачайте последнюю прошивку для MB3180 и через ПО MGate Manager выполните обновление прошивки (***Upgrade Firmware***).

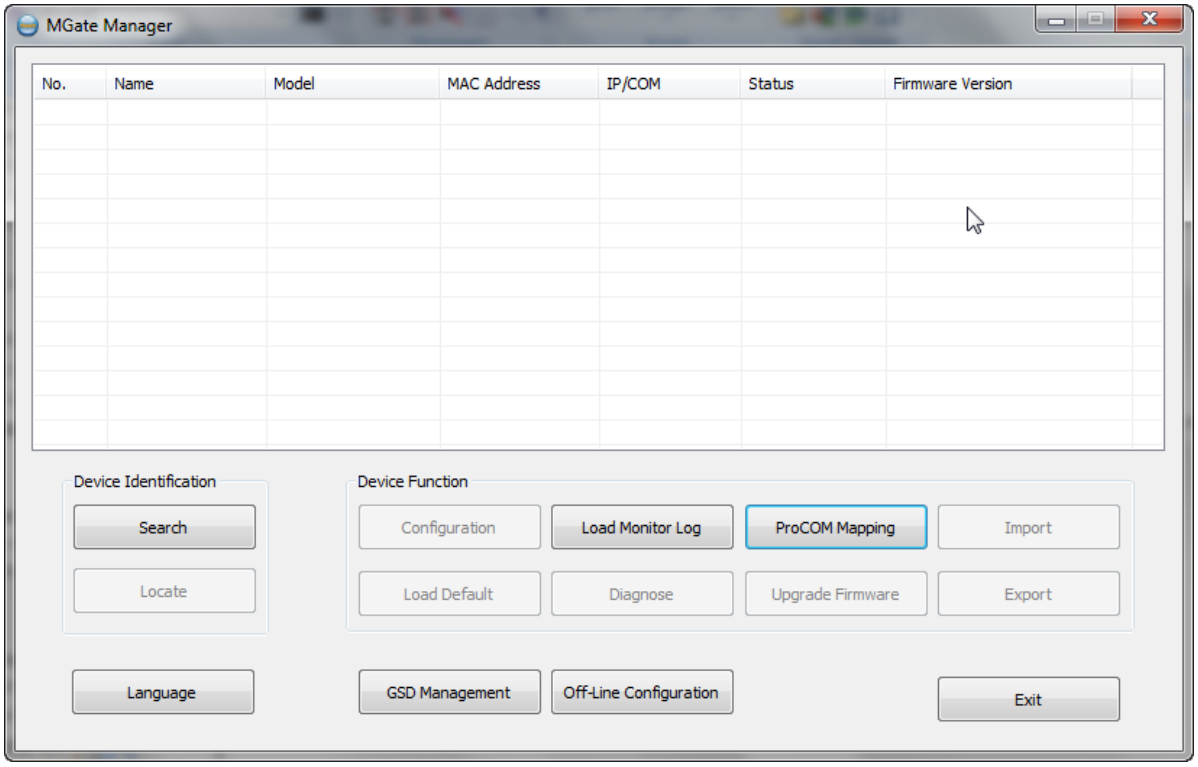


Рисунок 24 - MGate Manager. Вид по умолчанию при первом запуске

Настройка устройства

1. Выполните поиск устройств в сети командой ***Поиск*** (Search)
2. В диалоговом окне (см. рис. 25) осуществите широковещательный поиск всех подключенных устройств (***Поиск по сети***) или же укажите конкретный IP адрес устройства.

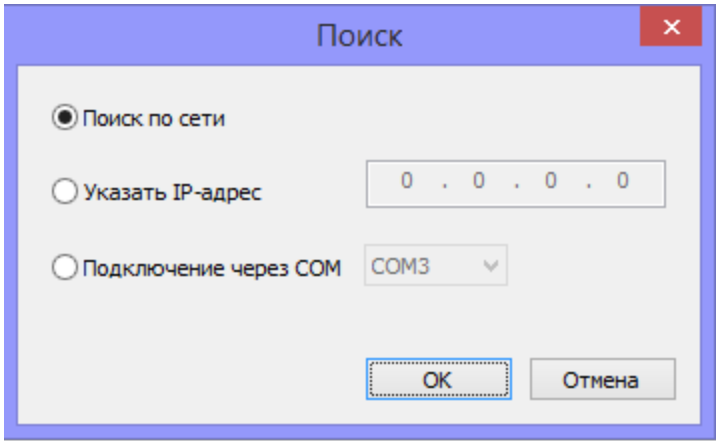


Рисунок 25 - MGate Manager. Диалоговое окно для поиска устройства

Если устройство найдено, его название отображается в главном окне программы.

3. Выберите устройство и на вкладке настройки сетевых параметров выставите IP адрес, маску и шлюз в соответствии с параметрами вашей сети. Нажмите на кнопку ***OK***.

Настройка режимов работы и обмена

После того как найдено устройство, необходимо выполнить его настройку.

Рекомендуются следующие параметры:

- Вкладка ***Режим работы > COM-порт > Порт 1 > RTU Slave*** (см. рис. 26);

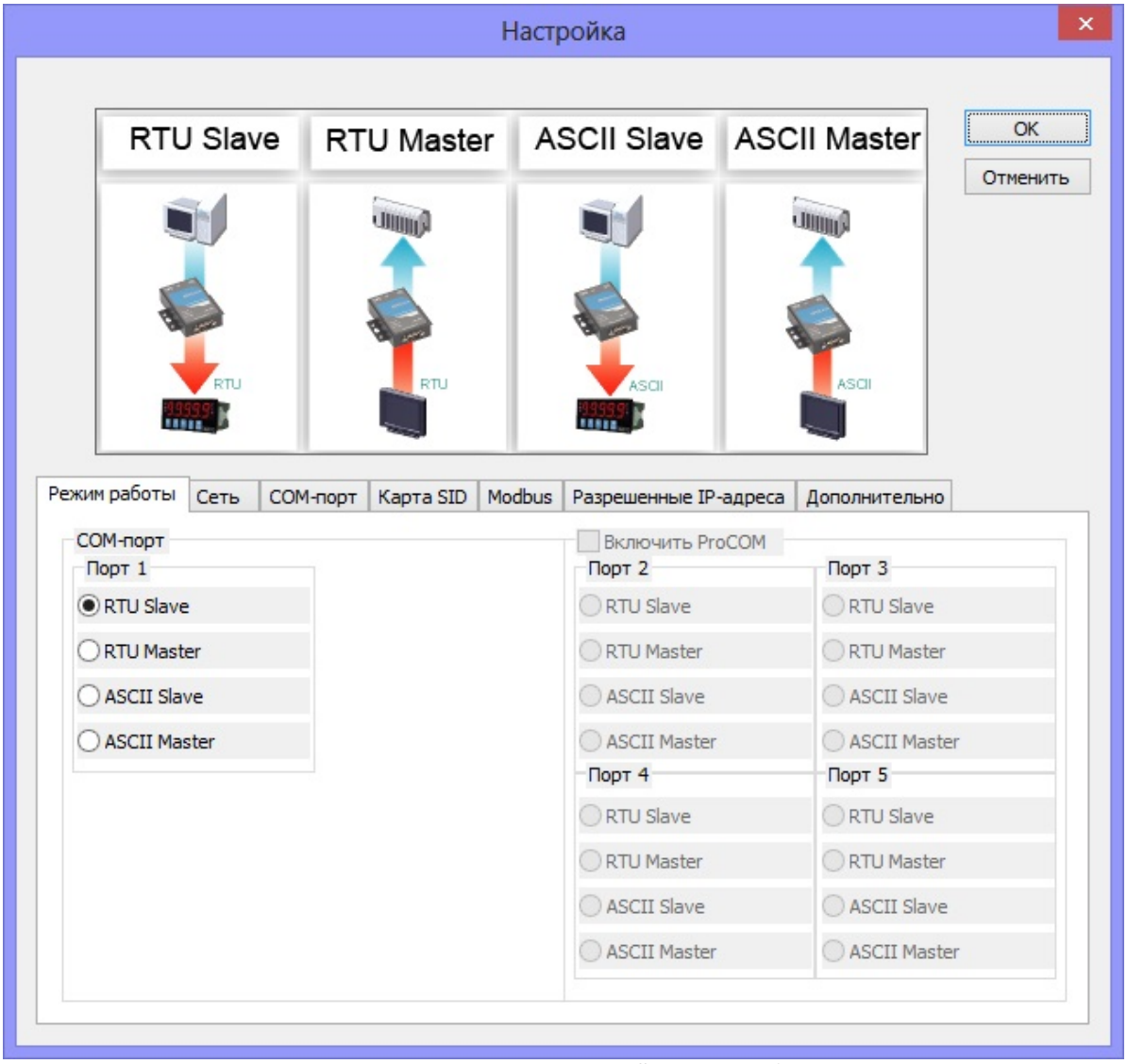


Рисунок 26 - MGate Manager. Настройка режима работы

- Вкладка ***COM-порт > скорость 9600*** (см. рис. 27);

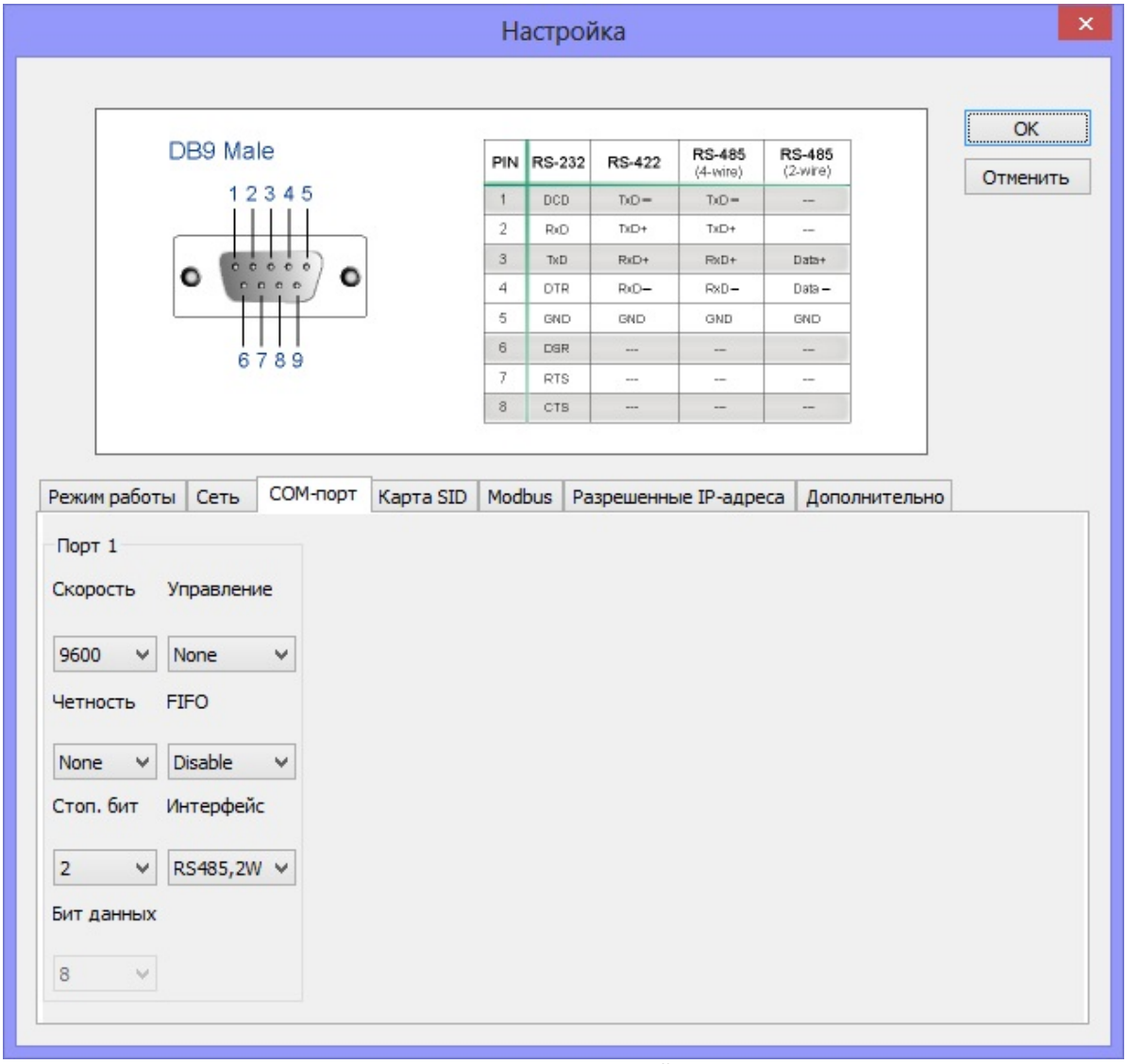


Рисунок 27 - MGate Manager. Настройка COM-порта

- На вкладке ***MODBUS*** рекомендуется выполнить автоматическую проверку наличия соединения. Для этого надо нажать на кнопку ***Автоматически***.

МОХА выполняет поиск подключенных к ней по MODBUS устройств (в данном случае С2000-ПП) по адресам (1 - 255) . Если устройство найдено успешно, данные о нем отображаются в нижней части вкладки и проставляется значение в поле ***Таймаут ответа*** .

Поле может быть заполнено вручную, но это не дает возможности проверить корректность соединения.

Подключение считывателя ZKTeco

Интеграция в систему RusGuard биометрических терминалов ZKTeco 7500, мирового лидера в области производства биометрических систем, позволяет строить высокотехнологичные комбинированные СКУД, работающие не тольк с RFID-картами, но и с биометрическими данными пользователя.

Для того чтобы подключить настольное устройство:

1. Установите драйвер устройства (дистрибутив поставляется вместе с ПО RusGuard и находится в папке Redistributables комплекта). Процедура схода с настройкой драйвера считывателя, описанной здесь 407.
2. Подключите устройство к компьютеру. Дождитесь подтверждения от системы, что устройство найдено.

Подключение сетевого биометрического считывателя

Для того чтобы подключить и настроить сетевое устройство (см. рис. 167) сначала необходимо установить на ПК программное обеспечение от ZKTeco. Оно поставляется вместе с ПО RusGuard (папка Redistributables дистрибутивного комплекта). Установка выполняется стандартным образом.

Внимание: Перед началом настройки убедитесь, что параметры физического устройства сброшены (установлены заводские настройки). Это требование связано с недоступностью функции широковещательного поиска для данного типа устройств и необходимостью исползовать стандартный IP-адрес. Процедура восстановления заводских настроек описана в инструкции к устройству.

Для настройки терминала необходимо:

- добавить его в ПО ZKAcess
- настроить функционирование в формате Wiegand 26
- настроить IP-адрес
- установить порог точности идентификации, если требуется

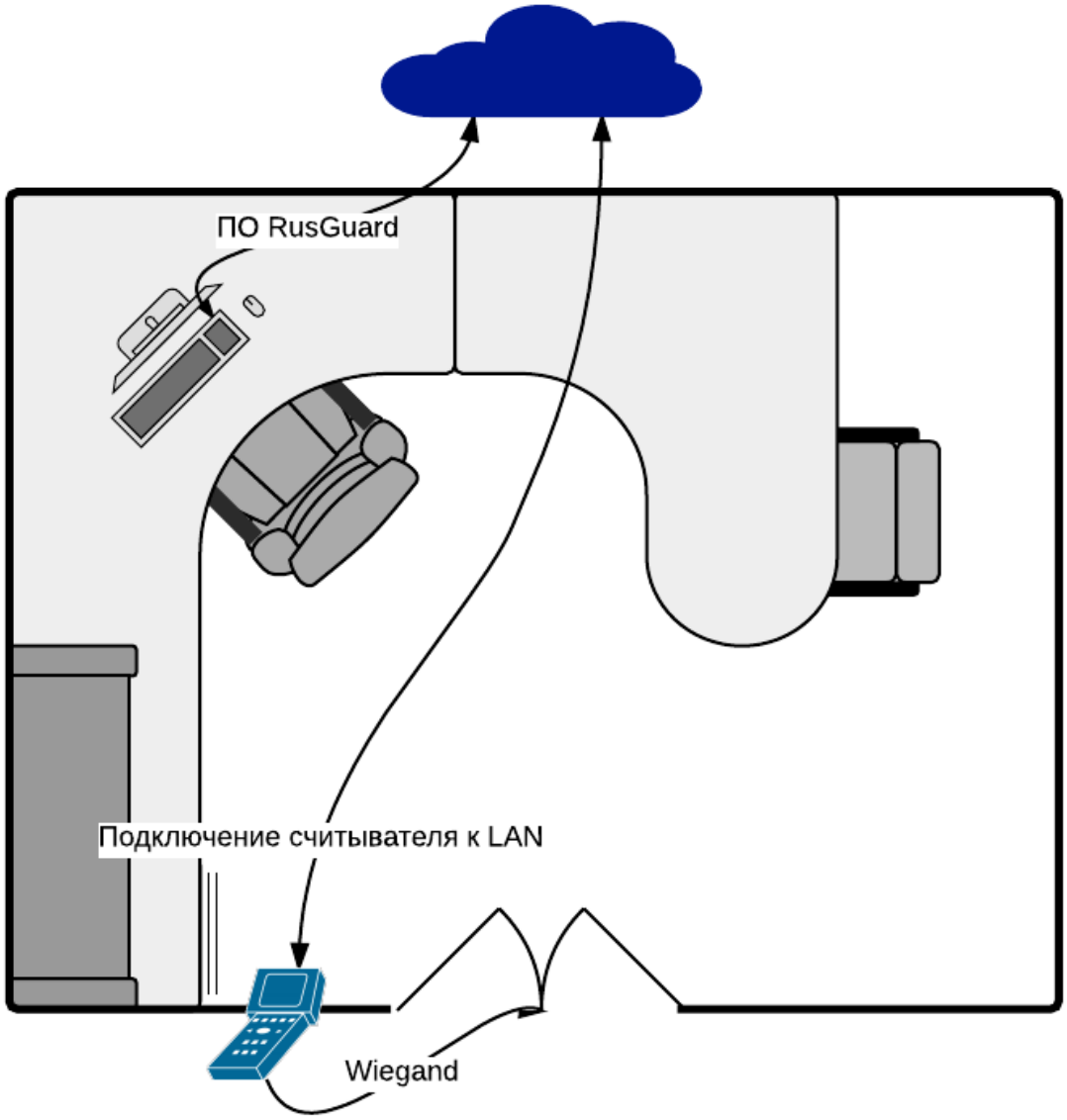


Рисунок 168 - Краткая схема подключения сетевого считывателя

Для того чтобы добавить устройство в ПО:

1. Включите устройство, дождитесь его инициализации.
2. Запустите ПО ZKTeco (ZKAcess). Введите логин и пароль (admin/admin) (см. рис. 168).

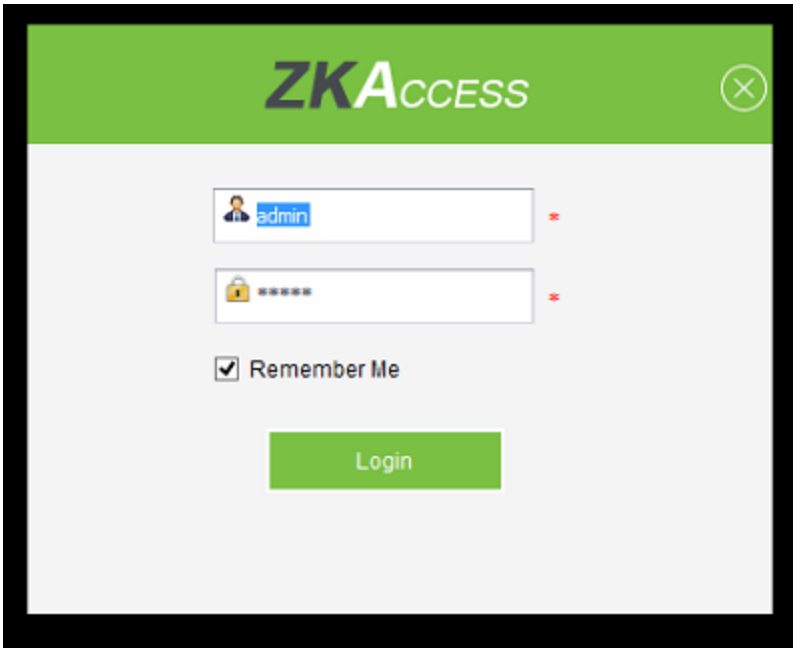


Рисунок 169 - ПО ZKAcess. Вход

3. Перейдите в раздел ***Device*** (см. рис. 169).

Рисунок 170 - ПО ZKAcess. Навигация в ПО

4. Нажмите на кнопку ***Add*** в верхней панели управления (см. рис. 170).

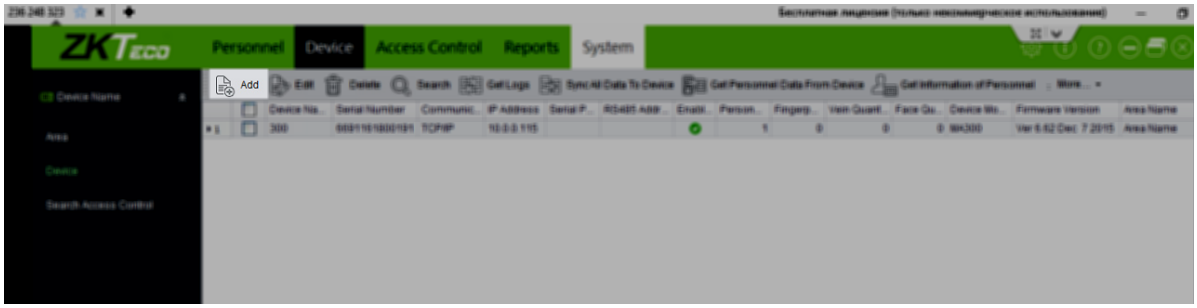


Рисунок 171 - ПО ZKAcess. Навигация в ПО

5. Следуйте инструкциям мастера настройки.
6. В шаге ***Communication settings*** введите IP-адрес по умолчанию: 192.162.1.201 (см. рис. 171).

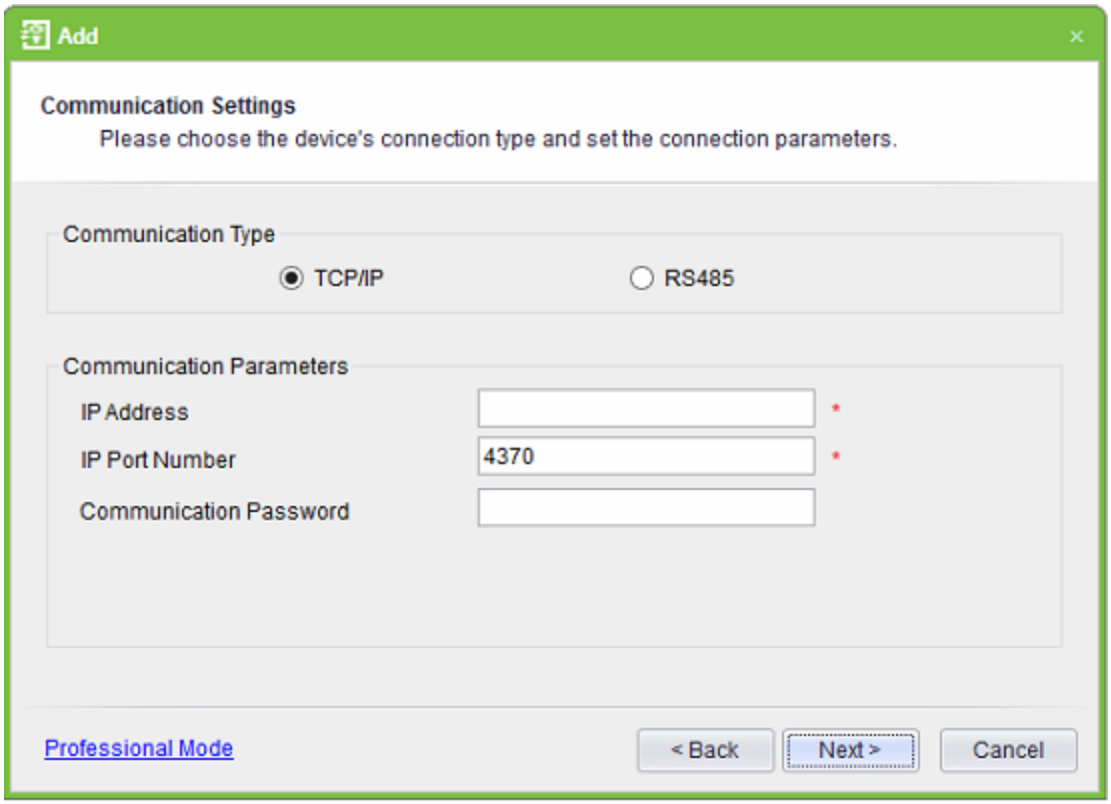


Рисунок 172 - ПО ZKAcess. Настройка IP-адреса

7. Когда мастер предложит выполнить очистку (Clear) устройства, рекомендуется согласиться и выполнить операцию (см. рис. 172).

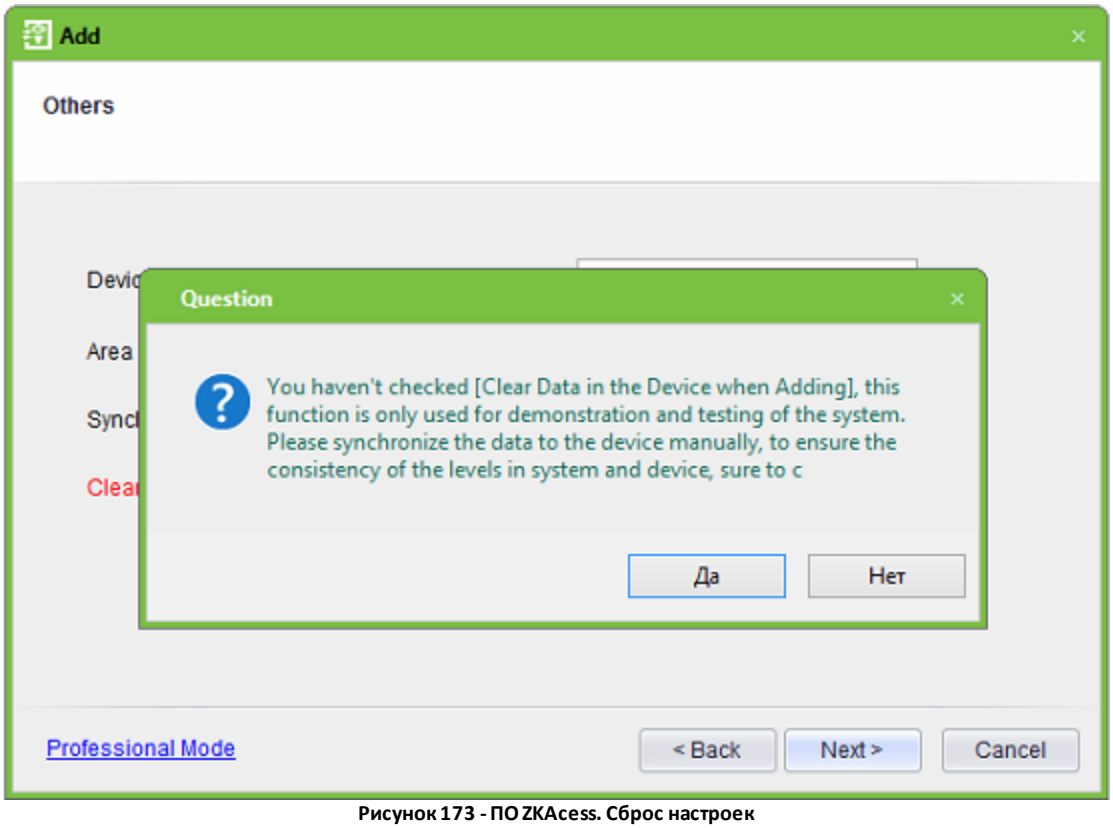


Рисунок 173 - ПО ZKAcess. Сброс настроек

8. Завершите процедуру добавления устройства. В случае успеха его название отобразится в списке.

Для того чтобы настроить функционирование в формате Wiegand:

1. Оставаясь в ПО ZKAcess, перейдите на вкладку ***Access Control*** в главном меню сверху.
2. Выберите пункт ***Door Settings*** в навигационной панели слева (см. рис. 173).

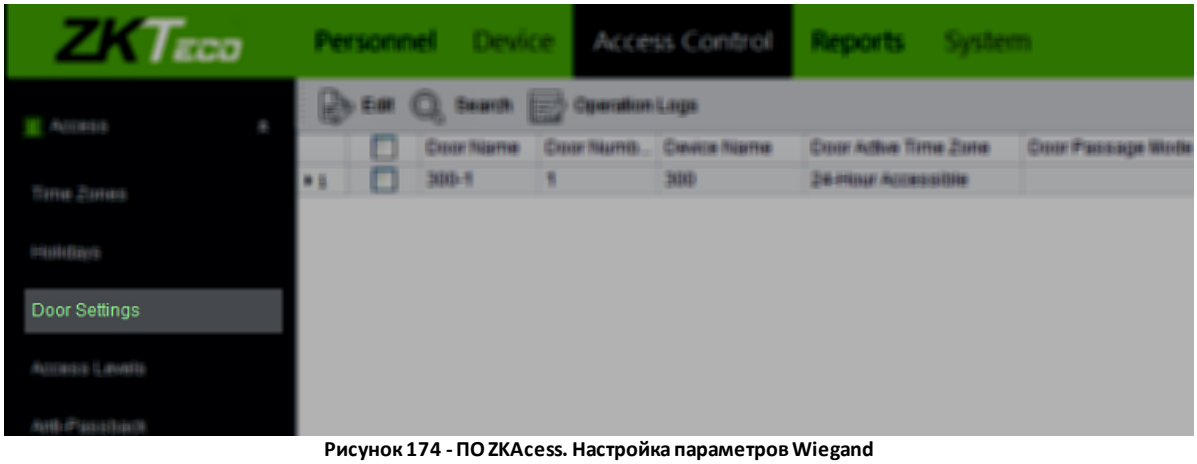


Рисунок 174 - ПО ZKAcess. Настройка параметров Wiegand

3. В открывшемся диалоге щелкните ссылку ***Wiegand Settings*** (см. рис. 174).

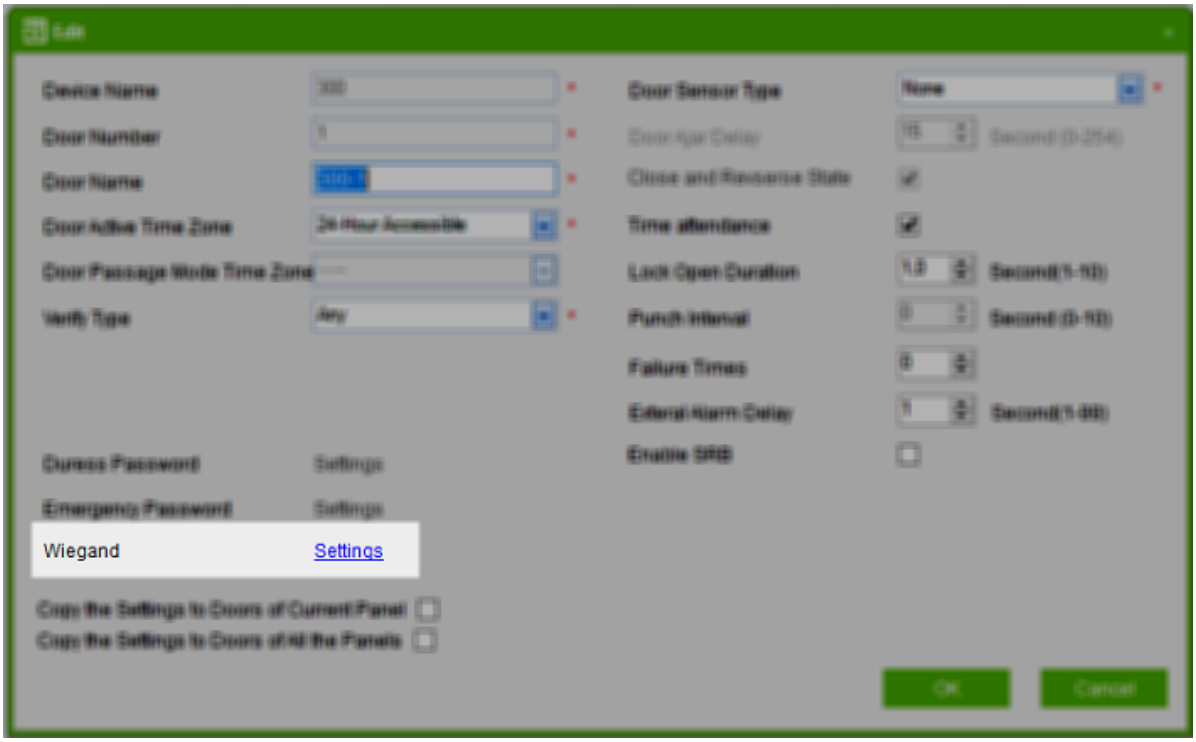


Рисунок 175 - ПО ZKAcess. Настройка параметров Wiegand

4. В следующем диалоге выберите параметр ***Card Number***, как показано на иллюстрации ниже (см. рис. 175). Сохраните настройки.

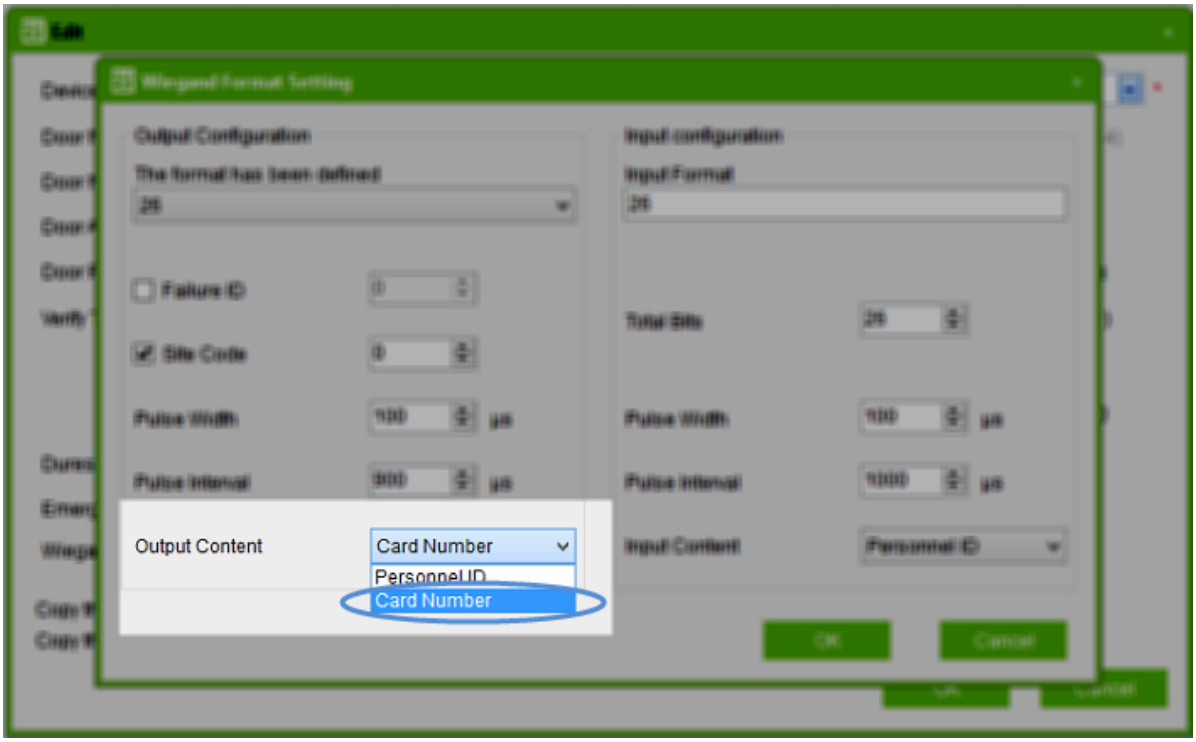


Рисунок 176 - ПО ZKAcess. Настройка параметров Wiegand

Для того чтобы настроить IP-адрес устройства:

Оставаясь в ПО ZKAcess, выберите добавленное устройство в списке на вкладке Device.

Раскройте пункт ***More*** верхней панели управления и выберите смену IP-адреса (см. рис. 176).

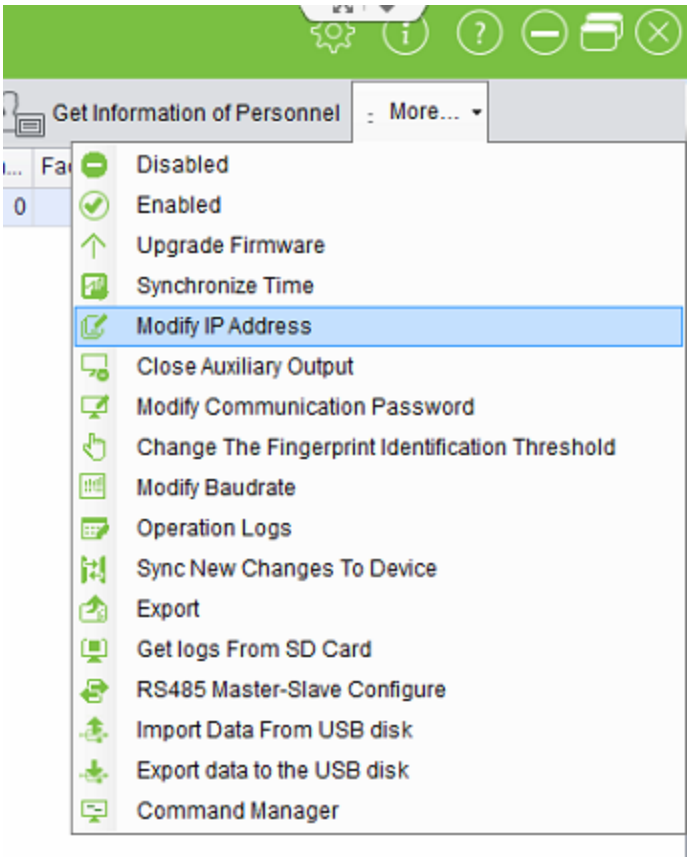


Рисунок 177 - ПО ZKAcess. Смена IP-адреса, пункт меню

Введите нужные параметры в диалоговом окне, которое откроется (см. рис. 177). Сохраните изменения.

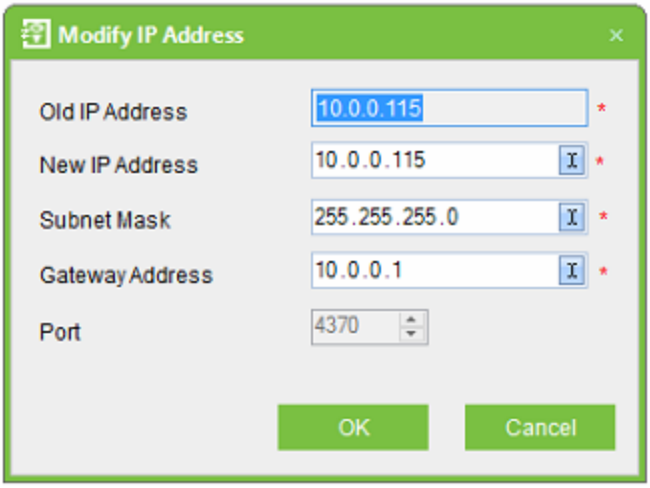


Рисунок 178 - ПО ZKAcess. Смена IP-адреса, диалог смены параметров

Для того чтобы изменить порог чувствительности устройства:

1. Оставаясь в ПО ZKAcess, вкладка ***Device***, выберите нужное устройство в списке настроенных.
2. Выберите функцию ***Edit*** (редактирование) в панели управления сверху или вызвав контекстное меню (см. рис. 178).

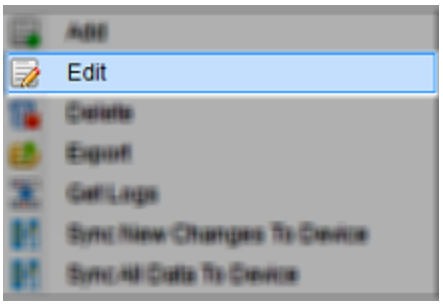


Рисунок 179 - ПО ZKAcess. Контекстное меню

3. Перейдите на закладку ***Verification and Protocol*** (см. рис. 179).

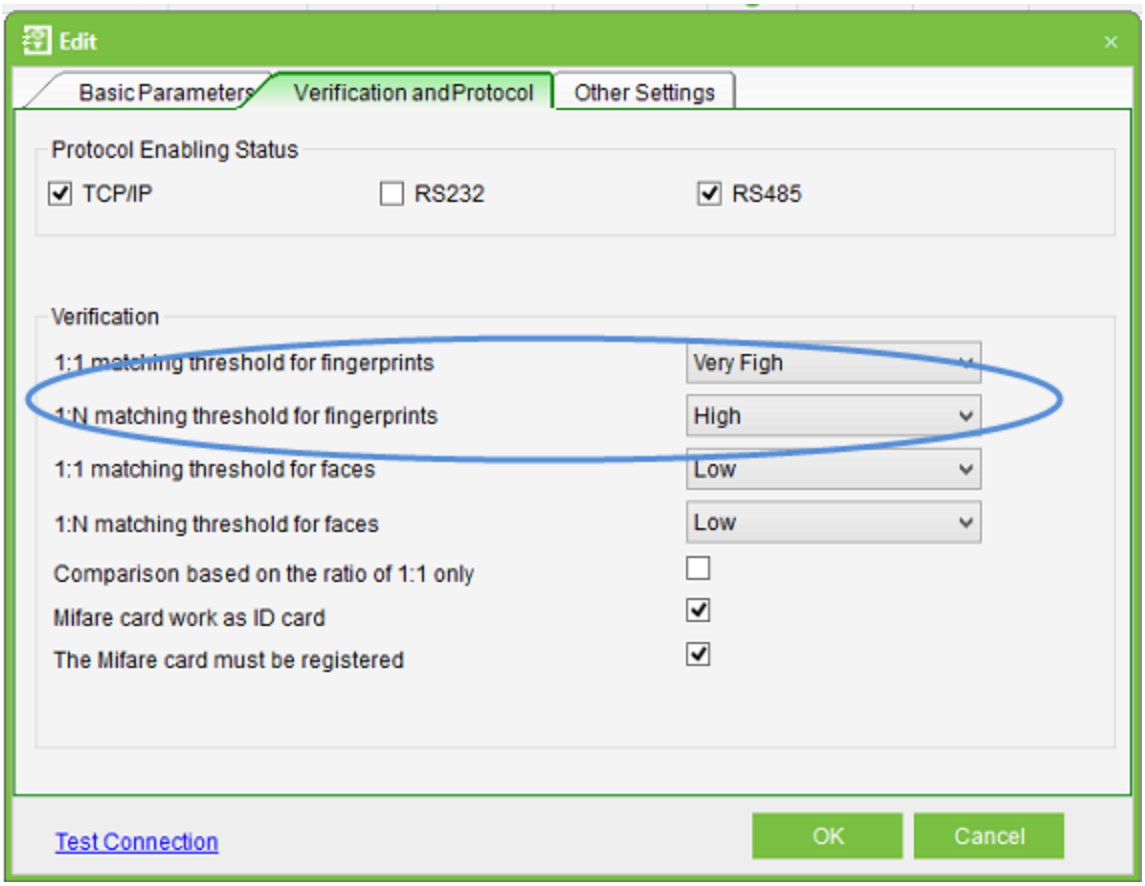


Рисунок 180 - ПО ZKAcess. Установка порога чувствительности

4. Установите нужный порог чувствительности для идентификации по отпечаткам пальцев (fingerprints). Сохраните изменения.
5. Перейдите на вкладку ***Other Settings*** и выберите версию считывания 10, как показано ниже (см. рис. 180). Сохраните настройки.

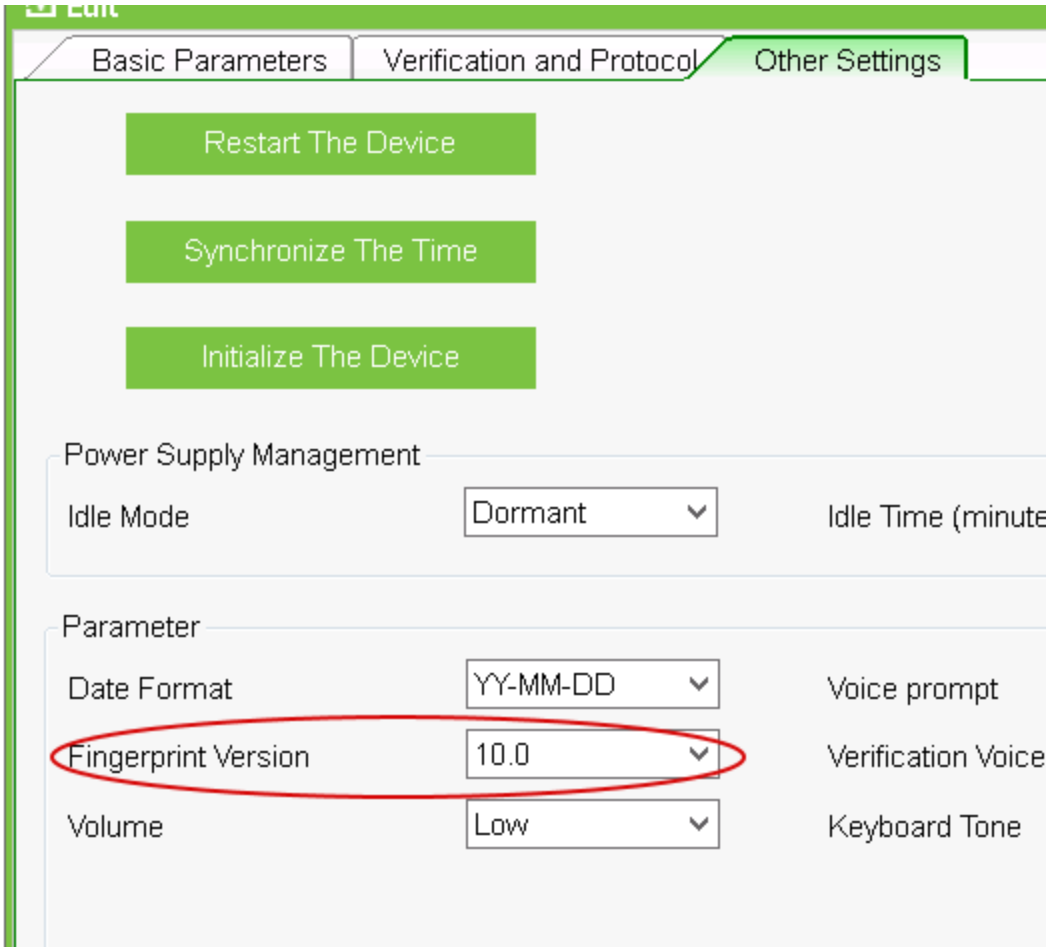


Рисунок 181 - ПО ZKAccess. Установка порога чувствительности

В дальнейшем вы сможете отредактировать настройки устройства, в том числе, в режиме оффлайн (синхронизация выполняется при подключении устройства к сети).

Описание процесса подлючения настольного устройства см. здесь 424.

Настройка контроллера ACS-102-CE (WF) с WiFi модулем MicRotic mAP2nD

Для того чтобы выполнить настройку контроллера ACS-102-CE (WF) с WiFi модулем MicRotic mAP2nD

1. Отключите LAN-порт модуля MicRotic mAP2nD (далее модуль) (см. рис. 181) от контроллера.
2. Отключите питание модуля.
3. Прижимая кнопку ***Reset***, подключите питание.Зажигается индикатор USR.
4. Дождитесь, чтобы индикатор начал мигать (индикатор AP\CAP не должен успеть загореться), отпустите кнопку ***Reset***.

Все индикаторы погаснут.

5. Дождитесь сброса модуля на заводские установки.

Рисунок 182 - Модуль MicRotic mAP2nD

6. Включите DHCP на порту LAN на ПК (см. рис. 182).

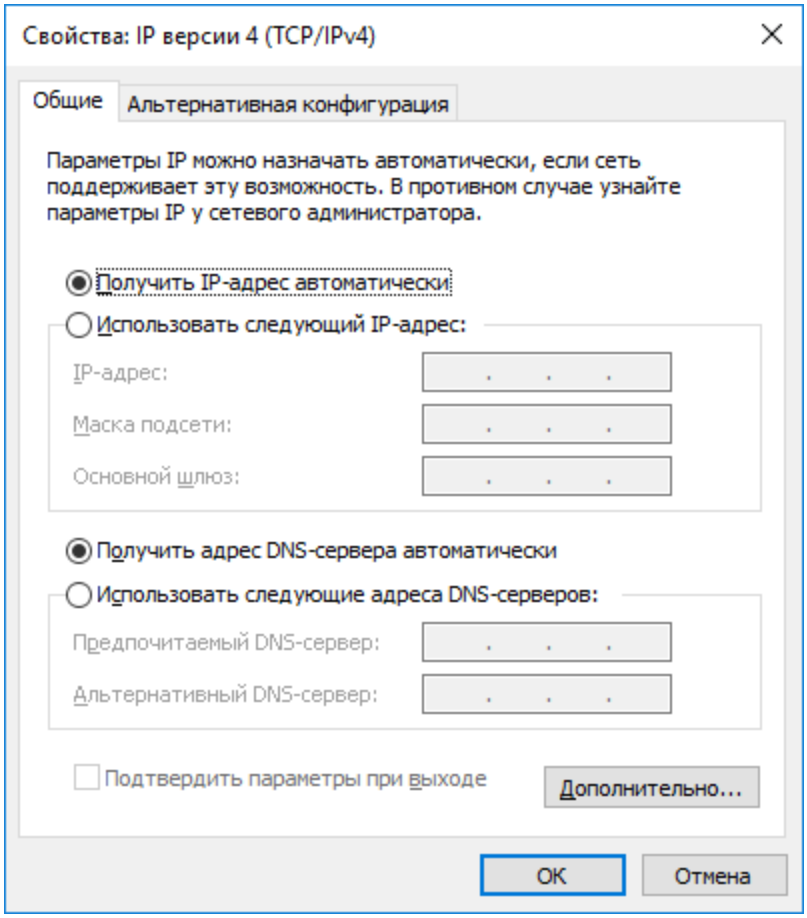


Рисунок 183 - Подключение к ПК. Настройка сетевых параметров

7. Подключите ПК к LAN порту модуля (порт Eth2). В панели ***Сетевые подключения*** можно проконтролировать обнаружение ПК DHCP сервера модуля (см. рис. 183) .

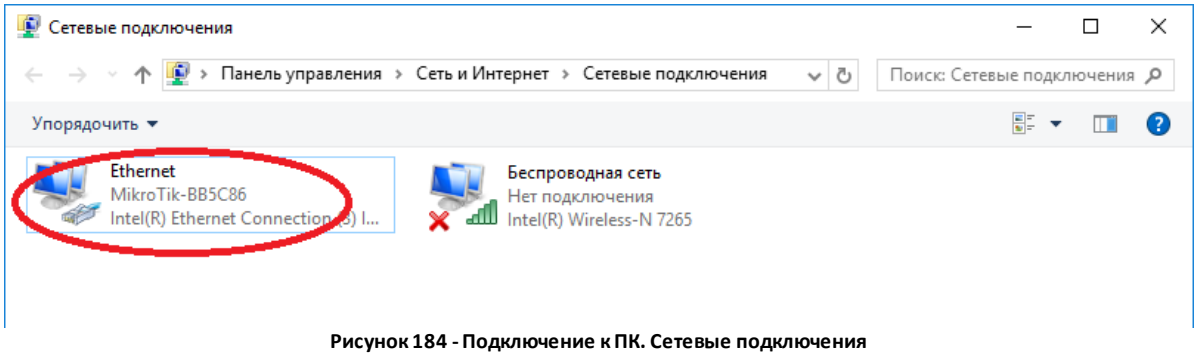


Рисунок 184 - Подключение к ПК. Сетевые подключения

8. Запустите программу WinBox. Найдите модуль (IP по умолчанию 192.168.88.1) и выполните подключение к нему (см. рис. 184) .

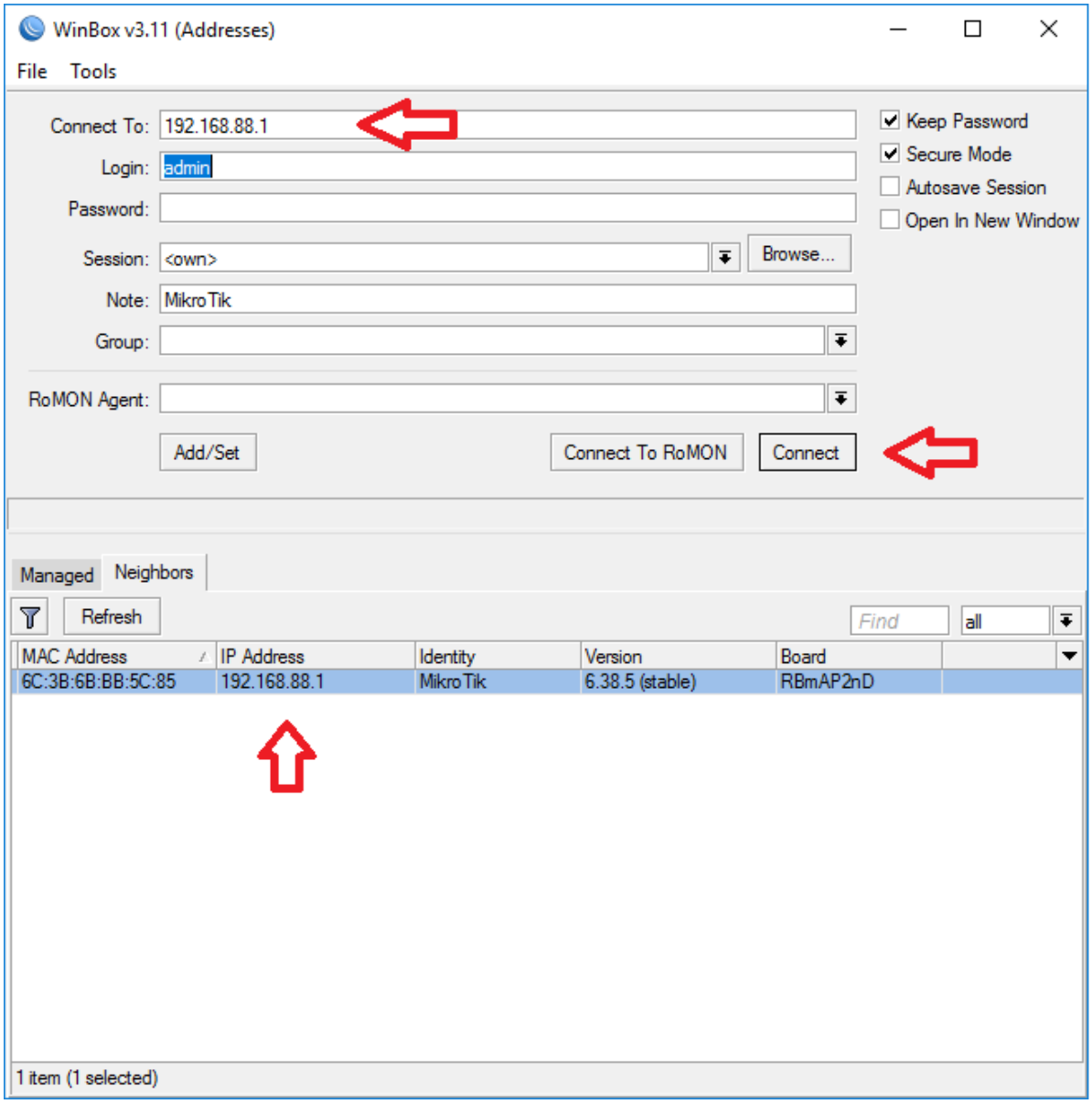


Рисунок 185 - Поиск в WinBox

9. Установите конфигурацию по умолчанию. Нажмите на кнопку ***OK*** в появившемся окне (см. рис. 185).

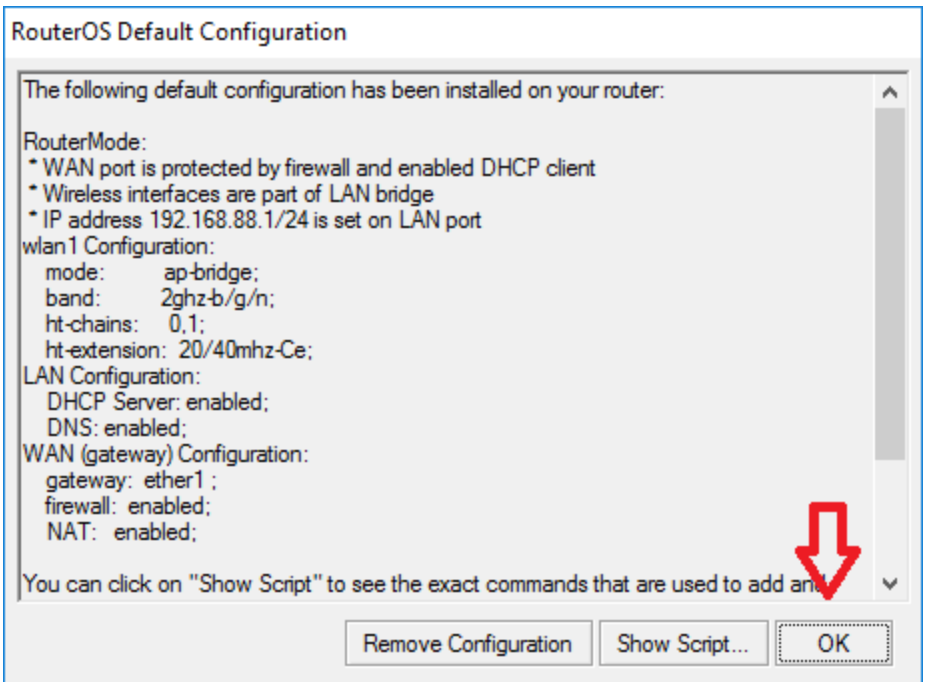


Рисунок 186 - Настройка конфигурации по умолчанию

10. Перейдите в меню ***Wireless >*** интерфейс ***Wlan1*** > вкладка ***Wireless***.
11. Измените значение поля ***MODE*** на ***STATION BRIDGE***. Нажмите на кнопку ***OK***, выйдите из ***Wireles tables*** (см. рис. 186).

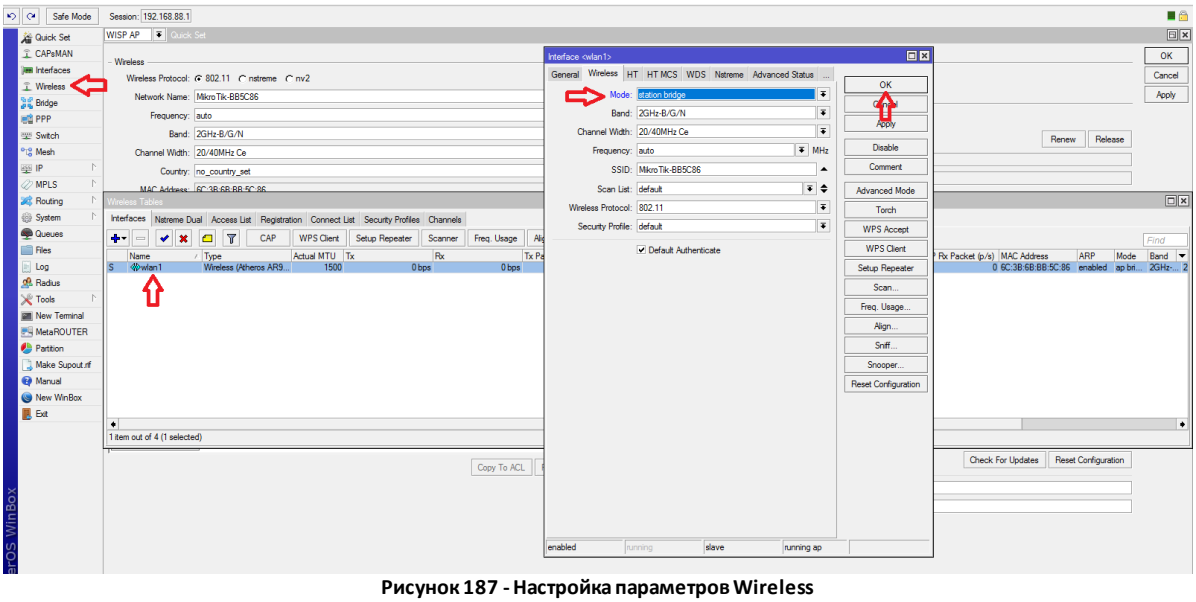


Рисунок 187 - Настройка параметров Wireless

12. В следующем окне нажмите на кнопку ***DISCONNECT*** (см. рис. 187).

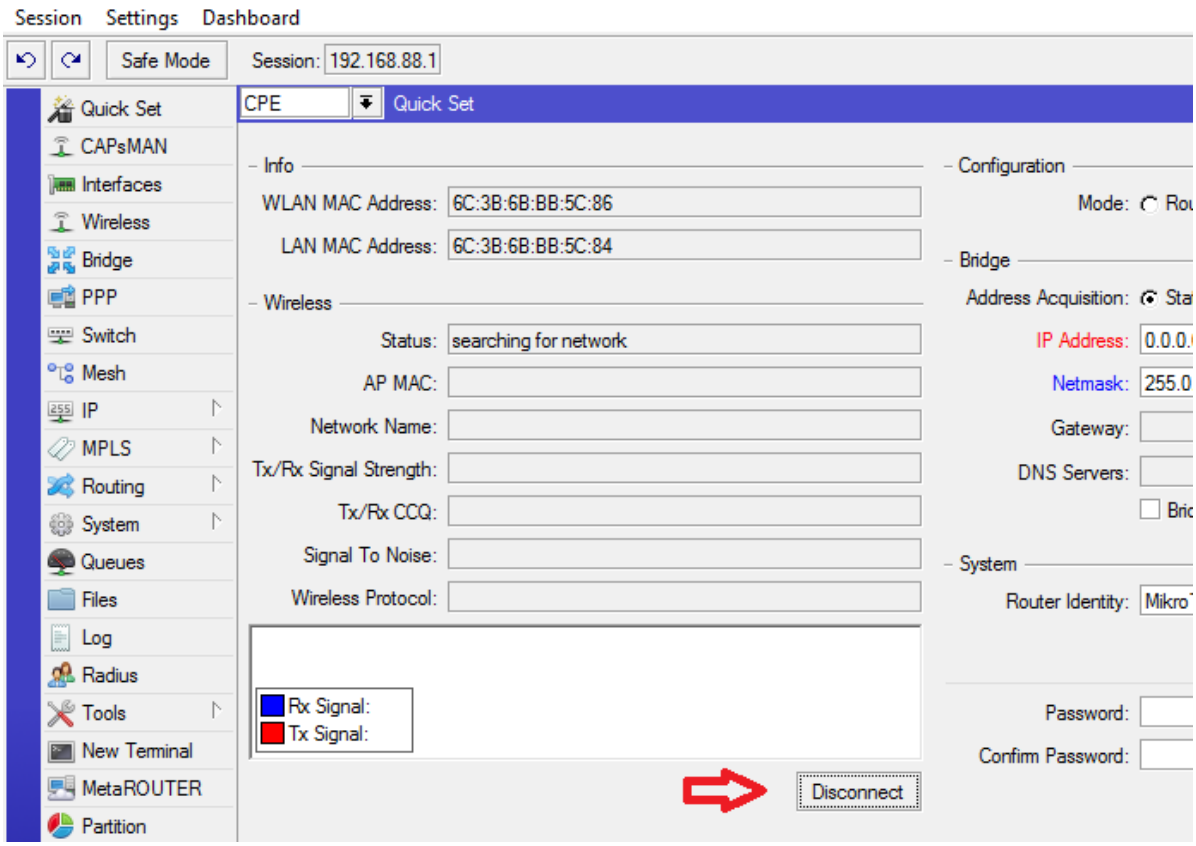


Рисунок 188 - Настройка параметров. Разрыв связи с сетью

13. Выберите нужную сеть, укажите пароль, нажмите на кнопку ***Connect*** (см. рис. 188).

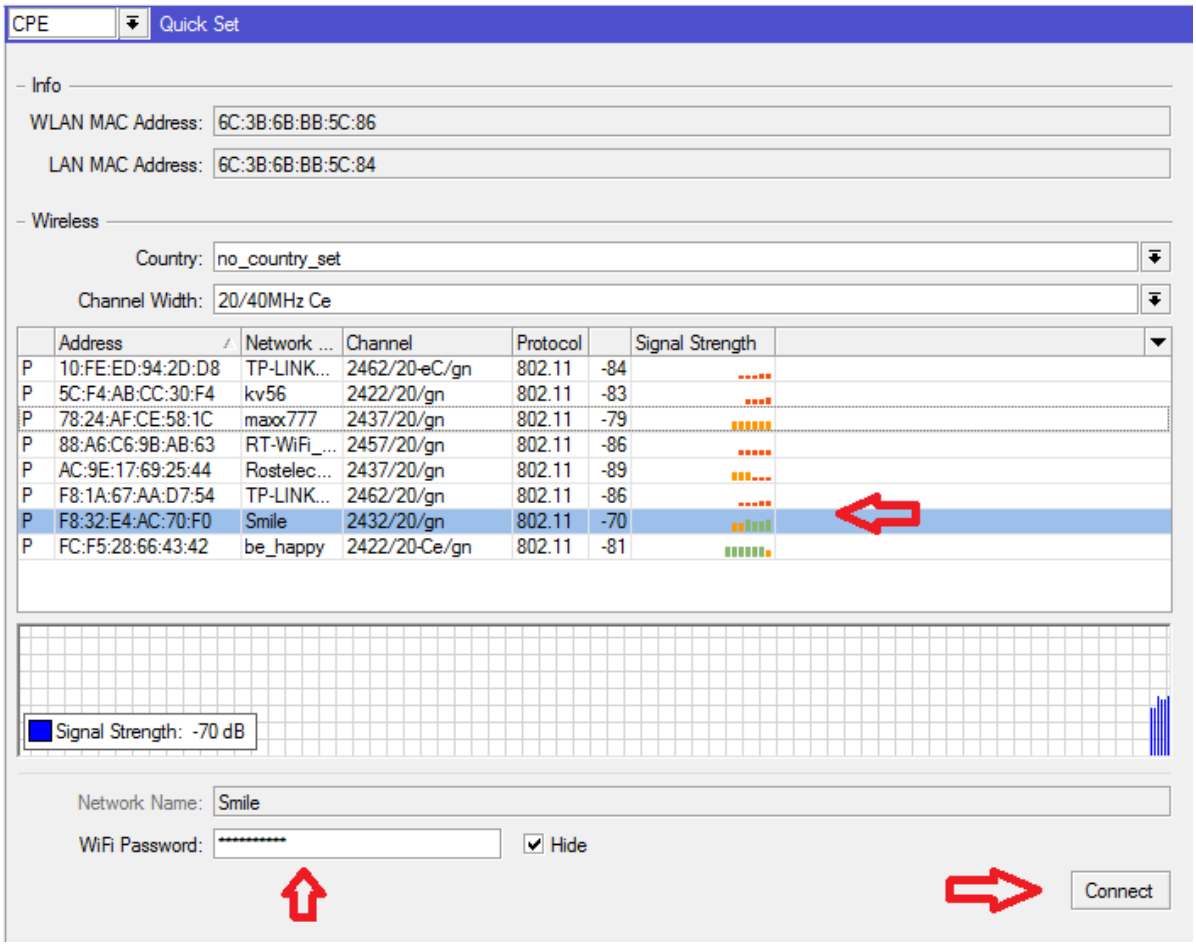


Рисунок 189 - Настройка параметров. Подключение к нужной сети

14. Проверьте правильность подключения (см. рис. 189).

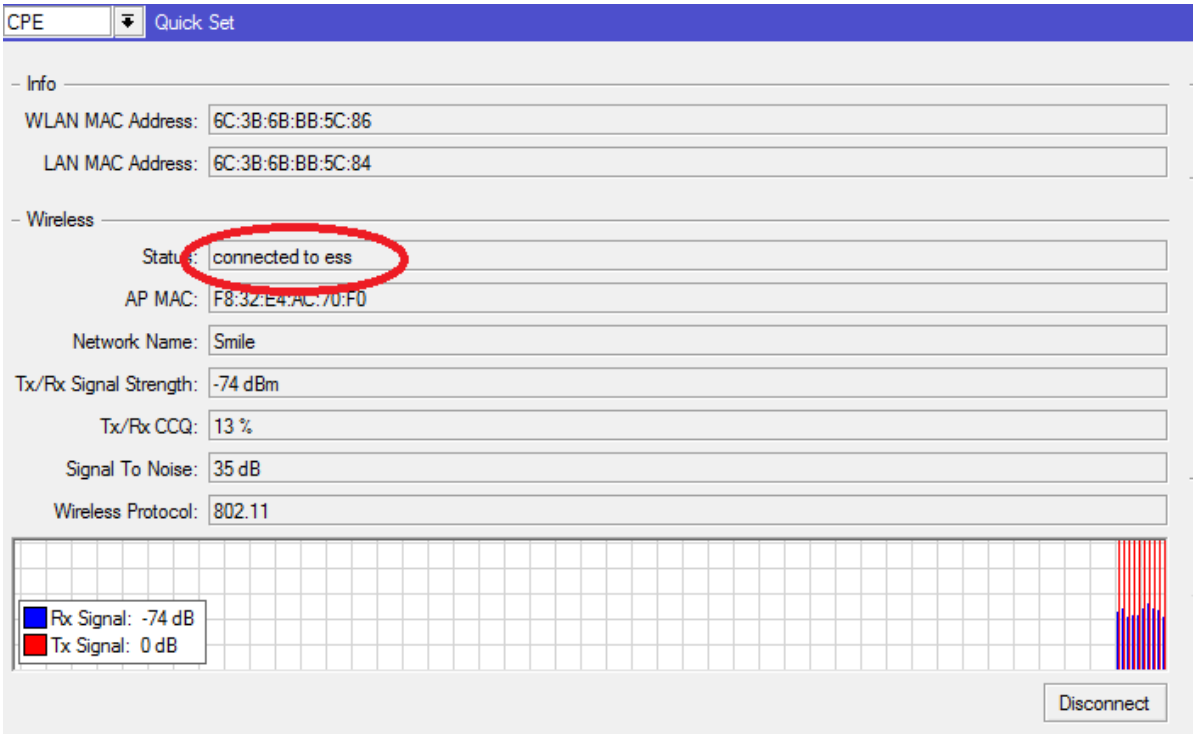


Рисунок 190 - Настройка параметров. Проверка подключения

15. Задайте IP и Netmask, рекомендуется выставить значения по умолчанию (192.168.88.1 \ 255.255.255.0) (см. рис. 190).
16. Установите флаг ***Bridge All LAN Ports***.
17. Примените настройки (***OK***).

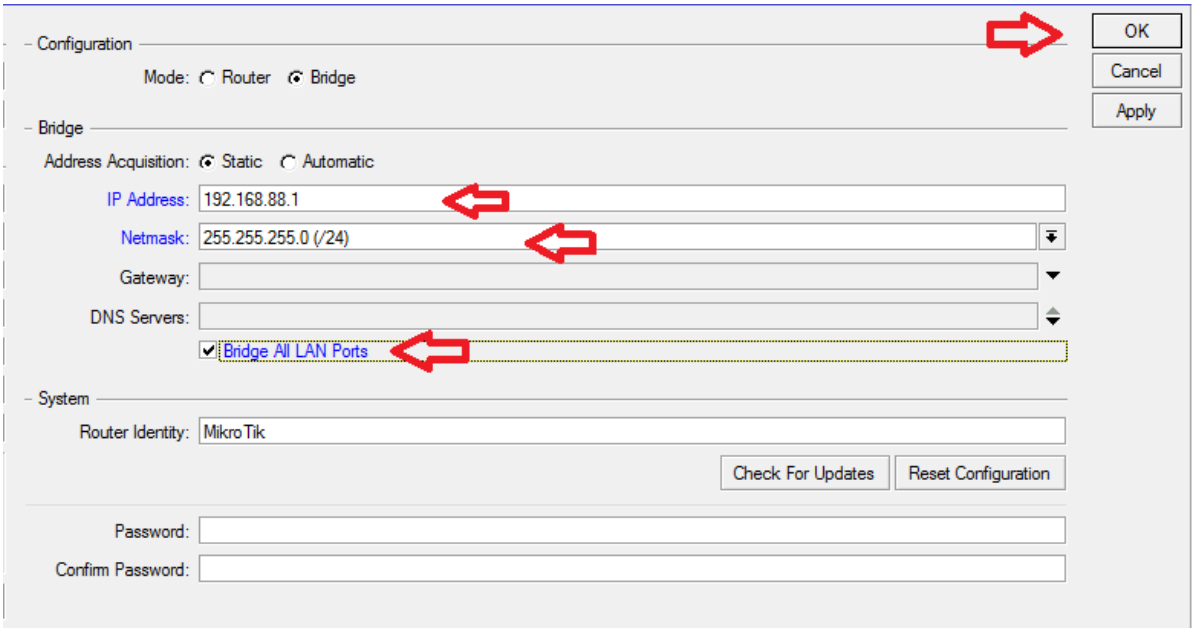


Рисунок 191 - Настройка сетевых параметров

18. В меню ***IP*** выберите ***Firewall***. Нажмите клавиши ***CTRL+A***, чтобы выделить все правила. Нажмите на кнопку удаления (см. рис. 191).

Удалятся все правила, кроме правила по умолчанию.

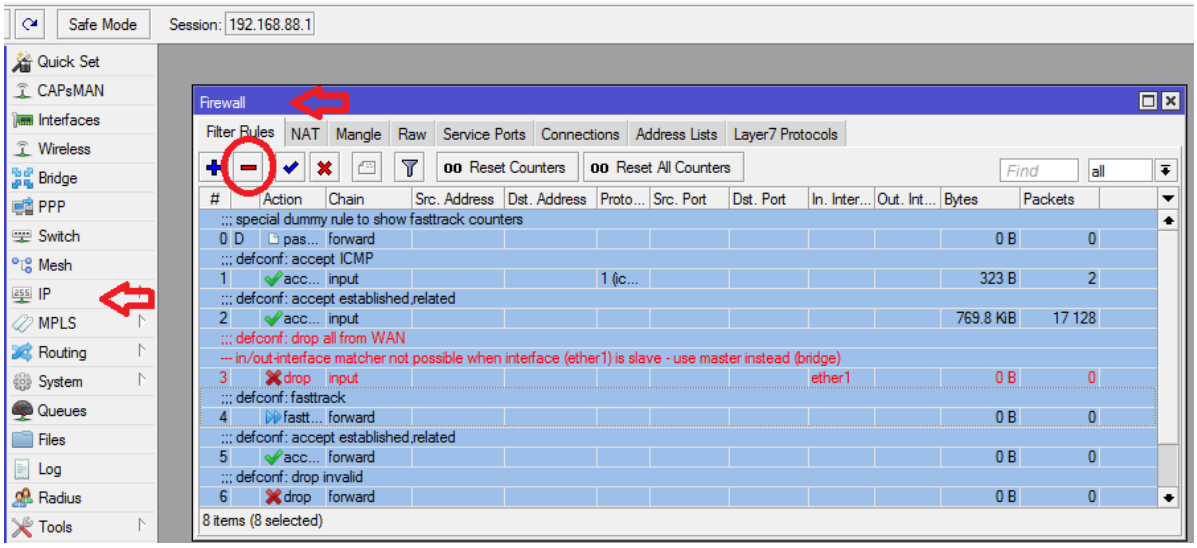


Рисунок 192 - Настройка правил Firewall (1)

19. На вкладке ***NAT*** нажмите клавиши ***CTRL+A***, чтобы выделить все правила. Запустите функцию удаления (см. рис. 192). Закройте окно.

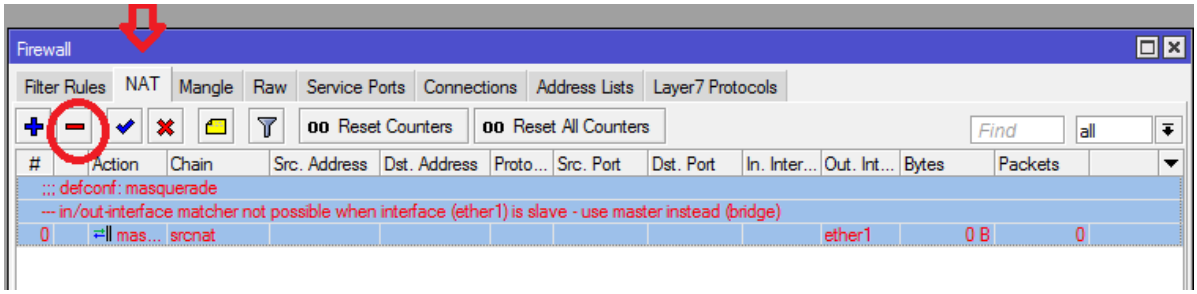


Рисунок 193 - Настройка правил Firewall (3)

20. В меню ***IP*** выберите ***DHCP SERVER***. Удалите запись (см. рис. 193).

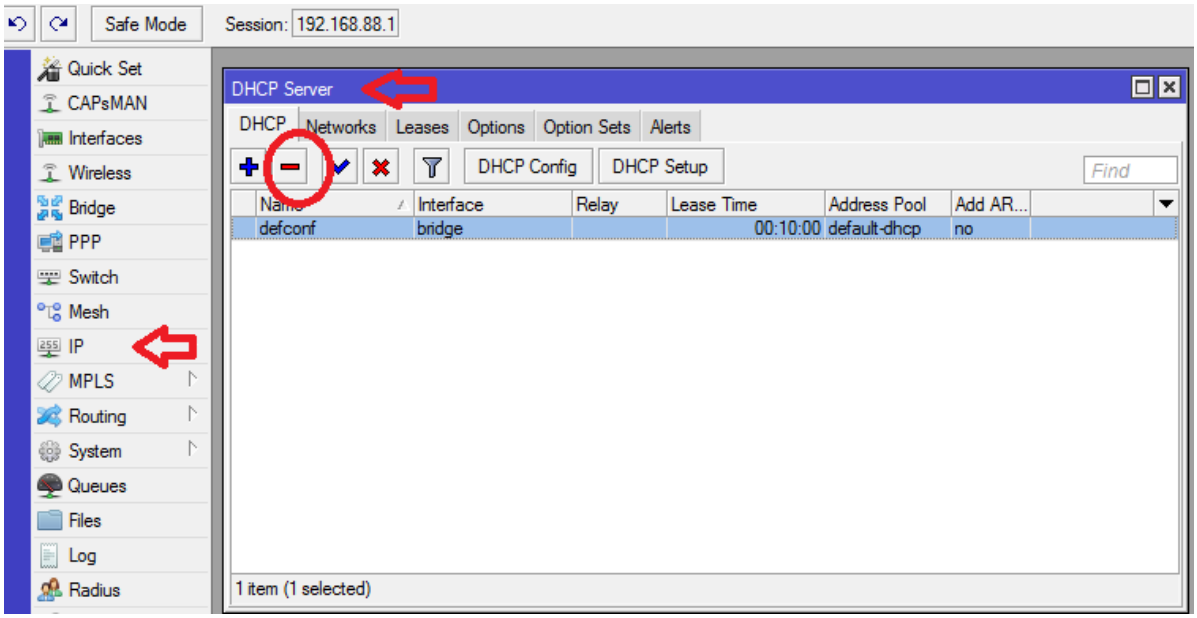


Рисунок 194 - Настройка DCHP

21. Закройте WinBox. Перейдите в свойства сетевого адаптера ПК и установите параметры IP адреса, маски подсети и шлюза, соответствующие параметрам выбранной WiFi сети.
22. Проверьте связь с сервером СКУД, убедитесь в отсутствии конфликтов IP адресов (уведомления в панели задач).
23. Отключите ПК от модуля, выполните подключение к контроллеру.
24. Через утилиту "Сетевые настройки" выполните поиск контроллера и настройте его параметры как в п. 21. Сохраните данные.
25. Отключите ПК от контроллера. Подключите контроллер к порту Eth2 модуля.
26. С сервера СКУД выполните проверку связи с контроллером по параметрам из п. 22.

Индекс

ABBYY PassportReader SDK 390
Antipassback 274

Bolid 363

Courier Mail Server 257

Gmail 128
Gmail.com 128
Google mail 128
Google почта 128

Mail.ru 128

Panasonic 389
Prog 363

Rbus 119
RusGuard агент. Сервер отчетов 307
RusGuard агент. Сервисы 302
RusGuard агент. Управление событиями 310

SQL-сервер не установлен 36
SQL-сервер установлен 39

Uprog 369

Windows Server 2008 R2 42
Windows Server 2012 42

Yadex mail 129
yahoo 128

Z-2 Usb: драйверы для настольного считывателя Z-2 USB – RG 27
ZKTeco 425
АПБ 274
АРМ RusGuard 76
Аудит действий операторов (отчет) 217
Биометрические данные 65
Биометрический считыватель 114
биометрический терминал 425
биометрия 114, 425
БИТ: Управление доступом (СКУД) 8. Синхронизация уровней доступа 397
БИТ: Управление доступом (СКУД). Синхронизация контроллеров 396
БИТ: Управление доступом (СКУД). Синхронизация помещений 397
БИТ: Управление доступом (СКУД). Синхронизация сотрудников 395
Блокировка сотрудника 141
Болид 363
Быстрый поиск 133
Быстрый старт 65
Варианты конфигурации 25
Варианты установки 25
Ведение базы адресов электронной почты, Ввод e-mail адресов 125
Ведение базы данных сотрудников 267
Ведение рабочих графиков 181
Ведение списка типов дней 178
Версия 1.1.0 18

Версия 1.2.0 17
Версия 1.3.0 17
Версия 1.4.0 16
Версия 1.5.0 15
Версия 1.6.0 13
Версия 1.7.0 13
Версия 1.7.1 13
Версия 1.7.2 12
Версия 1.8.0 12
Версия 1.9 12
Вкладка Лицензии 311
Возможности рабочего стола 42, 298
Восстановление 348
Вход без пароля 260
группам сотрудников 135
Дверь 93
Добавить метку 206
Добавление выходного или праздничного дня 150
Добавление меток к контроллеру 90
Добавление переноса 151
Доступ к отчетам через web-интерфейс 275
Загрузка изображения в карточку сотрудника 144
здесь 401
Изменение уровня доступа сотрудника 137
Изменено имя компьютера 262
Интеграция личного кабинета Ivideon 386
Интеграция с ISS 402
Интеграция с видеоригстраторами Panasonic 389
Интеграция с ИСО "Орион" 363
Интеграция с ПО "Болид" 363
Интеграция сервера Ivideon с АРМ 384
Интеграция учетной записи Ivideon с АРМ 384
Интерфейс АРМ RusGuard 76
Использование лицензии 389
Использование Сервера Отчетов 214
Как настроить длину кода ключа 178
Как обратиться в службу поддержки 361
Как создать рабочее место 156
Как создать учетную запись оператора АРМ 264, 265
Картотека сотрудников 219
Кириллическое имя компьютера 286
Код ключа 178
Контакты службы поддержки 362
Контроль посещаемости 221
Конфигурация SQL-сервера 54
Конфигурация нового устройства 86
Конфликт версий ПО и БД 356
Координаты службы поддержки 362
Кто прописан в контроллер (отчет) 220
Лицензии 311
Лицензии, агент 311
Лицензионного соглашения 6
Лицензирование 389
Локальный просмотр сервера Ivideon 382
Метки 206
Модуль "Отчеты" 214
Модуль Конфигурация рабочих мест 155
Модуль Конфигурация СКУД 135
Модуль Статистика 252
Модуль Фотоидентификация 248
Настройка Courier Mail Server 259
Настройка GSM-модема 129
Настройка автозапуска 260
Настройка автоматического удаления событий 311
Настройка выполнения программы (действия) 204
Настройка длины кода ключа 178
Настройка дополнительных IP-адресов для контроллеров 318
Настройка доступа к АРМ через ярлык 260
Настройка записи видео (действия) 203
Настройка мобильных приложений 169
Настройка модуля Фотоидентификация в рабочем месте 163
Настройка нового события 195
Настройка отправки Email (действия) 202
Настройка отправки SMS (действия) 201
Настройка пароля кофигуратора сетевых насроек 319
Настройка почты 127
Настройка прав релейного доступа 115
Настройка принятия решения оператором 167
Настройка рабочих графиков 181
Настройка расписаний реакций 193
Настройка распознавания документов (Конфигурация рабочих мест) 168
Настройка рассылки 127
Настройка Реакций 194
Настройка режима Запрета повторного входа 274
Настройка сервера отчетов 55
Настройка сетевого терминала ZKTeco 425
Настройка срока действия уровня доступа 137
Настройка точки доступа 152
Настройки графиков работы 184, 185, 186

Настройки контроллера 88
Не удается зайти на сервер отчетов 295
Некорректное отображение отработанного времени 297
Нет прав доступа на сервер отчетов 295
Новое имя компьютера 262
Обновление версии БД 356
Обновление ПО 356
Обновление прошивки контроллера 331
Обращение в службу поддержки 361
Оперативное развертывание программного комплекса 65
Опоздания 226
Основные варианты конфигурации 25
Основные варианты установки 26
Особенности настройки профиля Mifare 211
Особенности установки 42
Отключение проверки подлинности 411
Отпечатки пальцев 65
Отработанное время 228, 297
Отработанное время (расширенный) 229
Ошибка АРМ 292
Ошибка настройки времени 293
Ошибка при запуске модуля Отчеты 294
Ошибка при запуске ПО 293
Ошибка репозитория 299
Ошибка репозитория драйверов 298
Ошибка серверных служб 299
Ошибки АРМ 293
Ошибки версий от 1.8 298, 299
Ошибки настроек SQL-сервера 294
Ошибки сервера 293
Ошибки сервера отчетов 286
Ошибки установки 286
Ошибки. Сервер недоступен 292
Параметры по умолчанию на Сервере Отчетов 214
Пароль 319
Пароль доступа к настройкам контроллера 318
Перемещение сотрудника в БД 142
Печать пропусков 281
Поддержка 361
Подключение считывающего устройства 407
Подключение шлюза MOXA MGate MB3180 363
Поиск сотрудника в БД 141
Поиск устройств по имени 133
Почта на gmail.com 128
Почта на mail.ru 128
Почта на yahoo 128
Почта на мейлру 128
Почта на Яндексе 129
Привязка меток к группам сотрудников 135
Привязка меток к точкам доступа 113
Привязка прав релейного доступа к уровню доступа 117
Привязка расписаний к точке доступа 152
Привязка точки доступа у уровню доступа. Быстрый старт 67
Примеры настройки графиков работы 186
Примеры рабочих графиков 186
Присвоение уровня доступа группе. Быстрый старт 69
Проблемы установки 286
Пропуска 207
Просмотр состояния точек доступа 154
Работа в модуле Фотоидентификация 248
Рабочие зоны 190
Разграничение доступа при помощи меток 262
Расписание на день 148
Расписание на неделю 149
Расписание на определенную дату 148
Расписание на сутки 147
Распознавание данных с отсканированных копий документов 145
Распределенная конфигурация 292
Реакция. Запись видео на камеру Ivideon, Запись видео на камеру Ivideon 285
Редактирование CAN-адреса 85, 325
Редактирование количества фотографий 314
Редактирование набора полей карточки сотрудника 313
Редактирование уровня доступа. Метки 153
Резервное копирование 348
Синхронизация контроллеров с БД 86
Синхронизация нового устройства с БД 86
Синхронизация с БД 86
Синхронизация событий (1С) 397
Системные события (отчет) 230
Системные требования 8
Скачать полный пакет ПО RusGuard Soft 6
Смена статуса всех точек на плане 243
Снятие биометрических данных сотрудника 65
Создание группы пользователей 172
Создание группы сотрудников 69
Создание действия 199
Создание должности. Быстрый старт 69
Создание новой реакции 194

Создание рабочего места 156
Создание расписания реакции 193
Создание сотрудника в группе. Быстрый старт 70
Создание уровня доступа. Быстрый старт 67
Создание учетной записи пользователя 176
Создание шаблонов пропусков 207
Создать расписание на день 148
Создать суточное расписание 147
Состав дистрибутива 27
Состав дистрибутива RusGuard 27
Состав программного комплекса 27
Состав программного комплекса RusGuard 27
Срок действия уровня доступа 137
Стандартные элементы интерфейса АРМ 77
Статистика проходов 222
Считывающее устройство 407
Табель Т-13 233
Табло посетителей 255
Термины 23
Типы дней 178
Типы конфигурации 25
Типы отчетов 214
Точка доступа типа "дверь" 93
Требования по установке 29
Удаление 353
Удаление событий вручную 310
Управление доступом к зонам 190
УРВ 226, 233
Условия установки 29
Установка ABBYY PassportReader 390
Установка SQL-сервера 48
Установка АРМ RusGuard 61
Установка драйвера на ОС Windows 8, Windows 2012 Server 411
Установка драйверов для USB-ключа модуля ABBYY PassportReader SDK 391
Установка сервера 31
Установка сервера RusGuard 31
Установка утилит RusGuard 61
Уход раньше времени 235
Учетная запись оператора АРМ 264, 265
Фильтрация отчета Приход-уход 218, 220, 221, 223
Формула: учет рабочего времени 401
Шаблон отчетов, Управление шаблонами отчетов, Удалить отчет 236
Шаблоны пропусков 207, 281
Шкафы/Витрины 115
Яндекс 129
яха 128