АПК «Бастион-2». Руководство администратора

Версия 2.1.12 (Oracle / PostgreSQL)

(15.12.2021)

Содержание

1 Общие сведения

1.1 Назначение этого документа

Этот документ предназначен для инсталляторов АПК «Бастион-2», а также для персонала, ответственного за его администрирование и техническое обслуживание. Рассматриваются вопросы установки, настройки и технического обслуживания системы в целом. Сведения о работе со вспомогательными программами рассмотрены в отдельных инструкциях на эти программы. Сведения о конфигурировании драйверов находятся в инструкциях на соответствующий драйвер.

Для лучшего понимания работы системы рекомендуется ознакомиться с полным комплектом документации на модули, используемые в конкретной системе. С правилами комплектации можно ознакомиться в документе «Правила комплектации АПК «Бастион-2».

Подразумевается, что администратор системы обладает, по крайней мере, начальными знаниями в следующих областях:

- Интегрированные системы безопасности;
- Установка и настройка используемых операционных систем;
- Протокол TCP/IP и администрирование компьютерных сетей;
- Администрирование СУБД Oracle или PostgreSQL (в зависимости от версии АПК «Бастион-2»).

1.2 Назначение и область применения системы

Аппаратно-программный комплекс **(АПК) «Бастион-2»** предназначен для интеграции в единую систему безопасности следующих подсистем:

- видеонаблюдения и/или видеорегистрации;
- охранно-пожарной сигнализации (ОПС);
- систем охраны периметра;
- систем охранного освещения;
- систем контроля и управления доступом (СКУД).

АПК «Бастион-2» позволяет создавать единую систему безопасности объекта с возможностью объединенного мониторинга, управления подсистемами и их автоматической взаимосвязью.

АПК «Бастион-2» обладает распределенной архитектурой, что позволяет использовать его одинаково эффективно на объектах разного масштаба: от небольших офисов до крупных предприятий с развитой филиальной сетью.

АПК «Бастион-2» позволяет объединять системы безопасности территориально удаленных объектов, обеспечивая централизованный мониторинг событий, управление приборами, удаленное видеонаблюдение, а также синхронизацию данных об электронных пропусках между объектами (филиалами) одного предприятия и управление личными данными сотрудников.

АПК «Бастион-2» может быть использован как часть системы управления предприятием, если интегрировать его в информационную среду компании. Используемые технологии позволяют обеспечить интеграцию с кадровыми и бухгалтерскими системами, использовать данные системы в ситуационных центрах и других сторонних системах управления.

Несколько территориально распределенных объектов с АПК «Бастион-2» можно объединить, используя системы «Бастион-2-Репликация» и «Бастион-2-ПЦН». При этом каждый объект будет работать со своей базой данных АПК «Бастион-2».

1.3 Общая структура системы

Компьютерная сеть АПК «Бастион-2» включает в себя следующие функциональные узлы (см. Рис. 1):

Сервер баз данных (БД). Здесь хранится вся информация о конфигурации системы. Сервер БД всегда один на весь комплекс. Этот компьютер должен работать в круглосуточном режиме, так как доступ к базе данных необходим для работы всех подсистем комплекса. В качестве СУБД используется Oracle 11g.

Сервер системы – центральный модуль системы, всегда один на систему. Выполняет функции проверки активации модулей, полномочий пользователей, управления выполнением сценариев и реакций на события, синхронизации времени и ряд других системных функций.

Серверы оборудования – один или несколько компьютеров (не ограничено программным способом), к которым выполняется подключение подсистем безопасности. Число драйверов, обслуживаемых каждым сервером оборудования, ограничивается только производительностью этого сервера.

Клиентские рабочие места. Неограниченное число рабочих мест, на которых возможно выполнение различных клиентских приложений (АРМ Оператора, АРМ Бюро пропусков и др.) без подключенного оборудования.

Несколько территориально распределенных объектов с АПК «Бастион-2» могут объединяться с использованием систем «Бастион-2 – Репликация» и «Бастион-2 – ПЦН». При этом каждый объект работает со своей базой данных АПК «Бастион-2».

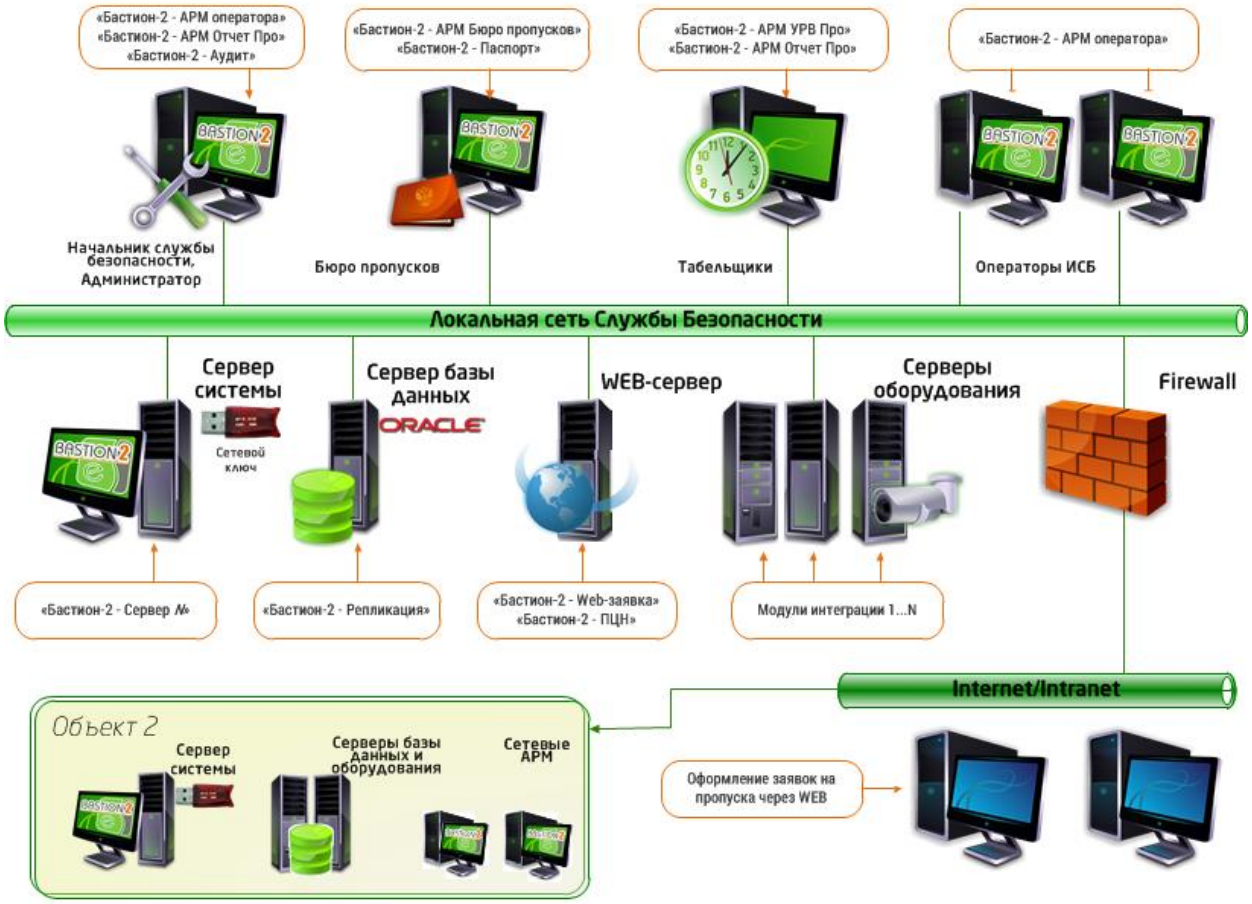

Рис. 1. Структура сети АПК «Бастион-2»

Все перечисленные узлы могут совмещаться на одном компьютере. Например, как правило, объединяется сервер баз данных, сервер системы и сервер оборудования.

Сеть АПК «Бастион-2» построена на основе протокола TCP/IP.

Программное обеспечение АПК «Бастион-2» структурно разделяется на четыре основные группы: сервер системы, драйверы, автоматизированные рабочие места (на текущий момент доступны модули «Бастион-2 – АРМ охраны» и «Бастион-2 – АРМ Бюро пропусков») и дополнительные программные модули (см. Рис. 2). Информация о возможности использования модулей и драйверов, а также об исполнениях каждого модуля, находится в ключе защиты HASP Net, устанавливаемом на сервере системы. Допускается использование нескольких ключей HASP в одной системе.

Подробную информацию о правилах комплектации АПК «Бастион-2» можно найти в документе «Правила комплектации» или в каталоге продукции.

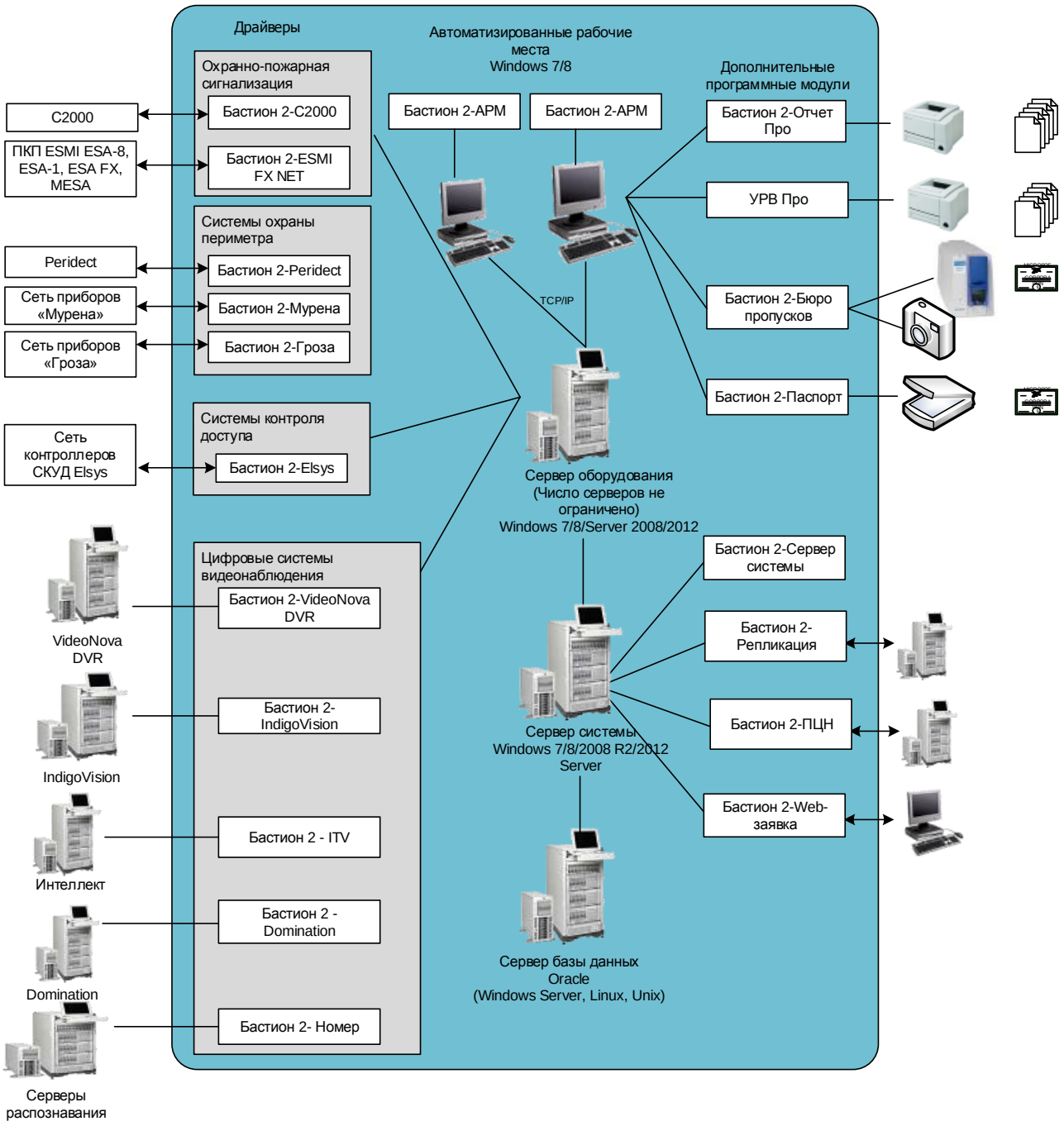

Рис. 2. Структура модулей АПК «Бастион-2»

1.4 Взаимосвязи с другими системами

1.4.1 Объединение нескольких АПК «Бастион-2»

Для объединения нескольких объектов под управлением АПК «Бастион-2» используются модули «Бастион-2 – Репликация» и «Бастион-2 – ПЦН».

Система «Бастион-2 – ПЦН» предназначена для централизованного мониторинга объектов, оснащённых АПК «Бастион-2».

Функции централизованного мониторинга включают:

- Отображение на ПЦН в текстовом виде событий, формируемых в удалённых филиалах;
- отображение на графической схеме ПЦН пиктограмм устройств удалённых объектов;
- отслеживание состояния устройств удалённых объектов с отображением на планах;
- централизованное протоколирование событий с возможностью получать отчеты.

Система может быть настроена таким образом, чтобы события в журнале ПЦН были связаны с соответствующей видеозаписью.

Системой также предусмотрена возможность управления устройствами на клиенте ПЦН с сервера ПЦН.

Система «Бастион-2 – Репликация» предназначена для синхронизации списка пропусков между филиалами организации, оснащёнными АПК «Бастион-2».

Модули «Бастион-2 – ПЦН» и «Бастион-2 – Репликация» могут использоваться совместно для обеспечения взаимодействия филиалов организации.

1.4.2 Интеграция с внешними системами обработки событий

АПК «Бастион-2» может быть интегрирован с внешними системами обработки событий с помощью следующих модулей:

- «Бастион-2 – OPC сервер»;
- «Бастион-2 – SNMP сервер»;
- «Бастион-2 – СС ТМК».

Драйверы «Бастион-2 – OPC сервер» и «Бастион-2 – SNMP сервер» реализуют идентичный функционал:

- Получение списка устройств АПК «Бастион-2»;
- Получение событий АПК «Бастион-2»;
- Получение состояний устройств АПК «Бастион-2»;
- Управление устройствами АПК «Бастион-2».

Драйвер «Бастион-2 – OPC сервер» поддерживает работу по протоколам OPC XML-DA и OPC DA.

Драйвер «Бастион-2 – SNMP сервер» поддерживает протоколы SMNP v1, v2 и v3.

Модуль «Бастион-2 – СС ТМК» предназначен для подключения АПК «Бастион-2» к системе сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры (СС ТМК).

Основной функцией модуля является формирование и передача событий от АПК «Бастион-2» к СС ТМК. В СС ТМК передаются события от следующих подсистем АПК «Бастион-2»:

- Система видеонаблюдения (включая интеллектуальное видеонаблюдение), видеозаписи и аудиозаписи;
- Система контроля и управления доступом;
- Охранно-пожарная сигнализация.

Передача событий осуществляется по подписке, параметры которой определяются в СС ТМК.

Дополнительно, драйвер предоставляет возможность вручную определить, какие события АПК «Бастион-2» будут передаваться в СС ТМК в качестве инцидентов.

1.4.3 Интеграция с системами учета персонала и пропусков

Для интеграции с внешними системами учёта персонала и пропусков в состав комплекса входит модуль «Бастион-2 – ИКС» (ИКС – интеграция кадровых систем).

С помощью этой системы может быть реализована интеграция с системами управления предприятием (ERP) в части обмена данными СКУД (персонал, пропуска, проходы). «Бастион-2 – ИКС» предоставляет API для интеграции и не содержит готовых конфигураций для каких-либо внешних систем.

Модуль «Бастион-2 – ИКС» позволяет интегрировать:

- Кадровые системы (HRMS);
- Автоматизированные системы заказа пропусков (АСЗП);
- Бухгалтерские системы.

Модуль решает следующие задачи:

- Передача в АПК «Бастион-2» заявок на пропуска из внешней системы с возможностью указания прав доступа для СКУД и номера карты доступа;
- Передача в АПК «Бастион-2» из внешней системы заявок на транспортные пропуска и пропуска на материальные ценности;
- Активация персональных, транспортных и материальных пропусков в СКУД из внешней системы;
- Управление пропусками из внешней системы (блокировка, разблокировка, возврат);
- Получение из АПК «Бастион-2» во внешнюю систему информации о персонах, персональных пропусках, транспортных пропуска, материальных пропусках, точках прохода, подразделениях, должностях и о других справочниках, доступных в АПК «Бастион-2»;
- Получение из АПК «Бастион-2» во внешнюю систему информации о последнем месте предъявления пропуска;

- Получение из АПК «Бастион-2» во внешнюю систему списка событий по заданному пропуску;
- Получение из АПК «Бастион-2» во внешнюю систему исходных данных для расчета отработанного времени (пары событий «вход-выход»).

Система поддерживает одновременную работу с несколькими АПК «Бастион-2».

2 Условия применения

2.1 Требования к программному обеспечению

Поддерживаемые операционные системы: Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 в любых исполнениях, кроме Starter, с наличием последних обновлений. Поддерживается работа на 32-х и 64-х разрядных операционных системах.

Сервер БД PostgreSQL 10 не устанавливается в ОС Windows 7 Home Basic.

Не поддерживаются Windows NT 4.0, Windows 95/98/Me, Windows 2000, Windows XP, Windows Vista, Windows Server 2000, Windows Server 2003, Windows Server 2008.

Часть модулей поддерживает работу в ОС Linux. На текущий момент это:

- «Бастион-2 – Web-заявка»;
- «Бастион-2 – ИКС».

Допускается работа сервера БД под управлением Linux. Однако в этом случае модули АПК «Бастион-2», на поддерживающие ОС Linux, не могут работать на сервере БД.

Не рекомендуется использование серверных ОС Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 для организации рабочих мест с видеонаблюдением или системой ввода фотографий с видеокамер, а также системой распознавания документов («Бастион-2 – Паспорт»). *Корректная работа функций видеонаблюдения и распознавания в этих системах не гарантируется!*

> ***Внимание!*** *Дополнительные ограничения на использование операционных систем могут вносить сторонние компоненты, используемые в драйверах АПК «Бастион-2». Сведения о таких ограничениях можно найти в руководстве на соответствующий драйвер.*

Не рекомендуется изменять региональные настройки (формат даты, формат времени и форматы других региональных стандартов) во время работы АПК «Бастион-2» и сопутствующих модулей, так как это может привести к искажению данных и нестабильной работе приложений. При изменении региональных настроек ОС Windows необходимо перезапустить АПК «Бастион-2» и все остальные модули.

> ***Внимание!*** *Все сервера оборудования и сервер системы должны находиться в одном часовом поясе. В противном случае возможны проблемы в работе некоторых модулей интеграции, в частности «Бастион-2 – ELSYS».*

Дополнительные компоненты, необходимые для работы комплекса:

- *Oracle 11g или Oracle 12c, либо PostgreSQL 10.*
- *Microsoft .Net Framework 4.7.2.*
- *DirectX 9.0* для систем видеонаблюдения.
- OpenGL.
- *Протокол TCP/IP* – входит во все используемые операционные системы.
- *Adobe Reader* – устанавливается отдельно с инсталляционного диска комплекса. Компонент необходим для чтения документации.

2.2 Требования к конфигурации компьютеров

Минимальная и рекомендуемая аппаратная конфигурация компьютеров комплекса зависят от масштаба системы, используемых операционных систем и требований сторонних продуктов (например, для рабочих мест, где предполагается работа с цифровыми системами видеонаблюдения, могут потребоваться дополнительные ресурсы). Определяющими факторами при выборе оборудования для серверов и рабочих мест, являются:

- Размер системы контроля доступа (число точек прохода и пользователей системы);
- Использование цифровых систем видеонаблюдения;
- Использование на рабочем месте дополнительных модулей АПК «Бастион-2» (например, «Бастион-2 – Паспорт», «Бастион-2 – Репликация»);
- Число и сложность графических планов;
- Общее число рабочих мест в системе.

Далее приведены *рекомендуемые* параметры для нескольких типовых случаев.

1. Комплекс со СКУД среднего масштаба (300 – 5000 пользователей, 1-20 точек прохода)

Сервер БД, системы и оборудования	Windows 10 Professional, Oracle 11g Express Edition | PostgreSQL 10, CPU 2 GHz 2 Cores, 4 Gb RAM, 1000 GB HDD
Клиентские рабочие места	Windows 10 Professional, CPU 2 GHz 2 Cores, 2 Gb RAM, 500 GB HDD

2. Комплекс с крупной СКУД (5000-100000 пользователей, 21-1000 точек прохода) и цифровой системой видеонаблюдения

Сервер БД и оборудования	Windows 2019 Server, Oracle 12c Standard Edition 2 | PostgreSQL 10, CPU 3 GHz 4 Cores, 8 Gb RAM, 1000 GB HDD
Клиентские рабочие	Windows 10 Professional, CPU 2 GHz 2 Cores, 4 Gb RAM, 500 GB HDD

места	

Наибольшее влияние на общую производительность системы (особенно при выполнении длительных операций, например, запросе отчетов) имеет производительность сервера БД. Размер БД протокола может достигать нескольких гигабайт. Это следует учитывать при установке.

Видеоадаптер и монитор должны обеспечивать разрешение не ниже, чем 1024*768, HiColor. Видеокарта должна поддерживать технологии DirectX и OpenGL. На всех рабочих местах комплекса рекомендуется использовать монитор с диагональю экрана не менее 17 дюймов. Для клиентских мест систем видеонаблюдения рекомендуется использовать видеокарты с 1 Gb и более оперативной памяти.

Для обеспечения штатной работы серверов (сервера системы, сервера БД и серверов оборудования) необходимо обеспечить автоматическое штатное завершение ОС Windows на этих компьютерах при отключении электропитания с использованием источников бесперебойного питания.

Нештатное выключение сервера БД может привести к потере пользовательских данных.

2.3 Выбор редакции СУБД

2.3.1 Поддерживаемые СУБД

АПК «Бастион-2» версий 2.1.x работает под управлением СУБД Oracle, либо СУБД PostgreSQL.

Рекомендации по выбору редакций каждой СУБД приведены в разделах ниже.

2.3.2 Выбор редакции СУБД Oracle

АПК «Бастион-2» работает с СУБД Oracle 11g или Oracle 12c. В комплект поставки входит Oracle 11g Instant Client и Oracle 11g Express Edition (Сервер СУБД Oracle 11g Express Edition находится на установочном диске, но инсталлируется всегда отдельно). Допускается развёртывание БД на серверах Oracle 11g и 12c Express Edition, Standard Edition One, Standard Edition, Standard Edition 2, Enterprise Edition. Возможно использование 64-разрядных версий сервера Oracle, а также серверов под управлением ОС Linux. Для любых редакций и версий СУБД Oracle необходимо создавать базу данных в кодировке CL8MSWIN1251, AL16UTF16 либо AL32UTF8, в противном случае при работе АПК "Бастион-2" могут возникать критические ошибки, связанные с отсутствием поддержки кириллических символов в базе данных.

Поставляемая в комплекте версия СУБД Oracle 11g Express обладает следующими ключевыми ограничениями:

- Использование только 1-го ядра процессора;
- Использование только 1 Gb оперативной памяти;
- Размер всех баз данных – не более 11 Gb.

В связи с этим настоятельно рекомендуется, при выполнении хотя бы одного из следующих условий использовать платные версии СУБД Oracle. Условия:

1. Использование в комплексе 20-и и более компьютеров;
2. Наличие в БД более 40 000 пропусков;
3. Использование 5 и более АРМ «Бюро пропусков»;
4. Наличие в БД 1 000 и более устройств с интенсивным потоком событий (контроллеры СКУД, зоны ОС периметра, видеокамеры с активным детектором движения);
5. Наличие требований к глубине хранения архива – более 9 000 000 событий. Возможное время хранения архива можно рассчитать только ориентировочно, исходя из предполагаемой интенсивности событий;
6. При использовании модуля «Бастион-2 – ПЦН», если для всех подключаемых объектов в сумме выполняется условие 4 или 5.
7. При использовании модуля «Бастион-2 – Аудит».

В этих случаях для использования можно рекомендовать **Oracle Database Standard Edition 2** (Oracle SE2). Основные особенности применения лицензионной политики СУБД Oracle для использования с АПК «Бастион-2» рассмотрены ниже:

1. При выборе для СУБД Oracle метрики лицензирования Processor, на каждый процессор сервера баз данных, содержащий до 16 потоков исполнения (8 ядер для процессоров Intel с hyper-threading), должна приобретаться одна процессорная лицензия. Для Oracle SE2 может быть применен сервер баз данных не более чем с 2-мя процессорами (сокетами).
2. При выборе для СУБД Oracle метрики лицензирования Named User Plus (NUP), лицензия приобретается на каждого так называемого именованного пользователя.

   Именованный пользователь – лицо (человек, пользователь), уполномоченное использовать СУБД Oracle, установленную на одном или нескольких серверах, не зависимо от того, использует ли оно программу в данный момент времени или нет. Автоматическое устройство (не требующее участия человека) при возможности доступа к СУБД Oracle считается пользователем (NUP) в дополнение ко всем лицам, уполномоченным использовать СУБД Oracle.
3. При использовании мультиплексирующих аппаратных или программных средств (например, монитора транзакций или веб-сервера) это число должно быть определено на входе мультиплексора. Иными словами, применительно к АПК «Бастион-2», к *именованным пользователям* относятся все сотрудники (лица), работающие с АПК «Бастион-2», а также все серверы АПК «Бастион-2» (автоматические устройства). Все АРМ АПК «Бастион-2» при этом относятся к «мультиплексирующим аппаратным или программным средствам» и не принимают участие в расчете, т. к. считаются пользователи, работающие на этих устройствах.

Пример 1

Пользователи АПК «Бастион-2» на объекте:

- Штат из 15 операторов АПК «Бастион-2», работающих в три смены по 5 человек в смене.
- Операторы Бюро пропусков – 2 оператора работающих постоянно и 1 оператор, работающий периодически по мере необходимости.
- Администраторы – 2 человека.
- Начальники подразделений – 10 человек, которые раз в неделю смотрят отчет АПК "Бастион-2".

Автоматизированное оборудование:

- Два сервера оборудования АПК «Бастион-2».
- Отдельный сервер баз данных (не учитывается в расчете, т.к. на нем работает сама СУБД).

Итого требуется: 15 + (2+1) + 2 + 10 + 2 = 32 лицензии NUP.

Пример 2

Пользователи АПК «Бастион-2» на объекте:

- Штат из 3-х операторов АПК «Бастион-2», работающих в три смены по 1 человеку в смене.
- 1 оператор Бюро пропусков.
- 1 администратор.
- 1 сервер АПК «Бастион-2».

Итого требуется: 3 + 1 + 1 + 1 = 6 лицензии NUP, но по условиям лицензирования должно быть куплено минимум 10 лицензий.

Использование **Oracle Database Enterprise Edition** оправдано только при наличии специфических требований по числу узлов кластера, шифрованию данных и пр. Более подробно об ограничениях разных редакций СУБД Oracle 11g можно посмотреть в документации на эти продукты.

2.3.3 Выбор редакции СУБД PostgreSQL

АПК «Бастион-2» версии 2.1.2 и выше поддерживает развёртывание базы данных на СУБД PostgreSQL 10. Начиная с версии 2.1.8 поддерживается PostgreSQL 11. Поддерживаются как 64-х, так и 32-х разрядные версии СУБД.

Рекомендуется использовать разрядность сервера СУБД, соответствующую разрядности операционной системы.

В большинстве случаев достаточно использовать бесплатную версию PostgreSQL 11.

Дополнительно, АПК «Бастион-2» работает с СУБД российского производства Postgres Pro, основанной на PostgreSQL, версии не ниже 10. Поддерживается работа с исполнениями Standard,

Enterprise и Certified. Выбор исполнения определяется потребностями пользователя в сфере защиты информации, масштабируемости и отказоустойчивости. Следует учитывать, что СУБД Postgres Pro всех исполнений является лицензируемой и платной для коммерческого использования.

Версия Postgres Pro Enterprise позволяет разворачивать кластерные системы, содержит дополнительные функции проверки целостности баз данных и резервных копий, имеет оптимизированный формат хранения данных и содержит ряд других усовершенствований.

Версия Postgres Pro Certified имеет сертификат ФСТЭК, удостоверяющий что, что СУБД Postgres Pro соответствует требованиям руководящих документов РД СВТ по 5 классу, РД НДВ по 4 уровню и Технических Условий (ТУ).

Детально различия между версиями СУБД Postgres Pro можно посмотреть на сайте производителя (https://postgrespro.ru/).

Также, АПК «Бастион-2» поддерживает работу с СУБД российского производства Jatoba (разработка ООО «ГазИнформСервис»), основанной на PostgreSQL 11.

2.4 Требования к компьютерным сетям

2.4.1 Общие сведения о структуре сети

Для сетевого обмена в АПК «Бастион-2» используется протокол TCP/IP (v4).

Системой могут устанавливаться сетевые соединения между следующими модулями системы:

- Клиентские рабочие места (АРМ) и сервер системы;
- Клиентские рабочие места и сервер базы данных;
- Серверы оборудования и сервер системы;
- Серверы оборудования и сервер базы данных;

Прямые соединения между клиентскими рабочими местами не используются. Информационный обмен между ними происходит через серверные модули.

2.4.2 Требования к пропускной способности

Необходимая минимальная пропускная способность сети зависит от масштаба системы: от количества событий в системе, от размера фотографий, количества и размера планировок, количества оборудования в системе. Чем больше пропускная способность, тем быстрее будут загружаться АРМ и прочие модули системы. Также на время загрузки сильно влияет время задержки передачи пакетов: желательно чтобы оно не превышало 10мс на запрос + ответ.

Для систем средних масштабов (до 200 устройств, до 5000 карт доступа, до 10 событий в секунду в системе) рекомендуется:

- для каждого АРМ оператора и АРМ формирования отчетов канал связи с сервером не менее 1 Mbit/s.

- для каждого АРМ оператора с фотоидентификацией и АРМ Бюро пропусков – не менее 2 Mbit/s (размер фотографий должен быть не более 640x480).

Для повышения комфорта работы (быстрая загрузка АРМ, быстрая работа интерфейса АРМ), а также при использовании на более крупных системах, рекомендуется использовать сеть с пропускной способностью не менее 10 Mbit/s.

Допустимые потери пакетов в сети: не более 1%.

Система допускает обрывы связи между рабочими станциями и сервером БД. Восстановление связи производится в автоматическом режиме серверными модулями, подсистемой протоколирования и приложением «АРМ Оператора». Приложения, активно использующие БД: АРМ «Бюро пропусков», «Генератор отчетов Про», «УРВ-Про» – автоматически не восстанавливают связь после обрыва.

Регулярные потери связи между узлами системы являются нештатной ситуацией и говорят о необходимости диагностики компьютерной сети.

2.4.3 Адресация и использование портов

Для рабочих станций, выполняющих роль сервера системы или оборудования, нельзя использовать динамический (изменяющийся при перезагрузке) IP-адрес.

Клиентские рабочие места, IP-адреса которых не вносятся в базу данных АПК «Бастион-2», могут работать с динамическими IP-адресами.

Системой используется ряд IP-портов. Значения по умолчанию приведены в таблице ниже:

Номер порта по умолчанию	**Назначение**	**Комментарий**
1521	Порт прослушивателя подключений к серверу БД Oracle. Требуется открыть на сервере БД.	Настраивается средствами администрирования Oracle
5432	Порт для подключений к серверу БД PostgreSQL. Требуется открыть на сервере БД.	Настраивается средствами администрирования или при установке PostgreSQL
63000	Порт сервера системы. Требуется открыть на сервере системы.	Настраивается в модуле «Настройка подключений».
5003	Порт, используемый драйвером «Бастион-2 – OPC сервер» при работе по протоколу OPC XML-DA.	Настраивается в конфигурации модуля «Бастион-2 – OPC сервер».
5004	Порт, используемый сервером модуля «Бастион-2 – web-заявка».	Настраивается в конфигурации модуля «Бастион-2 – web-заявка».
5005	Порт, используемый сервером модуля	Настраивается в конфигурации модуля

	«Бастион-2 – ИКС».	«Бастион-2 – ИКС».
161	Порт, используемый модулем «Бастион-2 – SNMP сервер».	Настраивается в конфигурации модуля «Бастион-2 – SNMP сервер».
8098	Порт, используемый модулем «Бастион-2 – ПЦН сервер». Должен быть открыт только на сервере ПЦН.	Не настраивается.
5077	Порт, используемый модулем «Бастион-2 – Elsys Mobile». Должен быть открыт только на сервере оборудования, где установлен этот модуль.	Настраивается в конфигурации модуля «Бастион-2 – Elsys Mobile».
8092	Порт, используемый модулем «Бастион-2 – ONVIF». Должен быть открыт только на сервере оборудования, где установлен этот модуль.	Не настраивается.

Для корректной работы системы все используемые порты должны быть разрешены в средствах сетевой защиты.

Внимание! *Работа сторонних компонентов, интегрированных в АПК «Бастион-2», может накладывать дополнительные требования и ограничения к конфигурации сети. Рекомендуется ознакомиться с документацией на все используемые модули для уточнения требований.*

Внимание! *При использовании драйверов, в SDK которых применяется технология DCOM, порты, использующиеся для сетевого взаимодействия, берутся из динамического диапазона портов и не настраиваются. Это особенность технологии DCOM, на которую невозможно повлиять.*

3 Использование АПК «Бастион-2» в информационных системах обработки персональных данных

3.1 Нормативное обеспечение

Под организацией обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Согласно Федеральному закону №152-ФЗ «О персональных данных» все информационные системы персональных данных (ИСПДн) должны быть приведены в соответствие с требованиями закона до 1.01.2010 года. Ответственность за исполнение мер по обеспечению безопасности ПДн законом возложена на операторов персональных данных.

Государственными регуляторами в указанной сфере являются:

- ФСТЭК РФ (техническая защита),
- ФСБ РФ (криптография),
- Россвязькомнадзор РФ (защита прав субъектов персональных данных).

К нормативному обеспечению необходимости защиты персональных данных можно отнести следующие документы:

1. Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных".
2. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.2 Роль АПК «Бастион-2» в ИСПДн

АПК «Бастион-2» может использоваться как компонент комплексной системы защиты персональных данных для ИСПДн. Для обеспечения соответствия всей системы, построенной на АПК «Бастион-2», требованиям Федерального закона №152-ФЗ «О персональных данных», должна быть создана соответствующая защищенная среда.

Параметры этой защищённой среды должен определить Оператор ПД, на основе требований нормативных документов, перечисленных в п.3.1, а также собственных требований.

При классификации ИС на основе АПК «Бастион-2» и определении необходимых мер защиты ПД, следует учитывать следующие параметры конкретной системы:

- Общее число Персон, данные о которых предполагается хранить в БД АПК «Бастион-2».
- Наличие Персон, не являющихся сотрудниками Оператора ПД, данные о которых предполагается хранить в БД АПК «Бастион-2».
- Применение в АПК «Бастион-2» биометрических данных, используемых для идентификации Персон.
- Типы актуальных угроз для ИС, в соответствии с постановлением №1119.

АПК «Бастион-2» позволяет реализовать следующие меры по защите ПД, предусмотренные нормативными актами РФ:

1. Автоматизация подготовки информированного согласия на обработку ПД. Отслеживание завершения сроков действия информированного согласия.
2. Идентификация, проверка подлинности и регистрация входа-выхода субъектов доступа в ИС.
3. Механизм ролевого разграничения доступа.
4. Непрерывный мониторинг и регистрация событий.
5. Мониторинг и регистрация операций над ПД.
6. Регистрация выдачи документов на твердую копию.

Таким образом, для реализации полноценной защиты ПД Оператор ПД должен провести комплекс дополнительных мероприятий. Перечень этих мероприятий должен быть определен самим оператором ПД в соответствии с требованиями законодательства. Само по себе

использование АПК «Бастион-2», без дополнительного комплекса мер не гарантирует соответствие ИС нормативным документам РФ по обработке ПД.

АПК «Бастион-2» не подлежит обязательной сертификации в системе сертификации ФСТЭК России № РОСС RU.0001.01БИ00 в качестве средства защиты информации (далее - СЗИ). Тем не менее, в АПК «Бастион-2» имеется функционал, позволяющий осуществлять аутентификацию и идентификацию пользователей аппаратно-программного комплекса, разграничение их доступа. Таким образом, в его составе имеются встроенные средства защиты информации от несанкционированного доступа.

Для ряда случаев, установленных законодательством Российской Федерации, а также в случае принятия решения владельцем информационной системы, может потребоваться проведение оценки соответствия АПК «Бастион-2» требованиям к СЗИ. Такая оценка может производиться в форме сертификации, испытаний или приемки.

4 Инсталляция АПК «Бастион-2»

4.1 Установка программного обеспечения

4.1.1 Установка сервера СУБД

Перед установкой АПК «Бастион-2» убедитесь, что СУБД установлена и доступна. При установке потребуется ввести данные для подключения к экземпляру СУБД Oracle или PostgreSQL. Для развёртывания схемы БД АПК «Бастион-2» должен быть известен пароль пользователя SYSTEM СУБД Oracle, либо пароль суперпользователя для PostgreSQL.

> ***Внимание!*** *В терминологии Oracle, понятия* ***схема*** *и* ***пользователь*** *идентичны и взаимозаменяемы. Таким образом, понятия* ***имя пользователя*** *и* ***имя схемы*** *– идентичны. Также, взаимозаменяемы понятия* ***пароль пользователя Oracle*** *и* ***пароль схемы Oracle****.*

4.1.2 Настройка параметров сервера PostgreSQL

После установки сервера СУБД PostgreSQL следует настроить конфигурационные файлы **postgresql.conf** и **pg_hba.conf**, находящиеся по умолчанию в папке C:\Program Files\PostgreSQL\10\data. Редактировать файлы можно в программе «Блокнот». Строки, начинающиеся с символа **#**, закомментированы (неактивны). Для активации параметра символ **#** следует удалить.

Рекомендуется проверить значения следующих параметров:

1. Проверить, какая временная зона прописалась в конфигурационном файле PostgreSQL. В файле:

   ```
   \PostgreSQL\10\data\postgresql.conf
   ```

   в параметр timezone должна прописаться временная зона, соответствующая часовому поясу, установленному на хосте. Например, для часового пояса "Самара, Ижевск" в postgresql.conf должно быть:

   ```
   timezone = 'Europe/Samara'
   ```

Посмотреть список поддерживаемых в СУБД PostgreSQL временных зон можно в результатах запроса

```
select * from pg_timezone_names
```

2. В файле \PostgreSQL\10\data\postgresql.conf рекомендуется установить следующие параметры:

```
# - Connection Settings -
max_connections = 500          # (change requires restart)

# - Memory -
shared_buffers = 256MB         # min 128kB
temp_buffers = 32MB            # min 800kB
work_mem = 64MB                # min 64kB
maintenance_work_mem = 128MB   # min 1MB

# - Background Writer -
bgwriter_delay = 20ms          # 10-10000ms between rounds
bgwriter_lru_maxpages = 400    # 0-1000 max buffers written/round
bgwriter_lru_multiplier = 4.0

# AUTOVACUUM PARAMETERS
autovacuum = on
autovacuum_max_workers = 6     # max number of autovacuum subprocesses
autovacuum_naptime = 20s       # time between autovacuum runs
autovacuum_vacuum_cost_limit = 400   # default vacuum cost limit for
```

3. В файле pg_hba.conf рекомендуется установить следующие параметры:

```
# Allow replication connections from localhost, by a user with the
# replication privilege.
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
host    all    all    0.0.0.0/0    md5
```

На носителе с дистрибутивом АПК «Бастион-2» в папке …\PostgreSQL\ConfigSamples находятся примеры готовых конфигурационных файлов для СУБД PostgreSQL версий 10 и 11.

4.1.3 Установка АПК «Бастион-2»

Рекомендуется в первую очередь выполнять установку на том компьютере, с которого будет разворачиваться схема базы данных АПК «Бастион-2». До развёртывания схемы работа системы будет невозможна.

Для проведения установки необходимо обладать правами администратора ОС.

Запустите программу установки АПК «Бастион-2» (из оболочки, появляющейся при автозапуске диска, либо запустив файл <CDROM>:\Install\Setup.exe). В процессе установки необходимо ответить на ряд вопросов.

Для работы АПК «Бастион-2» требуется наличие Microsoft .Net Framework 4.7.2. Если этот компонент не установлен, то программа инсталляции запустит его установку. По окончании установки Microsoft .Net Framework может потребоваться перезагрузить компьютер. После перезагрузки установка АПК «Бастион-2» продолжится.

Для установки АПК «Бастион-2» требуется принять права и обязанности покупателя АПК «Бастион-2».

На следующем этапе программа установки предложит выбрать папку установки АПК «Бастион-2».

> ***Внимание!*** *Общие файлы, используемые несколькими программными продуктами ООО «ЕС-пром», устанавливаются в папку* ***<ProgramFiles(x86)>\ES-Prom****, вне зависимости от выбранной папки установки АПК «Бастион-2».*

Далее, программа установки предложит выбрать компоненты, которые необходимо установить. По умолчанию отмечен набор компонентов, достаточный для работы системы в режиме «АРМ Оператора», «АРМ Бюро пропусков» и «Сервер оборудования».

> ***Внимание!*** *Перед продолжением установки убедитесь в правильности набора выбранных компонентов. Следует иметь в виду, что если в системе предполагается установить определённый драйвер, то его следует устанавливать на всех компьютерах системы. Для установки на рабочем месте администратора системы рекомендуется выбрать все компоненты. При установке на компьютер, с которого предполагается создать схему базы данных АПК «Бастион-2», следует выбрать компонент «Управление схемами АПК «Бастион-2».*

На следующем этапе программа установки попросит ввести данные для подключения к СУБД.

Для СУБД Oracle:

База данных Oracle – название псевдонима, который будет использоваться для подключения к Oracle.

Пользователь Oracle – имя пользователя Oracle, в схеме которого развёрнута БД АПК «Бастион-2».

Пароль пользователя Oracle – пароль пользователя, который будет использован для подключения к базе данных всеми модулями АПК «Бастион-2».

Имя сервиса Oracle – глобальное имя сервиса Oracle (Global Database Name), используемое на сервере БД Oracle.

Адрес сервера Oracle – IP-адрес или DNS-имя сервера Oracle.

Порт сервера Oracle – порт, используемый для подключения к серверу Oracle (1521 по умолчанию).

Для СУБД PostgreSQL:

Пользователь PostgreSQL – имя пользователя PostgreSQL для подключения к БД АПК «Бастион-2».

Пароль пользователя PostgreSQL – пароль пользователя для подключения к базе данных всеми модулями АПК «Бастион-2».

Имя базы данных PostgreSQL – название БД АПК «Бастион-2» на сервере PostgreSQL.

Адрес сервера PostgreSQL – IP-адрес или DNS-имя сервера *PostgreSQL*.

Порт сервера PostgreSQL – порт, используемый для подключения к серверу *PostgreSQL* (5432 по умолчанию).

Если вы не знаете точно необходимые значения параметров, проконсультируйтесь с администратором СУБД.

> ***Внимание!*** *Следует запомнить и сохранить в надёжном месте имя и пароль схемы БД АПК «Бастион-2» для установки АПК «Бастион-2» на других рабочих местах и для последующих действий по администрированию системы. На всех компьютерах следует вводить одинаковые параметры для подключения. Эти же параметры следует указывать при развёртывании схемы БД АПК «Бастион-2» после установки.*
>
> ***Внимание!*** *Если при установке на клиентском месте ввести неверные данные подключения, то сменить их можно с помощью утилиты «Настройка подключения». Более подробно см. документацию на этот модуль.*

Далее, программа установки попросит ввести настройки сервера системы:

Адрес сервера – IP-адрес или DNS-имя компьютера, на котором будет работать сервер системы.

Порт сервера – порт, на котором будет работать сервис сервера систем.

Код подключения – кодовое слово, использующееся для подключения к серверу системы. Необходимо вводить одинаковый код подключения на всех компьютерах системы.

Если выбрана установка модуля «УРВ-Про», то система запросит путь его установки.

После ввода всех параметров будет произведена установка системы.

Если при установке был выбран компонент «Управление схемами АПК «Бастион-2», то по окончании установки программа предложит запустить «Управление схемами АПК «Бастион-2».

> ***Внимание!*** *Для работы системы необходимо развернуть схему БД. См. п. 8.4.3. Развёртывание схемы базы данных.*

При завершении установки может потребоваться перезагрузить компьютер.

После этого программное обеспечение готово к запуску.

> ***Внимание!*** *После установки в уже развёрнутую систему новых типов драйверов необходимо перезапустить службу BAgentSvc на сервере системы.*

4.2 Запуск и выгрузка системы

В версии АПК «Бастион 2.1» и выше, драйверы вынесены из клиентского приложения Bastion.exe и работают на сервере оборудования без пользовательского интерфейса. Bastion.exe является клиентским приложением оператора системы.

Фактически, драйверы выполняются как отдельные процессы. Таким образом следует иметь в виду следующие особенности запуска системы:

1. Все драйверы стартуют при запуске компьютера, до входа пользователя в систему. Запуск драйверов производит служба BAgentSvc.

2. Каждый тип драйвера работает в отдельном процессе с именем Bastion.DriverHost. Если в системе несколько однотипных драйверов (например, 2 драйвера Peridect), то они будут работать в одном процессе. Перезапустить отдельно каждый из однотипных драйверов нельзя, только все вместе.

3. Перезапуск клиентского приложения Bastion.exe не приводит к перезапуску драйверов оборудования. Для перезапуска драйверов есть специальная форма «Управление драйверами» на вкладке «Драйверы» в «АРМ оператора». Все драйверы можно запускать и останавливать отдельно, не выходя из приложения «АРМ оператора», в том числе удаленно.

4. В зависимости от производительности рабочей станции и конфигурации системы, запуск серверов оборудования, получение информации с сервера системы и запуск самого драйвера могут занимать длительное время, в течение которого часть функций драйвера, предполагающих непосредственную работу с устройствами, будет недоступна.

Сервер оборудования и сервер системы могут работать без запущенного на них модуля Bastion.exe, то есть – без пользовательского интерфейса.

Клиентское приложение оператора (Bastion.exe) может запускаться в любой последовательности на всех рабочих местах комплекса.

> ***Внимание!*** *При первом запуске следует ввести* ***имя пользователя – «q» и пароль «q».*** *Этот пользователь имеет максимальные полномочия, и при первом запуске это единственный в базе данных АПК «Бастион-2». В дальнейшем рекомендуется изменить этот пароль.*

Запуск «АРМ оператора» невозможен при отсутствии связи с сервером системы и с базой данных. В ходе работы системы при потере связи с БД или с сервером системы блокируются функции настройки системы, а также ряд сервисных возможностей. После восстановления связи работа системы продолжается в штатном режиме.

Для запуска системы без полномочий администратора операционной системы см. п. 6.3.

4.3 Структура процессов

Первичный процесс, который запускает все необходимые модули системы – это служба BAgentSvc. Она выполняется на всех компьютерах АПК «Бастион-2», но в зависимости от роли компьютера в системе, выполняет разные функции.

Роль сервера системы выполняется именно этой службой. На серверах оборудования эта служба запустит все драйверы. На клиентах служба обеспечит взаимодействие с сервером системы.

Все драйверы работают в отдельных процессах с именем Bastion.DriverHost (Рис. 3). Если в системе несколько однотипных драйверов (например, 2 драйвера Perident), то они будут работать в одном процессе.

Многие задачи выполняются системой также в отдельных процессах с именем BAgent (Рис. 3). К таким задачам относятся, например:

- Сервис протоколирования событий;
- Графическая подсистема АРМ «Оператора»;
- Подсистема фотоидентификации.

Такие процессы также запускаются службой BAgentSvc по необходимости (например, при запуске «АРМ Оператора»).

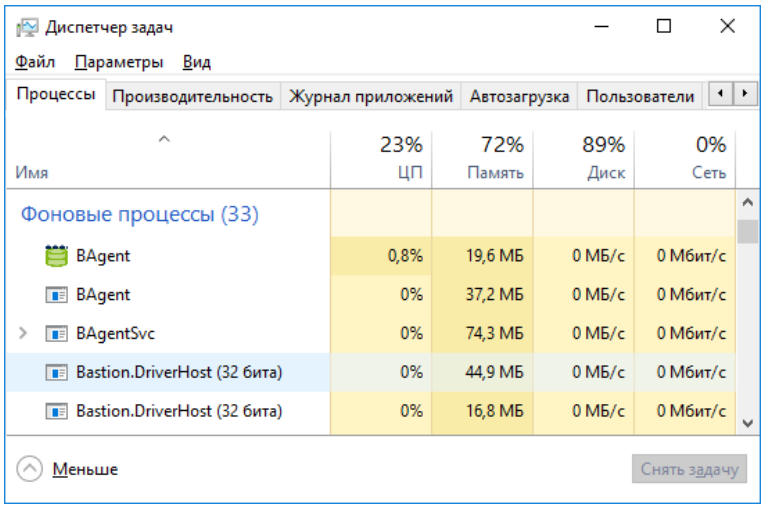

Рис. 3. Процессы АПК «Бастион-2» на сервере системы и оборудования

5 Настройка системы

5.1 Работа с формами редактирования баз данных

Все формы для работы с отдельными таблицами базы данных имеют сходный интерфейс для навигации по таблице и редактирования данных.

В верхней части таких форм находится специальный элемент управления, имеющий следующий вид:

Рис. 4. Навигатор по таблице базы данных

Назначение кнопок:

 Переход к первой записи.

 Переход к предыдущей записи.

 Переход к следующей записи.

 Переход к последней записи.

 Добавить новую запись.

 Удалить текущую запись.

 Войти в режим редактирования текущей записи.

 Сохранить изменения в текущей записи (сохранить запись).

 Отменить изменения текущей записи.

 Обновить (перечитать из базы данных) содержимое таблицы.

Отдельные кнопки в ряде случаев могут отсутствовать. Следует иметь в виду, что:

- Редактирование данных производится только в специальных элементах управления, но не в таблице в нижней части окна;
- Переход из режима просмотра в режим редактирования текущей записи происходит автоматически при попытке изменить содержимое любого поля;
- Сохранение изменений текущей записи происходит автоматически при попытке выбрать любую из кнопок (кроме кнопки «отмены изменений записи») навигатора.

Поиск данных производится в отдельном окне и позволяет искать записи по 1 или 2 полям, объединяя условия поиска по «*и*» или «*или*». Поиск может производиться по любым текстовым и числовым полям, принадлежащим редактируемой таблице.

Горячие клавиши для редактирования данных:

Ins	Вставка новой записи.
Ctrl+S	Сохранение текущей записи.
Esc	Отмена изменений в текущей записи.
Enter	Переход в режим редактирования текущей записи, если при нажатии была активна таблица.
Ctrl+F	Вызов окна поиска.

5.2 Последовательность действий при настройке

Настройку системы рекомендуется производить в следующем порядке:

1. Определить конфигурацию компьютерной сети и портов, к которым будет подключаться оборудование системы безопасности.

2. Добавить рабочие станции, выполняющие роль серверов оборудования, (п. 5.3.1), а затем драйверы (п. 5.3.2).
3. Настроить полномочия, список пользователей (п. 5.4), и профили пользователей (п. 5.5).
4. Настроить добавленные драйверы (см. инструкцию на соответствующий драйвер).
5. Расставить пиктограммы на графических планах (п. 5.6).
6. Настроить параметры обработки событий (п. 5.9.7), сценарии и реакции на события.
7. Настроить области контроля, глобальный контроль последовательности прохода и систему учёта рабочего времени.
8. Выполнить все остальные требуемые настройки (можно производить в произвольном порядке).

Далее рассматриваются указанные действия в рекомендуемой последовательности.

5.3 Конфигурация сети АПК «Бастион-2»

5.3.1 Внесение информации о серверах оборудования

В БД АПК «Бастион-2» должна быть добавлена информация о сервере системе, а также обо всех серверах оборудования, используемых в системе. Добавлять компьютеры, используемые только для запуска АРМ-ов, нет необходимости. Сервер системы добавляется в дерево автоматически.

Для добавления, удаления и редактирования свойств серверов оборудования необходимо выбрать в ленте «Конфигурация» в закладке «Система» пункт «Сеть». После этого откроется форма, представленная на Рис. 5.

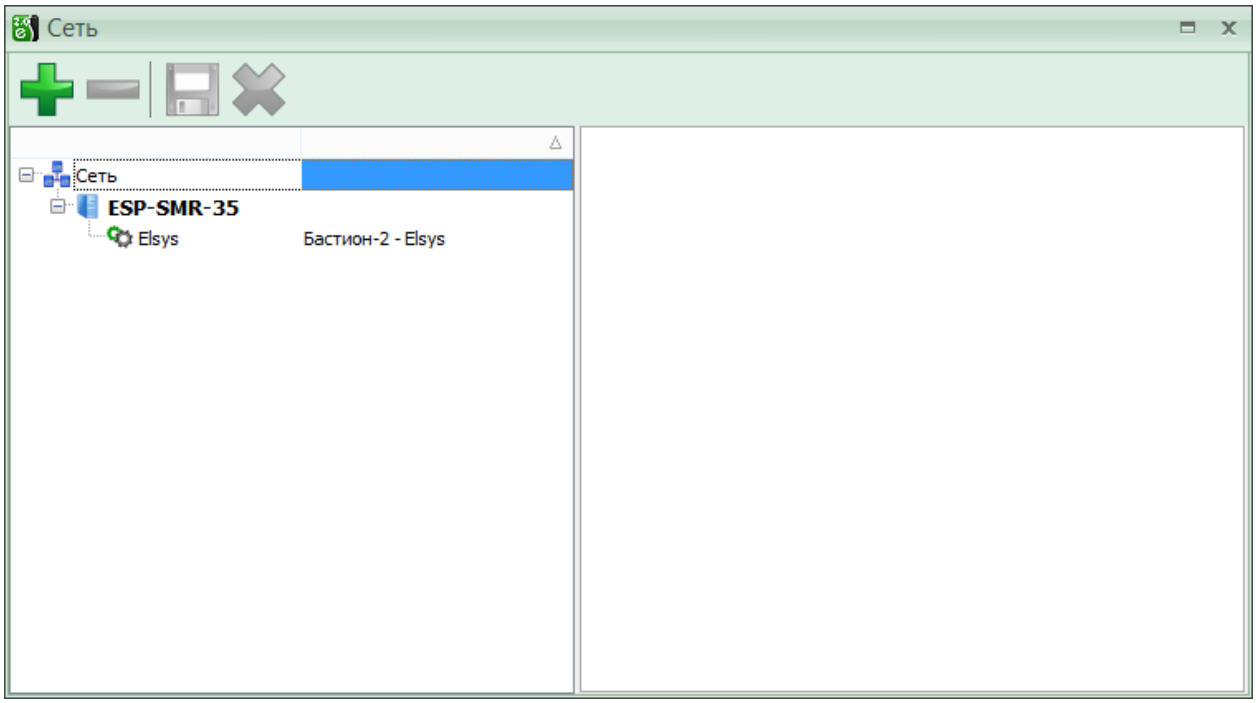

Рис. 5. Окно настройки «Сеть»

Для добавления сервера необходимо перейти на узел «Сеть» в дереве и нажать на кнопку «Добавить рабочую станцию» (Shift+Ins). При этом к дереву добавится новая безымянная ветвь, а в правой части формы отобразится поле «Имя», в которое нужно ввести имя или IP-адрес рабочей

станции. Также возможен выбор рабочей станции из списка машин в сети, который открывается по нажатию кнопки «…» рядом с полем ввода имени ПК.

> ***Внимание!*** *Имя рабочей станции можно использовать только в случае, если рабочая станция доступна для подключения по данному имени. Проверить доступность рабочей станции по имени можно с помощью команды* ***ping.*** *В противном случае необходимо использовать IP-адрес.*

Для редактирования присутствующей в списке рабочей станции следует выделить её в дереве мышью и в правой части формы отобразятся поля для редактирования.

> ***Внимание!*** *Компьютер, на который назначен сервер системы, недоступен для редактирования и выделен в дереве полужирным шрифтом.*

Созданную конфигурацию следует сохранить, нажав на кнопку «Сохранить» (Ctrl+S). Отмена внесенных несохраненных изменений осуществляется кнопкой «Отменить» (Ctrl+Z).

5.3.2 Добавление драйверов

Добавление драйверов в систему осуществляется с помощью пункта «Сеть» вкладки «Конфигурация».

Для добавления устройства (экземпляра драйвера) необходимо выбрать сервер в дереве, нажать кнопку «добавить драйвер» (Ctrl+Ins), ввести название устройства, выбрать один из доступных управляющих драйверов (соответствующий типу добавляемого устройства).

Если для подключения оборудования драйвера используются COM-порты, то их необходимо добавить к драйверу, выбрав узел драйвера и нажав кнопку «Добавить COM-порт» (Ctrl+Ins). Для некоторых драйверов COM-порт добавляется автоматически (см. Рис. 6). Номер может быть выбран из диапазона от 1 до 256, однако реальное количество свободных COM-портов может быть меньше. Для корректного выбора необходимо определить номера доступных (не занятых другими устройствами) COM-портов на выбранной рабочей станции.

Назначение и правила заполнения полей базы данных устройств:

Имя – служит для ввода уникального имени экземпляра драйвера, обеспечивающего его идентификацию при дальнейшей настройке ПО. Длина названия не должна превышать 40 символов, например, «Система ТВ наблюдения».

Тип драйвера – поле служит для выбора драйвера, обеспечивающего взаимодействие ядра с внешней системой.

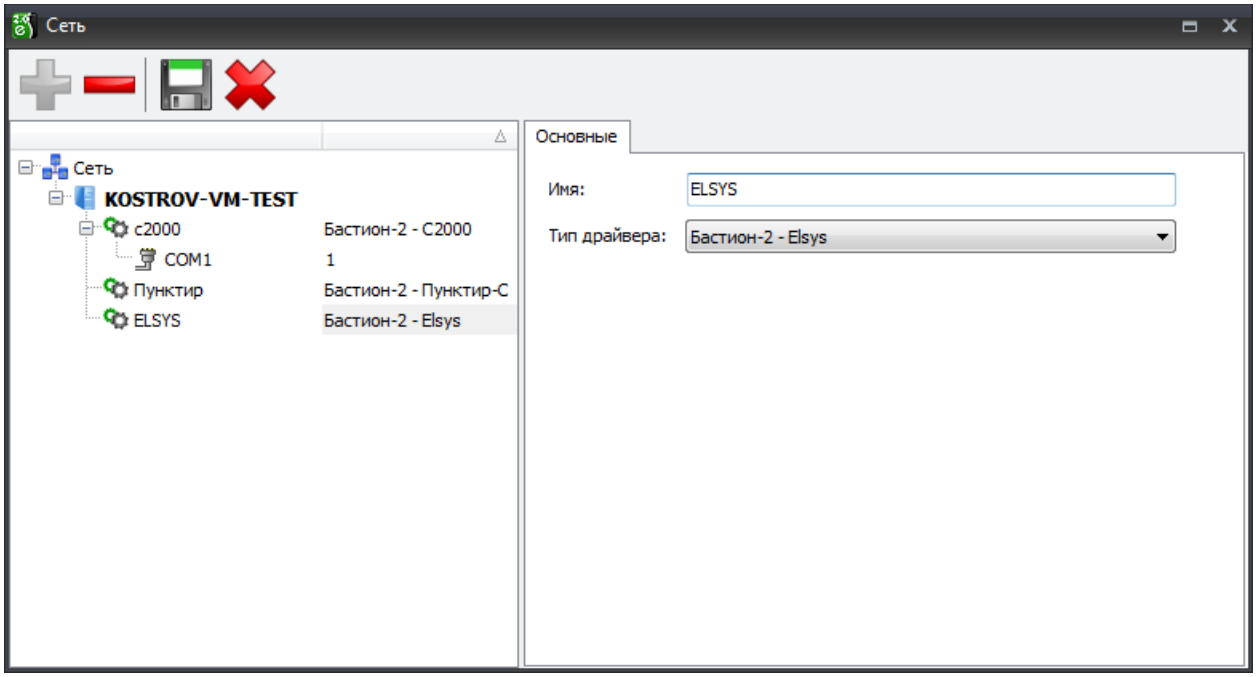

Рис. 6. Добавление экземпляров драйверов

Для того чтобы внесенные изменения вступили в силу, необходимо перезапустить программу на всех рабочих станциях системы безопасности.

После добавления драйвера и перезапуска АПК «Бастион-2» в ленте «Драйверы» появятся пункты, относящиеся к настройке добавленного драйвера (Рис. 7).

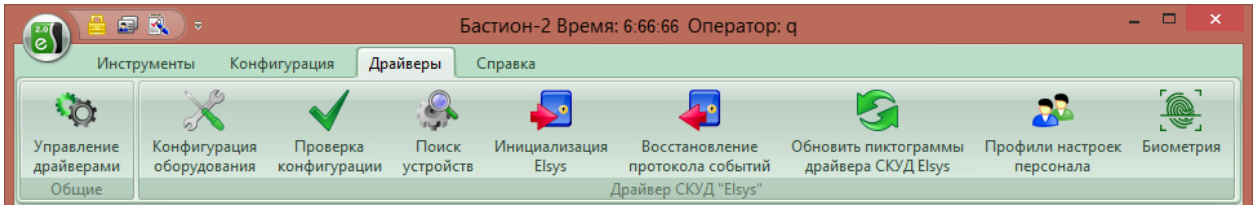

Рис. 7. Пример меню драйвера

5.3.3 Управление драйверами

В системе предусмотрена возможность ручной остановки и запуска драйверов независимо друг от друга. Осуществляются данные действия в окне «Управление драйверами», которое можно вызвать из блока «Общие» вкладки «Драйверы» главного окна. Внешний вид окна «Управление драйверами» представлен на Рис. 8.

Отключение драйверов в этой форме производится либо до перезагрузки компьютера, либо до запуска этого драйвера вручную.

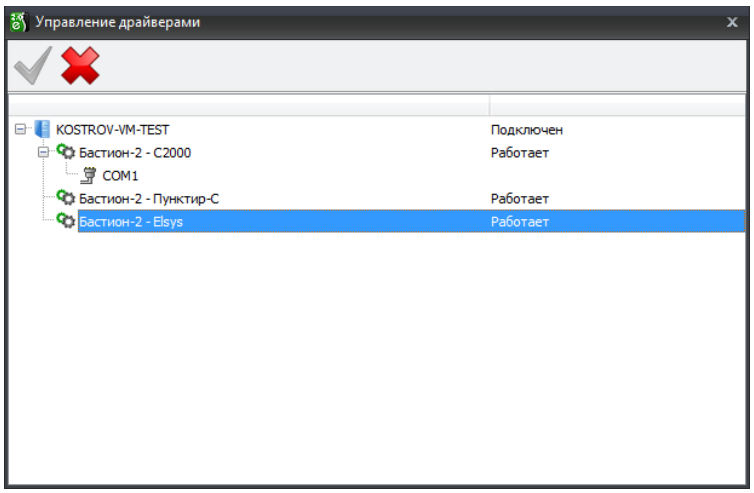

Рис. 8. Окно управления драйверами

5.4 Настройка пользовательских полномочий и добавление пользователей

Окно настройки пользовательских полномочий доступно из ленты «Конфигурация» в закладке «Операторы и полномочия» пункт «Полномочия операторов…», (Рис. 9). Окно содержит несколько вкладок, в соответствии с установленными подсистемами.

Поле *«Приоритет»* определяет минимально необходимый уровень пользовательских полномочий для выполнения операции. Большинство настроек полномочий пользователей можно оставить без изменений.

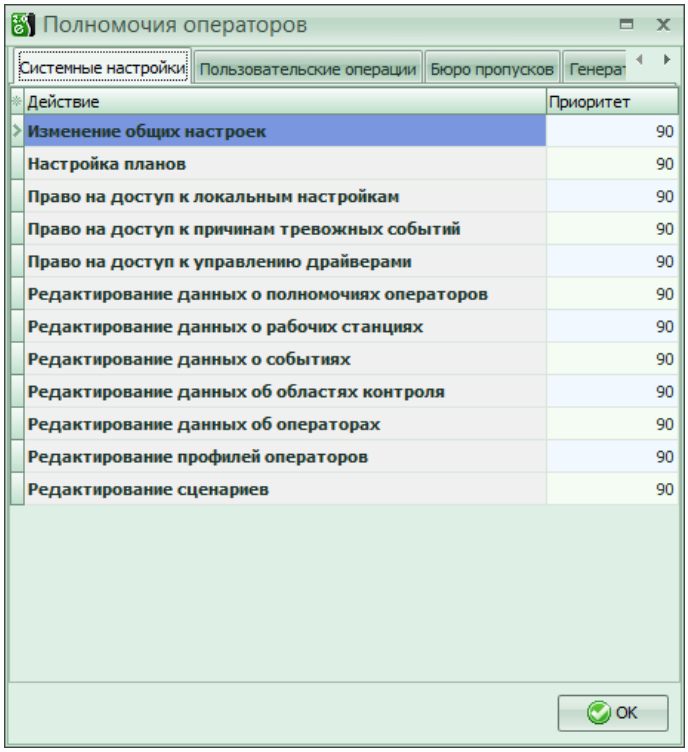

Рис. 9. Окно настройки полномочий пользователей

Для добавления пользователей и редактирования их полномочий следует выбрать в ленте «Конфигурация» в закладке «Операторы и полномочия» пункт «Операторы» (Рис. 10).

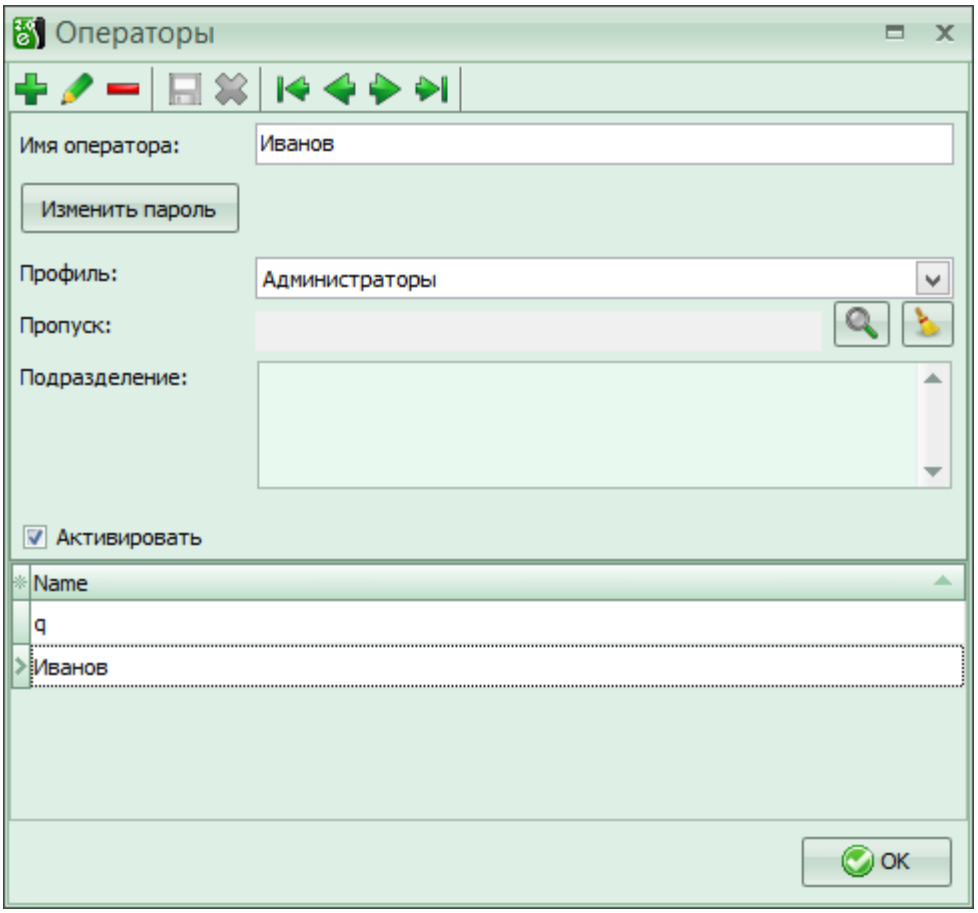

Рис. 10. Форма редактирования данных о пользователях

Для *добавления* нового пользователя необходимо:

- нажать клавишу «добавить запись»;
- ввести имя и пароль пользователя в соответствующих полях открывшегося окна добавления нового оператора. Имя и пароль могут содержать любые печатные символы русского или английского алфавита в разных регистрах и цифры, причем строчные и прописные буквы различаются при анализе пароля;
- подтвердить введенный пароль, набрав его повторно;
- указать требуемый профиль пользователя;
- нажать клавишу «сохранить запись».

Рекомендуется добавлять отдельного оператора комплекса «Бастион-2» на каждого человека, работающего с системой. Это может быть полезно при анализе протокола событий (например, определить, в чью смену случилось происшествие или кто изменял настройки). При смене дежурства следует проводить повторный вход в АРМ Оператора АПК «Бастион-2» под новым именем. Для каждого пользователя назначается один из настроенных заранее профилей пользователей.

Оператора системы можно связать с Персоной из базы данных пропусков. Это позволит более точно идентифицировать оператора. Такая привязка необходима при работе с модулем web-заявок на пропуска.

Флаг «Активировать» в снятом состоянии позволяет блокировать оператора системы, не удаляя его из базы данных.

5.5 Настройка профилей операторов

5.5.1 Общие настройки

Для настройки профилей пользователей следует выбрать в ленте «Конфигурация» в закладке «Операторы и полномочия» пункт «Профили операторов». Профиль оператора (Рис. 11) задаёт ряд настроек пользовательского интерфейса, специфичных для группы операторов. Кроме того, на основе профилей пользователей осуществляется маршрутизация сообщений, разграничивающая зоны ответственности пользователей и распределяющая поток событий между операторами системы. При входе в программу, независимо от компьютера, на котором это производится, загружается тот профиль, который указан для оператора. Один и тот же профиль можно назначить нескольким операторам.

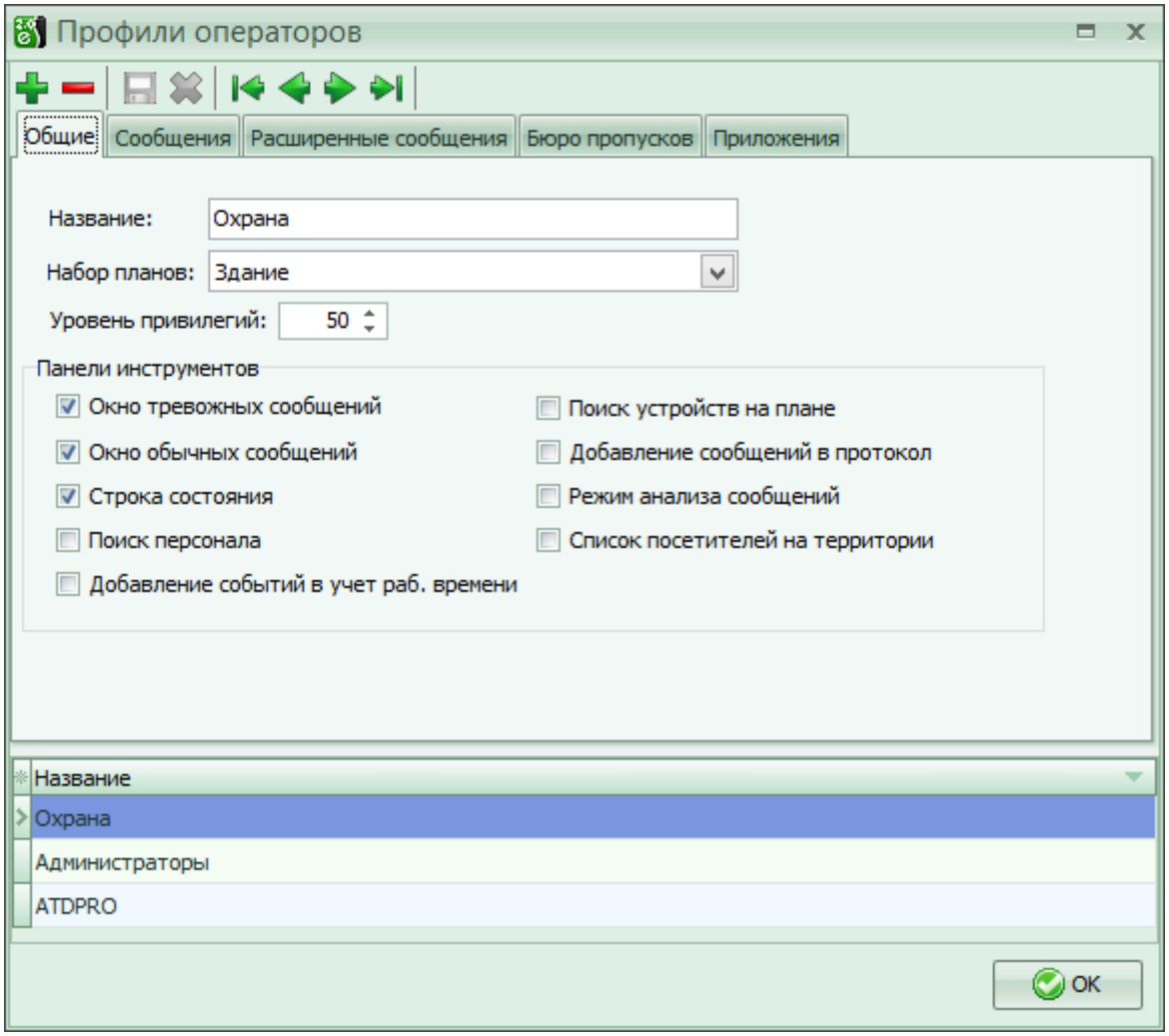

Рис. 11. Окно настройки профилей операторов

На вкладке «Общие» можно задать *название профиля,* определить *набор графических планов,* используемых для профиля, и выбрать, какие панели инструментов показать, а какие скрыть. Также на данной вкладке можно настроить уровень привилегий выбранного профиля. Обычно

рекомендуется профилю дежурного оператора поста охраны присвоить уровень полномочий 10, оператору бюро пропусков – 50, администратору – 90...99. Стоить заметить, что у встроенного профиля операторов «Администраторы» возможность смены уровня привилегий отсутствует.

5.5.2 Параметры обработки сообщений

На странице «Сообщения» (Рис. 12) можно задать, какие сообщения будут отображаться системой. Следует иметь в виду, что параметры отображения и параметры записи в протокол не влияют друг на друга. Поэтому, даже если сообщение не отображается, оно может быть записано в журнал событий.

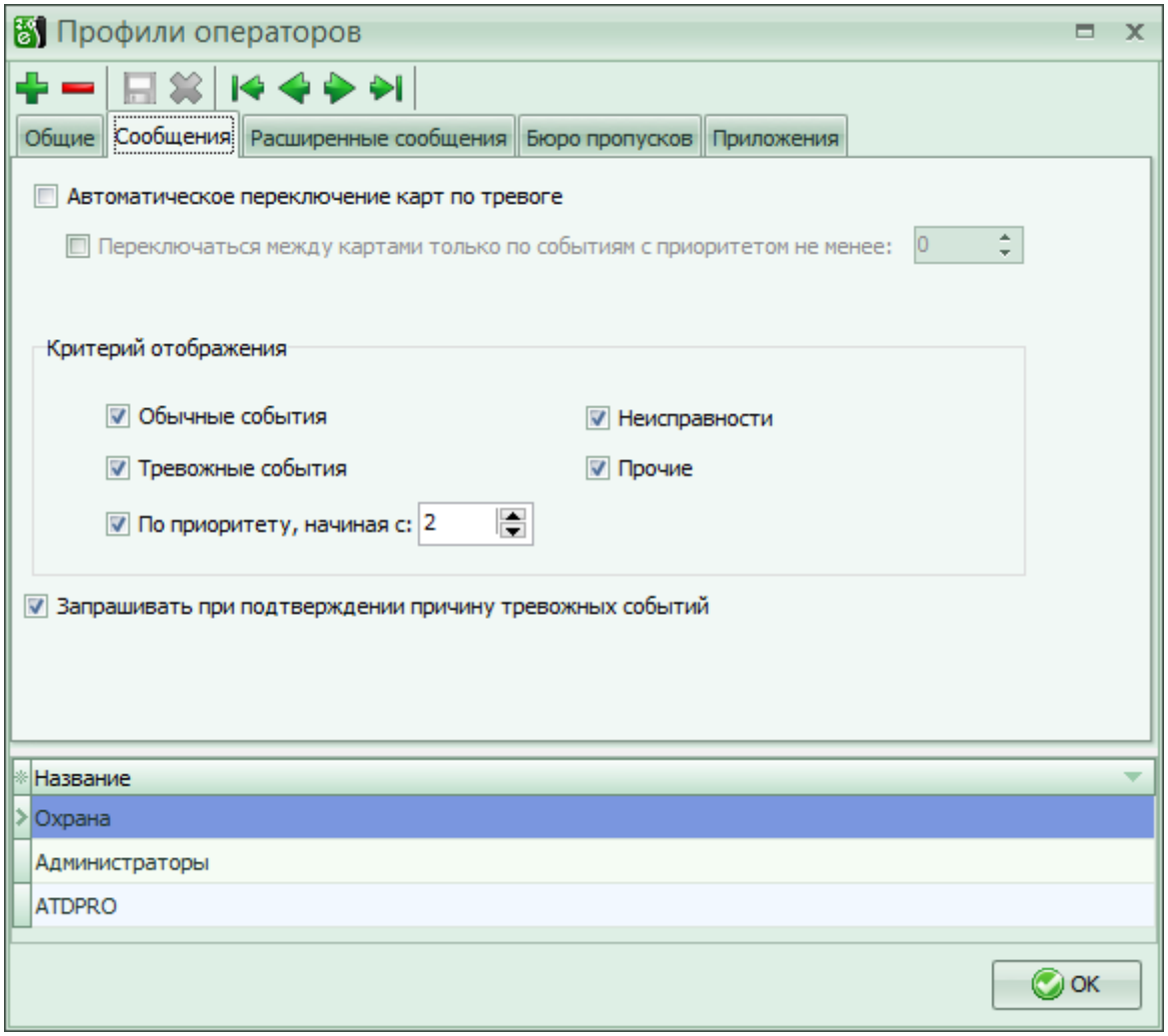

Рис. 12. Настройка параметров отображения сообщений

Система позволяет определять критерий отображения на основе типа сообщений (обычное, тревожное, неисправность, прочие), и их приоритета.

Флаги типов сообщений объединяются по логическому «или», а флаг отбора по приоритету – по логическому «и» со всеми остальными. Так, изображённые на Рис. 12 настройки обеспечивают вывод сообщений для всех событий с приоритетом от 4.

Автоматическое переключение карт по тревоге – при установленном флаге графические планы будут автоматически переключаться для отображения места возникновения последнего тревожного события.

Переключаться между картами только по событиям с приоритетом не менее заданного – опция имеет смысл только при включенном режиме автопереключения по событиям. В этом режиме при возникновении тревожного события система перейдет к тому графическому плану, на котором установлено устройство-источник данного события. Исключить излишне частое переключение планов можно, при помощи соответствующей настройки приоритетов событий.

Запрашивать при подтверждении причину тревожных событий – опция позволяет указать, необходимо ли оператору с выбранным профилем указывать причину тревожного события при его подтверждении.

5.5.3 Параметры отображения расширенных сообщений

Страница «Расширенные сообщения» (Рис. 13) предназначена для настройки параметров отображения расширенных сообщений.

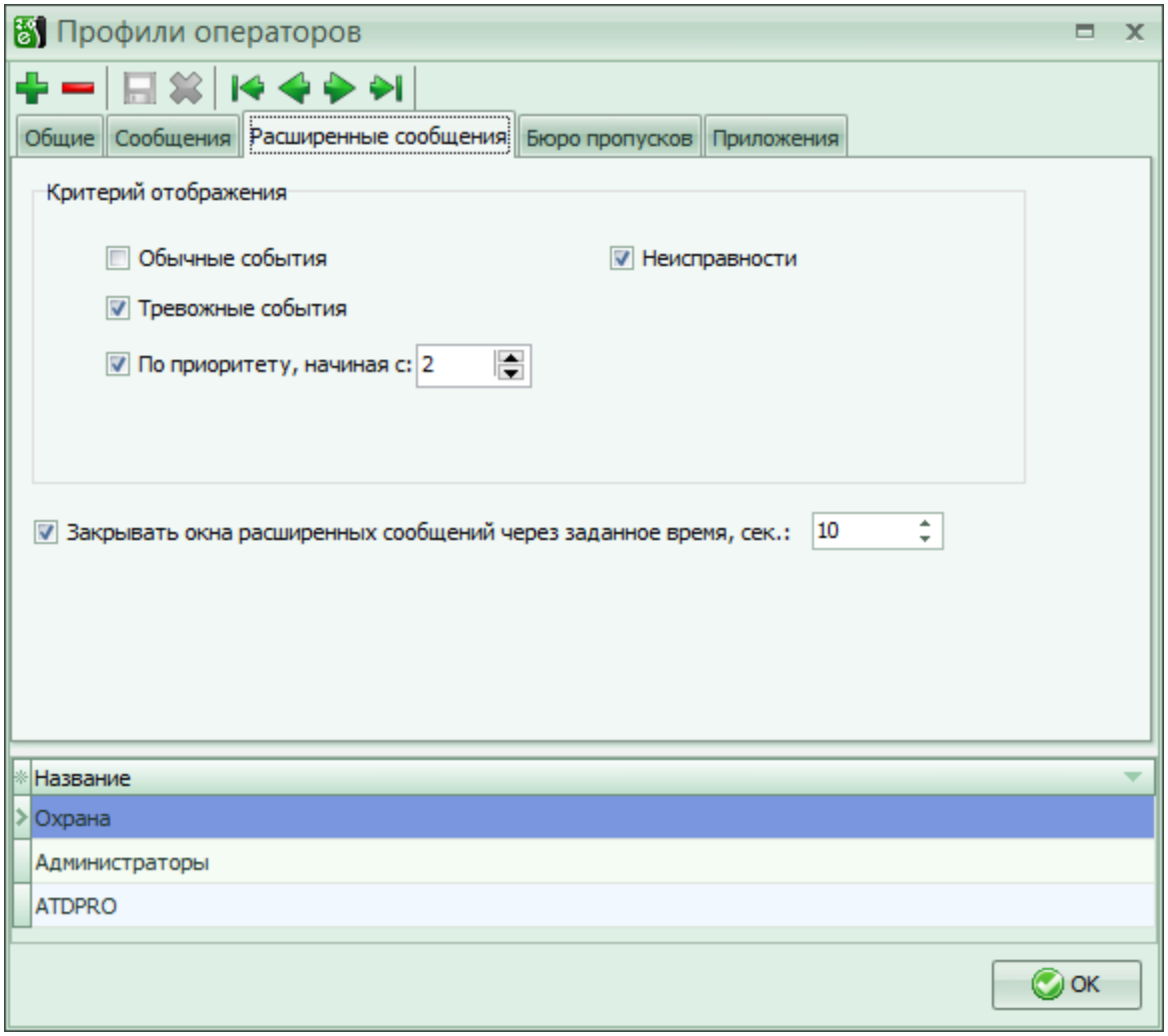

Рис. 13. Настройка параметров отображения расширенных сообщений

Окна расширенных сообщений (Рис. 14) предназначены для привлечения внимания оператора к особо важным сообщениям, поэтому к установке режима их отображения следует относиться особенно внимательно.

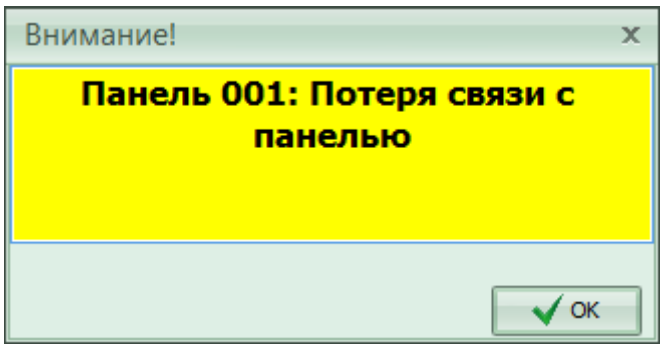

Рис. 14. Окно расширенного сообщения

Так же, как и для простых текстовых сообщений, система предоставляет возможность установки фильтра по типу события и его приоритету. Так, изображённые на Рис. 13 настройки обеспечивают вывод расширенных сообщений только для тревожных событий с приоритетом равным или большим 2.

> ***Внимание!*** *Для вывода расширенного сообщения, кроме выполнения условий фильтрации, у события должен быть приоритет, с включенной опцией «Выводить расширенное сообщение» (см. п. 5.10.4).*

Опция «*Закрывать окна расширенных сообщений автоматически*» (через заданный промежуток времени) предназначена для предотвращения загромождения основного окна программы излишней (устаревшей) информацией.

5.5.4 Настройки Бюро пропусков

Вкладка «Бюро пропусков» служит для настройки различных параметров профиля оператора относительно программного продукта Бастион-2 – АРМ Бюро пропусков. Инструкция по работе с данной вкладкой содержится в руководстве оператора Бастион-2 – АРМ Бюро пропусков.

5.5.5 Права на приложения

Вкладка «Приложения» (Рис. 15) служит для настройки прав запуска соответствующих приложений, входящих в состав поставляемой системы.

Опция «Право запуска АРМ оператора» позволяет разрешить, либо запретить вход пользователя, относящегося к соответствующему профилю, в приложение «Бастион-2 – АРМ Оператора».

Опцией «Право запуска Бастион-2 – АРМ УРВ про» можно указать, может ли оператор с данным профилем осуществлять вход в приложение УРВ Про.

Опция «Право запуска АРМ “Бюро пропусков”» управляет возможностью доступа к функционалу рабочего места Бюро пропусков.

Опция «Право доступа к системе WEB-заявок» позволяет выставить ограничение на доступ к системе WEB-заявок.

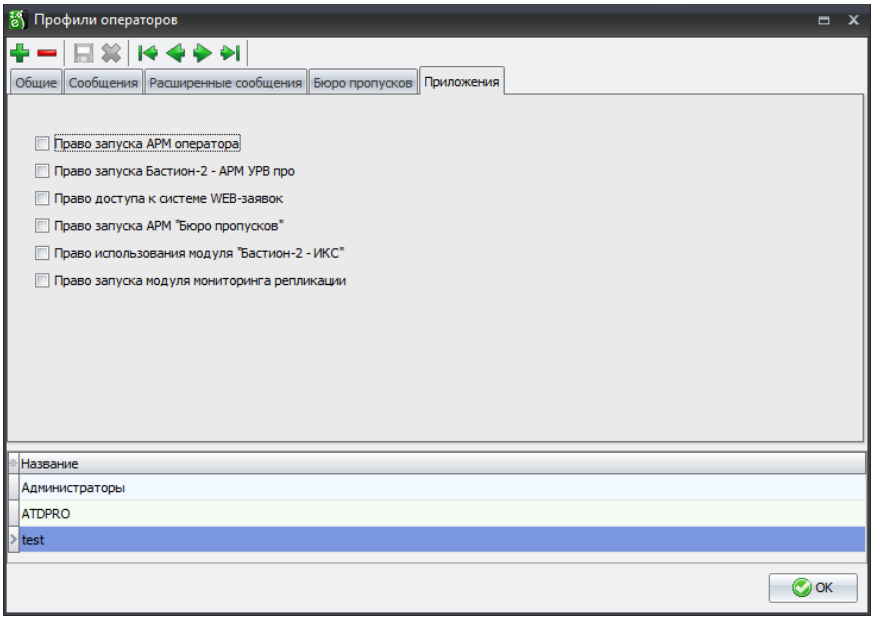

Рис. 15. Настройка прав доступа к приложениям

Опцией «Право использования модуля “Бастион-2 – ИКС”» можно разграничить доступ к модулю Бастион-2 – ИКС, основываясь на выбранном профиле оператора.

> ***Примечание***. *Профиль «Администраторы» имеет разрешения по всем вышеперечисленным опциям, при этом снять для него данные разрешения невозможно.*

5.6 Настройка списка операторов

Для настройки списка операторов системы выберите пункт «Операторы» на странице «Конфигурация». Откроется окно, представленное на Рис. 16.

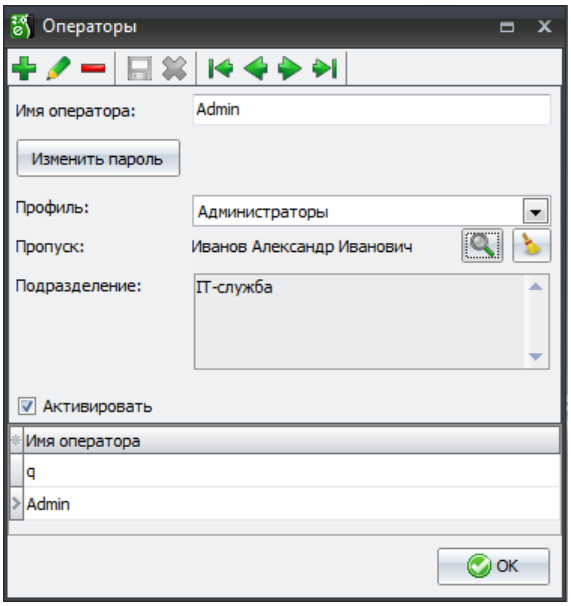

Рис. 16. Окно настройки операторов

Внимание! *По умолчанию, в системе присутствует единственный оператор с именем «q» и паролем «q». Рекомендуется сменить пароль этого оператора.*

Для добавления оператора можно нажать кнопку «+», при этом отобразится окно, представленное на Рис. 17. Здесь следует ввести имя пользователя и пароль с подтверждением.

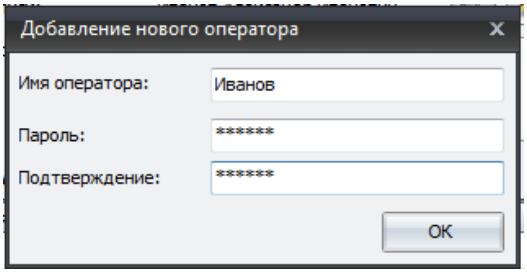

Рис. 17. Форма добавления оператора

Для смены пароля оператора следует нажать кнопку «Изменить пароль». В открывшемся окне необходимо ввести новый пароль и его подтверждение.

Каждому оператору должен быть назначен *профиль оператора*, определяющий его полномочия в системе и настройки пользовательского интерфейса.

Каждый оператор может быть связан с пропуском. Привязка задается через форму глобального поиска пропусков, вызываемую по кнопке «  ». Очистить привязку пропуска можно, нажав на кнопку «  ».

Привязка пропуска используется в следующих случаях:

1. Авторизация операторов в системе по карте доступа через настольный считыватель.
2. В модуле «Бастион-2 – Web-заявка» оператор может быть добавлен в схему согласования пропусков только, если он привязан к пропуску.
3. Отображение ФИО оператора в отчетах.

Оператора можно временно заблокировать, если снять у него флаг «Активировать». Заблокированный оператор не будет иметь доступ к системе.

5.7 Настройка прав доступа к устройствам

Для настройки прав доступа к устройствам системы выберите пункт «Доступ к устройствам…» на странице «Конфигурация».

Система предоставляет возможность разграничить к устройствам доступ по профилю оператора. Для установки ограничений выберите профиль оператора в списке в верхней части окна справа и устройство в левой части (см. Рис. 18). В правой нижней части окна будет отображён список доступных разрешений для выбранного устройства.

Дерево устройств может быть отображено в двух видах – по типу и по подключению. Изменить отображение можно из контекстного меню дерева.

Отображение устройств по типу облегчает массовую работу с однотипными устройствами – для изменения доступа ко всем устройствам типа «Дверь» достаточно дважды кликнуть по узлу «Двери» (узел развернется и все его дочерние элементы выделятся) и выбрать требуемые разрешения.

Отображение по подключению позволяет увидеть иерархию устройств в драйвере и понять, какие дочерние устройства добавлены к данному узлу.

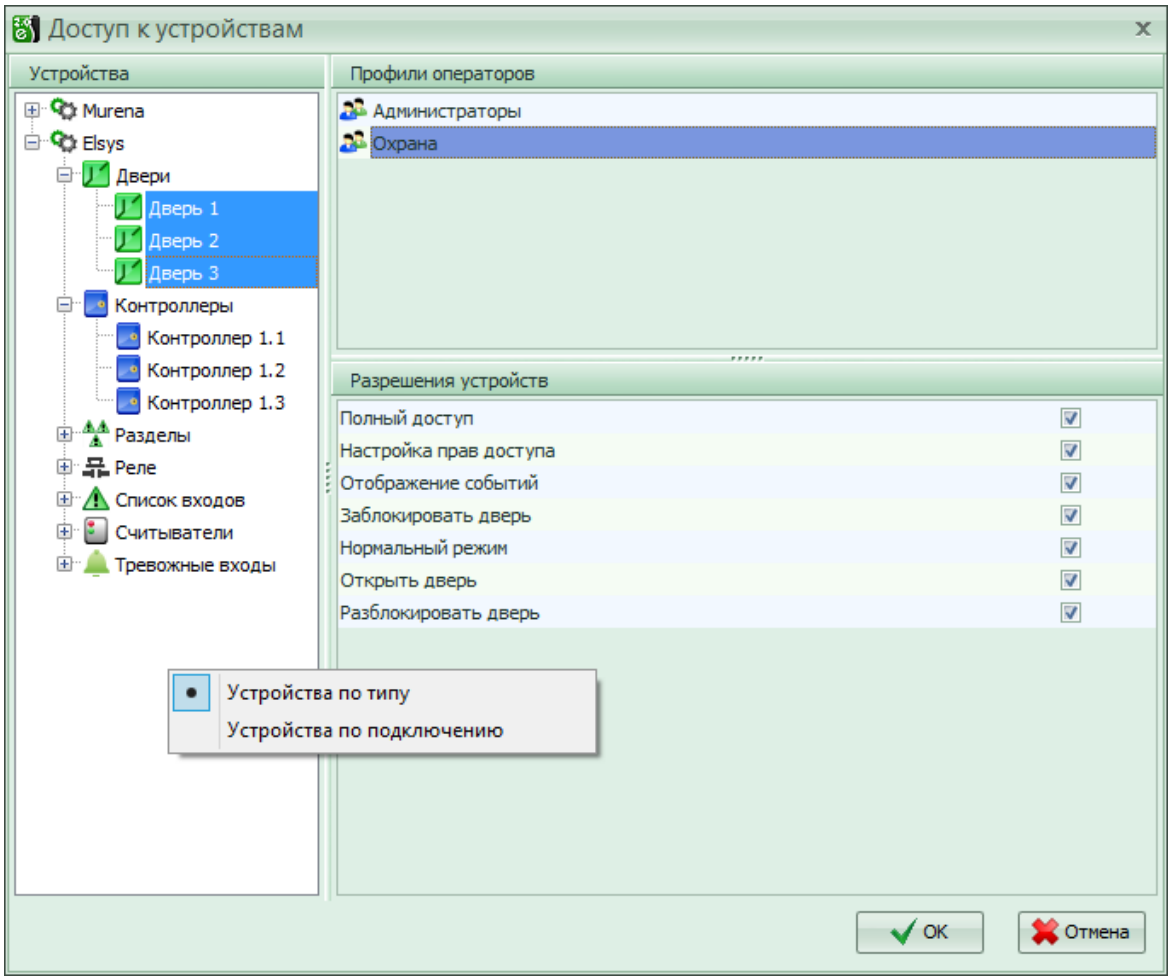

Рис. 18. Окно настройки прав доступа к устройствам

Содержимое списка разрешений зависит от типа выбранного устройства и управляющего драйвера. Набор разрешений, как правило, соответствует контекстному меню пиктограмм устройства.

Для всех элементов доступны 2 разрешения:

Полный доступ – разрешает все операции с устройством.

Настройка прав доступа – разрешает пользователю с выбранным профилем менять разрешения для этого устройства в данной форме.

> ***Внимание!*** *При добавлении новых устройств в систему, изначально все действия с ними будут разрешены для всех профилей операторов.*

5.8 Настройка прав доступа к подразделениям

Начиная с версии 2.1, в АПК «Бастион-2» поддерживается разделение прав доступа операторов к организациям и подразделениям. В версии 2.1 наличие прав на подразделение влияет на доступность оператору следующих возможностей:

- Отображение подразделений и выполнение любых операций с подразделением и его сотрудниками в АРМ «Бюро пропусков» и в АРМ «УРВ-Про»;
- Поиск местонахождения сотрудников, относящихся к заданному подразделению;
- Выбор подразделений для отчетов в АРМ «Генератор Отчётов».

Наличие прав на подразделение не влияет на отображение событий для оператора и фотоидентификацию.

Для настройки разграничения прав доступа по подразделениям, следует выбрать пункт «Настройка видимости подразделений» в ленте на странице «Конфигурация» в АРМ Оператора. Также, доступ к этой форме можно получить из АРМ «УРВ-Про», выбрав пункт меню «Управление – Настройки полномочий операторов». При это будет открыта соответствующая форма (Рис. 19):

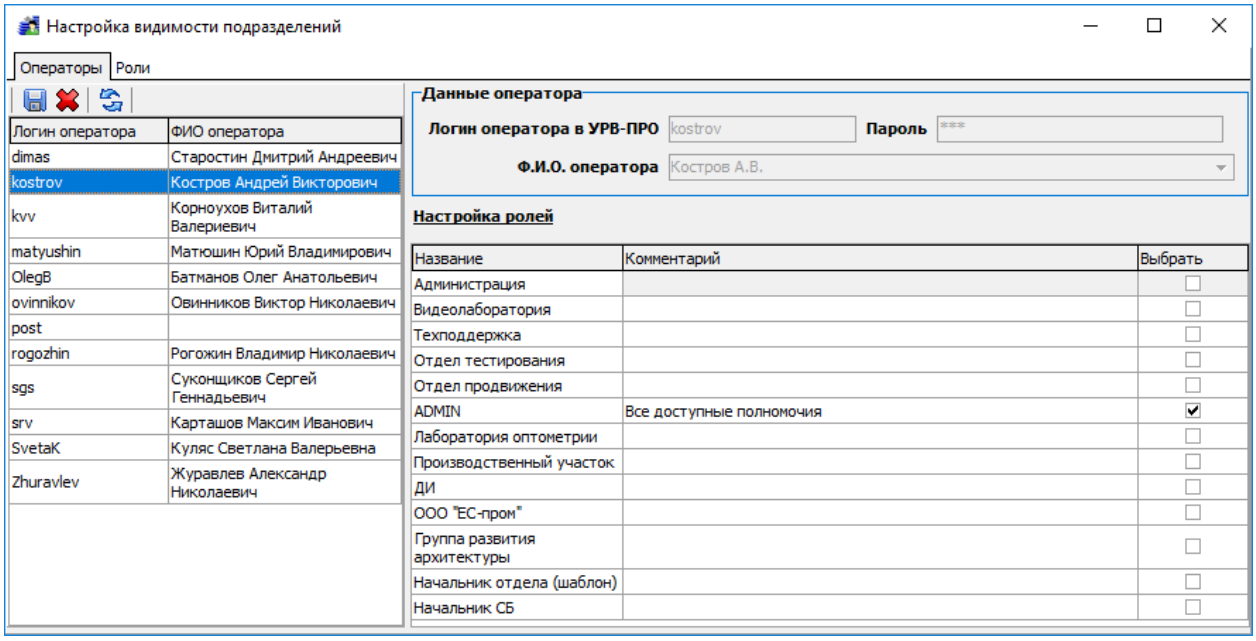

Рис. 19. Форма настройки видимости подразделений – настройка операторов

В системе можно создать ряд *ролей* операторов с разными полномочиями по доступу к подразделениям. Эти же *роли* будут использоваться в АРМ «УРВ-Про» для настройки разграничений доступа к функциям этого АРМ. После создания и настройки ролей, каждому оператору можно назначить одну или несколько ролей. Доступ к подразделению будет предоставлен оператору, если хотя бы у одной роли, назначенной ему, есть доступ к этому подразделению.

Видимость подразделений задаётся на странице «Роли» (см. Рис. 20). Для того, чтобы у роли ограничивались права на доступ к подразделениям, следует выбрать эту роль в левом списке,

установить флаг «Ограничить список подразделений», настроить список выбранных подразделений в нижней части окна и нажать кнопку «Сохранить изменения».

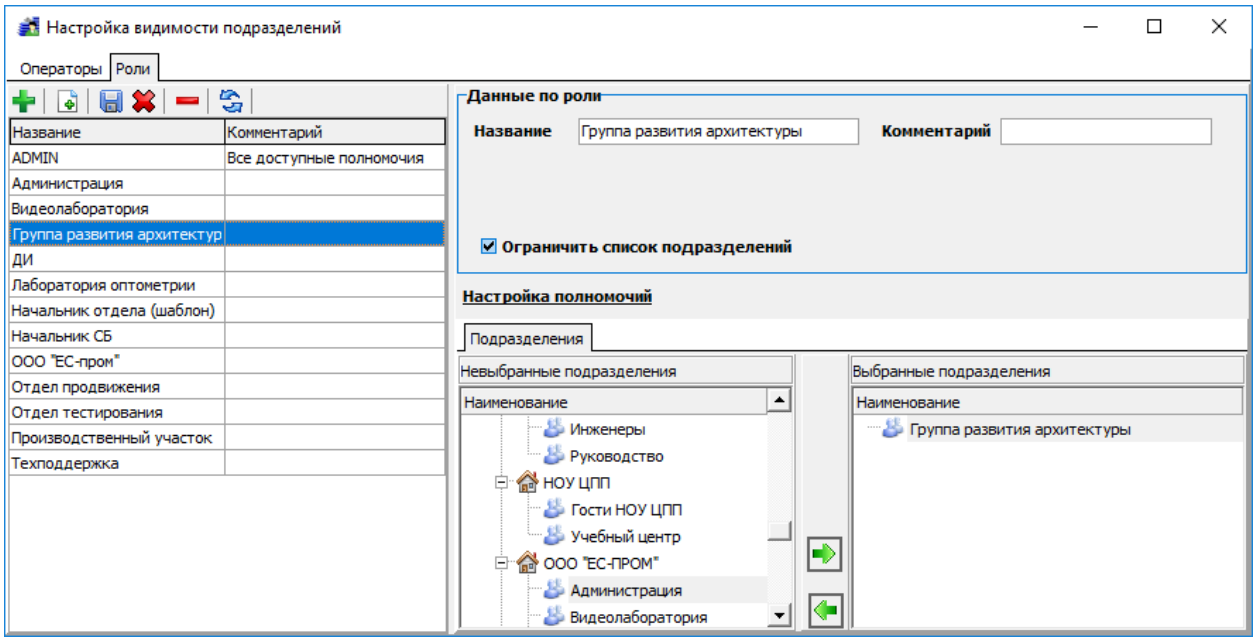

Рис. 20. Форма настройки видимости подразделений – настройка ролей

5.9 Настройка графических планов

Использование графических планов обеспечивает интерактивное управление устройствами и наглядное отображение текущего состояния устройств в системе.

На Рис. 21 изображены контекстные меню, с помощью которых оператор может управлять режимами различных устройств.

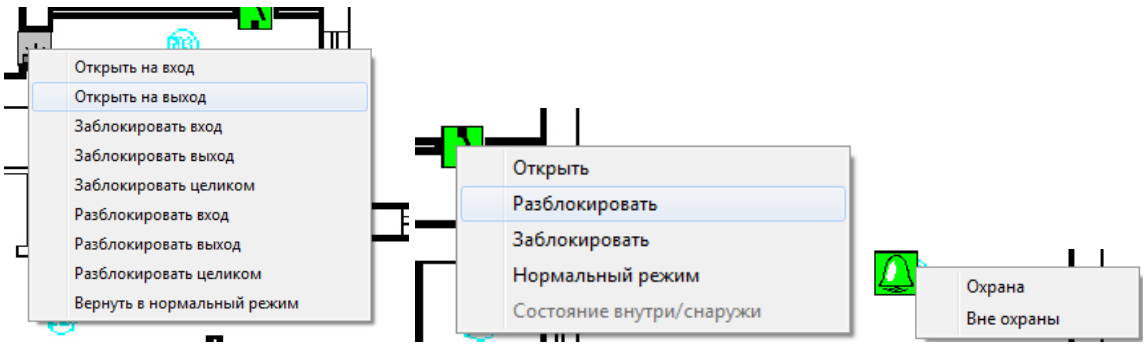

Рис. 21. Контекстные меню для управления устройствами.

В качестве графических планов могут быть использованы изображения как в векторном (*.DXF), так и в растровом (*.JPG, *.BMP) форматах. Для более корректного масштабирования плана рекомендуется использовать векторные планы. Не рекомендуется использовать растровые файлы с разрешением более 1024x1024.

5.9.1 Работа с деревом планов

Для входа в режим настройки графических планов выберите пункт меню «Конфигурация→Настройка планов». При этом откроется отдельное окно для редактирования планов, содержащее дерево устройств и дерево планов (Рис. 22).

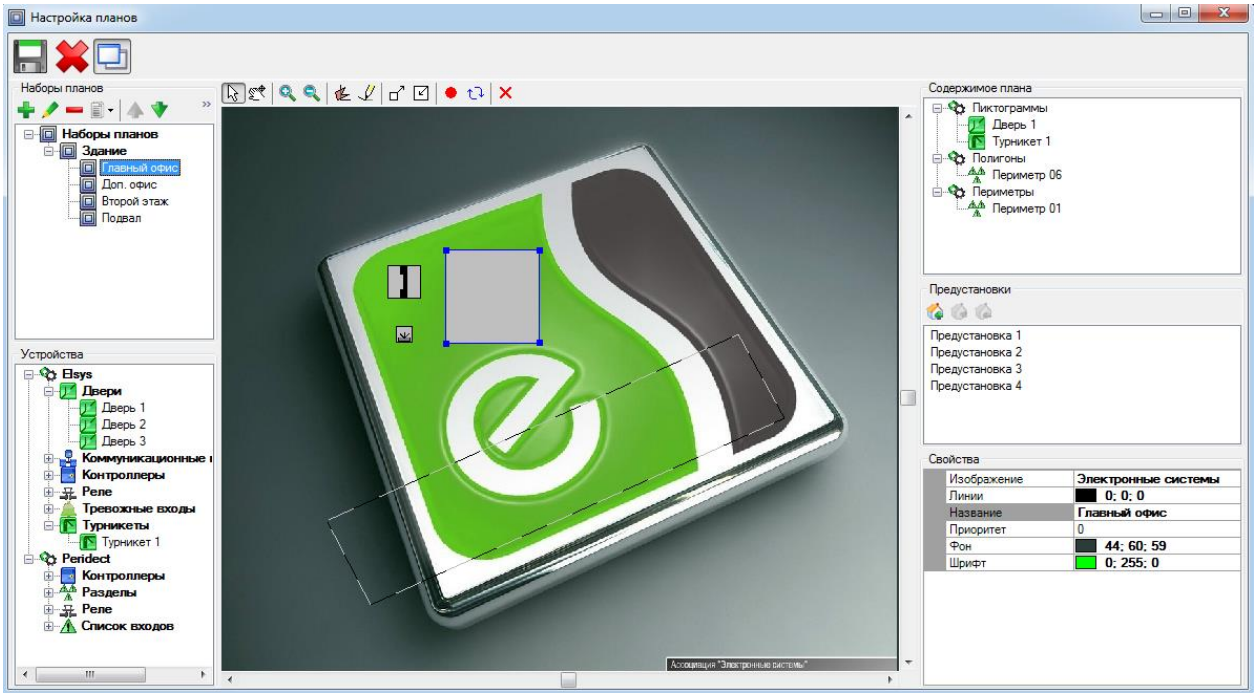

Рис. 22. Режим настройки планов

Изображения планов хранятся в базе данных. Управление ими осуществляется с помощью окна *«Список изображений»* (Рис. 23). Оно вызывается из свойства «Изображение» плана. В этом окне можно добавить из файла, переименовать, экспортировать в файл либо удалить изображение плана.

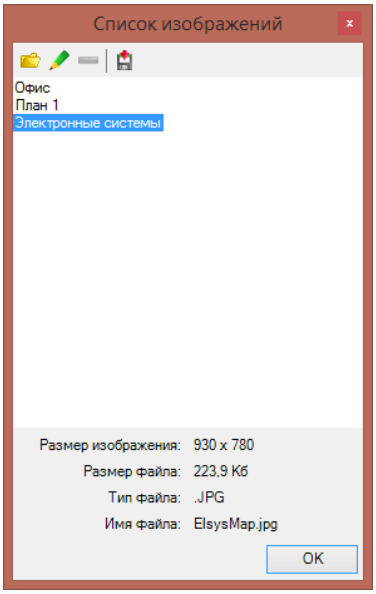

Рис. 23. Список изображений планов

Для добавления нового плана выберите нужный набор планов в дереве «Наборы планов» и нажмите кнопку «+» на панели над деревом планов. В появившемся окне укажите нужное изображение плана, либо добавьте новое. После этого можно переименовать добавленный план. Панель свойств плана содержит следующие параметры:

Изображение. Выбор изображения плана.

Линии. Выбор цвета линий векторного изображения.

Название. Текст, появляющийся в качестве названия плана (например, на закладках основной формы). Планы не могут иметь одинаковые названия.

Приоритет. Используется при включенном режиме автопереключения планов по событиям для выбора наиболее приоритетного плана с пиктограммой устройства-источника события.

Фон. Выбор цвета фона плана.

Шрифт. Выбор цвета шрифта для векторного изображения.

После добавления плана в главном окне появляется дополнительная вкладка с именем плана. Всего планов добавлено может быть до 255.

Для удаления объекта (плана, пиктограммы) из дерева планов, выберите этот объект и нажмите сочетание клавиш «Ctrl» + «Delete» или кнопку «Удалить с плана» («X») на панели над планом.

Привязка набора планов к профилю пользователя осуществляется в окне «Профили пользователей» (Рис. 11).

Для выхода из режима настройки планов закройте окно редактирования планов.

5.9.2 Расстановка пиктограмм

После добавления одного или нескольких планов на них могут быть вынесены пиктограммы устройств. Пиктограммы перетаскиваются (механизм «drag and drop») на план из окна дерева устройств. Все устройства в этом окне разделены на группы. Каждая группа соответствует одному драйверу, включенному в систему. Также существует возможность вынесения из дерева «Наборы планов» на план пиктограммы другого графического плана из того же набора планов для оперативного переключения и мониторинга состояния.

В режиме настройки карт возможно также перемещение, удаление или настройка свойств любых имеющихся на плане пиктограмм (с помощью контекстных меню пиктограмм). Имеется возможность выделять и выполнять основные действия (перемещение, удаление, изменение свойств) сразу нескольких пиктограмм. Для выделения группы пиктограмм поочерёдно щелкайте по ним мышью, удерживая клавишу Shift.

Перемещение пиктограмм и полигонов можно запретить для текущего плана. Для этого нажмите на кнопку «Фиксация иконок» на панели над деревом планов.

Удалить пиктограмму можно, выделив её и выбрав из её контекстного меню пункт «Удалить».

5.9.3 Предустановки

Для каждого плана можно задать набор предустановок, включающих в себя координаты горизонтального и вертикального сдвига, а также коэффициент приближения, переход к которым осуществляется в дежурном режиме при выборе соответствующего пункта в контекстном меню плана. Задать предустановку можно с помощью пункта контекстного меню «Предустановка→Задать», либо с помощью кнопки «Добавить предустановку» с панели «Предустановки». В панели свойств предустановки есть возможность задать её имя, вручную ввести сдвиги относительно горизонтали и вертикали вместе с приближением.

5.9.4 Рисование многоугольников

Каждое устройство в АПК «Бастион-2» может быть представлено на плане не только пиктограммой, но и многоугольником произвольной формы (см. Рис. 22).

Для того чтобы нарисовать многоугольник проделайте следующие операции:

Перейдите в режим рисования многоугольников. Для этого щелкните правой кнопкой мыши на свободном месте на плане и выберите пункт «Полигон».

Левой кнопкой мыши щелкайте в углах требуемого многоугольника.

Для завершения рисования щелкните правой кнопкой мыши. Две крайние вершины будут соединены между собой. На экране появится окно с деревом устройств (Рис. 24). Выберите устройство, которое будет обозначать многоугольник.

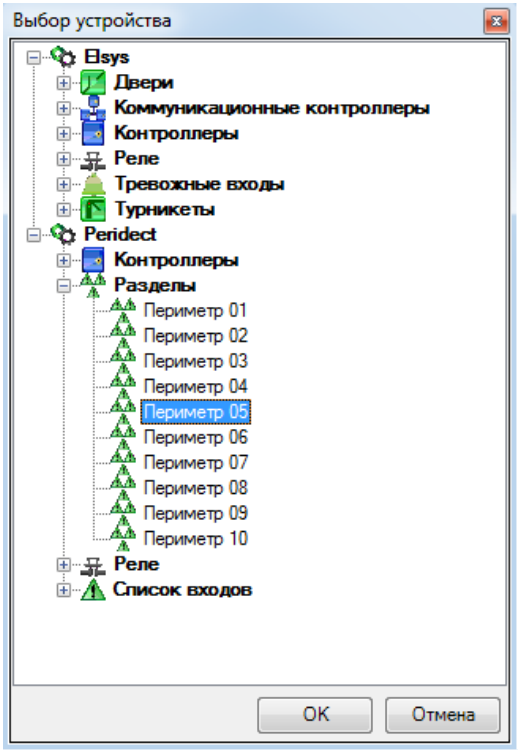

Рис. 24. Окно выбора устройства для многоугольника

Для выхода из режима рисования многоугольников из панели меню плана выберите пункт «Выбор».

Координаты и количество вершин многоугольника или периметра можно изменить после окончания рисования. Для этого необходимо нажать на кнопку «…» в поле «Вершины» свойств многоугольника. Появится форма (Рис. 25), в которой можно отредактировать координаты X и Y каждой вершины, а также добавить новые или удалить лишние.

5.9.5 Настройка свойств пиктограмм

С каждой пиктограммой или многоугольником связана панель свойств, расположенная в правом нижнем углу окна редактирования.

Здесь редактируются общие для всех типов устройств (кроме пиктограмм графических планов) свойства:

Направление пиктограммы. Кнопки со стрелками позволяют выбрать одно из направлений отображения пиктограммы. Для некоторых устройств доступна только часть направлений.

Размер. С помощью кнопок в группе размер можно установить требуемый масштаб пиктограммы.

Устройство. Свойство недоступно для редактирования и служит в качестве источника информации о привязанном к пиктограмме устройстве.

Не показывать пиктограмму в нормальном состоянии. Позволяет установить режим, при котором пиктограмма будет отображаться только при возникновении тревоги или неисправности (обычно этот режим используется для охранных шлейфов).

Вид. Если устройство может отображаться при помощи нескольких разных пиктограмм, то из выпадающего списка «Вид» можно выбрать вид пиктограммы.

Для пиктограммы плана вместо свойства «Устройства» доступно свойство «План», которое позволяет выбрать необходимый план из соответствующего набора.

Для многоугольников в этом же окне можно задать *степень прозрачности* в процентах (0 – непрозрачный, 100 – полностью прозрачный).

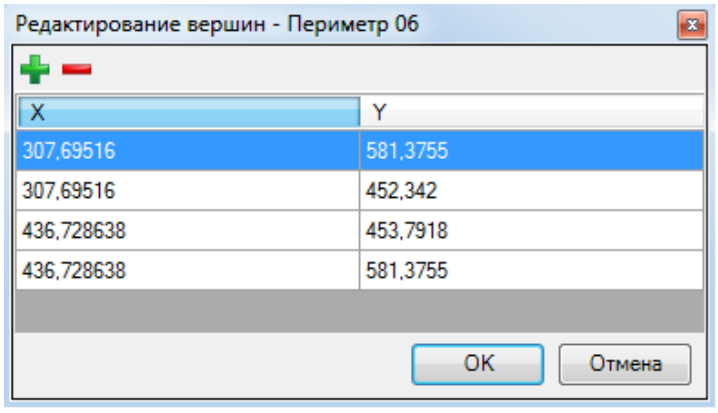

Рис. 25. Редактирование вершин многоугольника

5.9.6 Дополнительные параметры графической подсистемы

Если у вас возникают проблемы с отображением графических планов, то следует изменить один из параметров графической подсистемы АПК «Бастион-2». Это можно сделать, выбрав в ленте

«Конфигурация» на закладке «Система» пункт «Локальные настройки» закладка «Графика» (см. Рис. 26).

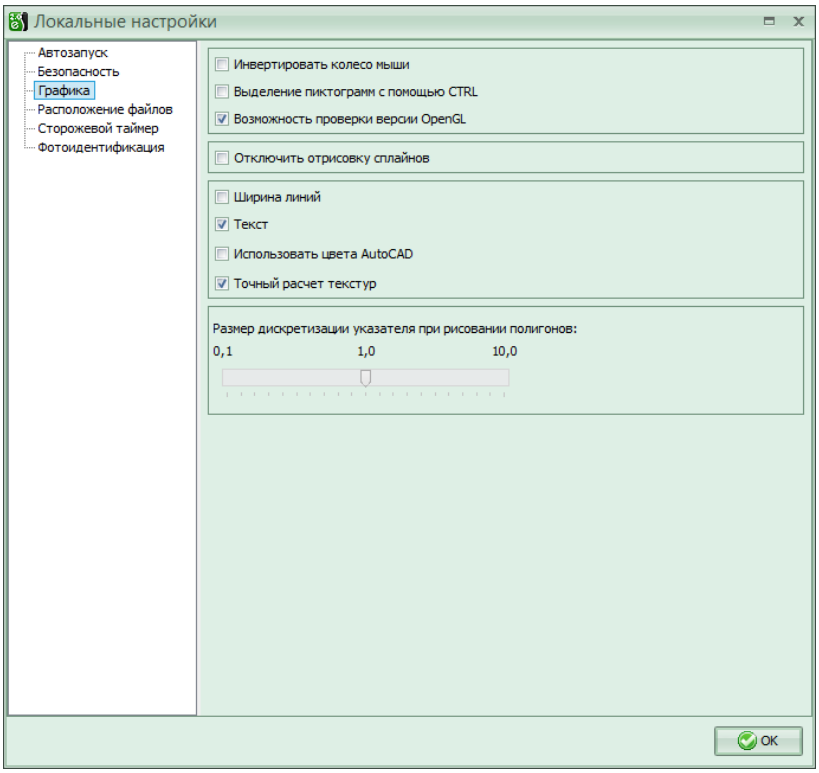

Рис. 26. Окно настройки параметров графической подсистемы

5.9.7 Редактор пиктограмм

В состав АПК «Бастион-2» входит отдельная утилита, позволяющая изменять вид пиктограмм устройств. Для её запуска можно в меню «Пуск» выбрать пункт «ES-Prom – АПБ «Бастион-2» – Администрирование – Редактор пиктограмм». Откроется форма редактора (Рис. 27).

Для каждого типа устройств может быть определено до 5 видов пиктограмм. Конкретный вид указывается в свойствах каждой пиктограммы, вынесенной на план. Для каждого «вида» пиктограмм необходимо нарисовать изображения под каждое состояние, доступное для этого типа устройств. Например, чтобы добавить новый вид пиктограммы «Тревожной кнопки», следует нарисовать изображение для 3-х состояний: «Состояние неизвестно», «Нормальное состояние» и «Недоступно».

Следует иметь в виду, что цвет фона пиктограммы не настраивается и зависит от текущего состояния устройства. Фон может быть серым (в нормально или не активном состоянии), зеленым (активность), жёлтым (неисправность) или красным (тревога). Возможные цвета фона следует учитывать при разработке вида пиктограммы.

Все пиктограммы, используемые в АПК «Бастион-2», хранятся в файле <Bastion2>\Maps\dlist.xml.

Окно редактора пиктограмм включает строку главного меню, панель инструментов, дерево пиктограмм и, собственно, поле для рисования.

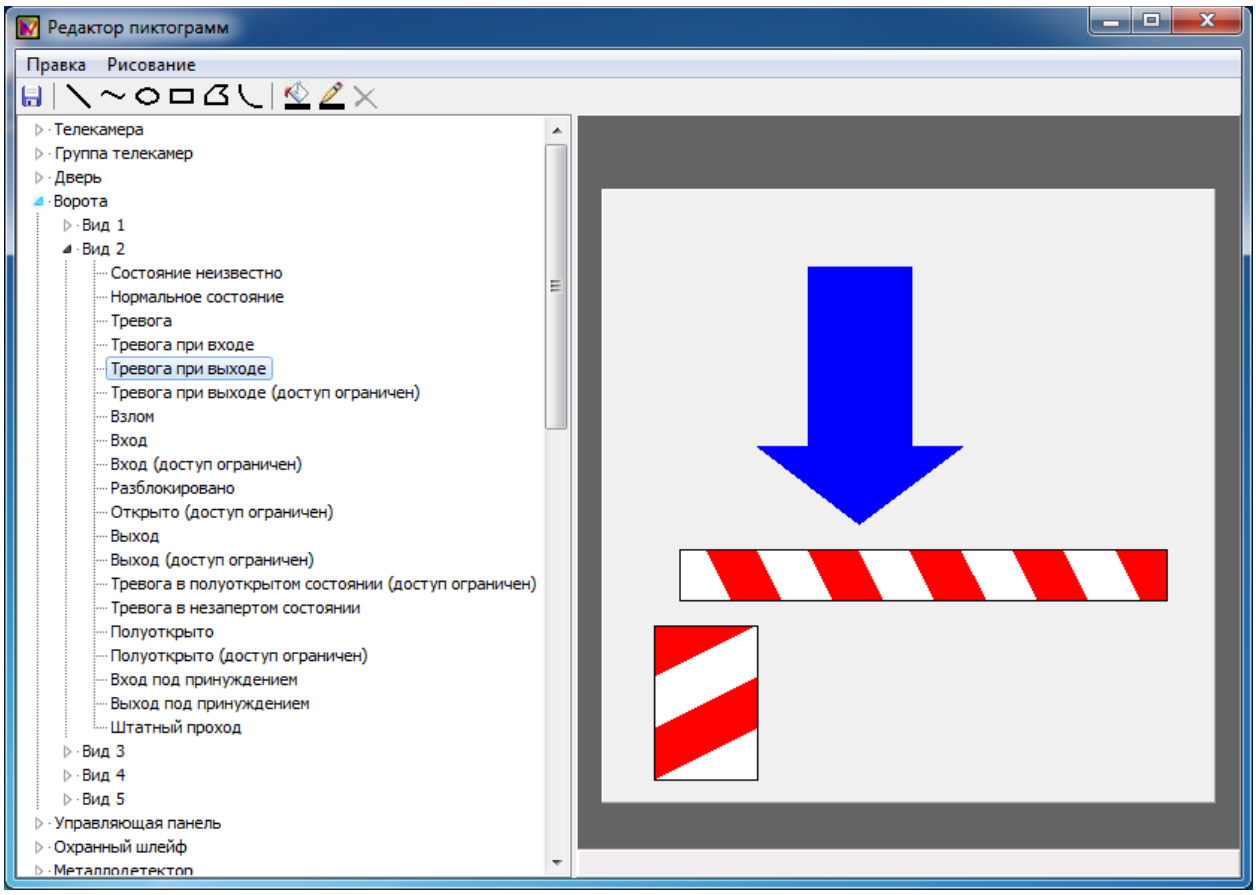

Рис. 27. Общий вид редактора пиктограмм

Строка главного меню содержит два пункта: «Правка» и «Рисование».

Пункт меню «Правка» содержит опции для работы с буфером обмена («Вырезать», «Копировать», «Вставить»), а также опции «Выделить всё» и «Удалить всё».

Пункт меню «Рисование» позволяет создавать пиктограммы из простых элементов. Этот пункт содержит следующие опции:

- «Создать…»
- (далее нужно выбрать нужный элемент: линию, многоугольник, и т.п.);
- «Переместить…»
- (на передний или на задний план);
- «Повернуть…»
- (на 90 градусов, на 180 градусов или на 270 градусов);
- «Отразить…»
- (по горизонтали или по вертикали)

На панели инструментов, расположенной ниже строки главного меню, находятся кнопки, дублирующие основные функции меню: кнопка «Сохранить», кнопки для рисования различных линий и фигур, кнопки выбора цвета линий и фигур, кнопка «Удалить»).

В левой части окна находится иерархический список типов устройств и их состояний, для которых можно создавать пиктограммы (телекамера, дверь, ворота и т. п.) Для каждого типа устройств может быть определено до пяти видов пиктограмм.

Создание, удаление и редактирование пиктограмм производится на специальном поле в центре окна редактора пиктограмм. Для этого необходимо выбрать в левой части экрана нужное устройство и на белом поле нарисовать соответствующую пиктограмму.

Чтобы нарисовать круг или прямоугольник, можно выбрать соответствующую кнопку на панели инструментов, щёлкнуть левой кнопкой мыши в поле для рисования и растянуть фигуру до нужного размера, а затем ещё раз щёлкнуть левой кнопкой мыши, чтобы закончить рисование.

Чтобы нарисовать многоугольник, можно выбрать кнопку «Многоугольник» на панели инструментов, затем в поле для рисования левой кнопкой мыши отметить точки углов многоугольника. Чтобы закончить рисование, на последнем углу многоугольника нужно щёлкнуть правой кнопкой мыши.

Чтобы нарисовать прямую линию, можно выбрать кнопку «Линия» на панели инструментов, щёлкнуть левой кнопкой мыши в поле для рисования и нарисовать линию нужной длины, а затем ещё раз щёлкнуть левой кнопкой мыши, чтобы закончить рисование.

Чтобы нарисовать изогнутую линию, можно выбрать кнопку «Дуга» на панели инструментов, левой кнопкой мыши отметить начало дуги, затем на показанной пунктиром окружности выделить нужную часть, и снова щёлкнуть левой кнопкой мыши в точке конца дуги.

Чтобы нарисовать ломаную линию, можно выбрать кнопку «Полилиния» на панели инструментов, левой кнопкой мыши отметить узлы ломаной, затем на последнем узле щёлкнуть правой кнопкой мыши, чтобы закончить рисование.

Для редактирования цвета фигуры можно выделить её левой кнопкой мыши, затем выбрать нужный цвет заливки на панели инструментов.

Для редактирования цвета контура фигуры можно выделить её левой кнопкой мыши, затем выбрать нужный цвет линии на панели инструментов. Толщина контура не регулируется.

Для редактирования цвета линии можно выделить её левой кнопкой мыши, а затем выбрать нужный цвет линии на панели инструментов.

Можно скопировать готовую пиктограмму из одного вида или устройства для другого. Сделать это можно с помощью меню «Правка»: сначала выбрать пункт «Выделить всё», затем - пункт «Копировать» и, наконец, пункт «Вставить», чтобы поместить скопированное изображение на требуемое место.

5.10Настройка параметров обработки событий

5.10.1 Время актуальности событий

Система позволяет указать длительность времени, в течение которого событие будет считаться актуальным (Конфигурация – Общие настройки – Обработка событий). Время актуальности

события позволяет указать, что для событий, пришедших с опозданием на заданное время (в минутах), не требуется:

- выводить расширенное сообщение;
- выполнять сценарии;
- производить фотоидентификацию.

Если указать 0 – то время актуальности событий ограничиваться не будет.

Дополнительно, можно запретить выводить устаревшие события совсем, если снять флаг «Выводить устаревшие события».

5.10.2 Обработка подтверждений событий

В системе есть возможность настроить, когда будет требоваться подтверждение событий, каким образом оператор должен подтверждать события и как подтверждения будут учитываться при определении текущего состояния устройства.

В «Общих настройках» на странице «Обработка событий» имеются следующие настройки (Рис. 28):

Требовать подтверждения нештатных событий только с приоритетом не менее заданного. Все события с приоритетом ниже заданного будут считаться штатными и выводиться в окне штатных сообщений справа. Подтверждения будут требовать только события с приоритетом выше заданного. Таким образом можно переопределить поведение системы по умолчанию.

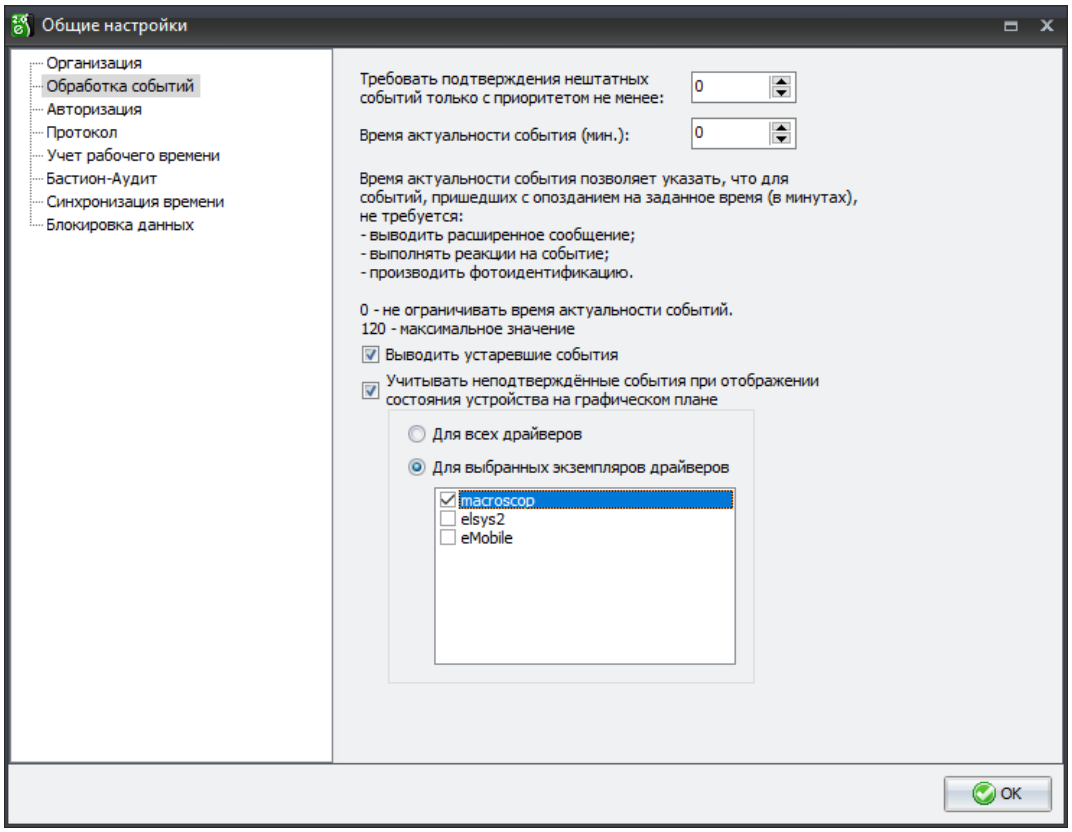

Рис. 28. Общие настройки обработки событий

Учитывать неподтверждённые события при отображении состояния устройства на графическом плане. При включенном флаге (по умолчанию), текущее состояние устройства на графических планах отображается с учётом наличия неподтверждённых событий для этого устройства. Устройство не будет возвращено в нормальное состояние до подтверждения оператором всех его тревожных событий. При выключенном флаге устройство вернётся в нормальное состояние сразу при получении любого события, переводящего его в штатный режим (например, «Сброс тревоги», «Штатный вход» или «Снятие с охраны»). Имеется возможность указать это поведение отдельно для каждого экземпляра драйвера (Рис. 28).

Система позволяет производить подтверждение в двух режимах – с запросом причины события или без него. Эта настройка задаётся для каждого профиля оператора отдельно (см. п. 5.5.2). Причина события при подтверждении выбирается из предварительно заполненного справочника.

Для настройки списка причин служит форма «Причины тревожных сообщений», вызвать которую можно из блока «События и реакции» вкладки «Конфигурация» главного окна. Для удобства, в системе уже добавлен список наиболее вероятных причин тревожных событий (Рис. 29). При подтверждении оператор также сможет ввести комментарий к событию.

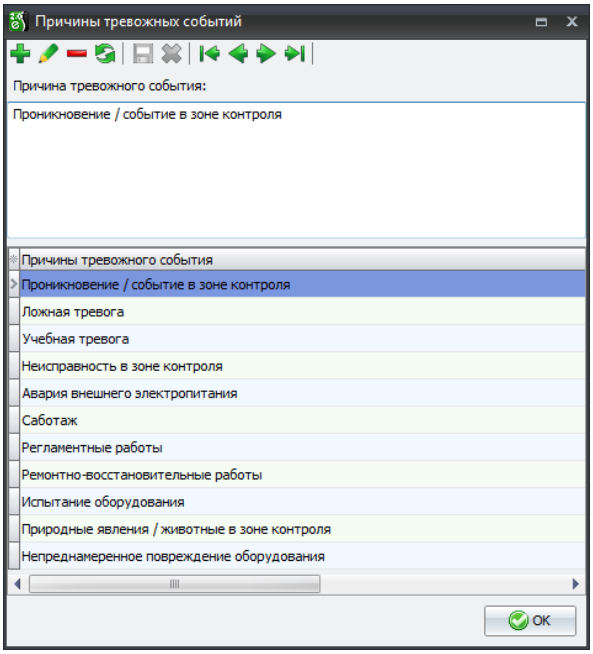

Рис. 29. Причины тревожных событий. Настройка по умолчанию

5.10.3 Параметры записи протокола

Для настройки параметров записи протокола следует выбрать в ленте «Конфигурация» на закладке «Система» пункт «Общие настройки» и открыть страницу «Протокол» (Рис. 30).

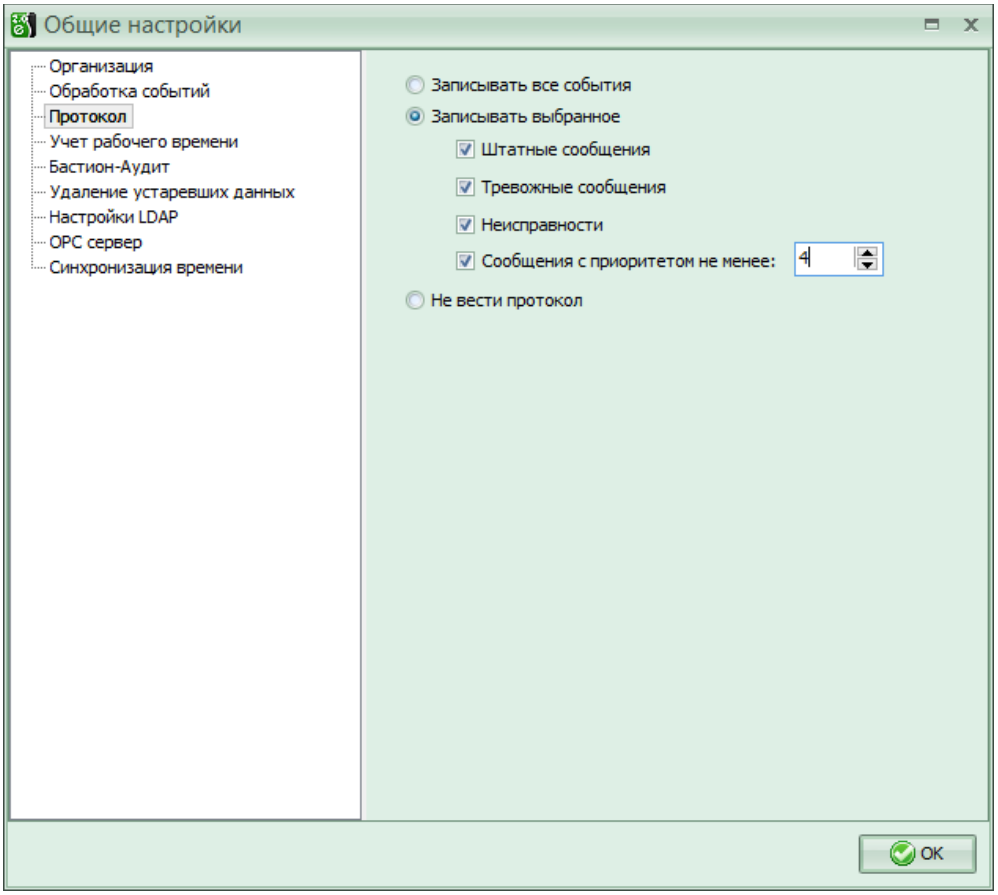

Рис. 30. Страница настройки параметров записи протокола

На этой странице можно указать, какие события будут записываться в базу данных протокола. Варианты записи основного протокола:

- записывать все события (по умолчанию);
- записывать выбранное;
- не вести протокол.

Если выбрана опция «записывать выбранное», то активизируется список опций, определяющих критерий записи:

Штатные сообщения. При включенной опции штатные сообщения, поступающие от оборудования комплекса, будут записываться в протокол.

Тревожные сообщения. При включенной опции тревожные сообщения будут записываться в протокол.

Неисправности. При включенной опции сообщения о неисправностях будут записываться в протокол.

Сообщения с приоритетом не менее. Если флаг включен, то дополнительно будет проверяться приоритет сообщения. Запись будет произведена только в том случае, если приоритет сообщения больше либо равен указанному и сообщение входит в одну из перечисленных выше групп.

5.10.4 Редактирование событий

Текст и приоритет событий, заданные по умолчанию, можно произвольно изменять. При этом имеется возможность указать отдельно для каждого устройства свои параметры.

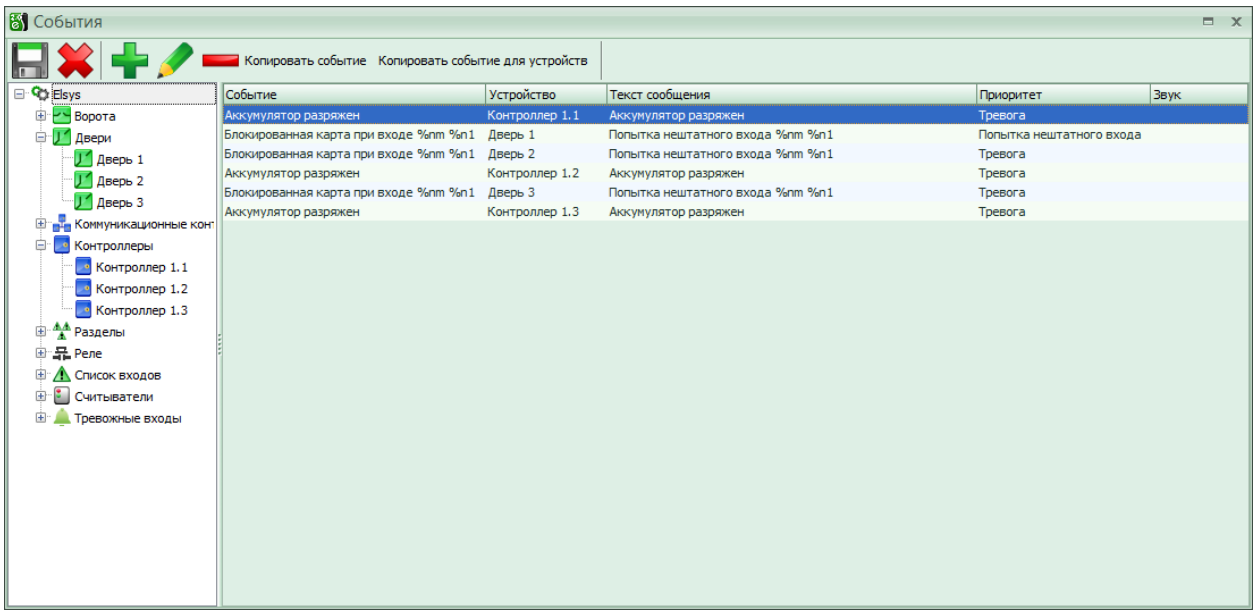

Рис. 31. Окно редактирования событий

Для выполнения этих действий следует выбрать в ленте «Конфигурация» на закладке «События и реакции» пункт «События…», после чего появится окно, изображённое на Рис. 31.

В левой части формы находится дерево устройств-источников событий, в правой – список переопределённых событий для выбранного устройства и всех его дочерних устройств.

Дерево устройств, аналогично форме «Доступ к устройствам», может быть отображено в двух видах – по типу и по подключению. Изменить отображение можно из контекстного меню дерева.

Для переопределения события выберите устройство-источник в дереве слева и нажмите кнопку «+» в панели инструментов. В появившейся форме (см. Рис. 32) настройте требуемые параметры события и нажмите «ОК».

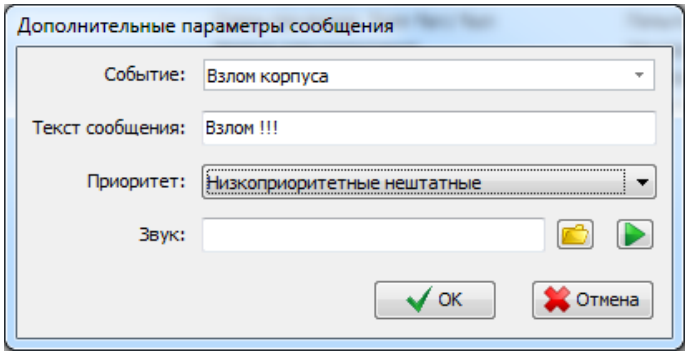

Рис. 32. Окно добавления события

Назначение отдельных параметров событий:

Событие – служит для выбора события, параметры которого необходимо переопределить.

Текст сообщения – служит для ввода нового текстового сообщения для выбранного события, которое будет отображаться в одной из областей сообщений. Текст сообщения может содержать *символы форматирования*, обеспечивающие вставку переменной информации. Такие символы могут находиться в любом месте сообщения и обеспечивают вывод следующих данных:

%dn Название устройства, вызвавшего событие. Может использоваться с любым типом драйвера.

%cn Номер карты доступа. Позволяет включить в сообщение номер предъявленной карты доступа для сообщений, формируемых устройствами системы контроля доступа. Если событие не содержит кода карты, символ будет выведен без изменений.

%cv Позволяет включить в сообщение номер транспортного средства, перекодированный из номера карты. Может использоваться для случаев, когда карту выдавали на основе номера транспортного средства.

%nm Фамилия владельца карты доступа. Символ используется в тех же случаях, что и предыдущий.

%n1 Имя владельца карты доступа.

%n2 Отчество владельца карты доступа.

%pn PIN-код, набранный владельцем карты доступа.

%st Site-код (серия) предъявленной карты доступа.

%nb Распознанный номер. Используется для систем транспортного учета.

Указанные коды могут использоваться в любой комбинации.

Приоритет – позволяет назначить один из заранее созданных приоритетов текущему событию.

Звук – позволяет выбрать файл звукового оповещения о событии. Это поле не является обязательным, поэтому его можно оставить пустым. АПК «Бастион-2» использует звуковые файлы формата Wave audio (.wav), которые по умолчанию должны располагаться в каталоге «<Bastion>\SOUND\». Имя файла можно задать вручную (непосредственный ввод текста в поле) или выбрать из имеющихся в стандартном окне открытия файла.

Существует возможность выполнить копирование событий. Для этого служат кнопки "Копировать событие для устройств..." и "Копировать событие...". В первом случае пользователь получает возможность установить для нескольких устройств один и тот же вид обработки какого-либо события сразу. Во втором – установить для текущего устройства одинаковые параметры обработки нескольких различных событий. При копировании имеется возможность выбрать, какие именно параметры копировать – текст события, приоритет, звук.

Для сохранения изменений необходимо нажать кнопку «Сохранить» в панели инструментов.

5.10.5 Настройка приоритетов событий

Для редактирования приоритетов событий выберите в ленте «Конфигурация» на закладке «События и реакции» пункт «Приоритеты событий…». То же самое окно можно вывести нажатием кнопки «Приоритет» в окне «Редактирование событий» (Рис. 33).

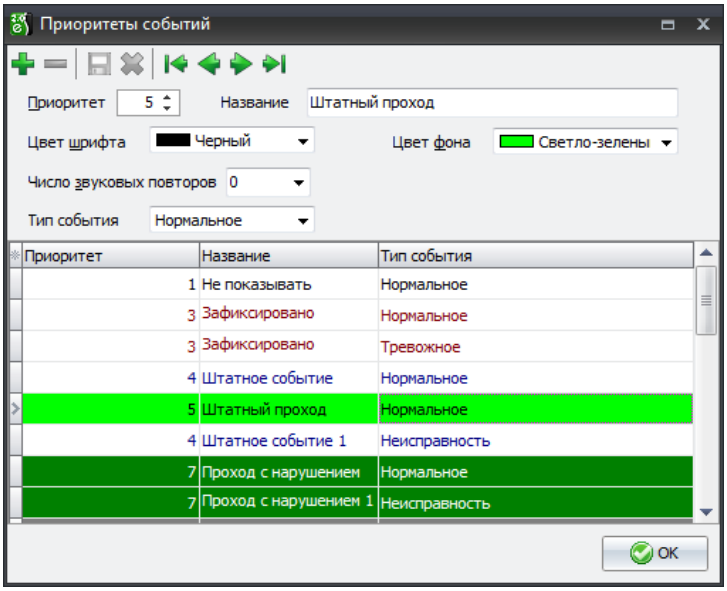

Рис. 33. Окно настройки приоритетов событий

Под *приоритетом события* уровень важности события, определяющий способ его вывода и обработки. Например, можно выводить только события с приоритетом больше заданного, выводить окно фотоидентификации для событий с приоритетом не менее заданного и т. д.

Каждая запись в таблице приоритетов событий содержит следующие поля:

Приоритет – служит для ввода числового значения уровня приоритета события. Число должно находиться в диапазоне от 0 до 99. Самый низкий приоритет имеет значение 0, самый высокий – 99.

Название – позволяет ввести название приоритета. Длина названия не должна превышать 40 символов, включая пробелы, например «Не показывать».

Цвет шрифта – обеспечивает выбор цвета шрифта, которым в окно тревожных или штатных сообщений будет выведено сообщение о событии с данным приоритетом.

Цвет фона – служит для выбора цвета фона, на котором в окно тревожных или штатных сообщений будет выведено сообщение о событии с данным приоритетом.

Число звуковых повторов – служит для указания количества повторов голосового сообщения при возникновении события с данным приоритетом.

Тип события – служит для задания типа выбранному событию. Может принимать одно из следующих значений: нормальное, тревожное, неисправность.

5.10.6 Установка шрифтов для отображения событий

Система позволяет задать вид и размер шрифтов, используемых для отображения обычных и тревожных сообщений. Для этого необходимо выбрать в ленте «Конфигурация» в закладке «Локальные настройки» пункт «Шрифты». Шрифты задаются на каждом рабочем месте отдельно и не привязываются к профилю пользователя. Цвет шрифта задаётся приоритетом события и в данном окне не регулируется.

5.10.7 Маршрутизация сообщений

Маршрутизация сообщений позволяет установить, каким пользователям, в зависимости от их профиля, будут передаваться сообщения от определенных устройств. Перед настройкой маршрутизации необходимо определить профили пользователей (см. п. 5.5). По умолчанию маршрутизация выключена, то есть все пользователи получают все сообщения, с учётом фильтров в профиле пользователя. Для настройки маршрутизации сообщений необходимо выбрать в ленте «Конфигурация» в закладке «События и реакции» пункт «Маршрутизация сообщений».

В появившемся окне (см. Рис. 34) необходимо выбрать профиль пользователя и отметить те устройства (поставить знак «✔» напротив названия устройства), наблюдение за которыми будут осуществлять пользователи с данным профилем.

> ***Внимание!*** *Если новые устройства были добавлены после включения маршрутизации сообщений, то, чтобы от них начали поступать сообщения, необходимо включить эти устройства в окне настройки маршрутизации для каждого пользовательского профиля, где это требуется.*

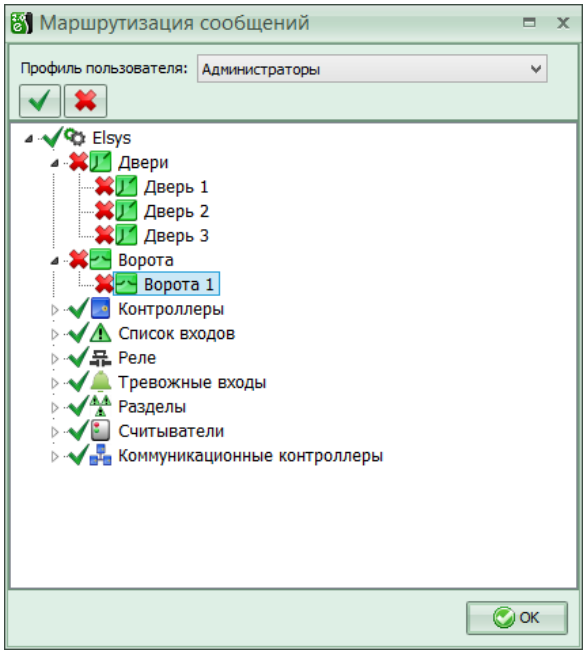

Рис. 34. Окно настройки маршрутизации сообщений

5.11Настройка сценариев и реакций на события

Сценарий – это последовательность действий, которая может выполняться автоматически при возникновении какого-либо события, по расписанию, либо выполняться по команде оператора.

Для создания и редактирования сценариев выберите в ленте «Конфигурация» в закладке «События и реакции» пункт «Сценарии…». При этом будет выведено окно следующего вида:

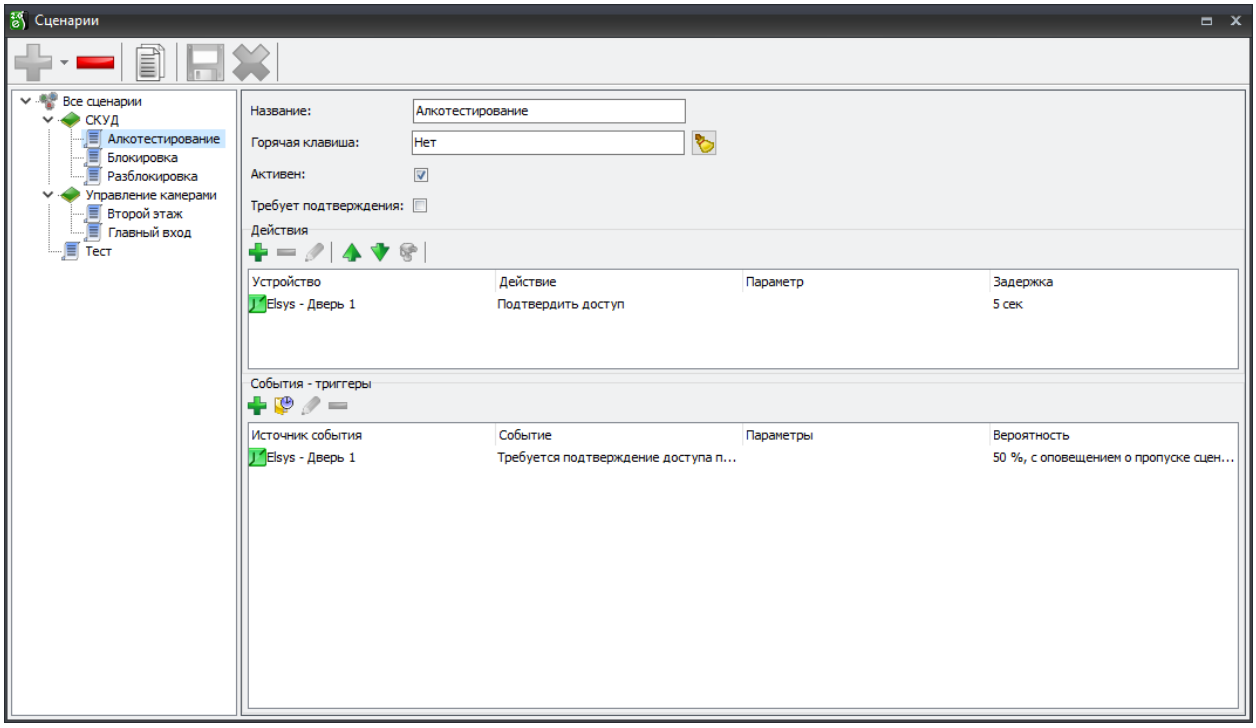

Рис. 35. Окно редактирования сценариев

Для *добавления нового сценария* нажмите кнопку "+" в левом верхнем углу окна, либо выберите пункт «Создать сценарий» в контекстном меню списка сценариев.

Заново созданный сценарий не содержит действий. Для *добавления действий* нажмите кнопку "+" в панели «Действия». При этом появится окно выбора действий (Рис. 36).

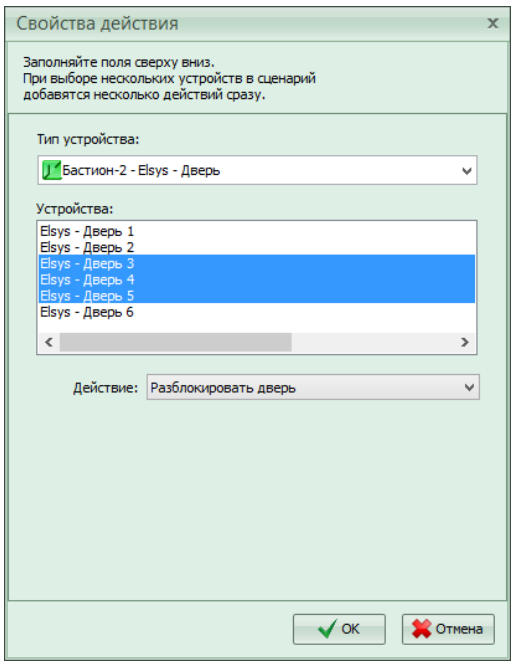

Рис. 36. Окно редактирования элементов сценария

При добавлении действий можно сразу выбрать несколько устройств и общее действие для них.

Все действия сценария выполняются в том порядке, в котором они присутствуют в списке действий. Для перемещения действий используются кнопки-стрелки над списком действий.

Для каждого действия можно указать задержку его выполнения в секундах. Если задержка указана для первого действия в сценарии, то это действие выполнится только по истечении указанного времени с момента возникновения события-триггера. Каждое последующее действие будет выполняться через указанное время задержки после предыдущего. Все действия в сценариях выполняются последовательно, с учётом указанных задержек для каждого действия.

Для установки задержки выберите требуемое действие в списке, щёлкните в поле «Задержка» и нажмите кнопку «…» в столбце «Задержка».

> ***Внимание!*** *Для действия «Запустить файл» драйвера «Система» необходимо указывать файл, локально хранящийся на сервере системы. Файл будет запущен от имени пользователя Windows “СИСТЕМА”, поэтому вывод каких-либо окон в этом случае невозможен.*

Для каждого сценария можно указать, при наступлении каких событий и условий он будет выполняться. Для настройки этого механизма следует:

1. Выбрать сценарий, для которого требуется задать события, по которым он будет выполняться;
2. Добавить в список необходимые события, нажав кнопку «+» над списком событий-триггеров.

Есть возможность одновременно добавлять несколько событий-триггеров, выбрав в окне добавления несколько однотипных устройств слева и несколько событий справа. Например, на Рис. 37 выбрано 3 устройства и 7 событий, что приведёт к добавлению 21 события-триггера.

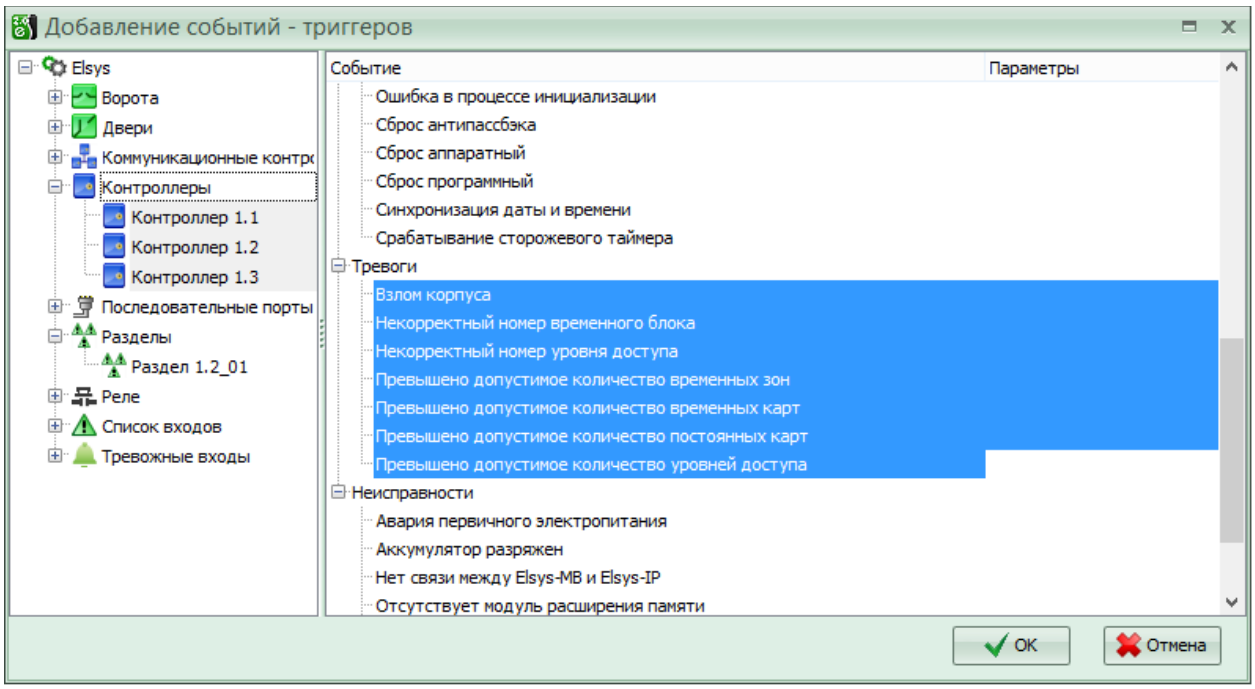

Рис. 37. Окно добавления событий-триггеров

Для событий-триггеров, текст которых содержит константы %po (позиция), %cn (номер карты) и %nm (фамилия персоны) можно добавить дополнительные параметры. Для добавления параметра необходимо выделить поле «Параметры» у события, в которое входит один из вышеперечисленных параметров (Рис. 38). В поле отобразится кнопка, открывающая окно настройки параметров события (Рис. 39).

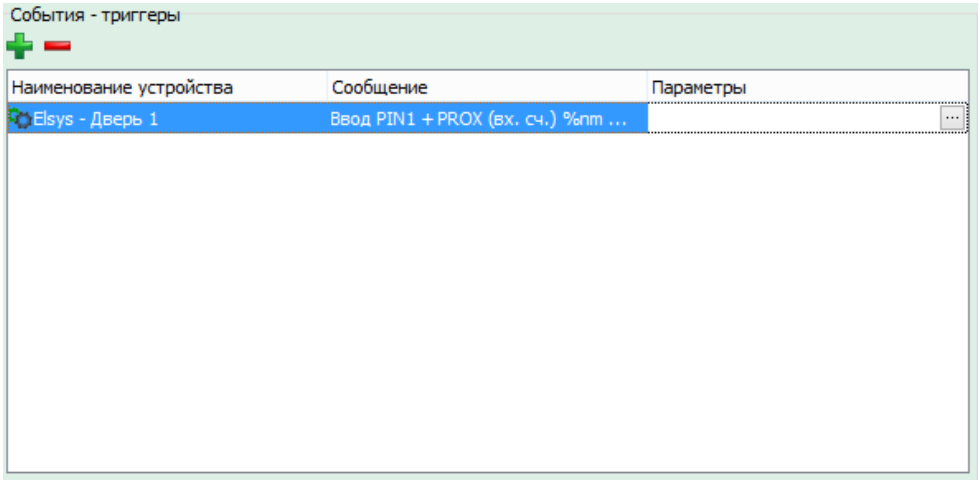

Рис. 38. Кнопка добавления параметров события-триггера

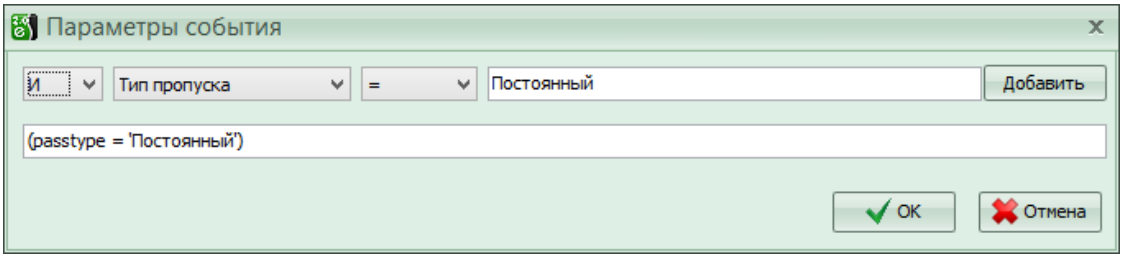

Рис. 39. Окно настройки параметров события

Дополнительно, для любых событий-триггеров можно указать параметры времени. Например, на Рис. 40 указано, что событие-триггер будет срабатывать только с 8:00 до 18:00. В другое время сценарий при возникновении выбранного события выполняться не будет.

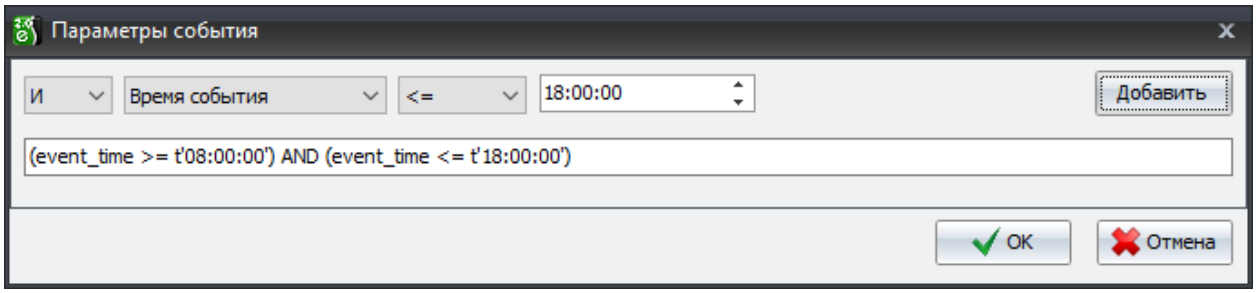

Рис. 40. Окно настройки параметров времени для событий-триггеров

Аналогично можно добавить параметры для события при его добавлении в окне «Добавление событий-триггеров».

Для каждого события-триггера можно указать, с какой вероятностью будет выполняться сценарий в случае возникновения этого конкретного события. На практике с помощью этой возможности можно организовать, например, выборочное алкотестирование при входе на территорию. Пример такой настройки приведён на Рис. 35. При этом есть возможность указать, оповещать ли оператора о пропуске выполнения сценария. Если эта опция установлена, при пропуске выполнения сценария будет сформировано системное событие «Запуск сценария пропущен».

Для настройки вероятности выполнения сценария, выделите требуемое событие-триггер в списке, щёлкните в поле «Вероятность» и нажмите кнопку «…» в этом поле.

Кроме настройки выполнения сценариев по событиям-триггерам, возможно задать одно или несколько расписаний выполнения сценариев. В системе доступны 4 вида расписаний:

- однократное – позволяет назначить выполнение расписания на конкретные дату и время;
- ежедневное – выполнение расписания каждый день в назначенное время;
- еженедельное – позволяет выбрать дни недели, в которые будет выполняться сценарий, а также настроить выполнение расписаний только по праздничным или коротким дням;
- ежемесячное – позволяет настроить выполнение сценария в конкретные месяцы, а также задать день выполнения либо указанием дня месяца, либо указанием номера недели и дня недели.

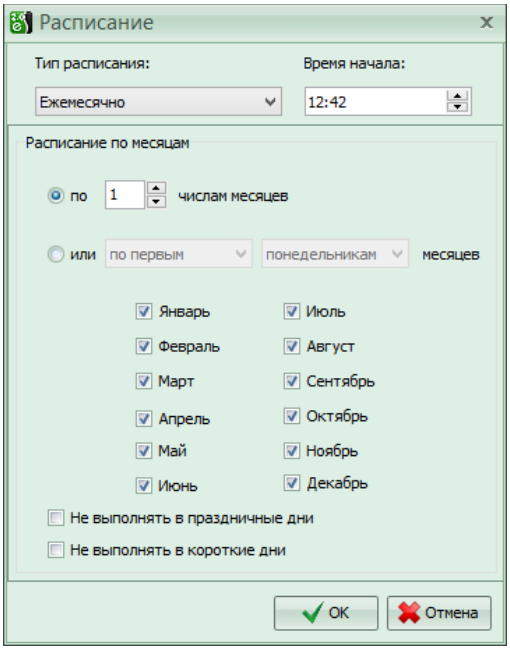

Рис. 41. Окно настройки параметров для ежемесячного расписания

Для еженедельного и ежемесячного расписания есть возможность отключить выполнение сценариев в праздничные и короткие дни, которые доступны для настройки в АРМ Бюро пропусков (см. Бастион-2 – АРМ Бюро пропусков. Руководство оператора, п. 6.2).

> ***Внимание!*** *Для корректной работы расписаний при смене часового пояса на сервере системы необходимо перезапустить службу BAgentSvc.*

Список сценариев, которые будут выполнены в ближайшие 24 часа можно просмотреть в форме «Расписание выполнения сценариев на следующие 24 часа». При необходимости, например при пуско-наладочных работах, можно остановить и запустить работу всех расписаний, используя кнопки на данной форме.

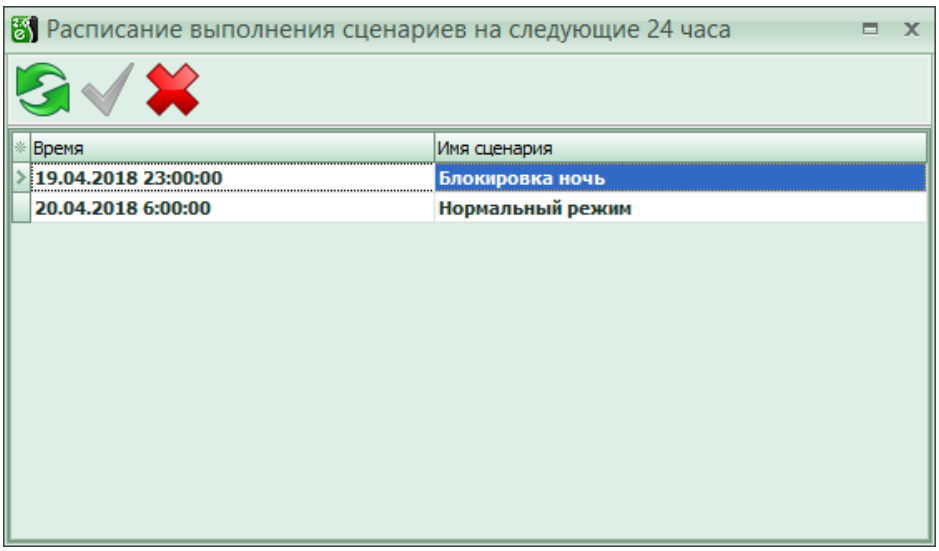

Рис. 42. Окно расписания выполнения сценариев на следующие 24 часа

Для сценариев, в которые добавлен вывод окон камер на экран также можно настроить отображение для различных профилей. С помощью кнопки «Изменить отображение камер…» на

панели действий можно открыть окно «Отображение камер» (Рис. 43) и изменить список профилей, для которых будут отображаться камеры при исполнении сценария.

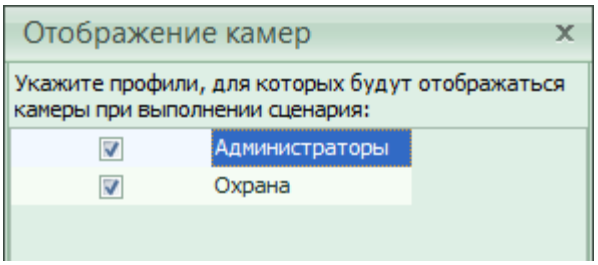

Рис. 43. Окно настройки отображения камер для профилей операторов

Для *удаления действия или сценария* выберите требуемый элемент и нажмите соответствующую кнопку «–» в панели инструментов, либо выберите нужный пункт из контекстного меню.

Сценарии можно объединять в ***группы сценариев***. Группы сценариев служат только для логической группировки сценариев.

Сценарии и группы сценариев являются устройствами системы, поэтому с ними можно работать так же, как с остальными устройствами – выносить пиктограмму на графический план, разграничивать доступ и пр.

При вынесении на графический план пиктограммы сценария, его контекстное меню позволяет выполнить сценарий. Для пиктограмм групп сценариев в контекстном меню отображается список входящих в неё сценариев, которые можно выполнить.

Разграничение доступа к выполнению сценариев в ручном режиме настраивается в окне «Доступ к устройствам» (см. п. 5.6).

5.12 Настройка областей контроля

Под *областью контроля* в АПК «Бастион-2» понимается некоторое пространство, ограниченное одной или несколькими точками прохода (дверями, турникетами, воротами и т. д.). Такой областью может являться одно конкретное помещение, группа помещений, здание целиком, территория завода и т. д. Области контроля могут быть вложенными. Например, область контроля «Все здание» может содержать несколько других областей – "Цех 1", "Бухгалтерия" и т. д. Тем не менее, следует учитывать, что вложенность носит чисто информативный характер и не используется программой.

Области контроля используются программным обеспечением в следующих случаях:

- Для обеспечения подсчета людей в области контроля.
- В качестве ограничивающей области в системе учета рабочего времени. При этом вход в область контроля считается приходом на работу, а выход из нее – уходом с работы.
- Для организации режима глобального контроля последовательности прохода (Global Antipassback).

Для настройки областей контроля выберите в ленте «Конфигурация» в закладке «Система» пункт Области контроля». При этом появится окно, представленное на Рис. 44.

По умолчанию в системе определены 2 области: «На территории» и «Вне территории». Эти области удалить нельзя. Область «На территории» всегда используется как «ограничитель территории предприятия», то есть по ней определяется вход и выход с объекта. Также, по умолчанию эта область используется для учета рабочего времени и подсчета людей.

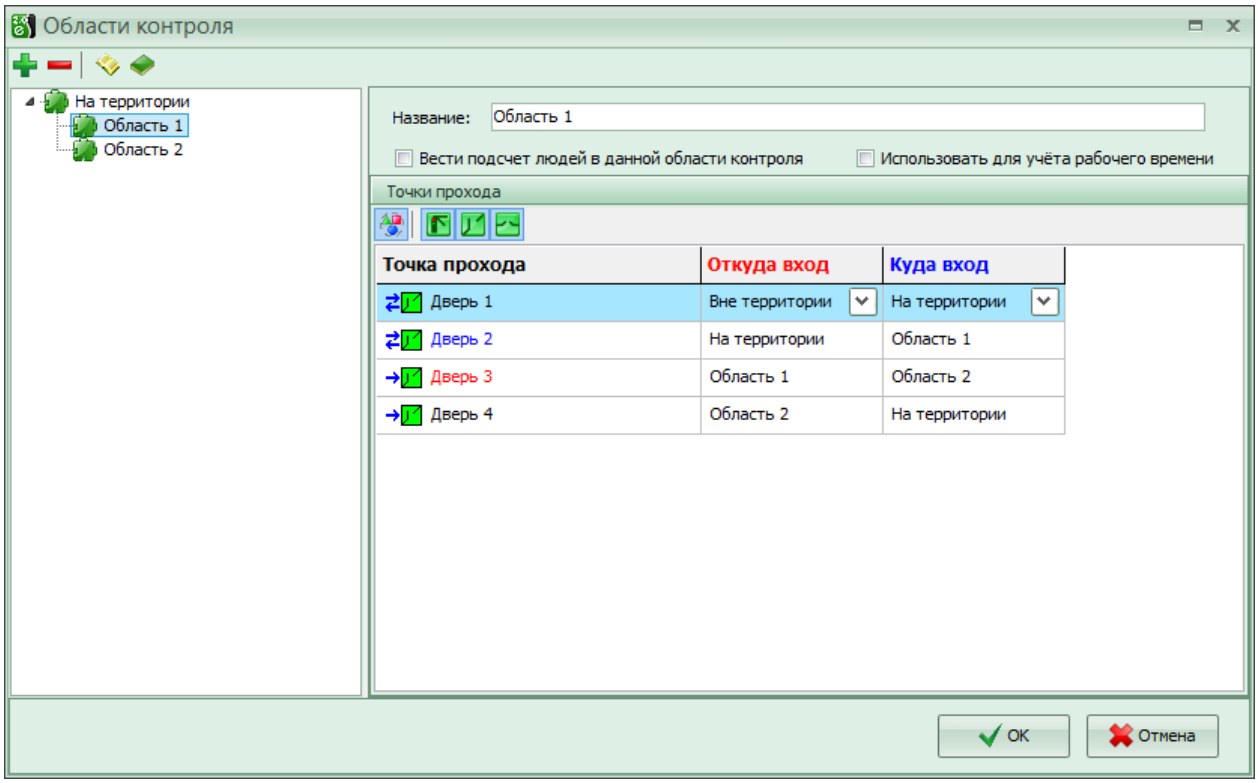

Рис. 44. Окно настройки областей контроля

Для *добавления области контроля* необходимо нажать кнопку «  » в панели инструментов или выбрать соответствующий пункт из контекстного меню в дереве областей контроля и ввести название области контроля.

После добавления областей контроля следует определить участие в них точек прохода. Для этого необходимо указать, откуда и куда ведет точка прохода. Например, на Рис. 44 «Дверь 1» ведет из области «Вне территории» в область «На территории».

> *Односторонние точки прохода также могут участвовать в областях контроля. Это имеет смысл, например, при использовании глобального антипассбэка – в этом случае, доступ по карточке не предоставляется в этой точке прохода, пока её владелец не зашел в область контроля, ограничивающую эту точку. При этом следует выбирать одну и ту же область в столбцах «Откуда вход» и «Куда вход». Например, на Рис. 44, односторонняя «Дверь 3» находится внутри области «На территории».*

Цветами шрифта отображается статус точки прохода в текущей области контроля (синий – входная точка, красный – выходная, черный – в текущей области не используется).

Также, можно отфильтровать список точек прохода с помощью кнопок в панели управления:

	Показывать точки прохода, используемые в областях контроля или в текущей области контроля (зависит от положения кнопки ).
	Показывать турникеты.
	Показывать ворота.
	Показывать двери.

Для настройки также доступны следующие опции:

Использовать для учёта рабочего времени. Если флаг установлен, то события по этой области контроля будут засчитываться как приход/уход с работы. В дальнейшем, в генераторе отчетов по рабочему времени можно будет выбрать область контроля, по которой формировать выбранный отчет.

Вести подсчет людей в данной области контроля. Если данный флаг установлен, программное обеспечение будет вести подсчет количества людей в области контроля на основе определенных для нее входных и выходных событий.

5.13Группы управления охраной

5.13.1 Определение, назначение и состав групп управления охраной

Группа управления охраной (ГУО) определяет права пользователей СКУД по управлению устройствами охранной сигнализации.

Группы управления охраной в АПК «Бастион-2» поддерживаются на системном уровне (на уровне ядра) и могут включать элементы разных драйверов. Группы управления охраной не являются устройствами АПК «Бастион-2». Группы управления охраной не связаны с уровнями доступа СКУД, это отдельная сущность.

Поддержка групп управления охраной на системном уровне позволяет единообразно управлять правами пользователей системы на постановку / снятие с охраны для всех драйверов АПК «Бастион-2».

ГУО делятся на программные и аппаратные.

Аппаратные ГУО всегда относятся к одному экземпляру драйвера и напрямую записываются в соответствующие контроллеры. Логика управления с использованием аппаратных ГУО может работать без участия АПК «Бастион-2».

Программные ГУО могут содержать элементы, относящиеся к разным экземплярам и классам драйверов. Программные ГУО объединяют аппаратные ГУО.

Аппаратные ГУО могут включать устройства типа «Раздел» и «Группа разделов», привязанные к одному и тому же экземпляру драйвера.

Программные ГУО группируют только аппаратные ГУО. Каждая программная ГУО может содержать 1 или несколько аппаратных ГУО, но не более чем по одной от каждого экземпляра драйвера.

При включении элементов в аппаратные ГУО, для каждого элемента указывается *признак возможности снятия с охраны*. При этом постановка на охрану доступна всегда.

5.13.2 Настройка групп управления охраной

Каждая ГУО, независимо от типа, обладает следующими атрибутами (Рис. 45):

Владелец. Экземпляр драйвера для аппаратных ГУО или «Система» для программных ГУО.

Название.

Адрес (номер). Для аппаратных ГУО содержит адрес или номер, под которым ГУО записывается в конфигурацию контроллеров.

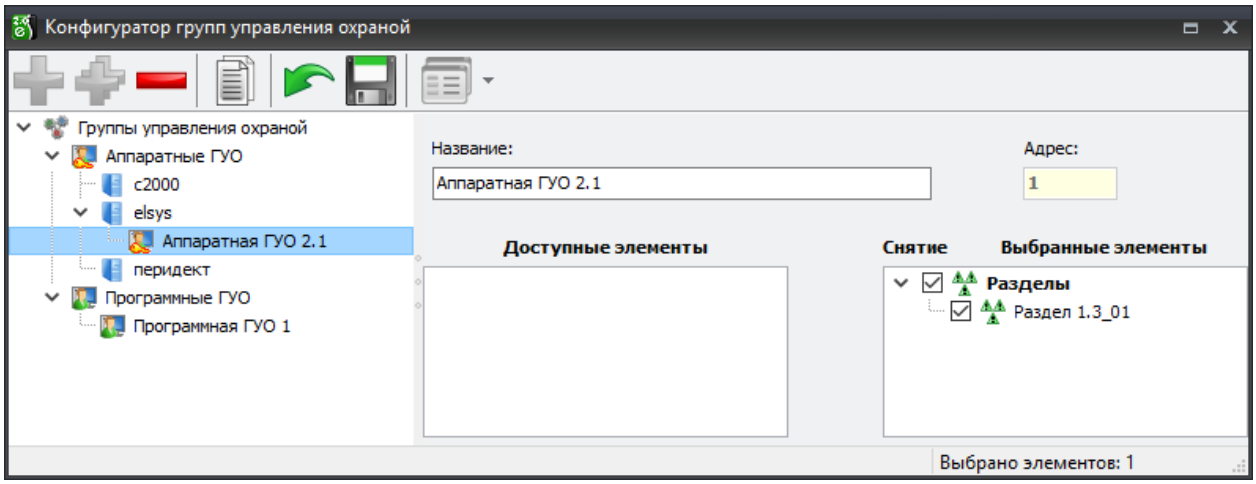

Рис. 45. Свойства аппаратной ГУО

Аппаратные ГУО могут импортироваться из внешних источников (файлы конфигурации, непосредственно из сети контроллеров и т. п.). При этом для таких ГУО может быть установлен атрибут «Только для чтения».

Импорт производится в конфигураторе соответствующего драйвера. При импорте аппаратной ГУО её состав может быть неизвестен в АПК «Бастион 2».

Настройка групп управления охраной производится в отдельной форме, вызываемой из АРМ Оператора (лента «Конфигурация – Операторы и полномочия», см. Рис. 45). Доступ к форме разграничивается отдельным полномочием «Редактирование ГУО».

Программные и аппаратные ГУО сведены в дерево в левой части формы и сгруппированы в отдельные узлы.

В правой части представлена настройка аппаратной ГУО. В «Доступных элементах» сведены имеющиеся разделы и группы разделов выбранного драйвера.

При настройке программной ГУО в левом списке отображается дерево аппаратных ГУО (Рис. 46):

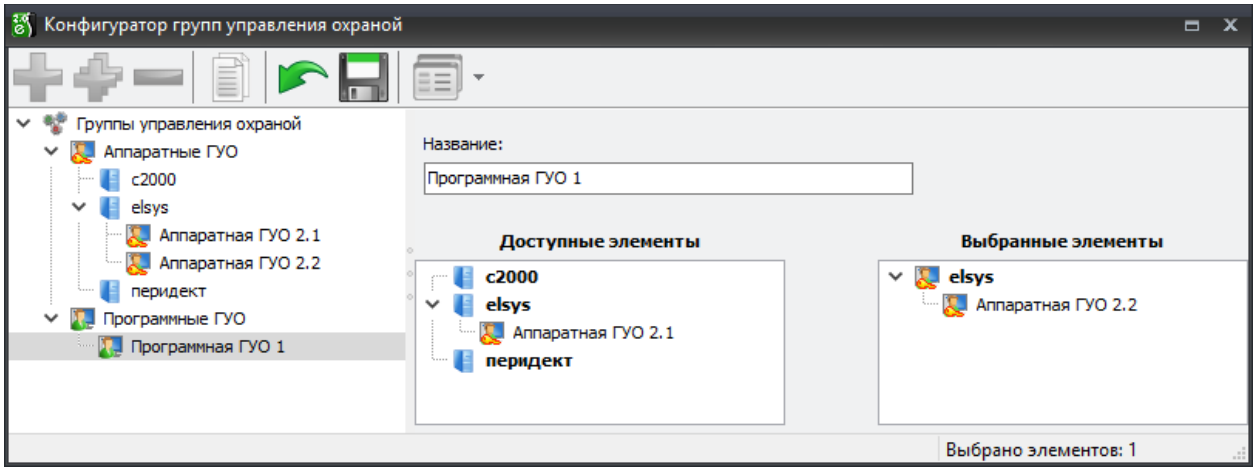

Рис. 46. Настройка программной ГУО

5.13.3 Привязка пропусков к группам управления охраной

К каждому пропуску может быть привязана максимум 1 группа управления охраной. Если обладателю пропуска необходимо управлять элементами из разных экземпляров драйверов, предварительно необходимо создать программную ГУО, объединяющую эти элементы.

При привязке ГУО к пропуску, необходимо указывать режим идентификации пропуска. Возможные режимы:

1. По карте доступа;
2. По PIN-коду;
3. По карте доступа или PIN-коду.

Привязка ГУО к пропуску производится в окне свойств пропуска на отдельной странице «Управление охраной». Доступ к этой странице разграничивается отдельным полномочием «Назначение группы управления охраной».

5.14Автотранспорт

Окно «Автотранспорт», вызываемое из блока «Пропуска» вкладки «Инструменты», предоставляет доступ к служебному справочнику, который необходим транспортным пропускам и в котором содержатся данные автомобилей. Описание работы с данной формой содержится в руководстве «Бастион-2 – АРМ Бюро пропусков. Руководство оператора».

5.15 Настройка глобального контроля последовательности прохода

СКУД «Elsys» обеспечивает возможность работы глобального контроля последовательности прохода, причём его функционирование возможно и при отсутствии компьютера на линии связи.

При настройке функции «Глобальный контроль последовательности прохода» следует учитывать следующие ограничения:

– каждый контроллер доступа может обслуживать не более двух областей контроля;

– глобальный контроль последовательности прохода работает либо в пределах одной линии связи RS-485, либо в пределах системы, построенной с использованием КСК «Elsys-MB-Net», поскольку отсутствует обмен информацией контроллеров доступа, подключенным к разным COM-портам, между собой и контроллерами, подключенными к КСК «Elsys-MB-Net»;

– контроллеры «Elsys-MB-SM» поддерживают функцию «Глобальный контроль последовательности прохода», если в памяти контроллера содержится не более 150 карт доступа.

Для настройки глобального контроля последовательности прохода необходимо, в первую очередь, сконфигурировать области контроля (см. п. 5.12).

Затем необходимо включить функцию глобального контроля последовательности прохода в настройках драйвера ELSYS или сетевого контроллера, нажав на кнопку **«Включить antipassback»** (Рис. 47).

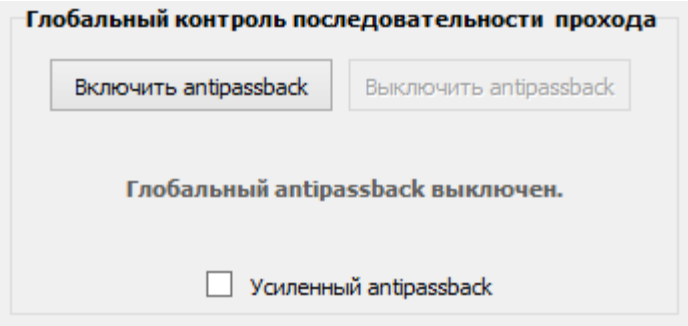

Рис. 47. Функция глобального контроля последовательности прохода выключена

Если необходимо выключить функцию глобального контроля последовательности прохода, то необходимо нажать кнопку **«Выключить»** (Рис. 48) в настройках драйвера или сетевого контроллера.

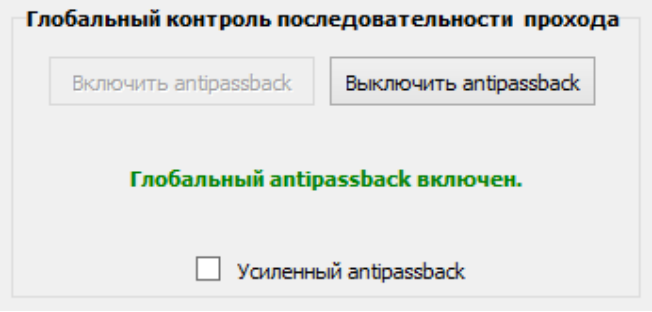

Рис. 48. Функция глобального контроля последовательности прохода включена

При необходимости следует включить настройки **«Сброс в полночь»** контроллеров «Elsys-MB» и **«Не проверять исправность областей контроля»** (см. «Бастион-2 – Elsys. Руководство администратора»). Эти настройки вступают в силу после инициализации оборудования.

В свойствах пропуска (см. инструкцию «Бюро пропусков») имеется опция **«Не отслеживать последовательность прохода»** (по умолчанию выключена). Её включение позволяет отключить функцию **«Глобальный контроль последовательности прохода»** для отдельных лиц.

Инициализация контроллеров происходит автоматически при закрытии окна конфигуратора драйвера или окна настройки областей контроля.

Если необходимо исключить контроллер из системы глобального контроля последовательности прохода, то необходимо в настройках контроля последовательности прохода для контроллера доступа выставить значение **«Не использовать»**.

5.16 Синхронизация времени

Комплекс «Бастион-2» предоставляет возможность синхронизации времени серверов оборудования (при поддержке функции установки времени) с локальным временем компьютера. Синхронизация времени позволяет более точно отслеживать последовательность событий, происходящих в системе.

Пользователю предоставляется возможность выбора следующих параметров синхронизации (лента «Конфигурация» вкладка «Система» пункт «Общие настройки» страница «Синхронизация времени»):

Синхронизировать время при запуске сервера оборудования. При установке этого флага время будет синхронизироваться при каждом запуске сервера оборудования.

Синхронизировать время периодически. Доступные варианты: раз в час и раз в день.

5.17 Сторожевой таймер

Сторожевой таймер предназначен для автоматического перезапуска системы при ее зависании. Таймер периодически проверяет активность основного потока главного программного модуля (Bastion.exe), и в случае, если он не отвечает, производит перезапуск программы. Не отслеживаются сбои оборудования и операционной системы. Таймер реализован в виде службы Windows.

Для активизации таймера необходимо выбрать лента «Конфигурация» вкладка «Система» пункт «Локальные настройки» и перейти на страницу «Сторожевой таймер». Таймер имеет два параметра:

Время отсутствия отклика. Если основной поток программы не отвечает в течение этого времени, система будет перезапущена.

Задержка перед перезапуском. Система будет запущена повторно через заданное время после ее аварийного завершения.

5.18 Организация возврата временных и разовых пропусков

В системе предусмотрено 2 варианта организации возврата временных и разовых электронных пропусков.

Первый вариант предполагает наличие специальной точки прохода (турникета, шлюза) и рабочего места оператора, контролирующего выход по временным и разовым пропускам. При

этом система должна быть настроена таким образом, чтобы решение об открывании точки прохода на выход принимал оператор. При предъявлении карты на выход у оператора появляется окно фотоидентификации с двумя дополнительными кнопками «Сдал» и «Не сдал». Если выходящий сдает пропуск оператору, то оператор должен нажать кнопку «Сдал». При этом в программе пропуск переводится в архив, в протокол записывается соответствующее событие, а карта доступа может быть выдана повторно. При нажатии кнопки «Не сдал» окно фотоидентификации закрывается, и система не производит никаких дополнительных действий. Описание настройки данного режима содержится в пункте «Настройки параметров фотоидентификации».

Второй вариант предполагает использование специального картоприёмника со встроенным считывателем. В этом случае для выхода за территорию предприятия посетитель должен поместить карту доступа в картоприёмник, после чего точка прохода открывается на выход.

Для реализации такого режима необходимо создать сценарий, в котором будет действие «Вернуть предъявленную карту» и задать для него событие-триггер «Предоставление доступа на выход» у соответствующей точки прохода. После выполнения этого сценария карту доступа можно будет выдавать повторно.

5.19 Настройки параметров фотоидентификации

Фотоидентификация может использоваться, если в состав АПК «Бастион-2» входит драйвер СКУД (например, СКУД «Elsys»). Режим фотоидентификации сотрудников предназначен для проведения сравнения лица, предъявившего карту, с фотографией подлинного владельца карты доступа и принятия решения о предоставлении или не предоставлении доступа.

Для настройки параметров фотоидентификации следует открыть форму «Локальные настройки» («Конфигурация» – «Локальные настройки») и перейти на пункт «Фотоидентификация» (см. Рис. 49).

> ***Внимание!*** *Фотографии сотрудников должны быть предварительно занесены в базу данных программы.*

Вкладка «Отображение» страницы настройки параметров содержит следующие опции:

Разрешить фотоидентификацию – если опция включена, на текущем рабочем месте будут отображаться окна фотоидентификации.

Блок «Режим вывода окон по событию» позволяет настроить, каким образом будут выводиться окна фотоидентификации. Поддерживаются следующие опции:

Автоупорядочивание. В этом режиме окна фотоидентификации будут располагаться друг под другом с перекрытием на основном мониторе.

Режим проходной (окна занимают все доступное пространство на указанном мониторе). Этот режим можно использовать на рабочем месте поста охраны на проходной. При этом окна с фотографиями владельцев карт будут занимать все доступное пространство на указанном мониторе. Окна фотоидентификации не будут перекрывать друг друга. Основной монитор имеет номер 0.

Привязка к точкам прохода. В этом режиме положение окна фотоидентификации будет зависеть от точки прохода, от которой пришло событие. Настроить расположение окон можно на вкладке «Точки прохода».

Система позволяет регулировать отображение окон фотоидентификации по следующим признакам:

Номер монитора для вывода окон фотоидентификации – при наличии более одного монитора в конфигурации настраиваемой рабочей станции позволяет назначить, на каком именно мониторе следует производить вывод окон фотоидентификации.

Использовать для событий с приоритетом не менее заданного. Опция позволяет установить фильтр на вывод окон фотоидентификации по приоритету события.

Использовать для карточек с приоритетом не более заданного. Опция позволяет установить фильтр на вывод окон фотоидентификации по приоритету карты доступа.

Закрывать окно фотоидентификации автоматически через заданное время. Позволяет закрывать окна с устаревшей информацией автоматически.

Максимальное число одновременно отображаемых окон. Позволяет автоматически закрывать окна фотоидентификации при предъявлении новых карт доступа при достижении заданного числового предела.

Показывать при открытых модальных окнах. Если выключено (по умолчанию), то при работе в любых окнах настройки системы окна фотоидентификации отображаться не будут.

Показывать при свёрнутом главном окне. Если выключено (по умолчанию), то при сворачивании главного окна, окна фотоидентификации отображаться не будут.

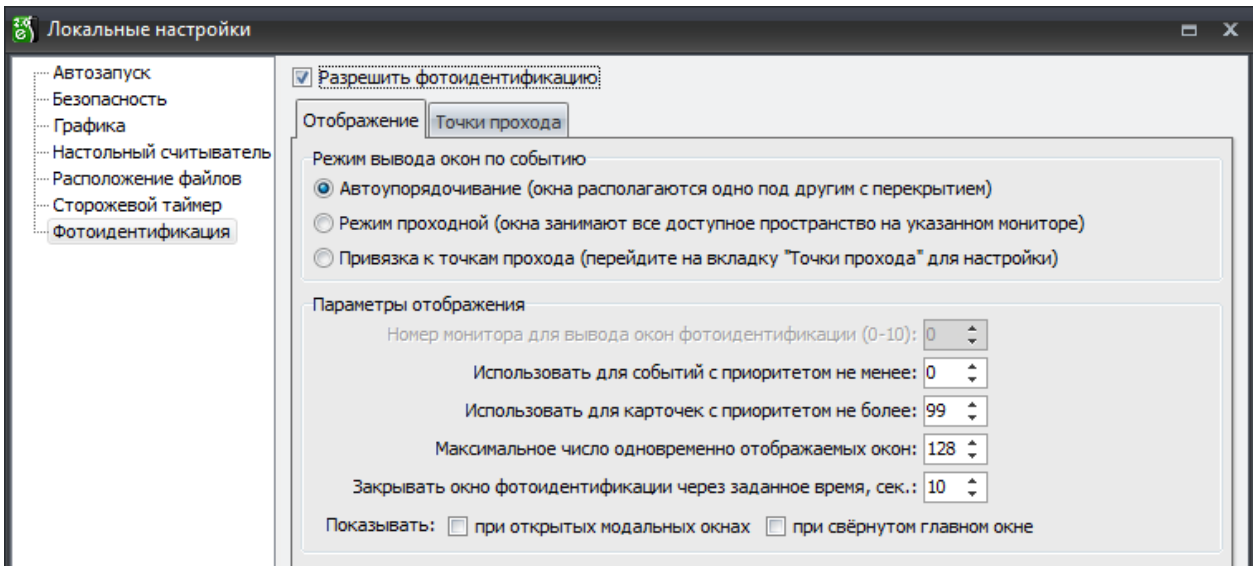

Рис. 49. Окно настройки параметров фотоидентификации

Вкладка «Точки прохода» позволяет настроить параметры вывода окон фотоидентификации.

Список слева содержит все точки прохода, которые добавлены в драйвере СКУД. Для каждой из этих точек прохода на вход и на выход можно задать следующие параметры:

Выводить окно фотоидентификации. Включает и отключает вывод окон фотоидентификации при проходе через точку прохода в выбранном направлении.

Отображать информацию о материальных пропусках. Позволяет настроить показ и возврат материальных пропусков через точку прохода.

Отображать информацию о транспортных пропусках. Позволяет настроить показ транспортных пропусков.

Блок «Положение формы» служит для настройки расположения окна, привязанного к точке прохода. Соответственно, этот блок доступен для редактирования, если на вкладке «Отображение» выбран режим вывода «Привязка к точкам прохода». При этом, помимо блока настройки расположения в режиме привязки к точкам, доступна кнопка «Установить расположение форм фотоидентификации», позволяющая расставить окна фотоидентификации с помощью указателя мыши.

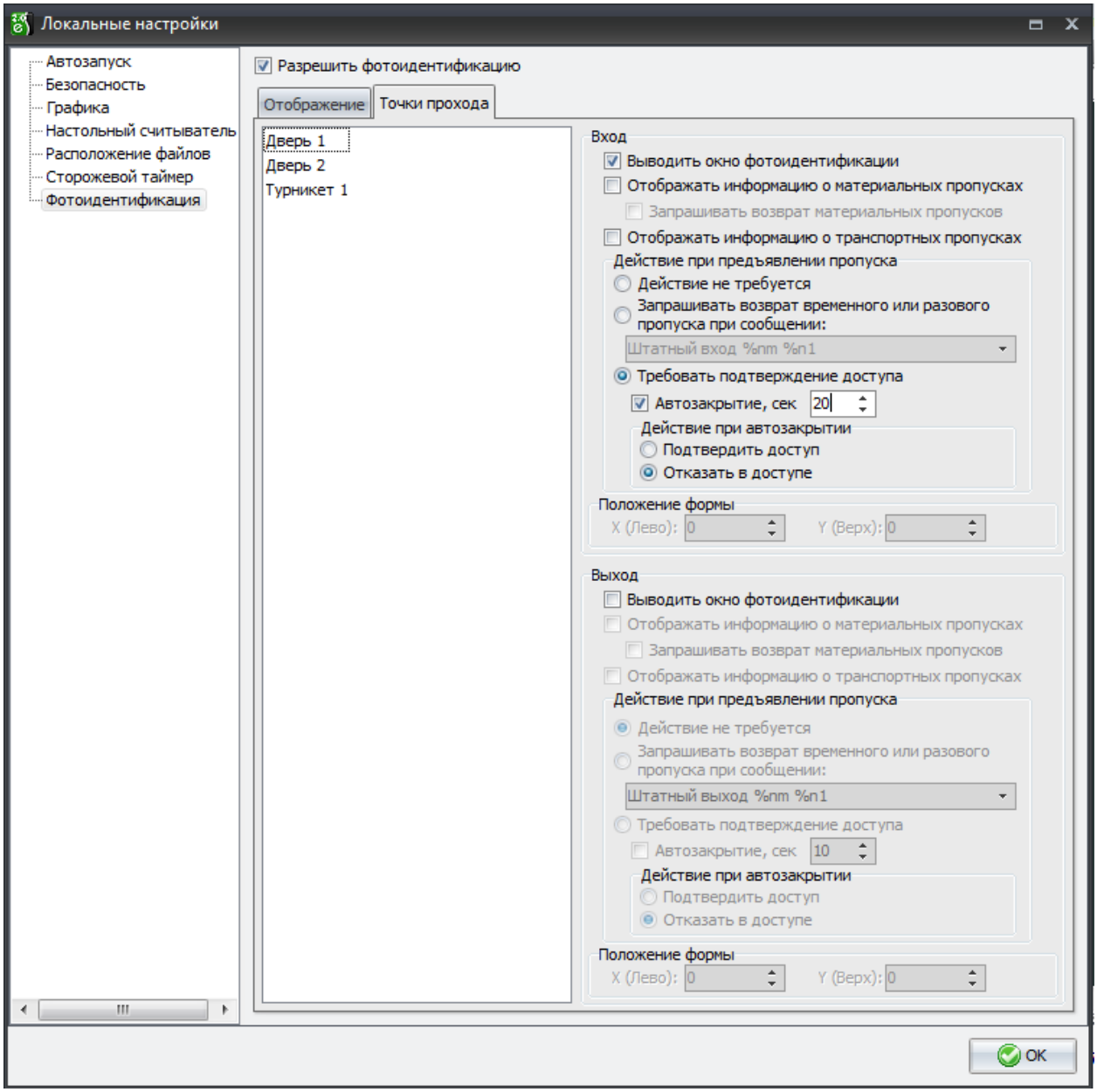

Рис. 50. Настройки точек прохода фотоидентификации

В блоке «Действие при предъявлении пропуска» можно выбрать режим вывода окон фотоидентификации настраиваемой точки прохода.

Если выбрана опция «Действие не требуется», то окно фотоидентификации по истечении заданного времени автозакрытия исчезнет с экрана монитора, не требуя при этом никакого активного действия от оператора.

При выборе опции «Запрашивать возврат пропуска при сообщении» становится активным выбор сообщения, при котором будет выведен запрос на возврат временного, либо разового пропуска, причем окно фотоидентификации, в случае прихода выбранного события, не закроется автоматически.

Опция «Требовать подтверждение доступа» служит для указания того, что на данном рабочем месте будет происходить подтверждение доступа оператором. При этом можно выбрать опцию «Автозакрытие» и указать время, по истечении которого произойдет автоматическое закрытие окна фотоидентификации и выполнено указанное действие, а именно произойдет подтверждение доступа, либо в доступе будет отказано. Время, оставшееся до закрытия окна будет выводиться в его заголовке. Подробнее о настройке подтверждения доступа указано в руководстве драйвера СКУД.

5.20 Настройка расположения файлов

Для выполнения настройки расположения файлов комплекса «Бастион-2» откройте форму «Локальные настройки» («Конфигурация» -- «Локальные настройки») и перейдите на закладку «Расположение файлов» (Рис. 51).

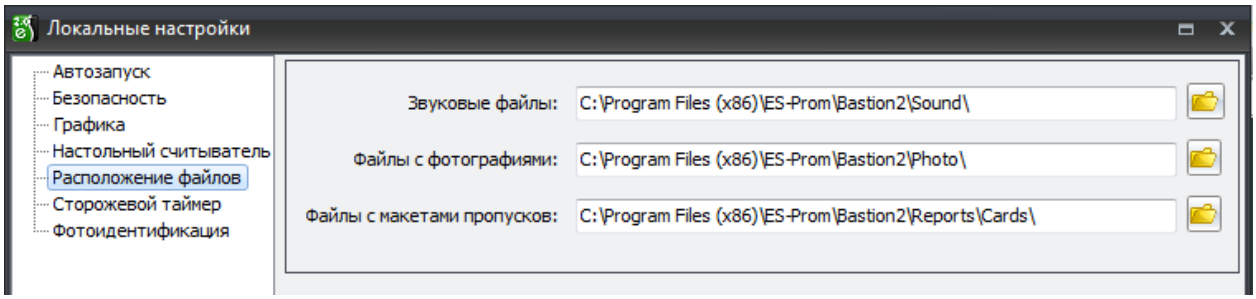

Рис. 51. Настройки расположения файлов

Система позволяет установить пути к следующим группам файлов (в скобках указан путь по умолчанию):

- Звуковые файлы (<Bastion>\Sound)
- Файлы фотографий – используются только при начальной настройке системы (для ввода фотографий в базу данных) при наличии СКУД (<Bastion>\Photo).
- Файлы с макетами пропусков (<Bastion>\ Reports\Cards\)

Для вызова окна выбора папки нажмите кнопку «Обзор» справа от соответствующей строки редактирования.

Обычно без особой необходимости не следует изменять расположение файлов, используемое по умолчанию.

6 Расширенные возможности запуска системы

6.1 Параметры командной строки

Исполняемый файл "bastion.exe", а также модуль генератора отчетов (BRptGen.exe) могут быть запущены с одним или несколькими из следующих параметров, предназначенных для автоматизации процесса запуска системы:

user=<UserName> – имя пользователя для входа в программу

pwd=<Password> – пароль пользователя

quickexit. Если программа запущена с этим параметром, то при выходе из программы не будет запрашиваться подтверждение.

Общий синтаксис командной строки:

```
bastion.exe [user=<UserName> pwd=<Password>] [quickexit]
```

6.2 Запуск системы с ожиданием загрузки драйвера HASP

В состав АПК «Бастион-2» входит специальная утилита (DelayedLaunch.exe), позволяющая ожидать загрузки драйвера ключа HASP перед запуском требуемой программы.

Например, эта утилита используется при установке Bastion.exe вместо оболочки Windows (см. п. 6.4). Также, рекомендуется использовать утилиту DelayedLaunch.exe в том случае, если требуется прописать Bastion.exe (или любую другую программу, требующую наличия ключа HASP) в папку автозагрузки ОС.

Синтаксис использования командной строки DelayedLaunch.exe:

```
DelayedLaunch.exe app=<исполняемый модуль> [user=<UserName>
pwd=<Password>] [quickexit]
```

Назначение параметров см. выше, в п. 6.1.

6.3 Запуск системы без полномочий администратора

6.3.1 Параметры безопасности NTFS

Если система установлена в раздел NTFS, то пользователи Windows, работающие с АПК «Бастион-2», должны иметь полный доступ к основному каталогу **Bastion** и всем вложенным каталогам.

Далее приводится инструкция, как дать полный доступ к папке АПК «Бастион-2» и всем её подпапкам всем пользователям компьютера. Настройки, приведенные ниже, гарантировано

позволяют работать с АПК «Бастион-2» без прав администратора. Если, дополнительно, требуется ограничить права пользователей на операции с отдельными файлами, следует схожим образом настроить параметры безопасности для каждого этих файлов, убрав лишние разрешения.

Для предоставления полных прав на все объекты папки Bastion всем пользователям компьютера:

1. Выберите в проводнике главный каталог АПК «Бастион-2» (например, c:\Program Files\ES-Prom\Bastion2) и из контекстного меню выберите «Свойства». В открывшемся окне перейдите на страницу «Безопасность» (см. Рис. 52).

2. Выберите группу "Пользователи (<ИМЯ_КОМПЬЮТЕРА>\Пользователи)" или “Users (<ИМЯ_КОМПЬЮТЕРА>\Users)”, (см. Рис. 52).

3. Установите флаг «Полный доступ» в колонке «Разрешить». Например, на Рис. 52 установлен полный доступ для всех пользователей компьютера ANDREYK-VIRTXP.

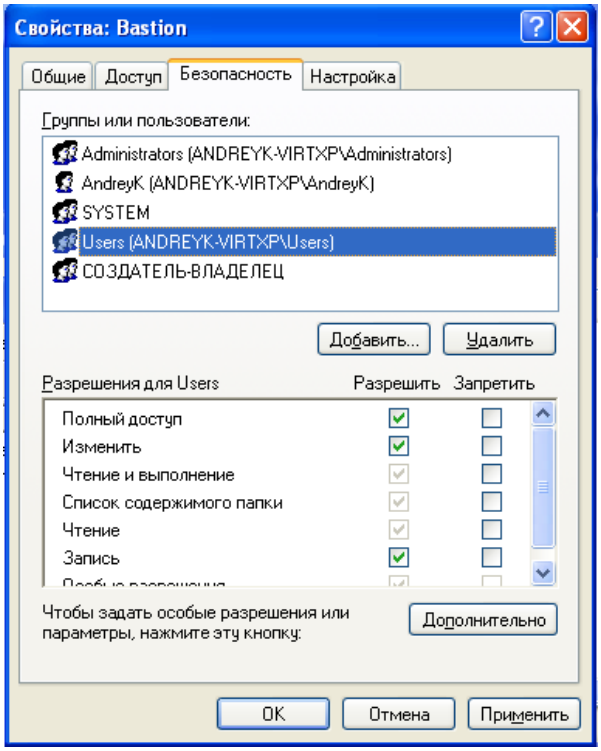

Рис. 52. Предоставление доступа к папке Bastion

4. Нажмите кнопку «Дополнительно». В открывшемся окне (см. Рис. 54) снимите флаг «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне». Появится запрос (Рис. 53), нажмите кнопку «Удалить».

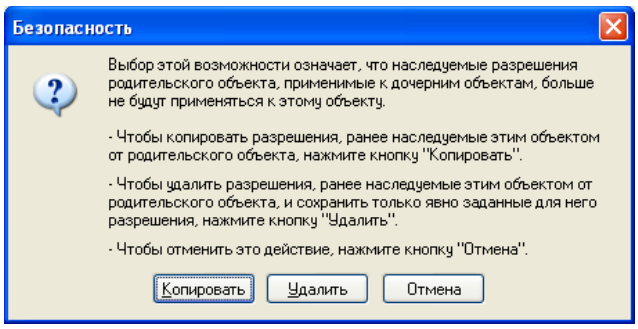

Рис. 53. Запрос подтверждения отмены наследования разрешений

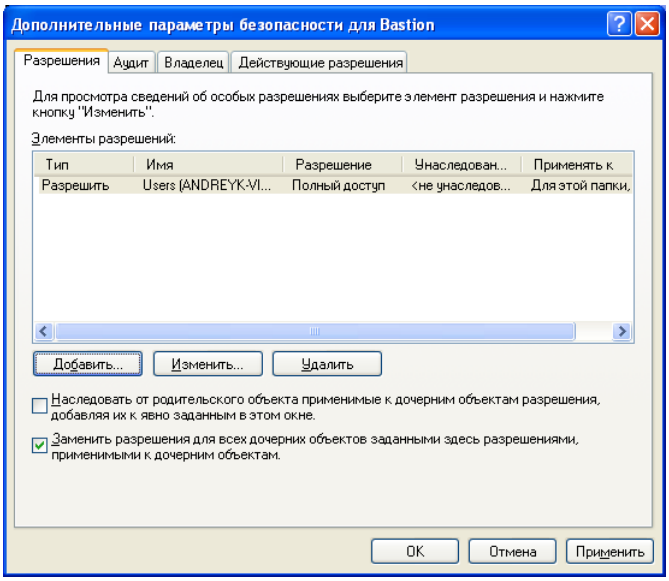

Рис. 54. Дополнительные параметры безопасности папки Bastion

5. В окне дополнительных параметров (Рис. 54) нажмите кнопку «Добавить». Введите имя добавляемой группы (“Пользователи” или “Users”) и нажмите ОК.

6. Появится окно установки прав для группы Users (Рис. 55). Установите флаг «Полный доступ» в колонке «Разрешить», как показано на Рис. 55 и нажмите ОК.

7. В окне на Рис. 54 установите флаг «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Окно должно принять вид, представленный на Рис. 54. Нажмите кнопку ОК.

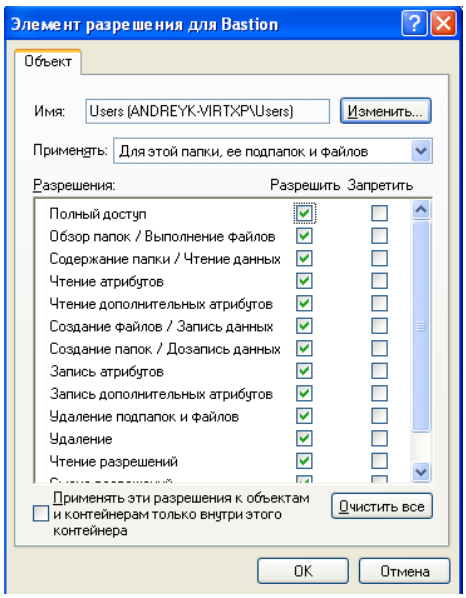

Рис. 55. Установка прав для группы Users

6.4 Использование режима расширенной безопасности

Основное назначение режима расширенной безопасности – ограничить полномочия оператора АПК «Бастион-2» на доступ к функциям операционной системы на выбранном рабочем месте.

> ***Внимание!*** *Настройки режима расширенной безопасности действуют только на компьютер, на котором производится настройка, при этом параметры, не относящиеся к запуску АПК «Бастион-2» и автоматическому входу в систему, действуют только на текущего пользователя Windows.*
>
> ***Внимание!*** *Для правильной работы настроек расширенной безопасности пользователь Windows должен обладать правами администратора.*

Для включения режима расширенной безопасности необходимо в общих настройках (Конфигурация→Общие настройки…) на странице «Безопасность» запустить программу редактирования расширенной безопасности и выбрать опцию «*Включить режим расширенного управления безопасностью*». Если опция выключена, то все параметры безопасности выключены, если включена – то доступ к функциям Windows определяется текущими настройками расширенного управления безопасности.

Здесь же можно задать ряд общих параметров режима расширенной безопасности на данном компьютере:

Загружать вместо стандартной оболочки ОС – эта опция позволяет автоматически загружать "Бастион" вместо оболочки Windows (вместо проводника) и блокировать доступ к элементам рабочего стола и меню программ.

Входить при этом под оператором – позволяет указать оператора АПК «Бастион-2», под чьим именем будет произведен автоматический вход в АПК «Бастион-2» при его загрузке. Если оператора не указать – будет выведено окно с запросом имени и пароля.

Использовать автологон – предназначен для автоматического ввода имени пользователя, домена и пароля при запросе ОС (т. е. при загрузке ОС не надо нажимать Ctrl+Alt+Del и вводить имя и пароль).

> ***Внимание!*** *Для работы опции «Использовать автологон» в случае работы компьютера в домене, поле «Домен» должно содержать имя домена, иначе – имя компьютера.*

Диспетчер задач – позволяет заблокировать вызов диспетчера задач (с помощью которого возможен запуск или завершение любой программы);

Блокировка компьютера – позволяет заблокировать кнопку «Блокировка компьютера» (при нажатии на Ctrl+Alt+Del);

Смена пароля пользователя ОС – позволяет заблокировать кнопку «Смена пароля» (при нажатии на Ctrl+Alt+Del);

Выход из системы – позволяет заблокировать кнопку «Выход из системы»;

Завершение работы – позволяет заблокировать кнопку «Завершение работы».

6.5 Авторизация через LDAP

6.5.1 Общие настройки

АПК «Бастион-2» позволяет использовать службу Active Directory или любой другой сервер LDAP (например, OpenLDAP) для идентификации пользователей. Настройка этой функции производится на форме «Общие настройки» (см. Рис. 56).

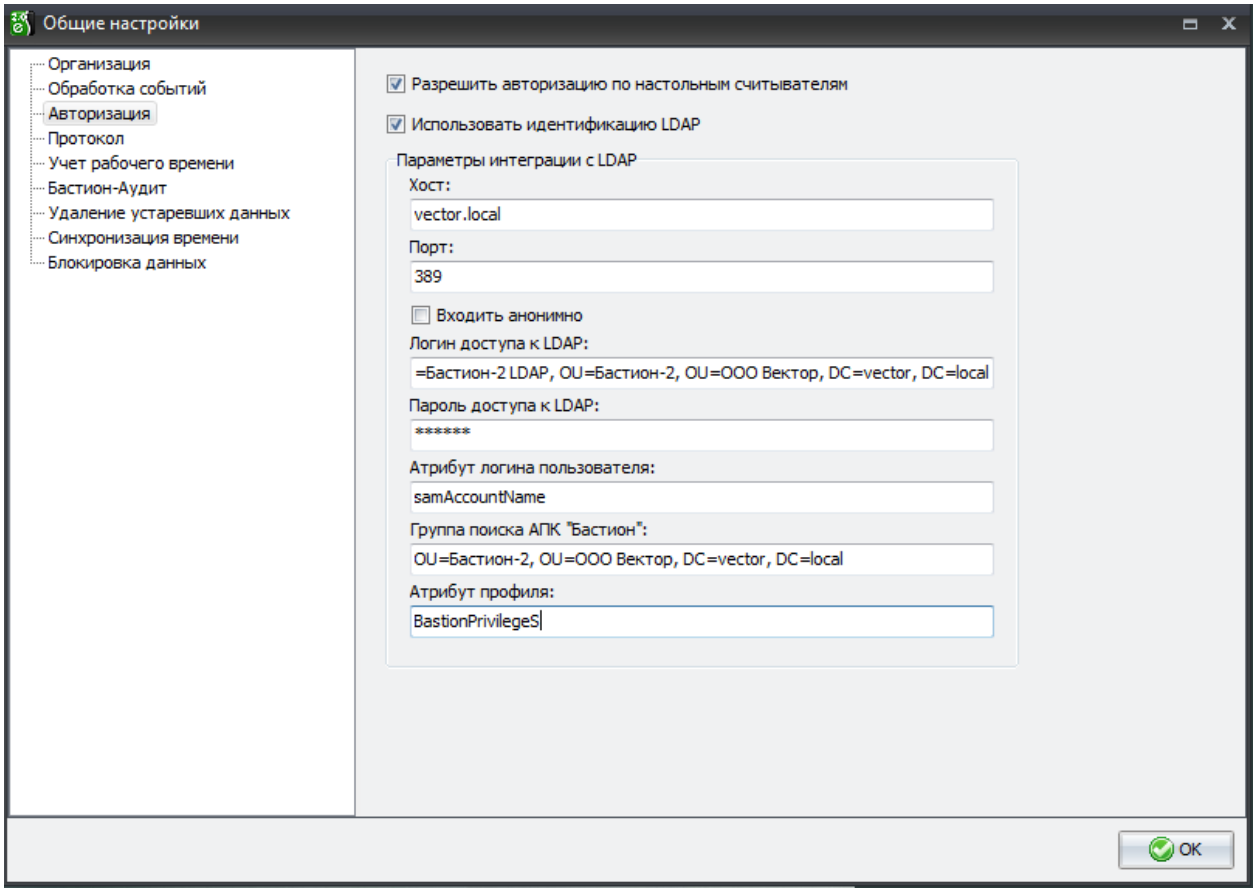

Рис. 56 Настройка расширенных возможностей авторизации

Опция «Использовать идентификацию LDAP» позволяет либо использовать (флаг установлен), либо не использовать (флаг не установлен) эту возможность. По умолчанию, флаг не установлен.

При установленном флаге активируются для настройки следующие опции:

Поле «Хост» должно содержать адрес сервера авторизации LDAP.

Поле «Порт» должно содержать порт, на который настроена служба сервера LDAP (обычно это 389 для незащищенного соединения и 636 – для сеансов, инкапсулированных в SSL).

Поле «Логин доступа к LDAP» должно содержать уникальное имя записи в каталоге LDAP, под которой будет производиться поиск.

Поле «Пароль доступа к LDAP» должно содержать пароль от логина доступа.

Флаг «Входить анонимно» может быть установлен, если на сервере LDAP настроена анонимная привязка. В таком случае поля «Логин доступа к LDAP» и «Пароль доступа к LDAP» не используются и будут недоступны для редактирования.

Поле «Группа поиска пользователей АПК «Бастион-2» должно содержать уникальное имя записи каталога LDAP, в которую входят пользователи АПК «Бастион-2».

Поле «Атрибут профиля» должно содержать название атрибута, где в свойствах пользователя в AD должно храниться название профиля оператора АПК «Бастион-2. Профиль в этом поле в свойствах

пользователя LDAP должен соответствовать профилю, существующему в АПК «Бастион-2» (см. п. 5.5 по настройке профилей). Выбранный атрибут должен быть текстовым.

6.5.2 Алгоритм работы

Если установлен флаг опции «Использовать идентификацию LDAP», то в момент ввода логина и пароля АПК «Бастион-2» проверяет, существует ли пользователь с именем, равным имени пользователя LDAP, в АПК «Бастион-2». Далее происходит анализ:

1) Если пользователь в LDAP имеет верную пару логин-пароль, а также заполненные атрибуты, позволяющие ему использовать АПК «Бастион-2», но в АПК «Бастион-2» данные о нём отсутствуют – этот пользователь добавляется в АПК «Бастион-2». Окно ввода пароля не появляется, блокировка АПК «Бастион-2» – отключается.

2) Если пользователь в LDAP имеет верную пару логин-пароль, а также заполненные атрибуты, не позволяющие ему пользоваться АПК «Бастион-2», а в АПК «Бастион-2» данные о нём отсутствуют – этот пользователь добавляется в АПК «Бастион-2», появляется окно ввода логина и пароля, опция блокировки АПК «Бастион» – включена.

3) Если пользователь в LDAP имеет неверную пару логин-пароль, а в АПК «Бастион-2» данные о нём присутствуют – появляется окно ввода логина и пароля, опция блокировки АПК «Бастион-2» – включена.

4) Если пользователь в LDAP имеет неверную пару логин-пароль, а в АПК «Бастион-2» данные о нём отсутствуют – появляется окно ввода логина и пароля, опция блокировки АПК «Бастион-2» – включена.

6.5.3 Настройка Active Directory для работы с АПК «Бастион-2»

6.5.3.1 Добавление атрибутов в схему Active Directory

На контроллере домена следует запустить **regsvr32 schmmgmt.dll** с правами локального администратора. Эта оснастка по умолчанию не зарегистрирована. После этого открыть из консоли **mmc** оснастку **Схема Active Directory** и перейти в раздел **Attributes (Атрибуты)**. Для добавления нового атрибута также потребуются права Администратора схемы. Если пользователь имеет права "Администратор предприятия", то этого достаточно.

Для добавления нового атрибута потребуется ввести X.500 OID – уникальный идентификатор объекта. Для формирования корректного идентификатора можно воспользоваться Power Shell скриптом (https://gallery.technet.microsoft.com/scriptcenter/Generate-an-Object-4c9be66a)

```
#---

$Prefix="1.2.840.113556.1.8000.2554"

$GUID=[System.Guid]::NewGuid().ToString()

$Parts=@()

$Parts+=[UInt64]::Parse($guid.SubString(0,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(4,4),"AllowHexSpecifier")
```

```
$Parts+=[UInt64]::Parse($guid.SubString(9,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(14,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(19,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(24,6),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(30,6),"AllowHexSpecifier")

$OID=[String]::Format("{0}.{1}.{2}.{3}.{4}.{5}.{6}.{7}",$prefix,$Parts[0],$Parts[1],$Parts
[2],$Parts[3],$Parts[4],$Parts[5],$Parts[6])

$oid

#---
```

Скрипт необходимо скопировать в окно консоли PowerShell и выполнить его.

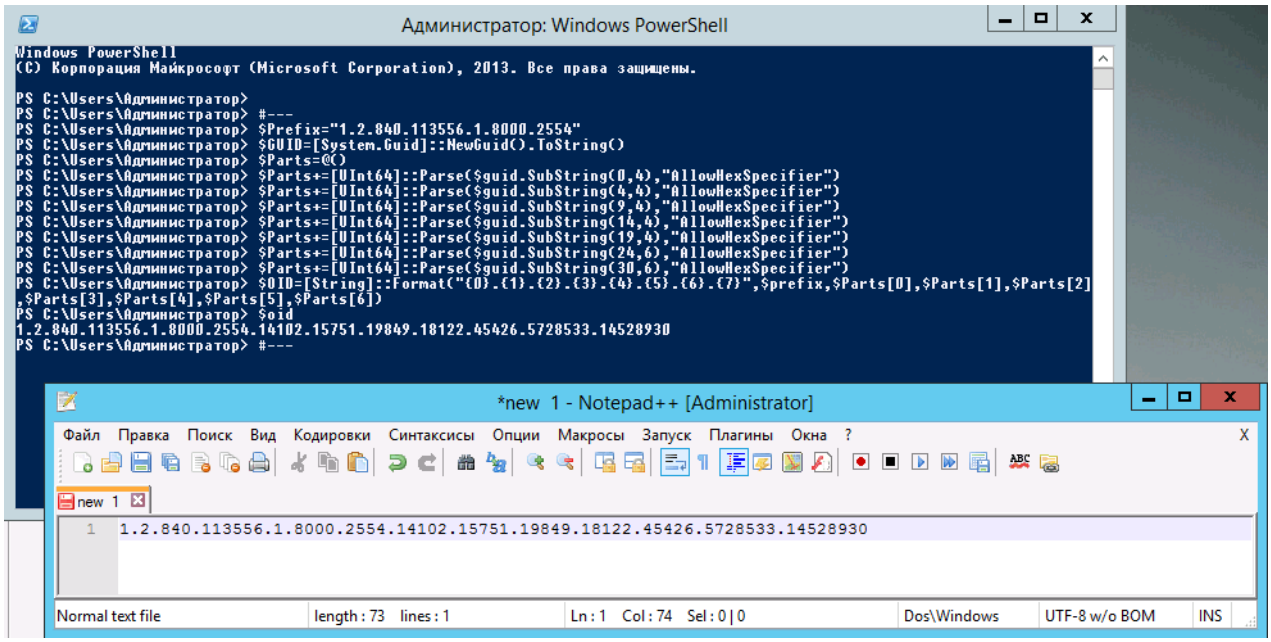

Рис. 57. Генерация X.500 OID

Результат выполнения скрипта – новый X.500 OID, который нужно будет ввести в соответствующее поле на форме создания атрибута.

Далее следует создать новый атрибут **bastionopers** (синтаксис «Строка Юникода»), необходимый для хранения профиля (см. Рис. 58).

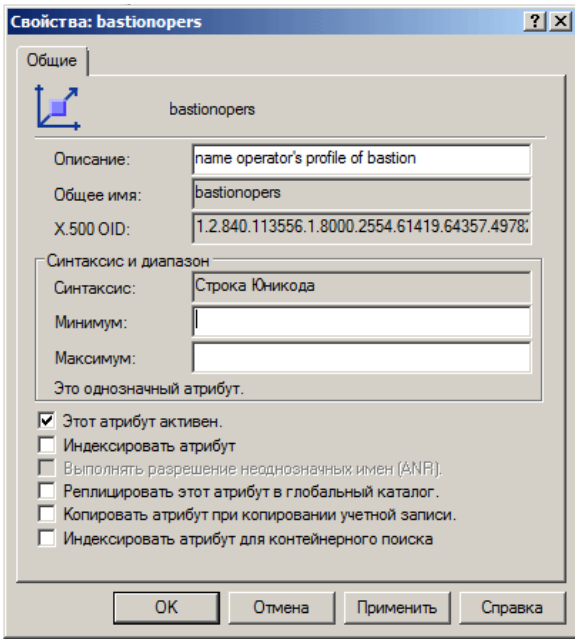

Рис. 58. Добавление атрибута bastionopers

Затем следует добавить атрибут в класс **user**. Для этого в оснастке «Схема Active Directory» можно перейти в раздел **Classes (Классы)**.

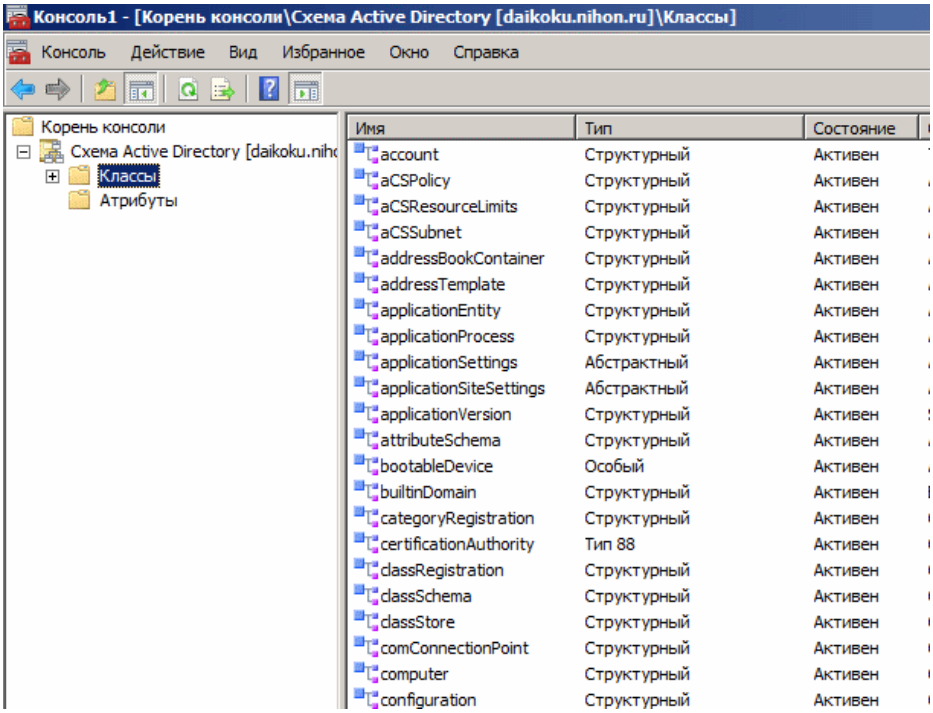

Рис. 59. Раздел "Классы" схемы Active Directory

В свойствах класса **user** необходимо перейти на закладку **Attributes (Атрибуты)** и там добавить новый атрибут класса.

Командой **adsiedit.msc** можно запустить редактор **ADSI Edit (Редактирование ADSI)** чтобы сделать новый атрибут видимым в оснастке **Active Directory Users and Computers**. В параметрах подключения следует выбрать **Configuration**. Затем перейти к контейнеру **CN=419, CN=Display Specifiers, CN=Configuration**. Для отображения в англоязычной консоли CN=409.

Для отображения атрибутов на уровне OU выбираем контейнер **CN=organizationalUnit-Display**. В свойствах контейнера необходимо найти атрибут extraColumns, который отвечает за вывод дополнительных атрибутов и добавить в него строку в формате:

1) Название атрибута;
2) Заголовок колонки, в которой будет отображаться атрибут;
3) Будет ли отображаться по умолчанию (ставим 1);
4) Ширина колонки в пикселях, значение 1 означает автоматический подбор ширины;
5) Зарезервированное значение (ставим 0).

Например: *ExtraColumns bastionopers.Bastion_operator.1.1.0*

Внимание! *Для того, чтобы новый атрибут стал виден в оснастке* ***Active Directory Users and Computers****, после добавления атрибута её необходимо переоткрыть.*

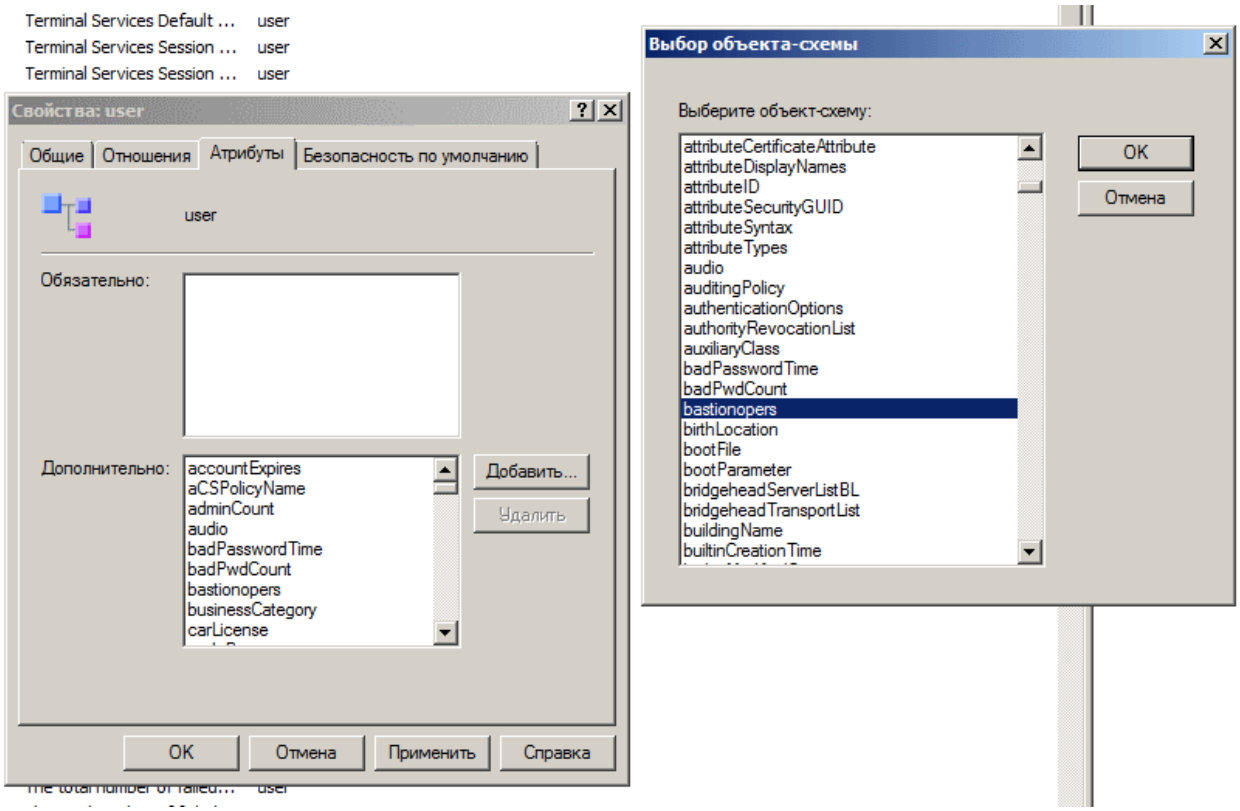

Рис. 60. Атрибуты класса user

6.5.3.2 Настройка идентификации пользователя Active Directory для АПК «Бастион-2»

Для настройки идентификации пользователей Active Directory для АПК «Бастион-2» следует выполнить последовательность действий, представленную ниже.

На контроллере домена Active Directory запустить оснастку Active Directory Users and Computers, выбрать в дереве слева узел Users и создать отдельную группу (**group),** предназначенную для пользователей АПК «Бастион-2», например, с именем apk_bastion_users.

Внимание! *Имя группы должно быть без пробелов и спецсимволов.*

Поместить в созданную группу тех пользователей AD, которые будут впоследствии работать с АПК «Бастион-2» с учетной записью AD (закладка member of в свойствах пользователя, см. Рис. 61).

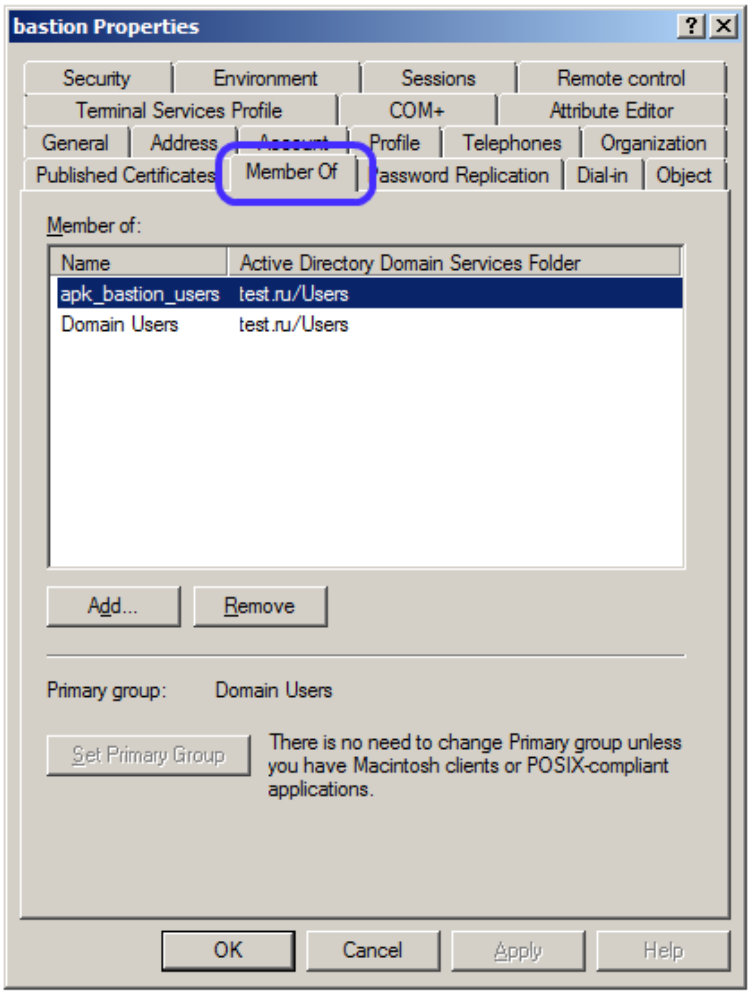

Рис. 61. Настройка членства в группах для пользователя АПК «Бастион»

Если в свойствах пользователя отображается закладка attribute editor (см. Рис. 62), то следует найти в списке атрибутов пользователя атрибут, заранее созданный для хранения профиля пользователя АПК «Бастион-2». После чего необходимо присвоить атрибуту, предназначенному для хранения профиля (созданного в АПК «Бастион-2») пользователя АПК «Бастион-2» символьное значение, совпадающее с именем профиля.

Если таких атрибутов нет, то следует найти любой незанятый атрибут, который принимает **символьные значения** (например, sn). Это будет атрибут для хранения профиля пользователя АПК «Бастион-2». Присвоить этому атрибуту символьное значение, совпадающее с именем профиля АПК «Бастион-2», созданного в АПК «Бастион-2» для пользователей AD.

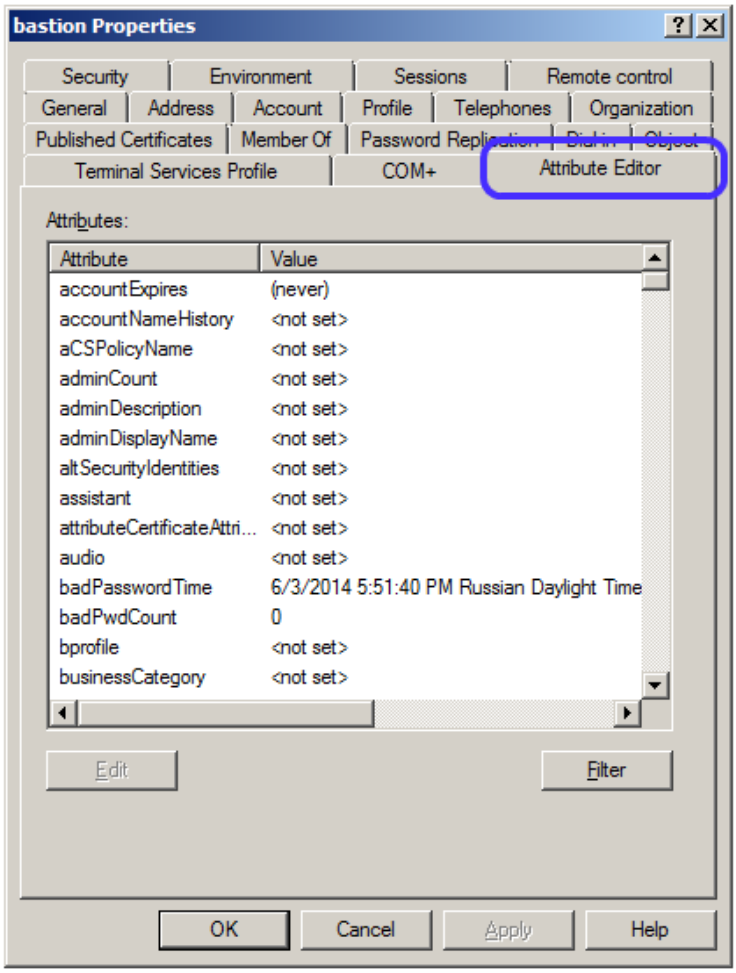

Рис. 62. Attribute Editor

Если в свойствах пользователя не отображается закладка attribute editor, тогда следует в меню «View» («Вид») выбрать опцию «Advanced features» («Расширенные возможности»). После этого attribute editor станет доступным (см. Рис. 63).

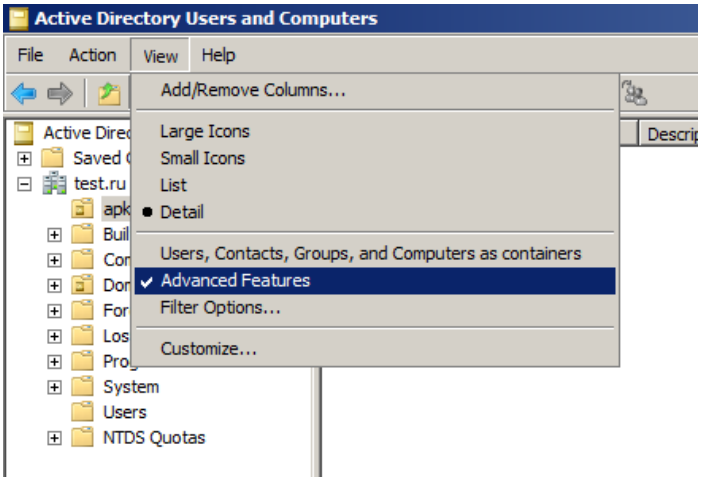

Рис. 63. Настройка отображения консоли Active Directory

После этого следует добавить рабочую станцию, где установлен АПК «Бастион-2» в домен Active Directory.

Затем, в АПК «Бастион-2» произвести настройку как указано в п.6.5.1.

После этого при первом запуске АПК «Бастион-2» должен будет появиться пользователь одноименный с пользователем Active Directory, под которым выполнен вход в систему на данной рабочей станции.

6.5.3.3 Использование авторизации LDAP совместно с функциями расширенной безопасности АПК «Бастион-2»

Для настройки совместной работы авторизации LDAP и функций расширенной безопасности АПК «Бастион-2», откройте форму «Общие настройки» в АПК «Бастион-2» и запустите программу настройки расширенного управления безопасностью (см. Рис. 64).

Для того, чтобы АПК «Бастион-2» запускался вместо проводника и использовал авторизацию LDAP, следует:

1. Отметить флаг «Загружать вместо стандартной оболочки ОС». Указать логин и пароль пользователя LDAP, под которым будет осуществляться вход в АПК «Бастион-2».
2. Отметить флаг «использовать автологон при загрузке Windows». Там указать имя пользователя Windows, который будет работать на данной рабочей станции, и его пароль.

Если необходимо — можно запретить использование консолей и управляющих элементов.

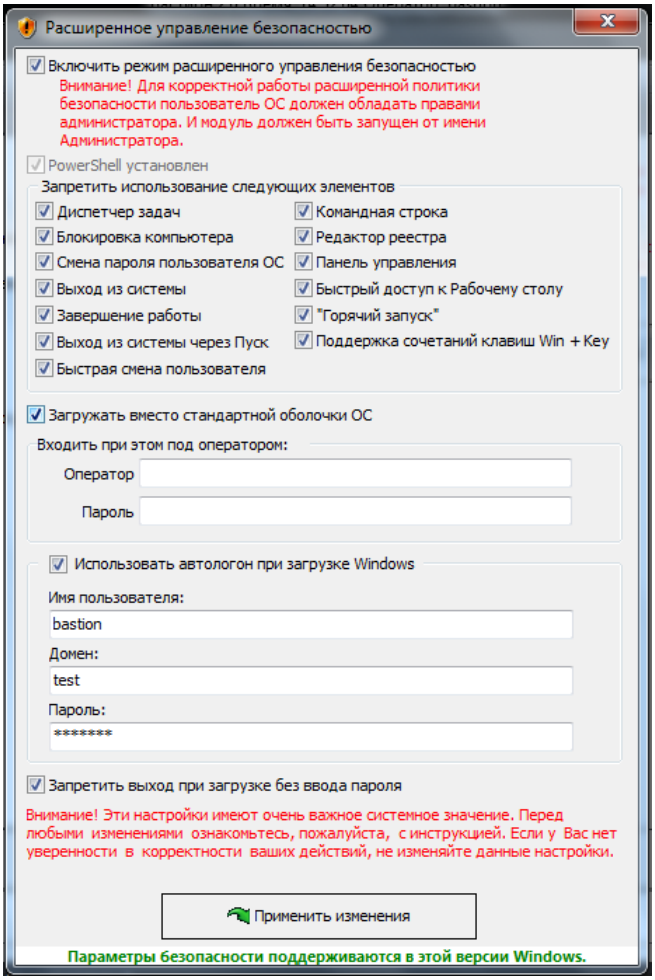

Рис. 64. Программа настройки расширенного управления безопасностью

После перезагрузки рабочей станции должен автоматически загрузиться АПК «Бастион-2» под оператором с соответствующим пользователем.

6.6 Авторизация с использованием настольных считывателей

Система, начиная с версии 2.1.9, поддерживает возможность авторизации пользователей с использованием настольных считывателей и карт доступа СКУД.

Для того, чтобы разрешить такую авторизацию, следует выполнить следующие действия:

1. Связать операторов АПК «Бастион-2» с пропусками, как описано в п.5.6.
2. Разрешить авторизацию по настольным считывателям в «Общих настройках», см. Рис. 56.
3. На каждом компьютере, где будет разрешена авторизация по настольным считывателям, следует установить тип используемого считывателя в «Локальных настройках», Рис. 65.

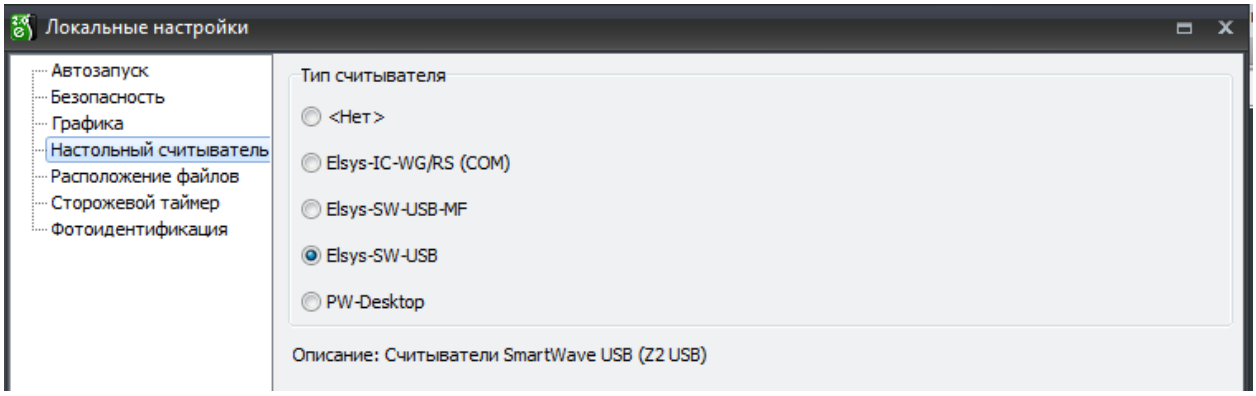

Рис. 65. Выбор типа считывателя в «Локальных настройках»

После выполнения указанных действий настольный считыватель будет активироваться каждый раз при запуске или блокировке системы.

Авторизация по настольному считывателю доступна в АРМ Оператора, АРМ Бюро пропусков, АРМ Генератор отчётов и АРМ УРВ Про.

В АРМ Оператора, дополнительно, предъявление карты активного оператора к настольному считывателю в штатном режиме работы будет приводить к блокировке системы.

7 Нештатные ситуации

7.1 Логи системы

При возникновении нештатных ситуаций в работе, а также в случае необходимости проведения диагностики в тех или иных случаях, система может создавать журналы – логи, различного содержания и назначения.

Информация сохраняется в журнале «Bastion Event Log», а также в лог-файлах, расположенных в папке установки АПК «Бастион-2». Журнал «Bastion Event Log» может быть просмотрен с помощью системной программы «Просмотр событий». В реальном времени события отображаются в приложении «Отладочная консоль», входящем в состав АПК «Бастион-2».

Логи могут содержать информацию об исключениях, возникших при выполнении программных модулей, протоколы отправки и получения различных данных и другую информацию.

При обращении в техническую поддержку может понадобиться предоставить эти журналы для анализа специалистами.

7.1.1 Настройки уровня логирования

Для сохранения логов в журнал «Bastion Event Log», на компьютере должна быть запущена служба «BAgentSvc».

При настройках по умолчанию в данный журнал сохраняются только события об ошибках системы.

Уровень логирования событий задаётся строковым параметром Level в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ES-Prom\Bastion2\Logs – для 64-битной системы и в ветке HKEY_LOCAL_MACHINE\SOFTWARE\ES-Prom\Bastion2\Logs для 32-битной. По умолчанию данный параметр имеет значение 0.

Для сохранения в журнал предупреждений и информационных сообщений нужно установить значение параметра равное 1, для сохранения всех сообщений - 2. Изменения вступят в силу в течение 2 минут, либо после перезапуска службы «BAgentSvc».

8 Обслуживание системы

8.1 Расширение системы

8.1.1 Общие сведения

Расширение системы производится путём закупки дополнительных модулей. Ключи активации для модулей записываются в ключ HASP Net. Обычно, используется 1 ключ на систему. В отдельных случаях, когда используется большое число рабочих станций (более 10), может потребоваться использование нескольких ключей HASP Net.

Если докупается новый модуль интеграции, которого не было в основном комплекте поставки, то такой драйвер необходимо установить на каждый компьютер системы отдельно.

8.1.2 Использование утилиты «Менеджер лицензий»

Изменение списка активных модулей производится при помощи утилиты «Менеджер лицензий» (LicenseManager.exe), входящей в комплект поставки программного комплекса.

Общая последовательность действий, в случае, когда необходимо изменить набор активных модулей, следующая:

1. Оплатить дополнительные модули.
2. Создать в «Менеджере лицензий» файл с текущим набором кодов активации c2v.
3. Отправить полученный файл в службу технической поддержки.
4. Получить файл активации модулей v2c для ключа HASP.
5. Применить полученное обновление в «Менеджере лицензий».

После приобретения дополнительных модулей необходимо выполнить следующие действия для их активации:

1. Вставить ключ HASP Net в свободный USB порт компьютера и запустить утилиту LicenseManager.exe (Пуск – Программы – Бастион-2 – Администрирование – Менеджер лицензий). Внешний вид окна программы с закладкой, содержащей информацию об активных модулях, представлен на Рис. 66:

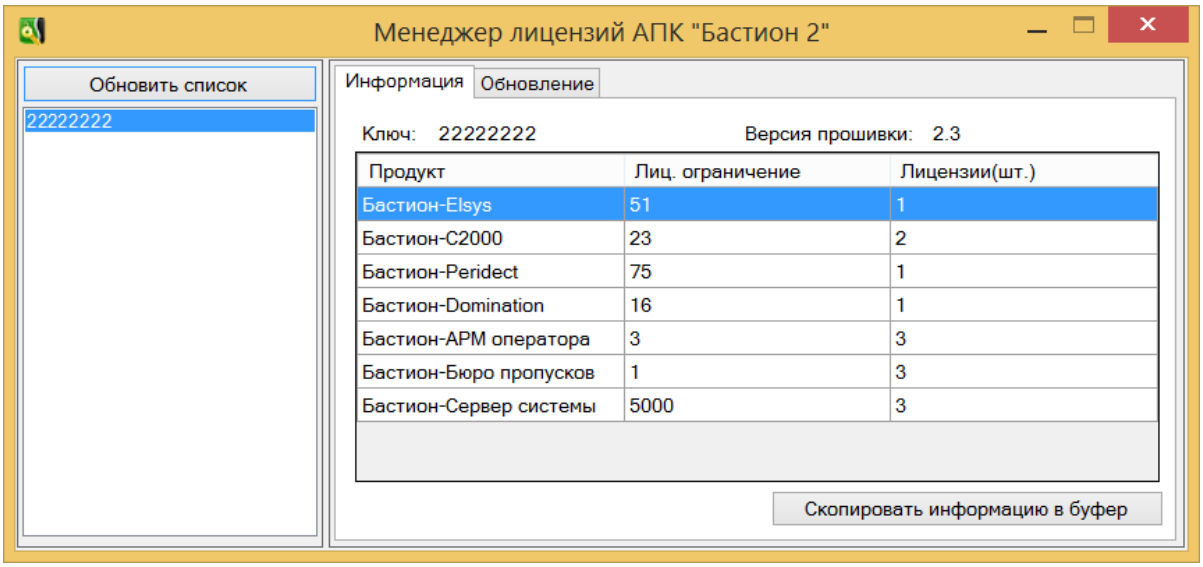

Рис. 66 Внешний вид программы «Менеджер лицензий»

В левой части окна находится список всех подключенных к компьютеру ключей HASP Net. В верхней части выводится идентификационный номер текущего ключа, а в нижней – информация об установленных компонентах в этом ключе. Если необходимо запрограммировать несколько ключей, подключите их все к компьютеру и нажмите кнопку Обновить список.

2. Перейти на вкладку «Обновление» (Рис. 67). Сформировать файлы c2v для каждого ключа, требующего обновления, поочередно выбирая их в левом списке и нажимая кнопку Сформировать файл лицензии на вкладке «Обновление».
3. Отослать сформированные файлы *.c2v в службу технической поддержки Ассоциации «Электронные системы».
4. После проверки факта оплаты Вам будут отправлены файлы обновлений в формате *.v2c для программирования указанных ключей. Каждому ключу соответствует свой, уникальный файл *.v2c.

5. Для программирования ключей следует подключить их к компьютеру и запустить утилиту LicenseManager.exe. Затем следует выбрать ключ из списка слева и перейти на вкладку «Обновление» (Рис. 67).

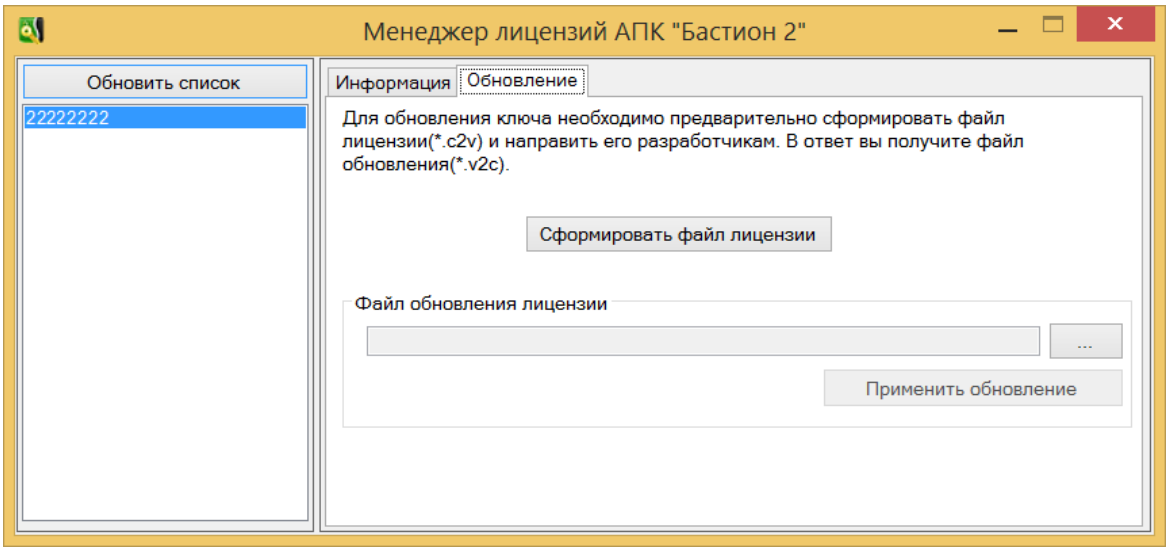

Рис. 67. Вкладка «Обновление»

6. После этого необходимо выбрать файл обновления *.v2c, нажав на кнопку ... и указав соответствующий ключу файл обновления. После выбора файла будет доступна кнопка Применить обновление. Нажмите её для запуска процесса обновления ключа.

Внимание! Не следует вынимать ключ из USB-порта компьютера до завершения процесса обновления.

После выполнения указанных действий всё готово для запуска и настройки АПК «Бастион-2» в новой конфигурации.

8.1.3 Установка дополнительных драйверов отдельно

Дополнительные драйверы могут не входить в комплект поставки основного релиза АПК «Бастион-2». Например, если драйвер был выпущен после выхода очередной версии АПК «Бастион-2», то его не будет в основном комплекте поставки.

Такие драйверы можно установить отдельно. Они поставляются в виде msi-пакетов (файл с расширением .msi).

Для установки пакета драйвера требуются права администратора Windows.

Драйвер, установленный отдельно, будет виден отдельной строкой в списке установленных программ. Соответственно, удалять его также следует отдельно.

Следует устанавливать драйвер на все компьютеры, оснащённые АРМ Оператора АПК «Бастион-2».

8.2 Настройка подключений

8.2.1 Общие сведения

Для работы с АПК «Бастион-2» должны быть настроены подключения к серверу системы и серверу баз данных. Все необходимые начальные параметры задаются при установке системы.

Для настройки этих подключений в дальнейшем используется утилита «Настройка подключений», а для управления схемами БД на одном и том же сервере, используется другая утилита – «Управление схемами».

Если на компьютере необходимо переключаться между разными серверами АПК «Бастион-2», то можно настроить несколько подключений и переключаться между ними с использованием утилиты «Настройка подключений». В этом случае, один и тот же компьютер может являться клиентом разных систем АПК «Бастион-2» с переключением текущего сервера через утилиту «Настройка подключений».

Для запуска утилиты «Настройка подключений» выберите в меню «Пуск» пункт «ES-Prom – АПК «Бастион-2» – Администрирование – Настройка подключений».

8.2.2 Утилита «Настройка подключений»

8.2.2.1 Добавление и настройка подключений

Для добавления нового подключения нажмите кнопку «+» в панели инструментов. В появившейся форме можно задать параметры подключения (Рис. 68):

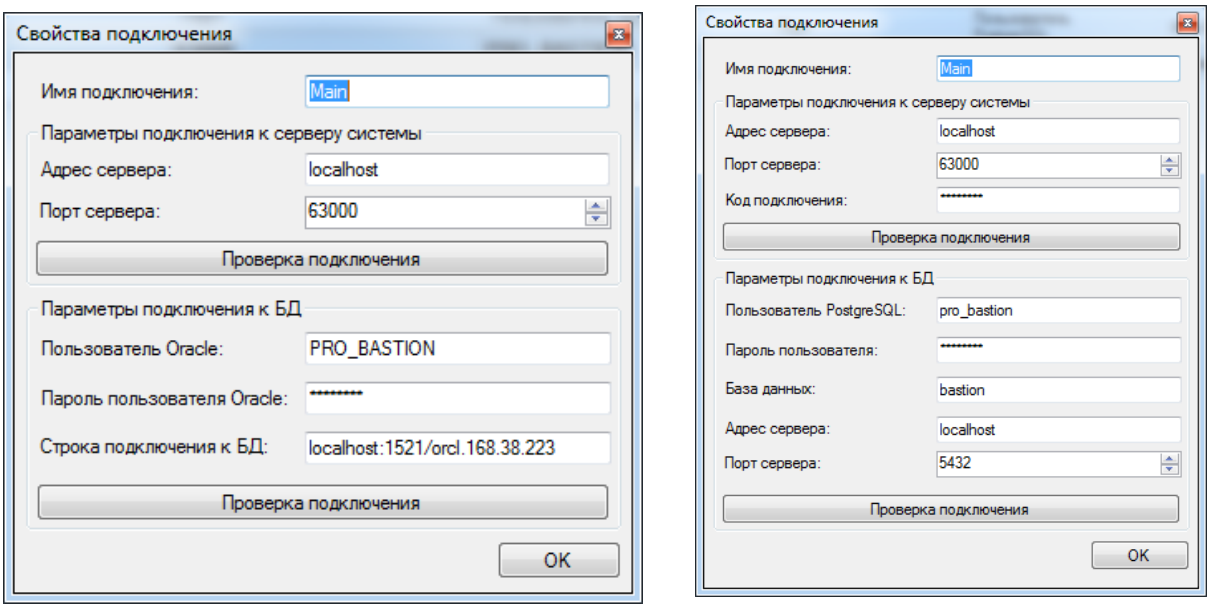

Рис. 68. Свойства подключения

Каждое создаваемое подключение объединяет данные о подключении к серверу системы АПК «Бастион-2» и к серверу баз данных. В этой форме необходимо указать:

Имя подключения – используется для обозначения, идентификации подключения.

Для подключения к серверу системы задаются *адрес сервера* и используемый TCP-порт (*Порт сервера*). В поле «Адрес сервера» может быть указано как имя, так и IP-адрес сервера.

Для подключения к серверу баз данных Oracle указываются следующие параметры:

Пользователь Oracle – имя пользователя, схемы Oracle.

Пароль пользователя Oracle – пароль для подключения к указанной схеме.

Строка подключения к БД. Указывается в виде:

```
host:port/servicename
```

Например:

```
BServer:1521/ORCL
```

Для подключения к серверу баз данных PostgreSQL указываются следующие параметры:

Пользователь PostgreSQL – имя пользователя PostgreSQL.

Пароль пользователя – пароль пользователя для подключения к БД.

База данных – имя базы данных на сервере PostgreSQL.

Адрес сервера – адрес сервера PostgreSQL.

Порт сервера – порт сервера PostgreSQL.

Перед сохранением изменений рекомендуется проверить наличие подключения к серверам системы и БД.

Для сохранения внесенных изменений после закрытия формы свойств подключения следует нажать кнопку «Сохранить» на панели инструментов главной формы.

8.2.2.2 Активация подключений

Для активации подключения нажмите кнопку «√» в панели инструментов. Необходимо перезапустить все программы АПК «Бастион-2» для подключения их с новыми параметрами в следующей последовательности:

1. Выгрузить все АРМ и программы АПК «Бастион-2».
2. Остановить сервис BAgentSvc (если настройка выполняется на сервере системы).
3. Дождаться завершения работы всех процессов АПК «Бастион-2» (BAgent.exe, Bastion.DriverHost.exe и т. п.).
4. Запустить сервис BAgentSvc (если настройка выполняется на сервере системы).
5. Загрузить требуемые АРМы и программы.

8.3 Администрирование поиска ключей HASP

АПК «Бастион-2» использует аппаратные сетевые ключи HASP Net для хранения ключей активации. Проверяет наличие и корректность использования ключей активации сервер системы. В некоторых случаях может потребоваться использование нескольких серверов системы и

нескольких ключей HASP. Для настройки такой конфигурации следует учитывать следующую особенность:

> ***Внимание!*** *Сервер системы подключается и занимает все доступные коды активации модулей на всех ключах, которые он может найти в сети.*

Для того, чтобы сервер системы подключался и использовал только конкретные ключи, необходимо настроить параметры поиска удаленных лицензий в Sentinel Admin Control Center.

Для этого, на компьютере, где выполняется сервер системы, следует запустить браузер и перейти по адресу: http://localhost:1947. Для удобства работы можно выбрать русский язык, нажав ссылку «More Languages…» и затем нажав кнопку Install в строке Russian (для выполнения этого действия требуется интернет-подключение).

Далее, на странице Sentinel Admin Control Center следует выбрать пункт «Конфигурация» (Configuration) и перейти на страницу «Доступ к удаленным Менеджерам лицензий» (Access To Remote License Managers). Здесь, в поле «Параметры поиска удаленных лицензий» (Remote License Search Parameters), можно указать, где будет производиться поиск ключей HASP. Можно указывать конкретные IP-адреса, маски подсетей, а также имена конкретных компьютеров. Каждая запись должна быть на отдельной строке.

Например, чтобы ограничить поиск ключей компьютером HASPSRV и подсетью 192.168.21.255, настройка должна выглядеть так, как показано на Рис. 69.

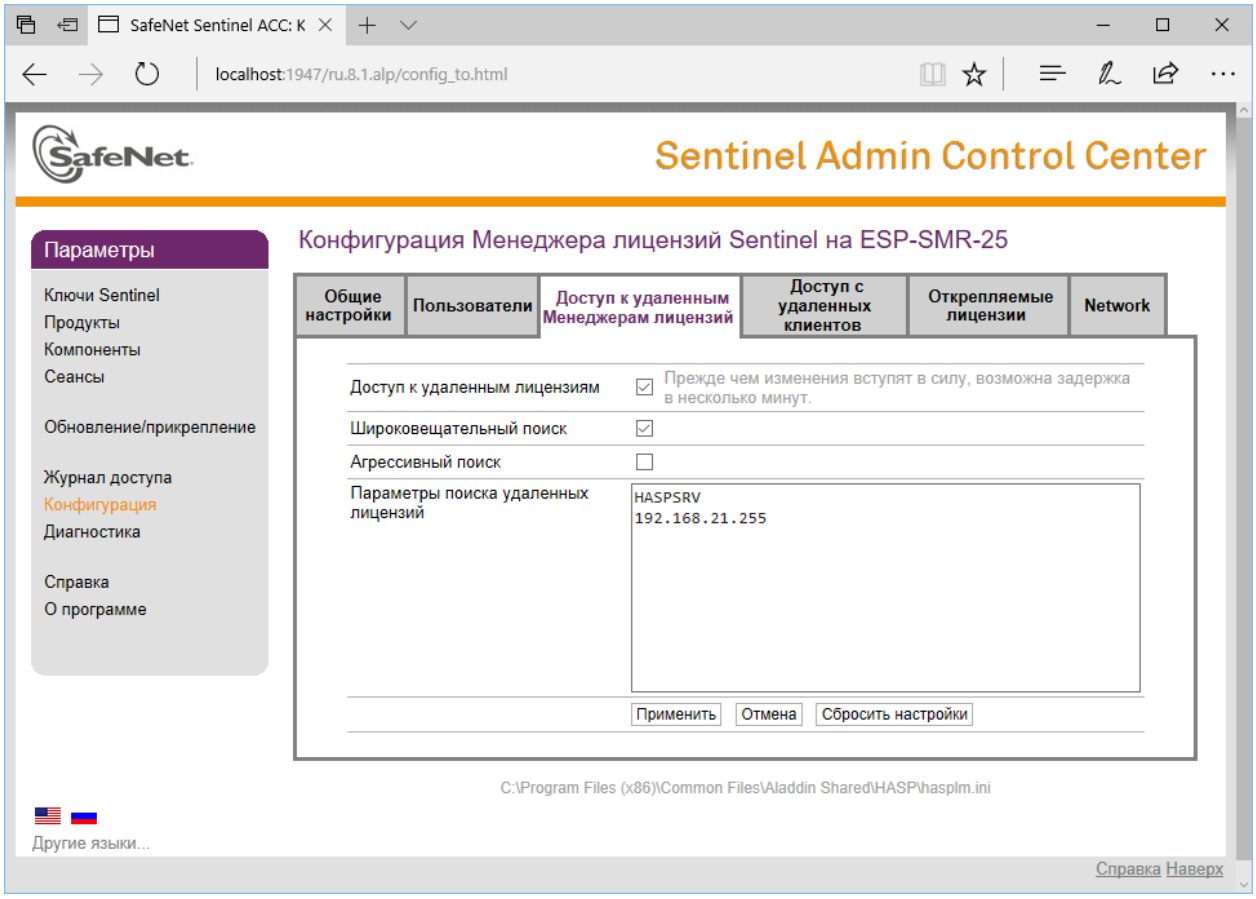

Рис. 69. Настройка режима поиска ключей HASP

8.4 Администрирование баз данных

8.4.1 Общие сведения

Для администрирования БД АПК «Бастион-2» предназначена утилита «Управление схемами АПК «Бастион-2». Также, для выполнения задач администрирования могут быть использованы встроенные средства СУБД и сторонние приложения. В этом руководстве приводится описание работы утилиты «Управление схемами АПК «Бастион-2».

АПК «Бастион-2» устанавливает клиента Oracle для Windows x86 с именем **BastionHome**. Рекомендуется использовать именного этот экземпляр клиента Oracle для работы с БД АПК «Бастион-2». Клиент Oracle устанавливается в папку <ProgramFiles (x86)>\ES-Prom\Bastion2\OracleClient. В этой же папке находится файл tnsnames.ora, который будет использоваться для подключения к БД.

> ***Внимание!*** *Для работы АПК «Бастион-2» должна быть установлена именно 32-разрядная версия клиента Oracle. Тем не менее, может использоваться 64-разрядный сервер Oracle.*

В случае работы с PostgreSQL отдельных клиентов СУБД для работы АПК «Бастион-2» не требуется. Все необходимые библиотеки устанавливаются вместе с АПК «Бастион-2», их настройка не требуется.

8.4.2 Запуск модуля «Управление схемами АПК «Бастион-2»

Для запуска модуля выберите из меню «Пуск» пункт «ES-Prom – АПК ‘Бастион-2’ – Администрирование – Управление схемами БД».

При запуске необходимо ввести параметры подключения к БД.

В случае Oracle:

Клиент Oracle – экземпляр клиента, через который будет выполнено подключение. Рекомендуется использовать BastionHome, предлагаемый по умолчанию.

TNS-псевдоним сервера Oracle – псевдоним, указанный при установке АПК «Бастион-2» в поле «*База данных Oracle».* По умолчанию – Bastion2.

Пароль пользователя SYSTEM – если вы не знаете этот пароль, обратитесь к администратору СУБД Oracle.

В случае PostgreSQL:

Сервер базы данных – сетевое имя или IP-адрес сервера БД.

Порт – порт подключения к серверу БД.

Имя пользователя и пароль – параметры суперпользователя сервера PostgreSQL.

8.4.3 Развёртывание схемы базы данных

Для развёртывания схемы нажмите кнопку «Создать схему» («Создать БД») в основном окне модуля «Управление схемами». Откроется окно, приведённое на Рис. 70.

Здесь необходимо ввести параметры создания БД.

Параметры для Oracle

Имя схемы – имя пользователя Oracle, который будет создан и для которого будет развёрнута схема АПК «Бастион-2». Следует указывать то же имя, что вводилось при установке системы в поле «Имя пользователя».

Пароль и подтверждение – пароль пользователя и его подтверждение. Следует вводить тот пароль, который был указан при установке системы в поле «Пароль пользователя Oracle».

DMP-файл – полный путь к файлу с дампом базы данных. АПК «Бастион-2» поставляется в комплекте с эталонным дампом TargetDump.dmp, расположенным в каталоге <Program Files (x86)>\ES-Prom\Bastion2\Data.

Схема, с которой был создан DMP-файл – необходимо ввести имя схемы (пользователя), с которой был сделан дамп. Для эталонного дампа следует ввести значение PRO_BASTION.

Утилита для работы с dmp-файлами. Для экспорта и импорта данных могут быть использованы утилиты Oracle Exp.exe / Imp.exe (Exp/Imp) или ExpDp.exe / ImpDp.exe (Data Pump). Эти утилиты используют дампы разных форматов. Поэтому, для корректного создания схемы следует указать способ, которым был создан дамп. Эталонный дамп поставляется в формате для использования с Exp/Imp. Таким образом, на компьютере, с которого предполагается произвести развертывание базы данных, необходимо наличие утилиты imp.exe, которая устанавливается при инсталляции любой версии СУБД Oracle, включая бесплатную версию Oracle XE, либо расширенную версию клиента Oracle, входящего в состав Oracle Enterprise Edition. Путь к этой утилите должен быть указан в переменной среды Path (при установке Oracle Database Server это выполняется автоматически).

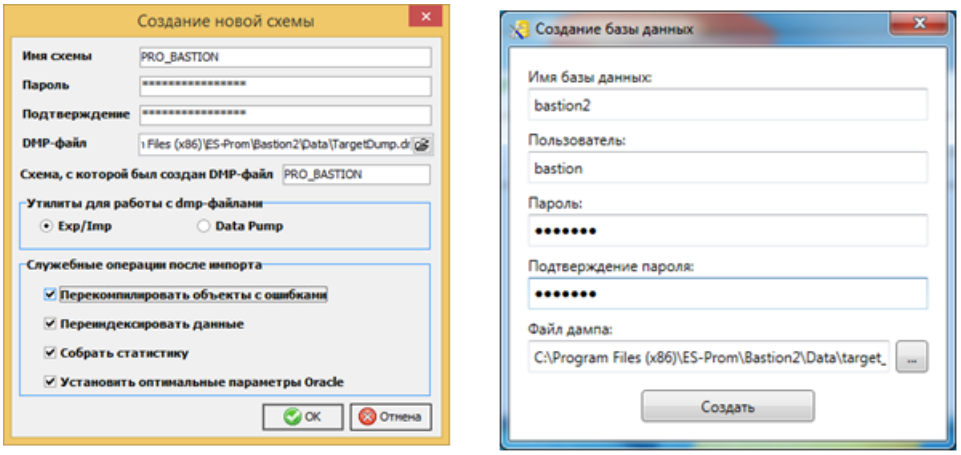

Рис. 70 Форма создания схемы БД (слева для Oracle, справа – PostgreSQL)

Внимание! *Утилиты Exp/Imp могут использоваться с любого компьютера, где установлен* ***полный клиент*** *Oracle. Клиент Oracle, устанавливаемый с АПК «Бастион-2»,* ***не содержит*** *утилит Exp/Imp.*

Внимание! *Утилиты Data Pump могут быть использованы только на компьютере, где установлен сервер Oracle. Дамп должен находиться на сервере СУБД.*

Внимание! *При использовании утилит Data Pump путь к файлу и его имя могут содержать только символы латинского алфавита, пробел и символы \:.№!@#$%^&()_+=-*

_{}[];', ., использование кириллицы может привести к ошибкам чтения и сохранения файла.

Внимание! *Развернуть схему на компьютере, где установлен только 64-разрядный полный клиент Oracle, можно через Exp/Imp, если вручную прописать данные о подключении BASTION2 в файл TNSNAMES.ORA полного клиента Oracle. Эти данные можно скопировать из аналогичного файла в папке <Bastion2>\OracleClient.*

Более подробно информацию о различиях этих способов экспорта / импорта данных можно посмотреть в документации на СУБД Oracle.

Раздел «Служебные операции после импорта» позволяет выполнить ряд операций после создания схемы, которые оптимизируют работу сервера Oracle для созданной схемы.

Перекомпилировать объекты с ошибками – если в ходе первичного развёртывания дампа остались объекты с ошибками, то будет сделана попытка их перекомпилировать повторно. Повторная компиляция может дать эффект, если имели место зависимости между объектами. Рекомендуется оставлять этот флаг включенным.

Переиндексировать данные – установите флаг для пересоздания всех индексов в БД после импорта. Используется для ускорения работы системы в дальнейшем. Рекомендуется оставлять флаг включенным.

Собрать статистику – установите флаг для оптимизации скорости выполнения запросов к БД в дальнейшем. Рекомендуется оставлять флаг включенным.

Установить оптимальные параметры Oracle – задает значения ряда параметров сервера Oracle для оптимальной работы с АПК «Бастион-2». Устанавливаются значения для числа открытых курсоров на каждое подключение (OPEN_CURSONS = 500) и числа одновременных подключений (PROCESSES = 1000). Рекомендуется оставлять флаг включенным.

Параметры для PostgreSQL

Имя базы данных – название БД на сервере PostgreSQL.

Пользователь и пароль – параметры пользователя БД АПК «Бастион-2».

Файл дампа – полный путь к файлу с дампом базы данных. АПК «Бастион-2» поставляется в комплекте с эталонным дампом target_dump.dmp, расположенным в каталоге <Program Files (x86)>\ES-Prom\Bastion2\Data.

После установки всех параметров, нажмите кнопку «ОК» («Создать»). Начнётся процедура создания схемы.

При выполнении импорта будет создан Log-файл в каталоге <ProgramFiles (x86)>\ES-Prom\Bastion2\Tools\Logs, который может использоваться для диагностики ошибок.

В случае использования Oracle, если развертывание схемы не было произведено корректно, необходимо убедиться в наличии корректно установленной утилиты импорта (imp.exe), а также в том, что в серверном файле tnsnames.ora прописан тот же псевдоним и параметры подключения,

что и в клиентском tnsnames.ora. При установке Бастиона соответствующие записи производятся автоматически, при условии, что сервер Oracle является 32-разрядным.

Система также позволяет создавать несколько экземпляров схемы (БД) АПК «Бастион-2» на одном сервере БД и переключаться между ними.

> ***Внимание!*** *В случае использования Oracle, если необходимо развернуть несколько экземпляров схем АПК «Бастион-2» под разными пользователями, то необходимо, чтобы все дополнительные дампы были созданы через Data Pump.*

8.4.4 Переключение активной базы данных

Для переключения активной базы данных (той схемы, с которой работает АПК «Бастион-2») следует воспользоваться утилитой «Настройка подключений». Для её запуска выберите из меню «Пуск» пункт «ES-Prom – АПК ‘Бастион-2’ – Администрирование – Настройка подключений».

> ***Внимание!*** *Для запуска утилиты пользователь Windows должен обладать правами администратора.*

Если в списке баз данных присутствует необходимая и её параметры совпадают с текущими используемыми в системе, то её нужно выбрать и нажать кнопку «Активировать подключение». В противном случае можно выбрать текущую базу данных, и нажать кнопку «Редактировать подключение», либо создать новую. Отобразится окно, приведенное на Рис. 71.

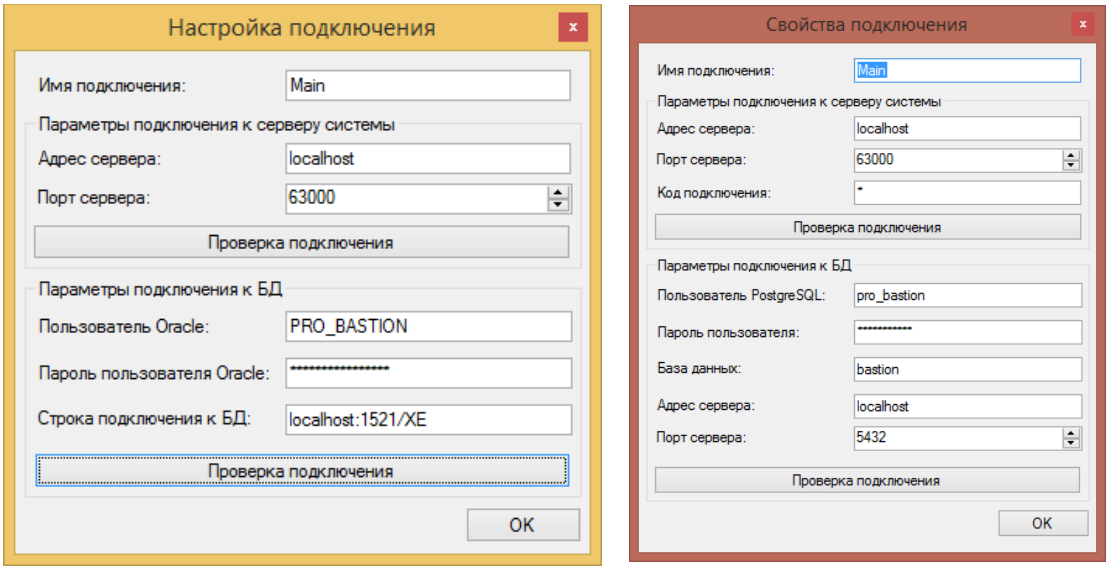

Рис. 71 Форма редактирования подключения (слева – Oracle, справа – PostgreSQL)

Адрес сервера – сетевое имя или IP адрес сервера системы,

Порт сервера – порт, выбранный в настройках подключения на сервере системы,

Код подключения – слово, используемое для подключения серверов оборудования,

Параметры подключения к БД (см. п.8.2.2.1).

Созданную либо отредактированную неактивную БД нужно активировать.

8.4.5 Резервное копирование

Для выполнения резервного копирования выбранной схемы следует нажать кнопку «Экспортировать в файл». Появится окно, приведённое на Рис. 72.

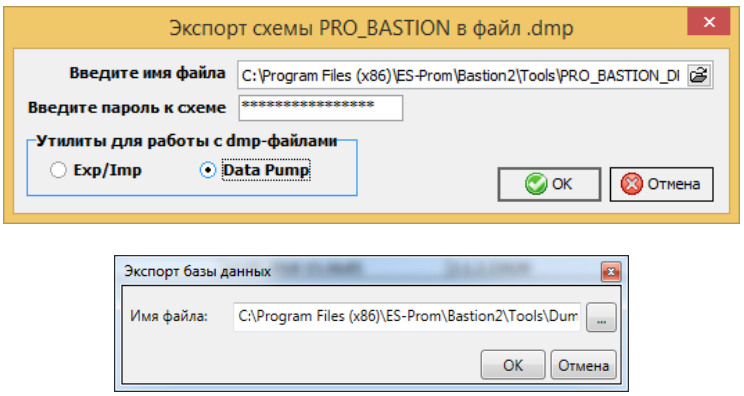

Рис. 72 Форма экспорта дампа БД (сверху – для Oracle, снизу – для PostgreSQL)

Здесь следует ввести имя файла, куда будет сохранён дамп и пароль к схеме.

Также, для Oracle необходимо выбрать утилиту для выполнения резервного копирования. Рекомендуется выполнять эту задачу на сервере БД с использованием способа Data Pump.

Задачу выполнения резервного копирования можно автоматизировать, если создать bat-файл, выполняющий соответствующие команды Oracle, и добавить этот файл в планировщик Windows. Процесс создания такого фала приведен в следующем разделе.

8.4.6 Настройка автоматического резервного копирования схемы Oracle АПК «Бастион-2»

Резервное копирование схемы выполняется с помощью набора командных файлов и sql-скриптов. Используется утилита EXPDP, находящаяся на сервере СУБД ORACLE, дамп-файл также создается на сервере СУБД ORACLE. Пользователь операционной системы должен обладать правами администратора и входить в группу **ora_dba**. Предполагается, что схема АПК «Бастион-2» уже развернута.

В комплект поставки системы входят следующие файлы: create_backupdir.cmd, exp_dp.cmd, create_backupdir.sql, расположенные на установочном диске в папке **Redist\BackupCmd**. Все их нужно поместить в один каталог с произвольным именем на сервере СУБД Oracle. Настройка выполняется в следующей последовательности:

1. Отредактировать (например, в программе «Блокнот») файл **create_backupdir.cmd**. В соответствующих строках нужно указать фактические значения параметров:
   - пароль системного пользователя **SYS** СУБД Oracle (для примера указан как **1**);
   - имя схемы, для которой будет создаваться дамп (для примера указано как **pro_bastion**);
   - имя сервиса (для примера указано **XE**, в ORACLE 11.2g Express Edition не может быть другим);

- путь к папке резервирования, в которую будет помещен дамп-файл (для примера указан как **c:\backup_dir**). Если в этой строке будут символы пробела, следует заключить ее в двойные кавычки, например, "d:\B2 backup".

2. Сохранить изменения в файле **create_backupdir.cmd** и **однократно** запустить его. Будет создана папка с выбранным именем по указанному пути (следует в этом убедиться), в структуре БД создастся каталог выгрузки дампа, пользователь БД будет наделен необходимыми правами на доступ к каталогу.

3. Отредактировать файл **exp_dp.cmd**. В соответствующих строках нужно указать фактические значения параметров:

   - имя схемы, для которой будет создаваться дамп (для примера указано как **pro_bastion**);

   - пароль системного пользователя **SYSTEM** СУБД Oracle (для примера указан как **1**);

   - имя сервиса (для примера указано как **XE**, в ORACLE 11.2g Express Edition не может быть другим);

   - путь к папке резервирования, в которую будет помещен дамп-файл (для примера указан как **c:\backup_dir**). Если в этой строке будут символы пробела, следует заключить ее в двойные кавычки, например, "d:\B2 backup";

   - путь к папке программы архивации, которая будет упаковывать дамп-файл в zip-архив (для примера указан как **"C:\Program Files\7zip"**).

4. Сохранить изменения в файле **exp_dp.cmd**, запустить его.

Процесс создания резервной копии выполняется следующим образом:

1. Утилита EXPDP создает в папке резервирования дамп-файл с именем вида **ИмяСхемы_DP_ГГГГ-ММ-ДД.dmp** и одноименный файл с расширением **log** (протокол создания дампа).

2. В папке резервирования создается каталог с именем вида **ГГГГ-ММ-ДД**, в который затем перемещаются дамп и лог-файл.

3. Запускается консольная версия программы архивации, добавляющая в архив с именем вида **ИмяСхемы_DP_ГГГГ-ММ-ДД.zip** дамп и лог-файл. Если процесс архивации завершается без ошибок, то исходные дамп и лог-файл удаляются, в противном случае работа завершается, исходные файлы остаются в неизменном виде.

4. Архив для повышения надежности хранения копируется на сетевой ресурс, предварительно подключенный как сетевой диск.

По окончании работы процесса следует убедиться, что в папке резервирования имеется каталог с именем вида **ГГГГ-ММ-ДД**, в котором будет находиться файл **ИмяСхемы_DP_ГГГГ-ММ-ДД.zip**, скопированный также на сетевой ресурс. Например, создание дампа схемы **pro_bastion** выполнено 30.07.2015 г., тогда в папке **c:\backup_dir\2015-07-30** будет файл

PRO_BASTION_DP_2015-07-30.zip. Если в ходе процесса возникают ошибки, нужно выяснить и устранить их причину, после чего снова запустить файл **exp_dp.cmd**.

Если процедура в ручном режиме отработала штатно, то для проверки правильности создания дампа нужно развернуть полученный дамп на тестовой системе и убедиться, что схема создается без ошибок. Развёртывание схемы из дампа выполняется вручную при помощи утилиты «Управление схемами БД», входящей в комплект АПК «Бастион-2».

Для автоматизации создания дампов следует добавить в планировщик заданий Windows задачу, которая будет запускать в заданное время файл **exp_dp.cmd**. Создание задачи в планировщике описано в справочной системе Windows.

8.4.7 Настройка автоматического резервного копирования БД АПК «Бастион-2» на СУБД PostgreSQL.

Резервное копирование БД выполняется с помощью командного файла. Используется утилита pg_dump, находящаяся на сервере СУБД PostgreSQL. Файл дампа также создается на сервере СУБД PostgreSQL. Пользователь операционной системы должен обладать правами администратора. Предполагается, что БД АПК «Бастион-2» уже развернута.

Файл: **pg_dump.cmd** нужно поместить в каталог с произвольным именем на сервере СУБД PostgreSQL. Настройка выполняется в следующей последовательности:

1. Отредактировать файл **pg_dump.cmd**. В соответствующих строках нужно указать фактические значения параметров:

   - указать путь расположения утилиты pg_dump (для примера указано как **C:\PostgreSQL\10\bin**);

   - имя пользователя (схемы), для которой будет создаваться дамп (для примера указано как **pro_bastion**);

   - пароль пользователя (схемы), для которой будет создаваться дамп (для примера указан как **1**);

   - наименование схемы, для которой будет создаваться дамп (для примера указано как **bastion**);

   - IP сервера БД (рекомендуем всегда указывать **localhost**) и порт для подключения к БД (для примера указан стандартный порт **5432**);

   - путь к папке резервирования, в которую будет помещен дамп-файл (для примера указан как **c:\backup_dir**). Если в этой строке будут символы пробела, следует заключить ее в двойные кавычки, например, "d:\B2 backup";

   - путь к папке программы архивации, которая будет упаковывать дамп-файл в zip-архив (для примера указан как **"C:\Program Files\7zip"**).

2. Сохранить изменения в файле **pg_dump.cmd**, запустить его.

Процесс создания резервной копии выполняется следующим образом:

а) утилита pg_dump создает в папке резервирования дамп-файл с именем вида

ИмяСхемы_ГГГГ-ММ-ДД.dmp и лог-файл с именем **ИмяСхемы_ГГГГ-ММ-ДД.log**

б) в папке резервирования создается каталог с именем вида **ГГГГ-ММ-ДД**, в который затем перемещаются дамп и лог-файл;

в) запускается консольная версия программы архивации, добавляющая в архив с именем вида **ИмяСхемы_ГГГГ-ММ-ДД.zip** дамп и лог-файл. Если процесс архивации завершается без ошибок, то исходные дамп и лог-файл удаляются, в противном случае работа завершается, исходные файлы остаются в неизменном виде;

г) архив для повышения надежности хранения копируется на сетевой ресурс, предварительно подключенный как сетевой диск.

По окончании работы процесса следует убедиться, что в папке резервирования имеется каталог с именем вида **ГГГГ-ММ-ДД**, в котором будет находиться файл **ИмяСхемы_ГГГГ-ММ-ДД.zip**, скопированный также на сетевой ресурс. Например, создание дампа схемы **bastion** выполнено 09.10.2018 г., тогда в папке **c:\backup_dir\2018-10-09** будет файл **bastion_2018-10-09.zip**. Если в ходе процесса возникают ошибки, нужно выяснить и устранить их причину, после чего снова запустить файл **pg_dump.cmd**.

Если процедура в ручном режиме отработала штатно, то для проверки правильности создания дампа нужно развернуть полученный дамп на тестовой системе и убедиться, что схема создается без ошибок. Разворачивание схемы из дампа выполняется вручную при помощи утилиты «Управление схемами БД», входящей в комплект ПО АПК «Бастион-2».

Для автоматизации создания дампов следует добавить в планировщик заданий Windows задачу, которая будет запускать в заданное время файл **pg_dump.cmd**. Создание задачи в планировщике описано в справочной системе Windows.

8.4.8 Дополнительная информация по командным файлам резервного копирования

Для архивирования дамп-файла используется консольная (работающая через параметры командной строки) версия бесплатного архиватора 7zip, исполняемый файл которой называется 7za.exe. Если будет использован другой архиватор, следует соответствующим образом отредактировать строку

```
%arch_path%\7z.exe u
%dmp_dir%\%curr_date%\%schema%_%curr_date%.zip
%dmp_dir%\%curr_date%\*
```

Здесь нужно будет указать имя файла консольной версии архиватора и параметры командной строки (см. документацию к программе архивации).

Предполагается, что архивы с дампами будут для надежности копироваться на сетевой ресурс, подключенный как сетевой диск (с буквой **Y:**). Предварительно этот сетевой ресурс (сетевой диск) нужно создать и подключить средствами операционной системы. Если сетевой диск будет иметь другое имя, следует соответствующим образом отредактировать строку

```
copy /y %dmp_dir%\%curr_date%\%schema%_%curr_date%.zip Y:\
```

Если копирование архива на сетевой ресурс не требуется, вышеуказанную строку нужно закомментировать, добавив в начало строки команду **REM**.

8.4.9 Общие рекомендации по резервированию БД АПК «Бастион-2»

Выполнение задачи по созданию дампа в планировщике заданий Windows следует назначать на время, когда система наименее загружена (например, в ночь).

Для создания и хранения дампов не используйте тот же диск, на котором расположены файлы базы данных СУБД. Используйте другой физический диск сервера либо аппаратное резервирование (RAID-массив). Для надежности можно организовать дополнительное хранилище дампов на другом ПК.

Рекомендуется архивировать дампы, поскольку, во-первых, так они занимают меньше дискового пространства, во-вторых, при повреждении файла архива (например, при сбое диска) факт повреждения будет установлен при распаковке из архива.

Периодически проверяйте правильность создания архивных дампов - разворачивайте схему из дампа на тестовой системе.

8.4.10 Восстановление из резервной копии

Для восстановления базы данных из резервной копии необходимо проделать следующие шаги:

1. Если необходимо заменить текущую рабочую схему, то предварительно рекомендуется сделать резервную копию текущей схемы (см. п. 8.4.5).
2. Удалить схему, которую необходимо заменить. Для этого в форме «Управление схемами БД» следует нажать кнопку «Удалить схему» (см. п.8.4.12).
3. Создать новую схему, используя имеющийся дамп (см. п.8.4.3).

8.4.11 Смена пароля пользователя БД

Для изменения пароля пользователя БД требуется:

1. Изменить собственно пароль на сервере БД;
2. Изменить параметры подключения к БД на всех компьютерах системы.

Для выполнения первой задачи необходимо в окне «Управление схемами» нажать кнопку «Сменить пароль». В появившемся окне необходимо ввести новый пароль и его подтверждение, нажать «ОК».

На всех остальных компьютерах следует отредактировать используемое подключение и активировать схему (см. 8.4.4).

> ***Внимание!*** *При установке сервера СУБД Oracle срок действия паролей пользователей СУБД ограничивается 6-ю месяцами. Вы можете самостоятельно изменить срок действия паролей средствами СУБД Oracle. Если пароль будет просрочен, то для его изменения можно запустить «Управление схемами БД» из комплекта АПК «Бастион-2». При запуске и вводе старого пароля будет выведен запрос на его изменение.*

8.4.12 Удаление схемы

Для успешного удаления схемы, к ней не должно быть активных подключений. Для удаления выбранной схемы можно нажать кнопку «Удалить схему» в основном окне модуля «Управление схемами». При наличии активных подключений к схеме будет отображено сообщение со списком компьютеров и запущенных приложений, имеющих активные подключения к схеме.

Внимание! *После удаления активной схемы АПК «Бастион-2» работать не сможет.*

Удаление схемы может потребоваться в случае, если надо заменить базу данных на импортированную из дампа.

8.4.13 Оптимизация базы данных

Для оптимизации выполнения запросов к БД предусмотрен ряд функций (доступны через выпадающее меню «Служебные операции»):

Перекомпилировать объекты с ошибками (Oracle) – если в базе данных присутствуют объекты с ошибками, то можно попробовать их перекомпилировать повторно. Повторная компиляция может дать эффект, если имели место зависимости между объектами. Рекомендуется пробовать выполнять перекомпиляцию до тех пор, пока число объектов с ошибками не перестанет уменьшаться.

Переиндексировать данные – используется для пересоздания всех индексов в БД. Используется для ускорения работы системы в дальнейшем.

Собрать статистику – используется для оптимизации скорости выполнения запросов к БД. Рекомендуется выполнять эту операцию не реже 1 раза в 3 месяца.

Также, для Oracle можно задать параметры регулярного обслуживания БД. Для этого выберите пункт меню «*Регулярное обслуживание БД*». В открывшейся форме можно задать регулярно выполняемые операции (индексировать данные, собирать статистику), а также время и периодичность их выполнения (каждую неделю или каждый месяц, указывается день недели или месяца). В этой же форме необходимо указать пароль пользователя (схемы).

8.4.14 Устранение проблемы превышения размеров файла базы данных

При превышении размеров базы данных порога в 32 гигабайта для платной версии Oracle могут возникнуть ошибки "ORA-01691: unable to extend lob segment", "ORA-01653: unable to extend table", "ORA-01654: unable to extend index" и т. п. Эта ошибка вызвана тем, что при настройках по-умолчанию в базе данных добавлен только один файл данных, максимальный размер которого равен 32 гигабайтам. Для устранения, либо предупреждения данной проблемы необходимо в утилите «Управление схемами БД» запустить служебную операцию "Добавить файл данных".

8.4.15 Удаление устаревших данных

8.4.15.1 Задачи и инструменты удаления устаревших данных

АПК «Бастион-2» собирает и протоколирует множество данных, а именно:

- Журнал событий системы. Все события от устройств АПК «Бастион-2», все действия операторов и системные события хранятся здесь.

- Журнал учёта рабочего времени. События входов / выходов сотрудников в области контроля, для которых включен учёт рабочего времени, дополнительно хранятся в отдельном журнале. Этот журнал ведётся, только если включена подсистема учёта рабочего времени.

- Журналы аудита хранят историю изменений данных системы. Протоколируются изменения персональных данных, устройств, пропусков, операторов, рабочих станций, справочников, карт доступа, уровней доступа, транспортных средств и транспортных пропусков. Эти журналы ведутся только в случае использования модуля «Бастион-2 – Аудит» и при включённой настройке «Включить протоколирование» на странице «Бастион-Аудит» в «Общих настройках системы».

Поэтому, с течением времени, размер целого ряда таблиц базы данных может значительно увеличиваться. Скорость увеличения объёма хранимых данных зависит от множества факторов, таких как:

- Интенсивность событий в системе;

- Настройки протоколирования и системы аудита;

- Количество пропусков и интенсивность их изменений.

В любом случае, для оптимизации производительности системы рекомендуется периодически удалять устаревшие данные из системы, даже при использовании версий СУБД без ограничений на размер БД.

> ***Внимание!*** *При использовании в качестве СУБД Oracle 11g Express Edition следует иметь в виду, что в этой БД есть ограничение на размер базы данных в 11 Гб. После достижения этого размера БД, система не сможет работать. Наличие такого ограничения не позволит выполнить требования к глубине хранения архивов в рабочей базе данных при использовании СУБД Oracle 11g Express Edition.*

В системе предусмотрено несколько способов удаления устаревших данных:

- Ручное удаление устаревших данных из журнала событий системы с помощью утилиты «Управление схемами БД».

- Периодическое удаление устаревших данных, задаваемое в «Общих настройках» системы.

- Автоматическое удаление устаревших данных с помощью специальной «утилиты автоматической очистки».

Все эти способы и их особенности будут рассмотрены далее.

8.4.15.2 Ручное удаление устаревших данных

Самый простой способ удаления устаревших данных *журнала событий* предоставляет утилита «Управление схемами БД». Рекомендуется использовать этот способ для разовых операций, когда необходимо в срочном порядке выполнить очистку (например, в случае переполнения БД при использовании Oracle 11g Express Edition).

Для выполнения очистки этим способом можно в модуле «Управление схемами БД» выбрать из меню «Служебные операции» пункт «Удаление устаревших данных». В появившемся окне будет выведено общее число событий, которые на текущий момент сохранены в БД. Здесь можно выбрать, за какой промежуток времени оставить события в журнале (1 неделя (7 дней), 1 месяц (30 дней), 2 месяца (60 дней), 3 месяца (90 дней), 6 месяцев, 1 год, 2 года, 3 года). После этого следует нажать кнопку «Выполнить очистку журнала». Система покажет, сколько событий будет удалено, после чего будет выполнена очистка. Очистка может занять длительное время.

Также, эта операция пересоздаёт индексы таблиц журнала событий. Не рекомендуется выполнять операцию удаления устаревших данных при активной работе системы (при наличии интенсивного потока событий).

8.4.15.3 Периодическое удаление устаревших данных

Система предоставляет возможность создать расписание периодического удаления устаревших данных (только для СУБД Oracle). Это можно сделать в «Общих настройках» системы, на странице «Удаление устаревших данных» (Рис. 73).

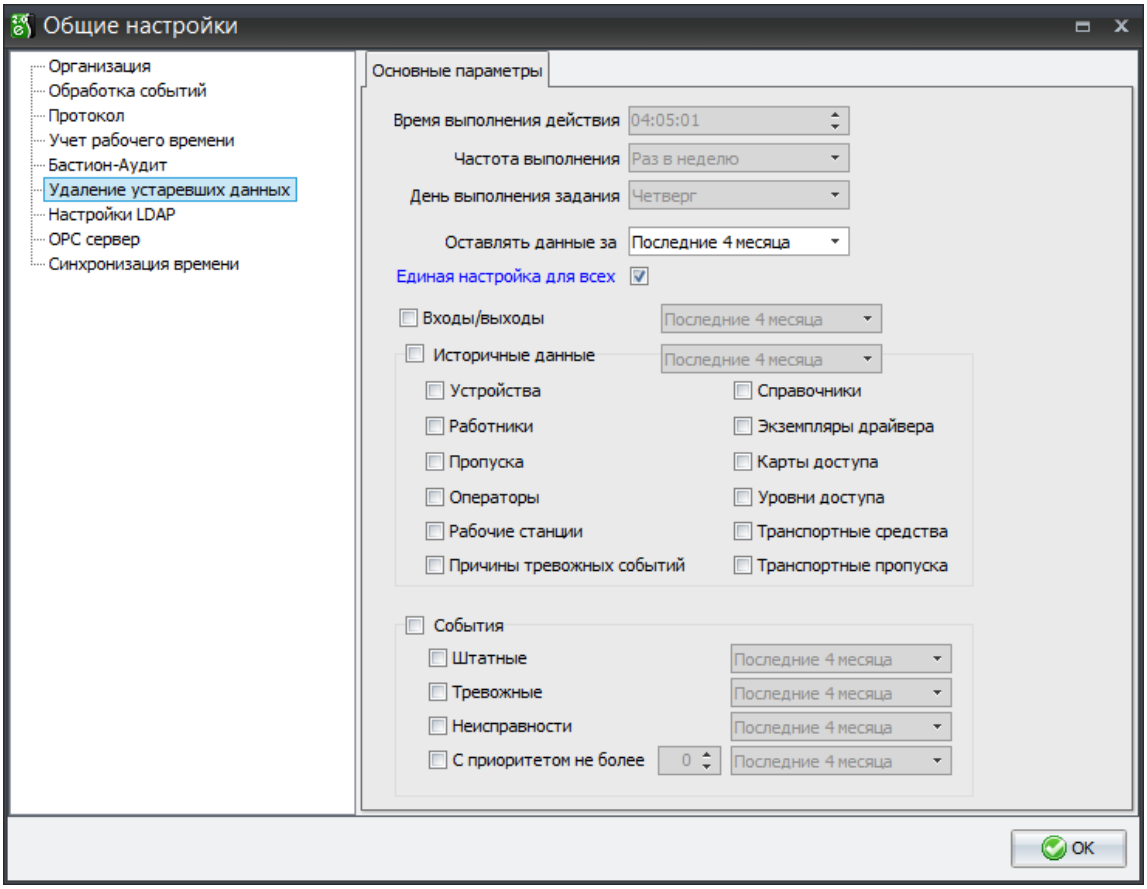

Рис. 73. Настройка периодического удаления устаревших данных

Рассматриваемая система очистки БД не выгружает удаляемые данные, а также не пересоздаёт индексы после удаления данных. Поэтому, рекомендуется использовать этот способ удаления устаревших данных при использовании платных версий СУБД Oracle без ограничения на размер базы данных.

Назначение и рекомендации по применению основных параметров приведены в таблице ниже:

Параметр	Назначение	Рекомендации
Время выполнения действия	Позволяет указать время, в которое будут выполняться операции очистки БД	Рекомендуется указать время наименьшей нагрузки на систему. Как правило, это ночное время. Следует иметь в виду, что очистка может занять продолжительное время.
Частота выполнения	Позволяет указать, с какой частотой будет проводиться очистка БД. Возможные варианты: раз в неделю, раз в месяц, раз в 2 месяца, раз в 3 месяца.	Если нет дополнительных условий, рекомендуется выполнять очистку раз в неделю. Это позволит сократить время операции очистки.
День выполнения задания	Позволяет указать, в какой день будет производиться очистка. Если периодичность указана в месяцах – можно выбрать первый или последний день месяца. Если в неделях – можно указать день недели.	Рекомендуется указывать день с наименьшей нагрузкой на систему, выходной.
Оставлять данные за	Позволяет указать, данные за какой период должны оставаться в БД после очистки. Можно выбрать от 1 месяца до 3-х лет.	Необходимо подбирать этот параметр с учётом требований по глубине хранения архивов. Система не может гарантировать глубину хранения архива при использовании версий СУБД с ограниченным размером табличного пространства (Oracle 11g Express Edition).
Флаг «Единая настройка для всех»	Позволяет указать, что система будет применять единые настройки по глубине хранения всех журналов.	Рекомендуется включить единые настройки для всех, если нет специфических требований по глубине хранения разных журналов.
Флаг «Входы / выходы»	Позволяет включить / выключить очистку журналов УРВ.	Рекомендуется включить при использовании системы УРВ.
Группа флагов «Историчные данные»	Позволяет включить / выключить очистку журналов аудита (истории изменения данных).	Рекомендуется включить все флаги группы при использовании системы аудита (модуль «Бастион-2 – Аудит», включена настройка «Включить протоколирование» на странице

		«Бастион-Аудит» в общих настройках).
Группа флагов «События»	Позволяет включить / выключить очистку журналов событий системы.	Рекомендуется включить флаги для всех типов событий (Штатные, Тревожные, Неисправности). При необходимости можно оставлять наиболее приоритетные события, указав максимальный приоритет удаляемых событий с помощью флага «С приоритетом не более».

8.4.15.4 Использование утилиты автоматической очистки

Для бесплатной версии Oracle 11g Express Edition с ограничением размера табличного пространства в 11 Гб, существует специальная утилита для удаления устаревших данных.

Утилита выполняет постоянный мониторинг наполненности табличного пространства. В случае превышения указанного порога наполненности выдаётся предупреждение и в указанное в настройках время выполняется очистка устаревших данных.

Также, утилита позволяет перед выполнением очистки выгрузить удаляемые данные в файл формата CSV.

Эта утилита поставляется отдельно от АПК «Бастион-2».

Рекомендуется использовать этот способ удаления устаревших данных при использовании Oracle 11g Express Edition согранничением на размер базы данных.

Более подробно о настройке и работе с этой утилитой можно прочитать в руководстве на её использование.

8.4.16 Анализ размера БД

Для просмотра информации о размере БД можно выбрать из меню «Служебные операции» пункт «Статистика размера БД». В появившемся окне (Рис. 74) будет выведена информации о всех табличных пространствах БД (их полный размер, используемое и свободное место), так же информации о размерах объектов текущей выбранной схемы.

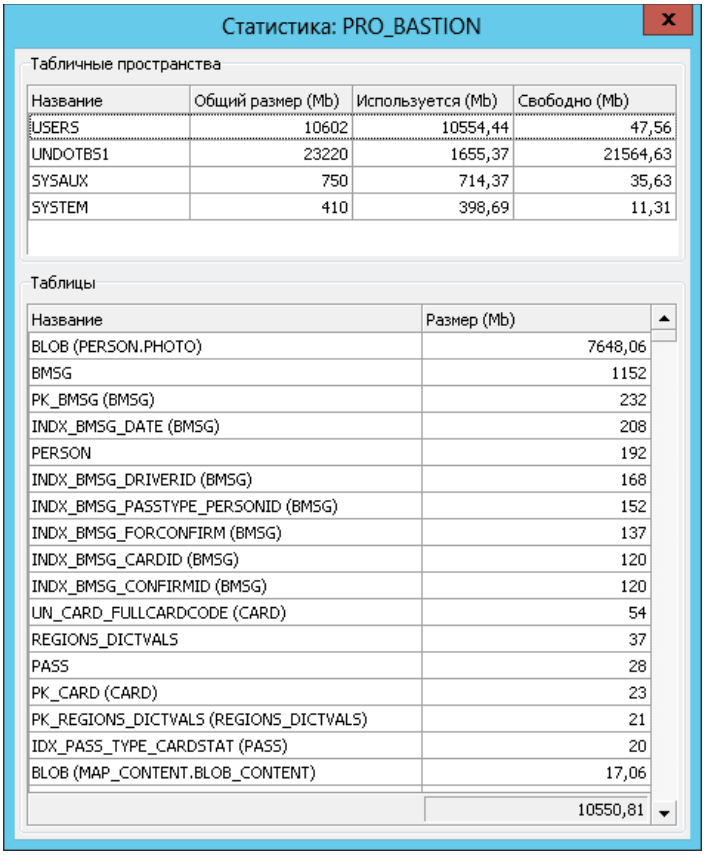

Рис. 74 Информация о размере БД

8.4.17 Смена сервера системы

В случае, если у сервера системы изменился IP адрес, используемый в настройках подключения, необходимо изменить адрес сервера системы **на всех рабочих станциях** с помощью утилиты «Настройка подключений». Для этого нужно изменить параметры текущей схемы (см. пункт 8.4.4). При этом требуется перезапуск всех клиентских приложений.

Если же было изменено имя компьютера сервера системы, то нужно убедиться в правильности настроек подключения на всех рабочих станциях, а также проверить настройки сервера системы в форме «Сеть» АПК «Бастион-2» и при необходимости изменить имя компьютера для соответствующей записи.

8.4.18 Обновление схемы

В случае обновления версии АПК «Бастион-2» требуется обновление соответствующей схемы Oracle или БД PostgreSQL с помощью скриптов обновления, поставляемых в пакете инсталляции. Для этого следует нажать на кнопку «Обновить схему» в основном окне модуля «Управление схемами». Откроется окно, приведённое на рисунке 75.

Внимание! *Перед обновлением схемы необходимо остановить службу BAgentSvc на сервере системы!*

Модуль обновления автоматически определяет текущую версию базы данных и предлагает обновиться по последней возможной. Для запуска процедуры обновления следует ввести пароль текущей схемы АПК «Бастион-2» и нажать на кнопку «ОК».

Внимание! *Обновление схемы следует производить непосредственно на сервере базы данных!*

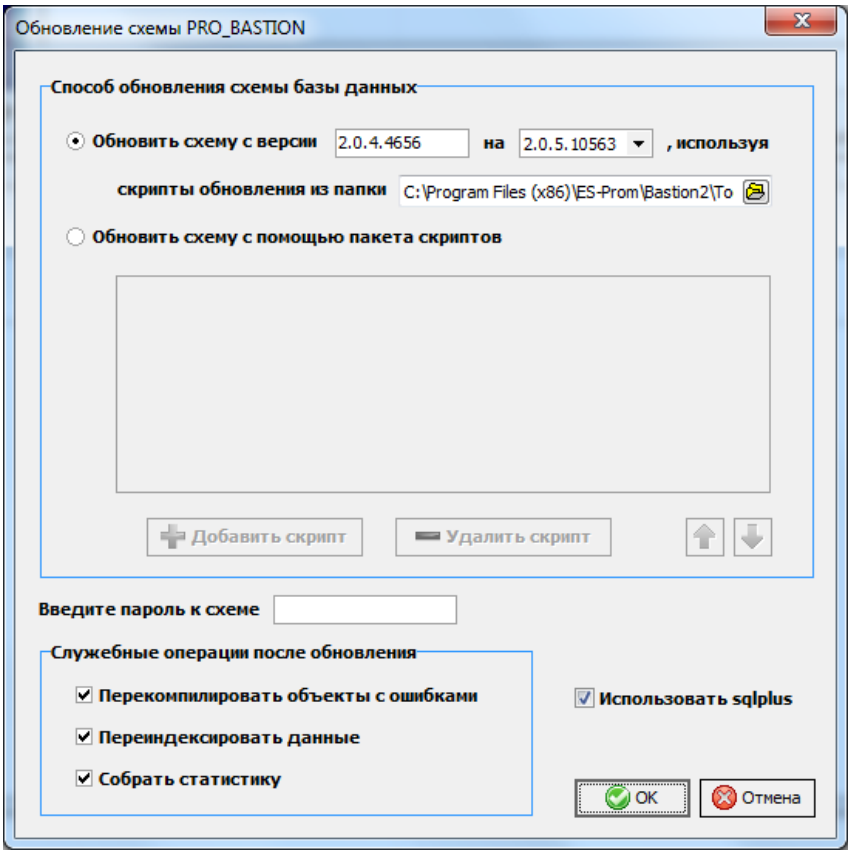

Рис. 75 Форма обновления схемы БД

8.4.19 Администрирование БД Oracle при помощи Oracle SQL Developer

8.4.19.1 Подключение к базе данных с помощью Oracle SQL Developer

На установочном диске АПК «Бастион-2» поставляется бесплатная утилита для администрирования баз данных Oracle SQL Developer (папка Redist\Oracle SQL Developer).

Для установки Oracle SQL Developer достаточно распаковать архив из указанной выше папки на диск (например, в папку c:\sqldeveloper).

Для работы утилиты необходим также установленный пакет Java Development Kit (JDK) 7. Установщики этого пакета для Windows x86 и x64 находятся в той же папке на установочном диске АПК «Бастион-2». Запустите требуемый установщик и следуйте его указаниям.

Для установки соединения с базой данных АПК «Бастион-2» из Oracle SQL Developer, необходимо произвести следующие настройки:

1. Указать используемого клиента Oracle. Для этого в Oracle SQL Developer необходимо выбрать пункт меню Tools – Preferences… и на закладке «Database – Advanced» поставить флаг «Use Oracle Client» и указать путь к клиенту, устанавливаемому вместе с АПК «Бастион-2» (Рис. 76).

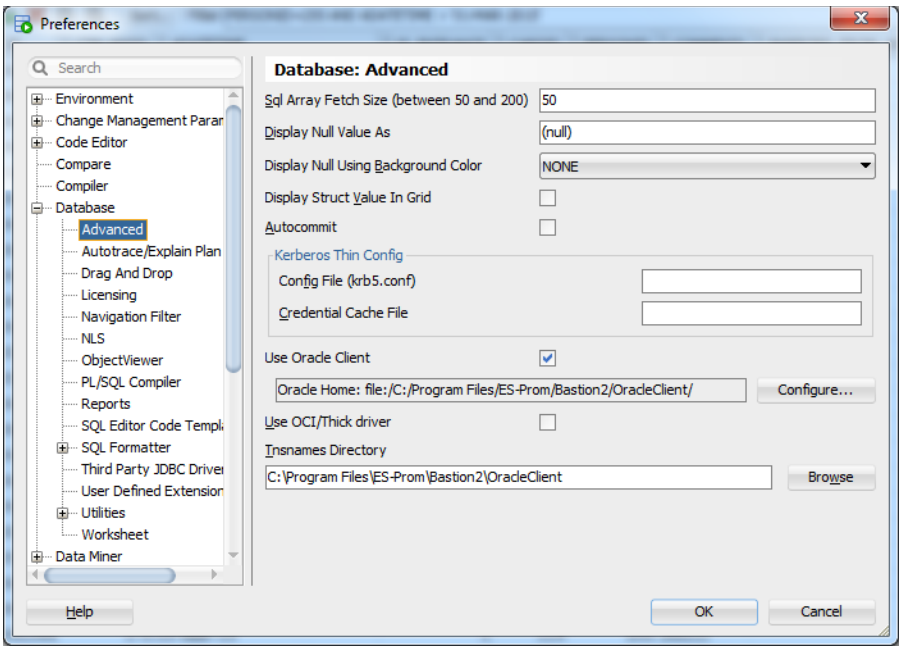

Рис. 76. Выбор клиента Oracle для использования в Oracle SQL Developer

2. На странице «Database – NLS» указать параметры для используемого языка (Language, Data Language, Territory), как показано на Рис. 77. Это равносильно внесению следующих записей в файл конфигурации Oracle SQL Developer (<sqldeveloper>\bin\ide\ide.conf): `AddVMOption -Duser.language=en` `AddVMOption -Duser.region=us`

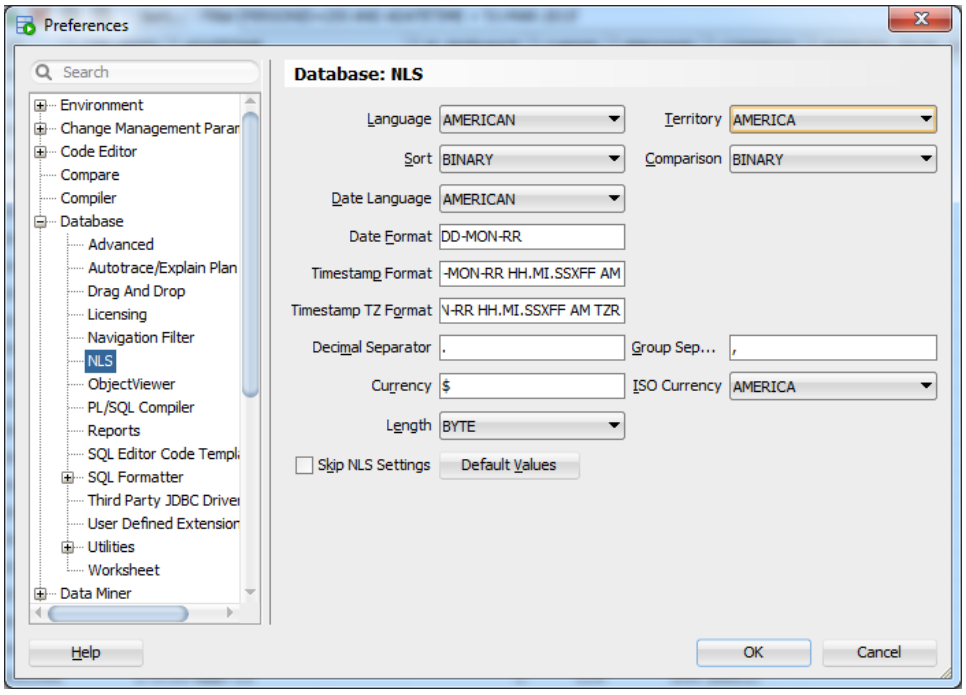

Рис. 77. Установка языковых параметров Oracle SQL Developer

3. Создать новое соединение с базой данных. В форме создания соединения выбрать Connection Type – TNS и Network Alias, соответствующий БД АПК «Бастион-2». Указать произвольное имя соединения (Connection Name), имя пользователя и пароль для подключения к БД (Рис. 78).

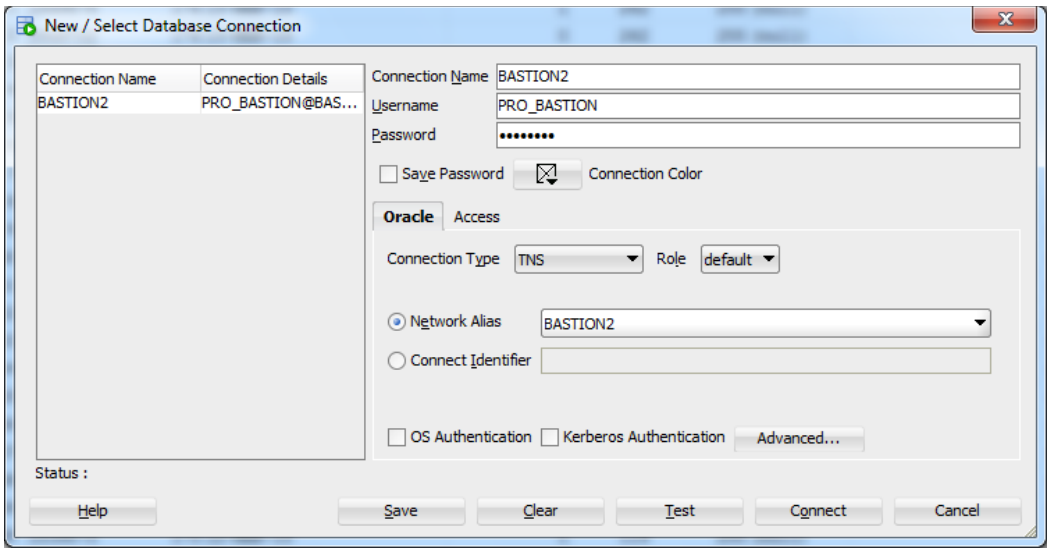

Рис. 78. Создание нового соединения с базой данных АПК «Бастион-2»

После выполнения указанных действий можно нажать кнопку Test для проверки соединения. В любом случае, рекомендуется нажать кнопку Save для сохранения соединения, чтобы иметь возможность использовать и редактировать его в дальнейшем.

8.4.19.2 Выполнение основных операций в Oracle SQL Developer

С помощью Oracle SQL Developer можно выполнять множество операций. Полное их рассмотрение выходит за рамки этого руководства. Здесь будут рассмотрены только базовые операции:

- Выполнение запросов к БД;
- Просмотр содержимого таблиц БД;
- Просмотр структуры таблиц, а также прочих объектов БД;
- Экспорт данных, в том числе для Microsoft Excel.

Для выполнения запроса к БД выберите пункт меню «Tools – SQL Worksheet» (также можно нажать Alt + F10) и укажите используемое соединение. На странице Worksheet введите текст SQL-запроса и нажмите кнопку Run Statement (Ctrl + Enter).

Для просмотра содержимого таблиц БД раскройте соединение в дереве слева, выберите нужную таблицу из списка и перейдите на страницу Data.

Для просмотра структуры таблиц или кода любых других объектов БД, выберите требуемый объект в дереве соединений слева.

Для экспорта данных из таблиц в формате Excel щелкните правой кнопкой мыши по таблице в дереве соединений и выберите пункт меню «Export…». В появившемся окне (Рис. 79) установите флаг Export Data, чтобы экспортировать содержимое таблицы и снимите флаг Export DDL. Выберите формат excel 2003+ (xlsx). Укажите имя файла. Нажмите Next.

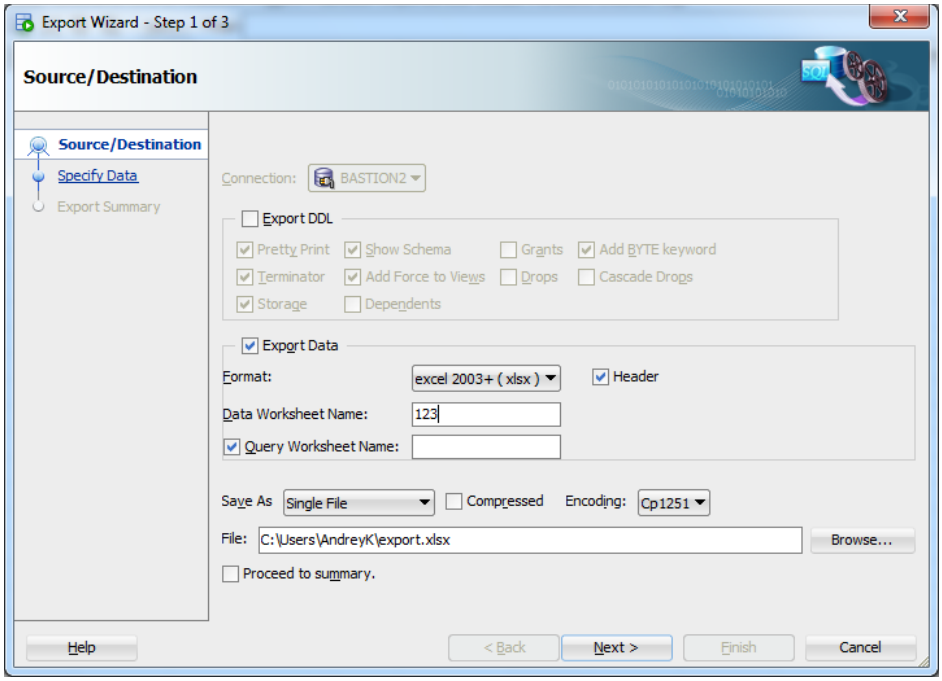

Рис. 79. Установка параметров экспорта данных в Oracle SQL Developer

На следующей странице можно выбрать данные, которые требуется экспортировать. Фильтр на экспортируемые данные можно указать как выражение SQL WHERE в колонке Object Where (Рис. 80).

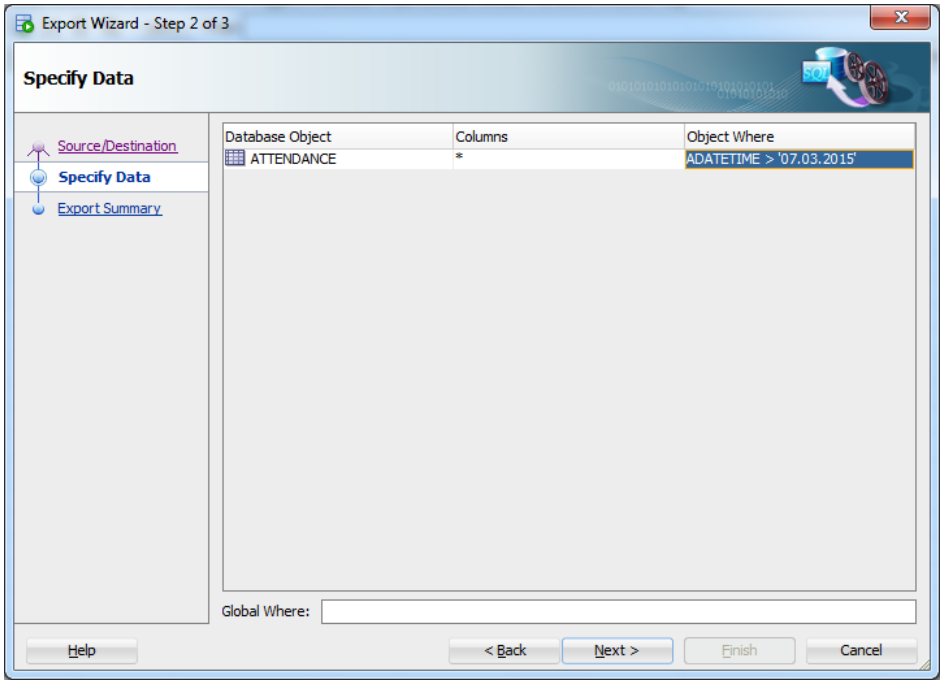

Рис. 80. Настройка фильтра данных при экспорте в Oracle SQL Developer

Подробные инструкции на утилиту Oracle SQL Developer находятся на установочном диске АПК «Бастион-2» в папке Redist\Oracle SQL Developer.

8.4.20 Администрирование БД PostgreSQL при помощи pgAdmin 4

8.4.20.1 Настройка pgAdmin 4

В установочном комплекте АПК «Бастион-2» поставляется бесплатная утилита для администрирования баз данных pgAdmin 4 (папка Redist\pgAdmin4).

Для установки pgAdmin 4 достаточно запустить установщик и следовать его указаниям. Следует иметь в виду, что pgAdmin 4 работает в браузере.

Для русификации интерфейса pgAdmin, после его установки, откройте пункт меню File - Preferences - Miscellaneous - User language, выберите Russian и перезапустите программу.

Для установки соединения с базой данных АПК «Бастион-2» из pgAdmin 4, необходимо добавить сервер PostgreSQL, к которому необходимо подсоединиться, в список Servers. Для этого следует нажать ссылку «Добавить новый сервер». В появившемся окне требуется ввести имя сервера (будет отображаться в списке), а также параметры соединения (на странице «Соединение»):

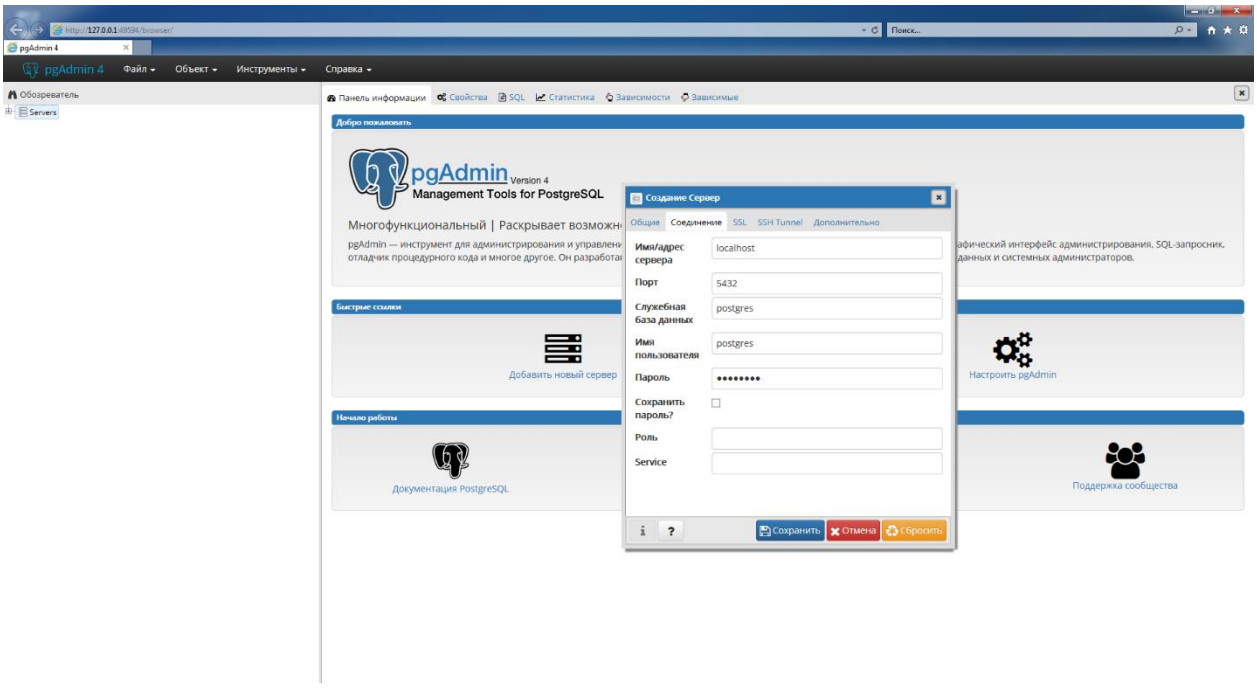

Рис. 81 Параметры соединения с сервером PostgreSQL в pgAdmin

8.4.20.2 Выполнение основных операций в pgAdmin 4

С помощью pgAdmin 4 можно выполнять множество операций. Полное их рассмотрение выходит за рамки этого руководства. Здесь будут рассмотрены только базовые операции:

- Выполнение запросов к БД;
- Просмотр содержимого таблиц БД;
- Просмотр структуры таблиц, а также прочих объектов БД;
- Экспорт данных, в том числе для Microsoft Excel.

Для выполнения запроса откройте необходимую БД и выберите пункт меню «Инструменты – Запросник». В верхнем поле введите текст SQL-запроса и нажмите кнопку Execute/Refresh (F5).

Для просмотра содержимого таблиц БД раскройте соединение в дереве слева, выберите нужную таблицу из списка, щелкните по ней правой кнопкой мыши и из контекстного меню выберите пункт «Просмотр/редактирование данных – Все строки».

Для просмотра структуры таблиц или кода любых других объектов БД, выберите требуемый объект в обозревателе слева.

Для экспорта данных из таблиц в формате CSV щелкните правой кнопкой мыши по таблице в обозревателе и выберите пункт меню «Импорт/Экспорт…». В появившемся окне (Рис. 82) укажите имя файла, выберите формат csv и укажите кодировку для файла.

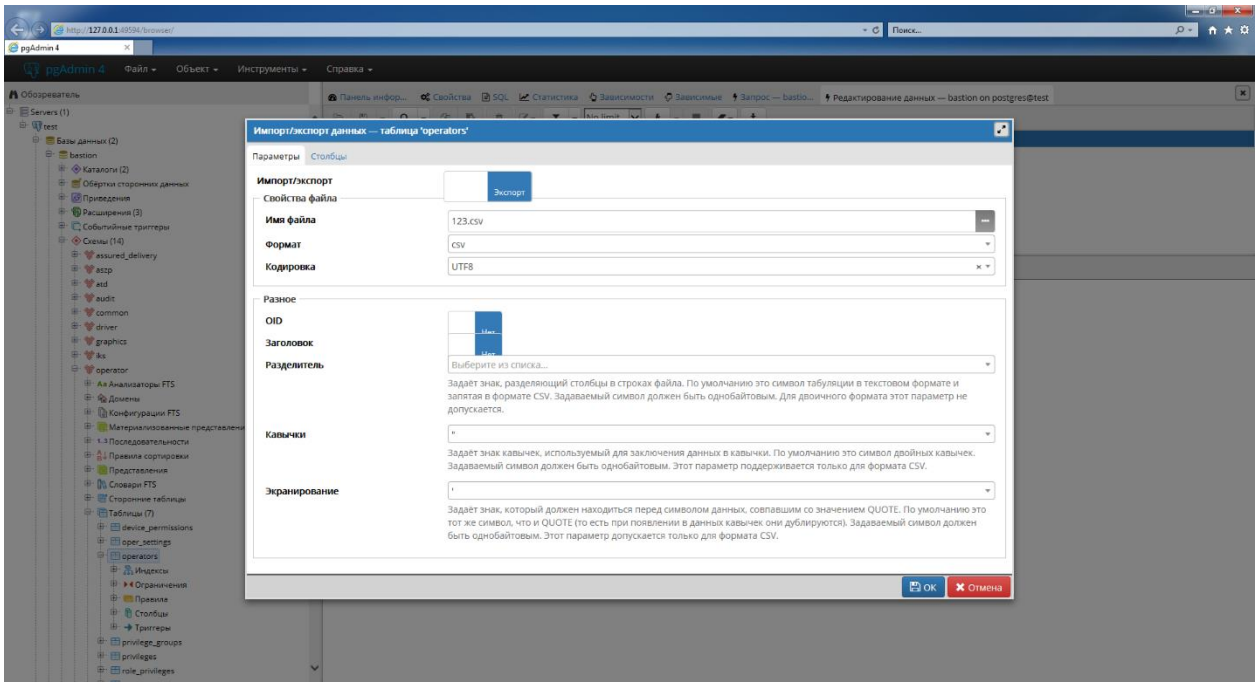

Рис. 82. Установка параметров экспорта данных в pgAdmin 4

На второй странице можно выбрать столбцы, которые требуется экспортировать (Рис. 83).

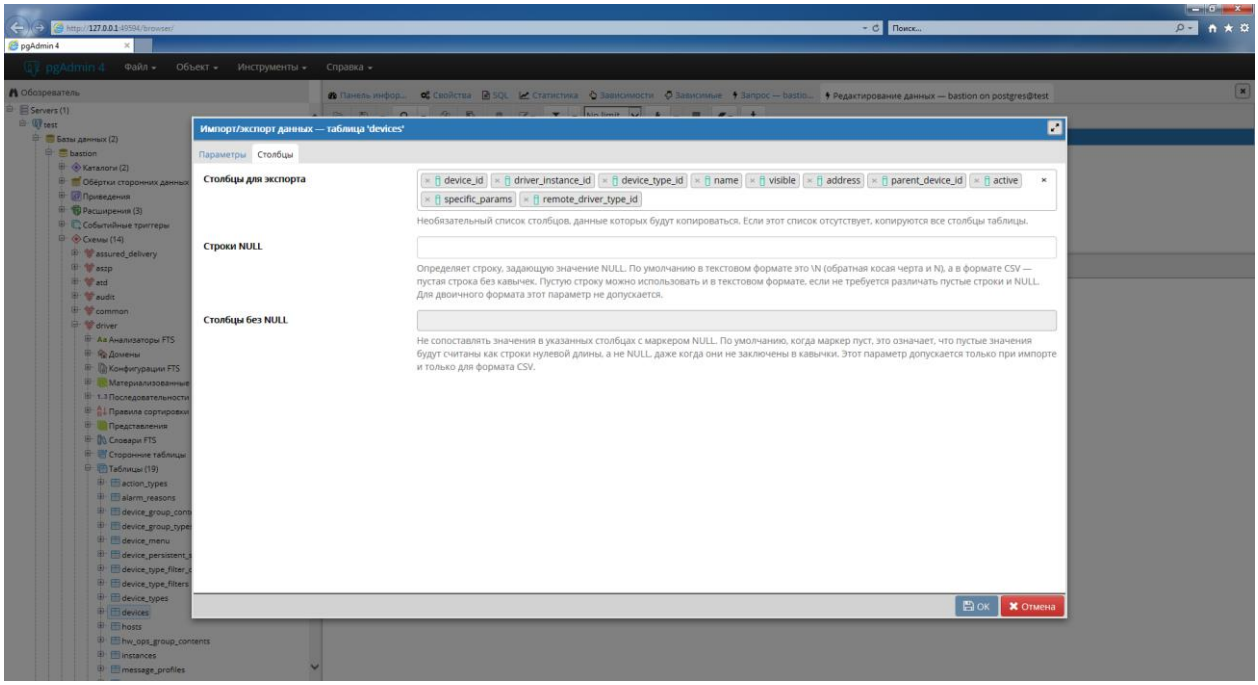

Рис. 83. Настройка столбцов при экспорте в pgAdmin 4

Для просмотра подробных инструкции на утилиту pgAdmin следует выбрать пункт главного меню «Справка – Веб-справка».