«Бастион-3». Руководство администратора

Версия 2025.1

(23.12.2024)

Самара, 2025

Оглавление

1. Общие сведения

1.1. Назначение этого документа

Этот документ предназначен для инсталляторов «Бастион-3», 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.

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 ОС;
- Администрирование PostgreSQL (в зависимости от версии ПК «Бастион-3»).

1.2. Назначение и область применения системы

Программный комплекс **(ПК) «Бастион-3»** 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).

ПК «Бастион-3» позволяет создавать единую систему безопасности объекта с возможностью объединенного мониторинга, управления подсистемами и их автоматической взаимосвязью.

ПК «Бастион-3» обладает распределенной архитектурой, что позволяет использовать его одинаково эффективно на объектах разного масштаба: от небольших офисов до крупных предприятий с развитой филиальной сетью.

ПК «Бастион-3» 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.

ПК «Бастион-3» 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 ПК «Бастион-3» можно объединить, используя системы «Бастион-3 – Репликация» и «Бастион-3 – ПЦН». При этом каждый объект будет работать со своей базой данных ПК «Бастион-3».

1.3. Общая структура системы

Компьютерная сеть ПК «Бастион-3» включает в себя следующие функциональные узлы (см. Рис. 1):

Сервер баз данных (БД). Отвечает за хранение всей информации о конфигурации системы и журнала событий системы. Реализуется на базе СУБД с открытым исходным кодом PostgreSQL, а также отечественных продуктах PostgresPro или Jatoba.

Сервер системы – центральный модуль системы, всегда один на систему. Выполняет функции, обеспечивающие взаимодействие модулей системы, реализацию правил бизнес-логики, проверки лицензий, управления выполнением сценариев и реакций на события, проверку прав доступа, запуск модулей расширения и ряд других системных функций.

Модули расширения сервера системы обеспечивают широкий набор дополнительного функционала – это модули «Бастион-3 – Репликация», «Бастион-3 – ПЦН», «Бастион-3 – OPC UA Сервер», «Бастион-3 – SNMP Агент», «Бастион-3 – LDAP», «Бастион-3 – МТП». Набор этих модулей постоянно расширяется.

Серверы оборудования – один или несколько компьютеров (не ограничено программным способом), к которым выполняется подключение подсистем безопасности с использованием *драйверов (модулей интеграции)*. Число драйверов, обслуживаемых каждым сервером оборудования, ограничивается только производительностью этого сервера и ограничениями самого драйвера.

Клиентские приложения. Неограниченное число рабочих мест, на которых возможно выполнение различных клиентских приложений («Пост охраны», «Бюро пропусков» и др.) без подключенного оборудования.

Мобильные и веб-приложения. Неограниченное число таких приложений может подключаться к серверу системы по интернет-протоколам.

Несколько территориально распределенных объектов с ПК «Бастион-3» могут объединяться с использованием систем «Бастион-3 – Репликация» и «Бастион-3 – ПЦН». При этом каждый объект работает со своей базой данных ПК «Бастион-3».

ПК «Бастион-3» может взаимодействовать с внешними системами через различные интеграционные модули.

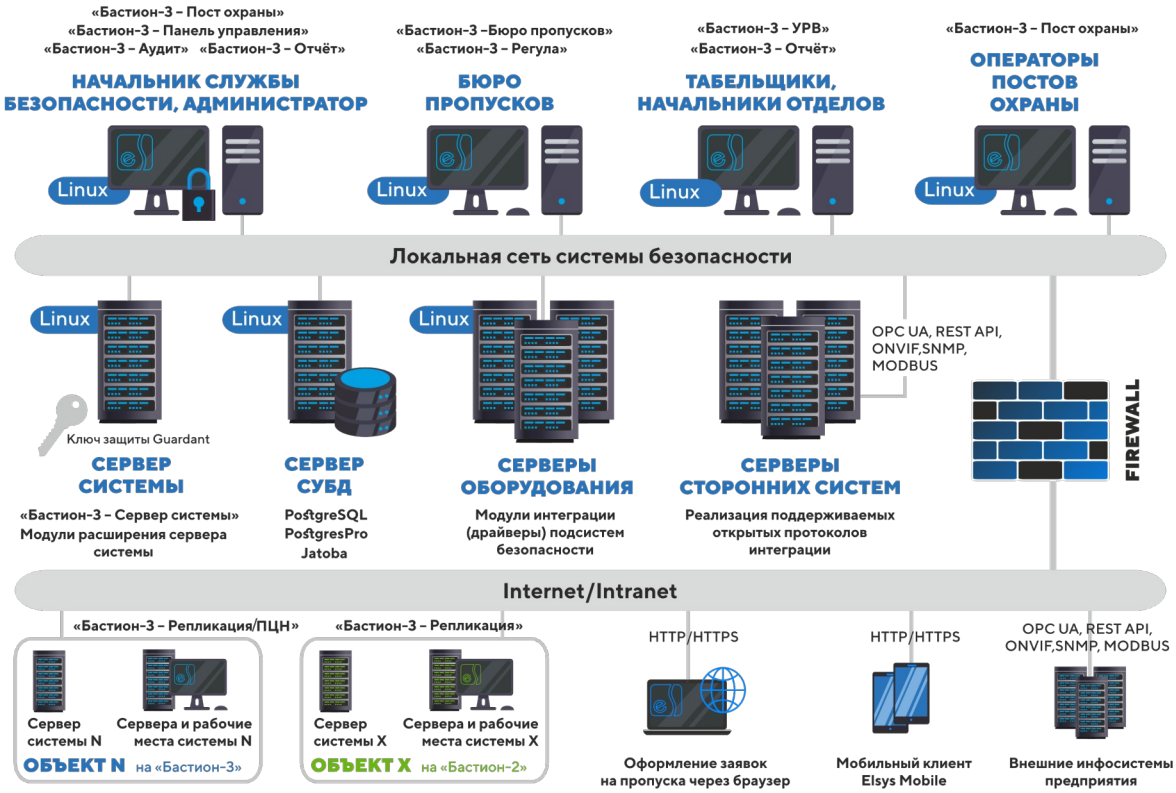

Рис. 1. Структура сети ПК «Бастион-3»

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

Сеть ПК «Бастион-3» построена на основе протокола TCP/IP.

ПК «Бастион-3» структурно разделяется на четыре основные группы: сервер системы и модули его расширения, серверы оборудования и драйверы (модули интеграции), клиентские приложения и дополнительные программные модули. Информация о возможности использования модулей и драйверов, а также об исполнениях каждого модуля, находится в ключе защиты, устанавливаемом на сервере системы. Допускается использование нескольких ключей защиты в одной системе.

ПК «Бастион-3» построен на основе трёхзвенной архитектуры. Клиентские приложения не обращаются напрямую к БД, а всегда работают через сервер системы.

1.4. Взаимосвязи с другими системами

1.4.1. Объединение нескольких ПК «Бастион-3»

Для объединения нескольких объектов под управлением ПК «Бастион-3» используются модули «Бастион-3 – Репликация» и «Бастион-3 – ПЦН».

Система «Бастион-3 – ПЦН» предназначена для централизованного мониторинга объектов, оснащённых ПК «Бастион-3».

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.

Внимание! *Модуль «Бастион-3 – ПЦН» не совместим с модулем «Бастион-2 – ПЦН». Использование в одной системе клиентов от АПК «Бастион-2» и ПК «Бастион-3» не допускается.*

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-3 – Репликация» предназначена для синхронизации списка пропусков между филиалами организации, оснащёнными ПК «Бастион-3».

Внимание! *Модуль «Бастион-3 – Репликация» совместим с модулем «Бастион-2 – Репликация». Допускается подключение филиалов от АПК «Бастион-2» к ПК «Бастион-3» с центром репликации на базе «Бастион-3 – Репликация».*

Модули «Бастион-3 – ПЦН» и «Бастион-3 – Репликация» могут использоваться совместно для обеспечения взаимодействия филиалов организации.

1.4.2. Интеграция с внешними системами обработки событий

ПК «Бастион-3» может быть интегрирован с внешними системами обработки событий с помощью следующих модулей:

- «Бастион-3 – OPC UA сервер»;
- «Бастион-3 – SNMP агент»;
- «Бастион-3 – CC ТМК».

Модули «Бастион-3 – OPC UA сервер» и «Бастион-3 – SNMP агент» реализуют идентичный функционал:

- Получение списка устройств ПК «Бастион-3»;
- Получение событий ПК «Бастион-3»;
- Получение состояний устройств ПК «Бастион-3»;
- Управление устройствами ПК «Бастион-3».

Модуль «Бастион-3 – OPC UA сервер» поддерживает работу по протоколам OPC.TCP и HTTPS.

Модуль «Бастион-3 – SNMP агент» поддерживает протоколы SMNP v1, v2 и v3.

Модуль «Бастион-3 – СС ТМК» предназначен для подключения ПК «Бастион-3» к системе сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры (СС ТМК).

Основной функцией модуля является формирование и передача событий от ПК «Бастион-3» к СС ТМК. В СС ТМК передаются события от следующих подсистем ПК «Бастион-3»:

- 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, модуль предоставляет возможность вручную определить, какие события ПК «Бастион-3» 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-3 – 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-3 – ИКС» предоставляет API для интеграции и не содержит готовых конфигураций для каких-либо внешних систем.

Модуль «Бастион-3 – ИКС» позволяет интегрировать:

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

Модуль решает следующие задачи:

- Передача в ПК «Бастион-3» заявок на пропуска из внешней системы с возможностью указания прав доступа для СКУД и номера карты доступа;
- Передача в ПК «Бастион-3» 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 ПК «Бастион-3» во внешнюю систему информации о персонах, персональных пропусках, транспортных пропуска, материальных пропусках, точках прохода, подразделениях, должностях и о других справочниках, доступных в ПК «Бастион-3»;

- Получение из ПК «Бастион-3» во внешнюю систему информации о последнем месте предъявления пропуска;
- Получение из ПК «Бастион-3» во внешнюю систему списка событий по заданному пропуску;
- Получение из ПК «Бастион-3» во внешнюю систему исходных данных для расчета отработанного времени (пары событий «вход-выход»).

Система поддерживает одновременную работу с несколькими ПК «Бастион-3».

1.4.4. Интеграция систем распознавания лиц

В системе предусмотрен специальный интерфейс для интеграции систем распознавания лиц – модуль «Бастион-3 – Face». Взаимодействие со внешними системами производится с использованием протокола на основе стандарта ONVIF Profile A, C. Интеграция может быть выполнена силами производителей внешней системы.

Основной функцией модуля является обеспечение доступа посетителей через точки прохода системы контроля и управления доступом (СКУД) путём сопоставления изображения лица человека, полученного с камеры видеофиксации с его фотографией, сохранённой в ПК «Бастион-3».

Модуль позволяет использовать как режим двухфакторной аутентификации (по изображению лица с прикладыванием карты доступа к считывателю), так и режим идентификации по изображению лица. Одновременно могут быть заданы различные режимы доступа для разных точек прохода.

Доступ на выбранных точках прохода возможен для посетителей с пропусками любых типов (постоянные, временные и разовые).

Дополнительно, модуль предоставляет возможность создавать *виртуальные точки прохода*.

Виртуальная точка прохода не связана с реальным преграждающим устройством, но позволяет отслеживать местоположение персонала и посетителей в зонах, контролируемых камерами видеофиксации, подключенных ко внешней системе.

1.4.5. Интеграция стороннего оборудования по стандартным протоколам

Драйвер «Бастион-3 – Modbus» предназначен для мониторинга событий и управления различными устройствами, поддерживающими протокол Modbus. Поддерживаемые Modbus-команды: 0x01, 0x02, 0x03, 0x04, 0x05, 0x06.

Оборудование подключается с помощью портов RS-232/RS-485 (протокол Modbus RTU) или Ethernet (протокол Modbus TCP). Настройка оборудования производится с помощью программного обеспечения, поставляемого производителем.

Система поддерживает до 16 одновременно работающих COM-портов, на каждом порту до 255 Modbus-устройств первого уровня (для удобства назовём их контроллерами, хотя тип не имеет значения). Параллельно драйвер обеспечивает работу до 255 Modbus-устройств, подключенных через Ethernet. В каждом устройстве поддерживается до 2047 дочерних адресных устройств. Для

каждого дочернего адресного устройства доступно до 65535 событий. Также для любых адресных устройств доступно несколько команд, зависящих от типа подключённого оборудования.

Адресные устройства могут представлять собой совместимые с оборудованием различные датчики (тепловые, оптические и т. д.), исполнительные модули, контроллеры и прочее совместимое оборудование. При этом драйвер не накладывает ограничений на тип используемых адресных устройств, предоставляя возможность выбора типа устройства в ПК «Бастион-3».

Драйвер обеспечивает:

- Индикацию потери и восстановления связи контроллеров с соответствующими событиями;
- Отображение событий от адресных устройств, включая штатные события, неисправности и тревоги;
- Цветовое отображение состояния любых устройств на графическом плане объекта;
- Настройку линии приборов в ПК «Бастион-3» с помощью общего конфигуратора;
- Возможность импорта и экспорта конфигураций в/из файла;
- Возможность выбора отдельно события и состояния устройства в зависимости от данных в Modbus-регистрах;
- Одновременный опрос устройств по Modbus RTU и Modbus TCP;
- Разграничение доступа к настройкам драйвера в зависимости от уровня полномочий оператора.

Драйвер не обеспечивает настройку аппаратных частей системы. Для настройки линий приборов следует использовать стороннее ПО, поставляемое с оборудованием.

2. Условия применения

2.1. Требования к программному обеспечению

Поддерживаемые операционные системы: Astra Linux 1.7 SE с последними оперативными обновлениями, Astra Linux 1.8 SE, RedOS 8, Red Hat Enterprise Linux 8.x, Red Hat Enterprise Linux 9.x, Windows 10, Windows 11, Windows Server 2019, Windows Server 2022 в любых исполнениях, кроме Starter, с наличием последних обновлений. Поддерживается работа только в 64-разрядных операционных системах.

Серверные компоненты системы (сервер БД, сервер системы, серверы оборудования) могут выполняться на ОС семейства Linux без установленной графической оболочки. В этом случае, для настройки локальных параметров следует использовать консольные утилиты. Следует учитывать, что некоторые драйверы (модули интеграции) могут не поддерживать работу сервера в консольном режиме.

Работа части модулей может обеспечиваться не во всех ОС. Допускается использование других версий ОС, основанных на Linux, но тестирование для этих ОС не производится. При

использовании других версий ОС возможны проблемы с конфигурацией пакетов и программной среды для ПК «Бастион-3».

Не рекомендуется использование серверных ОС Windows Server 2022, Windows Server 2019 для организации рабочих мест с видеонаблюдением или системой ввода фотографий с видеокамер. *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 ПК «Бастион-3». 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 ПК «Бастион-3» и сопутствующих модулей, так как это может привести к искажению данных и нестабильной работе приложений. При изменении региональных настроек ОС Windows необходимо перезапустить ПК «Бастион-3» и все остальные модули.

Дополнительные компоненты, необходимые для работы комплекса:

- *PostgreSQL 10 или более новый.*
- *.Net Core 8.*
- *OpenGL 2.1.*

> ***Внимание!*** *Не рекомендуется использовать в качестве СУБД PostgreSQL версий 10 и 11, так как для этих версий есть известные проблемы с производительностью некоторых операций.*
>
> ***Внимание!*** *При отключенном 3D-ускорении на компьютерах с Windows может использоваться программная реализация OpenGL 1.1. При этом, для работы ПК «Бастион-3» будет требоваться установка сторонней реализации OpenGL более новой версии, например, пакета Mesa3d.*

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 ПК «Бастион-3» (например, «Бастион-3 – Регула», «Бастион-3 – 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	Astra Linux 1.8 SE, PostgreSQL 14, CPU 2 GHz 2 Cores, 8 Gb RAM, 1000 GB HDD
Клиентские рабочие места	Astra Linux 1.8 SE, CPU 2 GHz 2 Cores, 8 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	Astra Linux 1.8 SE, PostgreSQL 14, CPU 3 GHz 4 Cores, 16Gb RAM, 1000 GB HDD
Клиентские рабочие места	Astra Linux 1.8 SE, CPU 2 GHz 2 Cores, 8 Gb RAM, 500 GB HDD

> ***Внимание!*** *Для корректной работы системы требуется наличие файла подкачки с минимальным объемом равным половине объема оперативной памяти.*

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

Видеоадаптер и монитор должны обеспечивать разрешение не ниже FullHD (1920x1080). 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.

Рекомендуется использовать источники бесперебойного питания, особенно на сервере БД. Нештатное выключение сервера БД может привести к потере пользовательских данных.

2.3. Выбор редакции СУБД

ПК «Бастион-3» поддерживает развёртывание базы данных на СУБД PostgreSQL 10 и выше. Поддерживаются 64-разрядные версии СУБД.

В большинстве случаев достаточно использовать бесплатную версию PostgreSQL.

Дополнительно, ПК «Бастион-3» 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, ПК «Бастион-3» поддерживает работу с СУБД российского производства Jatoba (разработка ООО «ГазИнформСервис»), основанной на PostgreSQL 11 и выше.

2.4. Требования к компьютерным сетям

2.4.1. Общие сведения о структуре сети

Для сетевого обмена в ПК «Бастион-3» используется протокол TCP/IP (v4).

Весь сетевой обмен между компонентами системы происходит через сервер системы. Клиенты и драйверы не соединяются напрямую между собой и с базой данных.

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 приложения 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 модуля «Пост охраны» и «Отчёт» канал связи с сервером не менее 1 Mbit/s.
- для каждого модуля «Пост охраны» с фотоидентификацией и «Бюро пропусков» – не менее 2 Mbit/s (размер фотографий должен быть не более 640x480).

Для повышения комфорта работы (быстрая загрузка приложений, быстрая работа интерфейса), 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 «Пост охраны». Приложения, активно использующие БД: «Бюро пропусков», «Отчёт», «УРВ» – 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 ПК «Бастион-3», могут работать с динамическими IP-адресами.

> ***Внимание!*** *При работе в среде Astra Linux порты, используемые службами и модулями Бастиона следует выбирать из диапазона 1024 - 65535. Порты с номерами до 1024 могут использоваться только суперпользователем.*

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

Номер порта по умолчанию	**Назначение**	**Комментарий**
5432	Порт для подключений к серверу БД PostgreSQL. Требуется открыть на сервере БД.	Настраивается средствами администрирования или при установке PostgreSQL
6300	Порт сервера системы. Требуется открыть на сервере системы.	Настраивается в модуле «Локальные настройки».
62561	Порт, используемый модулем «Бастион-3 – OPC UA сервер» при работе по протоколу OPC.TCP.	Настраивается в конфигурации модуля «Бастион-3 – OPC UA сервер».
62563	Порт, используемый модулем «Бастион-3 – OPC UA сервер» при работе по протоколу HTTPS.	Настраивается в конфигурации модуля «Бастион-3 – OPC UA сервер».
5004	Порт, используемый сервером модуля «Бастион-3 – web-заявка».	Настраивается в конфигурации модуля «Бастион-3 – web-заявка».
5005	Порт, используемый сервером модуля «Бастион-3 – ИКС».	Настраивается в конфигурации модуля «Бастион-3 – ИКС».
161	Порт, используемый модулем «Бастион-3 – SNMP сервер».	Настраивается в конфигурации модуля «Бастион-3 – SNMP сервер».
8098	Порт, используемый модулем «Бастион-3 – ПЦН сервер». Должен быть открыт только на сервере ПЦН.	Не настраивается.
5077	Порт, используемый модулем «Бастион-3 – Elsys Mobile». Должен быть открыт только на сервере оборудования, где установлен этот	Настраивается в конфигурации модуля

	модуль.	«Бастион-3 – Elsys Mobile».
8092	Порт, используемый модулем «Бастион-3 – ONVIF». Должен быть открыт только на сервере оборудования, где установлен этот модуль.	Не настраивается.
8089	Порт, используемый модулем «Бастион-3 – СС ТМК».	Настраивается в конфигурации модуля «Бастион-3 – СС ТМК»

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

Внимание! *Работа сторонних компонентов, интегрированных в ПК «Бастион-3», может накладывать дополнительные требования и ограничения к конфигурации сети. Рекомендуется ознакомиться с документацией на все используемые модули для уточнения требований.*

2.5. Использование дополнительных полномочий операторов ОС при работе системы

При штатной работе системы использование дополнительных полномочий для операторов ОС не требуется.

Дополнительные права могут требоваться в следующих случаях:

1. При установке системы. Дополнительные права могут требоваться для следующих операций:
   a) В ОС Linux – для создания служебного пользователя bastion, от имени которого выполняются службы, устанавливаемые ПК «Бастион-3» (BDriverHost, BagentSvc, BlogStorageSvc). Пользователь bastion не имеет прав на вход в систему и запуска приложений с пользовательским интерфейсом. В ОС Windows службы выполняются от системной учётной записи.
   b) Права на запись в папки установки (/opt/ES-prom, /opt/bastion3, /opt/guardant в ОС Linux, c:\Program Files\ES-Prom\Bastion3\ в ОС Windows), а также в системный реестр ОС Windows (HKEY_LOCAL_MACHINE\SOFTWARE\ES-Prom\Bastion3).
2. При запуске утилиты «Локальные настройки».
   a) Права на запись в папку установки (/opt/bastion3).
   b) Права на запись в папку хранения локальной конфигурации (/usr/share/es-prom/bastion3 в ОС Linux, c:\Users\Все пользователи\ES-prom\bastion3\ в ОС Windows).
3. При выполнении задач администрирования системы.
   a) Права на запуск и остановку служб системы, а также служб СУБД.

От имени пользователя bastion также выполняются назначенные задания формирования отчётов. Поэтому, этому пользователю могут потребоваться права на запись в папки, куда должны сохраняться сформированные отчёты.

2.6. Особенности использования системы в виртуальной среде

Если предполагается развертывание ПК «Бастион-3» в динамической виртуальной среде, следует учесть следующие особенности:

1. Для работы в динамической виртуальной среде необходимо использовать программный ключ защиты. Это необходимо обговорить на этапе размещения заказа. При этом, для активации ключа будет использоваться привязка только к постоянному идентификатору экземпляра операционной системы. Все остальные параметры системы, включая IP и MAC-адреса, CPUID, HDDID – могут произвольно меняться во время работы системы.

2.7. Особенности работы отдельных модулей системы в разных часовых поясах

Для поддержки работы системы, элементы которой располагаются в разных часовых поясах, применяются следующий правила и алгоритмы работы:

1. Часовой пояс устройства.
    1. Для каждого устройства в системе, поддерживающего установку времени, доступно задание локального часового пояса. Обычно это устройства типа «контроллер», «сервер» и т.п.
    2. Значение хранится в БД для каждого устройства.
    3. По умолчанию используется часовой пояс сервера системы.
    4. При изменении значения оно автоматически тиражируется на все дочерние устройства, для которых ранее не было задано отличное значение для локального часового пояса.
2. Время события устройства.
    1. Драйвер передаёт в ядро событие с локальным временем устройства, т.е. если время получено от устройства, то оно передаётся без преобразований, если время генерируется на сервере оборудования (например, при генерации сообщения о потере связи с устройством), то перед передачей в ядро оно будет преобразовано к локальному времени устройства.
    2. Запись события в протокол выполняется во времени сервера системы с указанием информации о локальном часовом поясе устройства.
    3. На рабочих местах «Постов охраны» отображается время клиентского рабочего места (в окнах событий, оперативном отчёте, в форме поиска персонала и др.).
3. Время, используемое драйвером при обращении к устройству (отправка команд, синхронизация).
    1. Драйвер при необходимости преобразует время при обращении к устройству с учётом информации о локальном часовом поясе устройства.
    2. Если команда для устройства содержит время, то она приходит с локальным временем хоста, на котором вызывается эта команда.

4. При формировании отчётов в приложении «Бастион-3 — Отчёт» доступны 2 столбца: «Время» и «Локальное время оборудования». В первом отображается время возникновения события в часовом поясе сервера системы. Во втором — время события в часовом поясе устройства-источника события.
5. В журнал учёта рабочего времени записывается локальное время и часовой пояс событий. Отчёты УРВ формируются по локальному времени исходных событий. При необходимости, в эти отчёты также можно вывести информацию о часовом поясе.

Внимание! *В ОС Linux для применения нового изменённого локального часового пояса, необходимо выполнить перезапуск пользовательских приложений ПК «Бастион-3».*

3. Использование ПК «Бастион-3» 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 ПК «Бастион-3» в ИСПДн

ПК «Бастион-3» может использоваться как компонент комплексной системы обработки персональных данных для ИСПДн. Для обеспечения соответствия всей системы, построенной на ПК «Бастион-3», 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 ПК «Бастион-3» и определении необходимых мер защиты ПД, следует учитывать следующие параметры конкретной системы:

- Общее число Персон, данные о которых предполагается хранить в БД ПК «Бастион-3».
- Наличие Персон, не являющихся сотрудниками Оператора ПД, данные о которых предполагается хранить в БД ПК «Бастион-3».
- Применение в ПК «Бастион-3» биометрических данных, используемых для идентификации Персон.
- Типы актуальных угроз для ИС, в соответствии с постановлением №1119.

ПК «Бастион-3» позволяет реализовать следующие меры по обработке 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 событий доступа к ПД.
6. Регистрация выдачи документов на твердую копию.
7. Регистрация событий уничтожения ПД с печатью соответствующего акта.

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 ПК «Бастион-3», без дополнительного комплекса мер не гарантирует соответствие ИС нормативным документам РФ по обработке ПД.

ПК «Бастион-3» не подлежит обязательной сертификации в системе сертификации ФСТЭК России № РОСС RU.0001.01БИ00 в качестве средства защиты информации (далее - СЗИ). Тем не менее, в ПК «Бастион-3» имеется функционал, позволяющий осуществлять аутентификацию и идентификацию пользователей 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 ПК «Бастион-3» требованиям к СЗИ. Такая оценка может производиться в форме сертификации, испытаний или приемки.

4. Инсталляция ПК «Бастион-3»

4.1. Установка программного обеспечения

4.1.1. Установка .Net Core 8

Проверить версию установленного .Net Core можно командами:

```
sudo dotnet --list-sdks
sudo dotnet --list-runtimes
```

Перед установкой .Net Core 8 рекомендуется удалить предыдущие версии .Net Core командами:

```
sudo dnf remove dotnet-* или sudo apt purge -y dotnet*.
```

В ОС Astra Linux 1.7 SE установку .Net Core 8 из внешних репозиториев можно сделать следующим образом:

1. Проверить, установлены ли пакеты ca-certificates и apt-transport-https командой:

   ```
   dpkg-query -l ca-certificates apt-transport-https
   ```

   Если не установлены – установить:

   ```
   sudo apt install ca-certificates apt-transport-https
   ```

2. Добавить ключ подписывания пакетов Microsoft в список доверенных ключей:

   ```
   wget -O - https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/microsoft.asc.gpg > /dev/null
   ```

3. Загрузить параметры репозитория Microsoft (параметры сохраняются в файле /etc/apt/sources.list.d/microsoft-prod.list):

   ```
   sudo wget https://packages.microsoft.com/config/debian/10/prod.list -O /etc/apt/sources.list.d/microsoft-prod.list
   ```

4. Обновить кэш пакетов:

   ```
   sudo apt update
   ```

5. Установить пакет:

   ```
   sudo apt install aspnetcore-runtime-8.0*
   ```

В ОС Red Hat Linux 8 для установки .Net Core следует выполнить команду:

```
sudo yum install aspnetcore-runtime-8.0* -y
```

Для проверки установленной версии .Net Core следует выполнить команду:

```
$ dotnet --info
```

В случае, если подключение к внешним репозиториям по каким-либо причинам запрещено, для установки .Net Core 8 можно использовать предварительно собранные пакеты, поставляемые вместе с ПК «Бастион-3».

Для этого необходимо установить следующие пакеты (формата deb или rpm), в том порядке, как они перечислены:

1. aspnetcore-runtime-8.0*

Deb-пакеты поставляются с электронной подписью, выданной АО «НПО РусБИТех», и позволяют запустить ПК «Бастион-3» в условиях замкнутой программной среды Astra Linux.

При возникновении проблем с установкой, рекомендуется проверить приоритеты репозиториев и убедиться, что пакеты загружаются из требуемого репозитория.

> ***Внимание!*** *В Astra Linux при установке .Net 6 из репозиториев Astra Linux появляются две переменные окружения DOTNET_ROOT = /usr/lib/dotnet/dotnet6-6.0.110 и DOTNET_BUNDLE_EXTRACT_BASE_DIR = /home/<username>/.cache/dotnet_bundle_extract. Если установить .Net 8 (из репозитория Microsoft или используя пакеты из дистрибутива ПК "Бастион-3"), предварительно не удалив .Net 6, то эти две переменные не исчезнут и не поменяют своего значения. Из-за этого после обновления до 2024.2 приложения Бастиона будут требовать полномочий sudo. Для исправления этой ситуации следует стереть значения переменных окружения DOTNET_ROOT и DOTNET_BUNDLE_EXTRACT_BASE_DIR. Для этого необходимо запустить утилиту fly-admin-env (не под sudo!) и удалить значения переменных. После этого перезапустить пользовательскую сессию.*

> ***Внимание!*** *В RedOS, если до обновления .Net 6 был установлен из репозиториев RedOS, то после последующей установки .Net 8 из комплекта поставки Бастиона 2024.2 необходимо перезапустить пользовательскую сессию, иначе для запуска приложений потребуются права sudo.*

4.1.2. Установка сервера СУБД

Перед установкой ПК «Бастион-3» убедитесь, что СУБД установлена и доступна. При установке потребуется ввести данные для подключения к экземпляру СУБД. Для развёртывания схемы БД ПК «Бастион-3» должен быть известен пароль суперпользователя СУБД.

В ОС семейства Linux СУБД PostgreSQL, как правило, установлена по умолчанию.

За инструкциями по установке конкретной версии СУБД в конкретной версии Linux обращайтесь к документации на СУБД и ОС.

Для создания БД ПК «Бастион-3» необходимо, чтобы было установлено расширение uuid-ossp. Расширение может быть установлено следующей командой при использовании rpm-пакетов:

```
sudo yum install postgresql-contrib
```

Необходимость отдельной установки этого пакета зависит от конкретной редакции СУБД и способа её установки.

Проверить наличие установленного расширения можно, выполнив sql-запрос:

```
SELECT 1 FROM pg_extension WHERE extname = 'uuid-ossp';
```

Если в результате выполнения запроса СУБД вернула строку, то дальнейшие действия не требуются. В противном случае следует выполнить sql-запрос:

```
CREATE EXTENSION "uuid-ossp";
```

4.1.3. Установка драйверов Guardant

Для работы с постоянными лицензионными ключами на сервере системы необходимо установить модуль Guardant Control Center. Актуальную версию можно загрузить с сайта производителя ключей: https://www.guardant.com/support/users/control-center/

Для установки через deb-пакет можно использовать команду:

```
sudo dpkg -i grdcontrol-*.deb
```

Для установки через rpm-пакет можно использовать команду:

```
sudo yum install grdcontrol-*.rpm
```

В ОС Windows на сервере системы для работы с ключами Guardant необходимо дополнительно установить драйверы Guardant. Актуальная версия драйверов доступна по ссылке: https://www.guardant.com/support/users/drivers/

> ***Внимание!*** *Для установки драйверов ключей Guardant в Windows 11 следует отключить систему контроля памяти ядра (Core Isolation / Изоляция ядра). При установке драйвера с этой включенной опцией происходит падение системы с невозможностью загрузки в нормальном режиме. Чтобы выключить эту опцию зайдите в панель управления Windows 11 и выберите «Конфиденциальность и защита — Безопасность Windows — Безопасность устройства — Изоляция ядра — Сведения об изоляции ядра» и отключите опцию «Целостность памяти».*

4.1.4. 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\XX\data в Windows, и /etc/postgresql/XX/main в Linux (XX – версия СУБД). Редактировать файлы можно в программе «Блокнот» в Windows, и в текстовом редакторе с правами администратора в Linux (например Kate). 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\XX\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\XX\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 ПК «Бастион-3» в папке …\PostgreSQL\ConfigSamples находятся примеры готовых конфигурационных файлов для СУБД PostgreSQL версий 10 и 11.

После изменения конфигурации необходимо перезапустить сервер СУБД.

4.1.5. Установка ПК «Бастион-3»

4.1.5.1. Установка ПК «Бастион-3» в Windows

Рекомендуется в первую очередь выполнять установку на том компьютере, с которого будет разворачиваться схема базы данных ПК «Бастион-3». До развёртывания схемы работа системы будет невозможна.

Для проведения установки необходимо обладать правами администратора ОС.

Запустите программу установки ПК «Бастион-3». В процессе установки необходимо ответить на ряд вопросов.

Для работы ПК «Бастион-3» требуется наличие Microsoft .Net Core 8. Если этот компонент не установлен, то программа инсталляции запустит его установку. По окончании установки Microsoft .Net Core 8 может потребоваться перезагрузить компьютер. После перезагрузки установка ПК «Бастион-3» продолжится.

Для установки ПК «Бастион-3» требуется принять лицензионное соглашение ПК «Бастион-3».

На следующем этапе программа установки предложит выбрать папку установки ПК «Бастион-3».

> ***Внимание!*** *Общие файлы, используемые несколькими программными продуктами ООО «ЕС-пром», устанавливаются в папку* ***<ProgramFiles(x86)>\ES-Prom****, вне зависимости от выбранной папки установки ПК «Бастион-3».*

Далее, программа установки предложит выбрать компоненты, которые необходимо установить.

> ***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 ПК «Бастион-3», следует выбрать компонент «Управление схемами ПК «Бастион-3».*

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

Для СУБД PostgreSQL:

Пользователь PostgreSQL – имя пользователя PostgreSQL для подключения к БД ПК «Бастион-3».

Пароль пользователя PostgreSQL – пароль пользователя для подключения к базе данных всеми модулями ПК «Бастион-3».

Имя базы данных PostgreSQL – название БД ПК «Бастион-3» 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 ПК «Бастион-3» для установки ПК «Бастион-3» 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 ПК «Бастион-3» 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 ПК «Бастион-3», то по окончании установки программа предложит запустить «Управление схемами ПК «Бастион-3».

> ***Внимание!*** *Для работы системы необходимо развернуть схему БД. См. п. 8.6.3.*

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 Bastion3AgentSvc на сервере системы.*

4.1.5.2. Установка ПК «Бастион-3» с использованием deb-пакетов

Перед установкой ПК «Бастион-3» следует убедиться, что в системе установлены:

1. .Net Core 8.
2. СУБД PostgreSQL или аналог.
3. Guardant Control Center.

Для установки или обновления ПК «Бастион-3» в ОС семейства Debian, в частности в Astra Linux 1.7 SE, необходимо выполнить установку соответствующих deb-пакетов ПК «Бастион-3».

Это можно сделать, перейдя в консоли в папку с установочными пакетами ПК «Бастион-3» и выполнив команду:

```
sudo dpkg -i bastion3-*
```

После этого следует перейти в папку с установочными пакетами драйверов ПК «Бастион-3» и выполнить ту же команду для установки всех драйверов, либо установить только необходимые драйверы по отдельности.

ПК «Бастион-3» будет установлен в каталог /opt/Bastion3.

Для удаления ПК «Бастион-3» можно выполнить команды:

```
sudo apt purge bastion3-platform
```

Удаление модуля управления БД:

```
sudo apt purge bastion3-db
```

4.1.5.3. Установка ПК «Бастион-3» с использованием rpm-пакетов

Перед установкой ПК «Бастион-3» следует убедиться, что в системе установлены:

1. Net Core 8.
2. СУБД PostgreSQL или аналог.
3. Guardant Control Center.

Для установки или обновления ПК «Бастион-3» через rpm-пакеты, необходимо перейти в консоли в папку с установочными пакетами ПК «Бастион-3» и выполнить команду:

```
sudo yum install bastion3-*
```

После этого следует перейти в папку с установочными пакетами драйверов ПК «Бастион-3» и выполнить ту же команду для установки всех драйверов, либо установить только необходимые драйверы по отдельности.

ПК «Бастион-3» будет установлен в каталог /opt/Bastion3.

Для удаления ПК «Бастион-3» можно выполнить команды:

```
sudo yum remove bastion3-platform
```

Удаление модуля управления БД:

```
sudo yum remove bastion3-db
```

4.2. Запуск и выгрузка системы

В версии ПК «Бастион-3» драйверы работают на сервере оборудования без пользовательского интерфейса 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 Bastion3AgentSvc.
2. Каждый тип драйвера работает в отдельном процессе с именем BDriverHost. 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 «Панели управления». Все драйверы можно запускать и останавливать отдельно, не выходя из приложения «Пост охраны», 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.

В ОС Linux запуск сервера системы можно произвести, выполнив команду:

```
sudo systemctl start bastion3-localagent
```

Сервер оборудования и сервер системы могут работать без пользовательского интерфейса.

Клиентское приложение «Пост охраны» (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 ПК «Бастион-3». В дальнейшем рекомендуется изменить этот пароль.*

Запуск модуля «Пост охраны» 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. 6.2.

4.3. Структура процессов

Первичный процесс, который запускает все необходимые модули системы – это служба Bastion3AgentSvc. Она выполняется на всех компьютерах ПК «Бастион-3», 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 BDriverHost (Рис. 2). Если в системе несколько однотипных драйверов (например, 2 драйвера Peridect), то они будут работать в одном процессе.

Многие задачи выполняются системой также в отдельных процессах с именем BAgent (Рис. 2). К таким задачам относятся, например:

- Сервис протоколирования событий;
- Графическая подсистема модуля «Пост охраны»;
- Подсистема фотоидентификации.

Такие процессы также запускаются службой Bastion3AgentSvc по необходимости (например, при запуске «Бастион-3 – Пост охраны»).

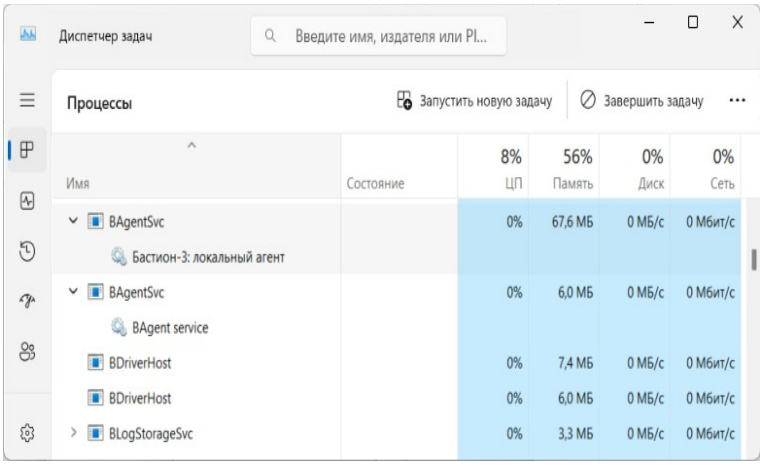

Рис. 2. Процессы ПК «Бастион-3» на сервере системы и оборудования

5. Настройка системы

5.1. Общая информация о настройке системы

Для настройки ПК «Бастион-3» предназначено специальное приложение «Панель управления» (admin.exe). Все настройки в нём сгруппированы в ряд блоков (см. Рис. 3). Набор доступных блоков может отличаться в зависимости от установленных модулей системы. Тем не менее, рассмотренные далее блоки (структура объекта, операторы и полномочия, драйверы, обработка событий, локальные настройки) присутствуют всегда.

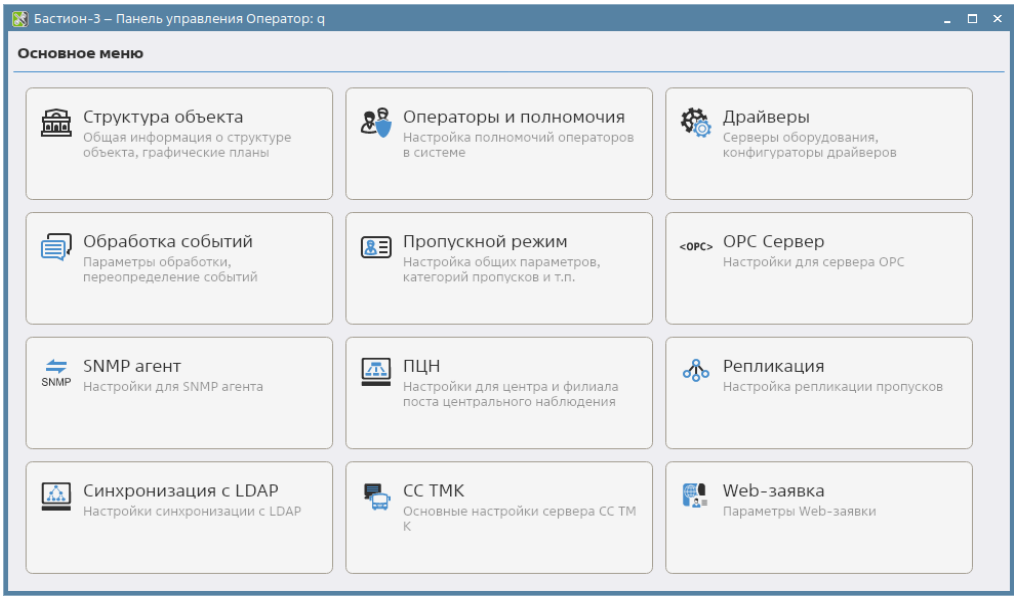

Рис. 3. Главное окно панели управления ПК «Бастион-3»

Ряд настроек, индивидуальных для каждого рабочего места, выполняется в приложении «Локальные настройки». Для его запуска требуются полномочия администратора ОС.

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 серверы оборудования, а затем драйверы (п. 5.4.1.).
3. Настроить полномочия, список ролей и операторов (п. 5.5.).
4. Настроить добавленные драйверы (см. инструкцию на соответствующий драйвер).
5. Расставить пиктограммы на графических планах (п. 5.3.2.).
6. Настроить параметры обработки событий (п. 5.6.), сценарии и реакции на события.
7. Настроить территории, 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 соответствии с их группировкой в панели управления ПК «Бастион-3».

5.3. Настройка структуры объекта

5.3.1. Общие сведения об объекте

Для редактирования общих сведений об объекте следует выбрать блок «Структура объекта – общие сведения об объекте» в панели управления ПК «Бастион-3». Откроется форма, представленная на Рис. 4:

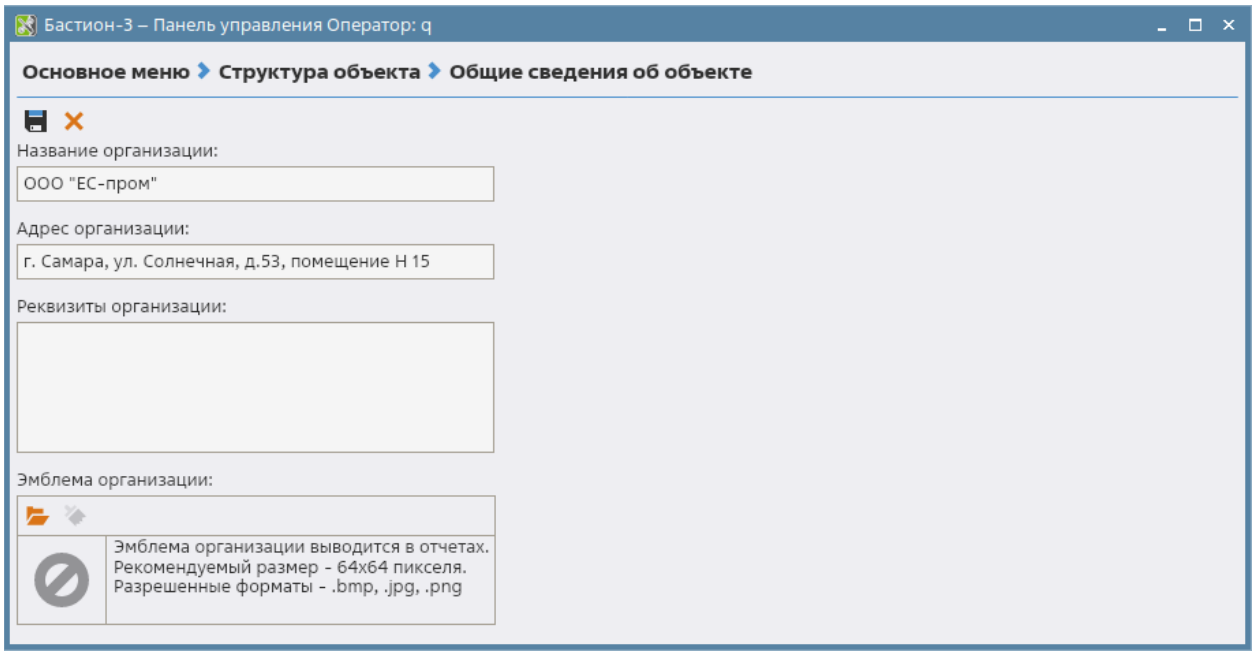

Рис. 4. Редактирование общих сведений об объекте

Здесь можно указать:

Название организации, *Адрес организации* и *Реквизиты организации* – они будут выводиться в отчётах системы.

Эмблема организации – также используется для вывода в отчётах. Можно загружать изображения в форматах BMP, PNG и JPG. Рекомендуется использовать изображения размером 64x64 пикселя.

5.3.2. Настройка графических планов

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

В качестве графических планов могут быть использованы изображения как в векторном (*.DXF), так и в растровом (*.JPG, *.BMP, *.PNG) форматах. Для более корректного масштабирования плана рекомендуется использовать векторные планы. Не рекомендуется использовать растровые файлы с разрешением более 1920x1080.

5.3.2.1. Работа с деревом планов

Для входа в режим настройки графических планов выберите блок «Структура объекта→Графические планы». При этом откроется форма для редактирования планов, содержащее дерево устройств и дерево планов (Рис. 5).

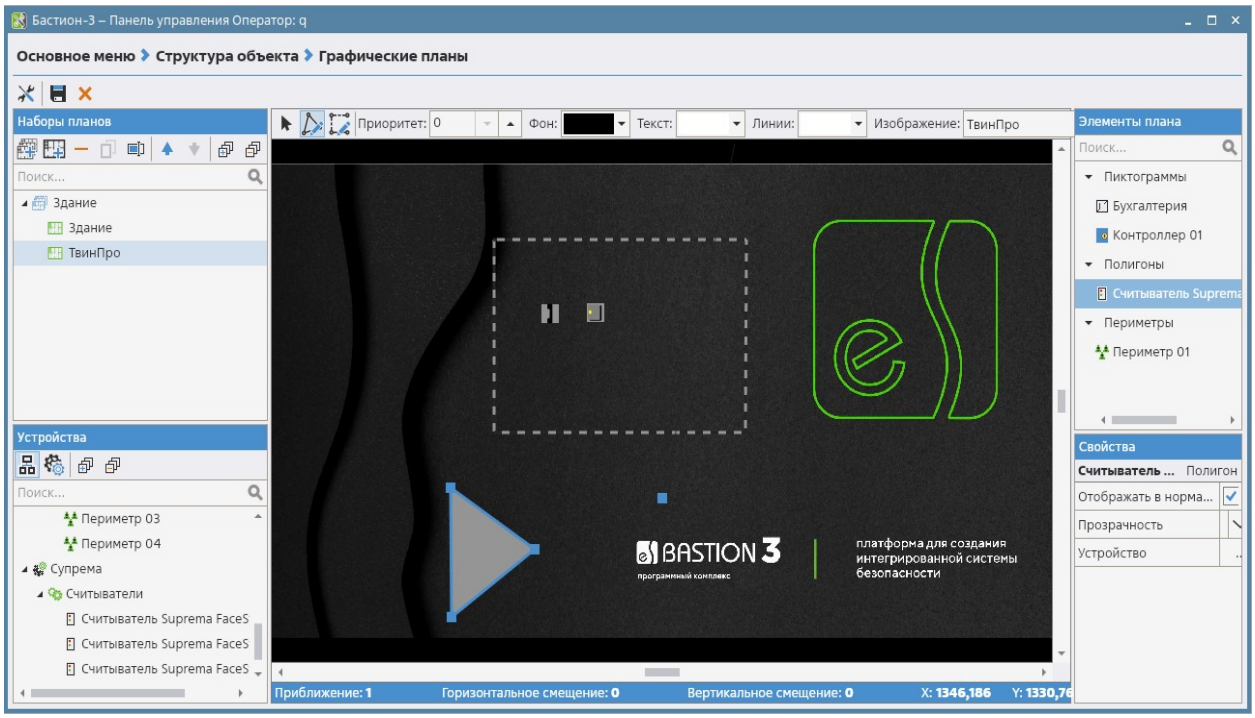

Рис. 5. Режим настройки планов

Изображения планов хранятся в базе данных. Управление ими осуществляется с помощью окна *«Список изображений»* (Рис. 6). Оно вызывается при добавлении нового плана или из блока «Изображение» в панели инструментов. В этом окне можно добавить из файла, переименовать, экспортировать в файл либо удалить изображение плана.

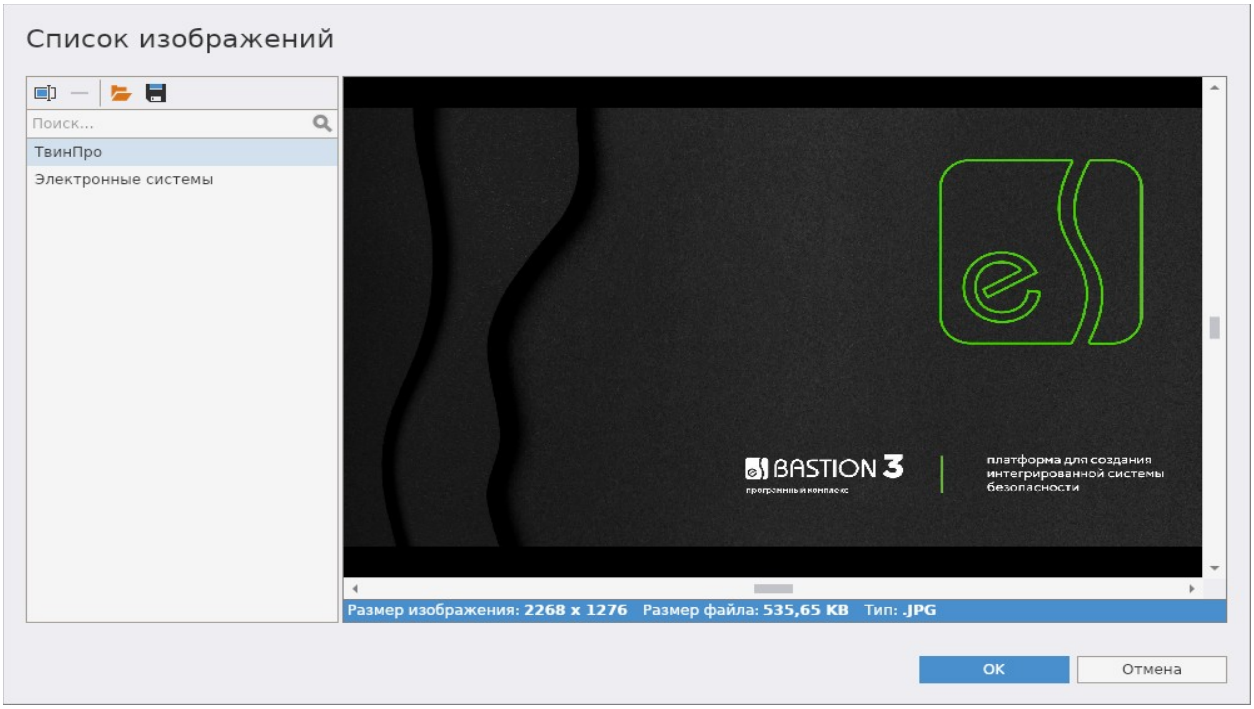

Рис. 6. Список изображений планов

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.

Для векторных планов можно указать цвета фона, текста и линий. Эти цвета будут использоваться только, если отключена настройка «Использовать цвета AutoCAD» в «Локальных настройках». Цвет фона применяется также и для растровых изображений за границами самого изображения.

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

Для удаления плана или набора планов из дерева планов, выберите этот объект и нажмите кнопку «Удалить с плана» (« ») на панели над планом.

Для удаления пиктограмм и других графических объектов с плана используйте кнопку « » в панели инструментов.

Привязка набора планов к роли оператора осуществляется в окне «Роли операторов».

Для выхода из режима настройки планов закройте окно редактирования планов.

5.3.2.2. Расстановка пиктограмм

После добавления одного или нескольких планов на них могут быть вынесены пиктограммы устройств. Пиктограммы перетаскиваются на план из дерева устройств, расположенного слева в нижней части окна. Все устройства в дереве сгруппированы по подключению. Также можно вынести 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 и блока свойств в

правой нижней части окна редактора планов). 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.

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

5.3.2.3. 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 команды «Добавить предустановку  » с панели инструментов (будет создана предустановка, соответствующая текущим настройкам плана в редакторе). В панели свойств предустановки есть возможность задать её имя, вручную ввести сдвиги относительно горизонтали и вертикали вместе с приближением.

Для того, чтобы выполнить предустановку плана непосредственно в редакторе планов, выберите её в дереве элементов плана и дважды щёлкните по ней.

5.3.2.4. Рисование многоугольников

Каждое устройство в ПК «Бастион-3» может быть представлено на плане не только пиктограммой, но и многоугольником произвольной формы (см. Рис. 5).

Для того чтобы нарисовать многоугольник проделайте следующие операции:

Перейдите в режим рисования многоугольников («  »). Левой кнопкой мыши щелкайте в углах требуемого многоугольника.

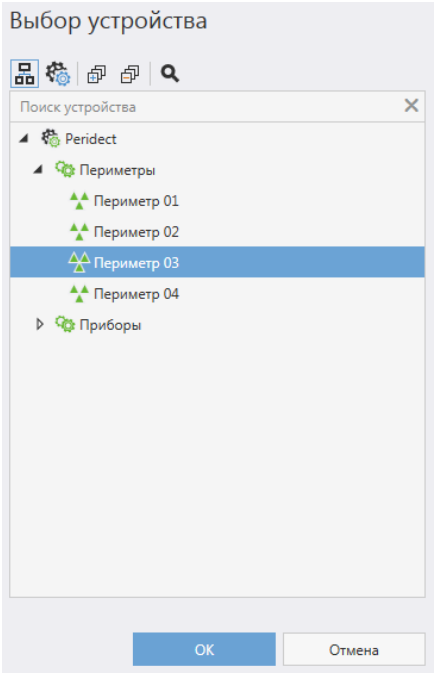

Рис. 7. Окно выбора устройства для многоугольника

Для завершения рисования щелкните правой кнопкой мыши. Две крайние вершины будут соединены между собой. На экране появится окно с деревом устройств (Рис. 7). Выберите устройство, которое будет обозначать многоугольник и нажмите «ОК». При нажатии «Отмена» нарисованный многоугольник будет удален с плана.

Для выхода из режима рисования многоугольников перейдите в режим «Выбор элементов ».

Координаты и количество вершин многоугольника можно изменить после окончания рисования. Для этого необходимо нажать на кнопку «Редактировать вершины » в панели инструментов. Появится форма (Рис. 8), в которой можно отредактировать координаты X и Y каждой вершины, а также добавить новые или удалить лишние.

Рис. 8. Редактирование вершин многоугольника

5.3.2.5. Рисование периметров

Периметры в ПК «Бастион-3» могут быть отображены на плане с помощью специальных объектов – ломаных линий произвольной формы (см. Рис. 5).

Для того чтобы нарисовать периметр проделайте следующие операции:

Перейдите в режим рисования периметров («»). Левой кнопкой мыши щелкайте в углах требуемой ломаной линии.

Для завершения рисования щелкните правой кнопкой мыши. На экране появится окно с деревом устройств (). Выберите устройство, которое будет обозначать периметр и нажмите «ОК». При нажатии «Отмена» нарисованный периметр будет удален с плана.

Для выхода из режима рисования периметров перейдите в режим «Выбор элементов ».

Координаты и количество вершин периметра можно изменить после окончания рисования. Для этого необходимо нажать на кнопку «Редактировать вершины » в панели инструментов. Появится форма (Рис. 8), в которой можно отредактировать координаты X и Y каждой вершины, а также добавить новые или удалить лишние.

Кнопка «Изменить направление периметра » позволяет поменять порядок следования вершин периметра на обратный. Это может потребоваться для корректного отображения точки сработки периметра.

5.3.2.6. Настройка свойств графических элементов

С каждым графическим элементом плана (пиктограммой, многоугольником или периметром) связана панель свойств, расположенная в правом нижнем углу окна редактирования.

Здесь могут редактироваться следующие 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. Можно изменить связанное с пиктограммой устройство уже после установки на план.

Не показывать пиктограмму в нормальном состоянии. Позволяет установить режим, при котором элемент 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.

Координаты X, Y. Позволяют вручную указать координаты левого верхнего угла пиктограммы.

Прозрачность. Для полигонов позволяет задать степень прозрачности (0 – непрозрачный, 100 – полностью прозрачный).

Угол поворота. Для пиктограмм позволяет установить произвольный угол поворота в градусах.

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

5.3.3. Редактор пиктограмм

В ПК «Бастион-3» есть возможность изменять вид пиктограмм устройств и добавлять свои собственные пиктограммы. Для этого в панели управления следует выбрать блок «Структура объекта – Редактор пиктограмм». Откроется форма редактора (Рис. 9).

Для каждого типа устройств может быть определено несколько 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 ПК «Бастион-3», хранятся в базе данных.

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

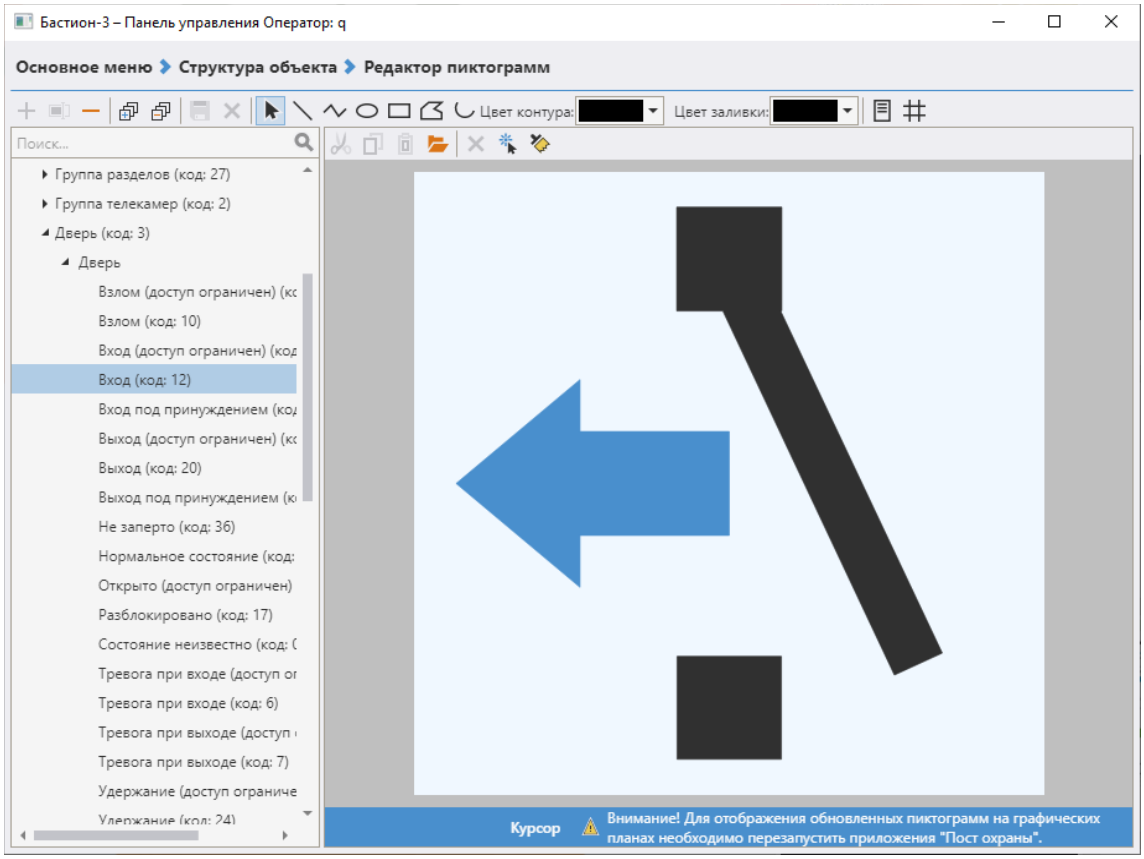

Рис. 9. Общий вид редактора пиктограмм

Для редактирования пиктограммы следует выбрать в дереве слева необходимое устройство и состояние.

Для добавления нового вида пиктограммы следует выделить в дереве необходимый тип устройства и нажать кнопку «Добавить  ». В появившемся окне следует выбрать состояние, для которого предназначена пиктограмма. Здесь же можно загрузить пиктограмму из файла формата SVG. При импорте из SVG-файлов есть ряд ограничений:

1. Не должны использоваться слои (группировки), либо весь рисунок должен быть в одном слое.
2. Рисунок должен быть выполнен только объектами *<path>* (после рисования следует преобразовывать фигуры в *<path>*).
3. Координаты точек у *<path>* должны быть в интервале *[0; 24]* , т.к. размеры пиктограмм 24x24.
4. Обводку у фигуры указывать не нужно, только заливку. Визуальную имитацию обводки фигуры можно нарисовать следующим образом: нарисовать фигуру с заливкой того цвета, который должен быть у обводки, нарисовать такую же фигуру меньшего размера с заливкой основного цвета и поместить меньшую фигуру поверх большой. Разница в размере и будет обводкой. При загрузке svg в редакторе пиктограмм все объекты *<path>* конвертируются в сплошные полигоны (многоугольники), которые не могут иметь внутри себя «пустоты».
5. Желательно каждую фигуру рисовать отдельным *<path>.*
6. *<path>* в svg-файле должны идти в следующем порядке: элемент *<path>* для фигуры А, которая должна отобразиться поверх фигуры Б , должен располагаться позже элемента

<path> для фигуры Б (подробнее https://www.w3.org/TR/SVG11/render.html#RenderingOrder).

С помощью кнопок на панели инструментов можно выполнять основные операции с элементами пиктограмм:

Операции выделения и копирования – «Вырезать », «Копировать », «Вставить », «Выделить всё » и «Удалить всё ». Рекомендуется использовать операции копирования и вставки для создания однотипных пиктограмм для разных состояний устройств.

Операции рисования прямых « » и ломаных линий “ ”, эллипсов “ ”, прямоугольников “ ”, многоугольников “ ” и кривых “ ”.

Операции установки цвета контура и заливки (Цвет контура: Цвет заливки:).

Также, отдельно можно вывести список элементов пиктограмм, нажав на кнопку « ».

Для ломаной линии и многоугольника можно вручную отредактировать список вершин, нажав на кнопку « ».

Операции поворота ( ) и отражения ( ) выделенных элементов пиктограмм.

После завершения редактирования пиктограмм изменения следует сохранить, нажав на кнопку .

> ***Внимание!*** *После сохранения изменений, внесенных в пиктограммы устройств, необходимо перезапустить модуль «Пост охраны» для отображения обновленных пиктограмм на графических планах.*

5.3.4. Группы управления охраной

5.3.4.1. Определение, назначение и состав групп управления охраной

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

Группы управления охраной в ПК «Бастион-3» поддерживаются на системном уровне и могут включать элементы разных драйверов. Группы управления охраной не являются устройствами ПК «Бастион-3». 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 ПК «Бастион-3».

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 ПК «Бастион-3».

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.

5.3.4.2. Настройка групп управления охраной

Настройка групп управления охраной производится на странице «Структура объекта – Группы управления охраной» в панели управления ПК «Бастион-3». Доступ к форме разграничивается отдельным полномочием «Редактирование ГУО».

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

Для каждой ГУО, независимо от типа, здесь можно задать её *название*, непосредственно в дереве ГУО (Рис. 10).

Адрес (номер). Для аппаратных ГУО содержит адрес или номер, под которым ГУО записывается в конфигурацию контроллеров. Здесь этот номер доступен только для чтения.

При настройке аппаратных ГУО в списке по центру отображаются доступные разделы, справа – разделы, включенные в выбранную аппаратную ГУО (Рис. 10):

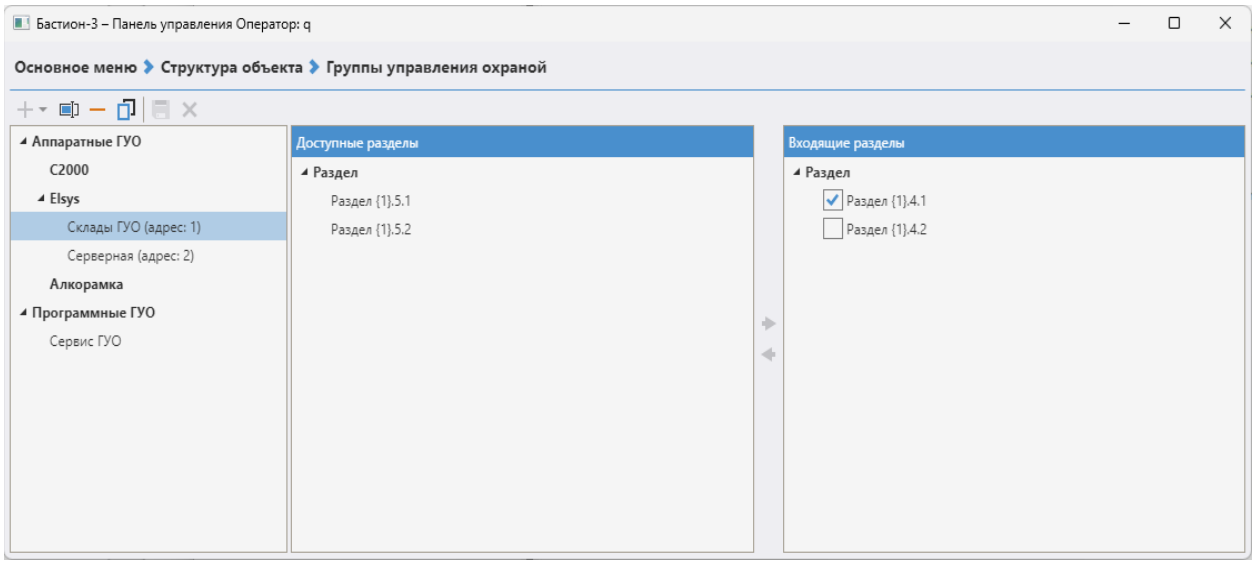

Рис. 10. Свойства аппаратной ГУО

Для разделов, входящих в аппаратную ГУО, можно указать, предоставлять ли в этой ГУО права на снятие с охраны. Для предоставления таких прав следует установить флаг рядом с названием раздела, входящего в ГУО (Рис. 10).

Аппаратные ГУО могут импортироваться из внешних источников (файлы конфигурации, непосредственно из сети контроллеров и т. п.) и настраиваться в конфигураторах соответствующих драйверов (например, драйверы Elsys или С2000). При импорте аппаратной ГУО её состав может быть неизвестен в АПК «Бастион-3».

При настройке программной ГУО в списке по центру отображаются доступные аппаратные ГУО, справа – аппаратные ГУО, включенные в выбранную программную ГУО (Рис. 11).

Для некоторых драйверов может быть недоступным включение нескольких аппаратных ГУО в одну программную. В этом случае они помечаются значком « ».

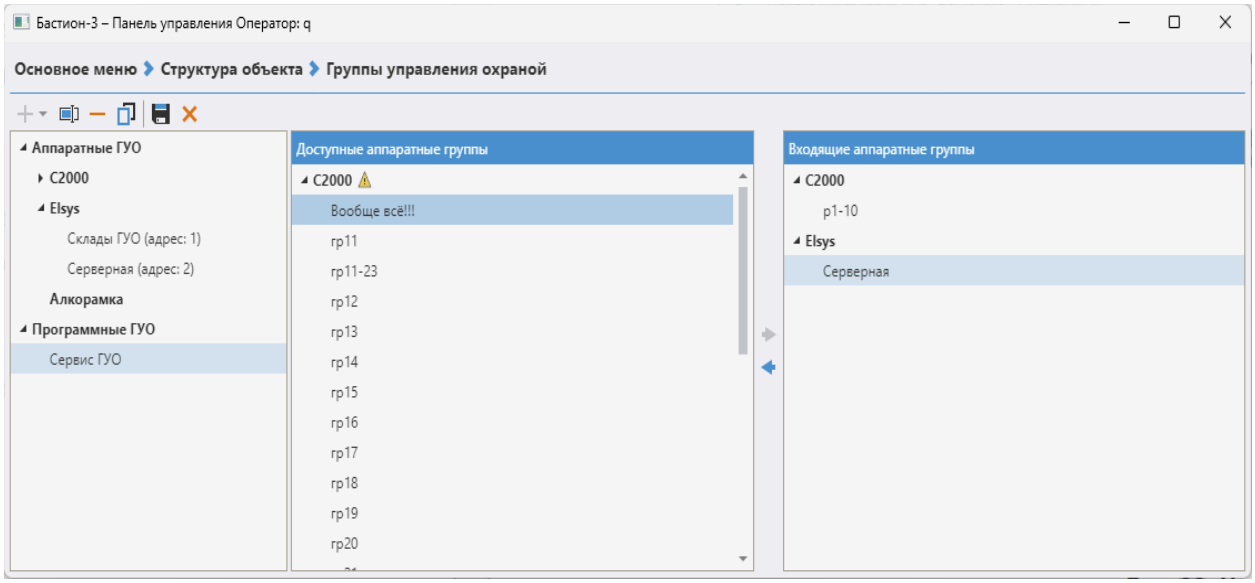

Рис. 11. Настройка программной ГУО

5.3.4.3. Привязка пропусков к группам управления охраной

К каждому пропуску может быть привязана одна 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 номеру карты;
2. По ПИН-коду;
3. По ПИН-коду и номеру карты.

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». Кроме того, оператору должна быть разрешена соответствующая ГУО.

5.3.5. Настройка территорий

Под *территорией* в ПК «Бастион-3» понимается некоторое пространство, ограниченное одной или несколькими точками прохода (дверями, турникетами, воротами и т. д.). Такой территорией может являться одно конкретное помещение, группа помещений, здание целиком, территория завода и т. д. Территории могут быть вложенными. Например, область контроля «На территории» может содержать несколько других областей – "Цех №1", "Бухгалтерия" и т. д.

Территории используются в следующих случаях:

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

Для настройки территорий в панели управления ПК «Бастион-3» следует выбрать пункт «Структура объекта – Территории». При этом появится окно, представленное на Рис. 12.

По умолчанию в системе определены две территории: «На территории» и «Вне территории». Эти области удалить нельзя. Область «На территории» всегда используется как «ограничитель территории предприятия», то есть в эту территорию должны входить все остальные. Также, по умолчанию эта область используется для учета рабочего времени. Область «Вне территории» не отображается в дереве, но её можно выбрать при настройке состава территорий.

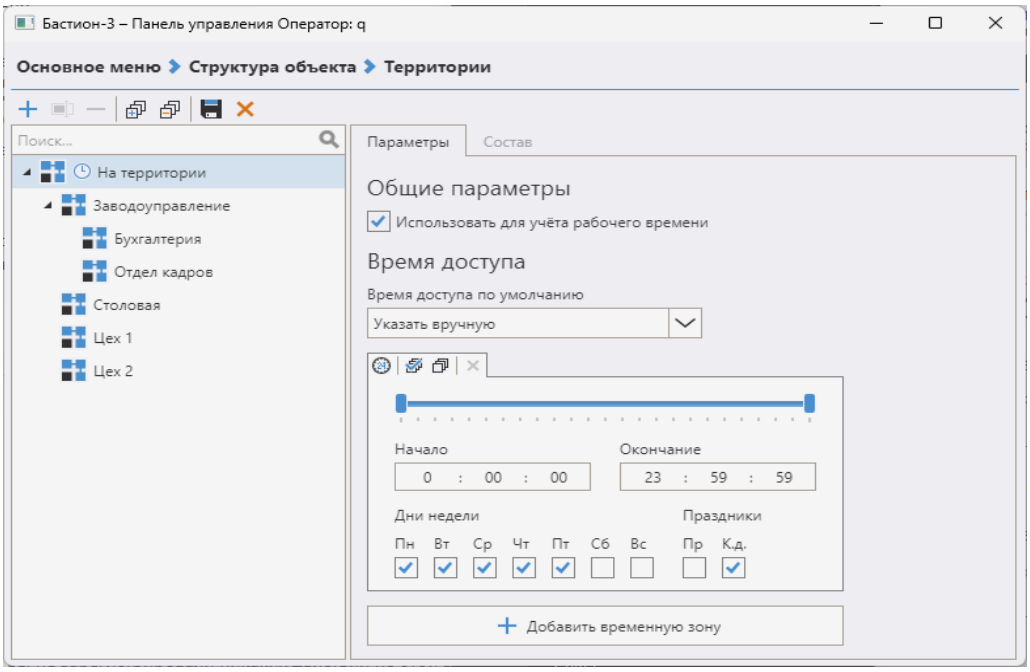

Рис. 12. Окно настройки территорий, страница «Параметры»

Для добавления территории можно нажать кнопку «+» в панели инструментов и ввести название новой территории.

После добавления территорий следует определить, что будет являться входами и выходами для каждой территории. Для этого необходимо указать, откуда и куда ведут точки прохода. Например, на Рис. 13 дверь «Заводоуправление» ведет из области «На территории» в область «Заводоуправление».

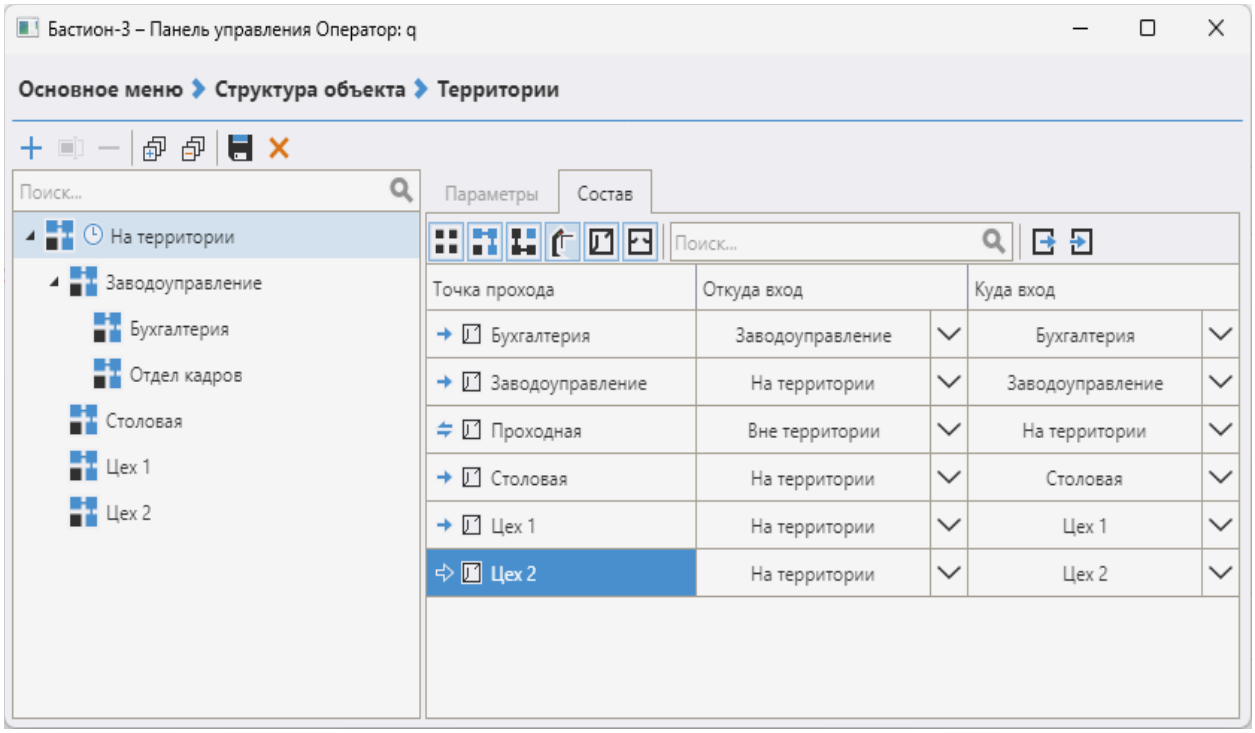

Рис. 13. Настройка состава территорий

Односторонние точки прохода также могут участвовать в территориях. 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 на территорию, ограничивающую эту точку. При этом следует выбирать одну и ту же территорию в столбцах «Откуда вход» и «Куда вход».

Можно отфильтровать список точек прохода с помощью кнопок в панели управления:

	Показывать свободные точки прохода, то есть те, которые не задействованы в территориях.
	Показывать точки прохода, связанные с выбранной в дереве территорией.
	Показывать точки прохода, не связанные с выбранной в дереве территорией.
	Показывать турникеты.
	Показывать ворота.
	Показывать двери.

На странице «Параметры» (Рис. 12) можно настроить следующие опции:

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

Время доступа по умолчанию. Если это время задано, то при включении территории в уровень доступа, по умолчанию она будет включена с заданным временем доступа. Время доступа можно

задать вручную или выбрать один из созданных заранее временных блоков. Территории, для которых задано время доступа по умолчанию, помечаются значком « ».

5.3.6. Настройки почты

В системе можно задать общие настройки подключения к почтовому серверу, которые будут использоваться для отправки электронной почты. Эти настройки могут использоваться для рассылок отчётов по временным расписаниям, для отправки оповещений модуля «Бастион-3 — Информ» и в других местах системы, где указывается «Использовать системные настройки почты». Для этого следует открыть страницу «Структура объекта — Настройки почты» (Рис. 14).

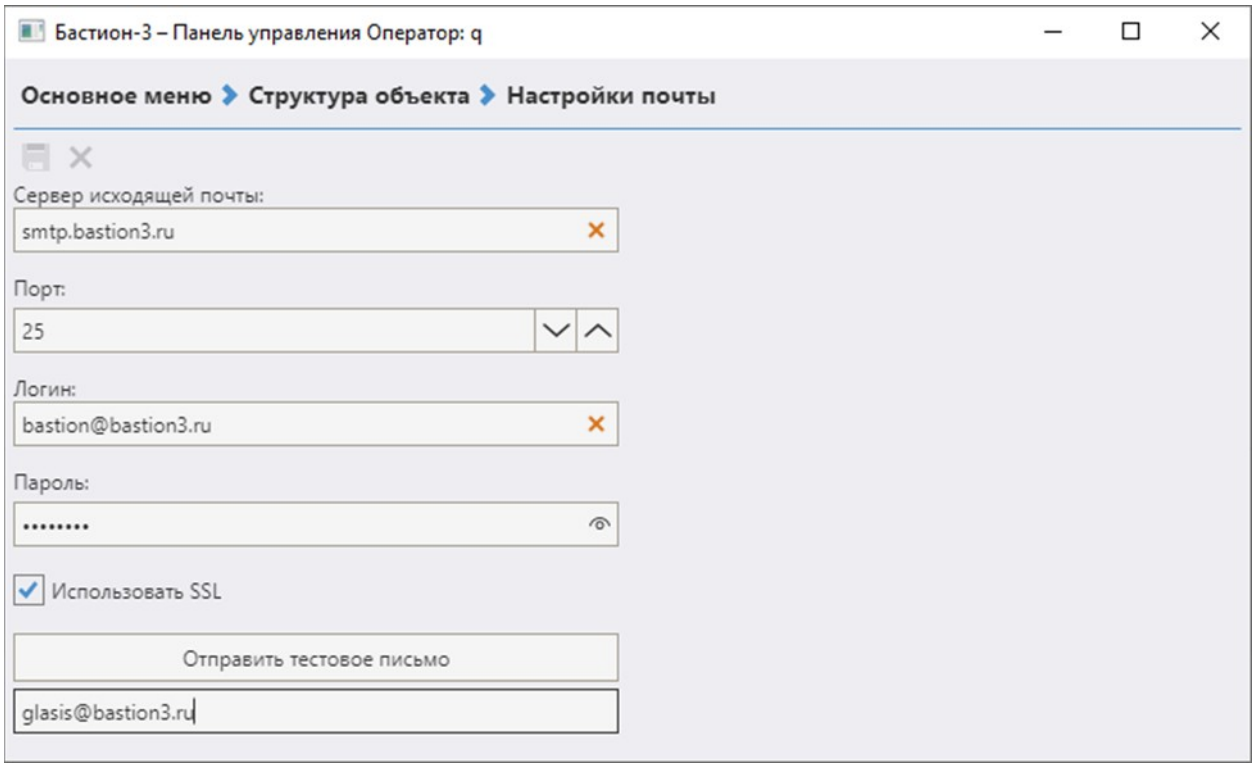

Рис. 14. Настройки почты

Сервер исходящей почты – имя или адрес сервера SMTP.

Порт – порт сервера, обычно 25, 587 или 465.

Логин — адрес электронной почты, с которого будут отправляться письма.

Пароль – пароль для логина, указанного в предыдущем пункте.

Использовать SSL – использовать ли протокол SSL при отправке.

Здесь же можно проверить настройки, отправив тестовое письмо на адрес, указанный в нижней строке ввода (Рис. 14).

5.3.7. Настройка внешних систем

К ПК «Бастион-3» можно подключать внешние системы через «Бастион-3 — Web API».
В этом случае, например, при использовании модуля «Бастион-3 — Логические схемы» возможна организация режима прохода через точки доступа с выполнением запроса на подтверждение доступа во внешние системы, подключенные через «Бастион-3 — Web API».

Внешняя система должна быть предварительно добавлена на странице «Структура объекта — Внешние системы» (Рис. 15).

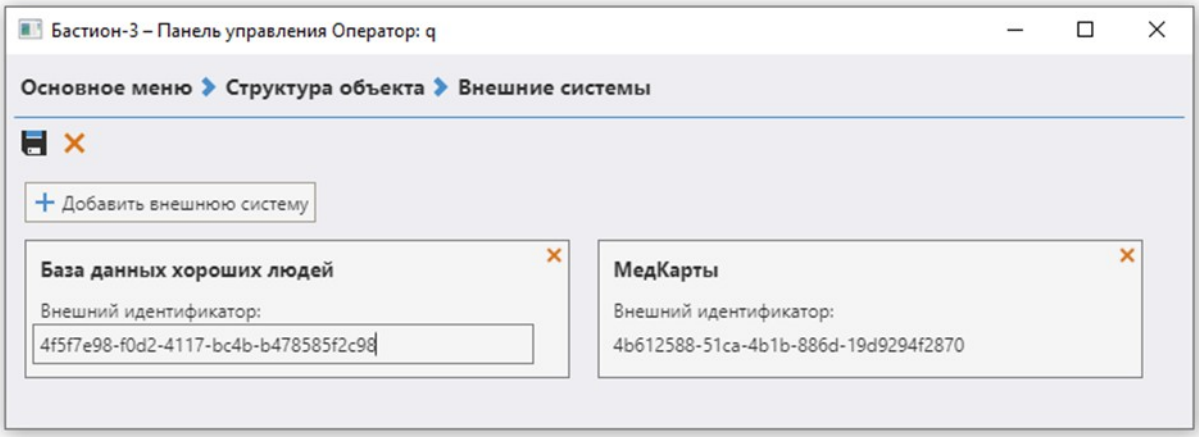

Рис. 15. Страница настройки внешних систем

Каждая внешняя система имеет название и внешний идентификатор. Внешний идентификатор будет передаваться в командах и событиях Web API. Более подробно см. «Бастион-3 — Web API. Руководство программиста».

5.4. Конфигурация драйверов

5.4.1. Внесение информации о серверах оборудования и драйверах

Сеть ПК «Бастион-3» состоит из сервера системы, серверов оборудования, клиентских рабочих станций и устройств, обслуживаемых драйверами.

В ПК «Бастион-3» должна быть добавлена информация обо всех серверах оборудования, используемых в системе. Добавлять компьютеры, используемые только для запуска клиентских приложений, нет необходимости.

Для добавления, удаления и редактирования свойств серверов оборудования необходимо выбрать блок «Драйверы» в основном окне и затем блок «Серверы оборудования». После этого откроется форма, представленная на Рис. 16.

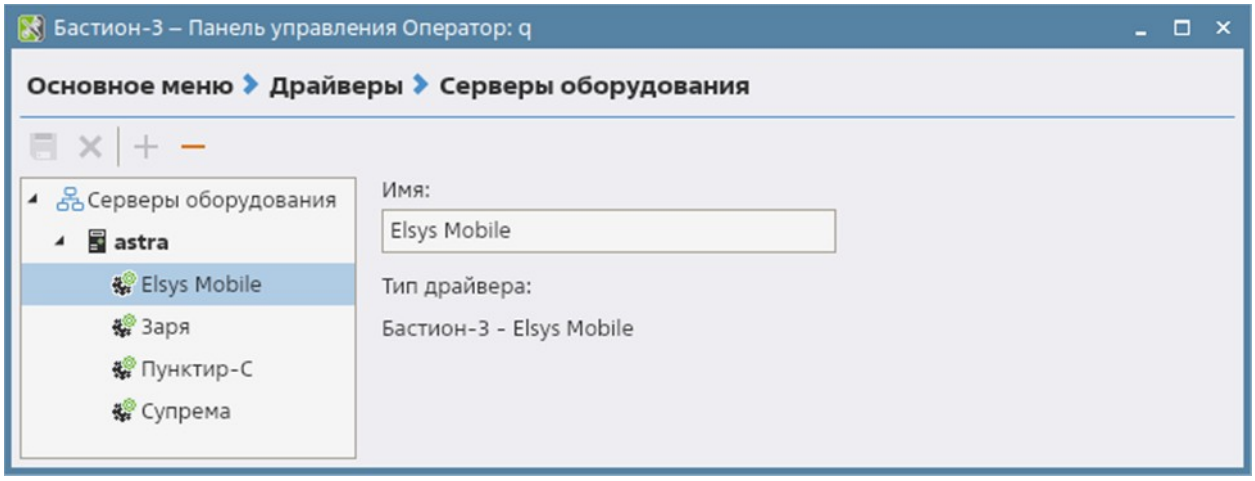

Рис. 16. Окно настройки «Серверы оборудования»

Для добавления сервера необходимо перейти на узел «Серверы оборудования» в дереве и нажать на кнопку «Добавить новый сервер оборудования» (Shift+Ins). При этом в дереве добавится новый узел, а в правой части формы отобразится поле «Имя», в которое нужно ввести имя или IP-адрес сервера оборудования.

> ***Внимание!*** *Имя сервера оборудования можно использовать только в случае, если он доступен для подключения по данному имени. Проверить доступность сервера по имени можно с помощью команды* ***ping.*** *В противном случае следует использовать IP-адрес.*

Для добавления экземпляра драйвера необходимо выбрать сервер оборудования в дереве, нажать кнопку «добавить драйвер» (Ctrl+Ins), ввести название устройства, выбрать тип добавляемого драйвера (Рис. 16).

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. 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 выбранном сервере оборудования.

> ***Внимание!*** *Для возможности работы сервера оборудования с COM-портами в операционной системе семейства Линукс необходимо на комьютере, на котором работает сервер оборудования, добавить пользователя* ***bastion*** *в группу* ***dialout****, например выполнив команду:* `sudo usermod -aG dialout bastion`.

Для каждого драйвера необходимо заполнить два поля:

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 с внешней системой.

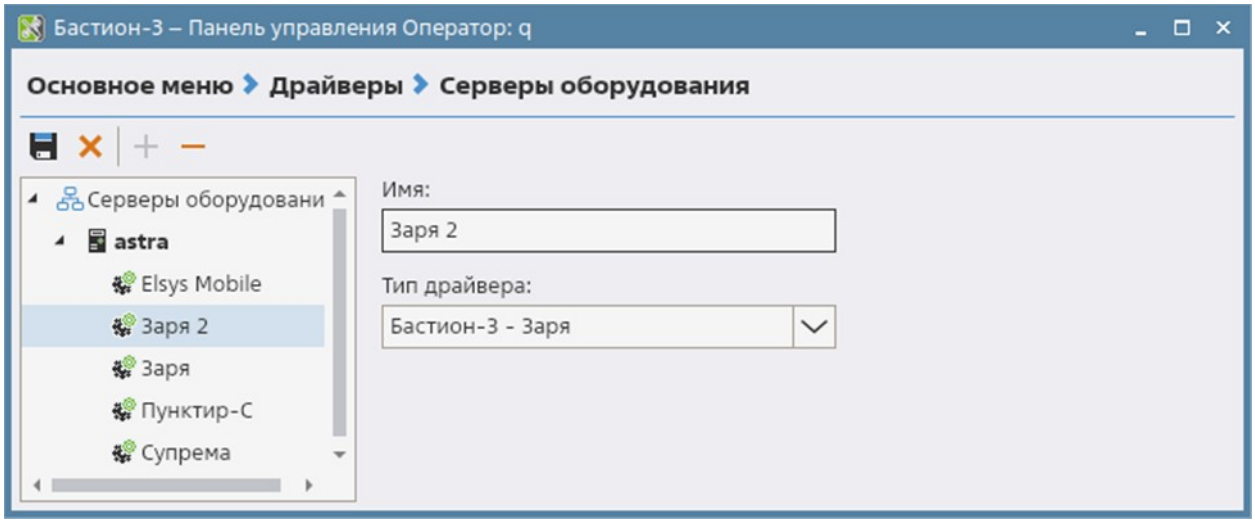

Рис. 17. Добавление экземпляров драйверов

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

После добавления драйвера в блоке «Драйверы» панели управления появятся пункты, относящиеся к настройке добавленного драйвера (Рис. 17). Сведения о настройках каждого драйвера см. в руководстве на этот драйвер.

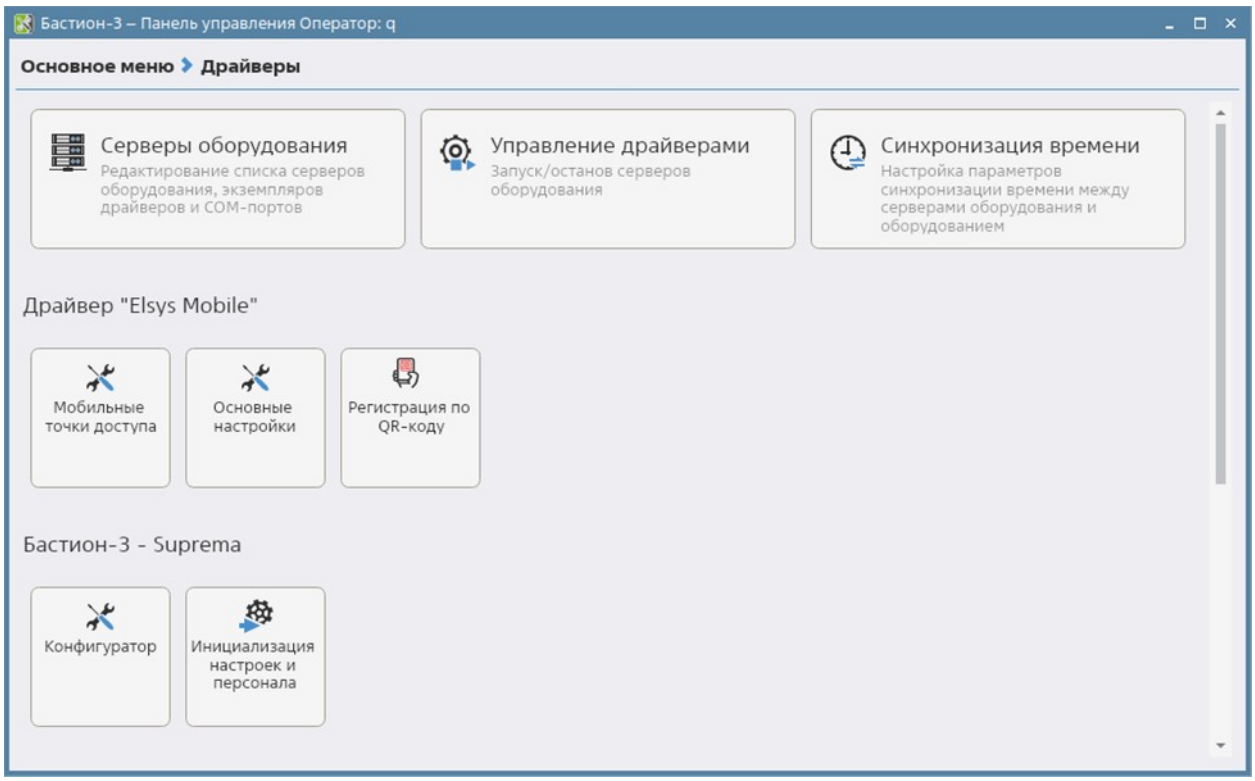

Рис. 18. Пример меню драйвера

Для редактирования имеющегося в списке сервера или драйвера следует выделить его 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 не сохраненных изменений осуществляется кнопкой «Отменить» (Ctrl+Z).

5.4.2. Управление драйверами

В системе предусмотрена возможность ручной остановки и запуска драйверов независимо друг от друга. Осуществляются данные действия в окне «Управление драйверами» панели управления. Внешний вид окна «Управление драйверами» представлен на Рис. 19.

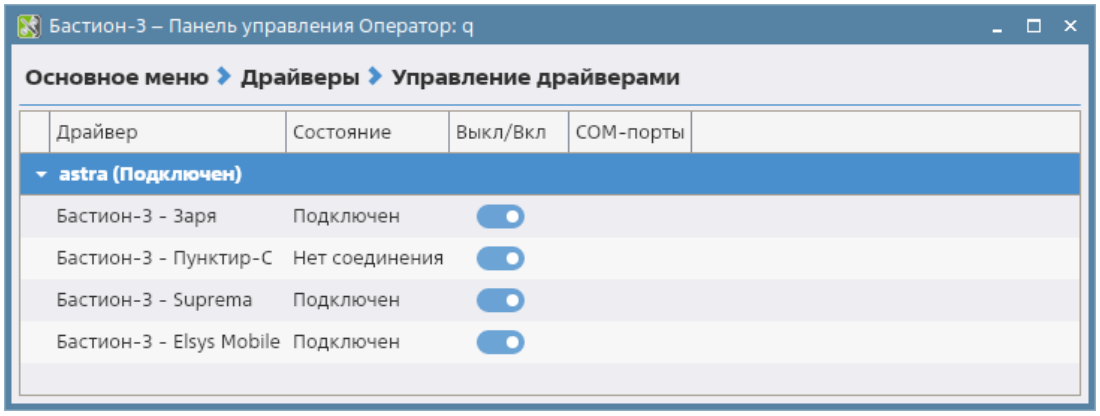

Рис. 19. Окно управления драйверами

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

5.4.3. Параметры синхронизации времени

В системе предусмотрена возможность синхронизации времени с устройствами добавленных драйверов. Для включения синхронизации следует выбрать блок «Драйверы – Синхронизация времени» в панели управления ПК «Бастион-3».

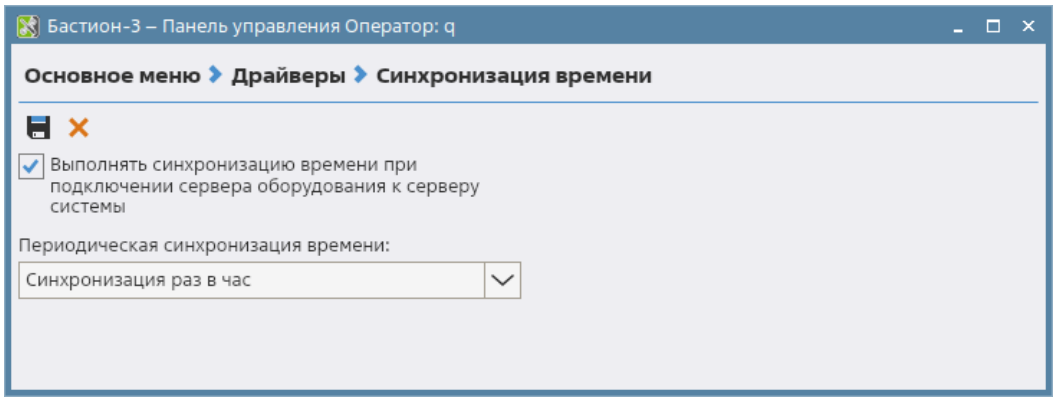

Рис. 20. Параметры синхронизации времени для драйверов

В открывшейся форме следует выбрать один из вариантов (отключена, раз в час, раз в день), см. Рис. 20:

Синхронизация времени между компьютерами ПК «Бастион-3» также необходима и должна выполняться средствами операционной системы.

5.4.4. Дополнительные поля для устройств

В системе есть возможность создавать и использовать до 100 дополнительных полей для устройств. Дополнительные поля являются типизированными. Доступны следующие типы полей: целое число, дробное число, строка, булев, дата, время, дата и время.

Дополнительные поля можно добавлять как для всех устройств, так и для отдельных типов устройств. Заполнение дополнительных полей возможно в конфигураторе драйверов в модуле «Панель управления», а также в модуле «Пост охраны». По дополнительным полям можно осуществлять поиск устройств и включать их в некоторые виды отчётов.

Для редактирования набора дополнительных полей оператор должен обладать полномочием «Редактирование набора дополнительных полей устройств».

Для редактирования списка дополнительных полей следует выбрать блок «Драйверы — Дополнительные поля». Откроется окно, представленное на Рис. 21.

Для каждого дополнительного поля можно ввести его описание, которое будет выводиться в качестве подсказки при заполнении поля.

В блоке «Правила применения» можно настроить, для каких типов устройств будет использоваться конкретное дополнительное поле. По умолчанию создаваемые дополнительные поля применяются для всех типов устройств.

На Рис. 21 приведен пример, когда дополнительное поле будет применяться только для телекамер двух драйверов — «Бастион-3 — Domination» и «Бастион-3 — Интеллект X».

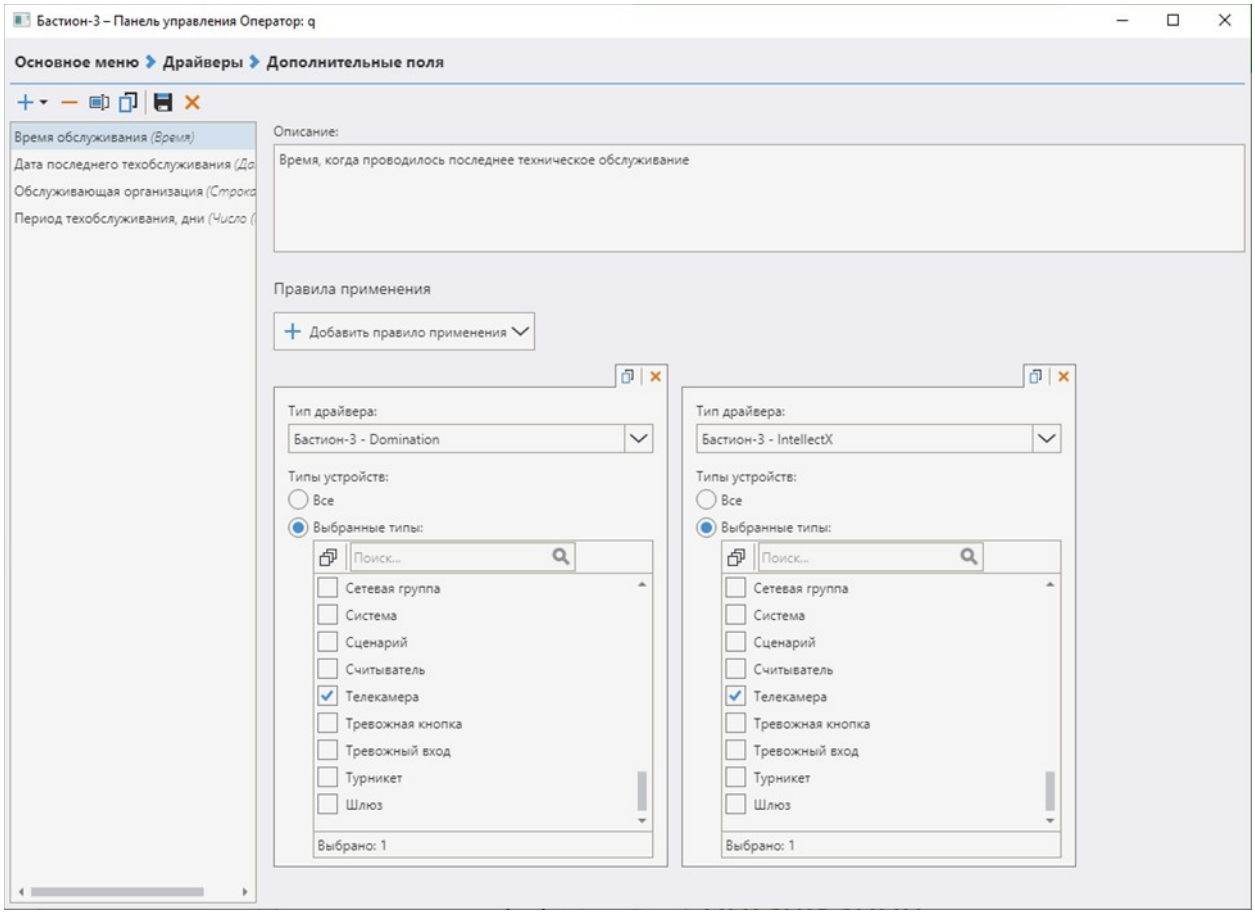

Рис. 21. Редактирование списка дополнительных полей устройств

Несколько правил применения следует использовать, когда требуется отфильтровать устройства различных драйверов. Правила применения можно копировать для других драйверов, нажав кнопку «  » в заголовке блока правила применения (Рис. 22).

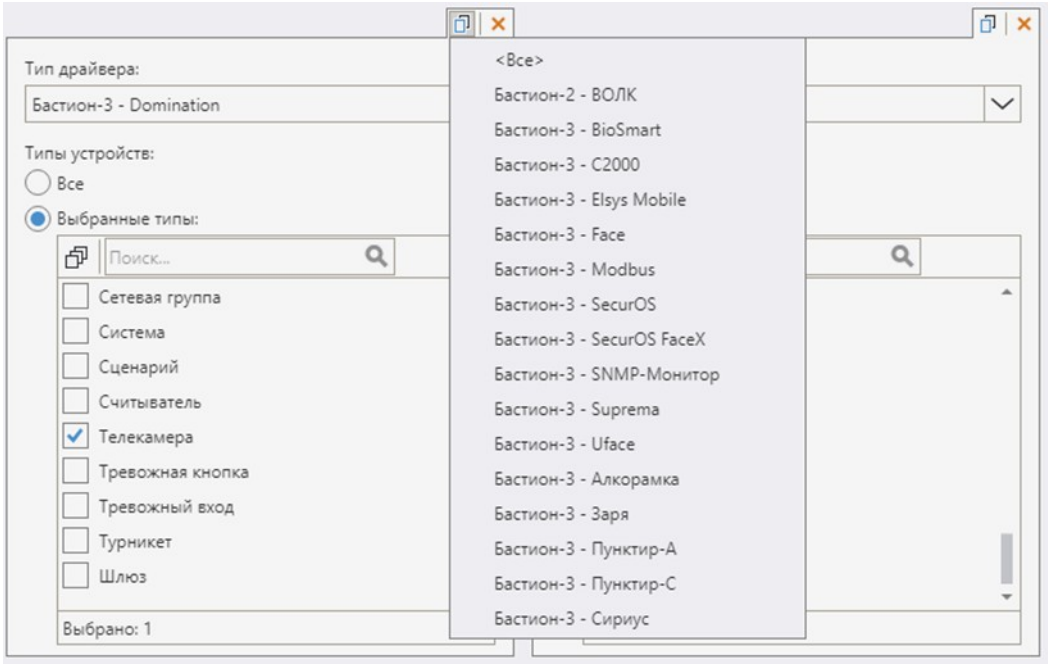

Рис. 22. Копирование правил применения дополнительных полей устройств

Внимание! *Если для конкретного типа драйвера есть отдельное правило, то для его устройств применяется именно оно, независимо от того, есть ли правило с типом драйвера "Все". Например, в случае, изображенном на Рис. 23, дополнительное поле драйвера Elsys будет отображаться только у контроллеров, а у других драйверов - для всех устройств.*

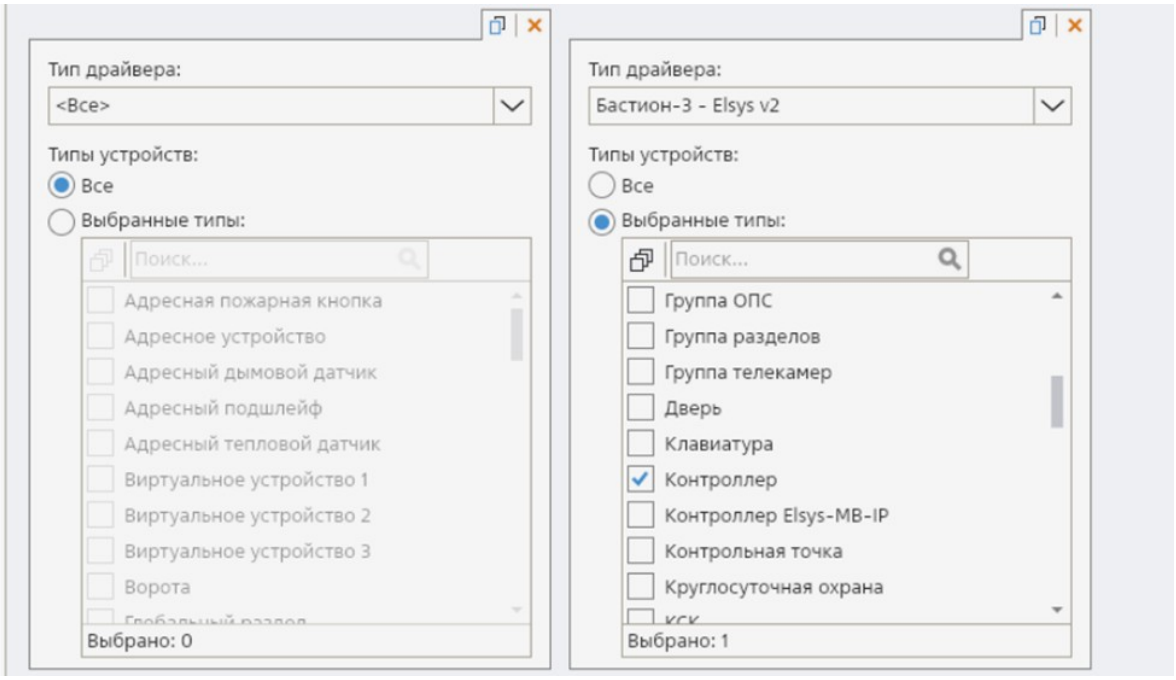

Рис. 23. Правила применения для дополнительных полей устройств

Для редактирования значений дополнительных полей в модуле «Панель управления» следует открыть конфигуратор требуемого драйвера, выбрать устройство и перейти на страницу «Дополнительные поля» (Рис. 24).

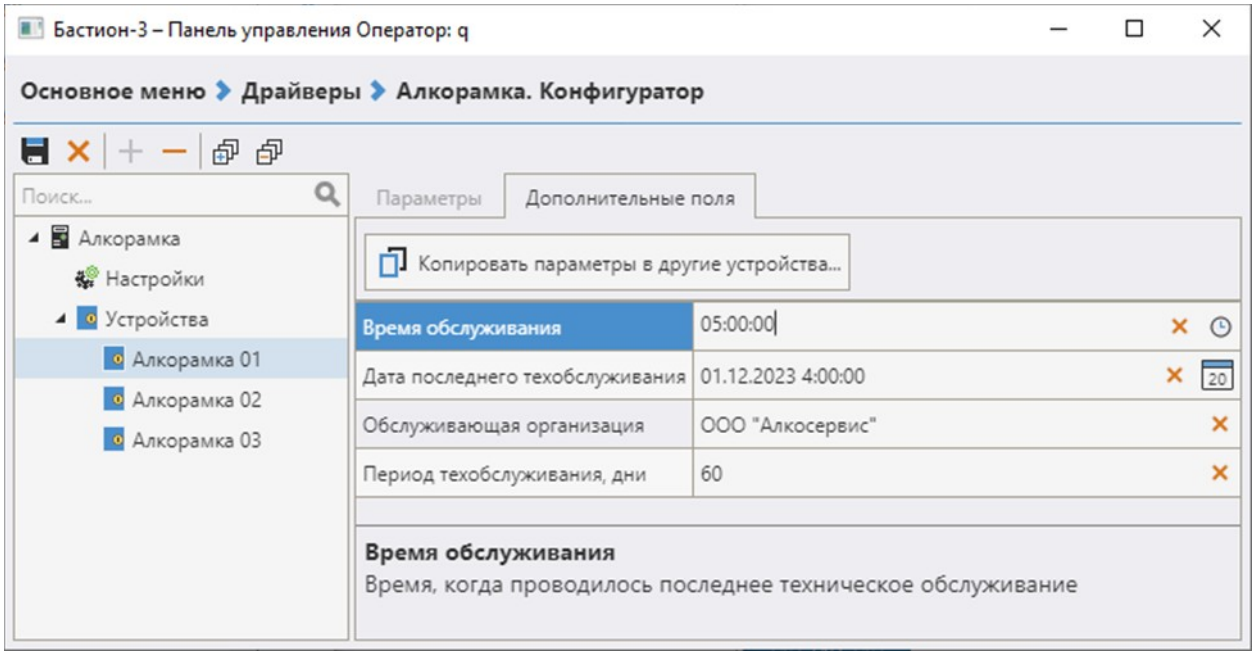

Рис. 24. Редактирование значений дополнительных полей

5.5. Настройка операторов и полномочий

5.5.1. Общие сведения о разграничении доступа операторов

В ПК «Бастион-3» применяется ролевая модель разграничения доступа операторов к функциям системы. Для каждого оператора в системе определена его *роль* (одна). Все права доступа к функциям системы определяются настройками ролей операторов.

По умолчанию, в системе определена единственная роль «Администратор», которую нельзя удалить.

> ***Внимание!*** *При первом запуске системы доступен логин оператора q с паролем q. Рекомендуется как можно быстрее сменить этот пароль.*

Система не хранит пароли операторов в открытом виде. Для сброса пароля предусмотрена специальная процедура.

ПК «Бастион-3» реализует регистрацию следующих событий безопасности в собственном протоколе событий:

- факты или попытки идентификации и аутентификации операторов;
- факты изменения полномочий, модификация ролей операторов;
- факты создания, изменения или блокирования учетных записей;
- действия пользователей по настройке и изменению конфигурации ИС;
- факты запуска (завершения) программ;
- факты доступа к защищаемым объектам доступа.

Обеспечивается фиксация следующей информации для каждого регистрируемого события безопасности:

- тип события безопасности;
- дата и время события безопасности;
- адрес компьютера события безопасности;
- результат события безопасности (успешно или неуспешно);
- оператор.

5.5.2. Работа со списком операторов

Для работы со списком операторов следует в модуле «Панель управления» выбрать блок «Операторы и полномочия – Операторы» (Рис. 25).

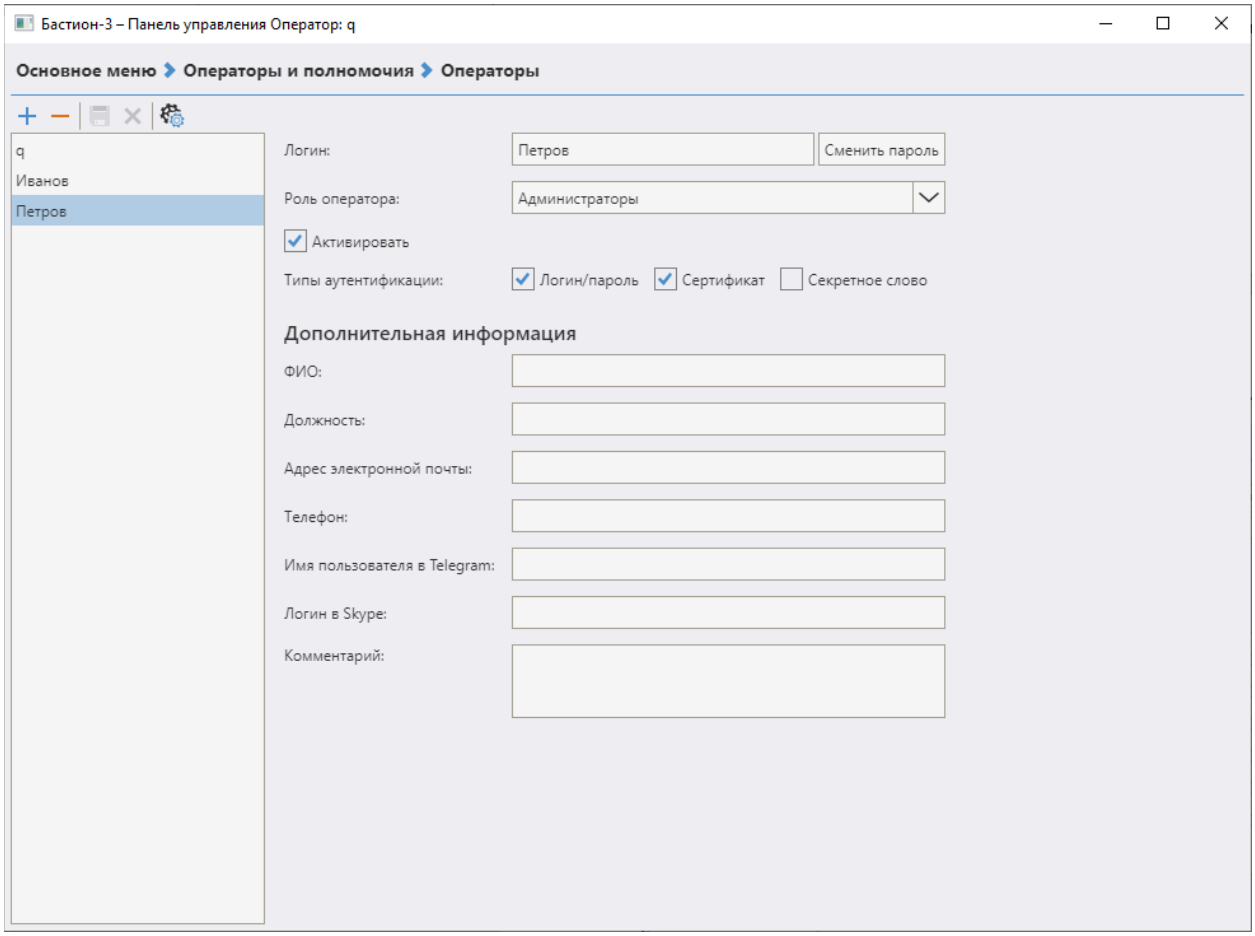

Рис. 25. Форма редактирования данных об операторах

Для *добавления* нового пользователя необходимо:

- нажать клавишу «добавить нового оператора» (Shift+Ins);
- ввести логин и пароль оператора в соответствующих полях. Логин и пароль могут содержать любые печатные символы русского или английского алфавита в разных регистрах, цифры и специальные символы, причем строчные и прописные буквы различаются при анализе пароля;
- подтвердить введенный пароль, набрав его повторно;
- нажать кнопку «ОК».

Рекомендуется добавлять отдельного оператора комплекса «Бастион-3» 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 модуле «Бастион-3 – Пост охраны» под новым именем. Для каждого пользователя назначается одна из настроенных заранее *ролей*.

Реквизиты оператора используются для вывода в отчётах, а также могут использоваться системой оповещений по дополнительным каналам связи «Бастион-3 — Информ».

Для оператора можно указать доступные для него способы аутентификации в системе. Возможные способы аутентификации: логин/пароль (используется обычными операторами системы), сертификат и секретное слово (могут использоваться системными, техническими операторами).

Если снять флаг «Активировать», то оператор будет временно заблокирован. При этом нет необходимости удалять его из системы. Повторная установка флага разблокирует оператора.

Для удаления оператора следует выбрать его в списке и нажать кнопку «Удалить оператора» (Shift+Del).

Для сохранения изменений следует нажать кнопку «Сохранить изменения» (Ctrl+s).

Для отмены изменений следует нажать кнопку «Отменить изменения» (Ctrl+Z).

5.5.2.1. Системные операторы

Имеется несколько предустановленных системных операторов, используемых службами ПК «Бастион-3». Просмотреть информацию по этим операторам можно, нажав на кнопку « » на панели инструментов (Рис. 26). Удалять учётные записи системных операторов или редактировать их настройки не разрешено.

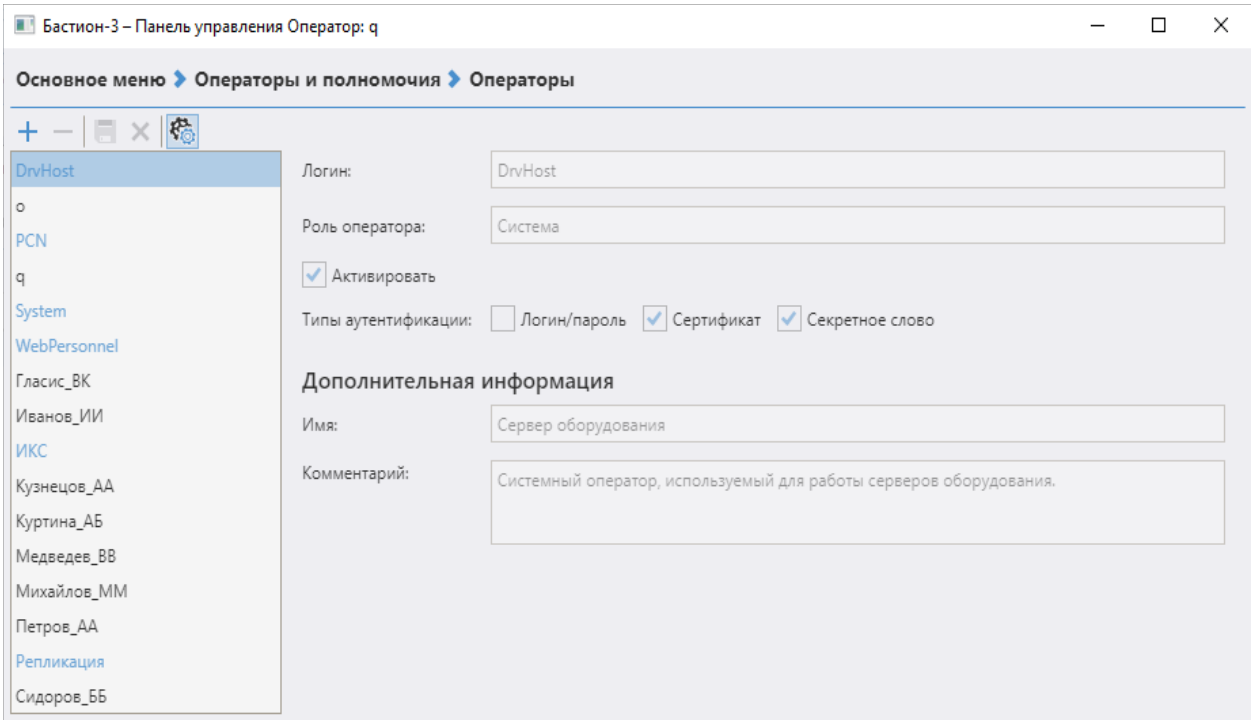

Рис. 26. Просмотр информации по системным операторам

5.5.3. Смена пароля оператора

Если вы забыли пароль для доступа к системе, единственный вариант действий – сменить этот пароль. Посмотреть сохранённые в системе пароли никаким образом нельзя.

Для смены пароля необходимо зайти в форму настройки операторов и нажать кнопку «Сменить пароль». В открывшейся форме необходимо ввести новый пароль и подтвердить его. После этого можно войти в систему с новым паролем.

5.5.4. Настройка ролей операторов

5.5.4.1. Основные операции с ролями операторов

Для настройки ролей пользователей следует выбрать блок «Операторы и полномочия – Роли операторов». Роль оператора (Рис. 27) задаёт все полномочия, а также ряд настроек пользовательского интерфейса. Одну и ту же роль можно назначить нескольким операторам.

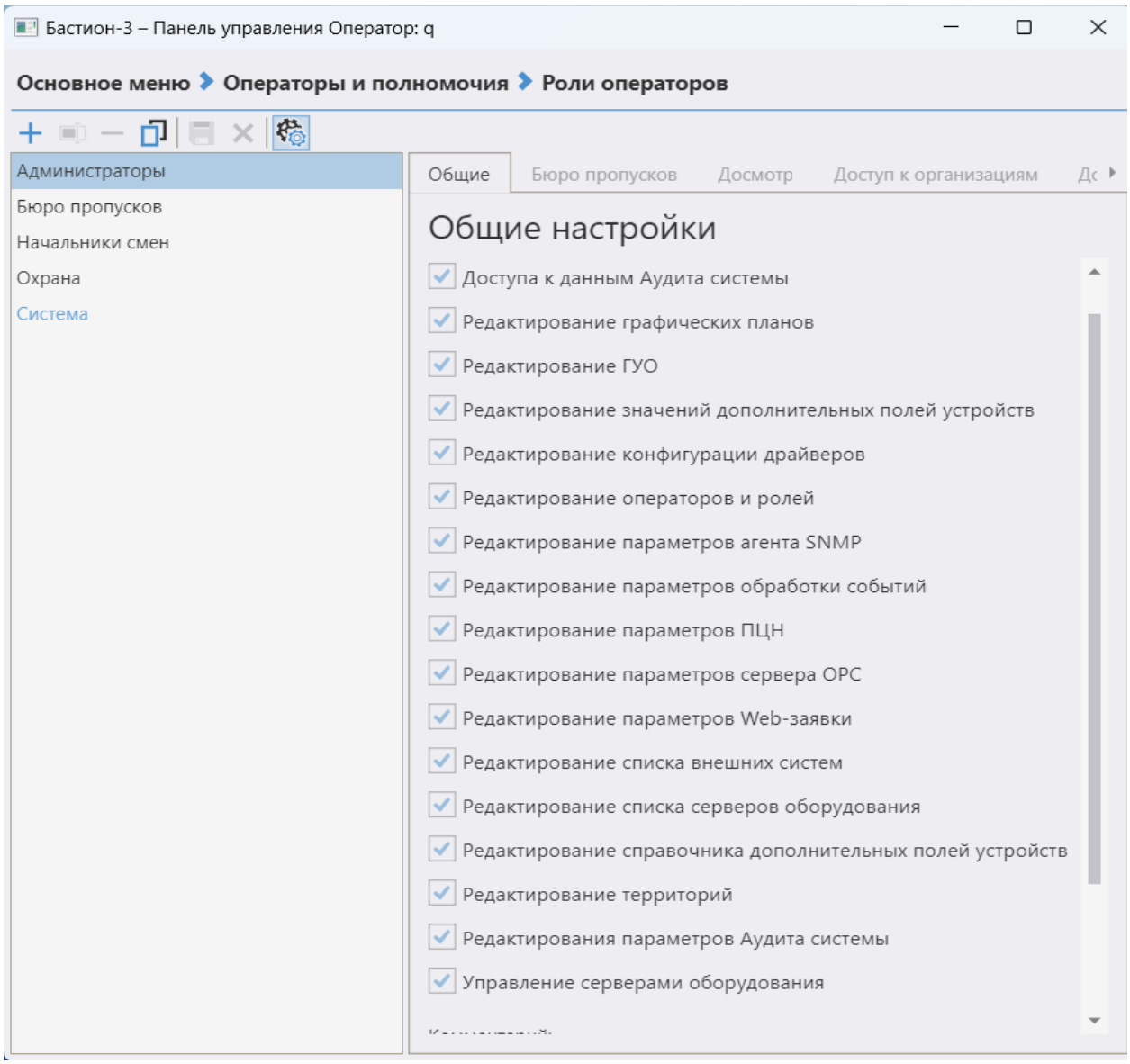

Рис. 27. Окно настройки ролей операторов

По умолчанию в системе доступна роль «Администраторы», которую нельзя редактировать или удалить. Для этой роли доступны все операции в системе.

Пользователь может создать неограниченное число ролей.

В дополнение к стандартным операциям добавления, редактирования и удаления, роль оператора может быть скопирована с сохранением всех настроек. Это позволяет быстро настраивать схожие роли операторов.

Для копирования роли выберите в списке исходную роль и нажмите кнопку « ». В результате будет создана новая роль, идентичная исходной. Необходимо задать новое имя для новой роли, настроить её параметры и сохранить внесённые изменения.

Также, система поддерживает групповую настройку ролей операторов. Для изменения свойств сразу нескольких ролей, следует выбрать их в списке ролей (мышью с использованием кнопок Shift и Ctrl), изменить необходимые свойства и сохранить изменения.

Для каждой роли можно посмотреть, каким операторам назначена выбранная роль (Рис. 28).

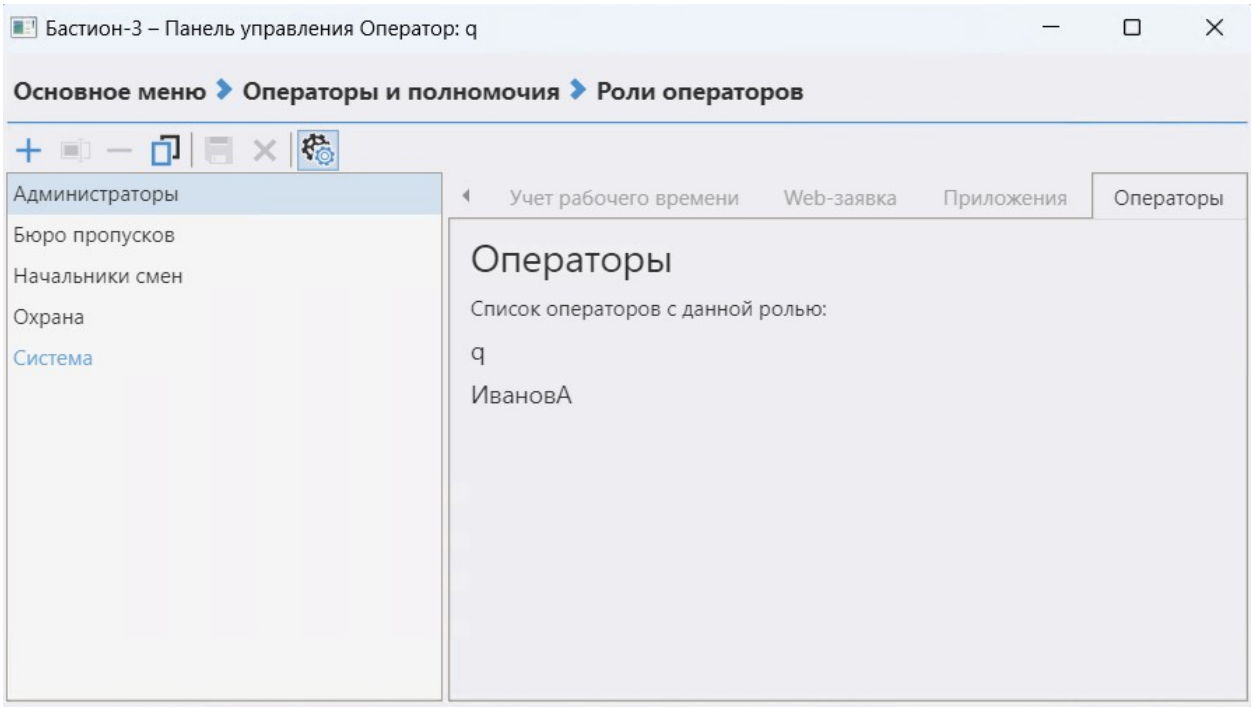

Рис. 28. Список операторов с выбранной ролью

Некоторые страницы, описанные ниже, могут отсутствовать в системе в случае, если соответствующий модуль не установлен.

Кроме обычных ролей операторов, в системе есть системные, технические роли (на текущий момент в системе только одна системная роль «Система», но это может изменится в будущем). Для их просмотра служит кнопка « » на панели инструментов. Часть настроек системных ролей предопределены, часть – доступны для редактирования. Операторами системных ролей являются предустановленные операторы, используемые различными службами системы.

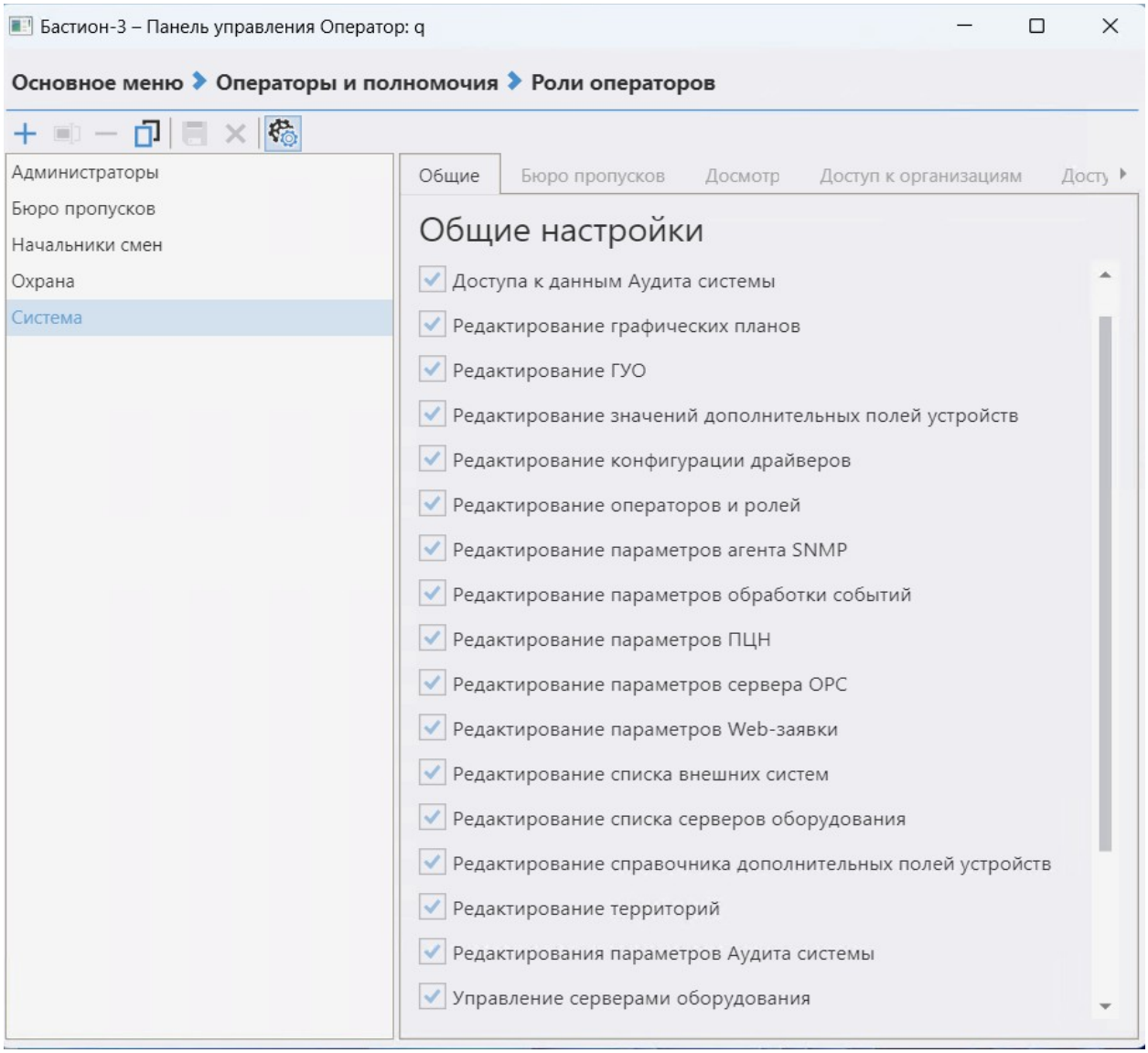

Рис. 29. Отображение системной роли

5.5.4.2. Общие настройки ролей

На вкладке «Общие» можно задать следующие настройки (см. Рис. 29):

Доступ к данным Аудита системы. Определяет, будет ли у операторов с этой ролью возможность просмотра данных журнала аудита системы.

Редактирование графических планов. Определяет, будет ли у роли доступ к редактированию графических планов.

Редактирование ГУО. Определяет, будет ли у роли доступ к редактированию групп управления охраной.

Редактирование значений дополнительных полей устройств. Определяет, будет ли у операторов с этой ролью возможность изменения значений дополнительных полей для устройств системы.

Редактирование конфигурации драйверов. Определяет, будет ли у операторов с этой ролью возможность запускать конфигураторы драйверов.

Редактирование операторов и ролей. Определяет, будет ли у роли доступ к редактированию ролей и операторов системы.

Редактирование параметров агента SNMP. Определяет, будет ли у роли доступ к редактированию параметров агента SNMP.

Редактирование параметров обработки событий. Определяет, будет ли у роли доступ к редактированию параметров обработки событий.

Редактирование параметров ПЦН. Определяет, будет ли у операторов с этой ролью возможность настройки параметров модуля «Бастион-3 — ПЦН».

Редактирование параметров сервера OPC. Определяет, будет ли у роли доступ к редактированию параметров сервера OPC.

Редактирование параметров LDAP. Определяет, будет ли у роли доступ к редактированию параметров аутентификации операторов через LDAP.

Редактирование параметров Веб-заявки. Определяет, будет ли у роли доступ к редактированию настроек модуля «Бастион-3 — Веб-заявка».

Редактирование списка внешних систем. Определяет, будет ли у операторов с этой ролью возможность настройки списка внешних систем.

Редактирование списка серверов оборудования. Определяет, будет ли у роли доступ к редактированию списка серверов оборудования, драйверов, а также возможность управления запуском драйверов.

Редактирование справочника дополнительных полей устройств. Определяет, будет ли у операторов с этой ролью возможность настраивать список используемых дополнительных полей для устройств.

Редактирование территорий. Определяет, будет ли у роли доступ к редактированию территорий.

Редактирование параметров Аудита системы. Определяет, будет ли у операторов с этой ролью возможность настройки параметров Аудита системы.

Управление серверами оборудования. Определяет, будет ли у операторов с этой ролью возможность останавливать и запускать драйверы на серверах оборудования.

5.5.4.3. Настройки роли для модуля «Пост охраны»

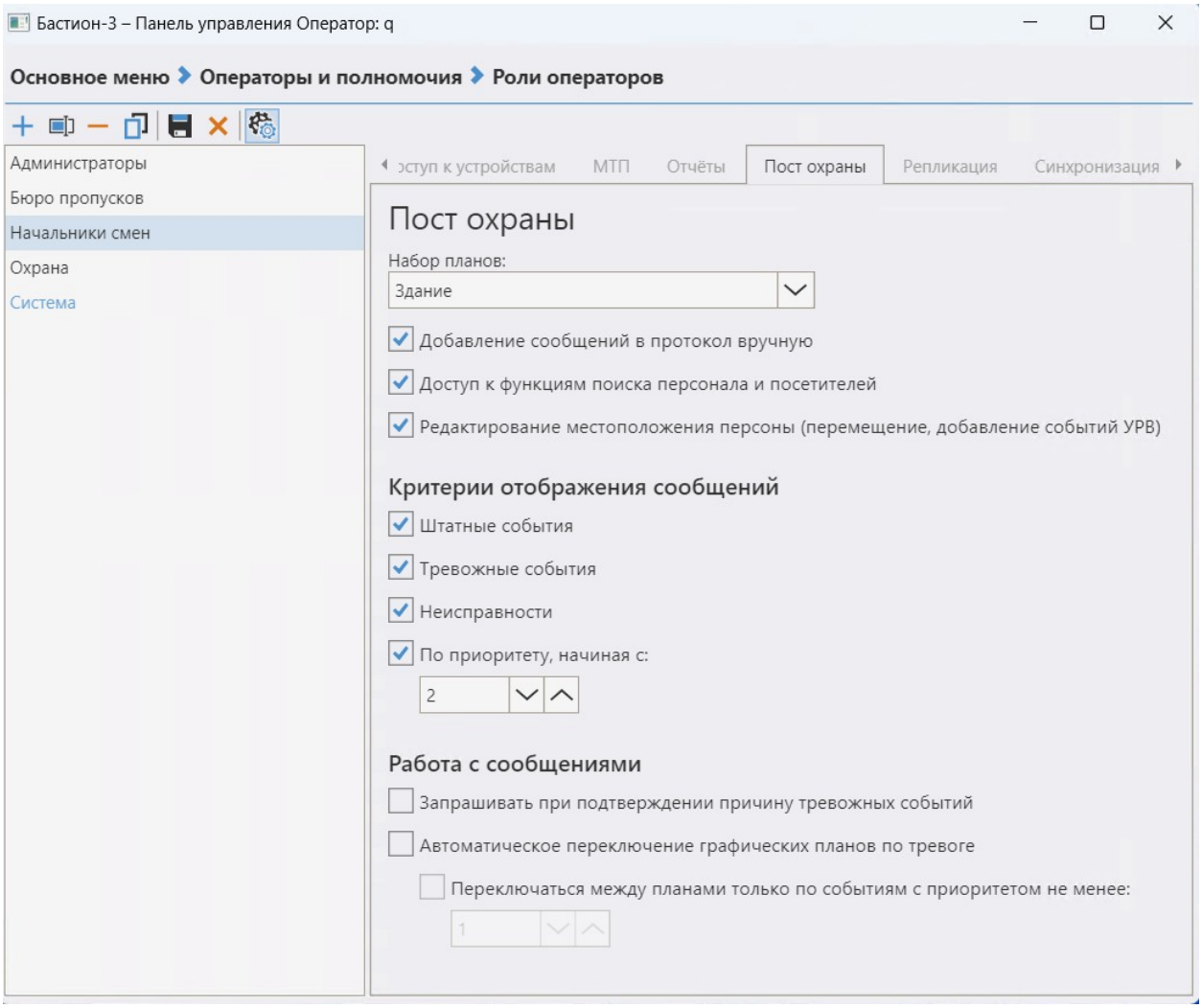

Рис. 30. Настройка роли для модуля «Пост охраны»

На странице «Пост охраны» (Рис. 30) можно задать ряд параметров, которые будут использоваться для выбранной роли оператора в модуле «Бастион-3 – Пост охраны».

Система позволяет определять задать следующие параметры:

Набор планов – позволяет задать для роли используемый набор графических планов.

Добавление сообщений в протокол вручную – позволяет определить, будет ли оператор с выбранной ролью иметь возможность добавлять события в журнал событий вручную.

Доступ к функциям поиска персонала и посетителей – позволяет определить, будет ли оператор с выбранной ролью иметь возможность открывать окна поиска персонала и «Посетители на территории».

Редактирование местоположения персоны – позволяет определить, будет ли оператор с выбранной ролью иметь возможность вручную указывать территорию, на которой находится персона, а также добавлять события УРВ.

Критерии отображения сообщений на основе типа сообщений (штатное, тревожное, неисправность), 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. 30 настройки обеспечивают вывод сообщений для всех событий с приоритетом от 2.

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

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

Переключаться между планами только по событиям с приоритетом не менее – 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.

5.5.4.4. Настройка роли для «Бюро пропусков»

На странице «Бюро пропусков» (Рис. 31) можно задать ряд параметров, которые будут использоваться для выбранной роли оператора в модуле «Бюро пропусков», а также в других приложениях.

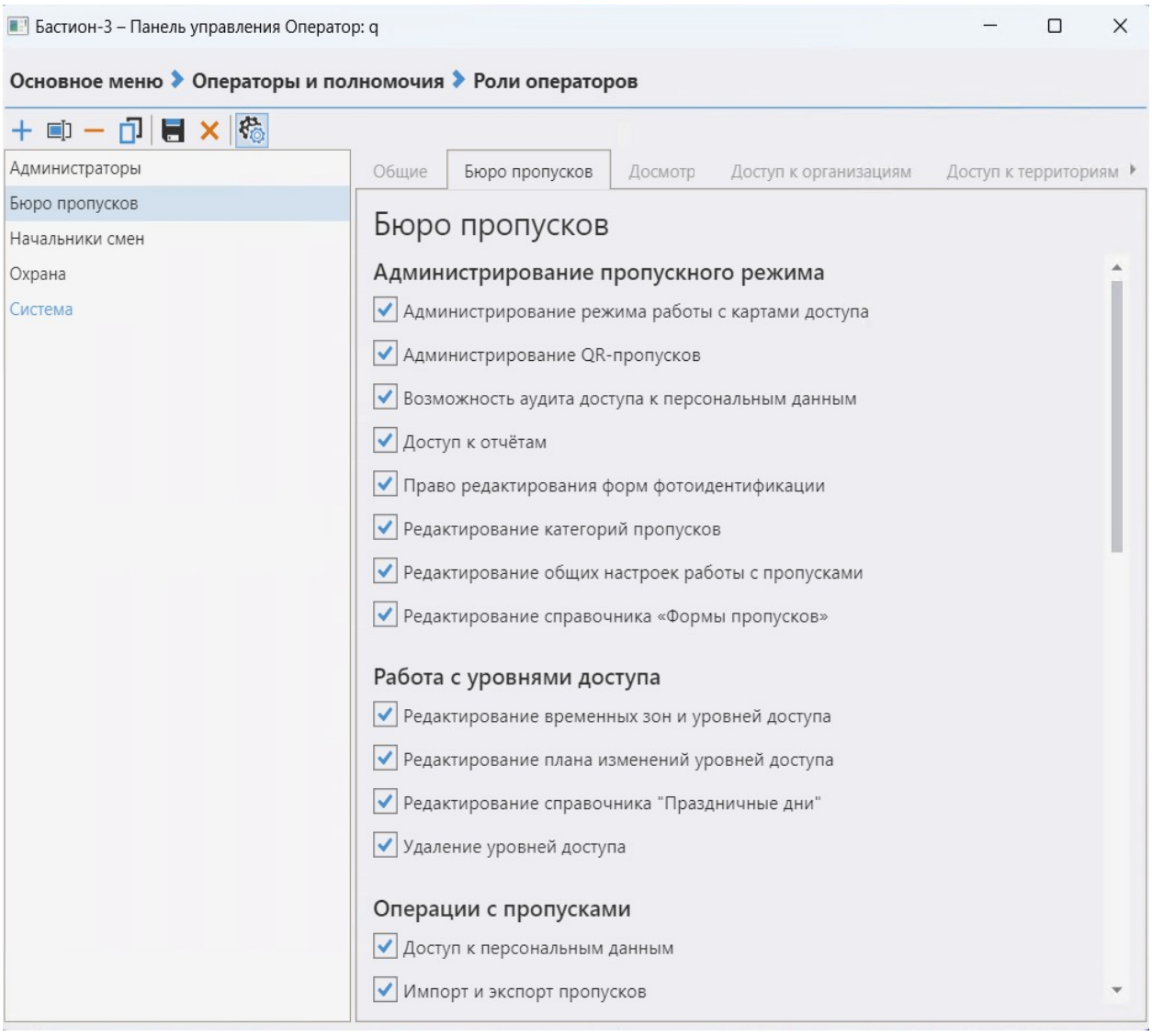

Рис. 31. Настройка роли для «Бюро пропусков»

Система позволяет задать следующие параметры:

Администрирование пропускного режима

Администрирование режима работы с картами доступа – определяет, будет ли оператор с выбранной ролью иметь возможность настраивать параметры работы с картами доступа на странице «Пропускной режим — Параметры — Карты доступа» в панели управления.

Администрирование QR-пропусков – определяет, будет ли оператор с выбранной ролью иметь возможность настраивать параметры работы с QR-пропусками на странице «Пропускной режим — Параметры — QR-пропуска» в панели управления.

Доступ к отчётам – определяет, будет ли оператор с выбранной ролью иметь возможность просмотра отчётов о пропускном режиме. Не влияет на возможность печати пропуска и на доступ к отчётам в модуле «Бастион-3 – Отчёт».

Редактирование категорий пропусков – определяет, будет ли оператор с выбранной ролью иметь возможность редактирования параметров категорий пропусков.

Редактирование общих настроек работы с пропусками – определяет, будет ли оператор с выбранной ролью иметь возможность настройки общих параметров работы с пропусками в модуле «Панель управления».

Работа с уровнями доступа

Редактирование временных зон и уровней доступа – позволяет определить, будет ли оператор с выбранной ролью иметь возможность редактирования набора и содержимого уровней доступа и временных зон.

Редактирование плана изменения уровней доступа – позволяет определить, будет ли оператор с выбранной ролью иметь возможность создавать задания на изменения уровня доступа для пропусков, которые должны выполняться в будущем.

Редактирование справочника «Праздничные дни» – позволяет определить, будет ли оператор с выбранной ролью иметь возможность редактирования специальных дней в системе.

Операции с пропусками

Доступ к персональным данным – определяет, будет ли оператор с выбранной ролью иметь возможность просмотра и редактирования персональных данных, включающих дату и место рождения, паспортные данные, контактные данные персоны. Полномочие действует на всю систему в целом, то есть, если у оператора его нет – он не сможет увидеть перечисленные персональные данные нигде в системе.

Импорт и экспорт пропусков – определяет, будет ли оператор с выбранной ролью иметь возможность импорта и экспорта пропусков в/из системы.

Право на изменение статуса пропуска – определяет, будет ли оператор с выбранной ролью иметь возможность выполнять операции выдачи, возврата, изъятия, продления, блокировки и разблокировки пропусков.

Право получать / продлевать согласие на обработку персональных данных – определяет, будет ли оператор с выбранной ролью иметь возможность выполнить операцию получения согласия на обработку ПД или продлить действие этого согласия.

Редактирование даты окончания действия пропусков – если отключено, оператор не будет иметь возможности вручную установить срок действия выдаваемых пропусков. Этот срок, в таком случае, будет определяться на основе правил обработки категорий пропусков.

Редактирование пропусков в архиве – определяет, будет ли оператор с выбранной ролью иметь возможность редактирования пропусков со статусом «возвращён» и «изъят». Следует иметь в виду, что если для одной персоны имеется и заявка, и пропуск в архиве, то изменение персональных данных в заявке приведёт к изменению отображаемых сведений о персоне и для архивных пропусков.

Редактирование свойств пропусков – определяет, будет ли оператор с выбранной ролью иметь возможность редактирования свойств пропуска и персоны.

Удаление пропусков – определяет, будет ли оператор с выбранной ролью иметь возможность удалять пропуска из системы.

Доступные категории пропусков – эта группа параметров определяет, пропуска каких категорий сможет создавать оператор с выбранной ролью. При добавлении категории необходимо указать роли операторов, которые смогут работать с новой категорией.

Дополнительные операции с пропусками

Назначение группы управления охраной – определяет, будет ли оператор с выбранной ролью иметь возможность назначать группу управления охраной для пропусков. Если запрещено, группа управления охраной будет устанавливаться системой на основе правил для категорий пропусков.

Право на внесение биометрических данных – определяет, будет ли оператор с выбранной ролью иметь возможность вносить биометрические данные в систему.

Просмотр и редактирование PIN-кода – определяет, будет ли оператор с выбранной ролью иметь возможность просматривать и назначать PIN-код пропуска.

Редактирование профилей персонала – определяет, будет ли оператор с выбранной ролью иметь возможность назначать профили СКУД для пропусков. Если запрещено, профиль будет устанавливаться системой на основе правил для категорий пропусков.

Редактирование справочников

Отдельно для каждого справочника можно установить, может ли оператор с выбранной ролью его редактировать. Если отключено, оператор сможет только выбирать значения из введённых в систему ранее. Список доступных справочников:

1. Дополнительные поля для персон.
2. Карты доступа. Если отключено, список карт доступа должен быть внесён в систему предварительно. У оператора будет возможность только выбрать карту доступа из имеющихся в системе.
3. Виды документов.

4. Гражданство.
5. Должности.
6. Кем выдан документ.
7. Причины блокировки.
8. Причины возврата пропуска.
9. Цель посещения.

5.5.4.5. Настройка прав доступа к организациям

На странице «Доступ к организациям» формы настройки роли оператора можно задать все права доступа к организационной структуре системы.

Для установки ограничений выберите роль оператора в списке слева и подразделение в средний части (см. Рис. 32). В правой части окна будет отображён список доступных разрешений для выбранного подразделения.

При настройке поддерживается возможность выбирать одновременно несколько ролей операторов и несколько организаций/подразделений (см. Рис. 32). Разрешения, которые даны не для всех выбранных ролей и устройств, будут отображены как « ».

Для всех организаций и подразделений предусмотрен следующий набор прав:

Просмотр событий и сотрудников – определяет, будет ли оператор с выбранной ролью иметь возможность просмотра событий с участием сотрудников выбранного подразделения, а также и списка сотрудников подразделения в системе.

Редактирование (название и внутренняя структура) – определяет, будет ли оператор с выбранной ролью иметь возможность редактировать название организации/подразделения, а также изменять дочерние организации/подразделения.

Редактирование списка сотрудников в подразделении – определяет, будет ли оператор с выбранной ролью иметь возможность назначать выбранное подразделение для пропусков.

При добавлении новой организации или подразделения для них устанавливаются такие же полномочия как у родительской организации или подразделения.

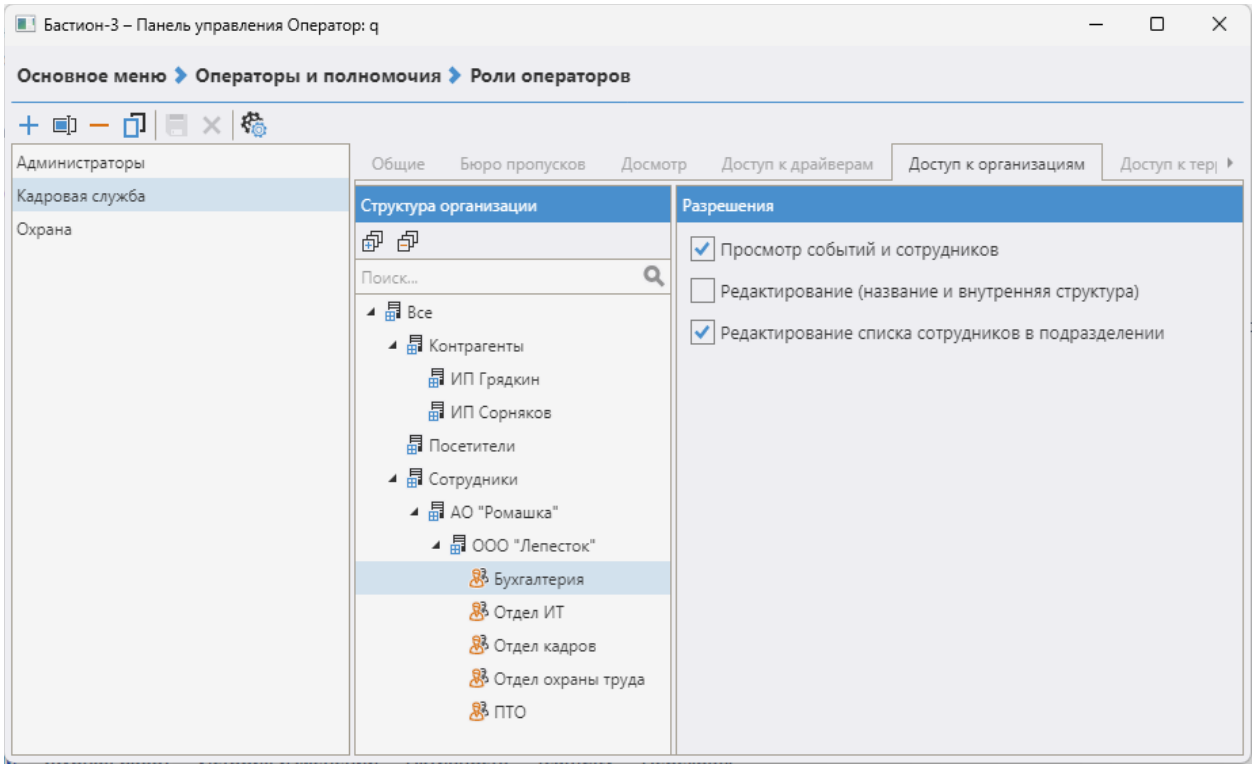

Рис. 32. Настройка прав доступа к организациям и подразделениям

5.5.4.6. Настройка прав доступа к территориям

На странице «Доступ к территориям» формы настройки роли оператора можно задать разграничение прав к территориям, которое будет использоваться при настройке уровней доступа.

Оператор сможет включать в уровень доступа только те территории и устройства, на которые у него есть права. Например, если считыватель является входным для территории «Цех 1», то оператор сможет включить этот считыватель в уровень доступа только, если у него есть право доступа к территории «Цех 1». При этом учитываются только входные считыватели. То есть, если «Считыватель 1» ведет из территории «Вся территория» в «Цех 1», а «Считыватель 2» - в обратном направлении, и у оператора есть право на доступа к территории «Вся территория» и нет права доступа к территории «Цех 1», то оператор сможет включить в уровень доступа «Считыватель 2», но не сможет включить «Считыватель 1».

5.5.4.7. Настройка прав доступа к устройствам

На странице «Доступ к устройствам» формы настройки роли оператора можно задать все права доступа к устройствам системы.

Для установки ограничений выберите роль оператора в списке слева и устройство в средний части (см. Рис. 33). В правой части окна будет отображён список доступных разрешений для выбранного устройства.

При настройке поддерживается возможность выбирать одновременно несколько ролей операторов и несколько однотипных устройств (см. Рис. 33). Разрешения, которые даны не для всех выбранных ролей и устройств, будут отображены как « ».

Дерево устройств может быть отображено в двух видах – по типу ( ) и по подключению (– отображать структуру устройств).

Группировка устройств по типу облегчает массовую работу с однотипными устройствами – для изменения доступа ко всем устройствам типа «Раздел» развернуть узел «Разделы» и выделить все его дочерние элементы, после чего можно выбрать требуемые разрешения.

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

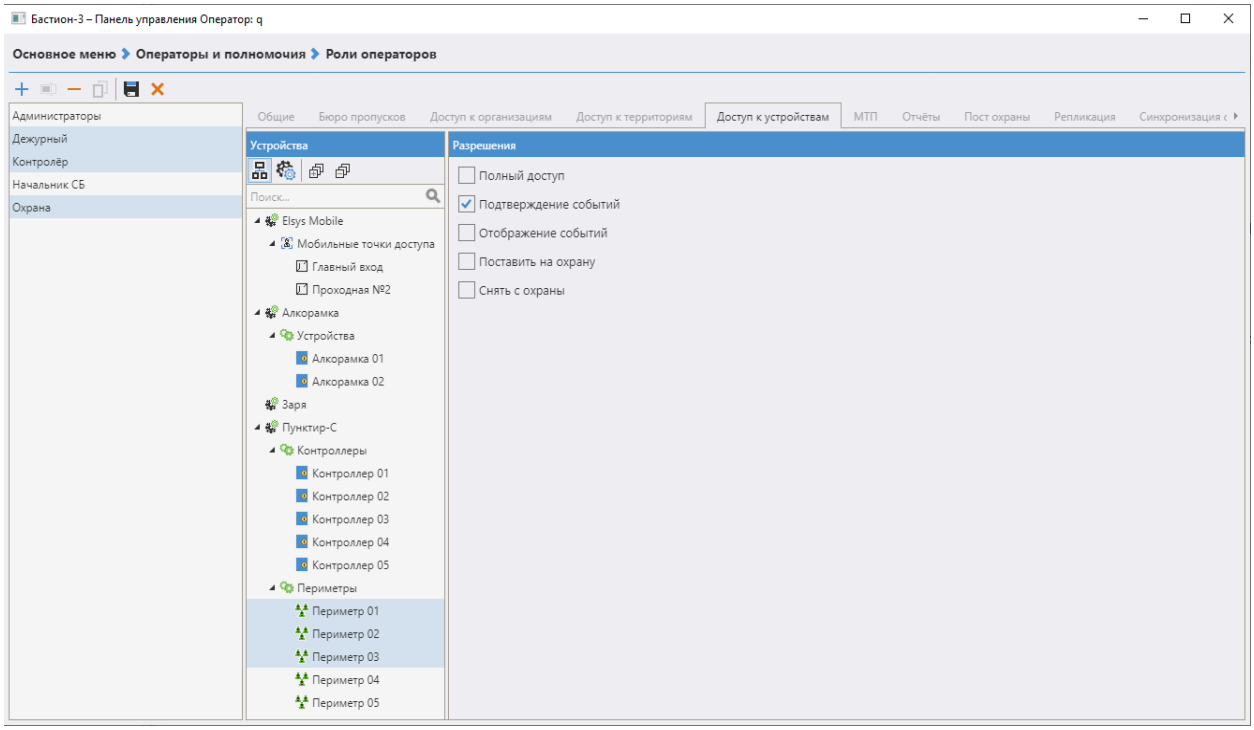

Рис. 33. Настройка прав доступа к устройствам

Содержимое списка разрешений зависит от типа выбранного устройства и драйвера. Набор разрешений, как правило, соответствует контекстному меню пиктограмм устройства, а также включает право на настройку прав доступа к устройству.

Для всех элементов доступны следующие разрешения:

Полный доступ – разрешает все операции с устройством.

Подтверждение событий – разрешает операторам с выбранной ролью подтверждать тревожные события от выбранных устройств.

Отображение событий – разрешает вывод событий от выбранных устройств для операторов с выбранной ролью. Это право влияет и на вывод событий в модуле «Пост охраны», и на отображение событий в отчётах, и распространяется на любые другие случаи, когда оператор запрашивает у системы список событий.

> ***Внимание!*** *При добавлении новых устройств в систему, изначально все действия с ними будут разрешены для роли, под которой добавили устройство, а также для роли «Администраторы».*

5.5.4.8. Права на работу с материальными и транспортными пропусками

На странице «МТП» можно настроить права ролей операторов на работу с материальными и транспортными пропусками. Доступны следующие параметры:

Настройка общих параметров работы с МТП — определяет возможность для роли оператора редактировать параметры обработки в системе материальных и транспортных пропусков.

Редактирование справочника материальных ценностей — определяет возможность для роли оператора редактировать справочник материальных ценностей.

Редактирование справочника автотранспорта — определяет возможность для роли оператора редактировать справочник автотранспорта.

Для материальных пропусков есть возможность задать следующие права для роли операторов:

- Возможность редактировать заявки;
- Возможность редактировать выданные пропуска;
- Возможность удалять пропуска;
- Право на изменение статуса пропуска;
- Право на редактирование даты окончания действия пропуска.

Для транспортных пропусков есть возможность задать следующие права для роли операторов:

- Возможность редактировать заявки;
- Возможность редактировать выданные пропуска и прикрепленные транспортные средства;
- Возможность удалять пропуска;
- Право на изменение статуса пропуска;
- Право на редактирование даты окончания действия пропуска;
- Возможность редактирования списка дополнительных полей транспортных пропусков;
- Возможность редактирования значения дополнительных полей транспортных пропусков.

5.5.4.9. Права на доступ к отчётам

Система предоставляет возможность установить права для ряда параметров генератора отчётов (Рис. 34).

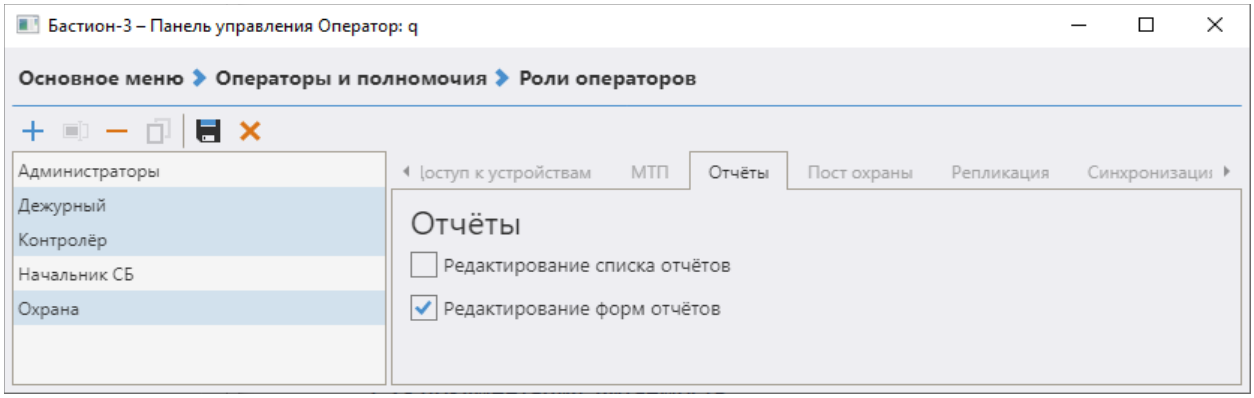

Рис. 34. Редактирование прав на доступ к отчётам

Редактирование списка отчётов – определяет, может ли оператор с выбранной ролью создавать свои виды отчётов или изменять имеющиеся.

Редактирование форм отчётов – определяет, может ли оператор с выбранной ролью изменять формы для печати отчётов.

5.5.4.10. Права для системы синхронизации пропусков с LDAP

На странице «Синхронизация с LDAP» есть возможность задать следующие права, используемые модулем «Бастион-3 — LDAP» для синхронизации списка пропусков с LDAP:

Редактирование настроек — определяет, сможет ли оператор с выбранной ролью изменять настройки подключения и синхронизации с LDAP.

Ручной запуск синхронизации — определяет, сможет ли оператор с выбранной ролью вручную запускать процедуру синхронизации с LDAP.

5.5.4.11. Права на группы управления охраной

На странице «Управление охраной» для каждой роли операторов можно указать набор групп управления охраной (ГУО), который они смогут использовать для назначения пропускам. Если у роли оператора нет прав на группу управления охраной, то оператор с этой ролью не сможет назначать эту ГУО для пропусков.

5.5.4.12. Права для системы учёта рабочего времени

На странице «УРВ» для каждой роли операторов можно указать права для доступа к функциям системы учёта рабочего времени. Доступен следующий набор прав:

Редактирование графиков сменности — определяет, сможет ли оператор настраивать графики сменности.

Редактирование списка и параметров отчётов — определяет, сможет ли оператор изменять набор и параметры отчётов.

Отладка отчётов — определяет, сможет ли оператор изменять шаблоны печатных форм отчётов.

Редактирование общих параметров — определяет, сможет ли оператор изменять общие настройки системы учёта рабочего времени.

Редактирование рабочих дней — определяет, сможет ли оператор изменять параметры рабочих дней, используемых для построения графиков сменности.

Редактирование справочника "Типы рабочих дней" — определяет, сможет ли оператор изменять справочник типов рабочих дней, используемых в системе.

Добавление записей учета рабочего времени вручную — определяет, сможет ли оператор вручную добавлять события входов и выходов в систему учёта рабочего времени.

Редактирование трудовых договоров — определяет, сможет ли оператор изменять трудовые договора сотрудников, используемые в системе учёта рабочего времени.

Редактирование специальных дней — определяет, сможет ли оператор создавать и управлять исключениями из обычного режима работы (специальные дни).

Право формировать события УРВ на основе основного протокола событий — определяет, сможет ли оператор выполнять операцию переформирования событий учёта рабочего времени на основе основного протокола событий системы.

Формирование отчётов — определяет, сможет ли оператор формировать отчёты по учёту рабочего времени.

Создание назначенных заданий на формирование отчётов — определяет, сможет ли оператор создавать задания на формирование отчётов УРВ по расписанию.

5.5.4.13. Настройки Веб-заявки

На странице «Веб-заявка» можно задать настройки, которые будут использоваться для выбранных ролей операторов при работе с модулем «Бастион-3 — Веб-заявка». Настройки, задаваемые на этой странице, влияют на внешний вид страниц Веб-заявки и на значения, используемые в ней по умолчанию. При работе с веб-заявкой применяются все права, заданные на доступ к организациям / подразделениям, устройствам, территориям и прочие применимые права.

Общие параметры настройки роли для веб-заявки включают:

Категория пропуска по умолчанию — задает категорию, которая будет использоваться при создании новых заявок через систему «Веб-заявка» по умолчанию.

Организация по умолчанию — задает организацию, которая будет использоваться при создании новых заявок через систему «Веб-заявка» по умолчанию.

Также, здесь можно установить следующие параметры работы с материальными и транспортными пропусками:

- Отображать заявки на транспортные пропуска;
- Отображать заявки на материальные пропуска;
- Подразделение назначения для материального пропуска по умолчанию (куда предназначаются материальные ценности);
- Установить право на внос по умолчанию (для новых материальных пропусков это право будет установлено по умолчанию);

- Установить право на вынос по умолчанию (для новых материальных пропусков это право будет установлено по умолчанию).

Отдельно можно установить видимость полей в интерфейсе веб-заявки.

Для персонального пропуска задается видимость следующих полей: табельный номер, организация / подразделение, должность, уровень доступа, фотография, фотография с паспортом в руках, категория пропуска, PIN-код, приоритет, тип документа, серия документа, номер документа, кем выдан документ, дата выдачи документа, дата рождения, место рождения, адрес проживания, гражданство, телефон, электронная почта, пол.

Для транспортного пропуска задается видимость следующих полей: фотография, модель, описание, год выпуска, цвет, вес, версия (кузов), владелец, тип.

Для материального пропуска задается видимость следующих полей: на внос, на вынос, организация назначения, количество, вес (кг), объем (л), номер доверенности, кем выдана доверенность, номер накладной, кем выдана накладная, № вет. Свидетельства, номер разнарядки, куда предназначается.

Также, если в системе настроены дополнительные поля, можно разграничить и их видимость в веб-заявке.

5.5.4.14. Права на приложения

Вкладка «Приложения» (Рис. 35) служит для настройки прав запуска приложений системы.

Право доступа к системе через мобильный клиент – определяет, будет ли у оператора с выбранной ролью возможность доступа к системе через мобильные приложения.

Право доступа к системе через WebAPI

Право доступа к системе «Веб-заявка» – определяет, будет ли у оператора с выбранной ролью возможность доступа к системе «Бастион-3 – Веб-заявка».

Право запуска приложения «Аудит системы»

Право запуска приложения «Бюро пропусков» – определяет, может ли оператор с выбранной ролью осуществлять вход в модуль «Бастион-3 – Бюро пропусков».

Право запуска приложения «Монитор состояния»

Право запуска приложения «Отчёт» – определяет, может ли оператор с выбранной ролью осуществлять вход в модуль «Бастион-3 – Отчёт».

Право запуска приложения «Панель управления» – позволяет разрешить, либо запретить вход пользователя с соответствующей ролью в приложение «Бастион-3 – Панель управления».

Право запуска приложения «Пост охраны» – позволяет разрешить, либо запретить вход пользователя с соответствующей ролью в приложение «Бастион-3 – Пост охраны».

Право запуска приложения «Учет рабочего времени» – позволяет разрешить, либо запретить вход пользователя с соответствующей ролью в приложение «Бастион-3 – Учет рабочего времени».

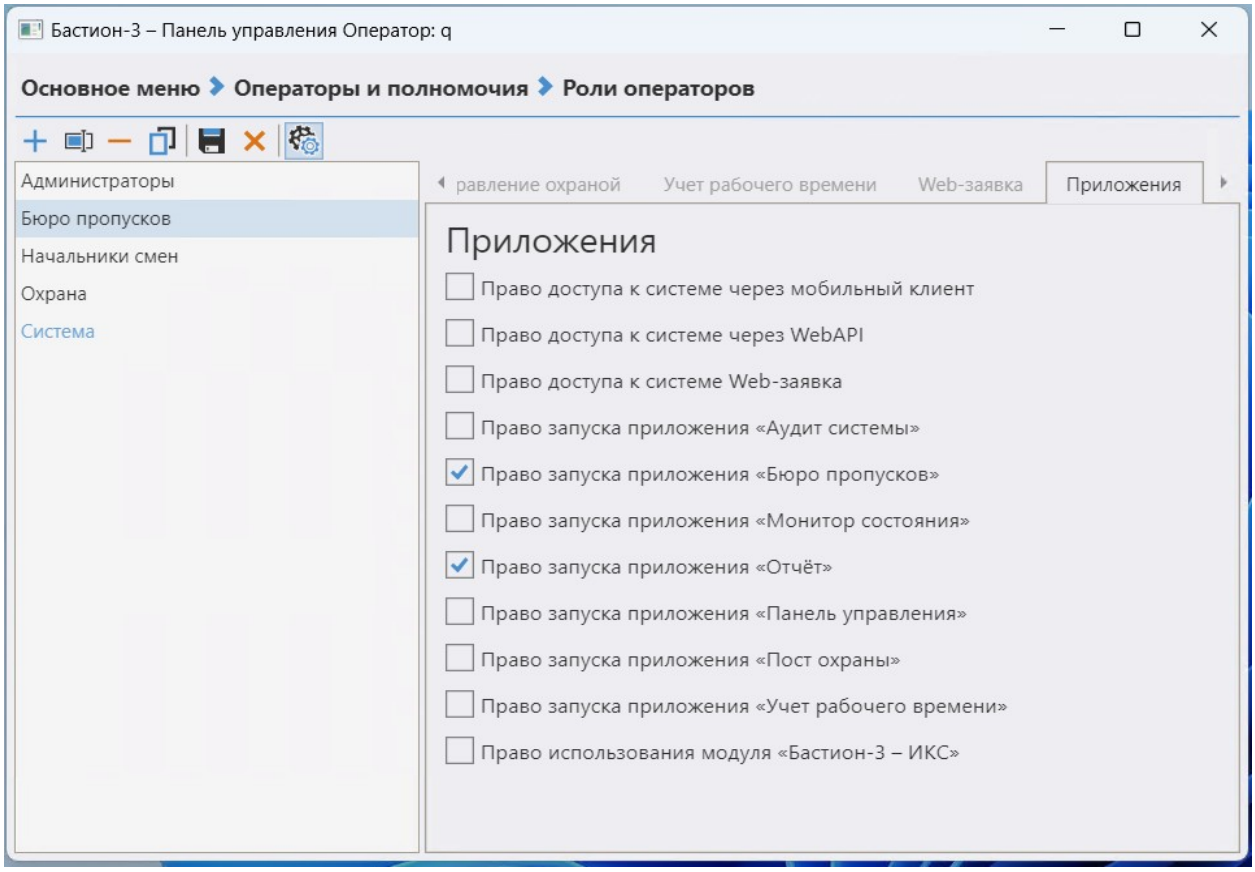

Рис. 35. Настройка прав доступа к приложениям

Право использования модуля «Бастион-3 – ИКС» – позволяет разрешить, либо запретить логин от имени пользователя с данной ролью через API «Бастион-3 – ИКС».

5.5.4.15. Разграничение доступа к пропускам, категориям и подразделениям

Права оператора с заданной ролью на выполнение различных операций с персональными пропусками определяются целым рядом полномочий:

1. Общесистемные полномочия в группе «Операции с пропусками» (см. п. 5.5.4.4.).
2. Полномочия на организации и подразделения (см. п. 5.5.4.5.).
3. Полномочия на редактирование пропусков в категориях (см. п. 5.5.4.4.).

Кроме того, для каждого подразделения могут быть настроены ограничения — какие категории пропусков могут быть там созданы (см. п. 2.2.4 документа «Бастион-3 — Бюро пропусков. Руководство оператора»).

Оператор получит доступ к выполнению конкретной операции только в том случае, если по всем перечисленным критериям он имеет доступ к её выполнению.

При этом следует учитывать, что при создании новых сущностей (категорий пропусков, подразделений) следует проверять настройки доступа к ним. По умолчанию, доступ к новым сущностям получат операторы с ролью того, кто создал сущность, и администраторы системы.

5.5.5. Параметры отображения расширенных сообщений

Параметры вывода расширенных сообщений о событиях задаются непосредственно в приложении «Пост охраны» ПК «Бастион-3» (Рис. 36).

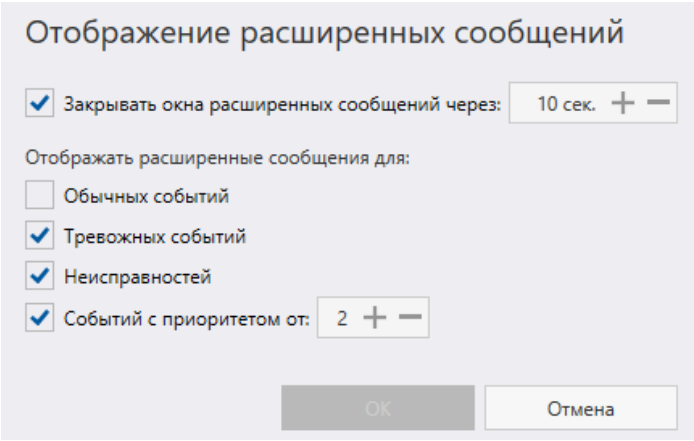

Рис. 36. Настройка параметров отображения расширенных сообщений

Окна расширенных сообщений (Рис. 37) предназначены для привлечения внимания оператора к особо важным сообщениям.

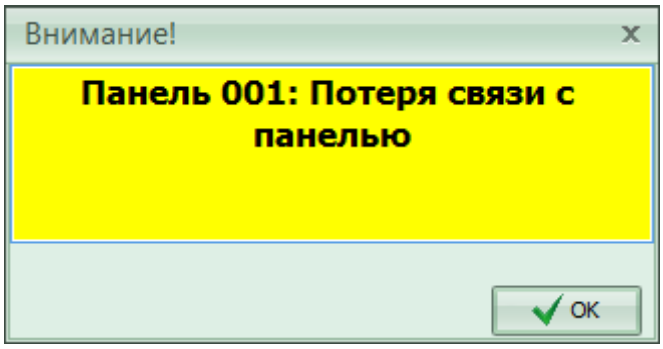

Рис. 37. Окно расширенного сообщения

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

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

5.5.6. Политики безопасности и авторизация через LDAP

5.5.6.1. Настройка политик безопасности

Для настройки политик безопасности паролей операторов следует в модуле «Панель управления» открыть форму «Операторы и полномочия – Политики безопасности» (Рис. 38).

На текущий момент на странице «Общие параметры» для встроенных политик безопасности доступна одна настройка:

Минимальная длина пароля оператора. Система проверяет длину пароля оператора при его изменении. Можно ввести значения от 1 до 20, по умолчанию 1.

5.5.6.2. Настройка авторизации LDAP

ПК «Бастион-3» позволяет использовать службу Active Directory или любой другой сервер LDAP (например, OpenLDAP) для идентификации пользователей. Настройка этой функции производится в панели управления на форме «Операторы и полномочия – Политики безопасности — Авторизация LDAP» (см. Рис. 38).

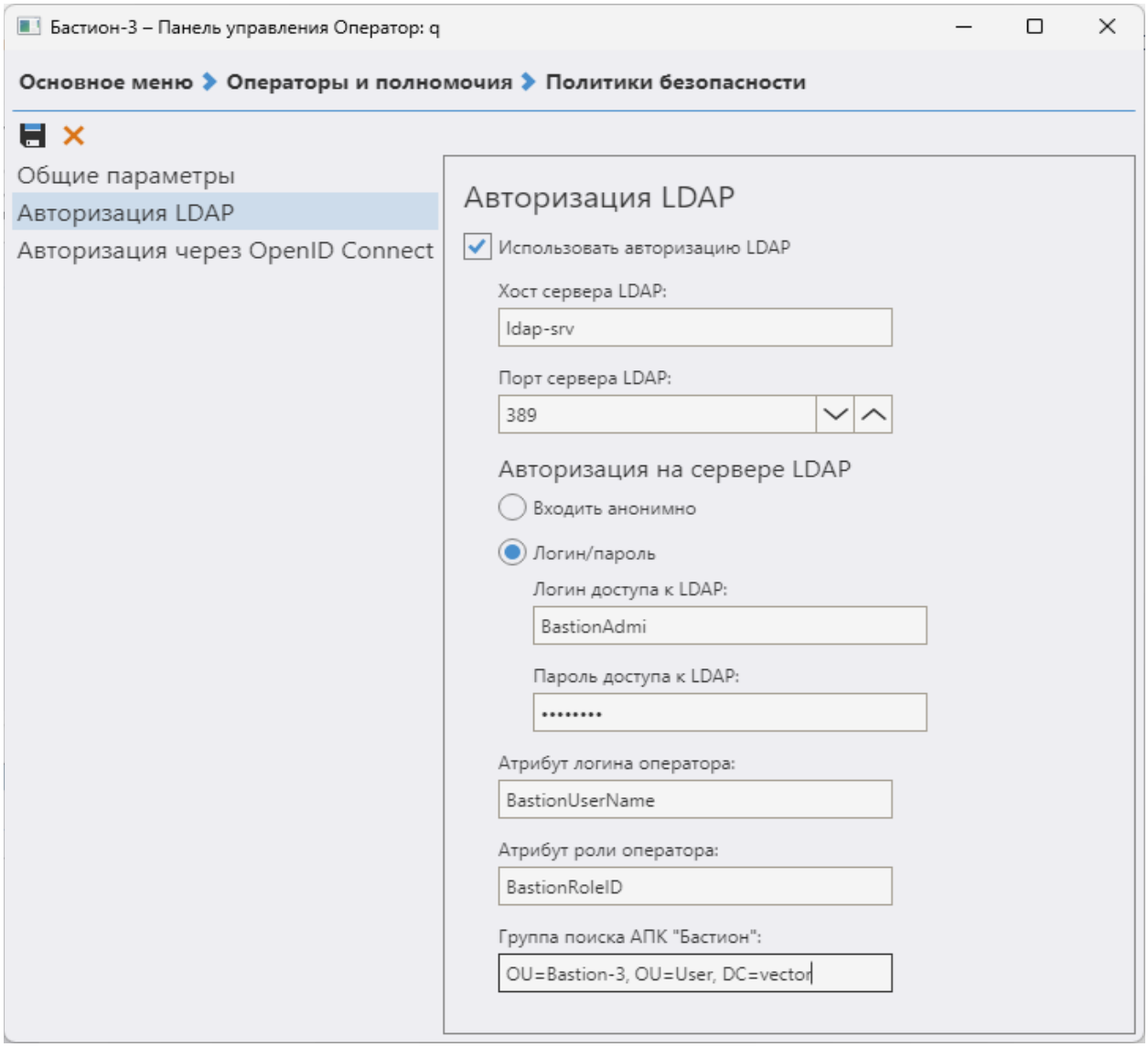

Рис. 38. Настройка политик безопасности и параметров авторизации LDAP

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

При установленном флаге активируются следующие опции:

Хост сервера LDAP – адрес сервера авторизации LDAP.

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

Логин доступа к LDAP – уникальное имя записи в каталоге LDAP, под которой будет производиться поиск.

Пароль доступа к LDAP – пароль для доступа.

Опция «*Входить анонимно*» может быть выбрана, 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 «*Атрибут логина оператора*» должно содержать название атрибута, где в свойствах пользователя в AD должен храниться логин оператора ПК «Бастион-3». Выбранный атрибут должен быть текстовым.

Поле «*Атрибут роли оператора*» должно содержать название атрибута, где в свойствах пользователя в AD должно храниться название роли оператора ПК «Бастион-3». Профиль в этом поле в свойствах пользователя LDAP должен соответствовать роли, существующей в ПК «Бастион-3». Выбранный атрибут должен быть текстовым.

Поле «*Группа поиска ПК «Бастион-3»*» должно содержать уникальное имя записи каталога LDAP, в которую входят пользователи ПК «Бастион-3».

5.5.6.3. Алгоритм работы авторизации LDAP

Если установлен флаг опции «Использовать идентификацию LDAP», то в момент ввода логина и пароля ПК «Бастион-3» проверяет, существует ли пользователь с именем, равным имени пользователя LDAP, в ПК «Бастион-3». Далее происходит анализ:

1) Если пользователь в LDAP имеет верную пару логин-пароль, а также заполненные атрибуты, позволяющие ему использовать ПК «Бастион-3», но в ПК «Бастион-3» данные о нём отсутствуют – этот пользователь добавляется в ПК «Бастион-3». Окно ввода пароля не появляется, блокировка ПК «Бастион-3» – отключается.

2) Если пользователь в LDAP имеет верную пару логин-пароль, а также заполненные атрибуты, не позволяющие ему пользоваться ПК «Бастион-3», а в ПК «Бастион-3» данные о нём отсутствуют – этот пользователь добавляется в ПК «Бастион-3», появляется окно ввода логина и пароля, опция блокировки АПК «Бастион» – включена.

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

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

5.5.6.4. 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. 39).

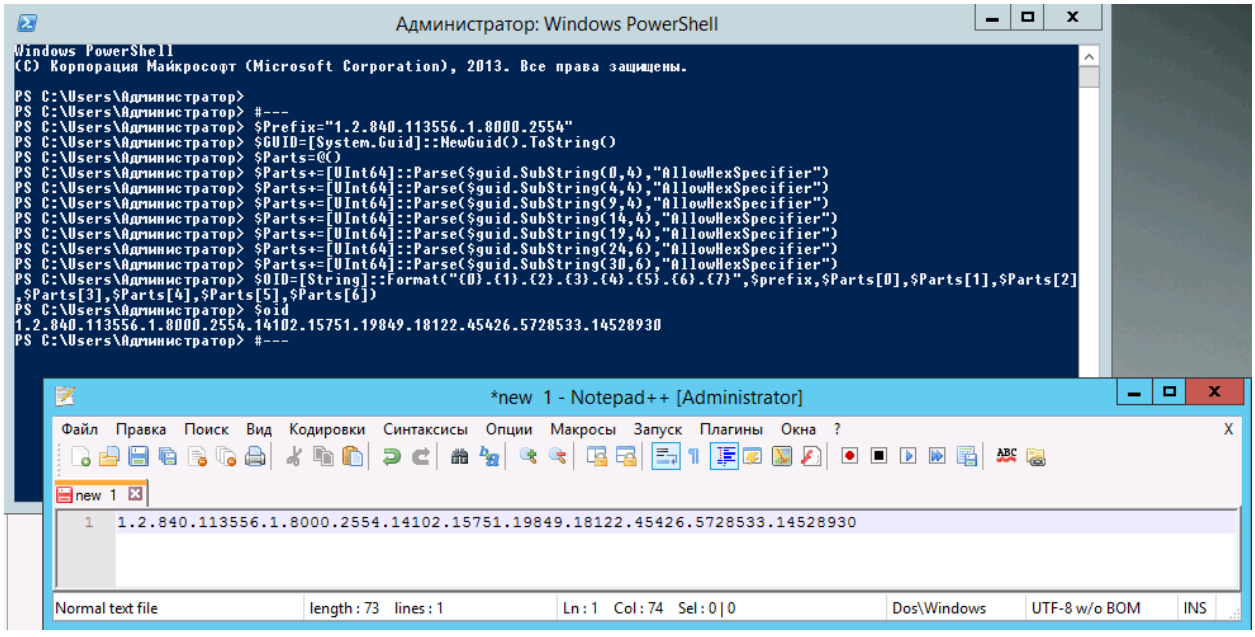

Рис. 39. Генерация X.500 OID

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. 40).

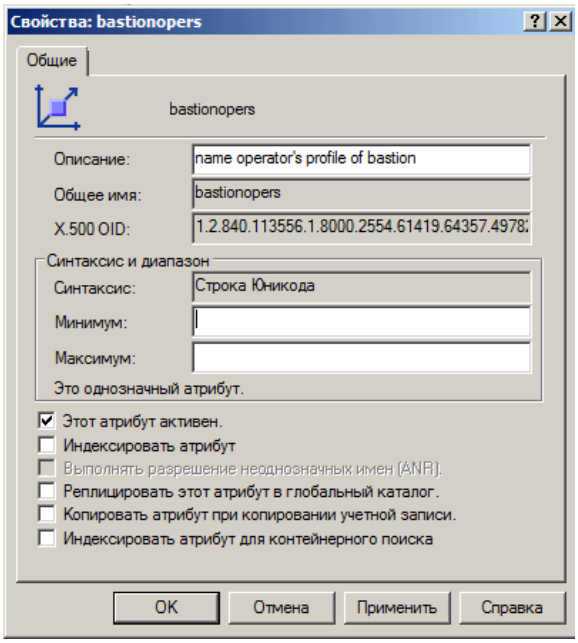

Рис. 40. Добавление атрибута bastionopers

Затем следует добавить атрибут в класс **user**. Для этого в оснастке «Схема Active Directory» можно перейти в раздел **Classes (Классы) (Рис. 41)**.

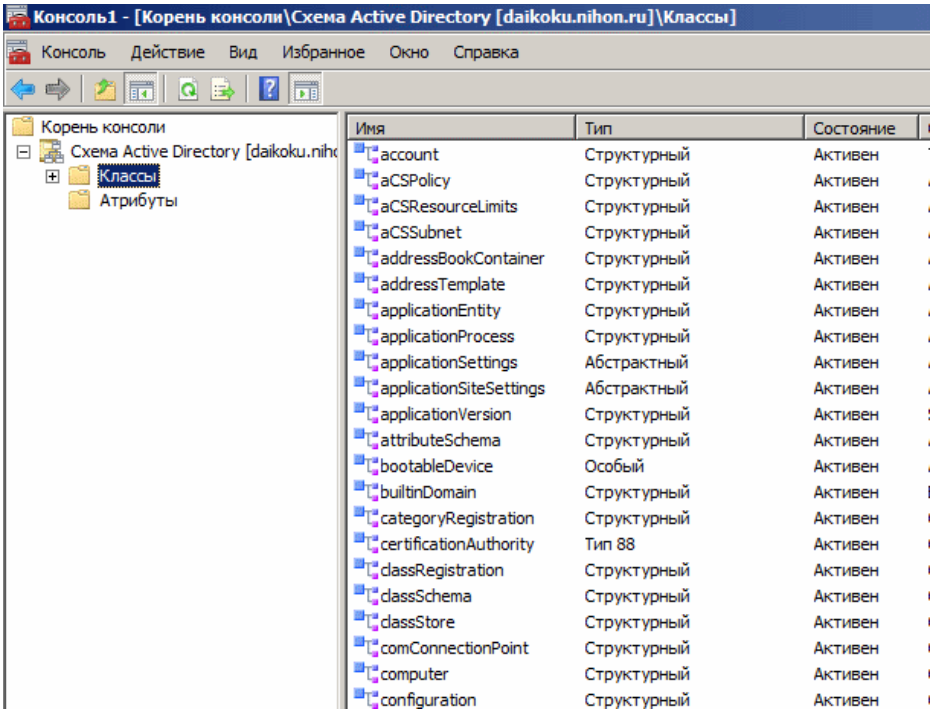

Рис. 41. Раздел "Классы" схемы Active Directory

В свойствах класса **user** необходимо перейти на закладку **Attributes (Атрибуты)** и там добавить новый атрибут класса (Рис. 42).

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.*

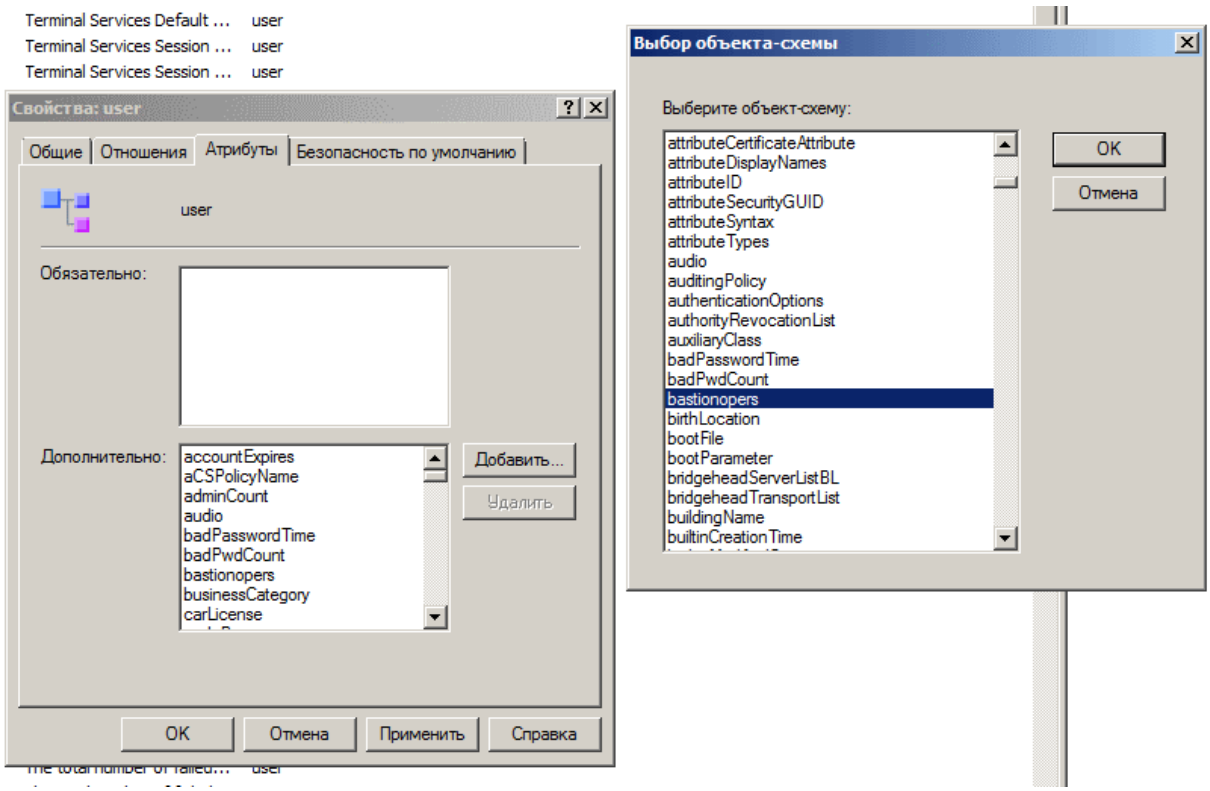

Рис. 42. Атрибуты класса user

5.5.6.5. Настройка идентификации пользователя Active Directory для ПК «Бастион-3»

Для настройки идентификации пользователей Active Directory для ПК «Бастион-3» 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 ПК «Бастион-3», 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 ПК «Бастион-3» с учетной записью AD (закладка member of в свойствах пользователя, см. Рис. 43).

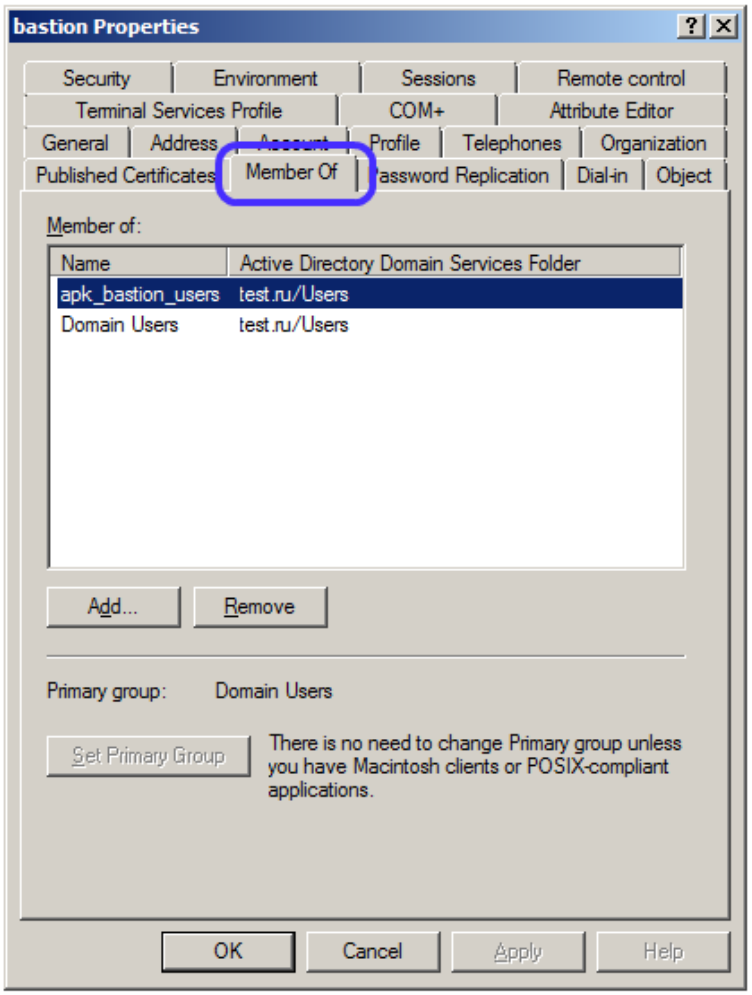

Рис. 43. Настройка членства в группах для пользователя ПК «Бастион-3»

Если в свойствах пользователя отображается закладка attribute editor (см. Рис. 44), то следует найти в списке атрибутов пользователя атрибут, заранее созданный для хранения роли пользователя ПК «Бастион-3». После чего необходимо присвоить атрибуту, предназначенному для хранения роли (созданного в ПК «Бастион-3») оператора ПК «Бастион-3» символьное значение, совпадающее с именем роли.

Если таких атрибутов нет, то следует найти любой незанятый атрибут, который принимает **символьные значения** (например, sn). Это будет атрибут для хранения роли оператора ПК «Бастион-3». Присвоить этому атрибуту символьное значение, совпадающее с именем роли ПК «Бастион-3», созданной в ПК «Бастион-3» для пользователей AD.

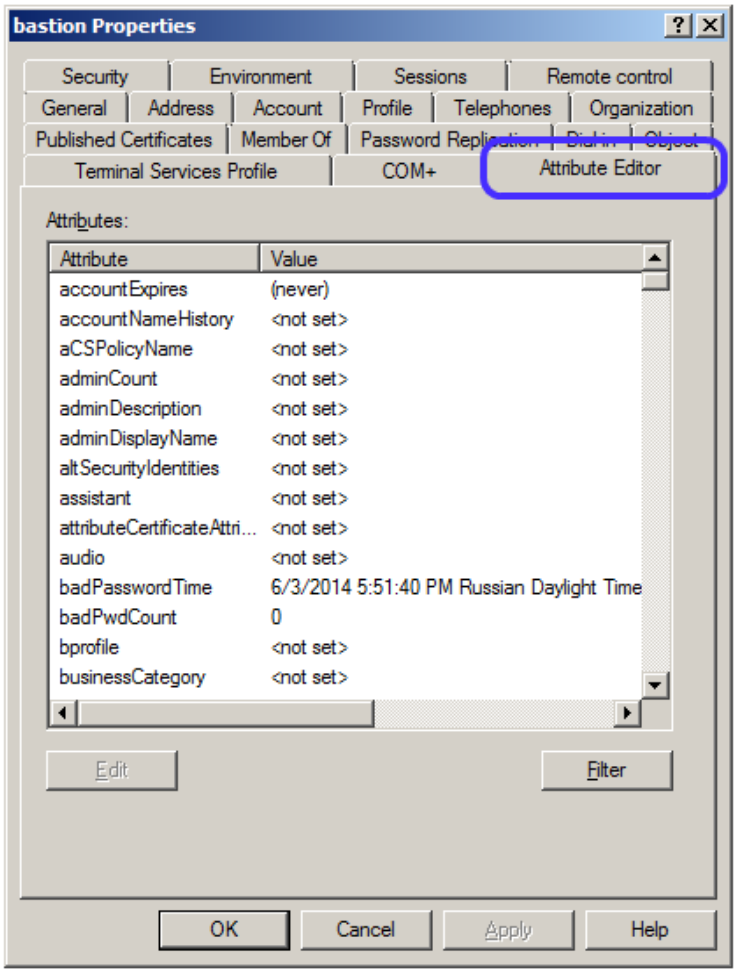

Рис. 44. Attribute Editor

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. 45).

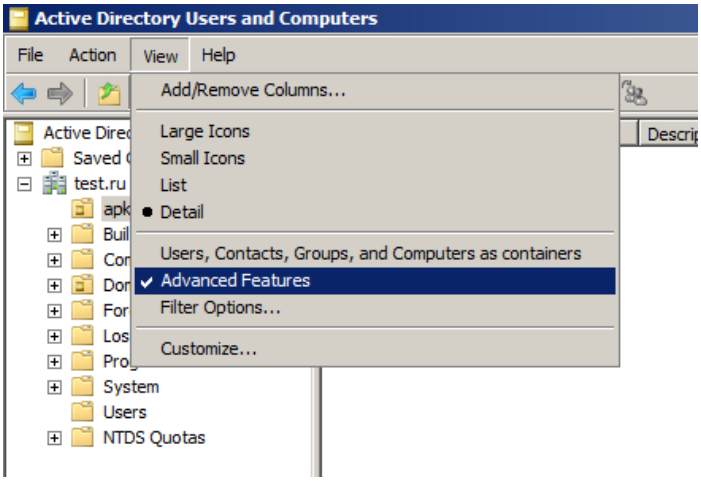

Рис. 45. Настройка отображения консоли Active Directory

После этого следует добавить рабочую станцию, где установлен ПК «Бастион-3» в домен Active Directory.

Затем, в ПК «Бастион-3» произвести настройку как указано в п.5.5.6.2.

После этого при первом запуске ПК «Бастион-3» должен будет появиться оператор, одноименный с пользователем Active Directory, под которым выполнен вход в систему на данной рабочей станции.

5.5.7. Авторизация через Open ID Connect

5.5.7.1. Сценарий авторизации через Open ID Connect

Начиная с версии 2024.1, ПК «Бастион-3» поддерживает авторизацию операторов через OpenID Connect. Использование авторизации через OIDC (OpenID Connect) позволяет приложениям ПК «Бастион-3» связаться со внешней службой идентификации, чтобы получить необходимые данные об операторах и вернуть их в приложение, обеспечив полную защиту данных.

В системе используется следующий сценарий авторизации через OIDC:

1. В окне входа в систему оператор нажимает кнопку «Войти через OpenID» (Рис. 46). При этом он будет перенаправлен в окно входа OIDC, которое будет открыто в браузере, установленном в системе по умолчанию. А приложение ПК «Бастион-3» в фоне будет показывать форму, приведенную на Рис. 47.

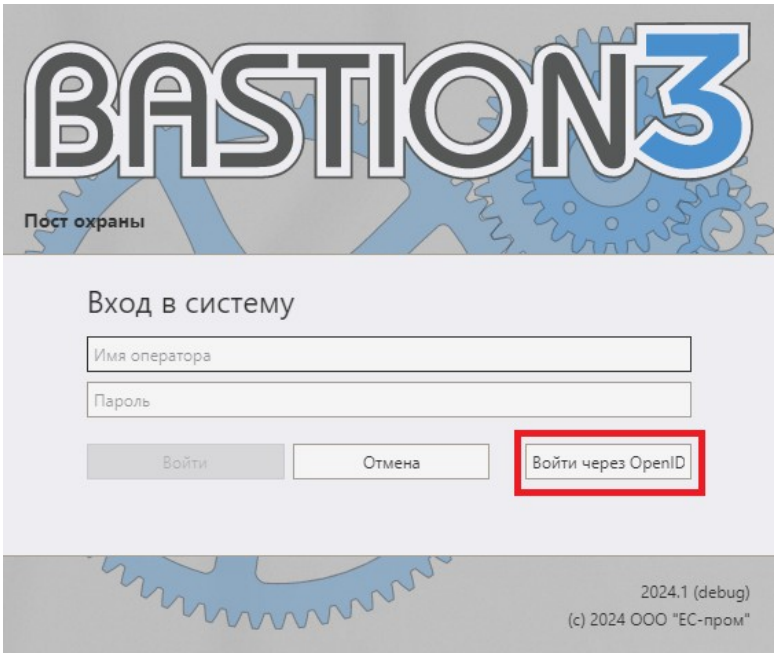

Рис. 46. Окно входа в систему

2. В браузере оператор должен ввести код для входа. Этот код автоматически копируется в буфер обмена при нажатии на кнопку «Войти через OpenID». При необходимости, код можно скопировать вручную или посмотреть в окне ожидания логина через OpenID Connect (Рис. 47).

3. После этого оператору будет предложено ввести свои авторизационные данные.

4. ПК «Бастион-3» периодически опрашивает службу идентификации о результате авторизации оператора. При получении положительного ответа система проверит роль оператора и авторизует его. При возникновении ошибок в авторизации будет отказано.

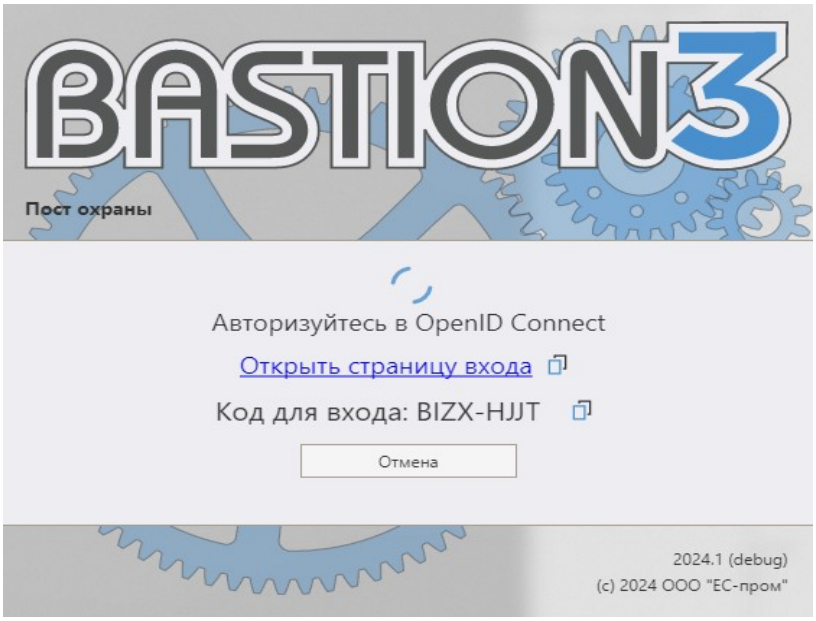

Рис. 47. Окно ожидания логина через OpenID Connect

Также, ПК «Бастион-3» производит фоновые проверки действительности сессии пользователя в OIDC. Если сессия стала недействительной, произойдет блокировка приложений ПК «Бастион-3», то есть — завершение пользовательской сессии.

Из окна блокировки оператор также может авторизоваться через OIDC (Рис. 48).

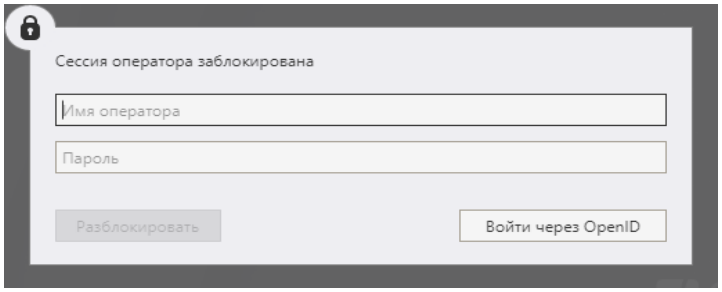

Рис. 48. Окно блокировки с возможностью авторизации через Open ID Connect

Оператор, добавленный в ПК «Бастион-3» через OpenID Connect, не может войти в систему с использованием логина и пароля без связи с OpenID Connect. Пароль такого оператора не хранится в ПК «Бастион-3».

5.5.7.2. Настройка KeyCloak

Наиболее распространенной системой, реализующей OpenID Connect, является KeyCloak. Руководство по установке KeyCloak выходит за рамки этого документа. Здесь приводятся сведения о тех настройках, которые необходимо выполнить в KeyCloak, чтобы интеграция заработала.

Для работы с KeyCloak необходимо определить Realm, через который будет производиться взаимодействие с ПК «Бастион-3». Realm — это высшая структурная единица конфигурации Keyloack. Realm содержит в себе набор клиентов, набор пользователей, набор scope, набор групп и т. д. Допускается работа через изначально существующий Realm с названием "master".

Для внешней системы идентификации ПК «Бастион-3» является клиентом. Поэтому, в KeyCloak необходимо создать отдельного клиента. Для этого следует:

1. Перейти в раздел Clients (в левой части веб-интерфейса) и нажать кнопку "Create client".
2. Заполнить следующие обязательные параметры:
   - Client type = OpenID Connect;
   - Client ID - произвольный текстовый идентификатор;
   - Client authentication = ON;
   - Authorization = ON;
   - OAuth 2.0 Device Authorization Grant = ON;
3. Сохранить параметры нажатием кнопки Save.

Настройка способа аутентификации клиента

В ПК «Бастион-3» доступно использование двух способов аутентификации клиента: "Client Id and Secret" и "X509 Certificate". Для использования второго нужно настраивать mTLS на сервере Keycloak и в ПК «Бастион-3».

Для настройки способа аутентификации клиента следует:

1. Зайти в настройки клиента (выбрать раздел "Clients" в левой части интерфейса и выбрать требуемого клиента из списка).
2. Перейти на вкладку "Credentials";
3. Выбрать "Client Id and Secret" или "X509 Certificate";
4. В случае выбора пункта "Client Id and Secret" сгенерировать и скопировать для конфигурации ПК «Бастион-3» текстовый секрет клиента;
5. Для варианта "X509 Certificate" можно задать конкретное значение "Subject DN", либо задать определённое regex-выражение для проверки клиентских mTLS-подключений по составу клиентского сертификата.

Создание групп

Роль оператора в ПК «Бастион-3» определяется по принадлежности соответствующего пользователя OpenID к определенной группе. Необходимо, чтобы в Keyloak был настроен набор групп, которые будут соответствовать ролям операторов в ПК «Бастион-3».

Для сужения множества используемых групп можно настроить определённый префикс, с которого будут начинаться имена групп, представляющих роли операторов в ПК «Бастион-3». Префикс настраивается в ПК «Бастион-3» в конфигурации подключения к серверу OpenID.

Соответствие групп OpenID ролям ПК «Бастион-3» определяется по текстовым идентификаторам — по именам (исключая префикс, если он есть), т.е. имя группы должно соответствовать имени роли операторов (без учёта регистра символов). Например, если в ПК «Бастион-3» есть роль с

именем admins и настроен префикс «bastion_», то в KeyCloak должна быть создана группа с именем bastion_admins.

В ПК «Бастион-3» оператор может принадлежать только к одной роли. Поэтому, вводится искусственное структурное ограничение на систему пользователей и групп в Keycloak: пользователь должен принадлежать только одной группе из множества групп, которые отображаются на роли операторов (а это все группы из соответствующего Realm, если в ПК «Бастион-3» не настроен префикс для таких группы, либо группы, которые начинаются с заданного префикса). Если пользователь принадлежит более чем к одной группе из тех, которые отображаются на роли операторов, то будет взята первая по списку.

Для создания групп в KeyCloak следует:

1. Перейти в раздел Groups.
2. Создать требуемый набор групп при помощи кнопки Create group. Для каждой группы следуют задать имя, начинающееся с префикса, если он определён.

Создание пользователей

Пользователи определенных групп OpenID соответствуют операторам ПК «Бастион-3». При входе пользователя OIDC в качестве оператора ПК «Бастион-3», оператор будут создан автоматически в случае его отсутствия в ПК «Бастион-3» (если по атрибутам пользователя можно определить роль оператора; если роль определить невозможно, или в системе отсутствует роль с нужным именем, то вход не произойдёт).

Для создания пользователя в KeyCloak следует:

1. Перейти в раздел Users.
2. Создать пользователей при помощи кнопки "Add user", присоединяя их к нужным группам при помощи кнопки "Join group" в настройках пользователя.
3. Задать пользователям пароли по умолчанию. Для этого в настройках пользователя нужно зайти на вкладку "Credentials" и нажать кнопку "Set password". Можно задать временный пароль, либо задать постоянный.

Keycloak поддерживает множество вариантов аутентификации конечного пользователя. Здесь описан базовый (по логину и паролю).

Настройка передачи информации о группа в атрибутах (Claims) пользователей

По умолчанию Keycloak не передаёт в ID-токене информацию о том, в каких группах состоит пользователь. Для того, чтобы настроить передачу информации о группах, необходимо:

1. Перейти в раздел Client scopes.
2. Нажать кнопку "Create client scope", задать обязательно имя и выбрать Type "Default" (чтобы атрибуты из этого Scope содержались в ID-токене всегда и не требовали дополнительных действий от клиентской системы).
3. В настройках нового scope перейти на вкладку Mappers и нажать кнопку "Configure new mapper".

4. В открывшемся окне выбрать mapper с именем "Group Membership" и описанием "Map user group membership".

5. Задать для него обязательное имя и заполнить настройку "Token Claim Name" значением, которое будет использовано в конфигурации ПК «Бастион-3» в настройке «Атрибут роли оператора».

6. Поставить значение настройки "Full group path" в OFF. Остальные настройки можно оставить со значениями по умолчанию.

7. Перейти в настройки клиента (выбрать раздел Clients в левой части интерфейса и выбрать нужного клиента из списка).

8. Перейти во вкладку Client scopes.

9. Нажать кнопку "Add client scope", выбрать из списка ранее созданную группу и добавить её путём нажатия кнопки Add. В появившемся меню выбирать пункт "default".

5.5.7.3. Настройка ПК «Бастион-3» для авторизации через OpenID Connect

Для настройки авторизации через OpenID Connect (OIDC) следует в модуле «Панель управления» открыть страницу «Операторы и полномочия — Политики безопасности — Авторизация через OpenID Connect» (Рис. 49).

Здесь следует включить флаг «Использовать авторизацию OpenID Connect», после чего настроить параметры, перечисленные ниже.

ID клиента — это идентификатор клиента, созданного во внешней системе идентификации (Client ID).

Хост подключения — имя или IP-адрес сервера внешней системы идентификации.

Порт подключения — порт сервера внешней системы идентификации.

Путь — часть вложенного пути портала внешней системы идентификации (оставьте поле пустым, если портал идентификации доступен по прямому пути хоста).

Набор Scope — набор scope внешней системы идентификации, необходимый для получения данных, задаётся через пробел, например: «openid basic access».

RealmID – идентификатор высшей структурной единицы конфигурации системы OIDC.

Атрибут логина оператора — имя атрибута, который будет использоваться в качестве логина оператора в ПК «Бастион-3». Заданное по умолчанию значение preferred_username соответствует настройкам KeyCloak по умолчанию.

Атрибут роли оператора — имя атрибута, который будет использоваться в качестве роли оператора в ПК «Бастион-3». Заданное по умолчанию значение groups соответствует группам пользователей в KeyCloak.

Префикс значения атрибута роли оператора — используется для сужения множества используемых в интеграции групп пользователей. Так как в ПК «Бастион-3» оператор может принадлежать только к одной роли, то использование префикса позволяет исключить конфликты с другими группами, в которых может состоять пользователь OIDC.

Приветственный текст — текст, отображаемый на форме ожидания логина через OpenID Connect (Рис. 47).

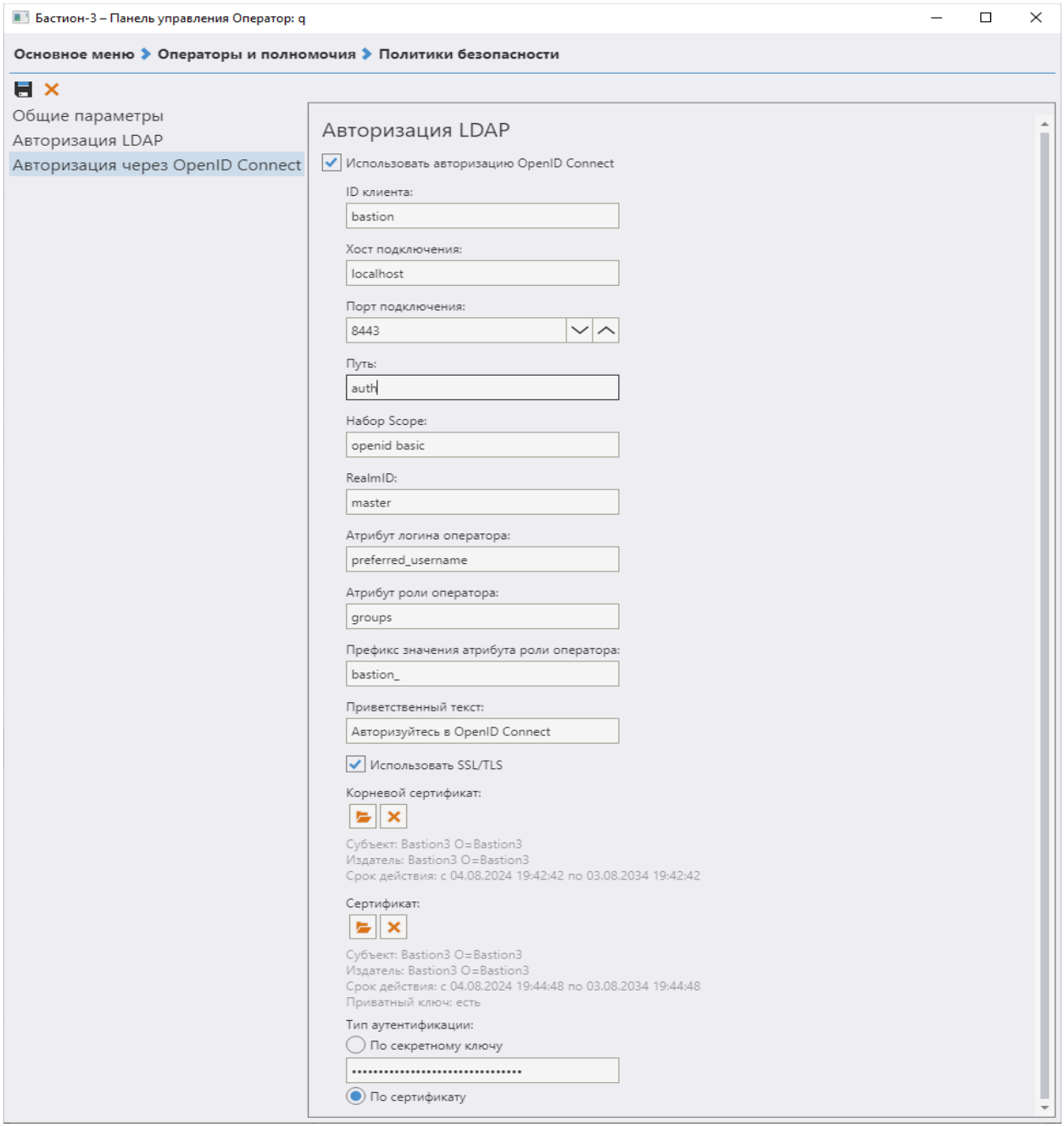

Рис. 49. Настройка авторизации через OpenID Connect

Использовать TLS – если включено, то при подключении к серверу OIDC будет использоваться защищенное соединенение с передачей сертификата клиента. Сертификат клиента и корневой сертификат необходимо загрузить здесь же. Использовать TLS обязательно при аутентификации клиента по сертификату.

Тип аутентификации — режим аутентификации клиента на сервере OIDC. Тип аутентификации должен соответствовать настройкам на сервере OIDC.

Секретный ключ — используется при аутентификации клиента на сервере OIDC по секретному ключу. Ключ необходимо скопировать из настроек клиента на сервере OIDC.

5.6. Настройка параметров обработки событий

5.6.1. Настройка общих параметров обработки событий

Для настройки общих параметров обработки событий следует в модуле «Панель управления» выбрать блок «Обработка событий – Параметры».

Здесь система позволяет задать следующие настройки:

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

Время актуальности событий – обозначает, что для событий, пришедших с опозданием больше заданного порога (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*».

5.6.2. Параметры протоколирования

Параметры протоколирования также настраиваются на странице «Обработка событий – Параметры».

Если выбрана опция «записывать в протокол сообщения», то активизируется список опций, определяющих критерии записи:

Штатные. При включенной опции штатные события, поступающие от драйверов, будут записываться в протокол.

Тревожные. При включенной опции тревожные события от драйверов будут записываться в протокол.

Неисправности. При включенной опции события о неисправностях от драйверов будут записываться в протокол.

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

Также, можно совсем отключить запись событий от драйверов, выбрав опцию «Не записывать в протокол сообщения устройств».

Ряд событий может сопровождаться изображением (фотографией события). Эти изображения также могут записываться в протокол. Система позволяет настроить, для каких именно событий

будут записываться изображения. Все параметры аналогичны настройкам записи сообщений от устройств, рассмотренным выше.

> ***Внимание!*** *Запись изображений всех событий может существенно влиять на объем записываемых в протокол данных. Рекомендуется оставлять запись только действительно необходимых изображений (например, только тревог).*

5.6.3. Настройка профилей сообщений

Параметры оповещения о событиях определяются профилями сообщений о событиях. Для редактирования профилей сообщений выберите блок «Обработка событий – Профили сообщений» (Рис. 50).

Всем событиям в системе всегда назначен один из *профилей сообщений*. Изменить профиль сообщения можно, если переопределить событие для конкретного устройства (см. п. 5.6.4.).

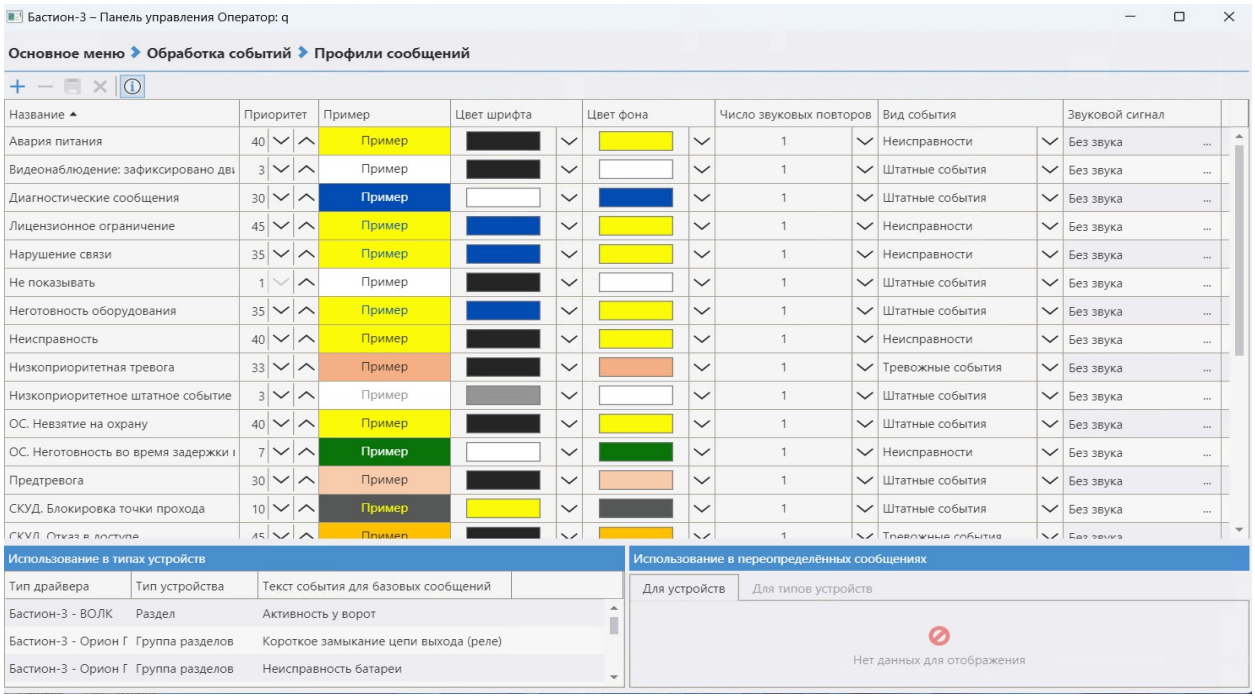

Рис. 50. Окно настройки профилей сообщений

Профиль сообщения определяет приоритет и тип события, его внешний вид при отображении в окне сообщений, а также звуковое сопровождение события.

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

Профили событий содержат следующие поля:

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

Приоритет – служит для ввода числового значения приоритета события в диапазоне от 1 до 99. Самый низкий приоритет имеет значение 1, самый высокий – 99. Можно создать несколько профилей событий с одинаковым приоритетом.

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

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

Число звуковых повторов – служит для указания количества повторов звукового сообщения при возникновении события с данным профилем.

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

В нижней части окна отображается использование выбранного профиля для разных событий. Слева отображается использование профиля для стандартных событий, справа – для переопределённых пользователем событий.

5.6.4. Переопределение событий

Текст и профиль событий, заданные по умолчанию, можно изменять. При этом имеется возможность указать параметры отдельно для каждого устройства, либо сразу для всех устройств одного типа, принадлежащих одному драйверу.

Для выполнения этих действий следует выбрать блок «Обработка событий – Переопределение событий» в панели управления, после чего появится окно, изображённое на Рис. 51.

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

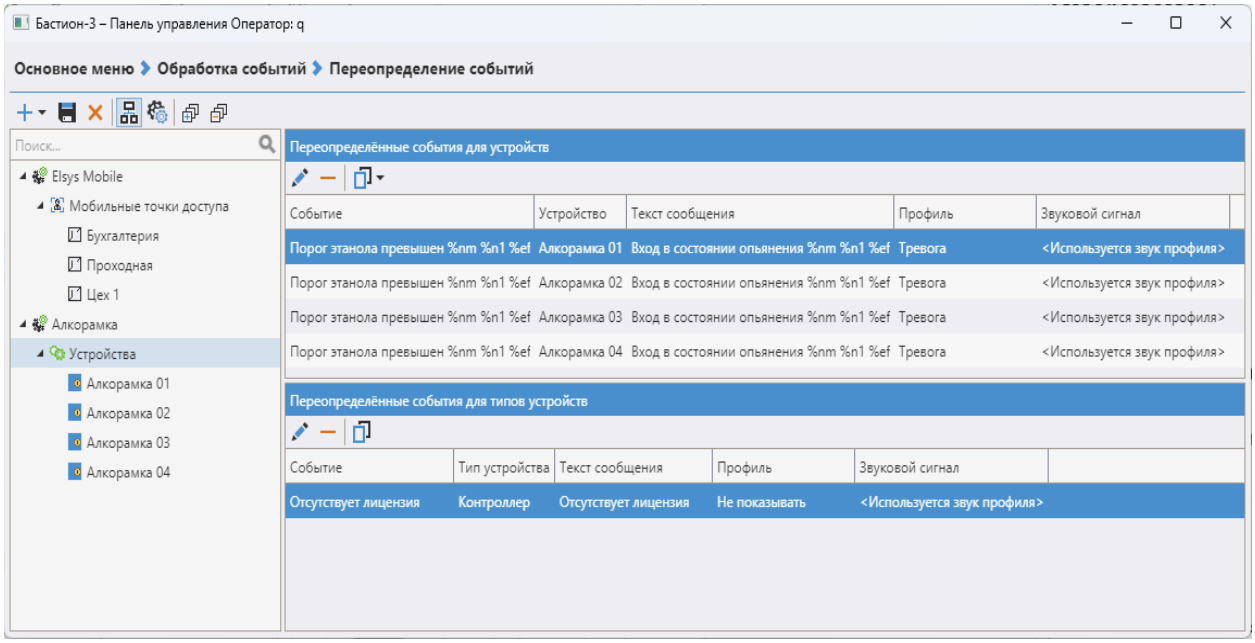

Рис. 51. Окно переопределения событий

Для переопределения события выберите устройство-источник в дереве слева и нажмите кнопку «+» в панели инструментов. Из выпадающего меню выберите, для чего требуется переопределить

событие — для отдельного устройства или для типа устройств. В появившейся форме (см. Рис. 52) настройте требуемые параметры события и нажмите «ОК».

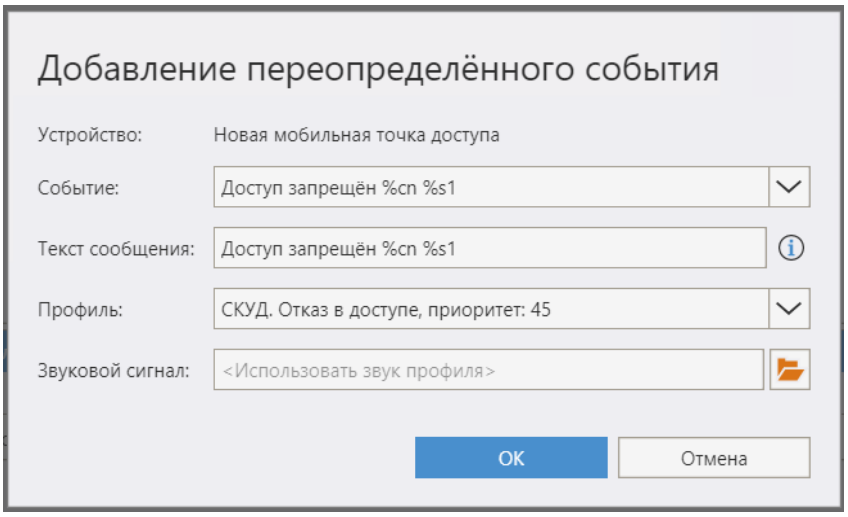

Рис. 52. Окно добавления события для отдельного устройства

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.
%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.

Профиль – позволяет назначить один из заранее созданных профилей текущему событию.

Звук – позволяет выбрать файл звукового оповещения о событии. Это поле не является обязательным, его можно оставить пустым. ПК «Бастион-3» использует звуковые файлы формата Wave audio (.wav) или MP3. Звуковые файлы загружаются в БД системы и будут доступны на всех компьютерах.

Существует возможность выполнить копирование событий. Для этого служит кнопка «  » с выпадающим меню "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, профиль, звук.

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

5.6.5. Настройка сценариев и реакций на события

Сценарий – это упорядоченная последовательность действий, которая может выполняться автоматически при наступлении каких-либо событий (при срабатывании так называемых триггеров), либо по команде оператора. Сценарии позволяют автоматизировать реакции на возникновение в системе каких-либо событий.

Сценарии для удобства можно объединять в *группы сценариев*, которые 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 прочее.

При вынесении на графический план пиктограммы сценария, его контекстное меню позволяет выполнить сценарий. Для пиктограммы группы 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. 5.5.4.7.).

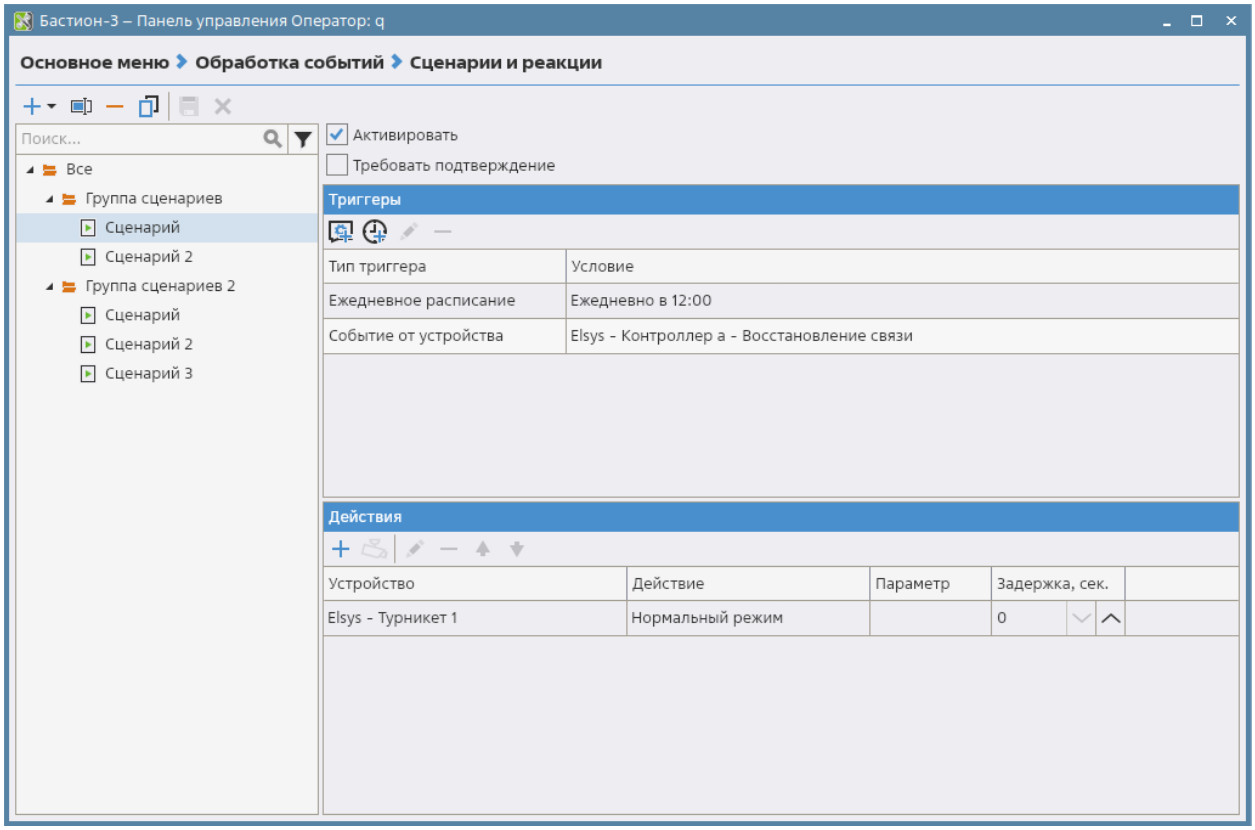

Рис. 53. Окно редактирования сценариев

Для редактирования сценариев выберите блок «Обработка событий – Сценарии и реакции». Общий вид редактора сценариев представлен на Рис. 53.

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

Только что созданный сценарий является пустым, то есть не содержит ни действий, ни триггеров. Для *добавления действий* нажмите кнопку "+" в панели «Действия». При этом появится окно для добавления действий (Рис. 54).

В этом окне необходимо выбрать устройство и его действие. Для некоторых действий также необходимо указывать параметры в панели под списком действий. Доступно выделение сразу нескольких однотипных устройств и их общего действия, при этом в сценарий для каждого выбранного устройства будет добавлено выбранное действие.

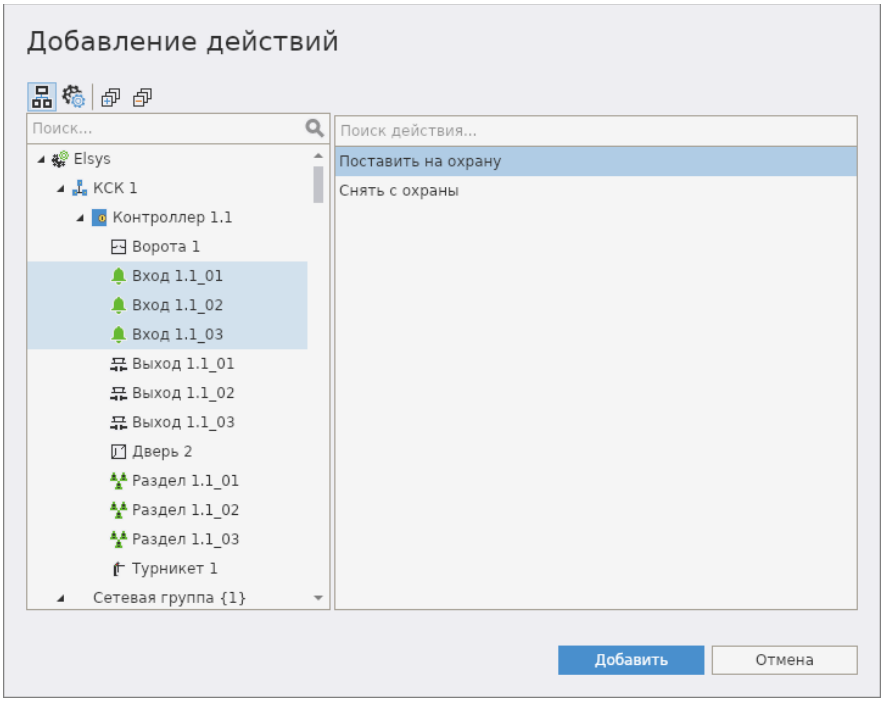

Рис. 54. Окно добавления действий сценария

Внимание! *Для действия «Запустить файл» драйвера «Система» необходимо указывать файл, локально хранящийся на сервере системы.*

Список действий сценария является упорядоченным — действия выполняются последовательно в том порядке, в котором они расположены в таблице действий. Для изменения порядка их выполнения используются кнопки со стрелками вверх и вниз, расположенные в панели «Действия».

Для *редактирования действия* нужно выбрать его в таблице и нажать на кнопку "Редактировать". При этом отобразится окно, аналогичное окну на Рис. 54.

Действие сценария может выполняться с *временной задержкой*, заданной в секундах. Редактирование задержки выполнения действия доступно в столбце «Задержка, сек.» таблицы действий.

Для сценария есть возможность настроить список ролей операторов, для которых будет отображаться изображение с видеокамер в приложении «Пост охраны». Для этого есть отдельное окно (см. Рис. 55), которое открывается с помощью кнопки «Редактировать отображение камер» с пиктограммой камеры наблюдения, расположенной в панели «Действия». Настройка данного списка актуальна для сценариев, у которых в списке действий есть отображение изображения с видеокамеры.

> ***Внимание!*** *К событию протокола может быть привязано не более 8 видеокамер. В связи с этим, если какое-либо событие послужило триггером для выполнения одного или нескольких сценариев, у которых есть действия для видеокамер, то в протоколе к данному событию будет привязано первые 8 камер, взятые среди всех действий данных сценариев. При этом, если событие поступило от видеокамеры, то один слот из восьми уже будет занят данной камерой.*

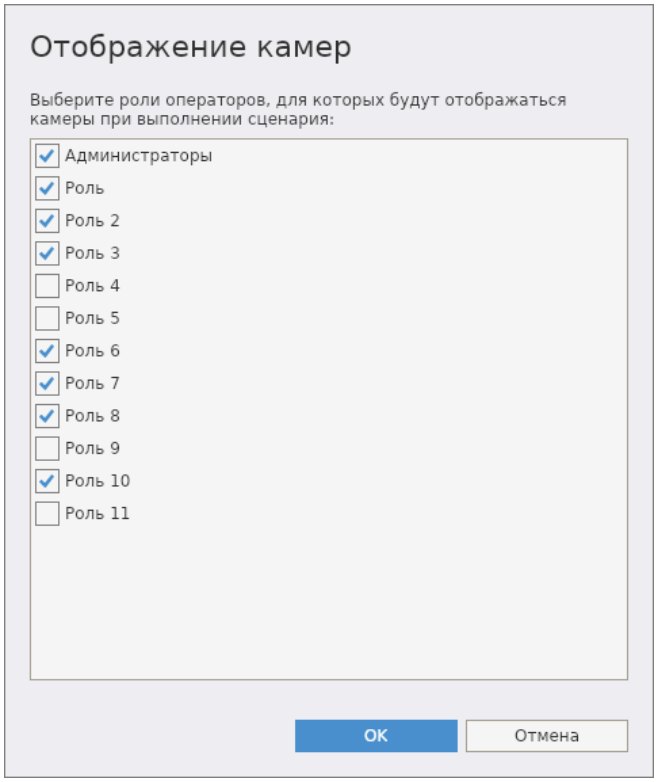

Рис. 55. Окно редактирования списка ролей операторов для отображения изображения с видеокамер

Помимо действий, для сценария необходимо добавить триггеры, при срабатывании которых действия будут выполняться.

В ПК «Бастион-3» есть возможность создавать сложные условия срабатывания триггера путём комбинирования условий различных типов. В отличие от АПК «Бастион-2», где для триггера задавалось одно условие срабатывания — возникновение конкретного события от конкретного устройства, в ПК «Бастион-3» для триггера задаётся основное условие, а также может задаваться одно или несколько дополнительных.

Условия (как основное, так и дополнительные) могут быть различных типов, например: «Устройство+событие» (возникновение конкретного события от конкретного устройства), «Устройство» (любое событие от конкретного устройства), «Персона» (любое событие, содержащее в себе информацию о выбранной персоне) и другие. Условия некоторых типов могут выступать как в качестве основных, так и в качестве дополнительных: например, «Профиль события» (событие с заданным профилем). Условия некоторых других типов могут быть только дополнительными: например, «Время» (время возникновения события).

В каждое *условие* можно добавить несколько элементов (например, несколько устройств). Условие будет считаться выполненным, если в событии получен хотя бы один из его элементов.

При возникновении в системе события, триггер запускает выполнение сценария, если выполняются его основное и дополнительные условия (если они заданы через «Параметры»), а также срабатывание триггера разрешено заданной *вероятностью срабатывания*. Дополнительные условия проверяются, если выполнено основное условие. Дополнительные условия считаются выполненными, если выполняется каждое дополнительное условие.

Для *добавления триггера* нажмите кнопку «Добавить триггер-событие» в панели «Триггеры». При этом появится окно для добавления триггер-события (Рис. 56).

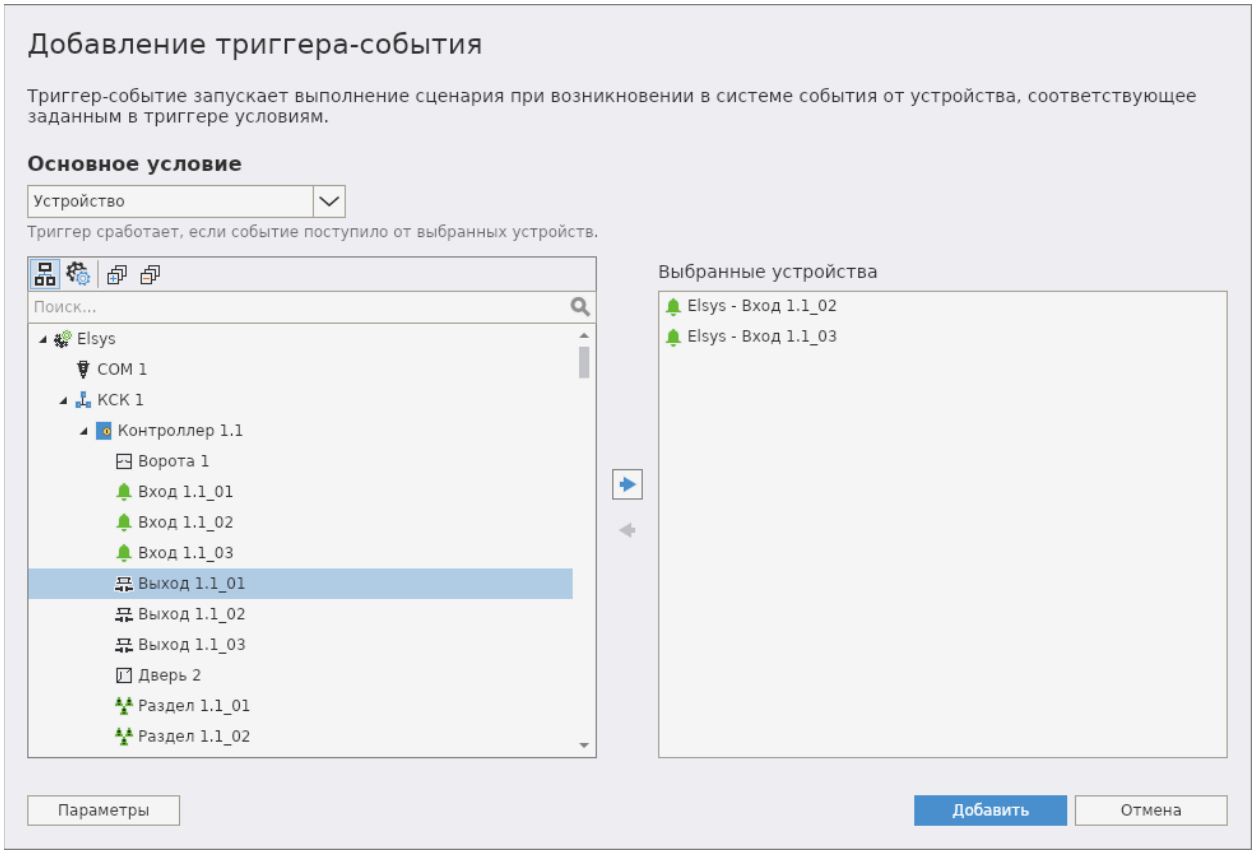

Рис. 56. Окно добавления триггер-события

Для триггера необходимо задать основное условие: выбрать в выпадающем списке тип условия и в панели ниже добавить один или несколько элементов в список выбранных. Например, для основного условия типа «Устройство» нужно выбрать одно или несколько устройств.

При необходимости, нажав на кнопку «Параметры», можно задать вероятность срабатывания триггера, выраженную в процентах, а также дополнительные условия. Окно редактирования параметров триггера представлено на Рис. 57.

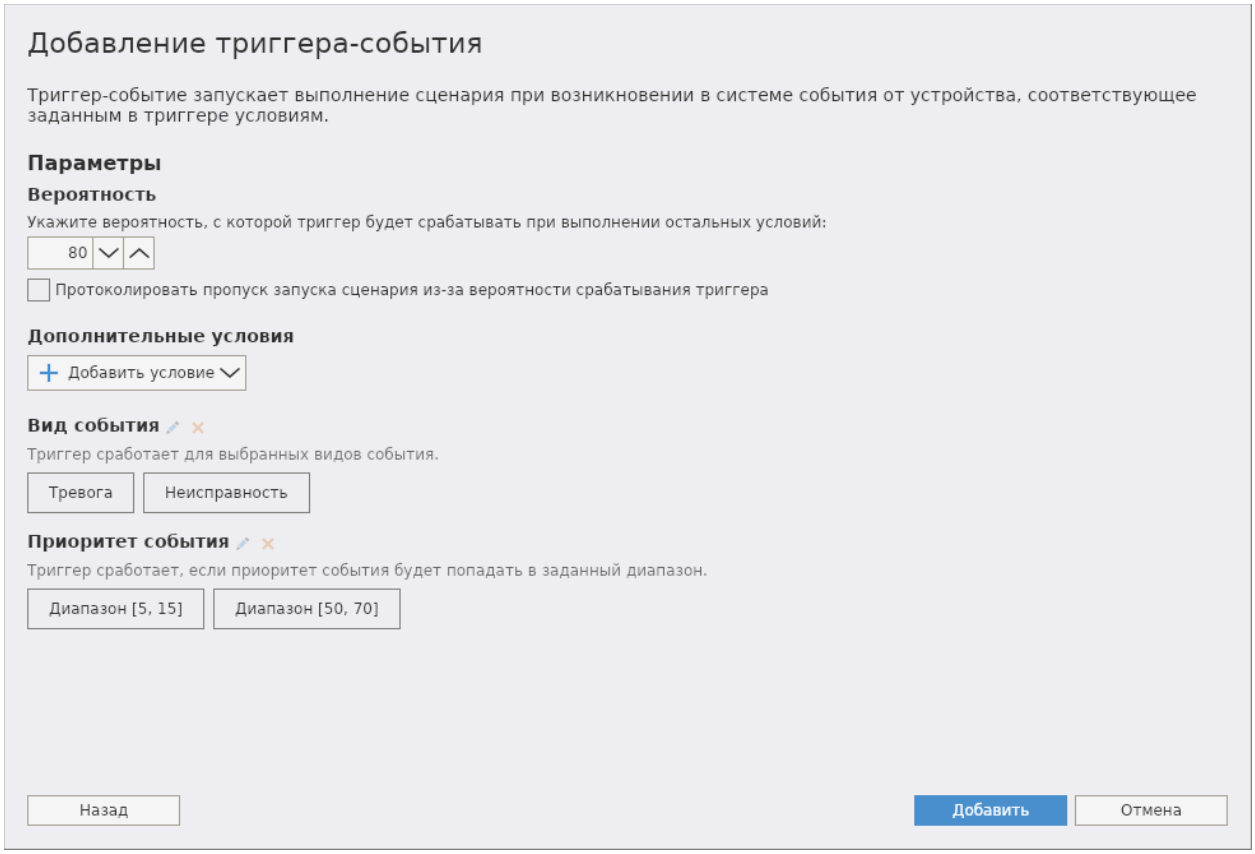

Рис. 57. Окно редактирования параметров триггер-события

Для *добавления дополнительного условия* нужно нажать на кнопку «Добавить условие», расположенную под заголовком «Дополнительные условия», и в выпадающем списке выбрать тип условия. После этого отобразится окно для редактирования условия. Пример окна редактирования дополнительного условия типа «Время» представлен на Рис. 58.

Под кнопкой добавления условия располагаются уже добавленные дополнительные условия. Для редактирования/удаления дополнительного условия нужно использовать кнопки, расположенные рядом с названием условия (Рис. 57).

Список типов дополнительных условий, доступных для добавления, зависит от основного условия: одни типы дополнительных условий могут быть доступны всегда, а другие доступны только при выполнении определённых требований. Например, для основного условия типа «Устройство» всегда доступны дополнительные условия типов «Вид события» (штатное, тревожное или неисправность), «Время», «Приоритет события» и «Профиль события», в то время как типы «Организация» и «Категория пропуска» доступны, только если у всех устройств, указанных в основном условии, есть типы событий, текст которых включает в себя константу подстановки %nm (фамилия персоны).

После того, как для триггера задано основное условие и параметры, нажмите кнопку «Добавить». Добавленный триггер отобразится в таблице в панели «Триггеры».

Для *редактирования параметров триггера* нужно выбрать его в таблице и нажать на кнопку «Редактировать». При этом отобразится окно, аналогичное окну на Рис. 57. Редактирование основного условия недоступно.

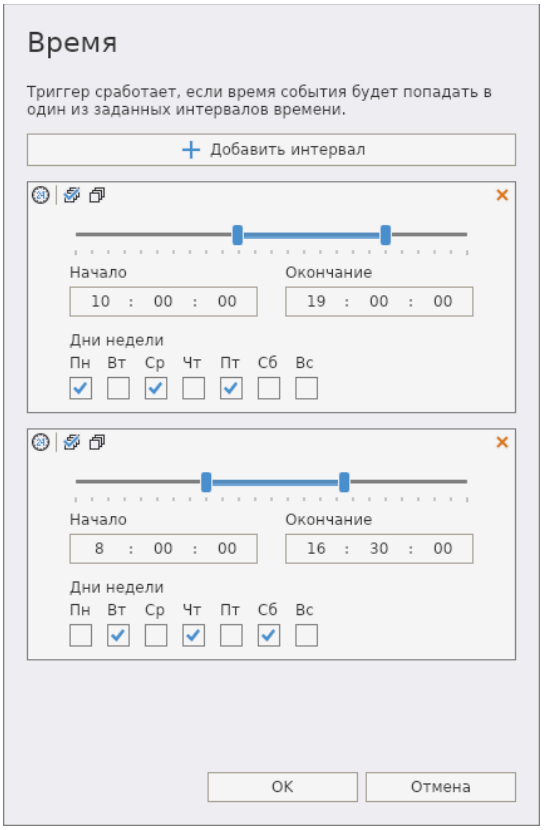

Рис. 58. Окно редактирования дополнительного условия типа «Время»

Сценарии могут выступать не только в качестве реакций на возникновение событий в системе, но могут выполняться и по расписанию.

В системе доступны 4 типа расписаний:

- *однократное* – однократное выполнение сценария в назначенные дату и время;
- *ежедневное* – ежедневное выполнение сценария в назначенное время;
- *еженедельное* – выполнение сценария каждую неделю в указанные дни недели в назначенное время;
- *ежемесячное* – выполнение сценария в назначенные день и время указанных месяцев года. День выполнения можно задать либо указанием порядкового номера дня месяца, либо указанием номера недели и дня недели.

Для *добавления расписания* нажмите кнопку «Добавить расписание» в панели «Триггеры». При этом появится окно для добавления расписания (Рис. 59). В окне нужно выбрать тип расписания и задать его параметры.

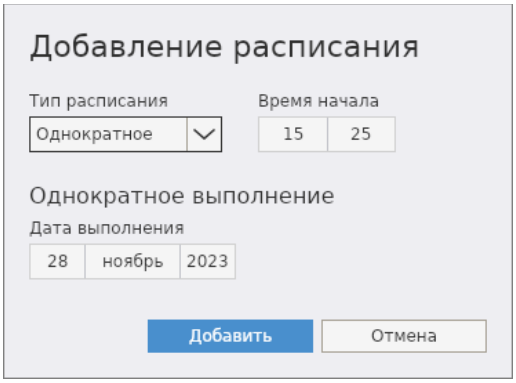

Рис. 59. Окно редактирования параметров расписания

Внимание! *Для корректной работы расписаний при смене часового пояса на сервере системы необходимо перезапустить службу Bastion3AgentSvc.*

Для *редактирования расписания* нужно выбрать его в таблице и нажать на кнопку "Редактировать". При этом отобразится окно, аналогичное окну на Рис. 59.

Список сценариев, которые будут выполнены *в следующие 24 часа*, можно посмотреть, выбрав блок «Обработка событий – Расписание сценариев» (Рис. 60). При необходимости, например, при пусконаладочных работах, можно остановить и запустить работу вообще всех расписаний (не только тех, что будут выполнены в следующие 24 часа), используя соответствующие кнопки в панели инструментов.

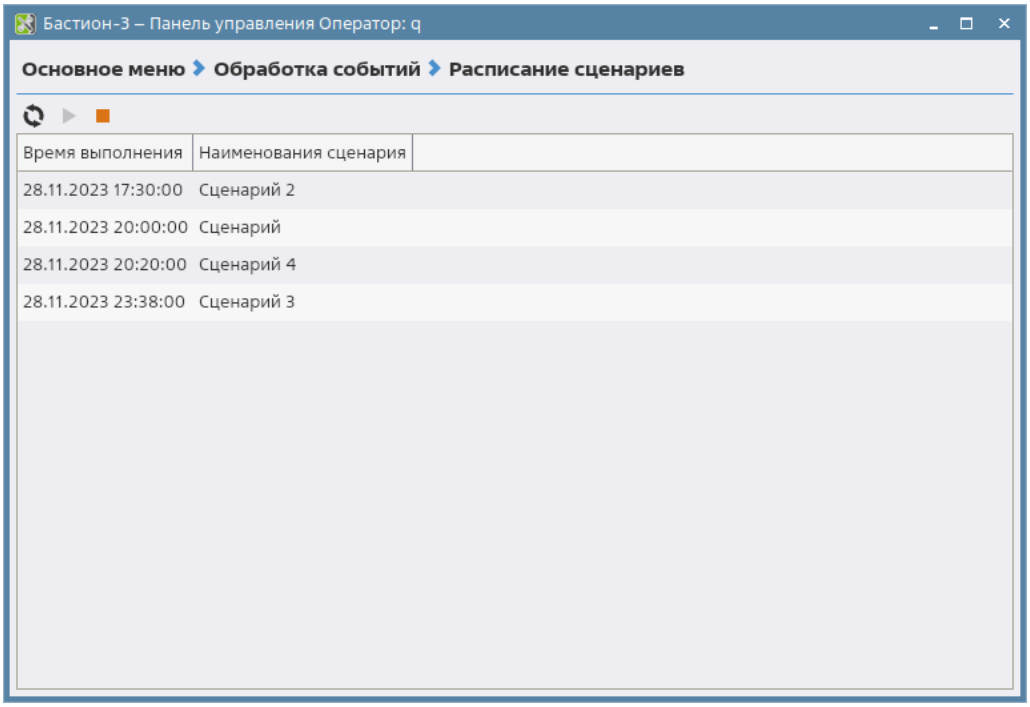

Рис. 60. Окно расписания выполнения сценариев на следующие 24 часа

5.6.6. 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.

На странице «Обработка событий – Параметры» имеются следующие настройки:

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.

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 установке драйвером нормального состояния устройства. (Например, при получении любого события, переводящего его в штатный режим (например, «Сброс тревоги», «Штатный вход» или «Снятие с охраны»)).

Система позволяет производить подтверждение в двух режимах – с запросом причины события или без него. Эта настройка задаётся для каждой роли оператора отдельно (см. п. 5.5.4.). Причина события при подтверждении выбирается из предварительно заполненного справочника.

Для настройки списка причин служит форма «Причины событий», вызвать которую можно из блока «События и реакции» вкладки «Конфигурация» главного окна. Для удобства, в системе уже добавлен список наиболее вероятных причин событий (Рис. 61). При подтверждении оператор также сможет ввести комментарий к событию.

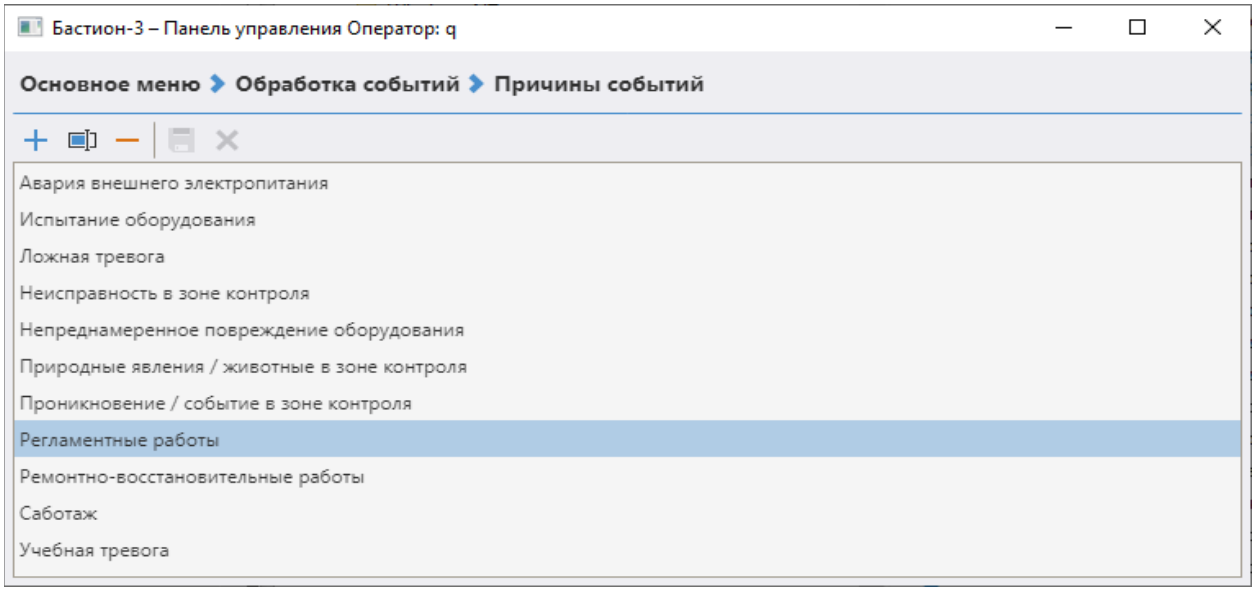

Рис. 61. Причины событий. Настройка по умолчанию

5.6.7. Маршрутизация сообщений

Маршрутизация сообщений позволяет установить, каким пользователям, в зависимости от их профиля, будут выводиться сообщения от определенных устройств. Маршрутизация сообщений настраивается на странице «Роли операторов – Доступ к устройствам» (см. п. 5.5.4.7.).

5.7. Локальные настройки

5.7.1. Общие сведения

Часть настроек системы, относящаяся к отдельному компьютеру, хранится локально. Эти настройки можно изменять двумя способами:

1. С помощью консольной утилиты Bcnfg.
2. С помощью приложения «Локальные настройки». Для запуска приложения «Локальные настройки» пользователю операционной системы потребуются права администратора.

Приложение «Локальные настройки» можно запустить из «Панели управления».

Настройки, относящиеся к пропускному режиму и настольным считывателям рассмотрены в документе «Бастион-3 – Бюро пропусков. Руководство оператора».

Настройки блокировки рабочих станций рассмотрены в документе «Бастион-3 – LDAP. Руководство администратора».

5.7.2. Работа с приложением «Локальные настройки»

5.7.2.1. Подключения к серверам системы

На каждом рабочем месте задаются параметры подключения к серверу системы (см. Рис. 62). При этом для служб и приложений ПК «Бастион-3» могут быть заданы разные настройки подключений. Дополнительно, для приложений есть возможность настроить несколько разных подключений к серверам системы, которые можно переключать при запуске приложений.

Для служб есть возможность выбора способа аутентификации: по секретному слову или по сертификату.

Службы и приложения могут использовать одни и те же настройки подключения к серверу системы, но также эти настройки могут быть разделены.

Для задания разных параметров подключения для служб и приложений следует снять флаг «Использовать одни параметры для работы служб и приложений» в окне на Рис. 62.

В общем случае, для подключений задаются следующие параметры:

Хост – адрес или имя хоста, где выполняется сервер системы ПК «Бастион-3».

Порт – IP-порт, который прослушивается сервером системы (должен совпадать с одним из портов прослушивания, указанных при установке или в конфигурации сервера системы).

Использовать SSL/TLS – при установке флага будет использоваться защищённое соединение с сервером системы. При этом возможна взаимная проверка сертификатов сервера и клиента при установке соединения. Значение данного флага должно быть синхронизировано со значением такого же флага в настройках прослушивателя с тем же портом в параметрах сервера системы. Например, если указан порт 6300 и установлен флаг «Использовать SSL/TLS», то в настройках сервера системы для прослушивателя с портом 6300 флаг «Использовать SSL/TLS» тоже должен быть установлен.

Проверять сертификат сервера — если флаг установлен, при подключении сервера клиент будет проверять действительность его сертификата.

Проверять имя сервера — если флаг установлен, при подключении к серверу клиент будет проверять имя сервера, указанное в сертификате.

Корневой сертификат — если указан, то валидность сертификата сервера будет проверяться этим сертификатом. Здесь может быть указан файл с публичной частью сертификата сервера, либо файл с публичной частью корневого сертификата сервера.

Отправлять сертификат клиента — если флаг установлен, то при подключении к серверу клиент будет отправлять сертификат, указанный в поле «Файл сертификата клиента». Клиентский сертификат должен быть либо самоподписанным, либо подписан сертификатом сервера, либо общим с сервером корневым сертификатом.

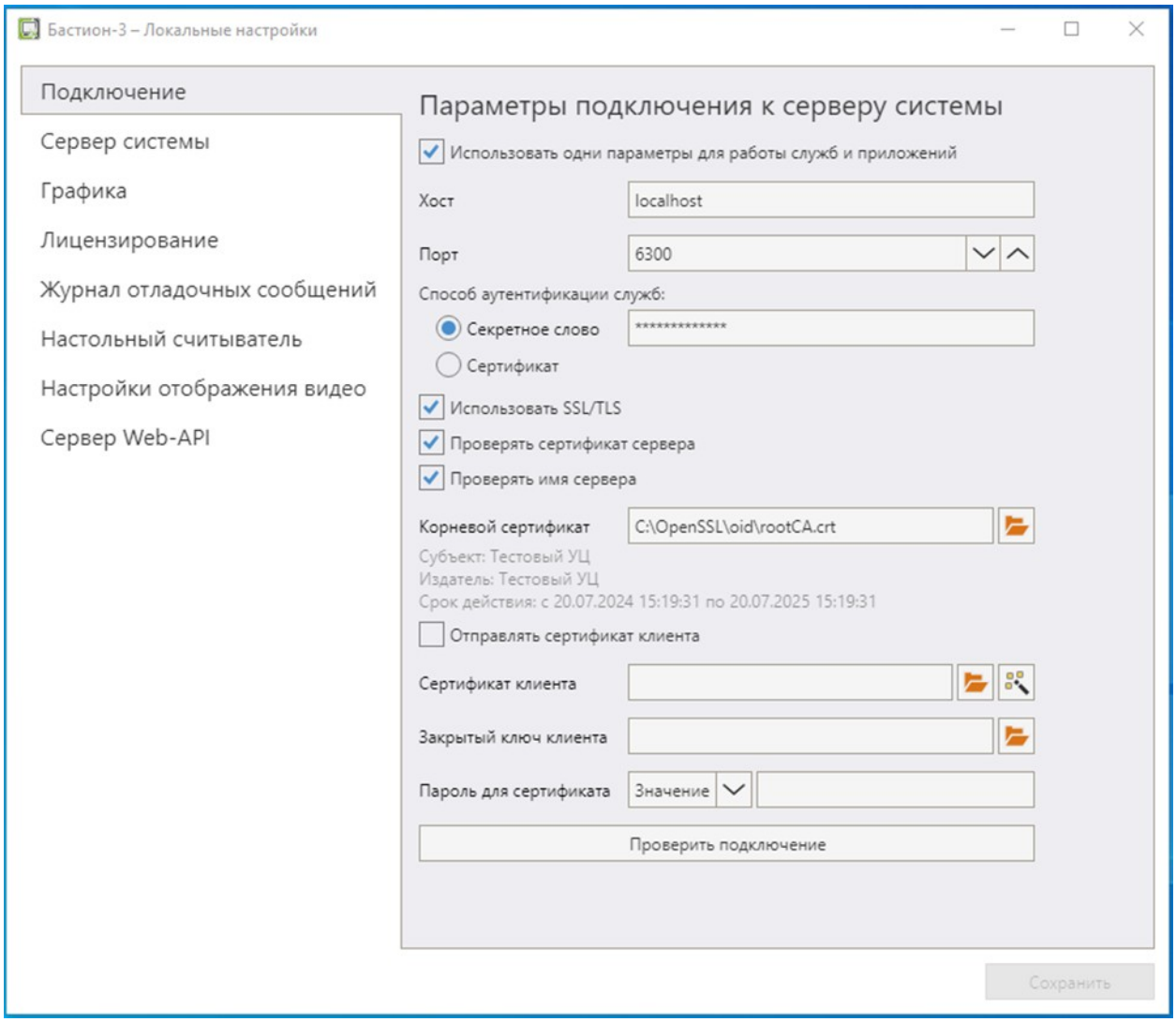

Рис. 62. Настройка подключений к серверам системы с общими параметрами для служб и приложений

Файл сертификата клиента — здесь должен быть указан файл сертификата, который будет отправляться на сервер при установке соединения. Самоподписанный сертификат клиента можно сгенерировать, нажав кнопку «».

Файл закрытого ключа клиента — здесь должен быть указан файл (*.key) с закрытым ключом сертификата клиента.

Пароль для сертификата можно указать в 3-х режимах:

Значение — пароль к сертификату вводится в поле ввода и сохраняется в файле настроек сервера системы в зашифрованном виде.

Переменная среды — в качестве пароля используется значение указанной переменной среды.

Команда — пароль должен возвращаться консольной командой, указанной в поле ввода.

Если в поле *«Файл сертификата клиента»* указан путь к файлу в формате PKCS#12, включающий в себя сертификат и закрытый ключ к нему, в поле *«Пароль для сертификата»* указывается пароль, который использовался при создании цепочки PKCS#12. Поле *«Файл закрытого ключа»* в этом случае остаётся пустым. При указании путей к отдельным файлам сертификата и закрытого ключа, в поле *«Пароль для сертификата»* указывается пароль к закрытому ключу.

Секретное слово – требуется для подключения служб к серверу системы. Вводимое секретное слово должно совпадать с секретным словом, указанным при установке или в конфигурации сервера системы. Используется только для подключения служб. Секретное слово можно не указывать, если для служб настроено подключение с использованием SSL/TLS, включена проверка сертификата сервера и отправка сертификата клиента, а также выбран тип аутентификации «Сертификат».

После установки всех параметров подключения, можно нажать кнопку «Проверить подключение», чтобы убедиться в корректности новых параметров.

О настройке подключений при запуске приложений см. п. 6.3.

Настройка аутентификации по сертификату для служб

На вкладке «Подключение» в разделе «Службы» (Рис. 63) можно настроить аутентификацию по сертификату для служб «Бастион-3 – Локальный агент» и «Бастион-3 – Сервер оборудования».

Для этого необходимо:

- Выбрать способ аутентификации служб: «Сертификат»;
- Настроить подключение с использованием SSL/TLS.

При настройке полей блока «SSL/TLS» обязательно должен быть проставлен флаг «Отправлять сертификат клиента» и заполнены поля, связанные с сертификатом.

В поле «Сертификат клиента» необходимо указать путь к файлу с сертификатом, либо к файлу в формате PKCS#12, содержащему сертификат и закрытый ключ к нему. Сертификат должен быть сохранён в PEM-формате. Для закрытого ключа поддерживаются форматы PKCS#1 и PKCS#8 (предпочтителен PKCS#8).

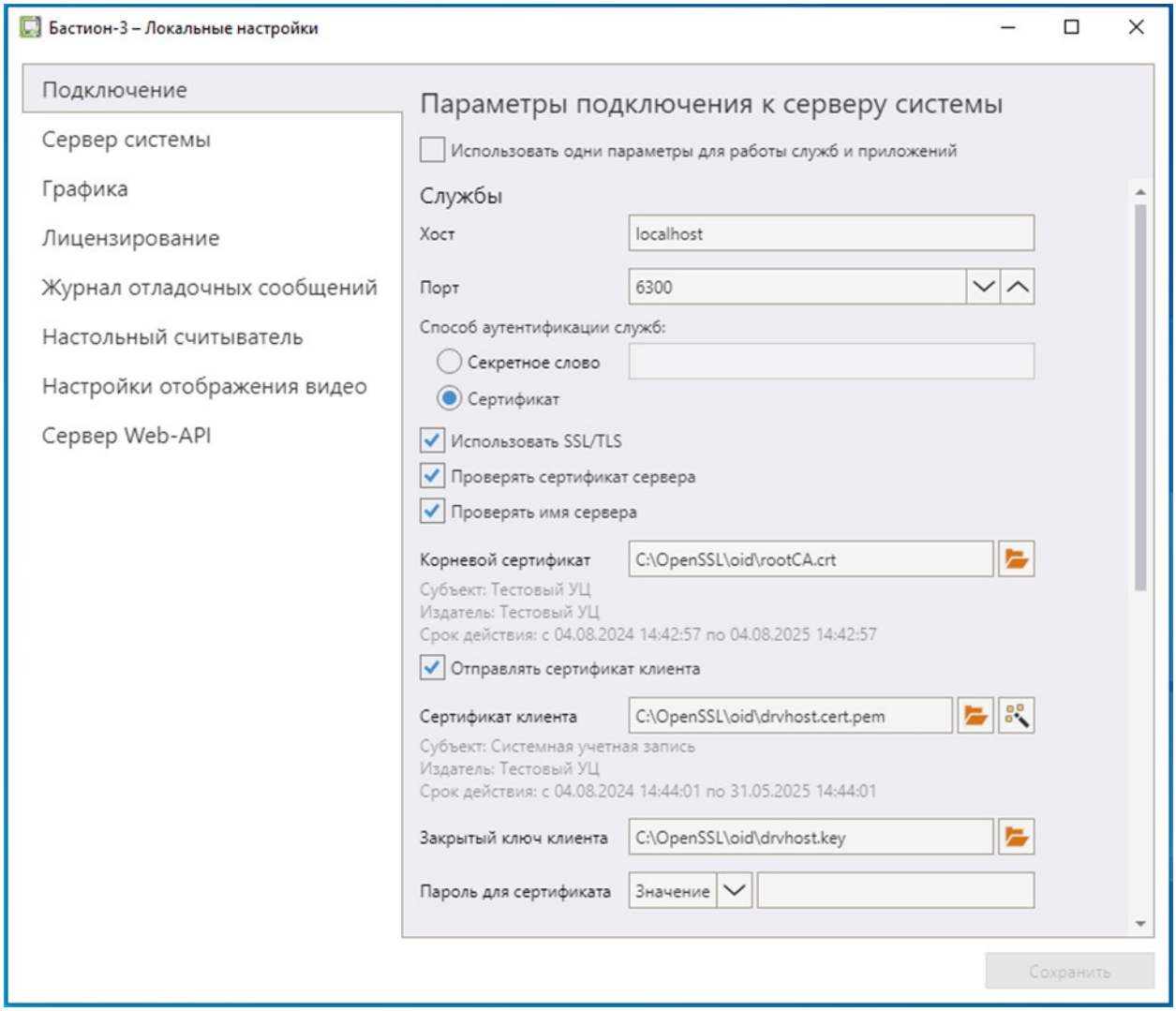

Рис. 63. Пример настройки аутентификации служб на сервере системы по сертификату

При создании сертификата для аутентификации служб «Бастион-3 – Локальный агент» и «Бастион-3 – Сервер оборудования» на сервере системы необходимо правильно указать имя пользователя. В данном случае «Имя пользователя» — это имя предустановленной технической учетной записи *DrvHost* (регистр значения не имеет). Имена технических учетных записей можно посмотреть в Панели управления в разделе «Операторы и полномочия -> Операторы», выбрав отображение системных операторов.

Имя пользователя в сертификате должно храниться в компоненте (секции) поля «Subject» с OID, значение которого указано в настройках сервера системы. В настройках сервера системы предлагается выбор одного из двух значений OID:

- 0.9.2342.19200300.100.1.1 – UserID, UID
- 2.5.4.3 – Common Name

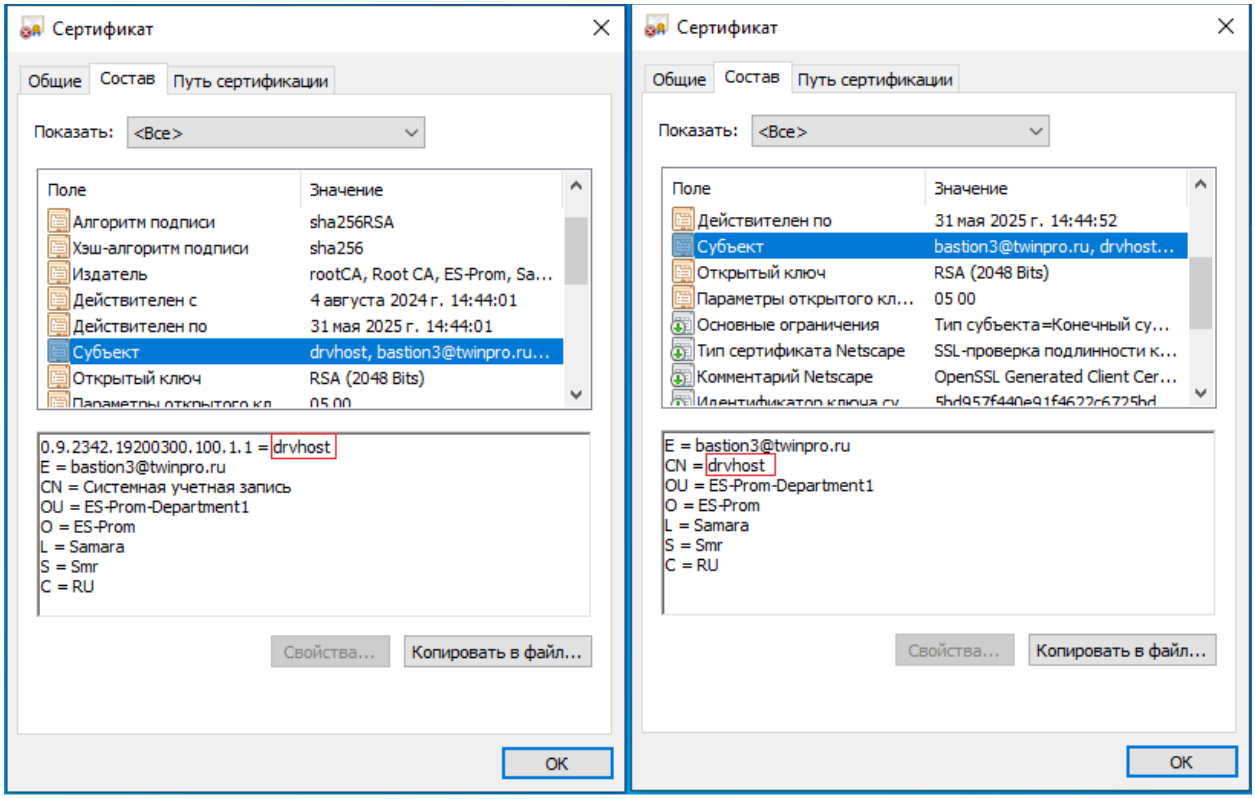

Рис. 64. Примеры сертификатов с именем пользователя в разных компонентах поля «Subject»

5.7.2.2. Параметры сервера системы

Если на компьютере установлен сервер системы, то его настройки можно изменить в приложении «Локальные настройки» на странице «Сервер системы» (см. Рис. 65).

> ***Внимание!*** *Указанные на этой странице настройки влияют только на сам «Сервер системы», но не на приложения, которые к нему подключаются с этого компьютера. Для настройки подключения приложений необходимо отдельно задать их параметры (см. п. 6.1.2.3.).*

В разделе «Аутентификация» указываются параметры, которые будут использоваться при аутентификации служб на сервере системы.

Секретное слово – строка, которая может быть использована при аутентификации подключающихся к серверу системы сервисов и служб (например, серверов оборудования).

OID имени оператора – этот параметр указывает на компонент поля «Subject» сертификата клиента, из которого будет получено имя оператора, учитывается при настройке mTLS-соединения с аутентификацией служб по сертификату.

Для входящих подключений к серверу системы можно настроить использование одного или нескольких портов прослушивания. По умолчанию, используется один порт 6300. Для каждого порта прослушивания можно указать, будет ли использоваться при подключении SSL/TLS, а также режим проверки сертификата клиента (Рис. 65).

При использовании одного общего прослушивателя и для служб, и для приложений с использованием SSL/TLS должно быть правильно настроено действие с сертификатом клиента. Поскольку для приложений поддерживаемый способ аутентификации – «логин/пароль», сертификат в настройках подключения для приложений может быть не указан. Если при этом службы аутентифицируются по сертификату, в настройках сервера системы для этого прослушивателя должно быть указано действие с сертификатом клиента: «Проверять при наличии».

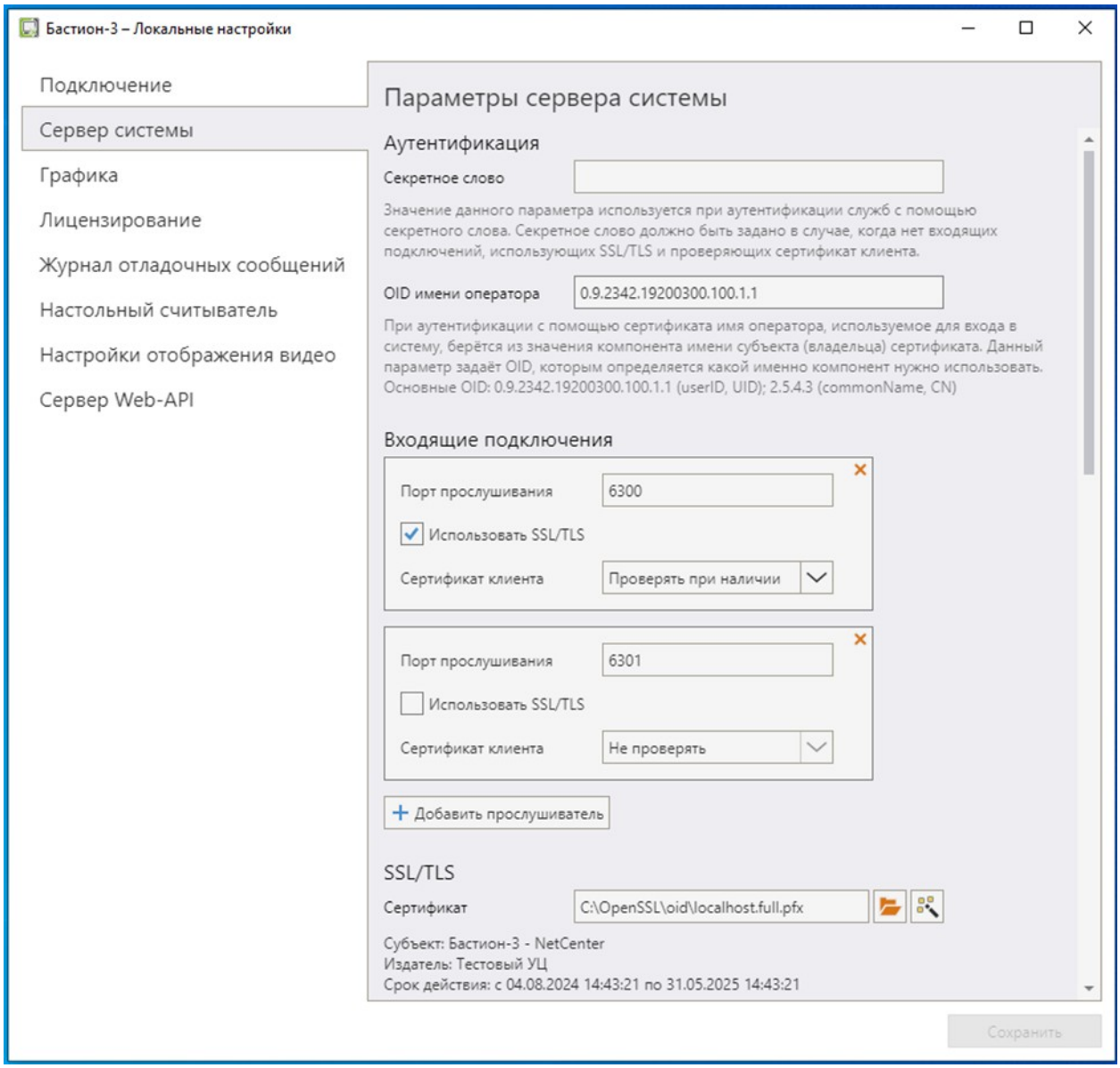

Рис. 65. Пример настройки прослушивателей с разным типом подключения

Доступные режимы проверки сертификата:

Не проверять — клиентский сертификат не проверяется сервером.

Проверять при наличии — действительность сертификата будет проверяться только, если клиент (служба или приложение) подключается с сертификатом. Если клиент не передает сертификат — проверка не выполняется и подключение будет установлено.

Всегда проверять — сервер всегда будет проверять наличие и действительность сертификата клиента.

Сервер системы и клиенты могут выполнять взаимную проверку сертификатов при подключении.

В текущей версии выполняются только базовые проверки действительности сертификата. Клиентский сертификат должен быть либо самоподписанным, либо подписан сертификатом сервера, либо общим с сервером корневым сертификатом.

Если в поле «*Файл сертификата*» указан корректный путь к файлу сертификата, то он будет передаваться клиентам при подключении. При этом клиенты смогут проверить валидность сертификата сервера системы.

При нажатии на кнопку «  » можно сгенерировать самоподписанный сертификат для сервера системы. Система запросит путь и имя файла для сохранения сертификата, после чего будут автоматически подставлены значения в поля «Файл сертификата» и «Файл закрытого ключа».

Пароль для сертификата можно указать в 3-х режимах:

Значение — пароль к сертификату вводится в поле ввода и сохраняется в файле настроек сервера системы в зашифрованном виде.

Переменная среды — в качестве пароля используется значение указанной переменной среды.

Команда — пароль должен возвращаться консольной командой, указанной в поле ввода.

В поле «Файл сертификата» можно также указать путь к файлу в формате PKCS#12, содержащему сертификат клиента и закрытый ключ к нему. В этом случае поле «Закрытый ключ» следует оставить пустым, а в поле «Пароль для сертификата» указать пароль к файлу PKCS#12, если он был задан.

Корневой сертификат — в случае, если сертификат клиента подписан корневым сертификатом, в этом поле следует указать путь к файлу с этим сертификатом. Для самоподписанных сертификатов следует указать файл с публичной частью сертификата клиента.

> ***Внимание!*** *На клиентах должны быть установлены параметры подключения к серверу системы, соответствующие настройкам сервера. Должен быть указан один из прослушиваемых сервером портов, режим использования SSL/TLS и все необходимые данные для проверки сертификатов.*

Все параметры в разделе «База данных» относятся к подключению к серверу баз данных:

Тип базы данных – Oracle или PostgreSQL (поддерживается только PostgreSQL).

Для подключения к серверу БД **PostgreSQL** указываются:

Хост – имя или адрес сервера БД.

Порт подключения – порт прослушивания сервера БД.

Имя базы данных – название базы данных, которое было указано при её создании.

Имя пользователя и пароль – будут использоваться для подключения к БД.

Использовать SSL/TLS – если включено, при соединении с сервером БД будут производиться проверки сертификатов, а соединение с БД будет защищённым.

Проверять сертификат сервера — если включено, сервер системы при подключении к серверу БД будет проверять наличие и действительность его сертификата.

Корневой сертификат — можно указать корневой сертификат, которым должен быть подписан сертификат сервера БД.

Проверять имя сервера — если включено, сертификат сервера БД должен содержать его имя, которое будет проверяться сервером системы при подключении.

Файл сертификата — файл сертификата клиента (сервера системы).

Файл закрытого ключа — файл закрытого ключа сертификата клиента (сервера системы).

Пароль для сертификата — пароль файла сертификата клиента (сервера системы).

> ***Внимание!*** *При применении новых параметров подключения сервера системы к БД необходимо на сервере системы вручную перезапустить службу «Бастион-3: локальный агент (Bastion3AgentSvc).*

При наличии интеграции с внешними системами через прямое подключение к серверу системы через Web API (Web-socket), необходимо разрешить подключения по Web API в настройках сервера системы. Для этого следует установить флаг «Принимать входящие подключения» в разделе Web API.

Для подключений по Web API можно задать следующие параметры:

Порт прослушивания — порт, который должен быть указан на внешних клиентах для подключения к серверу (по умолчанию 6333).

Использовать SSL/TLS – при установке флага будет использоваться защищённое соединение с сервером системы. При этом возможна взаимная проверка сертификатов сервера и стороннего клиента при установке соединения. Для сервера используется тот же сертификат, который указаны выше в разделе SSL/TLS.

Сертификат клиента — указывается режим проверки сертификата клиента (назначение режимов проверки см. выше).

В разделе «Другое» приведены разные дополнительные настройки. Которые могут влиять на работу сервера системы.

Включить сбор дополнительных метрик работы сервера системы — если включено, то система будет собирать дополнительные метрики о своей работе, которые могут быть полезными для диагностики каких-либо проблем в работе системы. Данные метрики вместе с основными доступны в json-файле в архиве, который формируется при сохранении состояния ПК «Бастион-3» в приложении «Монитор состояния».

Использовать подсистему блокировки при редактировании данных — если выключено, система не будет ограничивать одновременное редактирование одних и тех же данных с нескольких рабочих мест.

5.7.2.3. Настройки графики

Для подсистемы тревожной графики ПК «Бастион-3» можно указать ряд параметров:

Инвертировать колесо мыши. Позволяет задать, как будет вести себя план (приближаться или удаляться) при использовании колеса мыши.

Точный расчет текстур – рекомендуется оставлять включенным и отключать только при наличии проблем с отображением планов.

Отключить отрисовку сплайнов – рекомендуется оставлять включенным и отключать только при наличии проблем с отображением планов.

Ширина линий из векторных планов – использовать ли параметр «толщина линии», заданный в используемых векторных планах.

Отрисовка текста на векторных планах – выводить ли объекты, заданные как «Текст» в векторных планах. Рекомендуется оставлять включенным и отключать только при наличии проблем с отображением планов.

Использовать цвета AutoCAD – использовать ли цвета фона и линий, заданные в векторных планах.

Сглаживание – рекомендуется оставлять включенным и отключать только при наличии проблем с отображением планов.

5.7.2.4. Лицензирование

На странице «Лицензирование» отображается информация о ключах защиты, найденных в сети и используемых системой (Рис. 66).

Также, здесь можно задать режим поиска ключей Guardant (По сети, Локальный или Комбинированный).

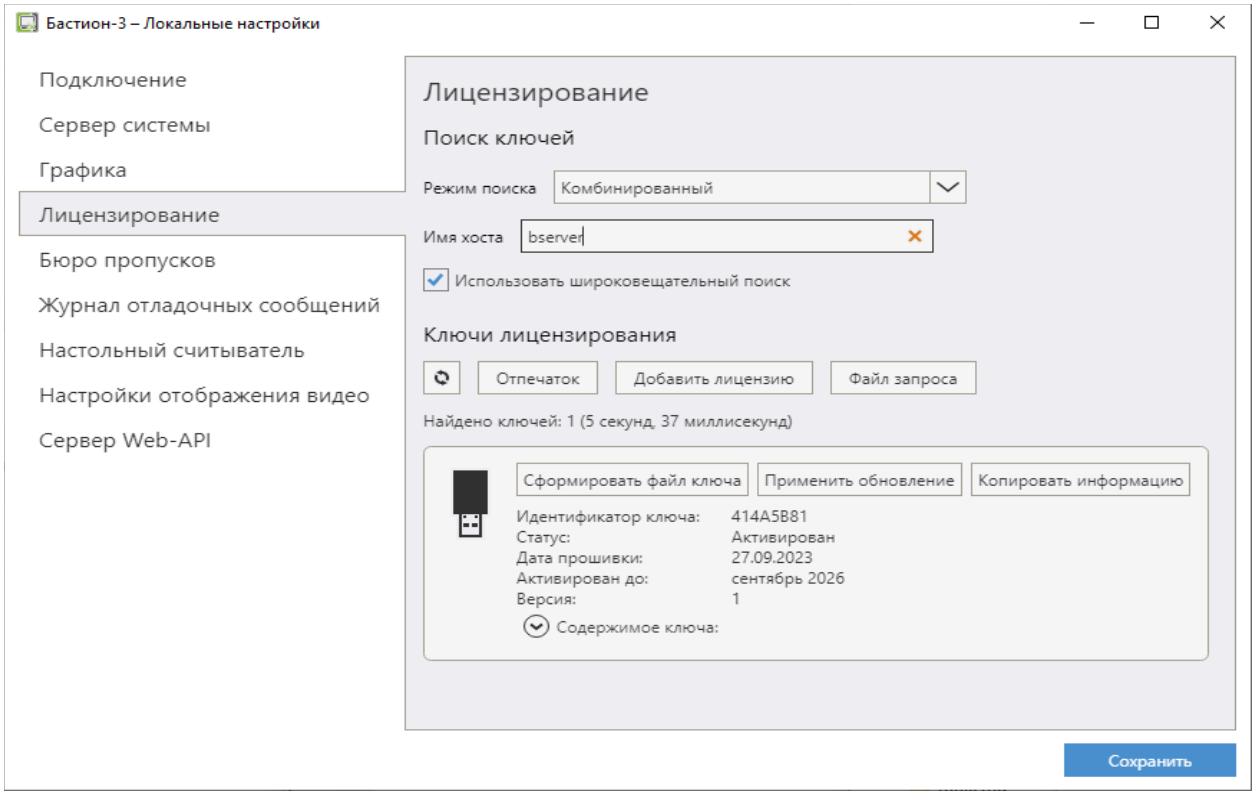

Рис. 66. Страница настройки ключей лицензирования

Можно задать имя хоста, на котором будет производиться поиск ключей, а также отключить широковещательный поиск.

Подробнее о режимах поиска ключей Guardant см. п. 8.4.

Подробно о доступных здесь операциях с ключами см. п. 8.3.2.

5.7.2.5. Журнал отладочных сообщений

В системе есть возможность ведения локального журнала отладочных сообщений. Такой журнал может потребоваться для предоставления в службу технической поддержки при возникновении ситуаций, требующих отладки работы системы.

В параметрах можно задать следующие параметры ведения журнала:

Включить ведение локального журнала отладочных сообщений — позволяет включить или полностью отключить ведение журнала.

Директория хранения — позволяет указать путь, по которому будет записываться журнал. Допускается указание абсолютного или относительного пути (относительно папки установки ПК «Бастион-3»).

Формат хранения — позволяет указать, в каком формате будет записываться журнал. Допустимые значения — Текст или БД SQLite.

Глубина хранения — позволяет задать срок хранения записей в журнале, в днях.

Уровень записи — позволяет задать, какие события будут сохраняться в журнале. Допустимые значения — хранить все события, события не ниже уровней Информация, Предупреждение, Ошибка.

5.7.2.6. Настройка отображения видео

Настройка видеоклиента производится отдельно на каждом рабочем месте, где предполагается вывод видео. Для этого пользователю необходимо открыть локальные настройки Бастиона и выбрать пункт «Настройки отображения видео» (Рис. 67).

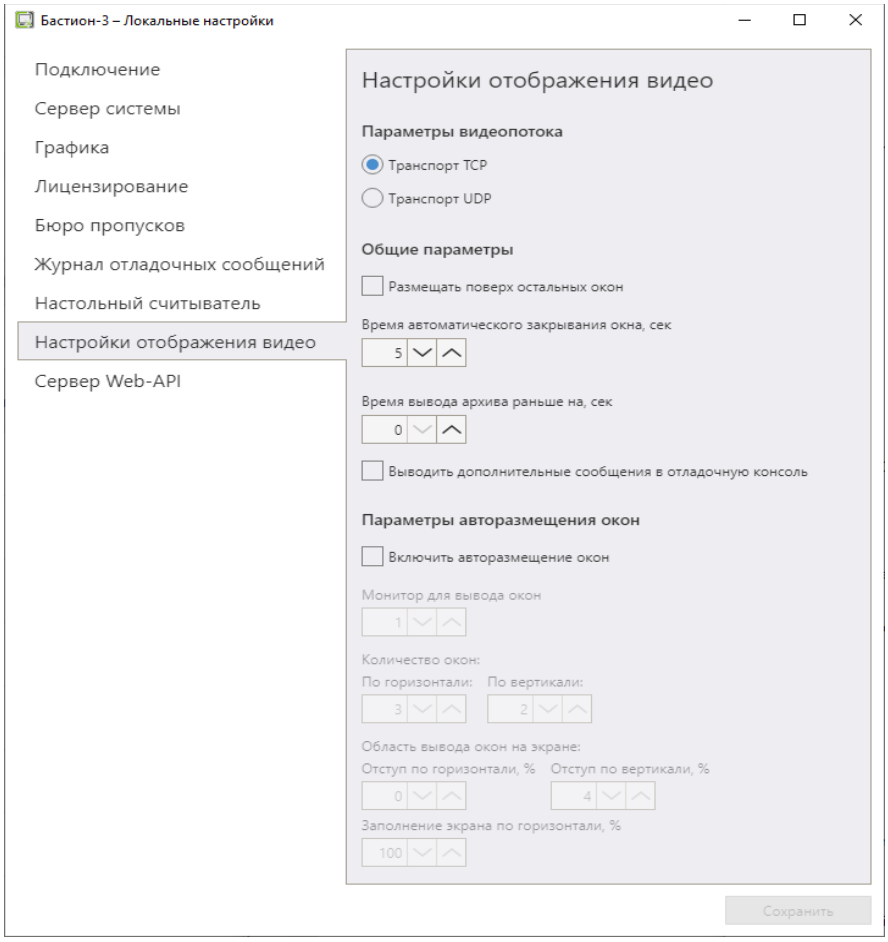

Рис. 67. Настройка отображения видео

В разделе «*Параметры видеопотока*» можно выбрать транспортный протокол, который будет использоваться для передачи потоков по RTSP от видеосерверов к клиенту. Если требуется снизить нагрузку на сеть — рекомендуется выбирать UDP. Если важна целостность получаемых изображений — рекомендуется выбирать TCP.

В разделе «Общие параметры» можно задать следующие настройки:

Размещать поверх остальных окон — указывает драйверу, что все окна с видеоизображением следует открывать поверх всех остальных окон;

Время автоматического закрывания окна, сек — задает время отображения тревожных окон;

Время вывода архива раньше на, сек. – при выводе архивного видео по событиям, архив будет позиционироваться со смещением на заданное количество секунд назад относительно момента возникновения события.

Выводить сообщения в отладочную консоль – при установке параметра будут выводиться отладочные события в отладочную консоль ПК «Бастион-3».

Также можно настроить автоматическое размещение окон на экране. Эта функция позволяет размещать окна с видеоизображениями на экране рядом так, чтобы они не перекрывали друг друга. Если функция отключена, то окна будут открываться в том месте экрана, где они были последний раз размещены, перед тем как их закрыли. Все типы окон (тревожные, архивного и живого видео) отображаются таким образом.

В разделе «*Параметры авторазмещения окон*» можно настроить следующие свойства:

Включить авторазмещение окон — включает/отключает авторазмещение окон;

Монитор для вывода окон — указывает номер монитора, на котором будут отображаться окна;

Количество окон — позволяет настроить количество окон в полиэкране по горизонтали и вертикали;

Область вывода окон — позволяет указать область целевого монитора, где будут выводиться окна с видеоизображениями. Параметры «по горизонтали / по вертикали» указывают отступ в процентном соотношении от разрешения экрана по вертикали и горизонтали от верхнего левого угла монитора, с которого будет отображаться полиэкран с окнами. Параметр «Заполнение экрана по горизонтали» настраивает ширину полиэкрана в зависимости от разрешения монитора в процентном соотношении.

5.7.2.7. Сервер Web API

Настройка сервера Web API производится на странице «Сервер Web-API» (Рис. 68).

В разделе «Подключение к серверу системы» задаются параметры для подключения сервера Web API к серверу системы. Здесь следует указать адрес сервера системы и его порт. Если сервер использует сертификат для подключения, следует выбрать «Использовать SSL/TLS». При необходимости, можно проверять сертификат сервера и его имя, выбрав соответствующие пункты. Для использования сертификата, укажите путь к корневому сертификату, а также сертификат клиента, если это необходимо серверу системы.

> ***Внимание!*** *По умолчанию сертификат клиента не отправляется. Если необходимо отправлять сертификат клиента выберете пункт «Отправлять сертификат клиента».*

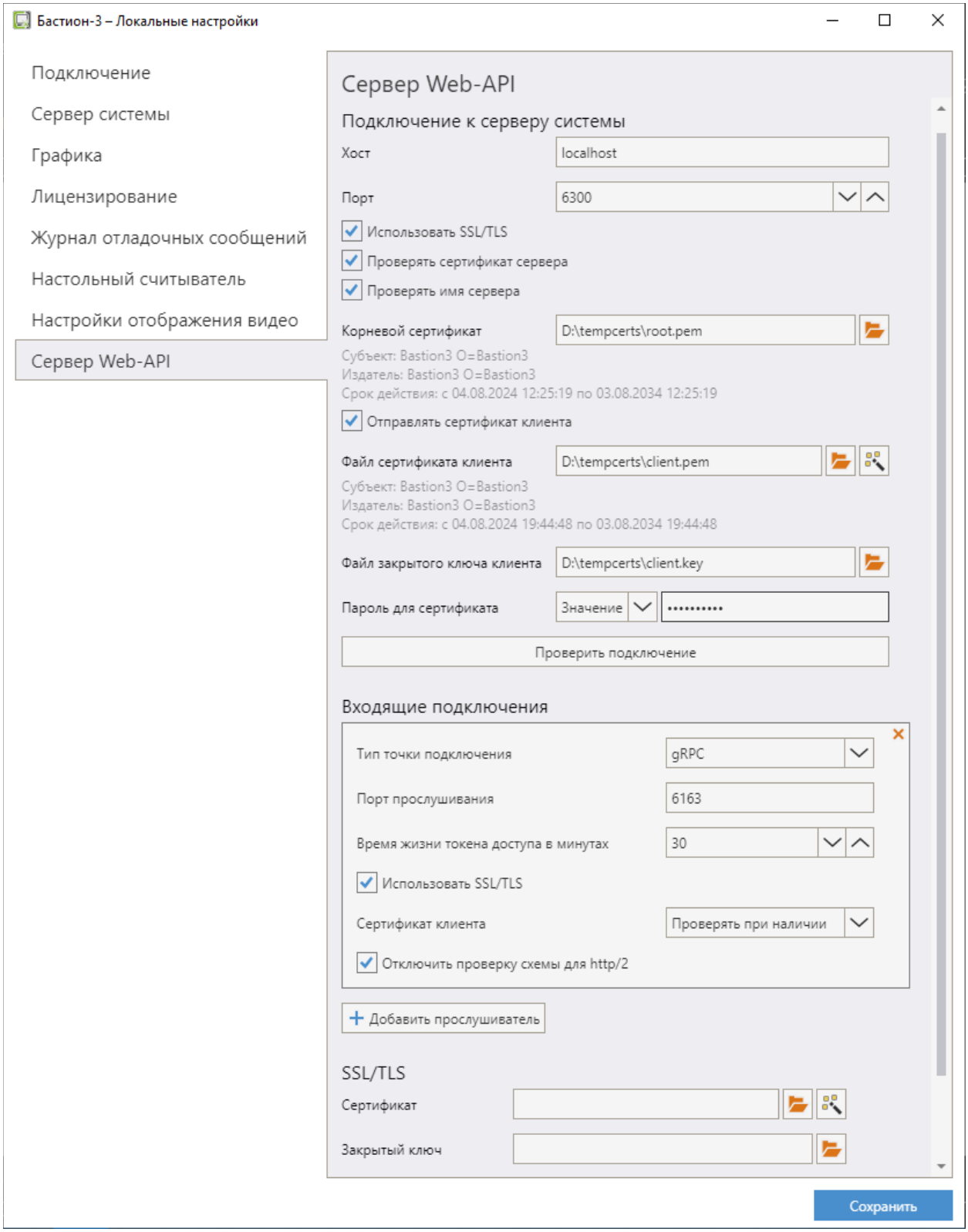

Рис. 68. Сервер Web API

В разделе «Входящие подключения» можно добавить прослушивателей для входящих подключений сторонних клиентов к серверу Web API.

В системе доступны два типа прослушивателей подключений: по WebSocket и gRPC. При добавлении прослушивателя нужно выбрать тип точки подключения, после чего следует задать порт, адрес (для WebSocket) и, если используется сертификат, то выбрать «Использовать SSL/TLS».

Для каждого подключения можно выбрать действие с сертификатом клиента: не проверять, проверять при наличии, всегда проверять. Для каждого прослушивателя подключений с типом gRPC задается время жизни токена доступа в минутах. Также для каждого прослушителя с типом gRPC имеется возможность отключить проверку схемы для http/2.

Имеется возможность добавить несколько прослушивателей входящих подключений (одного или разных типов), однако, каждому прослушивателю должен быть назначен свой уникальный порт.

Раздел «SSL/TLS» используется для настройки сертификатов для работы со входящими подключениями. Можно выбрать файл сертификата, хранящийся на диске, или сгенерировать его, выбрав путь хранения. Также можно выбрать закрытый ключ сертификата, указать соответствующий пароль и корневой сертификат.

Для загрузки сертификат должен быть экспортирован вместе с приватным ключом в файл формата *pfx* или *p12*. По стандарту PKSC#12 сертификат и закрытый ключ хранятся в одном зашифрованном файле, поэтому при загрузке сертификата понадобится ввести пароль от этого файла. Если сертификат загружен корректно и с правильным паролем, то в окне настроек появится издатель, субъект и срок действия сертификата. Если данные поля остались не заполненными, убедитесь в корректности сертификата и его пароля при вводе.

Рекомендуется использовать сертификаты с алгоритмом шифрования *RSA* или *ECDsa* и алгоритмом подписи *SHA256*, *SHA384* или *SHA512*.

5.7.3. Настройка локальных параметров сервера с помощью консольной утилиты BCnfg

5.7.3.1. Общие сведения

Утилита BCnfg запускается с одной из команд. Каждая команда имеет набор параметров.

Во всех случаях изменения настроек, если значение параметра не указано, но сам параметр указан – утилита запрашивает ввод отсутствующего значения.

Если какое-либо значение параметра уже задано в конфигурационном файле, но сам параметр не введен в команде – его значение не обновится.

Если какое-либо значение параметра не задано в конфигурационном файле, но сам параметр не введен в команде – его значение установится в значение по умолчанию.

Перезапись явно введенных параметров – без дополнительного запроса.

При обнаружении ошибки ввода данных (недопустимые значения), утилита завершает работу с выводом сообщения о том, какие параметры были введены некорректно.

При невозможности выполнения команды по любым причинам, утилита завершает работу с выводом сообщения о невозможности выполнения команды, кодом и текстом ошибки (при наличии).

Для работы с утилитой у пользователя ОС должны быть права на чтение и запись в каталоги установки ПК «Бастион-3», и в каталоги с конфигурационными файлами ПК «Бастион-3».

Для просмотра справки по утилите можно выполнить команду BCnfg help.

5.7.3.2. Настройка подключений к серверу системы

Для работы с подключениями к серверам системы используется команда connections.

Команда	Поведение
`BCnfg connections view`	Просмотр параметров (выполняется по умолчанию).
`BCnfg connections set`	Установка параметров подключения и для служб и для приложений.
`BCnfg connections set_svc`	Установка параметров подключения только для служб.
`BCnfg connections set_app`	Установка параметров подключения только для приложений.

Доступные параметры:

`--format=[text|xml|json]`

Задает формат вывода настроек при выполнении команды view (по умолчанию: text).

`--host=ИМЯ`

Имя или адрес сервера системы (по умолчанию при добавлении: localhost).

`--port=ПОРТ`

Указание номера порта сервера системы (по умолчанию при добавлении: 6300).

`--use_ssl=<on|off>`

Включение/отключение использования шифрования (по умолчанию: off).

`--validate_cert=<on|off>`

Включение / отключение проверки сертификата сервера (по умолчанию: off).

`--validate_name=<on|off>`

Включение/отключение проверки имени сервера системы (по умолчанию: off).

`--root_cert_file=ПУТЬ`

Путь к файлу корневого сертификата, используемого при валидации сертификата сервера.

`--cert_file=ПУТЬ`

Путь к файлу SSL-сертификата клиента.

`--private_key_file=ПУТЬ`

Путь к файлу закрытого ключа SSL-сертификата клиента.

`--cert_pwd=PWD_SOURCE`

Способ задания пароля к сертификату. Формат PWD_SOURCE: тип_источника[:параметр источника].

Доступные источники:

- notSet — источник не задан. Используется для сброса пароля.

- direct:ПАРОЛЬ — в качестве источника пароля используется явно заданное значение.
- env:ИМЯ_ПЕРЕМЕННОЙ — в качестве источника пароля используется значение заданной переменной окружения.
- shell:КОМАНДА — в качестве источника пароля используется результат выполнения внешней команды. Команда должна вывести пароль на устройство стандартного вывода и завершиться с кодом 0.

Параметры для команд: `set` и `set_svc`:

`--secret_word[=СЛОВО]`

Секретное слово. Если при добавлении не указано СЛОВО, то значение будет запрошено у пользователя.

`--svc_auth_type=<secret_word|cert>`

Способ аутентификации служб при подключении к серверу системы, доступные варианты:

- secret_word - аутентификация с помощью секретного слова (по умолчанию);
- cert - аутентификация с помощью сертификата.

5.7.3.3. Настройка работы сервера системы

Для работы с настройками сервера системы используется команда net_center.

Команда	Поведение
`BCnfg net_center view`	Просмотр основных параметров сервера системы
`BCnfg net_center set`	Установка параметров сервера системы
`BCnfg net_center add_listener`	Добавление нового порта прослушивания
`BCnfg net_center update_listener`	Редактирования существующего порта прослушивания
`BCnfg net_center remove_listener`	Удаление порта прослушивания

Общие параметры:

`--format=[text|xml|json]`

Установка формата вывод настроек при выполнении команды view (по умолчанию: text).

`--secret_word=СЛОВО`

Секретное слово.

`--operator_name_oid=OID`

Идентификатор имени оператора в имени субъекта сертификата.

`--lock_data=<on|off>`

Включение / отключение блокировки при редактировании данных.

`--gather_additional_metrics=<on|off>`

Включение / отключение сбора дополнительных метрик работы сервера системы.

Параметры портов прослушивания:

`--listener_idx=ИНДЕКС`

Индекс прослушивателя для редактирования или удаления. Обязательный параметр для команд update_listener и remove_listener.

`--port=ПОРТ`

Номер порта прослушивания (по умолчанию 6300).

`--use_ssl=<on|off>`

Включение / выключение защищенного соединения (по умолчанию off).

`--validate_cert_mode=<none|allow|require>`

Режим валидации сертификата клиента (по умолчанию: none).

Параметры SSL/TLS:

`--cert_file=ПУТЬ`

Путь к файлу SSL-сертификата сервера.

`--private_key_file=ПУТЬ`

Путь к файлу закрытого ключа SSL-сертификата сервера.

`-cert_pwd=PWD_SOURCE`

Способ задания пароля к сертификату. Формат PWD_SOURCE: тип_источника[:параметр источника].

Доступные источники:

- notSet — источник не задан. Используется для сброса пароля.
- direct:ПАРОЛЬ — в качестве источника пароля используется явно заданное значение.
- env:ИМЯ_ПЕРЕМЕННОЙ — в качестве источника пароля используется значение заданной переменной окружения.
- shell:КОМАНДА — в качестве источника пароля используется результат выполнения внешней команды. Команда должна вывести пароль на устройство стандартного вывода и завершиться с кодом 0.

`--root_cert_file=ПУТЬ`

Путь к файлу корневого сертификата, используемого при валидации клиентского сертификата.

Параметры подключения к БД:

`--db_host=ИМЯ`

Имя сервера баз данных (по умолчанию: localhost).

`--db_port=ПОРТ`

Порт сервера баз данных (по умолчанию: 5432).

`--db_name=ИМЯ`

Имя базы данных (по умолчанию: bastion).

`--db_user=ИМЯ`

Имя пользователя базы данных (по умолчанию: pro_bastion).

`--db_pwd=ПАРОЛЬ`

Пароль пользователя базы данных.

`--db_use_ssl=<on|off>`

Включение/отключение использования SSL для подключения к серверу баз данных.

`--db_validate_server_cert=<on|off>`

Включение/отключение проверки сертификата сервера баз данных.

`--db_validate_server_name=<on|off>`

Включение/отключение проверки имени сервера базы данных.

`--db_root_cert_file=ПУТЬ`

Путь к файлу корневого сертификата, используемого при валидации сертификата сервера баз данных.

`--db_cert_file=ПУТЬ`

Путь к файлу ssl-сертификата клиента базы данных.

`--db_private_key_file=ПУТЬ`

Путь к файлу закрытого ключа ssl-сертификата клиента базы данных.

`--db_cert_pwd=PWD_SOURCE`

Источник пароля к SSL-сертификату клиента базы данных. Формат PWD_SOURCE: тип_источника[:параметр источника].

Доступные источники:

- notSet — источник не задан. Используется для сброса пароля.
- direct:ПАРОЛЬ — в качестве источника пароля используется явно заданное значение.
- env:ИМЯ_ПЕРЕМЕННОЙ — в качестве источника пароля используется значение заданной переменной окружения.

shell:КОМАНДА — в качестве источника пароля используется результат выполнения внешней команды. Команда должна вывести пароль на устройство стандартного вывода и завершиться с кодом 0.

Параметры WebSocket:

`--ws=<on|off>`

Включение/отключение прослушивания входящих WebSocket-подключений (по умолчанию: off).

`--ws_port=ПОРТ`

Порт прослушивания входящих WebSocket-подключений (по умолчанию: 6363).

`--ws_ssl=<on|off>`

Включение/отключение использования шифрования (по умолчанию: off).

`--ws_validate_cert_mode=<none|allow|require>`

Режим валидации сертификата клиента (по умолчанию: none).

5.7.3.4. Работа с ключами лицензирования

Для работы с лицензиями используется команда license.

Команда	**Поведение**
`BCnfg license view`	просмотр информации о ключах лицензирования (выполняется по умолчанию)

`BCnfg license generate_upd_request`	генерация файла-запроса для обновления ключа
`BCnfg license apply_upd`	применение файла обновления для ключа
`BCnfg license attach_sw_key`	привязка/перенос программного ключа на хост
`BCnfg license detach_sw_key`	отвязка/перенос программного ключа с хоста
`BCnfg license generate_fingerprint`	генерация файла-отпечатка ключа для хоста

Доступные параметры:

`--format=[text|xml|json]`

Установка формата вывод при выполнении команды view (по умолчанию: text).

`--key=ИДЕНТИФИКАТОР_КЛЮЧА`

Ключ, для которого нужно выполнить команду.

`--file=ПУТЬ`

Путь к файлу либо для сохранения (generate_upd_request, detach_sw_key, generate_fingerprint), либо для загрузки данных (apply_upd, detach_sw_key).

5.7.3.5. Настройка режима поиска ключей Guardant

Для работы настройки режима поиска ключей Guardant используется команда license.

Команда	**Поведение**
`BCnfg license set`	Задать параметры поиска ключей Guardant

Доступные параметры:

`--search_mode=<local|network|combine>`

Установка режима поиска ключей (по умолчанию: combine).

`--control_center_host=<имя хоста|ip адрес>`

Имя или IP-адрес хоста, на котором установлен Guardant Control Center.

`--use_broadcast_search=<on|off>`

Включение / отключение использования широковещательного поиска.

5.7.3.6. Настройка журнала отладочных сообщений

Для работы с журналом отладочных сообщений системы используется команда log_storage.

Команда	**Поведение**
`BCnfg log_storage view`	Просмотр основных параметров сервера системы
`BCnfg log_storage set`	Установка параметров сервера системы

Доступные параметры:

`--format=[text|xml|json]`

Формат вывода настроек при выполнении команды view (по умолчанию: text).

`--state=<on|off>`

Включение/отключение службы журнала отладочных сообщений (по умолчанию: off).

`--depth=ГЛУБИНА`

Глубина хранения отладочных сообщений (значение в днях от 1 до 100, по умолчанию: 1).

5.7.3.7. Настройка сервера Web API

Для работы с настройками Web API используется команда web_api.

Команда	Поведение
`Bnfg web_api view`	Просмотр основных параметров сервера Web API
`Bnfg web_api set`	Установка параметров подключения сервера Web API к серверу системы
`Bnfg web_api add_end_point`	Добавить точку подключения клиента к серверу Web API
`Bnfg web_api update_end_point`	Изменить точку подключения клиента к серверу Web API
`Bnfg web_api remove_end_point`	Удалить точку подключения клиента к серверу Web API

Общие параметры:

`--format=[text|xml|json]`

Установка формата вывод настроек при выполнении команды view (по умолчанию: text).

Параметры подключения сервера Web API к серверу системы :

`--host=ИМЯ`

Имя или адрес сервера системы (по умолчанию localhost).

`--port=ПОРТ`

Номер порта сервера системы (по умолчанию 6300).

`--use_ssl=<on|off>`

Включение / отключение использования шифрования (по умолчанию off).

`--validate_server_certificate=<on|off>`

Включение / отключение проверки сертификата сервера системы (по умолчанию off).

`--validate_server_certificate_common_name=<on|off>`

Включение / отключение проверки имени сервера системы (по умолчанию off).

`--root_cert_file=ПУТЬ`

Путь к файлу корневого сертификата сертификата, используемого при валидации сертификата сервера системы.

`--cert_file=ПУТЬ`

Путь к файлу сертификата клиента.

`--private_key_file=ПУТЬ`

Путь к файлу закрытого ключа сертификата клиента.

`--cert_pwd=PWD_SOURCE`

Источник пароля к клиентскому SSL-сертификату сервера Web API. Формат PWD_SOURCE: тип_источника[:параметр источника].

Доступные источники:

- notSet — источник не задан. Используется для сброса пароля.
- direct:ПАРОЛЬ — в качестве источника пароля используется явно заданное значение.
- env:ИМЯ_ПЕРЕМЕННОЙ — в качестве источника пароля используется значение заданной переменной окружения.
- shell:КОМАНДА — в качестве источника пароля используется результат выполнения внешней команды. Команда должна вывести пароль на устройство стандартного вывода и завершиться с кодом 0.

Параметры точки подключения (команды add_end_point, update_end_point и remove_end_point):

`--end_point_idx=ИНДЕКС`

Индекс точки подключения для редактирования и удаления. Обязательный параметр для команд update_end_point и remove_end_point.

`--type=<websocket|grpc>`

Тип точки подключения (по умолчанию grpc).

`--port=ПОРТ`

Номер порта точки подключения. В конфигурацию может быть добавлено несколько точек подключения (одного или разных типов), однако, каждой точке должен быть назначен свой уникальный порт.

`--address=АДРЕС`

Адрес точки подключения.

`--use_ssl=<on|off>`

Включение / отключение использования шифрования для точки подключения (по умолчанию off).

`--validate_cert_mode=<none|allow|require>`

Режим валидации сертификата клиента.

`--access_token_lifetime=ТАЙМАУТ`

Время действия токена доступа, в секундах (по умолчанию 1800).

`--allow_alternate_schemes=<on|off>`

Отключение проверки схемы для http/2 (по умолчанию off – проверка схемы включена).

Параметры SSL/TLS точек подключения к Web API (команда set)

`--api_cert_file=ПУТЬ`

путь к файлу ssl-сертификата сервера Web API.

`--api_private_key_file=ПУТЬ`

Путь к файлу закрытого ключа ssl-сертификата сервера Web API.

`--cert_pwd=PWD_SOURCE`

Источник пароля SSL-сертификату сервера Web API. Формат PWD_SOURCE: тип_источника[:параметр источника].

`--api_root_cert_file=ПУТЬ`

Путь к файлу корневого сертификата, используемого при валидации клиентского сертификата.

6. Расширенные возможности запуска системы

6.1. Параметры командной строки

6.1.1. Синтаксис

Для того что бы проще было понимать синтаксис, приведём пример:

```
shell Bastion.exe --user=q --pwd=q --DebugMode --StartDelay=5000
```

Все параметры командной строки начинаются с символов `--`. Имена параметров регистронезависимые. Параметры бывают двух типов: * Параметр-флаг: `--{имя_параметра}` * Параметр-значение: `--{имя_параметра}={значение}`. Строковое значение, содержащее пробелы, должно быть заключено в двойные кавычки. Правила экранирования стандартные для командной строки: нужны кавычки в тексте – удваивайте кавычки.

6.1.2. Справочник параметров

6.1.2.1. Общие параметры

DebugMode (*параметр-флаг*) – если указан этот флаг, то при запуске будет открыто окно с предложением выбрать отладчик для приложения.

StartDelay (*параметр-значение*) – задаёт целое значение в миллисекундах, на которое приложение будет приостановлено после запуска. Удобно использовать, когда одно приложение должно успеть начать работать раньше, чем другие, например: `shell Bastion.exe --StartDelay=5000 LogViewer.exe` При этом LogViewer точно успеет начать прослушивать отладочный вывод Bastion-а.

IgnoreSingleInstance (*параметр-флаг*) – если задан этот флаг, то при запуске не будет происходить проверка на то, что должен быть запущен только один экземпляр приложения с ролью, которое выполняет приложение.

6.1.2.2. Параметры клиентских приложений

UiTheme (*параметр-значение*) – указание используемой темы при работе приложения. Возможные значения: light, dark.

IgnoreUserSettings (*параметр-флаг*) – не загружать пользовательские настройки, а использовать настройки по умолчанию. Может быть полезным в случае, когда необходимо сбросить существующие настройки (*например, когда окна оказались за пределами монитора*).

6.1.2.3. Параметры приложений, подключающихся к серверу системы

User (*параметр-значение*) – имя оператора, используемое для первичной авторизации.

Pwd (*параметр-значение*) – пароль оператора, используемый при первичной авторизации.

Если заданы оба параметра user и pwd, то при запуске приложение автоматически произведёт попытку авторизации на сервере системы с указанными параметрами.

6.1.2.4. Параметры серверов оборудования

Для отладки работы серверов оборудования необходимо запустить LocalAgent (процесс BAgent.exe) с параметром-флагом *DriverHostDebug*, это отключит автоматический запуск серверов оборудования. Сам сервер оборудования (роль: BDriverHost, процесс: BDriverHost.exe) необходимо запустить, указав параметр-значение *DriverId* – идентификатор типа драйвера, который будет запускаться на сервере оборудования.

6.1.2.5. Параметры сервера системы

TraceSql (*параметр-значение*) – если задано, то в отладочную консоль дополнительно будет выводиться информация о запросах к БД.

6.2. Запуск системы без полномочий администратора

6.2.1. Параметры безопасности NTFS

Обычно, все приложения системы должны работать без прав администратора ОС.

В некоторых случаях, например при использовании некоторых драйверов ПК «Бастион-3» от версии 2.1, требуется дать полные права на каталог, в который установлен драйвер.

Далее приводится инструкция, как дать полный доступ к папке ПК «Бастион-3» и всем её подпапкам всем пользователям компьютера. Настройки, приведенные ниже, гарантировано позволяют работать с ПК «Бастион-3» 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 ПК «Бастион-3» (например, c:\Program Files\ES-Prom\Bastion2) и из контекстного меню выберите «Свойства». В открывшемся окне перейдите на страницу «Безопасность» (Рис. 69).
2. Выберите группу "Пользователи (<ИМЯ_КОМПЬЮТЕРА>\Пользователи)" или “Users (<ИМЯ_КОМПЬЮТЕРА>\Users)”, (Рис. 69).
3. Установите флаг «Полный доступ» в колонке «Разрешить». Например, на Рис. 69 установлен полный доступ для всех пользователей компьютера ANDREYK-VIRTXP.

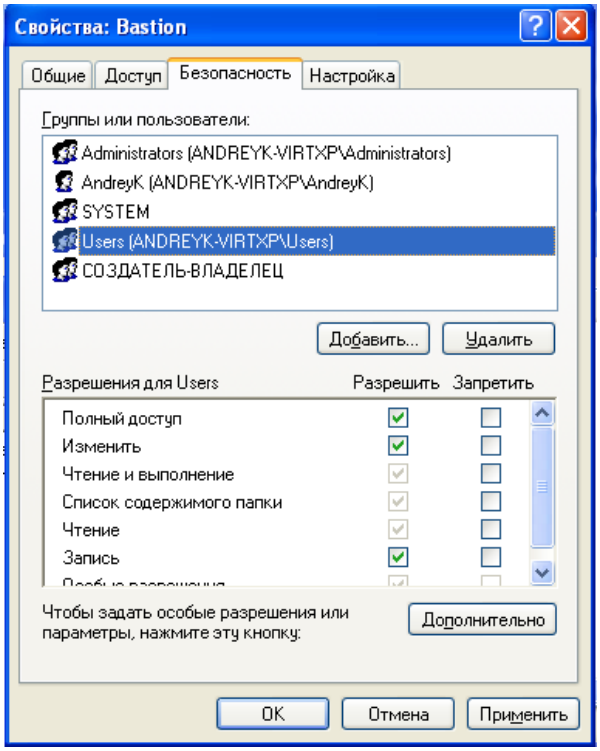

Рис. 69. Предоставление доступа к папке Bastion

4. Нажмите кнопку «Дополнительно». В открывшемся окне (см. Рис. 71) снимите флаг «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне». Появится запрос (Рис. 70), нажмите кнопку «Удалить».

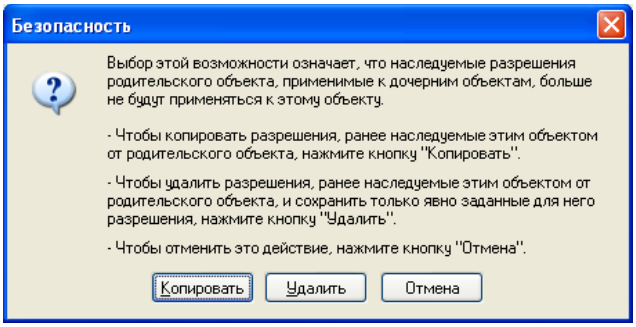

Рис. 70. Запрос подтверждения отмены наследования разрешений

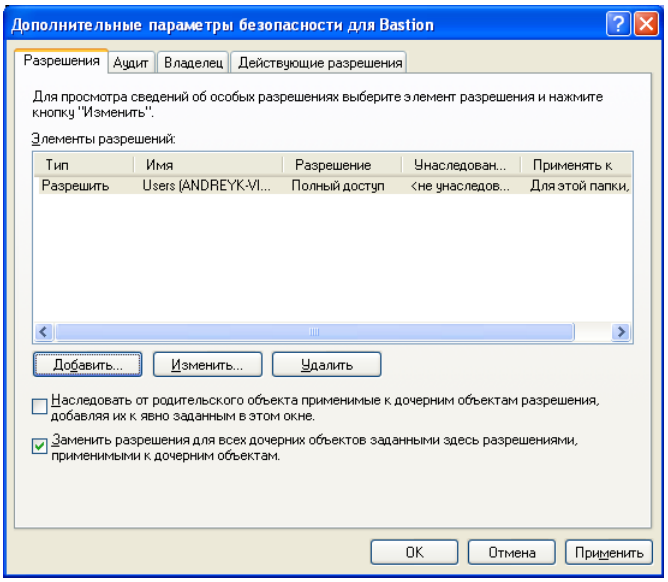

Рис. 71. Дополнительные параметры безопасности папки Bastion

5. В окне дополнительных параметров (Рис. 71) нажмите кнопку «Добавить». Введите имя добавляемой группы (“Пользователи” или “Users”) и нажмите ОК.

6. Появится окно установки прав для группы Users (Рис. 72). Установите флаг «Полный доступ» в колонке «Разрешить», как показано на Рис. 72 и нажмите ОК.

7. В окне на Рис. 72 установите флаг «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Окно должно принять вид, представленный на Рис. 72. Нажмите кнопку ОК.

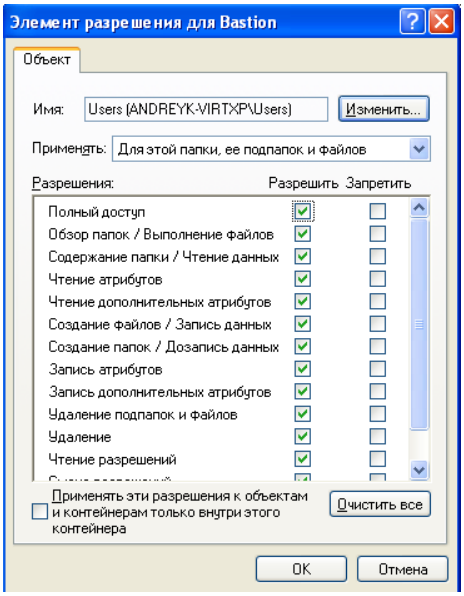

Рис. 72. Установка прав для группы Users

6.3. Настройка подключений при запуске приложений

В окне входа в систему всех приложений ПК «Бастион-3» в нижнем правом углу есть ссылка «Параметры подключения». Нажав её, можно изменить параметры подключения к серверу системы без запуска приложения «Локальные настройки», то есть без необходимости иметь расширенные права пользователя ОС. При нажатии на ссылку появится окно, приведённое на Рис. 73.

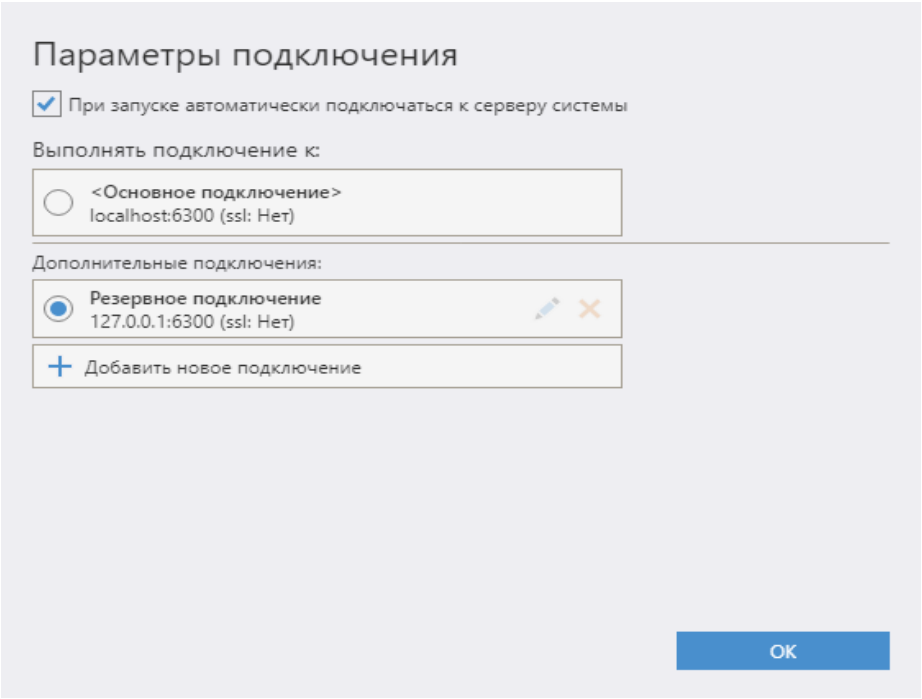

Рис. 73. Настройка параметров подключения при запуске приложений

Параметры основного подключения здесь изменить нельзя, но можно создать дополнительные подключения. Для дополнительных подключений можно задать все параметры, описанные в п. 5.7.3.2. Вид окна представлен на Рис. 74.

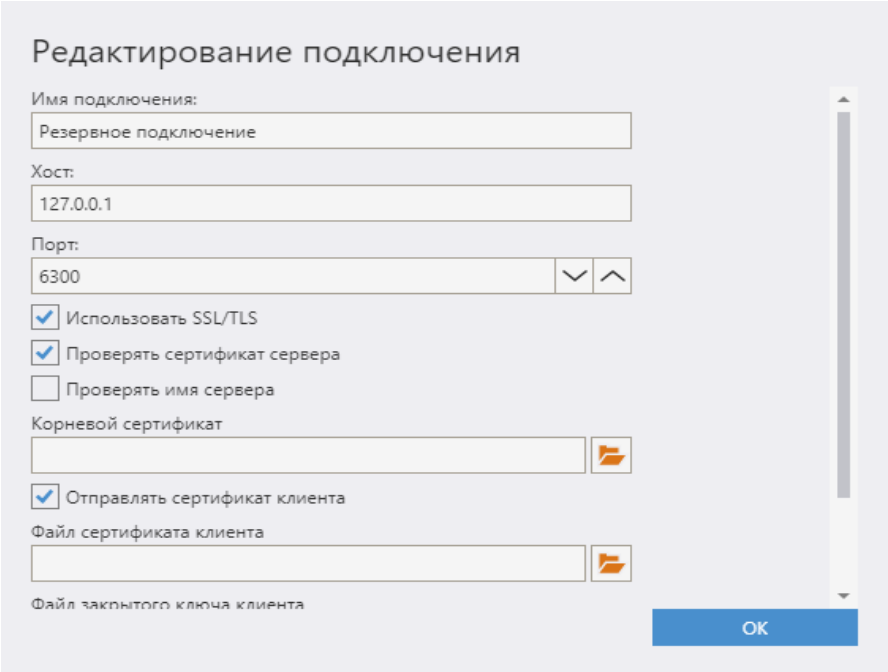

Рис. 74. Редактирование параметров подключения для приложений

Созданные в этом окне подключения сохраняются и будут доступны для использования во всех приложениях ПК «Бастион-3».

7. Мониторинг состояния системы

7.1. Монитор состояния ПК «Бастион-3»

В состав ПК «Бастион-3» входит специальное приложение для мониторинга текущего состояния работы комплекса – «Монитор состояния».

Монитор состояния позволяет просматривать следующую информацию:

1. На странице «Сервер системы» – список и версии установленных модулей сервера системы, адрес сервера системы и его текущее состояние.

2. На странице «База данных» — список и текущий размер таблиц и индексов БД, а также текущее состояние подключения к БД.

3. На странице «Серверы оборудования» - список, текущее состояние подключения и лицензирования, экземпляры выполняющихся драйверов для каждого сервера оборудования в системе (Рис. 75).

4. На странице «Подключения» — список всех текущих подключений к серверу системы, трафик и скорость обмена каждого клиента с сервером, а также длительность подключений, а также статус защищённого соединения SSL/TLS.

5. На странице «Протокол событий» – список сессий протоколирования, интенсивность поступления и скорость записи событий, а также состояние локального кэша протокола.

6. На странице «Лицензирование» – список доступных и занятых лицензий, а также информацию о ключах защиты.

7. На странице «Репликация» — состояние системы репликации пропусков.

8. На странице «ПЦН» — состояние системы ПЦН, состав центров и филиалов и наличие связи с ними.

9. На странице «Журнал отладочных сообщений» — параметры ведения журнала, его текущий размер, число записанных сообщений, а также содержимое журнала.

10. На странице «Локальные модули» — состав и версии установленных локально модулей системы.

11. На странице «Информация о системе» – общие сведения об аппаратном и программном обеспечении компьютера.

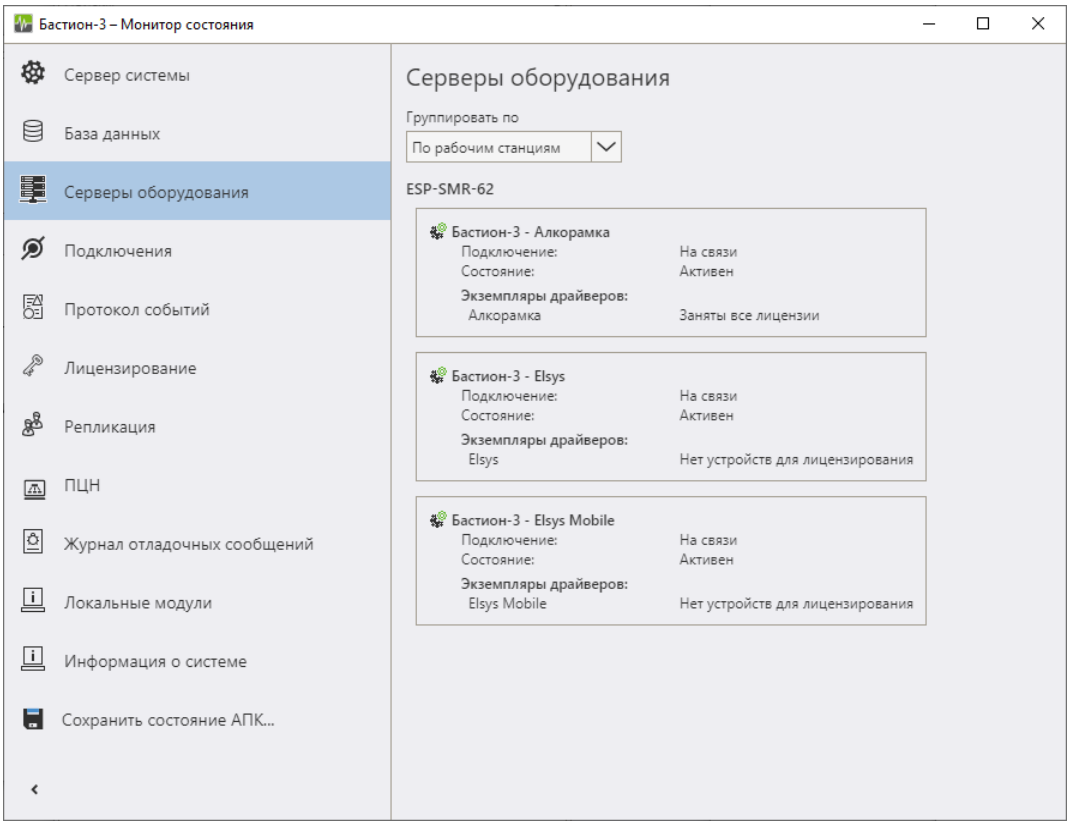

Рис. 75. Страница «Серверы оборудования» монитора состояния ПК «Бастион-3»

В приложении можно сохранить текущее состояние ПК «Бастион-3» в виде архива (Рис. 75). Этот архив можно передать в службу технической поддержки для диагностики каких-либо проблем.

7.2. Отладочные сообщения

7.2.1. Общие сведения

При возникновении нештатных ситуаций в работе, а также в случае необходимости проведения диагностики, система может выводить отладочные сообщения в специальную консоль, а также создавать журнал отладочных сообщений.

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.

7.2.2. Отладочная консоль

«Отладочная консоль» — это отдельное приложение (LogViewer.exe), входящее в комплект поставки ПК «Бастион-3». Отладочная консоль позволяет отслеживать отладочные сообщения всех приложений комплекса в режиме реального времени, а также анализировать сохранённые логи. Общий вид окна отладочной консоли представлен на Рис. 76.

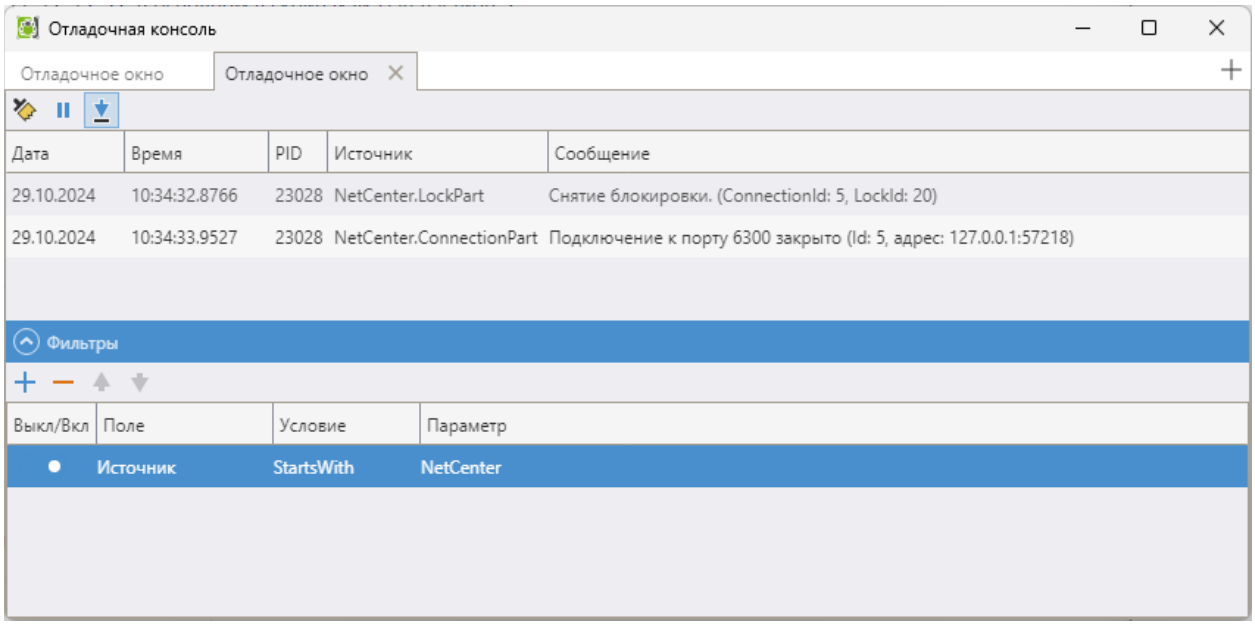

Рис. 76. Отладочная консоль

Для каждого сообщения может выводиться дата, время, источник, идентификатор процесса (PID) и текст сообщения. Список отображаемых полей можно настроить в контекстном меню заголовка таблицы сообщений.

Прием сообщений в консоль можно приостановить, нажав кнопку « ».

Очистить окно текущих сообщений можно, нажав кнопку « ».

По умолчанию, консоль будет пролистывать список в конец при поступлении новых сообщений. Этот режим можно отключить, отжав кнопку « ».

Список сообщений можно отфильтровать по источнику и тексту сообщения. Для этого можно раскрыть панель фильтров и добавить фильтр в список, указав параметры:

Вкл / выкл – определяет будут ли сообщения, соответствующие фильтру включены или исключены из списка сообщений.

Поле – Источник или Сообщение.

Условие – условие, по которому производится поиск. Доступны варианты Equal (равно), Not equal (не равно), StartsWith (начинается с), EndsWith (заканчивается на), Contains (содержит), RegExp (выражение RegExp).

Параметр – значение, по которому будет осуществляться фильтрация.

Отладочная консоль по умолчанию выводит текущие сообщения в режиме онлайн. Также, есть возможность открыть предварительно сохранённый журнал для анализа. Для этого следует нажать кнопку «Открыть журнал отладочных сообщений » в заголовке окна. Журнал будет открыт на отдельной закладке (см. Рис. 76). Фильтры для сохраненного журнала – отдельные.

Отладочную консоль можно выводить поверх всех окон, если нажать кнопку « » в заголовке окна.

Также, можно настроить внешний вид окна отладочной консоли, нажав кнопку « » в заголовке.

7.2.3. Настройка логирования

Настройка логирования производится в приложении «Локальные настройки», которое доступно из «Панели управления» ПК «Бастион-3» (Рис. 77). Соответственно, логирование следует включать и настраивать на каждом компьютере отдельно.

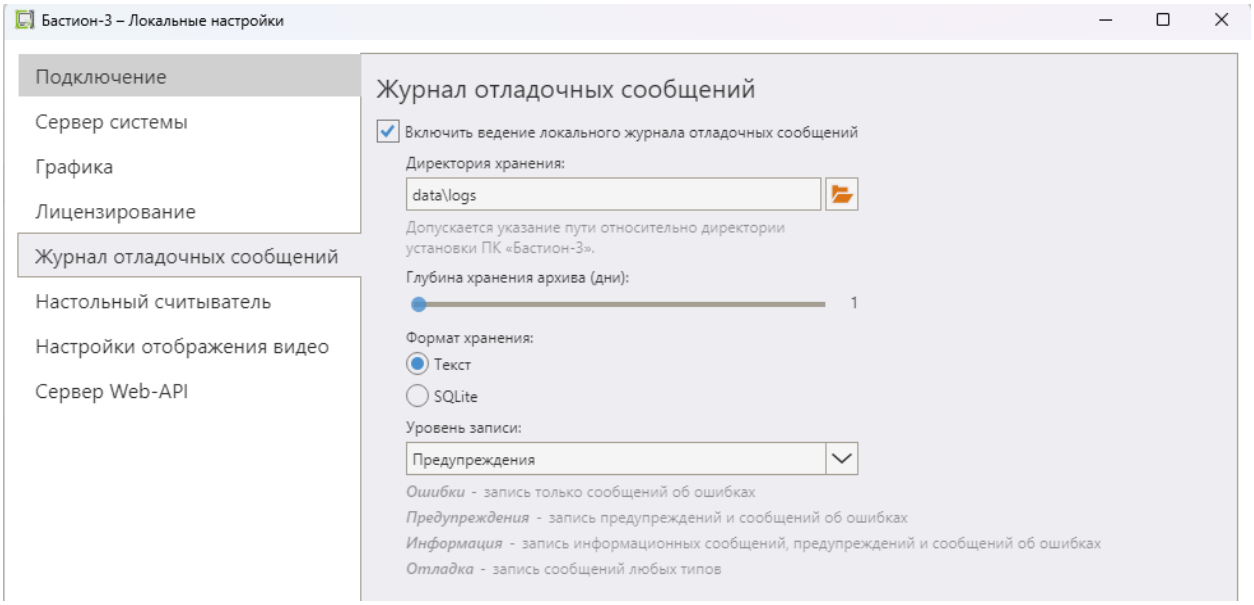

Рис. 77. Настройки логирования

Для включения логирования следует включить флаг «Включить ведение локального журнала отладочных сообщений».

Лог сохраняется в локальную БД, которая затем может быть открыта в «Отладочной консоли». По умолчанию, лог будет сохраняться в каталог «<Bastion3>\data\logs\» в Windows и «/opt/bastion3/data/logs» в Linux.

Также, можно задать глубину хранения архива логов в днях – от 1 до 100. Не рекомендуется хранить длительные логи, так как они могут занимать большой объем дискового пространства и замедлять работу системы.

Также, можно указать *формат хранения логов* — либо в текстовом виде (по умолчанию), либо в виде базы данных SQLite.

Уровень записи определяет минимальный уровень отладочных сообщений, записываемых в лог. Например, если установить уровень «Предупреждения», то в лог будут записываться «Ошибки» и «Предупреждения».

8. Обслуживание системы

8.1. Активация ключей Guardant

Аппаратные ключи Guardant могут поставляться предварительно активированными, либо требовать активации. Активация аппаратных ключей запускает отсчет периода доступа к обновлениям системы. Не активированные ключи не будут использоваться сервером системы.

Программные ключи Guardant всегда требуют активации. Активация программных ключей, помимо запуска периода доступа к обновлениям, выполняет привязку программного ключа к уникальным идентификаторам экземпляра операционной системы и / или оборудования.

Активация ключей производится при помощи модуля «Локальные настройки» на странице «Лицензирование».

Общая последовательность действий при активации ключа:

1. Создать на странице «Лицензирование» в «Локальных настройках» файл с текущей конфигурацией ключа (*.vreq).
2. Отправить полученный файл в службу технической поддержки.
3. Получить файл активации *.vres для ключа Guardant.
4. Применить полученное обновление в «Локальных настройках» на том компьютере, где установлен ключ защиты Guardant.

Перезапускать сервер системы после изменения состава лицензий не требуется.

На Рис. 82 представлено окно работы с ключами лицензирования в «Локальных настройках».

8.2. Активация программного ключа

8.2.1. Активация при помощи мастера лицензий Guardant

Для активации программного ключа следует запустить утилиту «Мастер лицензий Guardant» (license_wizard) на компьютере, где должна быть установлена лицензия.

В правом верхнем углу необходимо выбрать «Активация лицензии» (Рис. 78).

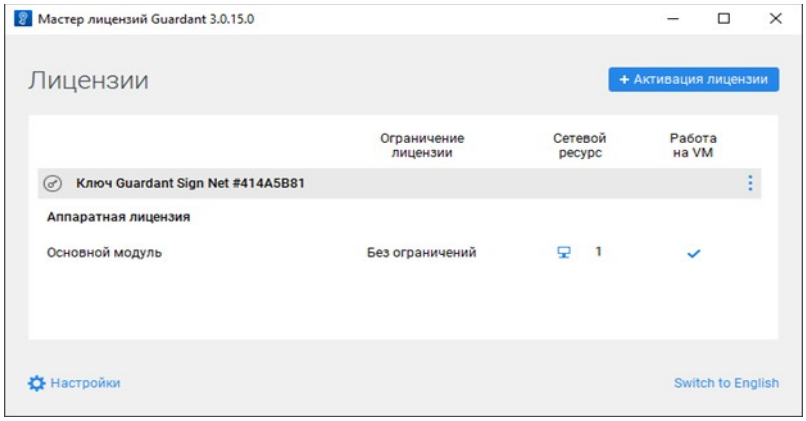

Рис. 78. Активация программного ключа

На следующей странице нужно выбрать «На этом» и нажать ссылку «Оффлайн активация». Затем в области №2 выбрать «Новая лицензия» и сохранить предлагаемый файл *.request

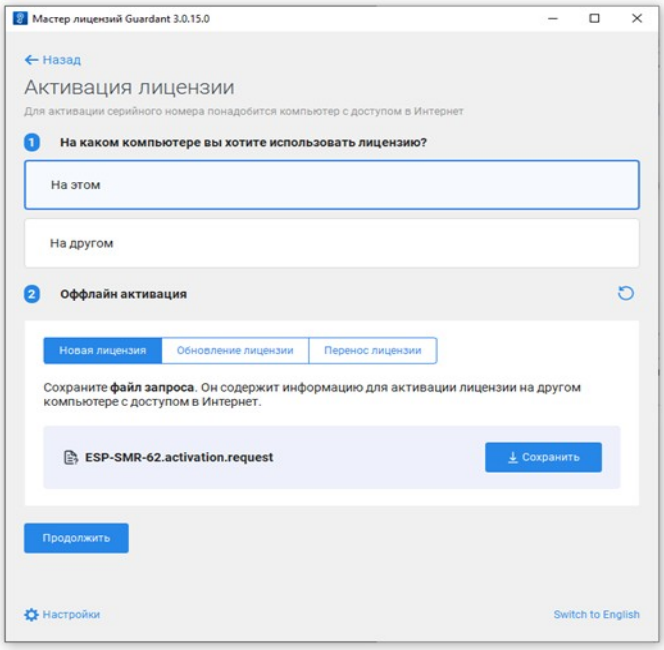

Рис. 79. Форма активации ключа

Сформированный файл нужно отправить в службу технической поддержки поставщика и дождаться получения сформированного поставщиком файла лицензии (*.license), и файла активации (*.vres). В «Мастере лицензий Guardant» (license_wizard) нажать кнопку "Продолжить", а затем кнопку "Продолжить, у меня есть файл лицензии".

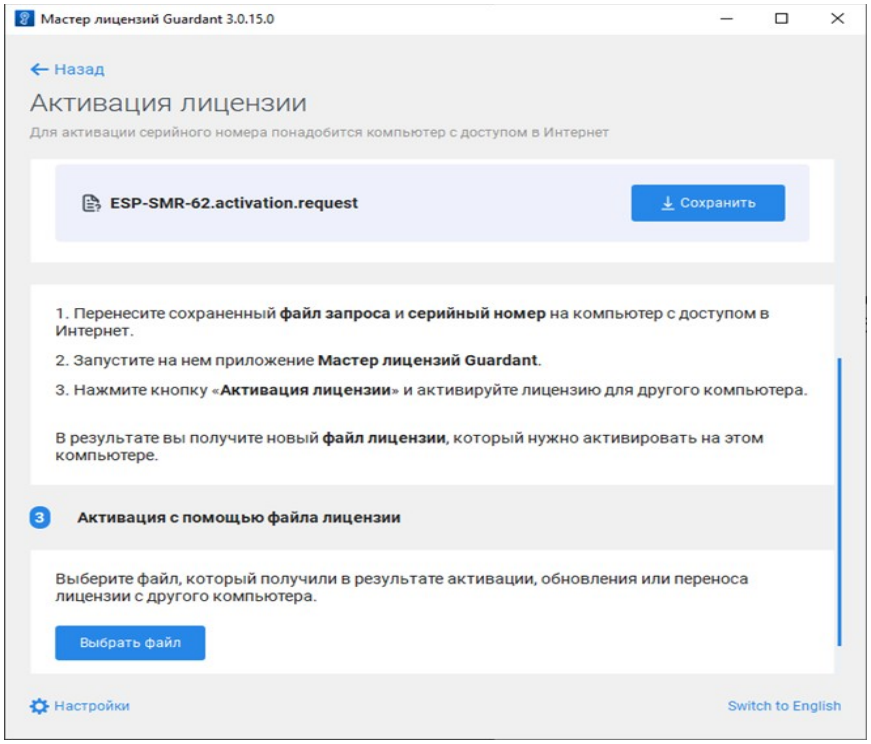

Рис. 80. Активация с помощью файла лицензии

Здесь необходимо загрузить полученный от поставщика файл *.license. После этого в «Локальных настройках» ПК «Бастион-3» должен появиться программный ключ в состоянии «Не активирован».

Затем следует в модуле «Локальные настройки» на странице «Лицензирование» нажать кнопку «Применить обновление» и выбрать файл *.vres, полученный от поставщика.

8.2.2. Активация программного ключа через утилиту «Локальные настройки»

Активировать программный ключ также можно через утилиту «Локальные настройки». Для этого следует открыть страницу «Лицензирование» (Рис. 81).

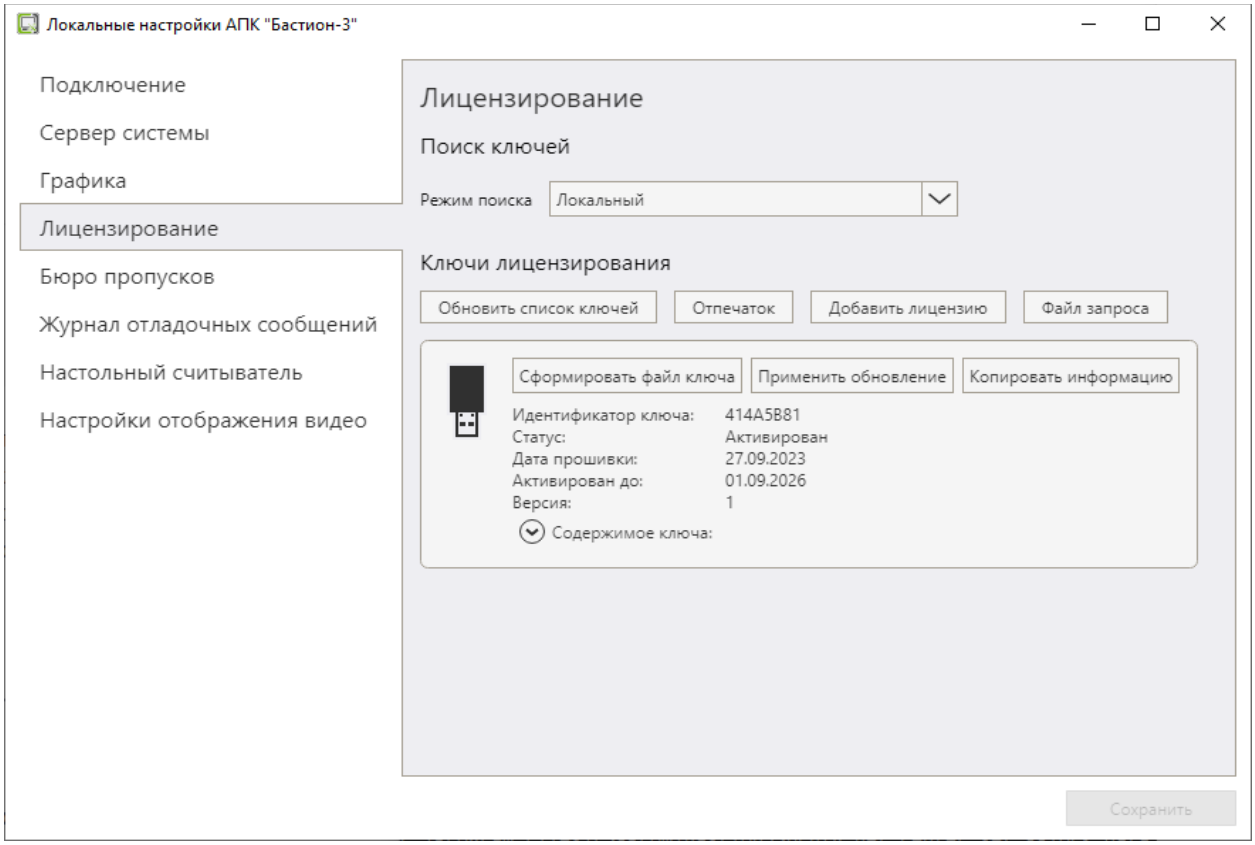

Рис. 81. Страница операции с ключами лицензирования

Для формирования файла запроса лицензии следует нажать кнопку «Запрос файла».

После получения ответных файлов от поставщика, для установки программного ключа следует нажать кнопку «Добавить лицензию» и указать файл *.license.

Для активации программного ключа можно нажать кнопку «Применить обновление» и указать файл *.vres.

8.2.3. Активация программного ключа на компьютере без пользовательского интерфейса

В случае, если необходимо установить программный ключ на компьютер без графического пользовательского интерфейса, можно выполнить следующие команды:

1. Сформировать файл запроса лицензии:

license_wizard --console --activate-request [путь к файлу *.request]

или

Bcnfg license generate_key_request --file=[путь к файлу *.request]

После получения ответных файлов от поставщика:

2. Установить лицензию:

license_wizard --console --activate-offline [путь к файлу *.license]

или

Bcnfg license attach_sw_key --file=[путь к файлу *.license]

3. Активировать лицензию:

```
BCnfg license apply_upd --key=[идентификатор ключа Guardant] --file=[путь к файлу *.vres]
```

8.3. Расширение системы

8.3.1. Общие сведения

Расширение системы производится путём закупки дополнительных лицензий. Лицензии записываются в аппаратный ключ Guardant Sign Net, либо в программный ключ Guardant DL. Обычно, используется 1 ключ на систему. В отдельных случаях может использоваться несколько ключей Guardant. При этом следует учитывать, что ключ с «Сервером системы» в рамках одной системы должен быть один.

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

8.3.2. Работа с ключами защиты

Изменение списка активных модулей производится при помощи модуля «Локальные настройки» на странице «Лицензирование».

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

1. Оплатить дополнительные модули.
2. Создать на странице «Лицензирование» в «Локальных настройках» файл с текущим набором кодов активации vreq.
3. Отправить полученный файл в службу технической поддержки.
4. Получить файл активации модулей vres для ключа Guardant.
5. Применить полученное обновление в «Локальных настройках» на том компьютере, где установлен ключ защиты Guardant.

Перезапускать сервер системы после изменения состава лицензий не требуется.

На Рис. 83 представлено окно работы с ключами лицензирования в «Локальных настройках».

> ***Внимание!*** *В локальных настройках отображается только содержимое установленного локально ключа Guardant.*

На форме отображается текущее содержимое ключа, состояние активации, срок действия доступа к обновлениям системы, номер ключа, дата и версия прошивки.

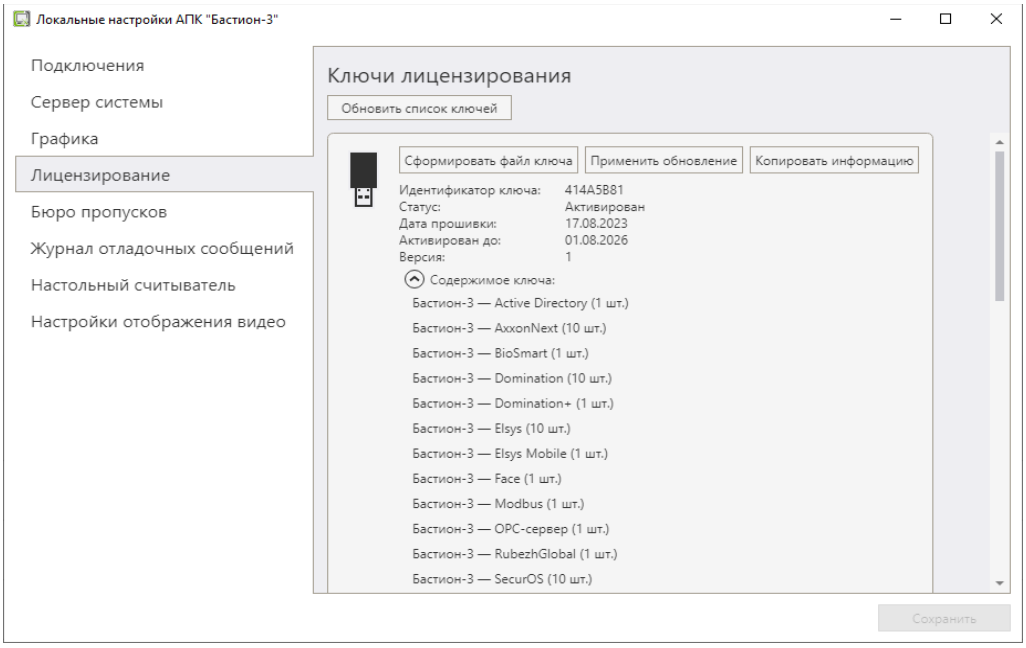

Рис. 82. Форма работы с ключами лицензирования в «Локальных настройках»

Имеющиеся кнопки позволяют выполнить следующие действия:

Сформировать файл лицензии. Будет сформирован vreq-файл, который следует отправить в службу технической поддержки.

Применить обновление. После получения vres-файла от службы технической поддержки эта кнопка позволяет применить обновление из этого файла.

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

Копировать информацию. Информация о ключе лицензирования будет скопирована в буфер обмена.

8.3.3. Установка дополнительных драйверов отдельно

Дополнительные драйверы могут не входить в комплект поставки основного релиза ПК «Бастион-3». Например, если драйвер был выпущен после выхода очередной версии ПК «Бастион-3», то его не будет в основном комплекте поставки.

Такие драйверы можно установить отдельно. Они поставляются в виде msi-пакетов (файл с расширением .msi) для Windows, либо deb и rpm-пакетов для Linux.

Для установки пакета драйвера требуются права администратора ОС.

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

Следует устанавливать драйвер на все компьютеры, оснащённые ПК «Бастион-3».

8.4. Администрирование поиска ключей Guardant

ПК «Бастион-3» использует аппаратные или программные сетевые ключи Guardant для хранения лицензий. Сервер системы проверяет наличие и корректность использования лицензий. В

некоторых случаях может потребоваться использование нескольких серверов системы и ключей Guardant в одной локальной сети. Для настройки такой конфигурации следует учитывать следующую особенность:

> ***Внимание!*** *Сервер системы подключается и занимает все доступные лицензии 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. Это можно сделать через модуль «Локальные настройки», см. 5.7.2.4. , через утилиту Bcnfg (см. п. 5.7.3.5.), через установку переменных среды, а также в Guardant Control Center. Переменные среды используются сервером системы и имеют более высокий приоритет. Доступные переменные:

BASTION_GUARDANT_SEARCH_MODE — поддерживаются значения от 1 до 3: 1 — искать ключи только локально; 2 — искать ключи только по сети; 3 — комбинированный поиск. *BASTION_GUARDANT_USE_BROADCAST* — булево значение: включает или отключает широковещательный поиск в локальной сети. *BASTION_GUARDANT_HOSTNAME* — строковое значение: имя компьютера или IP-адрес того компьютера, где установлен Guardant Control Center, раздающий сетевые лицензии; если параметр не задан, то используется широковещательный поиск внутри локальной сети, если опция BASTION_GUARDANT_USE_BROADCAST включена.

Для ускорения поиска ключей при старте системы следует настроить эти параметры (например, выставив BASTION_GUARDANT_SEARCH_MODE в 1 и BASTION_GUARDANT_USE_BROADCAST в false — тогда ключи будут искаться только на локальном компьютере).

Для настройки параметров поиска ключей через Guardant Control Center, на компьютере, где выполняется сервер системы, следует запустить браузер и перейти по адресу: http://localhost:3189. Для доступа к настройкам по умолчанию используется пароль admin.

Далее, на странице Guardant Control Center следует выбрать пункт «Поиск удаленных лицензий». Здесь можно полностью отключить поиск лицензий в сети, отключить широковещательный поиск в текущем сегменте локальной сети, а также указать список компьютеров, где будет осуществляться поиск.

Для настройки списка компьютеров следует включить флаг «Поиск лицензий по списку адресов» и ввести конкретные IP-адреса или имена конкретных компьютеров. Каждая запись должна быть на отдельной строке. Компьютеры могут находиться в разных сегментах локальной сети.

Например, чтобы ограничить поиск ключей компьютерами GSRV и 192.168.21.55, настройка должна выглядеть так, как показано на Рис. 83.

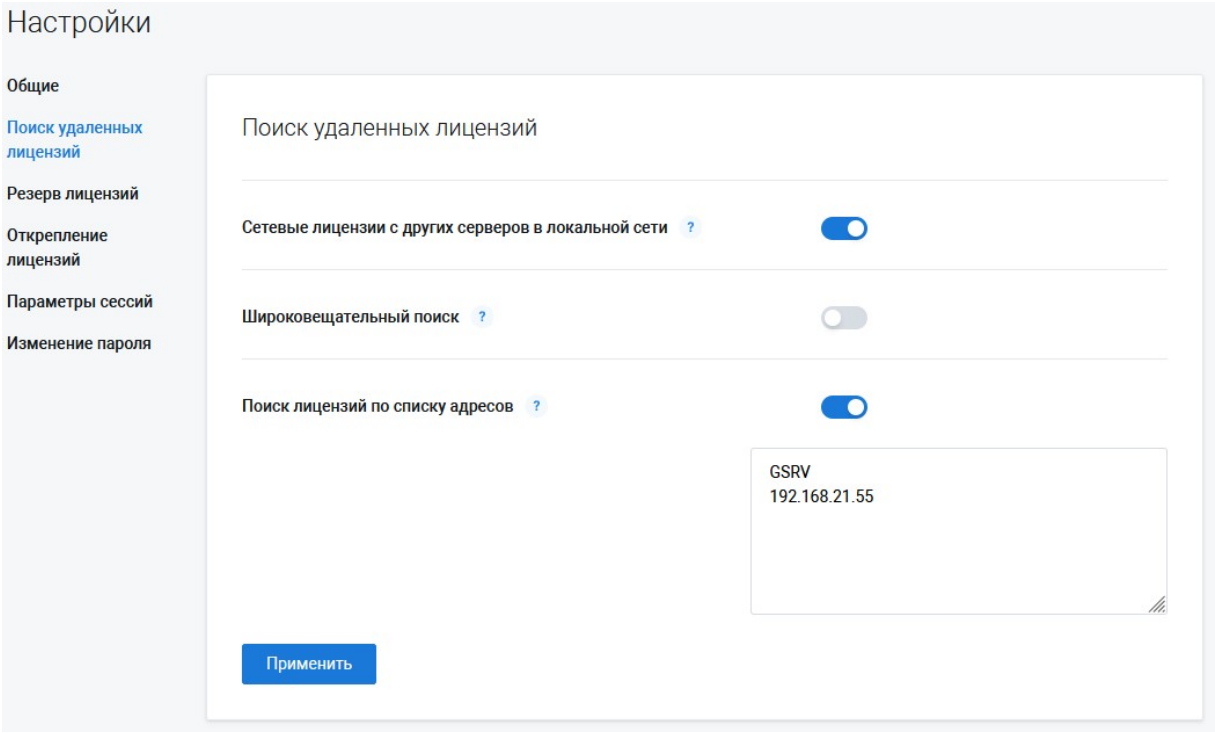

Рис. 83. Настройка режима поиска ключей Guardant

8.5. Смена сервера системы

В случае, если у сервера системы изменился IP адрес, используемый в настройках подключений, необходимо изменить адрес сервера системы **на всех рабочих станциях** с помощью утилиты «Локальные настройки». 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» ПК «Бастион-3» и при необходимости изменить имя компьютера для соответствующей записи.

8.6. Администрирование баз данных

8.6.1. Общие сведения

Для администрирования БД ПК «Бастион-3» предназначена утилита «Управление схемами баз данных». Также, для выполнения задач администрирования могут быть использованы встроенные средства СУБД и сторонние приложения. В этом руководстве приводится описание работы утилиты «Управление схемами баз данных».

Для работы с СУБД PostgreSQL из приложения «Управление схемами баз данных», установленного на компьютер с ОС Linux, необходимо на этот компьютер установить клиентские утилиты psql, pg_dump и pg_restore. Для корректной работы приложения необходимо, чтобы была установлена только одна версия клиентских утилит, совпадающая с версией СУБД. Для работы приложения на компьютере под управлением ОС Windows утилиты устанавливать не нужно, они поставляются вместе с приложением.

8.6.2. Запуск модуля «Управление схемами баз данных»

Для запуска модуля выберите из меню «Пуск» пункт «Управление схемами БД».

При запуске необходимо ввести параметры подключения к БД (Рис. 84):

Тип базы данных – PostgreSQL.

Адрес или имя сервера БД – сетевое имя или IP-адрес сервера БД.

Порт подключения к серверу БД.

Имя пользователя – имя пользователя БД.

Пароль – пароль пользователя.

> ***Внимание!*** *Для выполнения операций создания / удаления баз данных следует указывать пользователя СУБД с соответствующими правами. Это может быть пользователь postgres (суперпользователь СУБД PostgreSQL).*

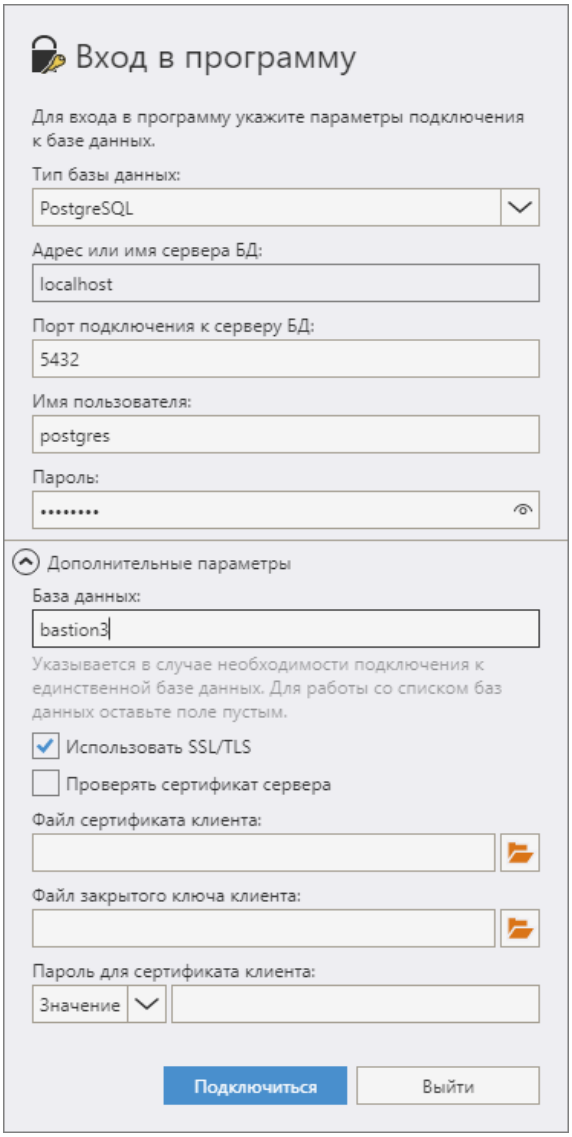

Рис. 84. Форма подключения к серверу БД

Если используется корпоративный сервер СУБД, то может потребоваться подключаться только к одной базе данных, относящейся к ПК «Бастион-3». В этом случае следует открыть «Дополнительные параметры» и указать имя базы данных.

> ***Внимание!*** *Создание новой схемы и удаление существующих схем будут недоступны при подключении к единственной БД.*

Также, поддерживается подключение к СУБД с использованием защищённого канала с SSL/TLS (Рис. 85).

8.6.3. Развёртывание схемы базы данных

Для развёртывания схемы нажмите кнопку «Создать схему» («Создать базу данных») в основном окне модуля «Управление схемами». Откроется окно, приведённое на Рис. 85.

Здесь необходимо ввести параметры создания БД.

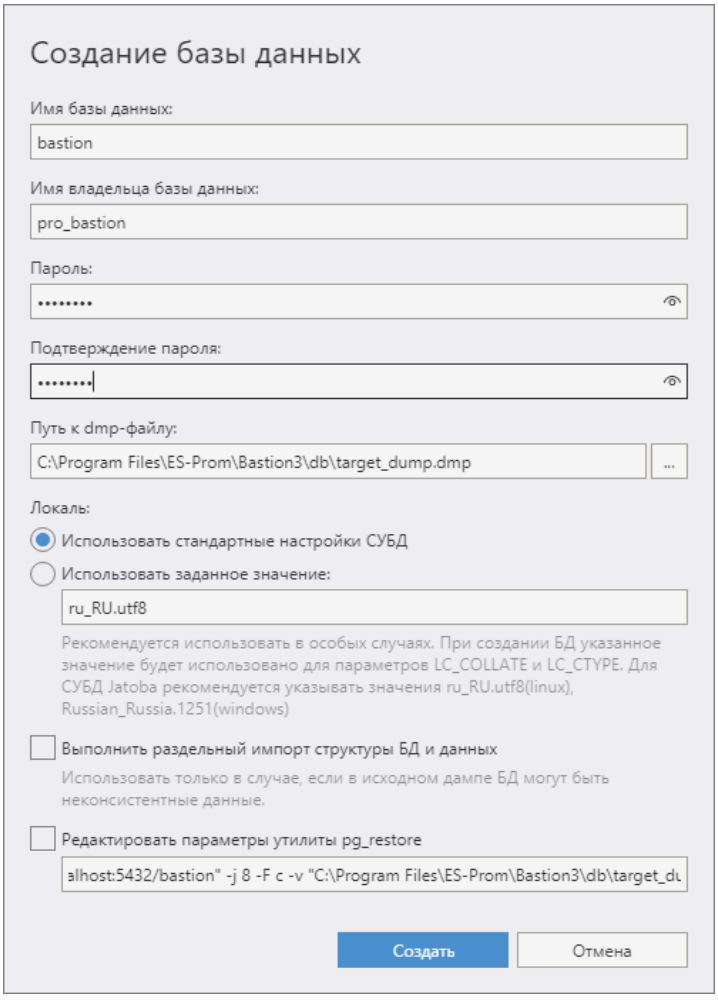

Рис. 85. Форма создания схемы БД PostgreSQL

Параметры для PostgreSQL

Имя базы данных – название БД на сервере PostgreSQL.

Пользователь и пароль – параметры пользователя БД ПК «Бастион-3».

Файл дампа – полный путь к файлу с дампом базы данных. ПК «Бастион-3» поставляется в комплекте с эталонными дампами, расположенным в каталоге <Program Files (x86)>\ES-Prom\Bastion2\Db в Windows и /opt/bastion3/db в Linux.

Локаль — позволяет задать, с какой локалью будет создана БД. При создании БД указанное значение будет использоваться для параметров LC_COLLATE и LC_CTYPE. По умолчанию используются стандартные настройки СУБД из шаблона template0. Также можно задать значение вручную. Для СУБД Jatoba рекомендуется указывать значения ru_RU.utf8(linux), Russian_Russia.1251(windows).

Опция «*Выполнить раздельный импорт структуры БД и данных*» полезна в случае, если обычный импорт БД завершается неудачно из-за наличия неконсистентных данных (например, нарушается ограничение внешнего ключа). С включенной опцией сначала выполняется импорт структуры БД, а затем импорт данных с временно выключенными триггерами БД.

Также, можно вручную отредактировать параметры командной строки утилиты pg_restore, используемой для создания БД (Рис. 85).

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

Рекомендуется перед созданием БД включить запись логов в «Локальных настройках». Это позволить сохранить и проанализировать лог создания БД.

Система также позволяет создавать несколько экземпляров схемы (БД) ПК «Бастион-3» на одном сервере БД и переключаться между ними.

8.6.4. Переключение активной базы данных

Для переключения активной базы данных (той схемы, с которой работают установленные локально модули ПК «Бастион-3») следует воспользоваться утилитой «Локальные настройки» (см. п. 8.6.4.) или утилитой командной строки Bcnfg.

8.6.5. Резервное копирование

Для выполнения резервного копирования выбранной схемы следует нажать кнопку «Экспортировать в файл». Появится окно, приведённое на Рис. 86.

Доступно 2 режима настройки параметров экспорта. В стандартном режиме можно указать путь к файлу, куда будет сохранён дамп и управлять экспортом мандатных атрибутов.

Опция «Не экспортировать мандатные атрибуты и метки безопасности» полезна в случае, когда требуется перенести базу данных с СУБД, работающей под управлением ОС Astra Linux и поддерживающей мандатные атрибуты, на СУБД, работающую под управлением ОС, не поддерживающей мандатное управление доступом. При этом утилита pg_dump на компьютере, на котором запущено приложение «Управление схемами ПК «Бастион-3», должна поддерживать возможность не экспортировать мандатные атрибуты и метки безопасности (параметры --disable-macs и --no-security-labels должны быть в списке доступных параметров, отображаемом при вызове справки для утилиты (pg_dump --help)).

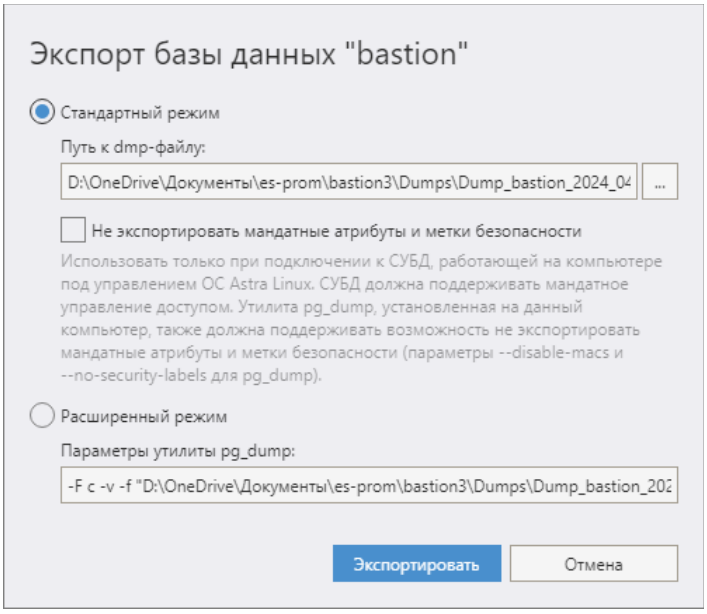

Рис. 86. Форма экспорта дампа БД для PostgreSQL

В расширенном режиме можно вручную отредактировать параметры командной строки утилиты pg_dump, используемой для экспорта.

Задачу выполнения резервного копирования можно автоматизировать. Можно создать скрипт, выполняющий соответствующие команды PostgreSQL, и добавить этот файл в планировщик Windows. Процесс создания таких файлов приведен в следующих разделах.

8.6.6. Настройка автоматического резервного копирования БД ПК «Бастион-3»

Резервное копирование БД можно выполнить с помощью командных файлов, образцы которых входят в комплект поставки системы. Для создания резервных копий в этих файлах используется утилита pg_dump, находящаяся на сервере СУБД PostgreSQL. Файл дампа также создается на сервере СУБД PostgreSQL. Пользователь операционной системы, от имени которого выполняется резервное копирование, должен обладать правами на запись в каталог, где будут создаваться резервные копии, а также правами на запуск утилит архивирования и pg_dump. Предполагается, что БД ПК «Бастион-3» уже развернута.

Файл: **b3-db-backup.cmd (в Windows)** или **b3-db-backup.sh (в Linux)** нужно поместить в каталог с произвольным именем на сервере СУБД PostgreSQL. В ОС Linux необходимо сделать командный файл выполняемым с помощью команды: `chmod +x ./b3-db-backup.sh`

Настройка выполняется в следующей последовательности:

1. Отредактировать файл **b3-db-backup.***. В соответствующих строках нужно указать фактические значения параметров:

   - указать путь расположения утилиты pg_dump (для примера указано как **C:\PostgreSQL\14\bin**);

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

Внимание! *Если требуется, чтобы пароль не указывался в явном виде в командном файле, можно отредактировать конфигурационный файл pg_hba.conf и выставить доверие (trust) для локального соединения с БД ПК «Бастион-3» (см. Рис. 88). Следует учитывать, что в этом случае снижается уровень защищенности соединения с базой данных. При необходимости сохранить исходныё уровень защищенности, рекомендуется использовать специализированные средства резервного копирования БД.*

Внимание! *Если выполняется резервное копирование в СУБД, поддерживающей метки безопасности и мандатные атрибуты, например PostgreSQL 11 в исполнении для Astra Linux, и планируется использовать этот дамп на СУБД PostgreSQL, не поддерживающей мандатных атрибутов, то в команде выполнения резервного копирования после $schema следует добавить --disable-macs —no-security-labels.*

- 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 командном файле и запустить его.

Процесс создания резервной копии выполняется следующим образом:

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

б) утилита pg_dump создает в созданной папке дамп-файл с именем вида

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

в) запускается консольная версия программы архивации, добавляющая дамп в архив с именем вида **ИмяСхемы_ГГГГ-ММ-ДД.zip (или *.tar в ОС Linux)**. Если процесс архивации завершается без ошибок, то исходный дамп удаляется, в противном случае работа завершается, исходные файлы остаются в неизменном виде;

г) архив для повышения надежности хранения может копироваться 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**. Например, создание дампа схемы **bastion** выполнено 09.10.2023 г., тогда в папке **c:**

\backup_dir\2023-10-09 будут файлы **bastion_2023-10-09.zip** и **bastion_2023-10-09.log**. Если в ходе процесса возникают ошибки, нужно выяснить и устранить их причину, после чего снова запустить файл **командный файл создания резервной копии БД**.

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 ПК «Бастион-3».

Для автоматизации создания дампов в ОС Windows следует добавить в планировщик заданий задачу, которая будет запускать в заданное время файл **b3-db-backup.cmd**. Создание задачи в планировщике описано в справочной системе Windows.

Для автоматизации создания дампов в ОС Linux можно воспользоваться планировщиком задач Cron. Для этого следует отредактировать конфигурационный файл crontab, в котором хранятся задания Cron. Это можно сделать, выполнив команду **crontab -e**, от имени пользователя с достаточными правами для редактирования. В файл следует добавить строку вида:

```
0 4 * * * /home/user/backup/b3-db-backup.sh
```

В приведенном примере случае резервное копирование будет запускаться ежедневно в 4 утра.

8.6.7. Сжатие файлов 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**.

8.6.8. Общие рекомендации по резервированию БД ПК «Бастион-3»

Выполнение задачи по созданию дампа следует назначать на время, когда система наименее загружена (например, ночью).

Для создания и хранения дампов не используйте тот же диск, на котором расположены файлы базы данных СУБД. Рекомендуется использовать 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.

8.6.9. Восстановление БД 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. 8.6.5.
2. Удалить схему, которую необходимо заменить. Для этого в форме «Управление схемами БД» следует нажать кнопку «Удалить схему», см. п. 8.6.11.
3. Создать новую схему, используя имеющийся дамп, см. п. 8.6.3.

8.6.10. 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. 140).

8.6.11. 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 ПК «Бастион-3» работать не сможет.*

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

8.6.12. Оптимизация базы данных

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

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.

Статистика размера БД – позволяет посмотреть размер отдельно каждой таблицы БД, а также общий размер БД.

Сброс пароля оператора – позволяет сбросить пароль оператора ПК «Бастион-3» в случае, если старый пароль забыт или утерян.

8.6.13. Удаление устаревших данных

8.6.13.1. Задачи и инструменты удаления устаревших данных

ПК «Бастион-3» не накладывает технических ограничений на срок хранения собственных журналов событий.

ПК «Бастион-3» собирает и протоколирует множество данных, а именно:

- Журнал событий (протокол) системы. Все события от устройств ПК «Бастион-3», 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 доступа к персональным данным. Протоколируются события добавления, доступа и удаления персональных данных по разным категориям. Эти журналы ведутся только при включённом протоколировании доступа к персональным данным.
- Журнал аудита системы. Протоколируются все действия операторов системы, включая информацию об изменениях всех объектов 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;
- Настройки аудита системы;
- Настройки системы аудита доступа к персональным данным;
- Количество пропусков и интенсивность их изменений.

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

В системе предусмотрена возможность архивирования устаревших данных и их удаления из основной базы данных.

8.6.13.2. Ручное архивирование устаревших данных

Для создания архива журнала событий (протокола) системы следует в модуле «Панель управления» выбрать пункт «Обработка событий – Архив протокола» и нажать кнопку +. Появится форма создания архива (Рис. 87).

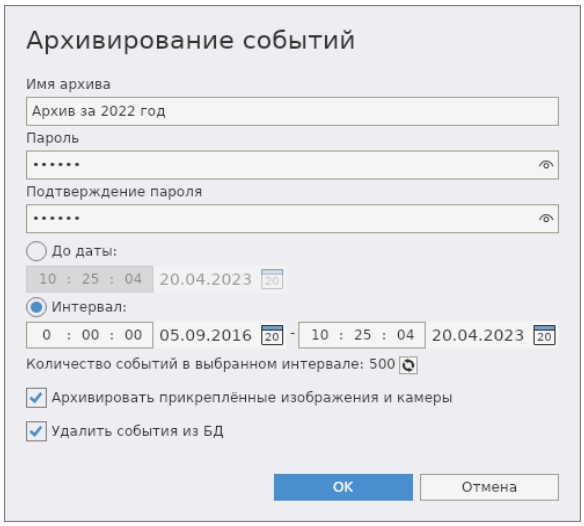

Рис. 87. Форма создания архива журнала событий

Здесь необходимо задать следующие параметры:

Имя архива – название, по которому можно будет выбрать архив в генераторе отчётов. Это же имя будет именем файла, в котором будет сохранён архив.

Пароль – пароль для доступа к архиву.

Интервал или граничная дата для архива («До даты»). В случае выбора граничной даты, в архив будут помещены все события до этой даты. В случае выбора интервала – только события из указанного временного интервала.

Архивировать прикреплённые изображения и камеры. Если включено, в архив будут выгружены привязанные к событиям изображения, а также ссылки на видеозаписи. Следует учитывать, что в этом случае архив может занимать значительно больше места.

Удалить события из БД – при установке флага выбранные события будут удалены из основной базы данных после их архивирования. Таким образом будет выполнена чистка основной БД. Установка этого флага может существенно увеличить время выполнения операции архивирования.

После создания архива он появится в списке архивов (Рис. 88). Созданный архив можно удалить, нажав кнопку −.

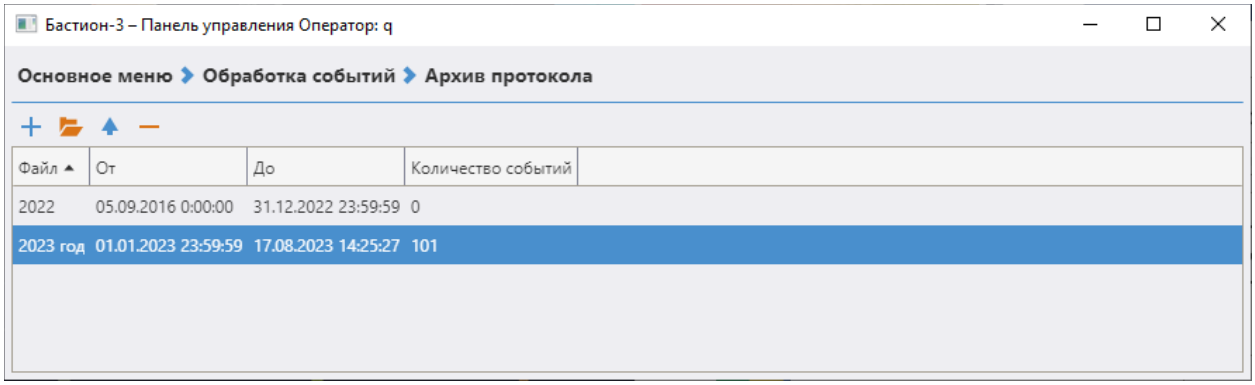

Рис. 88. Форма работы с архивами протокола

> ***Внимание!*** *Не рекомендуется выполнять операцию архивирования устаревших данных при активной работе системы (при наличии интенсивного потока событий).*

Архивы хранятся в отдельных базах данных SQLite в папке <ProgramData>\ES-prom\Bastion3\Archive на сервере системы. В основной БД сохраняются ссылки на выгруженные архивы. Просмотреть события из архивов можно в модуле «Отчёт».

Сохранённый локально архив можно *загрузить в список архивов*, нажав кнопку . В появившемся окне (Рис. 89) следует указать файл, из которого требуется загрузить события и пароль к архиву. Если нажать кнопку «Считать информацию об архиве», то появится информация о периоде архива и количестве событий в нём. После загрузки архива он появится в общем списке доступных архивов.

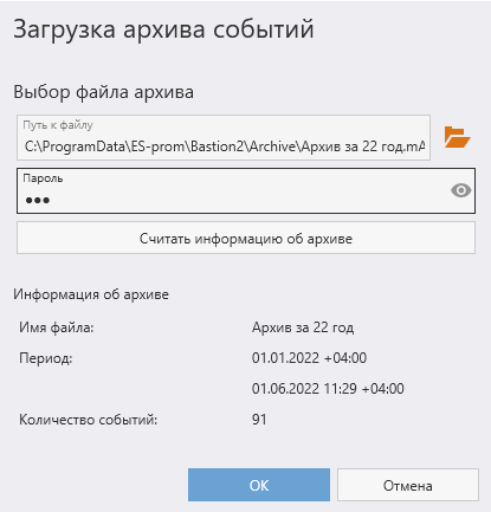

Рис. 89. Форма загрузки архива в основную БД

Также, архив можно выгрузить в локальную папку с сервера системы. Для этого можно нажать кнопку . В появившемся окне следует указать путь к файлу, куда будет сохранён архив. Также можно указать пароль для доступа к загруженному с сервера архиву.

8.6.14. Анализ размера БД

Для просмотра информации о размере БД можно выбрать из меню «Служебные операции» пункт «Статистика размера БД». В появившемся окне (Рис. 90) будет выведена информации обо всех табличных пространствах БД (их используемое место), так же информации о полном размере выбранной схемы.

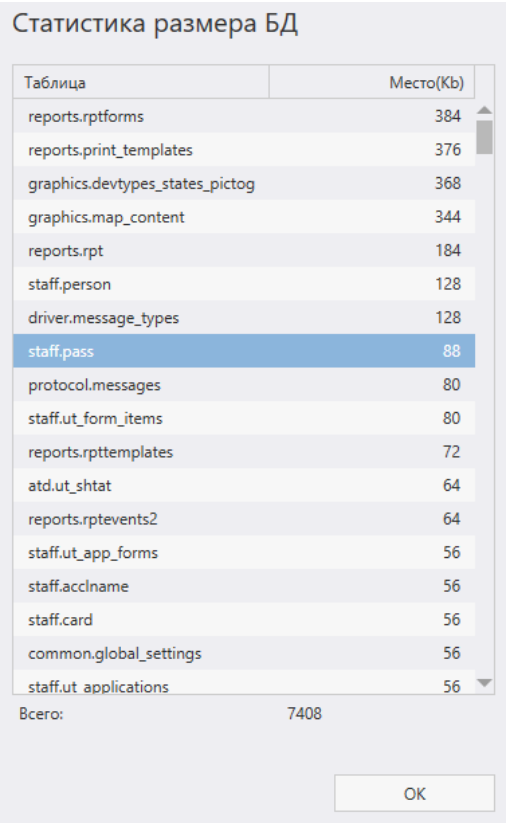

Рис. 90. Информация о размере БД

8.6.15. Смена сервера БД

В случае, если у сервера баз данных изменился IP-адрес или имя компьютера, необходимо проверить настройки подключения к БД в форме «Параметры сервера системы» приложения «Локальные настройки», см. п. 6.1.2.5. , либо через утилиту командной строки Bcnfg.

8.6.16. Обновление схемы

При обновлении версии ПК «Бастион-3» требуется обновление схемы БД с помощью скриптов обновления, поставляемых в пакете инсталляции. Для выполнения обновления следует нажать на кнопку «Обновить схему» в основном окне модуля «Управление схемами». Откроется окно, приведённое на Рис. 91.

> ***Внимание!*** *Перед обновлением схемы необходимо остановить службу Bastion3AgentSvc на сервере системы!*

Модуль обновления автоматически определяет текущую версию базы данных и предлагает обновиться по последней возможной. Для запуска процедуры обновления следует нажать на кнопку «Обновить».

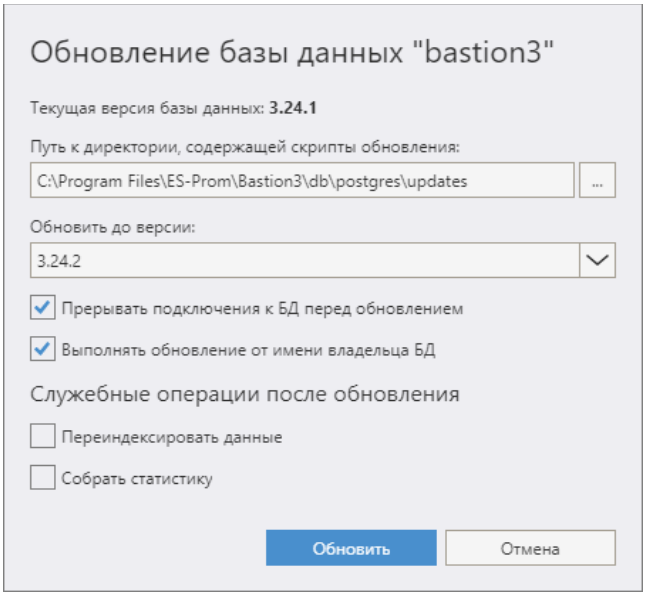

Рис. 91. Форма обновления схемы БД

Если обновление БД выполняется от имени пользователя, не являющегося суперпользователем, то настройку «Прерывать подключения к БД перед обновлением» необходимо отключить.

Если обновление БД выполняется от имени пользователя, не являющегося владельцем БД, то настройку «Выполнять обновление от имени владельца БД» необходимо отключить.

8.6.17. Администрирование БД PostgreSQL при помощи DBeaver

8.6.17.1. Настройка DBeaver

В установочном комплекте ПК «Бастион-3» поставляется бесплатная утилита для администрирования баз данных DBeaver Community Edition (папка Redist\DBeaver).

Для установки DBeaver достаточно запустить установщик и следовать его указаниям. В Linux необходимо установить соответствующий deb или rpm-пакет.

Для русификации интерфейса DBeaver, после его установки, откройте пункт меню Window - Preferences – User Interface - Language, выберите Russian и перезапустите программу.

Для установки соединения с базой данных ПК «Бастион-3» из DBeaver, необходимо добавить сервер PostgreSQL, к которому необходимо подсоединиться, в дерево «Базы данных». Для этого следует нажать ссылку «Новое соединение». В появившемся окне следует выбрать PostgreSQL и ввести имя сервера (будет отображаться в списке), а также параметры соединения (на странице «Соединение»), Рис. 92:

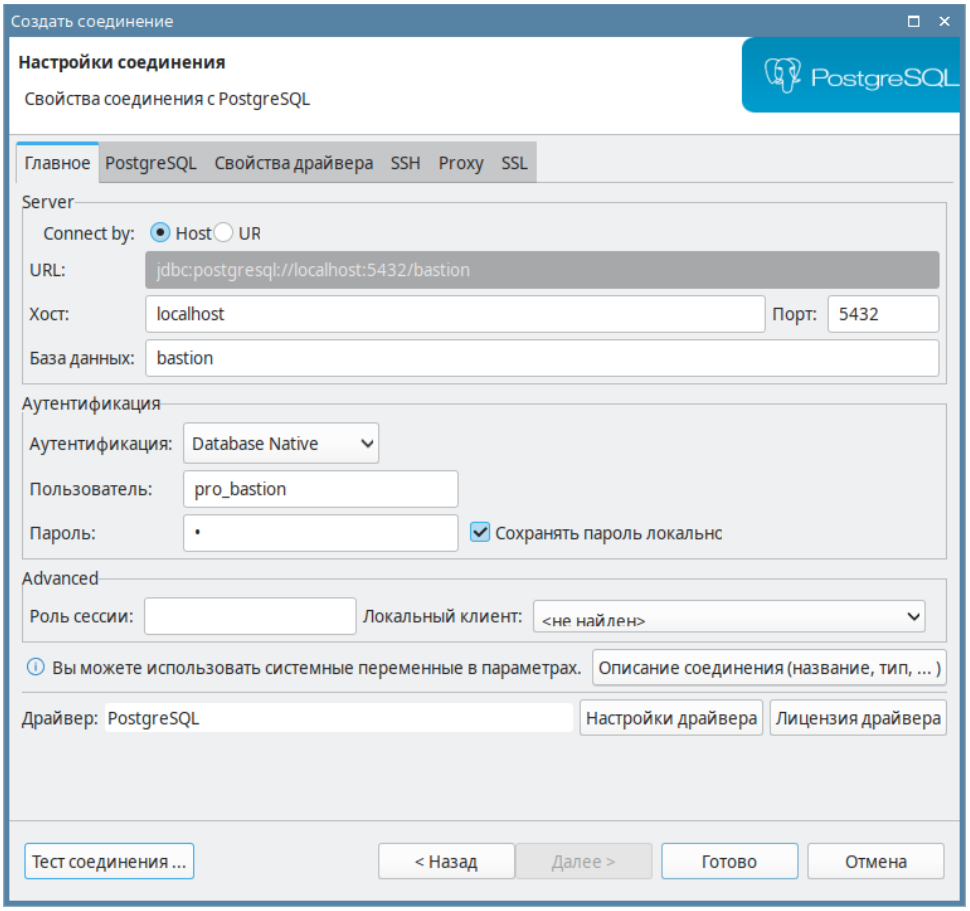

Рис. 92. Параметры соединения с сервером PostgreSQL в DBeaver

8.6.17.2. Выполнение основных операций в DBeaver

С помощью DVeaver 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 «Редактор SQL – Новый редактор SQL». В верхнем поле введите текст SQL-запроса и нажмите кнопку «Выполнить SQL запров (Ctrl + Enter)».

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 View Data.

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 «Экспорт данных...». В появившемся окне (Рис. 93) выберите формат csv, затем укажите имя файла и параметры экспорта данных.

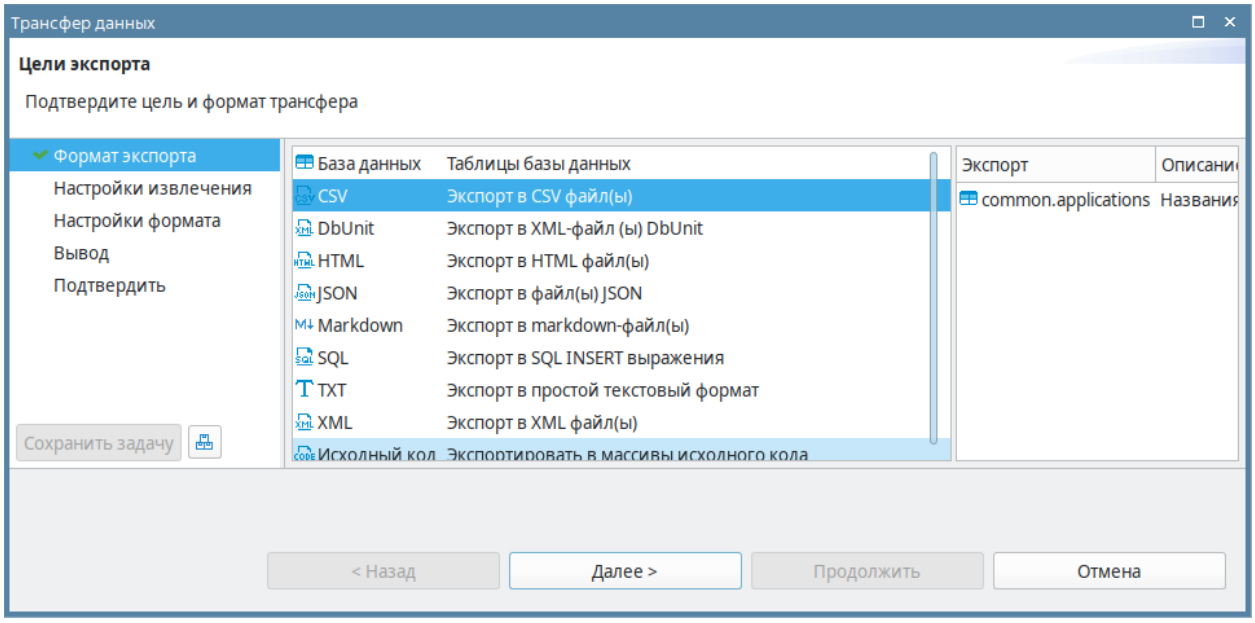

Рис. 93. Установка параметров экспорта данных в DBeaver

Для просмотра подробных инструкции на утилиту DBeaver следует выбрать пункт главного меню «Справка – Оглавление справки».