«Бастион-3». Общее описание системы

Версия 2024.2

(17.04.2024)

Самара, 2024

Оглавление

1 Назначение 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);
- систем противодействия беспилотным летательным аппаратам (БПЛА).

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

ПК «Бастион-3» обладает распределенной масштабируемой 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» поддерживает ряд открытых интерфейсов интеграции, что позволяет использовать его как часть системы управления предприятием. 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».

2 Описание системы

Программный комплекс (ПК) «Бастион-3» представляет собой набор программных модулей, которые становятся активными при наличии на сервере системы необходимых лицензий.

Все программные модули делятся на следующие группы (см. Рис. 1):

- Сервер баз данных;
- Сервер системы и модули его расширения;
- Модули интеграции оборудования и сторонних программных систем (драйверы), выполняемые на серверах оборудования;
- Модули клиентских приложений;
- Мобильные и веб-приложения.

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, выполнения 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.

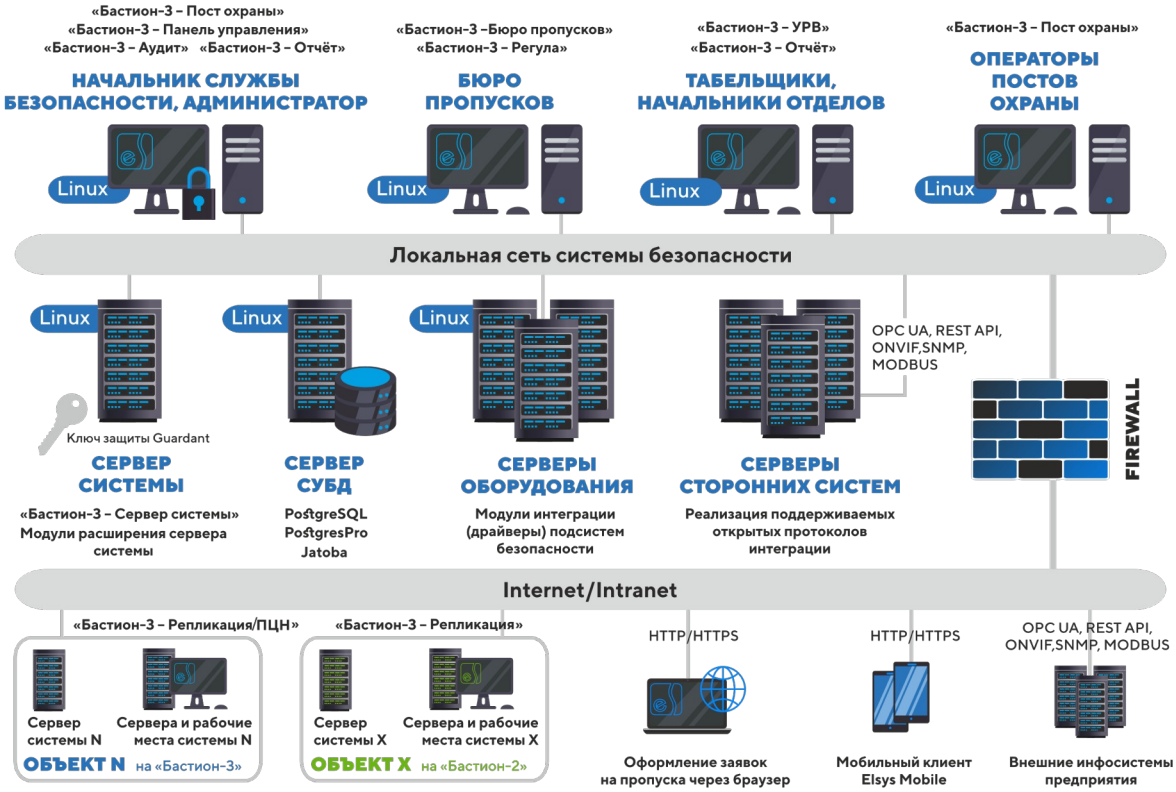

Рис. 1. Структура ПК «Бастион-3»

Серверы оборудования – один или несколько модулей, выполняемых на разных компьютерах (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.

Компьютеры в составе системы могут выполнять роли:

- Сервера базы данных;
- Сервера системы;

- Сервера оборудования;
- Клиентов.

Все роли могут совмещаться на одном компьютере.

Информация о доступных программных модулях записывается в **сетевой ключ защиты** (программный или аппаратный), который должен быть постоянно доступен с сервера системы (обычно, ключ защиты устанавливается непосредственно в сервер системы).

3 Условия применения

3.1 Требования к программному обеспечению

Поддерживаемые операционные системы: Astra Linux 1.7 SE (любые варианты исполнения), 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.

Работа части модулей может обеспечиваться не во всех ОС. Допускается использование других версий ОС, основанных на Linux и поддерживающих установку пакетов в формате DEB или RPM, однако тестирование системы производится на AstraLinux 1.7 SE.

Не рекомендуется использование серверных ОС Windows Server, 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.

> ***Внимание!*** *Все сервера оборудования и сервер системы должны находиться в одном часовом поясе. В противном случае возможны проблемы в работе некоторых модулей интеграции, в частности «Бастион-3 – ELSYS v2».*

Дополнительные компоненты, необходимые для работы комплекса:

- *PostgreSQL 10 или более новый.*
- *.Net Core 8 (для штатной работы системы, достаточно установить только пакет aspnetcore-runtime-8.0).*
- *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.*

3.2 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 1.7 SE, PostgreSQL 14, CPU 2 GHz 2 Cores, 8 Gb RAM, 1000 GB HDD
Клиентские рабочие места	Astra Linux 1.7 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 1.7 SE, PostgreSQL 14, CPU 3 GHz 4 Cores, 16Gb RAM, 1000 GB HDD
Клиентские рабочие места	Astra Linux 1.7 SE, CPU 2 GHz 2 Cores, 8 Gb RAM, 500 GB HDD

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.

3.3 Выбор СУБД

3.3.1 Поддерживаемые СУБД

ПК «Бастион-3» версий 3.x работает под управлением СУБД с открытым исходным кодом PostgreSQL, а также отечественных продуктах PostgresPro или Jatoba.

3.3.2 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.

3.4 Требования к компьютерным сетям

3.4.1 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.

3.4.2 Требования к пропускной способности

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

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

- для каждого модуля «Бастион-3 – Пост охраны» и «Бастион-3 – Отчёт» канал связи с сервером не менее 1 Mbit/s.
- для каждого модуля «Бастион-3 – Пост охраны» с фотоидентификацией и модуля «Бастион-3 – Бюро пропусков» – не менее 2 Mbit/s (размер фотографий должен быть не более 640x480).

Для повышения комфорта работы (быстрая загрузка клиентских приложений, быстрая работа клиентских приложений), 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 не создает прямых соединений клиентов с сервером СУБД. Допускаются временные обрывы связи между некоторыми клиентскими приложениями с сервером системы. Часть приложений необходимо перезапускать после обрыва связи с сервером системы.

Регулярные потери связи с сервером системы являются нештатной ситуацией и говорят о необходимости диагностики компьютерной сети.

3.4.3 Адресация и использование портов

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 модуль.	Настраивается в конфигурации модуля «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.*

4 Использование ПК «Бастион-3» в информационных системах обработки персональных данных

4.1 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».

4.2 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.4.1, 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 операций над ПД.
6. Регистрация выдачи документов на твердую копию.

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

5 Взаимосвязи с другими системами

5.1 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.

5.2 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 – СС 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.

5.3 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».

5.4 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.

5.5 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.

6 Комплектация

Система может поставляться с аппаратным или программным сетевым ключом защиты Guardant.

Аппаратный сетевой ключ защиты Guardant подключается к USB-порту компьютера, исполняющего роль сервера системы. В ключе должны находиться лицензии на все модули интеграции, клиентские приложения и вспомогательные программные модули, которые используются компьютерами в составе комплекса.

При этом не имеет значения, на каких компьютерах будут использоваться те или иные модули. При определении количества модулей указывается **количество одновременно работающих экземпляров** каждого модуля в системе. В процессе эксплуатации модули могут запускаться на любых ПК, входящих в ИСБ на основе ПК «Бастион-3».

Сервер системы ПК «Бастион-3» в каждой системе устанавливается всегда в единственном экземпляре. Исполнение сервера системы определяет список доступных модулей, которые могут

использоваться совместно с этим экземпляром сервера. Исполнение сервера системы не накладывает ограничений на количество пропусков в системе.

Вариант исполнения «Начальный» предназначен для объектов, где не требуются расширенные возможности системы, здесь доступны все наиболее часто используемые подсистемы безопасности, включая ОПС, СКУД, ТВСН.

Доступ к обновлениям системы в течение 1 года с момента записи серверной лицензии в ключ защиты системы.

Вариант исполнения «Стандартный» открывает все основные возможности ПК «Бастион-3» для локальных объектов, включая поддержку периметральных систем охраны, поддержку всех видов биометрии, использование модулей поддержки открытых протоколов интеграции, возможности использования API ПК «Бастион-3».

Доступ к обновлениям системы в течение 2 лет с момента записи серверной лицензии в ключ защиты системы.

Вариант исполнения «Корпоративный» дает доступ ко всем возможностям системы без ограничений. По сравнению со «Стандартным», добавляются возможности построения распределенных систем на базе ПК «Бастион-3» и возможность использования самых современных технологий, таких как системы противодействия БПЛА. Подходит для объектов транспортной инфраструктуры.

Доступ к обновлениям системы в течение 3 лет с момента записи серверной лицензии в ключ защиты системы.

Модуль «Бастион-3 – Пост охраны» предназначен для организации рабочего места охранника / оператора проходной. Обеспечивает оперативное наблюдение за текущей ситуацией и событиями и оперативное управление устройствами, в соответствии с заданными полномочиями и расписаниями. Настраиваемый пользовательский интерфейс модуля позволяет сделать взаимодействие программы и оператора максимально доступным и удобным для определенного сотрудника и/или роли в процессе функционирования системы безопасности.

Модуль «Бастион-3 – Бюро пропусков» позволяет автоматизировать операции (создание, редактирование, удаление пропусков, настройка уровней доступа, временных зон, праздничных дней, централизованное внесение в систему биометрических идентификаторов, хранение архива пропусков и т.д.), производимые со всеми видами пропусков, поддерживаемых в системе «Бастион-3». Включает подсистемы создания макетов пропусков и печати на картах доступа. Поддержка работы с материальными и транспортными пропусками доступна при наличии серверной лицензии «Бастион-3 – МТП».

Модули «Бастион-3 – УРВ», «Бастион-3 – Отчет» позволяют запустить на любом ПК по одному экземпляру генераторов соответствующих отчетов.

Исполнение модулей интеграции выбирается по количеству подключаемых к системе приборов/видеоканалов. Способ подключения устройств может быть любым из предусмотренных производителем приборов: к одному порту, к нескольким портам, к разным серверам оборудования, к сети Ethernet, а также комбинация этих вариантов.

При запуске модуля интеграции выполняется проверка числа приборов, разрешенных в ключе защиты, и их фактического количества в системе. Место и способ подключения приборов к ПК значения не имеет.

Можно приобрести несколько разных или одинаковых исполнений одного и того же модуля. В этом случае число поддерживаемых приборов суммируется. Например, для поддержки 140 контроллеров ELSYS можно приобрести 14 лицензий на «Бастион-3 – ELSYS» (Исп.10).

Модули интеграции видеосистем комплектуются исполнениями по 10 каналов. То есть, если необходимо обеспечить работу 26 видеоканалов, следует приобрести 3 модуля, работающих с десятью каналами. Для некоторых модулей интеграции видеосистем существуют дополнительные **модули расширения функциональности**. Эти модули добавляют возможности получать события аналитических детекторов камер и приобретаются дополнительно к основному модулю интеграции. Приобретение модуля расширения функциональности возможно только в дополнение к соответствующему модулю интеграции. Модули расширения функциональности поставляются поканально (по 1 каналу).

Модули интеграции биометрических считывателей могут использоваться совместно с любой СКУД.

Модули интеграции комплексов биометрической идентификации по изображениям лиц («Бастион-3 – SecurOS FaceX», «Бастион-3 – Face») требуют наличия контроллеров ELSYS-MB (Light, Std, Pro, Pro4) или ELSYS NG, подключенных через ELSYS-MB-Net или ELSYS-MB-Net-II для управления запирающими устройствами, и модуля «Бастион-3 – Elsys» для настройки и проверки полномочий пользователей СКУД.

Те же требования для управления запирающими устройствами предъявляются и модулем «Бастион-3 – Elsys Mobile».

Модуль **«Бастион-3 – ИКС»** может работать одновременно с несколькими ПК «Бастион-3». Для каждой из систем, обслуживаемых этим модулем, необходимо приобретать отдельный ключ активации. Например, если 3 объекта с установленным ПК «Бастион-3» необходимо интегрировать с единой системой VisitorControl, то необходимо приобрести 3 экземпляра ключа активации на модуль «Бастион-3 – ИКС» – по одному на каждый интегрируемый объект.

Модули **«Бастион-3 – Веб-заявка»**, **«Бастион-3 – ИКС»**, в связи с особенностями их архитектуры, дополнительно используют процедуру активации с привязкой к аппаратной конфигурации компьютера. Активация выполняется в момент установки системы, при наличии в ключе защиты соответствующих позиций. Для активации необходимо обратиться в службу технической поддержки. При переносе этих модулей на другой компьютер необходимо провести повторную активацию.

Модуль «Бастион-3 – ПЦН» обеспечивает работу подсистемы передачи событий между ИСБ автономных объектов, каждый из которых имеет свой сервер базы данных. Ключ активации этого м**одуля должен быть записан только в ключ объекта, на котором расположен пост централизованного наблюдения**. Количество модулей - 1 экземпляр на каждый автономный объект со своей БД, подключаемый к данному ПЦН.

Модуль «Бастион-3 – Репликация» обеспечивает работу подсистемы репликации (синхронизации данных) пропусков пользователей между автономными объектами, имеющими собственные базы

данных пользователей. Для каждого объекта, участвующего в репликации, в его ключ защиты записывается 1 экземпляр модуля.

Модуль **«Бастион-3 – СС ТМК»** предназначен для передачи событий из ПК «Бастион-3» в **систему сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры (СС ТМК)**. Модуль поставляется в составе ПАК-ов, сертифицированных на соответствие требованиям постановления Правительства РФ №969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности». Модуль обеспечивает выполнение в ПК «Бастион-3» требований указанного постановления к системам сбора и обработки информации.

Полный перечень модулей ПК «Бастион-3» доступных для заказа представлен в прайс-листе, размещённом на официальном сайте ГК «ТвинПро» – https://www.twinpro.ru/kupit/prices/.

7 Список сокращений

Термин	Определение
ПК	Программный комплекс
АСЗП	Автоматизированная система заказа пропусков
БД	База данных
ИКС	Интеграция кадровых систем
ИС	Информационная система
ИСБ	Интегрированная система безопасности
МТП	Материальные и транспортные пропуска
ОПС	Охранно-пожарная сигнализация
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПД	Персональные данные
ПМВ	Программно-математическое воздействие
ПЦН	Пост централизованного наблюдения
СКУД	Система контроля и управления доступом
СОО	Система охранного освещения
СОП	Система охраны периметра
СОТ	Система охранная телевизионная
СС ТМК	Система сбора результатов технического мониторинга и контроля
ССОИ	Система сбора и обработки информации
СУБД	Система управления базами данных
УРВ	Учёт рабочего времени на основе данных СКУД

OPC	OLE for Process Control
OPC-DA	Протокол Data Access стандарта OLE for Process Control
SNMP	Simple Network Management Protocol
XML	Extensible Markup Language

8 Глоссарий

Авторизация — это предоставление определённых прав.

Если идентификация и аутентификация прошли успешно, и пара логин-пароль верны, то система предоставит пользователю доступ к его ресурсам, то есть произойдет *авторизация*.

Процесс всегда происходит только в таком порядке: идентификация, аутентификация, авторизация.

Аутентификация — это процедура проверки подлинности, доказывающая, что пользователь именно тот, за кого себя выдает.

После идентификации следует процесс аутентификации, в котором пользователю нужно доказать, что он является человеком, который регистрировался под указанным при идентификации именем.

Для доказательства необходимо наличие одного из типов аутентификационных данных:

- Нечто, присущее только пользователю. Биометрические данные: сканеры лица, отпечатки пальцев или сетчатки глаза.
- Нечто, известное только пользователю. Сюда относятся pin-коды, пароли, графические ключи, секретные слова.
- Нечто, имеющееся у пользователя. В данном качестве может выступать токен, то есть компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации владельца. Самые простые токены не требуют физического подключения к компьютеру – у них имеется дисплей, где отображается число, которое пользователь вводит в систему для осуществления входа; более сложные подключаются к компьютерам посредством USB и Bluetooth-интерфейсов.

Биометрический считыватель — это считыватель, который воспринимает биометрические признаки (лица, пальцы, ладони, радужную оболочку, голос и т.п.) и выдает идентификатор пользователя СКУД (номер карты доступа).

Хотя большинство биометрических считывателей также являются полноценными контроллерами СКУД, в Бастион они интегрированы просто как считыватели, то есть они подключаются к контроллерам СКУД Elsys по интерфейсам считывателей (Wiegand, Touch memory, OSDP). Вся проверка полномочий (уровней доступа) осуществляется контроллерами Elsys.

Биометрический считыватель не является отдельным типом устройства в ПК "Бастион-3" и представлен просто как Считыватель.

Биометрический шаблон — это набор данных, представляющих собой биометрические характеристики зарегистрированного пользователя.

Виртуальная точка прохода не имеет преграждающего устройства. Используется в Elsys Mobile и в драйверах систем распознавания лиц. Может использоваться в любых других драйверах некооперативной биометрии для фиксации факта наличия человека в зоне какого-либо датчика. Ничто не мешает сделать виртуальную точку и на базе обычной СКУД Elsys (например, просто считыватель на стене). Виртуальная точка прохода может иметь один или два считывателя и быть односторонней или двухсторонней, как и любая другая точка прохода. Например, в случае распознавания лиц виртуальная точка прохода может быть связана с одной или двумя камерами, выполняющими распознавание. В этом случае камеры играют роль считывателей.

Отдельного типа устройства для виртуальных точек прохода в Бастионе нет. В БД это дверь.

Ворота — это один из типов точек прохода. В целом ведет себя как Дверь, но для ворот возможна дополнительная команда "Стоп" (остановить процесс открытия или закрытия ворот). Также, соответственно, возможно состояние "Полуоткрыто".

Является отдельным типом устройства в ПК «Бастион».

Временная зона – это интервал времени, активный в определённые, настраиваемые дни расписания.
Период временной зоны может изменяться в пределах от 1 до 31 дня (если это поддерживается оборудованием СКУД) и включать два типа исключительных дней: «праздник» и «короткий день». Временные зоны также могут быть составными. Таким образом можно составить расписание произвольной длительности, более чем на 31 день (поддержка таких временных зон реализована в контроллерах Elsys). Например, можно определить временную зону с 8:00 до 17:00, активную по рабочим дням (пн-пт) для недельного графика.

Временной блок представляет собой набор временных зон. Если требуется составить сложное расписание, состоящее из нескольких разных временных интервалов, то используются временные блоки.
Например, если требуется сделать уровень доступа, активный с 8:00 до 13:00 и с 14:00 до 18:00 в рабочие дни, то следует создать две временные зоны и объединить их в один блок.

В уровнях доступа используются непосредственно временные блоки, даже если они состоят из одной временной зоны.

Графический план — это план или карта охраняемой территории. Каждая территория может отображаться на отдельном плане (например, можно использовать поэтажные планы зданий). План состоит из подложки, загружаемой из внешних файлов (DXF, JPG) и набора графических элементов, связанных с устройствами Бастиона. Подложка может быть векторной (DXF), при этом из DXF импортируются не все элементы, а только основные. План является устройством ПК "Бастион-3", поэтому может иметь пиктограмму и участвовать в сценариях через собственные действия. Например, можно по событию переключиться на заданный план или вызвать предустановку плана).

Графические элементы в Бастионе могут быть следующих видов:

- *Пиктограмма* - векторный схематический рисунок устройства. Свои пиктограммы есть почти для всех типов устройств. Пиктограммы можно редактировать в специальном редакторе.

- *Многоугольник* - используется для обозначения замкнутой контролируемой области, и обычно связывается с зонами охранной / пожарной сигнализации.
- *Периметр (ломаная линия)* - специальный элемент для отображения периметров. Поддерживает отображение тревог на заданном участке периметра. При этом, может отображать множество одновременных тревог на одном периметре.

Одно и то же устройство можно отобразить на одном или нескольких планах несколько раз. Например, на плане "Общий вид" и на плане "Детальный 1-го этажа" могут отображаться одни и те же устройства. Графические планы объединяются в наборы планов.

Каждый графический план имеет название и приоритет. Приоритет плана используется при автоматическом переключении планов по тревоге. При тревоге с определённым устройством, будет произведено переключение на план с наибольшим приоритетом из тех, на которых это устройство расположено.

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

Группы управления охраной в ПК «Бастион-3» поддерживаются на системном уровне (т.е. на уровне ядра) 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 одну 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.

Для каждой ГУО определено «Право использовать для пропуска». Это право задаётся на уровне роли оператора. Оператор, для роли которого это право не задано для группы управления охраной, не может назначить пропуску эту ГУО.

Дверь — это один из типов точек прохода. Отличается тем, что дверь не позволяет определить, сколько людей и в каком направлении реально воспользовалось открытой дверью (может быть от нуля до бесконечности). События "фактический проход" для дверей формируются, когда дверь реально открыли после предоставления доступа. Как правило, дверь имеет датчик закрытия двери, позволяющий фиксировать события "Удержание двери" (дверь открыли и не закрывают в течение некоторого заданного времени), а также состояний "Открыто" и "Норма".

Драйвер *ПК "Бастион-3"* — это набор модулей, реализующих интеграцию с какой-либо подсистемой безопасности. Как правило, драйвер состоит из основного модуля, который выполняется на *сервере оборудования* и *конфигуратора драйвера*. Кроме того, драйвер может содержать дополнительные модули, встраиваемые в АРМ системы. Например, драйверы биометрических систем могут встраивать модули настольных биометрических считывателей в АРМ "Бюро пропусков".

С каждым драйвером поставляется *файл определения драйвера* (driver definition text) - это файл с расширением ddt в формате XML. В этом файле определяются:

- Название, идентификатор, тип, версия и некоторые другие параметры драйвера (корневой узел driver).
- Список типов устройств, поддерживаемых драйвером (узел devTypeList).
- Список возможных событий для каждого типа устройств, поддерживаемых драйвером (узел messageList).
- Список возможных команд для каждого типа устройств, поддерживаемых драйвером (узел actionList).
- Контекстное меню для пиктограмм каждого типа устройств (узел menu).
- Используемые для драйвера профили пользователей СКУД (узел ProfileTypeList).
- Поддерживаемые группировки устройств (узел groupTypeList).
- Политика лицензирования драйвера (узел licenseStrategy).

На основании данных в этом файле, при первом запуске сервер системы импортирует в БД все необходимые данные о драйвере.

Также, драйвер может использовать универсальный конфигуратор драйверов. Для этого он должен включать специальный файл в формате XML, содержащий определения параметров для этого конфигуратора.

Идентификатор пропуска - это некоторый код, по которому однозначно идентифицируется активный пользователь СКУД (владелец активного пропуска). Этот код может храниться на карте доступа (CARD ID или значение, записанное в определённую защищенную область памяти смарт-карты), выдаваться биометрическим считывателем при распознавании. Также он может быть получен из QR-кода, то есть *носители* идентификатора пропуска могут быть различными.

Идентификатор пропуска может иметь размерность от 3 до 6 байт (см. *форматы номеров карт доступа*).

Биометрические шаблоны не являются непосредственными идентификаторами пропуска. В случае использования биометрических СКУД каждому набору *биометрических шаблонов*, принадлежащих одному человеку, ставится в соответствие какой-либо идентификатор пропуска. Именно этот идентификатор передаётся на вход контроллеров СКУД в качестве номера карты. Также могут использоваться другие преобразования. Например, номер машины может быть преобразован в номер карты.

В ПК "Бастион-3" биометрические шаблоны относятся к сущности "Персона" (к одной персоне может быть привязано множество биометрических шаблонов), а номера карт - к сущности

"Пропуск" (к одному активному пропуску может быть привязана одна карта доступа, но одна карта может быть связана с многими пропусками в архиве).

Идентификатор пользователя СКУД

Технически это то же самое, что идентификатор пропуска. Пользователь идентифицируется в СКУД по своему пропуску, а тот - по идентификатору пропуска.

Идентификация — это процесс распознавания пользователя по его идентификатору. В контексте СКУД используется идентификатор пропуска.

Пример. Находясь на сайте банка, пользователь решает зайти в личный кабинет, чтобы сделать денежный перевод. На странице личного кабинета система вначале просит ввести идентификатор. Это может быть логин, адрес электронной почты или номер мобильного телефона. Какой конкретно вид данных необходимо ввести – зависит от ресурса. Данные, которые указывались при регистрации, необходимо ввести для получения доступа. Если при регистрации указывалось несколько типов данных – и логин, и адрес электронной почты, и номер мобильного, то система сама подскажет что ей конкретно нужно. Ввод этих данных необходим для идентификации человека за монитором как пользователя конкретного банка. Если пользователь в качестве идентификатора ввел «Александр Петров», и система нашла в своей базе запись о пользователе с таким именем, то идентификация завершилась.

Пример в контексте СКУД. При предъявлении карты доступа к считывателю сначала происходит *идентификация* пользователя СКУД (то есть поиск в БД СКУД карты с указанным номером). Если карта найдена, происходит аутентификация. В простейшем случае (проход только по карте) она заключается в том, что СКУД считает успешное предъявление карты достаточным признаком для подтверждения личности владельца карты доступа. После этого производится проверка полномочий владельца карты, и, если их достаточно для выполнения запрошенных действий, тогда пользователь СКУД *авторизуется*.

Карта доступа используется в качестве физического носителя *идентификатора пользователя СКУД*. Карты доступа могут иметь различный формат, использовать различные технологии для считывания, но в результате их считывания на выход считывателя передаётся номер -идентификатора пользователя СКУД. Этот номер может быть как идентификатором карты, так и неким числом, записанным в защищённую область памяти смарт-карты.

В ПК "Бастион-3" карты доступа связаны с пропусками. При этом одна активная карта доступа всегда связана с одним активным пропуском. Карты могут использоваться для временных пропусков повторно, поэтому в архиве может быть множество возвращённых или изъятых пропусков, связанных с одним и тем же номером карты доступа.

Категория пропуска определяет правила обработки определённой группы пропусков. Категория соответствует *видам пропусков* реальных объектов. Например, если на объекте применяются "пропуска для сотрудников", "пропуска для подрядчиков" и "пропуска для посетителей", то именно такие *категории пропусков* и должны быть настроены в ПК "Бастион-3".

Система поддерживает различные виды правил, установленные для разных категорий пропусков:

1. Значения по умолчанию для различных полей.

2. Отображение блоков (страниц) в форме свойств пропуска. Иначе говоря, возможность указывать те или иные параметры для категории пропуска.

3. Обязательность заполнения полей. Проверяется перед выдачей пропуска.

4. Проверка допустимости выдачи пропуска этой категории через внешние системы.

Механизм правил является расширяемым. Дополнительные модули системы, такие как Драйверы СКУД, Репликация и УРВ имеют возможность дополнить набор доступных правил. Например, драйвер СКУД может дополнить список действий в правилах установкой "Профиля драйвера СКУД XXX". Для Репликации может потребоваться установка "Глобального уровня доступа" и "Маршрута" по умолчанию, и т.д.

Правила могут применяться на разных этапах обработки пропусков:

1. Создание заявки на пропуск. Здесь и только здесь применяется установка значений по умолчанию.

2. Перед выдачей пропуска. Здесь должны проверяться заполненность обязательных полей, наличие всех необходимых утверждений заявки, проверяться подтверждение по внешним системам.

Проверка правил может выполняться как на сервере системы, так и в клиентских приложениях.

Для каждого подразделения должна быть возможность указать, какие категории пропусков могут быть использованы для создания новых пропусков. Логично указывать это сразу при создании подразделения. Возможность выбора подразделения для существующей персоны не зависит от наличия у персоны пропусков в категориях, не доступных к использованию в новом выбираемом подразделении.

Разграничение доступа операторов производится как на уровне подразделений, так и на уровне категорий пропусков. То есть, оператор должен иметь возможность создать пропуск категории "Постоянный" в подразделении "Бухгалтерия" только в случае, если он имеет право создавать пропуска категории "Постоянные" и имеет право создавать пропуска в подразделении "Бухгалтерия".

Правила должны позволять устанавливать значения по умолчанию для следующих полей: должность, гражданство, тип документа, кем выдан документ, печатная форма пропуска, форма фотоидентификации, группа охраны, причина блокировки, причина возврата, приоритет пропуска, дополнительные поля пропуска, уровень доступа.

Набор планов. Графические планы объединяются в *наборы планов*. Каждая *роль оператора* связана с каким-либо одним набором планов. Этот набор будет загружен в АРМ Оператора, когда осуществляется вход в систему *оператора* с заданной *ролью*.

Направление прохода. Обычно бывает два варианта: вход или выход. Одна точка прохода может работать в одном или в двух направлениях и, соответственно, может быть односторонней или двухсторонней. Направление прохода обычно ассоциируется со считывателем. У считывателя может указываться его роль, то есть направление прохода.

Настольный считыватель служит для внесения персональных идентификаторов в БД системы.

Как правило, настольные считыватели подключаются к компьютеру с АРМ "Бюро пропусков". Для подключения могут использоваться COM-порты, USB, Ethernet, Wi-Fi или Bluetooth.

Настольные считыватели могут считывать как номера карт, так и биометрические признаки. В случае работы с защищённой областью карт доступа, настольные считыватели могут также программировать карты доступа.

Настольные считыватели не являются устройствами ПК "Бастион-3". Они не отображаются на планах, и их нельзя использовать в сценариях.

Персона в системе безопасности - это прежде всего субъект СКУД, то есть лицо, в отношении которого определяются полномочия физического доступа, а также полномочия управления системой безопасности (снятие / поставновка на охрану и т.п.).

Только Персона в ПК "Бастион-3" может быть владельцем пропуска. Нельзя выдать пропуск, например, на автомобиль - это будет *транспортный пропуск*, привязанный к персональному пропуску.

Пропуск определяет права пользователя СКУД (Персоны). Одной Персоне может быть выдано несколько пропусков одновременно. Иными словами, для одной Персоны может быть установлено несколько наборов прав в СКУД, предоставляемых по разным *пропускам*.

Каждому пропуску должен быть назначен один *уровень доступа*. Если в пользовательском интерфейсе и можно назначить несколько уровней доступа для одного пропуска, то фактически эти уровни будут объединены в один. Пропуск может иметь период активности (даты начала и окончания действия), но может быть и без ограничения срока действия.

Для пропуска могут быть назначены:

- группа управления охраной
- профиль пользователя СКУД.

Пропуск может находиться в одном из статусов (см. статью «Статус пропуска»).

Профиль пользователя СКУД - это набор дополнительных настроек, определяющих режимы прохода пользователя СКУД через различные точки прохода. Набор этих настроек индивидуален для каждого драйвера СКУД. Внутри каждый профиль может содержать разные настройки для каждого контроллера СКУД (например, доступ только по ПИН-коду, доступ с подтверждением и т.п.).

Настройка доступных профилей производится в драйверах СКУД. Для каждой *категории пропуска* задаётся профиль по-умолчанию, который присваивается при создании заявки на пропуск. В свойствах каждого пропуска можно задать используемый профиль для каждого драйвера индивидуально.

Репликация — это синхронизация данных на основе заданных правил.

Серверы оборудования — это 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.

Сервер системы — это 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.

Статус пропуска

Каждый пропуск может находиться в одном из следующих статусов:

- отказано в утверждении (approval rejected),
- требует утверждения (appoval required),
- не активен (not active),
- активен (active),
- просрочен (expired),
- возвращён (returned),
- утерян (lost),
- списан с учёта (charged off),
- пришёл в негодность (broken).

Статусы «отказано в утверждении» и «требует утверждения» используются только при совместной работе с модулем «Бастион-3 – веб-заявка». При создании новой заявки в АРМ «Бюро пропусков» создаётся «неактивный» пропуск, отображающийся на странице «Заявки», при этом ему ещё не присвоена карта доступа. В процессе выдачи карты пропуск переводится в активное состояние, ему присваивается карта доступа и он переходит на страницу «Выданные». После этого пропуск может быть сдан (при этом карта доступа должна быть реально возвращена в бюро пропусков в рабочем состоянии) или изъят.

После изъятия пропуска карту доступа повторно использовать нельзя, но можно отдельно вернуть карту в обращение. При изъятии указывается причина, в соответствии с которой для пропуска устанавливается один из статусов: «утерян», «списан с учёта» или «пришёл в негодность».

Возвращённые и изъятые пропуска отображаются на странице «Архив».

По окончании срока действия пропуска ему автоматически (модулем сервера системы) присваивается состояние «просрочен», при этом он отображается на отдельной странице – «Просроченные».

Операции блокировки и разблокировки пропусков не меняют статус пропуска.

Сценарий — это предварительно настроенная именованная упорядоченная последовательность действий, задаваемая при настройке системы. Каждое действие в сценарии выполняется над устройством ПК «Бастион-3». Список доступных действий определяется для каждого типа устройств и для каждого драйвера в системе отдельно. Между действиями в сценариях могут быть вставлены задержки, например, задержка перед выполнением очередного действия, в секундах.

Все действия сценария выполняются последовательно, с учётом задержек.

Сценарии могут выполняться вручную, если это разрешено для конкретного сценария, а также при срабатывании какого-либо триггера (в качестве реакции на событие, ситуацию, наступление определённого времени и т. п.). Для каждого сценария можно указать набор триггеров, которые вызовут его выполнение.

У сценария есть контекст выполнения — например, исходное событие. Благодаря этому, сценарий может использовать параметры этого контекста, чтобы выполнить необходимые действия (например, вернуть предъявленную карту).

Для сценария может быть указана вероятность его выполнения в определенном контексте (по определенному триггеру). Применение — организация выборочных проверок, например алкотестирования.

Считыватель — это устройство, считывающее либо идентификатор пользователя СКУД, либо некий признак, которому ставится в соответствие идентификатор пользователя СКУД (биометрический шаблон или номер машины, например).

Как правило, считыватели являются дочерними устройствами для точек прохода. Считыватели относятся к базовым типам устройств, определяющих права доступа пользователей СКУД. То есть именно считыватели, а не точки прохода входят в состав уровней доступа.

Считыватель является отдельным типом устройств в ПК «Бастион-3». Как правило, считыватели не формируют событий и не отображаются на планах.

Территория — это пространство, ограниченное одной или несколькими точками прохода (дверями, турникетами или воротами). Территория может представлять собой одно конкретное помещение или группу помещений, здание целиком, территорию завода. Территории могут быть вложенными. Например, область контроля «Всё здание» может содержать несколько других областей: "Цех 1", "Бухгалтерия" и т. д.

Территории используются в следующих случаях:

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

Также, в дальнейшем территории могут использоваться для управления помещением или территорией в целом. Например, для взятия на охрану помещения, для снятия с охраны, в триггерах сценариев.

В ПК "Бастион-3" настройка территорий производится путем указания для точек прохода из какой в какую область контроля они ведут. Например, "Турникет 1" может вести из области "Вне территории" в область "На территории". При этом событие "Штатный вход" от этого турникета

будет означать переход владельца пропуска из области "Вне территории" в область "На территории".

Если пользователю СКУД разрешён доступ на какую-либо территорию, то ему должен быть предоставлен доступ:

1. На всех считывателях, обозначенных как входные в эту территорию.
2. На всех считывателях, обозначенных как выходные во внешние территории.
3. На все внутренние считыватели территории. Доступ в смежные территории по умолчанию предоставляться не должен, но оператор должен иметь возможность его дать.

Тип устройства

В ПК «Бастион» жёстко определен список типов устройств (зашит в коде). Принадлежностью к определенному типу определяется поведение устройства и его обработка в системе. Всего существует 50 типов устройств. Некоторые типы не используются. Некоторые типы называются совсем не так, как должны. Список типов устройств унаследован еще из «Бастион» 1.0 и является довольно архаичным.

Тип устройства влияет на:

- способ его отображения на графических планах (пиктограмма);
- группировку в деревьях устройств;
- возможность использования в областях контроля и уровнях доступа.

Точка прохода — это устройство, через которое осуществляется физический доступ. Точки прохода могут быть разных типов: дверь, турникет, ворота, шлагбаум, калитка, виртуальная точка прохода. Первые три типа определены в ПК «Бастион-3» как отдельные типы устройств и немного отличаются поведением.

Точки прохода определяют границы областей контроля. Каждая точка прохода может вести из одной области контроля в другую. Также, если точка прохода "внутренняя", то проход через неё не приводит к смене области контроля.

Точки прохода могут быть *односторонними* или *двухсторонними*. К односторонней точке прохода подключается один считыватель, он может быть как входным, так и выходным. К двухсторонней точке прохода подключается два считывателя - входной и выходной.

Как правило, точка прохода - это виртуальное устройство. Реально каждая точка прохода может состоять из:

- одного или двух считывателей,
- преграждающего устройства,
- запирающего устройства,
- датчика прохода,
- вспомогательных датчиков и кнопок управления.

Виртуальная точка прохода не имеет преграждающего устройства.

Точка прохода находится в *нормальном состоянии*, когда она закрыта и доступ разрешён в соответствии с полномочиями пользователей СКУД. Точка прохода *разблокирована*, когда она открыта (запирающее устройство отключено), проход разрешён всем без идентификации. Точка прохода *заблокирована*, когда она закрыта и проход запрещён для всех.

Триггер сценария - это набор условий, которые должны выполниться, чтобы сценарий был запущен. В версиях 2.1 и раньше триггерами могли являться только отдельные события (с учётом отдельных их параметров) и наступление определённого времени. В 2.2 введён расширенный механизм триггеров, который позволяет составлять сложные условия запуска сценариев. В качестве условий срабатывания триггера теперь могут выступать:

- отдельные события;
- любые параметры событий (например, ФИО предъявившего карту доступа или дальность для периметра, координаты события);
- местоположение (нахождение в определённой области контроля);
- текущие состояния устройств;
- время.

Условия могут объединяться в логические выражения с использованием операций И, ИЛИ, НЕ. Проверка условий происходит в один момент времени. То есть, нельзя сделать такой триггер, который бы ждал в течение определённого времени наступления нескольких событий.

Турникет - это один из типов точек прохода. Является отдельным типом устройства в ПК "Бастион-3". Имеет отличительные черты:

- В отличие от двери, у турникета есть датчик проворота, позволяющий пропускать по одному пропуску строго одного человека в заданном направлении.
- Турникет можно заблокировать, открыть и разблокировать отдельно на вход, на выход, либо и на вход, и на выход.

Универсальный конфигуратор драйвера — это модуль, который используется для единообразной настройки всех драйверов.

Уровень доступа (УД) определяет, в какое время, в какие дни и в какие помещения имеет право проходить владелец карты доступа. УД на нижнем уровне формируется из элементов, содержащих пары «считыватель – временной блок».

Поскольку такая детальная настройка на уровне считывателей, как правило, не требуется, то ПК «Бастион-3» позволяет формировать уровни доступа на основе *областей контроля*.

Как правило, число используемых УД рекомендуется сокращать, так как их число ограничено аппаратными возможностями контроллеров СКУД. Поэтому, у УД есть признак, используются ли они хотя бы одним активным пропусков (то есть - надо ли передавать этот УД хотя бы в 1 контроллер СКУД). Уровень доступа имеет *физический номер*, который устанавливается в NULL в случае, если УД не используется активными пропусками.

Уровень доступа может задаваться в разных режимах:

Уровень доступа может быть простым и составным.

Устройство в ПК «Бастион-3» — это базовый элемент системы безопасности. Только *устройства* могут быть *источниками событий* системы. Устройства подразделяются на различные *типы устройств*, которые жёстко определены в системе. Каждый драйвер может указать, какие типы устройств в нём могут использоваться, какие команды и события для них доступны. То есть набор команд и событий уникален для каждого драйвера и типа устройства.

Для всех устройств указывается *родительское устройство*. Таким образом, все устройства организованы в дерево устройств. Обычно, родительские устройства указываются «по подключению». Например, *считыватель* может быть элементом двери, *дверь* реализуется контроллером СКУД, к*онтроллер СКУД* подключен к коммуникационному сетевому контроллеру и последний - непосредственно к драйверу. Корневые узлы дерева устройств - это "Система", "Пользователь" и все *экземпляры драйверов*. Каждое устройство в результате относится к одному из экземпляров драйверов.

Для каждого устройства указывается физический адрес (address). Это идентификатор, используемый драйвером для адресации своих устройств. Для каждого устройства может быть установлен признак его *активности*. Только активные устройства участвуют в опросе приборов, могут присылать события и принимать команды управления.

С каждым устройством может быть связан набор специальных параметров (specific_params), которые задаются драйвером. Ядро системы не анализирует эти параметры. Задаются они в виде строки json в поле devices.specific_params.

Для устройств может быть определён список доступных команд управления. Устройства Бастиона могут соответствовать реальным устройствам, например: тревожный вход, датчик или кнопка, или быть виртуальными (дверь, план, система, сценарий).

Шлюз — это система, состоящая из небольшого пространства с двумя комплектами блокирующих дверей, так что первый комплект дверей должен закрываться до открытия второго комплекта.

Как правило, несколько человек не могут одновременно зайти внутрь шлюза. Двери блокируются снаружи, если внутри кто-то есть. Также в самом шлюзе может проводиться досмотр (документов или чего-либо еще, например может быть встроен металлодетектор), проход через шлюз может подтверждаться охранником. Идентификация может быть необходима для каждой двери шлюза, причем это могут быть разные виды идентификации.

Хотя в Бастионе есть тип устройства "Шлюз", на практике он не используется. Реально шлюз реализуется специальной конфигурацией контроллера Elsys-MB, с двумя дверями и настроенными взаимодействиями.

Экземпляр драйвера — это конкретный экземпляр модуля интеграции, добавленный в конфигурацию системы. Экземпляр драйвера выполняется на заданном сервере оборудования. Каждый экземпляр драйвера можно остановить и запустить независимо от остальных.