Бастион-3 – LDAP. Руководство администратора

Версия 2024.1

(05.04.2024)

Самара, 2024

Оглавление

1 Общие сведения

Система «Бастион-3 – LDAP» предназначен для синхронизации пропусков СКУД ПК «Бастион-3» с пользователями LDAP.

Возможности системы включают:

- Импорт пользователей из LDAP в ПК «Бастион-3» с созданием заявок на пропуска;
- Возврат, либо блокировка пропусков в ПК «Бастион-3» при блокировке в LDAP аккаунта владельца пропуска;
- Настройку правил присвоения уровней доступа в ПК «Бастион-3»;
- Настройку соответствий полей *пропуска* и *персоны* в ПК «Бастион-3» полям в LDAP;
- Экспорт пользователей в LDAP на основе активных пропусков, созданных и выданных в ПК «Бастион-3»;
- Ручной запуск синхронизации данных пропуска и персоны ПК «Бастион-3» с полями пользователя в LDAP;
- Запись настраиваемого текста событий прохода персоны из ПК «Бастион-3» в заданный атрибут связанного пользователя LDAP;
- Блокировка рабочей станции в ответ на действия пользователя в СКУД.

Система состоит из модуля расширения сервера системы ПК «Бастион-3», агента блокировки рабочей станции и страницы панели управления, как показано на Рис. 1.

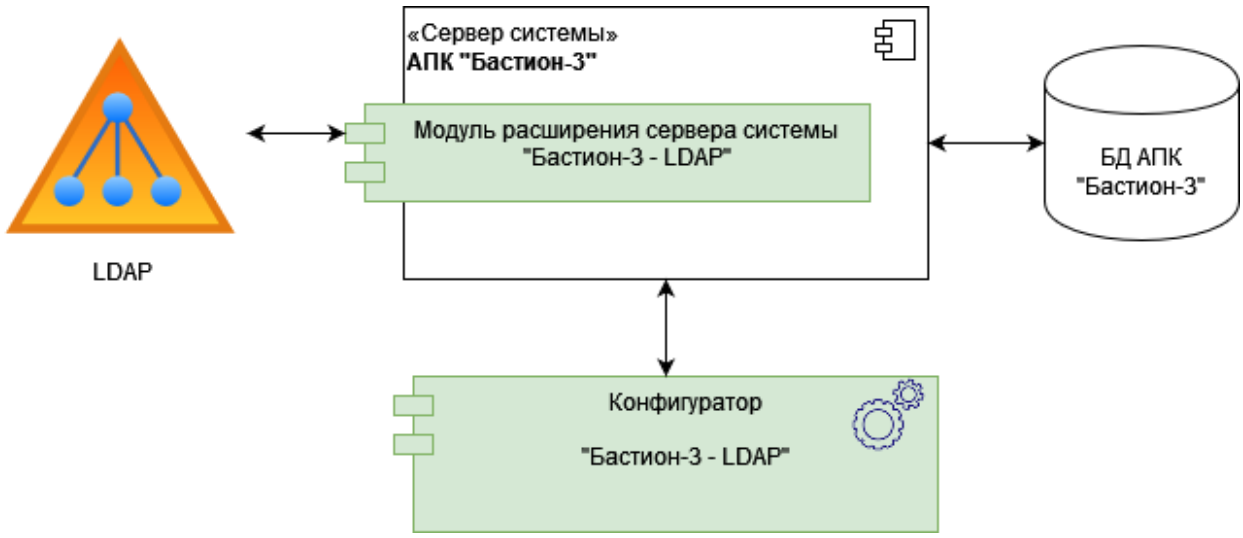

Рис. 1. Структура системы «Бастион-3 – LDAP»

Для настройки системы пользователь должен обладать знаниями о структуре и администрировании LDAP, организационной структуре предприятия и администрировании СКУД ПК «Бастион-3».

2 Условия применения

2.1 Требования к совместимости

На модуль «Бастион-3 – LDAP» распространяются те же требования к аппаратной и программной платформе, что и для ПК «Бастион-3».

Для работы требуется ПК «Бастион-3» версии не ниже 2023.1.

Технология интеграции подразумевает возможность использования в качестве каталога пользователей любые серверы LDAP, однако, тестирование системы производилось только с Active Directory.

2.2 Лицензирование системы

Для работы системы требуется наличие в ключе защиты строки активации модуля «Бастион-3 – LDAP». Модуль не имеет количественных ограничений на объем синхронизируемых данных.

Как видно из схемы на Рис. 1, всегда требуется наличие одного модуля «Бастион-3 – LDAP» на каждом сервере системы.

3 Установка

Модуль «Бастион-3 – LDAP» устанавливается в составе ПК «Бастион-3». Для его установки нужно отметить соответствующий флаг в списке компонентов расширения.

4 Настройка

4.1 Основные настройки

Чтобы синхронизация с LDAP начала работать, необходимо предварительно выполнить настройку – указать данные для подключения к серверу LDAP и, опционально, настроить соответствие уровней доступа организационным единицам (Organizational Unit – далее OU).

Настройка модуля осуществляется с помощью приложения «Панель управления», необходимо в меню выбрать «Синхронизация с LDAP» и вам откроется следующее меню, которое можно увидеть на Рис. 2.

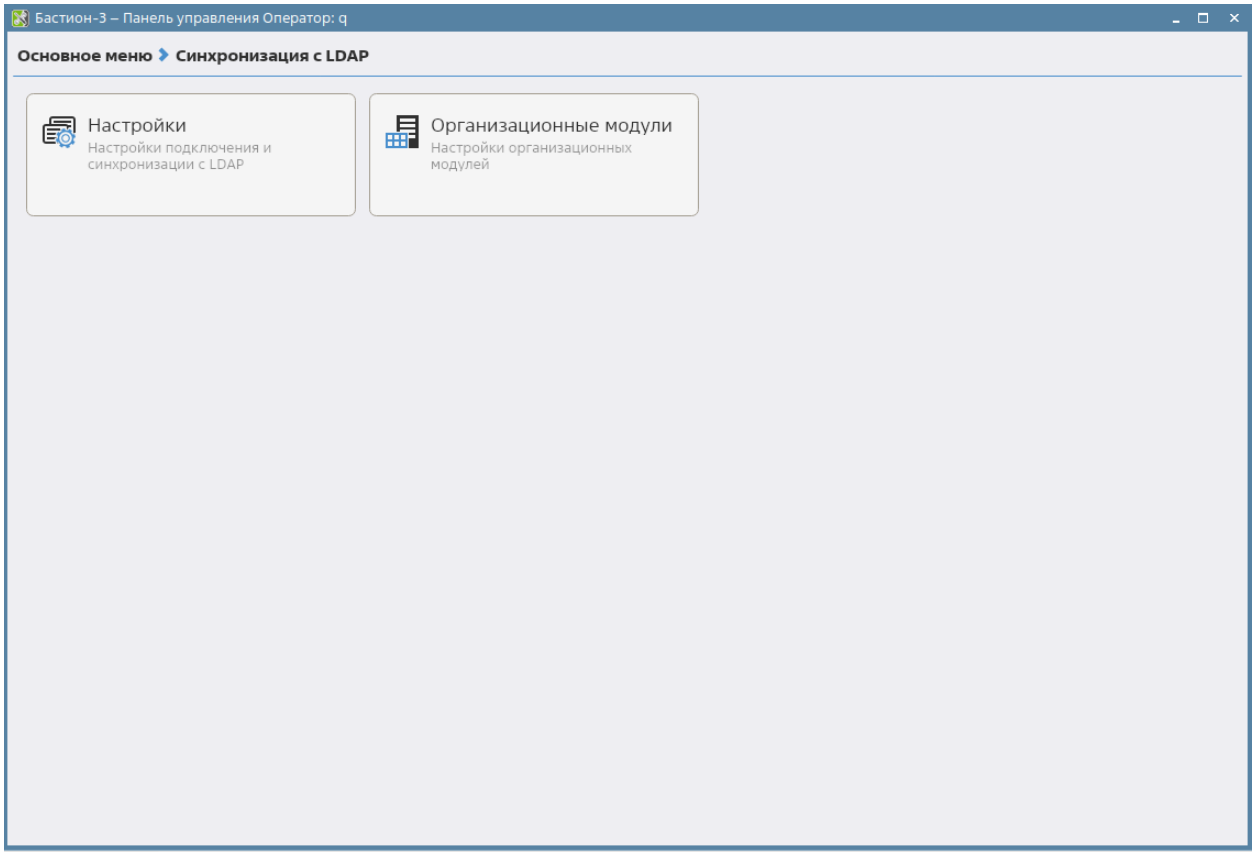

Рис. 2. Меню Синхронизации с LDAP

Для настройки синхронизации необходимо выбрать соответствующее меню.

Интерфейс настроек изображён на Рис. 2 и представлен тремя основными элементами:

1) Панель инструментов – содержит кнопки:
   - Сохранить изменения – сохраняет внесённые изменения;
   - Отменить изменения – отменяет все внесенные изменения;
2) Дерево настроек – содержит 5 основных узла, это:
   - Основные настройки – основные настройки модуля «Бастион-3 – LDAP»;
   - Импорт – настройки импорта пользователей из LDAP в ПК «Бастион-3»;
   - Экспорт персон – настройки экспорта пользователей из ПК «Бастион-3»;
   - Экспорт карт – настройки экспорта карт из ПК «Бастион-3»;
   - Экспорт событий прохода – настройки экспорта событий прохода из ПК «Бастион-3».
3) Область настройки – содержит доступные для редактирования параметры выбранного в дереве настроек узла.

Основные настройки представлены на Рис. 3.

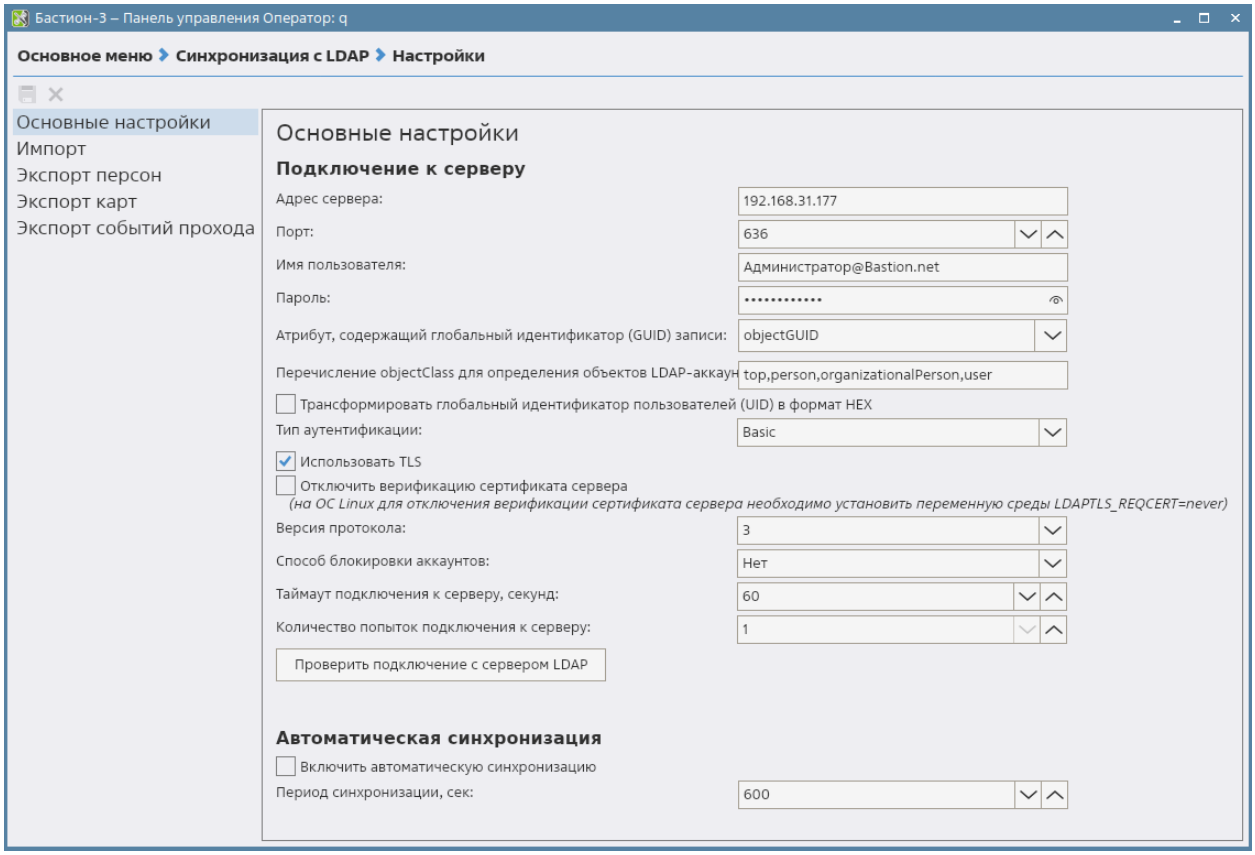

Рис. 3. Окно «Основные настройки»

Основные настройки включают в себя:

- *Адрес сервера* – IP-адрес или доменное имя сервера LDAP;
- *Порт* **–** порт сервера LDAP;
- *Имя пользователя* – логин пользователя LDAP, имеющего права на чтение данных пользователей, включая данные User Account Control (UAC);
- *Пароль* – пароль пользователя LDAP;
- *Атрибут, содержащий глобальный идентификатор записи* – атрибут, содержащий GUID записи. Доступен выбор из типовых вариантов, а также возможность ввести название атрибута вручную;
- *Перечисление objectClass для определения объектов LDAP-аккаунтов* — перечисленные через запятую названия типов объектов для точного определения пользователей сервера LDAP. Набор objectClass можно узнать при помощи cmd-команды ldapsearch на линуксе или в утилите AD Explorer для Active Directory;
- *Трансформировать глобальный идентификатор пользователей (UID) в формат HEX* – способ представления идентификатора пользователей LDAP в виде строки или в HEX-формате (например для Active Directory);
- *Тип аутентификации* – способ аутентификации на сервере LDAP. Из ниспадающего списка необходимо выбрать подходящий для конкретного сервера LDAP тип аутентификации;

- *Использовать TLS* – активация данной опции включает подключение с использованием TLS (LDAPS);
- *Отключить верификацию сертификата сервера* – при включении этой настройки подключение к серверу LDAP будет происходить даже в тех случаях, когда не удаётся проверить подлинность сертификата;
- *Версия протокола* – версия протокола LDAP для подключения. Можно выбрать 1, 2 или 3;
- *Способ блокировки аккаунтов* – настройка определяет способ, которым модуль синхронизации определяет при импорте данных с сервера LDAP, является ли аккаунт пользователя заблокированным, а также выполняет блокировку/разблокировку аккаунтов при экспорте данных на сервер LDAP. Необходимо выбрать один из четырёх вариантов: «нет» (в этом случае блокировка аккаунтов не отслеживается при импорте и не производится при экспорте), «UAC» - данный вариант необходимо выбрать, если выполняется подключение к серверу Microsoft Active Directory, «PPolicy» - этот способ следует выбрать, если выполняется подключение к серверу Open LDAP или другому серверу LDAP, который использует политику блокировки аккаунтов ppolicy, «Другой (указать атрибут)» - данный вариант позволит вручную указать, какой атрибут содержит данные о блокировке пользователя и какое значение данного атрибута является признаком заблокированного аккаунта;
- *Атрибут, используемый для блокировки аккаунта* – данный параметр доступен, если в предыдущей настройке выбран вариант «Другой (указать атрибут)». В качестве значения необходимо указать имя атрибута, который содержит данные о блокировке аккаунта пользователя на сервере LDAP;
- *Значение, являющееся признаком блокировки* – в данную настройку необходимо ввести значение, являющееся признаком блокировки аккаунта на сервере LDAP. При импорте данных обнаружение указанного значения будет означать для модуля синхронизации то, что данный аккаунт пользователя является заблокированным. При экспорте данных на сервер LDAP в атрибут, указанный в предыдущей настройке, будет записываться данное значение при блокировке пользователя, и стираться значение (устанавливаться пустое) при разблокировке аккаунта;
- *Таймаут подключения к серверу, секунд* – таймаут подключения к серверу LDAP;
- *Количество попыток подключения к серверу* – при установке в данной настройке значения, отличного от 1 модуль синхронизации будет выполнять несколько попыток подключения к серверу системы прежде, чем сообщить об ошибке подключения к серверу LDAP;
- *Включить автоматическую синхронизацию* – при отключенной синхронизации не будет выполняться ни импорт пользователей с сервера LDAP, ни экспорт данных на сервер LDAP;
- *Период синхронизации, сек.* – временной промежуток в секундах между итерациями синхронизации.

Настройки импорта представлены на Рис. 4.

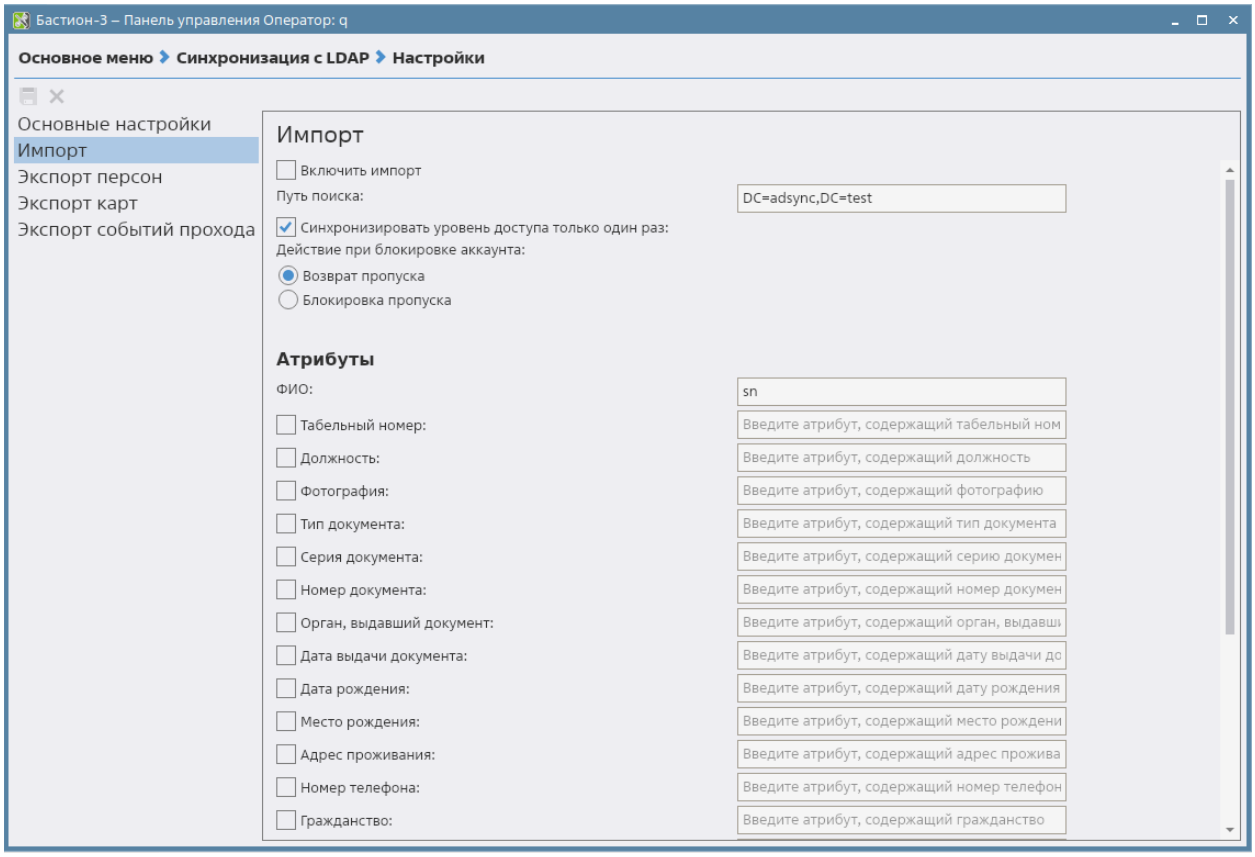

Рис. 4. Окно «Импорт»

Настройки импорта включает в себя:

- *Включить импорт* – при отключенной импорта не будет производиться импорт данных из LDAP;
- *Путь поиска* – путь к организационной единице LDAP (домен или OU), из которой будут загружаться пользователи, оформленный по правилам именования объектов в LDAP, например, «OU=OrgUnitOne,DC=test,DC=com»;
- *Синхронизировать уровень доступа только один раз* – при включении этой настройки уровень доступа для создаваемых в процессе импорта заявок на пропуска будет выставляться только один раз при создании заявки (при обнаружении в LDAP нового пользователя или при разблокировке пользователя, ранее бывшего заблокированным). При смене уровня доступа для OU, в котором находится пользователь, или при смене уровня доступа в атрибуте, заданном в настройке «Уровень доступа» в группе «Атрибуты» (при активной настройке «Использовать уровень доступа из атрибута») не будет изменяться уровень доступа уже существующей заявки на пропуск или активного выданного пользователю пропуска;
- *Действие при блокировке аккаунта:* значение этой настройки определяет действие, выполняемое при блокировке аккаунта LDAP. На выбор доступны два варианта: возврат пропуска (выполняется возврат всех активных пропусков пользователя, а также заявок) и блокировка (случае выполняется блокировка всех активных пропусков пользователя);
- *ФИО* –атрибут, который будет использоваться для чтения ФИО пользователей;

- *Табельный номер* – атрибут, который будет использоваться для чтения табельного номера;
- *Должность* – атрибут, который будет использоваться для чтения должности;
- *Фотография* – атрибут, значение которого будет использоваться для получения фотографии (в формате Base64). Фотография из LDAP загружается только один раз;
- *Тип документа* – атрибут, значение которого будет использоваться для чтения типа документа;
- *Серия документа* – атрибут, значение которого будет использоваться для чтения серии документа;
- *Номер документа* – атрибут, значение которого будет использоваться для чтения номера документа;
- *Орган, выдавший документ* – атрибут, значение которого будет использоваться для чтения органа, выдавшего документ;
- *Дата выдачи документа* – атрибут, значение которого будет использоваться для чтения даты выдачи документа;
- *Дата рождения* – атрибут, значение которого будет использоваться для чтения даты рождения;
- *Место рождения* - атрибут, значение которого будет использоваться для чтения места рождения;
- *Адрес проживания* - атрибут, значение которого будет использоваться для чтения адреса проживания;
- *Номер телефона* – атрибут, значение которого будет использоваться для чтения номера телефона;
- *Гражданство* – атрибут, значение которого будет использоваться для чтения гражданства;
- *Комментарий* – атрибут, значение которого будет использоваться для чтения комментария;
- *Email* – атрибут, значение которого будет использоваться для чтения электронной почты;
- *Категория пропуска* - атрибут, значение которого будет использоваться для чтения категории пропуска;
- *Категория пропуска по умолчанию* – значение этой настройки будет использоваться в тех случаях, когда у пользователя AD будет пустым значение атрибута, указанного в качестве атрибута для импорта категории пропуска;
- *Пин-код* - атрибут, значение которого будет использоваться для чтения пин-кода пропуска;
- *Примечание к пропуску* – атрибут, значение которого будет использоваться для чтения примечания к пропуску;

- *Использовать уровень доступа из атрибута* – при включении этой настройки уровень доступа для пропусков будет выставляться в соответствии с атрибутом, указанным в настройке «Уровень доступа», вместо уровня доступа, заданного для OU, в котором находится пользователь AD.

- *Уровень доступа* – атрибут, значение которого будет использоваться для чтения уровня доступа (если включена настройка «Использовать уровень доступа из атрибута»). Уровень доступа, указываемый в атрибуте пользователя, должен существовать в системе.

Настройки экспорта персон представлены на Рис. 5.

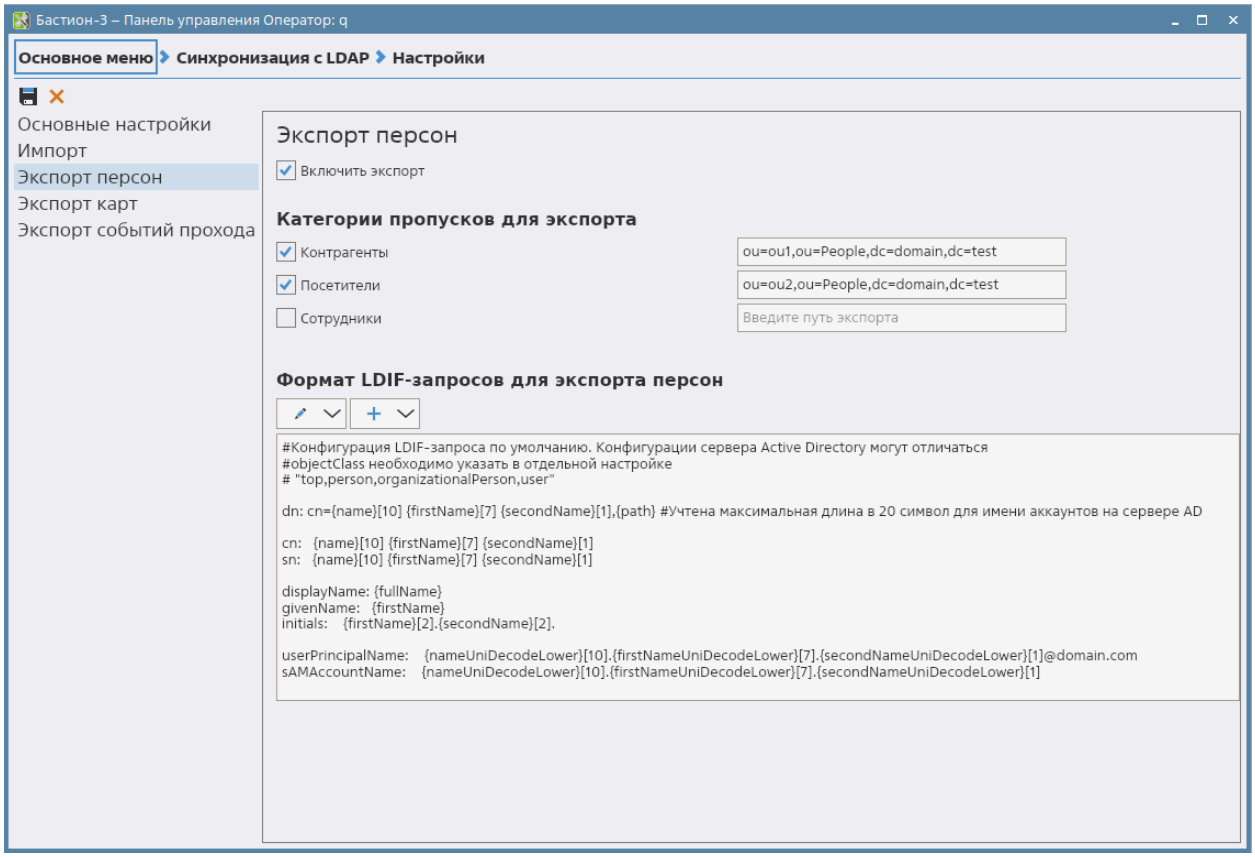

Рис. 5. Окно «Экспорт персон»

Настройки экспорта персон представлены настройкой «*Включить экспорт*» – данная настройка отвечает за включение/выключение экспорта данных из ПК «Бастион-3» в LDAP.

Далее следует меню настроек экспорта пропусков по категориям. Оно представляет собой список категорий пропусков, где для каждой категории можно включить/отключить в экспорт и указать путь для экспорта (который далее можно использовать в формате LDIF-запроса).

Настройка формата LDIF-запросов для экспорта персон предназначена для гибкой настройки запросов, которыми создаются пользователи на серверах LDAP. Представляет из себя текстовое поле с возможностью указания всех необходимых атрибутов и их значений, по которым создаются LDAP-пользователи.

Настройки экспорта карт представлена на Рис. 6.

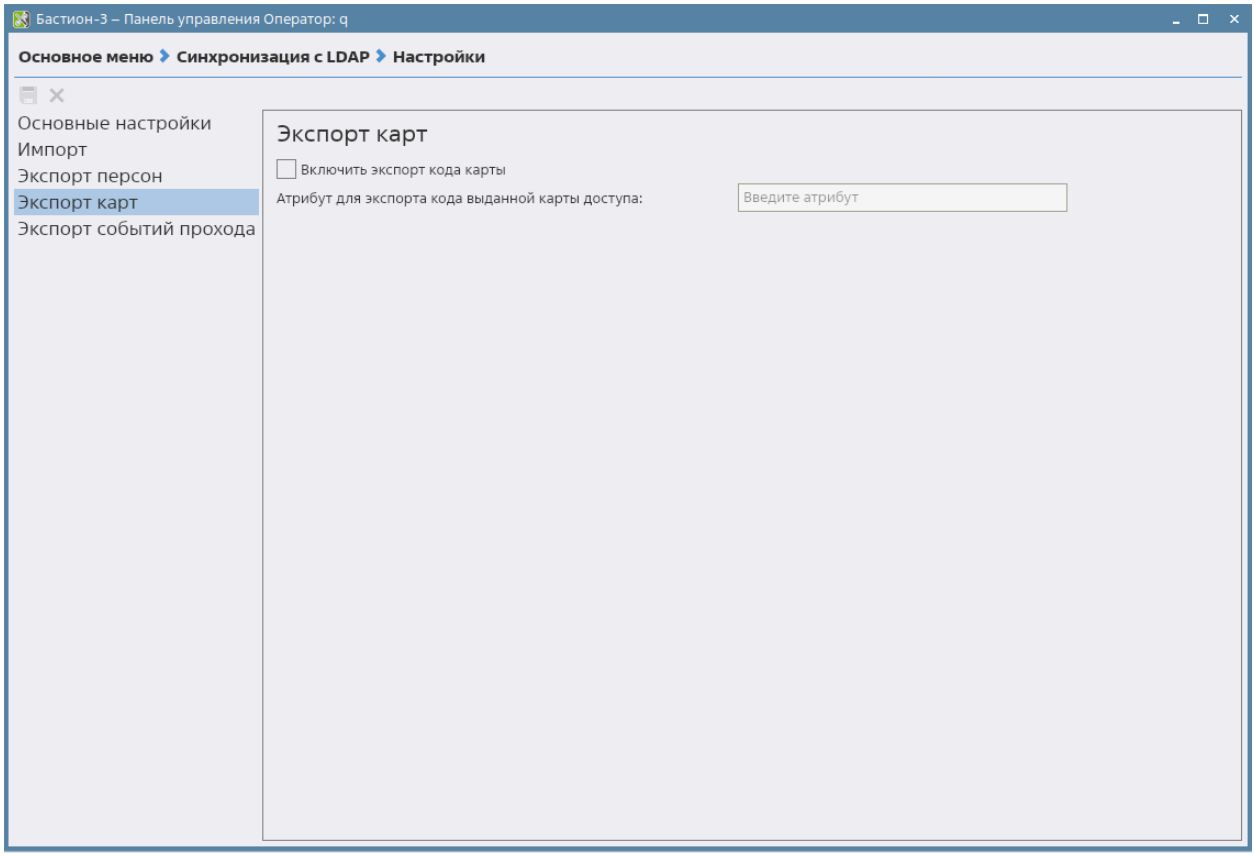

Рис. 6. Окно «Экспорт карт»

Настройки экспорта персон включает в себя:

- *Включить экспорт кода карты* – данная настройка отвечает за включение/выключение экспорта данных из ПК «Бастион-3» в LDAP;
- *Атрибут для экспорта кода выданной карты доступа* – атрибут карты в LDAP, в который будет записываться код выданных карт.

Настройки экспорта событий прохода на Рис. 7.

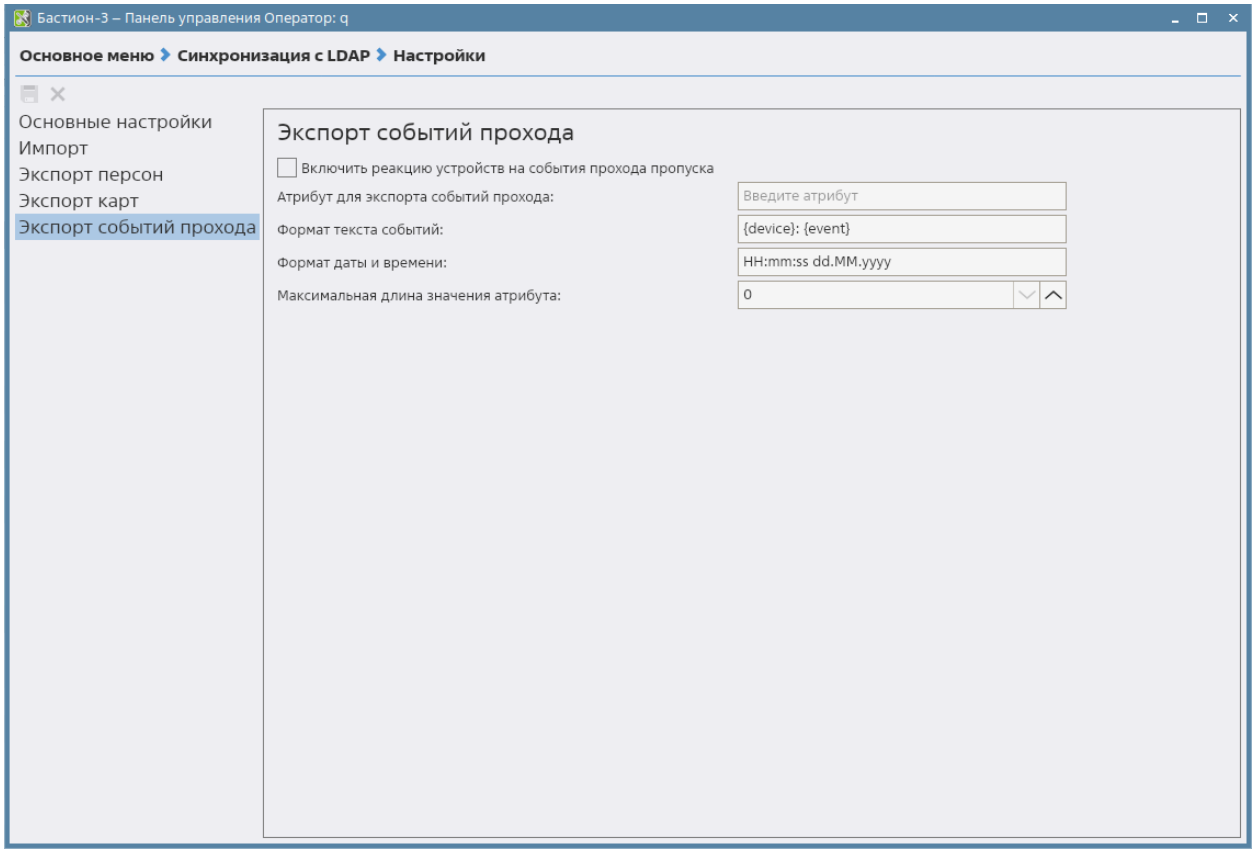

Рис. 7. Окно «Экспорт событий прохода»

Настройки экспорта событий прохода включает в себя:

- *Включить реакцию устройств на события прохода пропуска* – включает функционал записи событий прохода персонала в определенный атрибут для возможности блокировки компьютеров пользователей в случае их выхода из определенных областей контроля. Для данный функции необходима установка специального приложения-агента на компьютерах пользователей для блокировок их рабочих станций;
- *Атрибут для экспорта событий прохода* – атрибут пользователя в LDAP, в который будет записываться текст события прохода;
- *Формат текста событий* – задает формат текста событий прохода с использованием специальных переменных, окруженных фигурными скобками;
- *Формат даты и времени* – задает формат даты и времени, используя специальные символы.
- *Максимальная длина значения атрибута* – задает максимальную длину для атрибутов.

4.2 Настройка реакций устройств на события прохода

Передача событий прохода персонала осуществляется при помощи механизма Сценарий, из раздела «События и реакции» в ПК «Бастион-3». Чтобы создать сценарий, необходимо добавить Действие «Записать информацию в LDAP», которое относится к Системным действиям. Для отслеживания перемещения персонала необходимо добавить нужные события в список событий – триггеров, которые инициализируют запись текста события прохода в назначенный атрибут прошедшей персоны (Рис. 8).

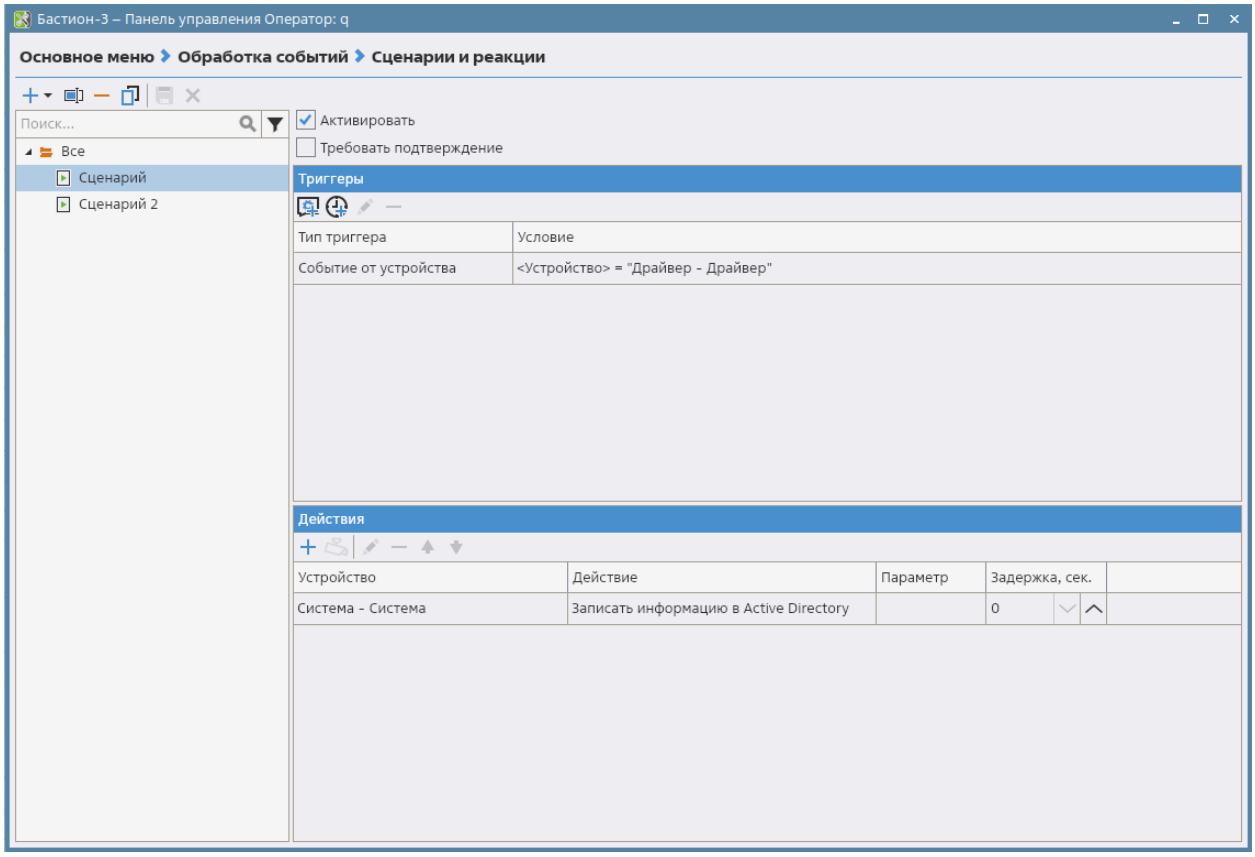

Рис. 8. Настройки сценария

Таким образом, при добавленном триггерном событии, например, «Потеря связи» во время работы, система «Бастион-3 – LDAP» передаст в атрибут пользователя LDAP текст события согласно настроенному формату.

4.3 Настройка формата текста событий

В конфигураторе «Бастион-3 – LDAP» есть возможность настроить формат текста событий для записи в атрибут пользователя LDAP. Для этого в блоке настроек «Параметры экспорта» есть 2 поля: «Формат текста событий» и «Формат даты и времени».

Настройка «Формат текста событий» позволяет настроить текст события прохода персонала. Для настройки используются специальные переменные, которые необходимо указывать в фигурных скобках. При подготовке сообщения на место переменной будет подставлена соответствующая ей информация.

Список переменных для «Формата сообщений»:

- *{name}* – полное ФИО сотрудника;
- *{datetime}* – время события, формат которого задается в поле «Формат даты и времени»;
- *{event}* – текст событий прохода: «Штатный вход», «Штатный выход» и другие события прохода;
- *{device}* – имя устройства события;
- *{cardcode}* – номер карты доступа сотрудника в формате HEX;

- *{category}* – название категории сотрудника;
- *{department}* – название отдела;
- *{organization}* – название организации.

В поле «Формат даты и времени» могут использоваться следующие подстановки:

- *d* – день месяца от 1 до 31, одноразрядные числа не дополняются нулем слева;
- *dd* – день месяца от 01 до 31, одноразрядные числа дополняются нулем слева;
- *ddd* – сокращенное название дня недели;
- *dddd* – полное название дня недели;
- *h* – часы в виде от 1 до 12, одноразрядные числа не дополняются нулем слева;
- *hh* – часы в виде от 01 до 12, одноразрядные числа дополняются нулем слева;
- *H* – часы в виде от 0 до 23, одноразрядные числа не дополняются нулем слева;
- *HH* – часы в виде от 00 до 23, одноразрядные числа дополняются нулем слева;
- *K* – часовой пояс;
- *m* – минуты в виде от 0 до 59, одноразрядные числа не дополняются нулем слева;
- *mm* – минуты в виде от 00 до 59, одноразрядные числа дополняются нулем слева;
- *M* – месяц в виде от 1 до 12, одноразрядные числа не дополняются нулем слева;
- *MM* – месяц в виде от 01 до 12, одноразрядные числа дополняются нулем слева;
- *MMM* – сокращенное название месяца;
- *MMMM* – полное название месяца;
- *s* – секунды в виде от 0 до 59, одноразрядные числа не дополняются нулем слева;
- *ss* – секунды в виде от 00 до 59, одноразрядные числа дополняются нулем слева;
- *y* – год в виде числа из одной или двух цифр. Если год имеет более двух цифр, то в результате отображаются только две младшие цифры;
- *yy* - год в виде числа из одной или двух цифр. Если год имеет более двух цифр, то в результате отображаются только две младшие цифры. Если год имеет одну цифру, то он дополняется нулем слева;
- *yyy* – год из трех цифр;
- *yyyy* – год из четырех цифр;
- *z* – представляет смещение в часах относительно времени UTC;

- *zz* - представляет смещение в часах относительно времени UTC, однозначные числа дополняются нулем слева.

Пример использования шаблонов формата сообщений:

«Формат сообщений»: «В *{datetime}* на точке прохода *{device}* был зафиксирован *{event}* сотрудника *{name}* из организации: *{organization}* отдела *{department}* с категорией *{category}*. Номер карты: {*cardcode*}»,

«Формат даты и времени»: «*dd-MM-yyyy HH:mm:ss zz*»,

Итоговый текст события, записанный в атрибут пользователя: «В 21-12-2020 18:50:37 +04 на точке прохода <имя_тустройства> был зафиксирован Штатный выход сотрудника Иванов Иван Иванович из организации: <имя организации> отдела <имя отдела> с категорией <имя категории>. Номер карты: *0011223344FC*».

4.4 Настройка присвоения уровней доступа

Для каждой организационной единицы (OU) в системе можно задать уровень доступа, который будет установлен для нового пропуска в ПК «Бастион-3», для этого необходимо перейти на страницу панели управления «Организационные модули» (Рис. 9).

Настройки каждого организационного модуля представлены одной единственной настройкой – «*Уровень доступа*», которая определяет уровень доступа по умолчанию для пропусков всех импортируемых из этого OU пользователей LDAP.

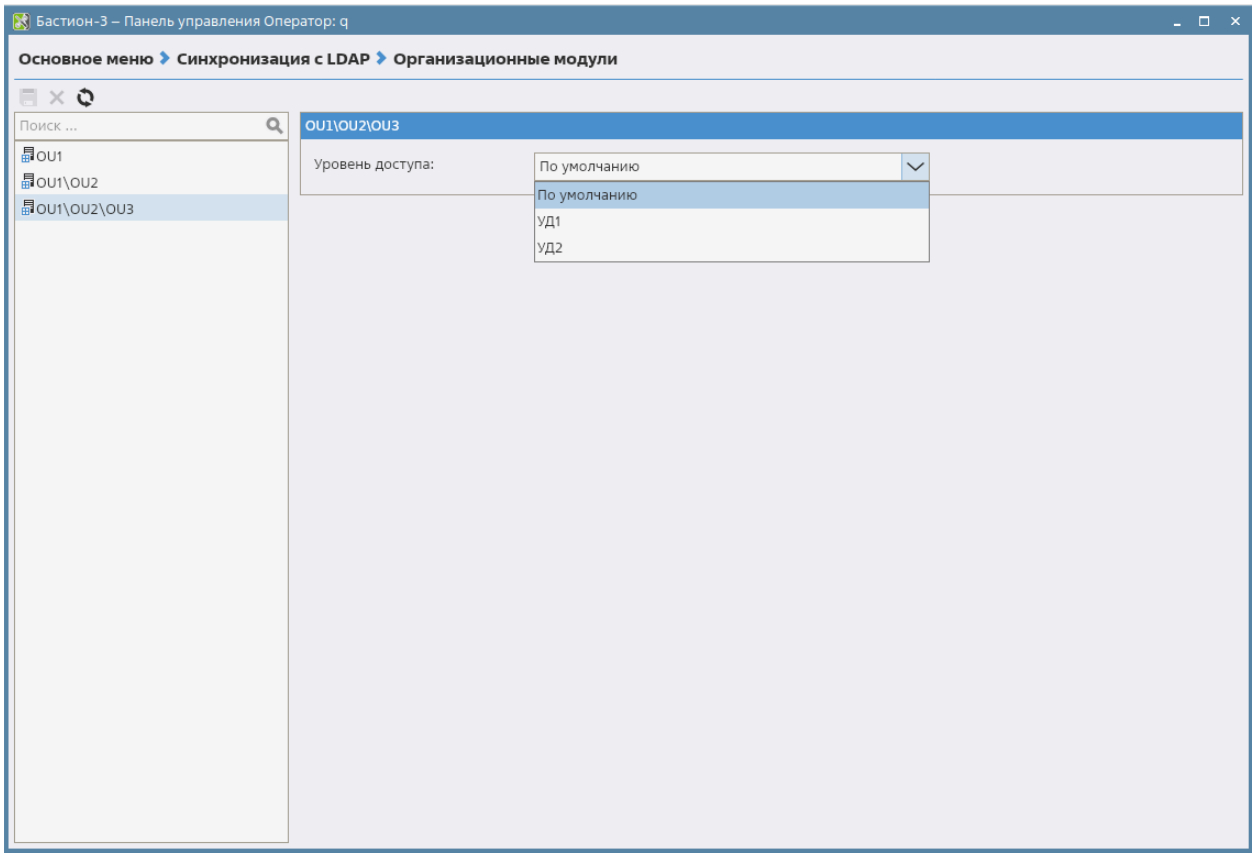

Рис. 9. Настройка связи OU и уровней доступа

4.5 Настройка форматирования LDIF-запросов для экспорта персон

Для удобства настройки имеется возможность подстановки конфигураций LDIF-запросов по умолчанию для серверов ALD, MS-AD и OpenLDAP. Конфигурации по умолчанию содержат в себе минимальный необходимый набор атрибутов для LDAP-серверов. Необходимо учитывать, что наборы атрибутов могут отличаться в зависимости от конфигураций LDAP сервера.

Атрибуты необходимо задавать в формате «attributeName:attributeValue» по одному значению в строке.

Дополнительно в поле форматирования LDIF-запроса можно использовать спецсимвол «#» в качестве символа комментария, всё что находится правее данного спецсимвола будет отбрасываться.

Для форматирования запросов имеется возможность подстановки мета-переменных, которые будут заменятся соответствующими данными:

- {path} – путь OU экспорта персоны, берется из общей настройки «Путь экспорта» или из «Категории пропуска для экспорта» если данные настройки включены;
- {password} – пароль по умолчанию, который задается в поле «Пароль по умолчанию»;
- {name} – фамилия персоны;
- {firstName} – имя персоны;
- {secondName} – отчество персоны;
- {fullName} – поное ФИО персоны;
- {fullNameLower} – полное ФИО персоны строчными буквами;
- {nameUniDecode} – фамилия персоны латиницей;
- {firstNameUniDecode} – имя персоны латиницей;
- {secondNameUniDecode} – отчество персоны латиницей;
- {nameUniDecodeLower} – фамилия персоны латиницей строчными буквами;
- {firstNameUniDecodeLower} – имя персоны латиницей строчными буквами;
- {secondNameUniDecodeLower} – отчество персоны латиницей строчными буквами;
- {fullNameUniDecode} – полное ФИО персоны латиницей;
- {fullNameUniDecodeLower} – полное ФИО персоны латиницей строчными буквами;
- {personId} – идентификатор персоны ПК «Бастион-3»;
- {personId+<целое_число>} – идентификатор персоны ПК «Бастион-3» с инкрементом;
- {creationDate} – дата создания последнего выданного персонального пропуска

- {creatorName} – имя выдавшего пропуск;
- {birthDate} – дата рождения персоны;
- {birthPlace} – место рождения персоны;
- {email} – электронная почта персоны;
- {phone} – телефон персоны;
- {personComment} – описание к персоне.

Некоторые атрибуты на LDAP-сервере могут иметь ограничения на максимальную длину значения, для этого в формате LDIF-запроса имеется возможность для каждой мета-переменной указать максимальную длину значения подставляемых данных. Пример подстановки фамилии персоны с максимальной длиной в 20 символов: «{firstName}[20]». Если исходная длина строки превысит лимит символов, то строка будет обрезана.

5 Процесс синхронизации

5.1 Начальная синхронизация

В системе предусмотрена начальная синхронизация OU, чтобы оператор системы мог назначить каждому OU уровни доступа перед тем, как будут загружены пользователи.

Оператор должен ввести настройки подключения, но не ставить флаг «Синхронизация включена», после чего сохранить настройки и нажать кнопку «Обновить». В результате список OU загрузится из AD и отобразится в конфигураторе.

После этого следует проставить уровни доступа для OU, включить галочку «Синхронизация включена» и нажать «Сохранить» повторно.

5.2 Штатный режим работы

Алгоритм работы системы в штатном режиме рассмотрен ниже.

- Синхронизация выполняется периодически с интервалом в N секунд, где N – значение параметра «Период синхронизации, сек.» в конфигурации.
- При нажатии кнопки ручной синхронизации в конфигураторе процесс синхронизации запускается немедленно.
- Для каждого активного (не заблокированного) пользователя LDAP, у которого еще нет активного выданного пропуска или заявки на пропуск в ПК «Бастион-3» добавляется заявка на выдачу постоянного пропуска. Уровень доступа для такого пользователя выставляется в соответствии с настроенным в конфигурации уровнем доступа по умолчанию для OU, в котором находится пользователь. Место работы пользователя - структура OU, в котором он находится. При этом верхний OU в иерархии добавляется в ПК «Бастион-3» в качестве организации, а все дочерние – в качестве подразделений.

- Сопоставление пользователей выполняется по их уникальным идентификаторам (UID), которые хранятся в атрибуте «objectGUID».
- Выдача пропуска для созданных в процессе синхронизации заявок выполняется вручную оператором «Бюро пропусков».
- Уровень доступа автоматически назначается один раз при создании новой заявки на пропуск, т. е. при обнаружении нового пользователя LDAP или при разблокировке ранее заблокированного. После этого уровень доступа не будет изменяться автоматически в процессе синхронизации.
- Уровень доступа для заявки на пропуск или для активного выданного пропуска может изменить вручную оператор «Бюро пропусков».
- При блокировке в LDAP аккаунта пользователя выполняется возврат активного пропуска или перенос в архив заявки на пропуск этого пользователя, либо блокировка активного пропуска, если в настройках выбрана соответствующая опция.
- При смене ФИО пользователя LDAP обновляются его ФИО в ПК «Бастион-3».
- При удалении пользователя в LDAP в ПК «Бастион-3» не выполняются никакие действия.
- При смене имени OU в LDAP в ПК «Бастион-3» будет создано новое подразделение, старое при этом не удаляется. Для всех пользователей, находящихся в этом OU, будет изменено место работы в соответствии с новым именем подразделения.
- Импорт аккаунтов в LDAP выполняется для активных пропусков, выданных на основании заявок, созданных вручную оператором ПК «Бастион-3».
- Если человек имеет несколько активных пропусков, то экспорт выполняется в соответствии с его *основным* пропуском. Основным считается постоянный пропуск, временный пропуск (при отсутствии постоянного), либо разовый (если отсутствуют активные пропуска других типов).
- Экспорт аккаунта выполняется в соответствии с типом *основного* пропуска и OU, настроенным для данного типа пропуска.
- Если OU для экспорта не задан, то персоны экспортироваться не будут.
- При возврате последнего активного пропуска экспортированной из ПК «Бастион-3» персоны, её аккаунт в LDAP будет заблокирован.
- При появлении у персоны с заблокированным экспортированным аккаунтом LDAP нового активного пропуска, аккаунт в LDAP будет разблокирован.
- OU экспортированного из ПК «Бастион-3» аккаунта задаётся при экспорте один раз, и в дальнейшем автоматически при синхронизации не изменяется.
- Значение тегов для экспорта даты создания и ФИО создавшего оператора задаются при экспорте один раз и в дальнейшем автоматически при синхронизации не изменяются.

- Если для экспорта даты создания и ФИО выдавшего пропуск оператора задан один и тот же тег, то дата создания и ФИО выдавшего пропуск оператора будут экспортированы в этот тег в формате «<create_date> <oper_name>», где “<create_date>” – дата выдачи *основного* пропуска в формате “yyyy.MM.dd”, а “<create_date> - дата выдачи пропуска”.
- При смене ФИО персоны в ПК «Бастион-3» будет изменено ФИО экспортированного аккаунта в LDAP.

6 Нештатные ситуации

6.1 Не работает подключение к Astra Linux Directory

Для корректной работы подключения по протоколу LDAP необходимо предварительно включить простой метод аутентификации (Simple Authentication). Для этого:

1. На контролере домена ALD выполнить команды в терминале (<Alt+T>):

   ```
   sudo apt install ldap-utils

   cd /etc/ldap/schema/
   ```

2. В каталоге /etc/ldap/schema/ создать файл 11-allow-simple-bind.ldif с содержимым по образцу:

   ```
   dn: cn=config

   changetype: modify

   delete: olcDisallows


   dn: olcDatabase={1}hdb,cn=config

   changetype: modify

   add: olcRootPW

   olcRootPW: secret
   ```

   Вместо secret указать пароль для подключения к базе LDAP от имени пользователя admin/admin, который был задан на этапе инициализации сервера ALD.

3. Получить билет Kerberos с помощью команды:

   ```
   kinit admin/admin
   ```

4. Внести изменения в LDAP:

   ```
   ldapmodify -f 11-allow-simple-bind.ldif
   ```

Подключение методом simple authentication возможно только пользователем admin/admin.

6.2 Нарушение целостности домена Astra Linux Directory

После экспорта персоны из ПК «Бастион-3» на сервер ALD может быть нарушена целостность домена. Просмотреть целостность можно в настройках ALD «Управление доменной политикой безопасности» (Рис. 10).

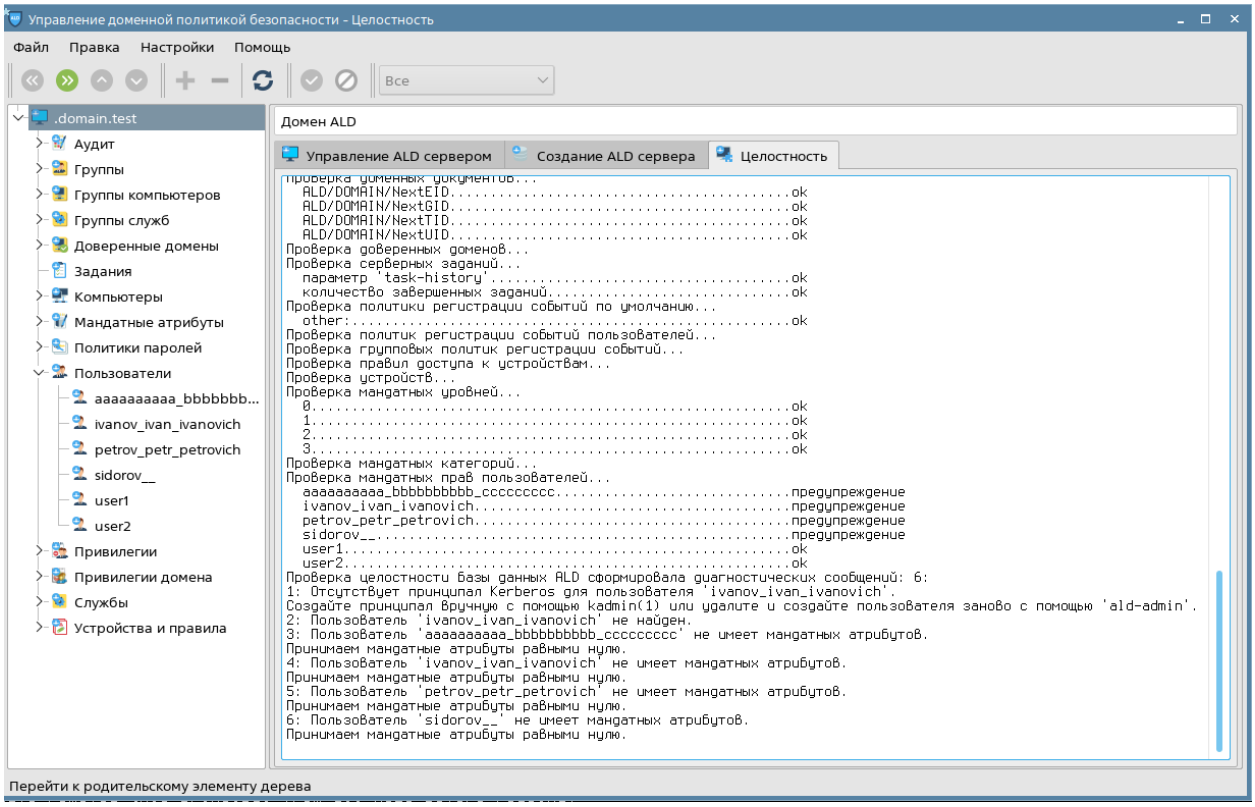

Рис. 10. Сведения о целостности домена ALD

Причинами нарушения целостности могут быть неправильные имена пользователей согласно политикам безопасности ALD, слишком короткие имена или недопустимые символы.

Обязательно для каждого экспортированного пользователя ALD необходимо вручную добавить принципал Kerberos – защищенный протокол сетевой аутентификации. Для этого:

1. На контролере домена ALD выполнить команды в терминале (<Alt+T>): `kadmin;`
2. `ввести Kerberos-пароль администратора;`
3. `выполнить команду addprinc <полное_имя_пользователя_ALD>;`
4. `указать Kerberos-пароль для пользователя согласно политикам безопасности.`

6.3 Пользователь имеет UID, который меньше, чем MINIMUM_UID

На сервере ALD минимальное значение uidNumber по умолчанию равно 2500 (10000 в OpenLDAP). Идентификаторы пользователей ПА «Бастион-3» могут быть меньше чем минимальные значения uidNumber, для этого в настройках

форматирования LDIF-запросов необходимо использовать мета-переменную с инкрементом 2500 (10000) или больше: {personId+2500}.

6.4 Не работает возврат пропусков

Для работы функции возврата пропусков для пользователей, заблокированных в LDAP, необходимо, чтобы пользователь, учётные данные которого используются для синхронизации (см. п. 4.1), имел права на чтение данных User Account Control (UAC). Если пользователь таких прав не имеет, то будут работать все функции синхронизации, за исключением функции возврата пропусков заблокированных пользователей.

6.5 Не работает импорт пользователей из ПК «Бастион-3»

Для импорта пользователей в LDAP необходимо, чтобы правильно были заданы OU для экспорта из ПК «Бастион-3», а пароль по умолчанию, если указан в формате LDIF-запроса, соответствовал политикам, настроенным в LDAP.

6.6 Не передаются значения в атрибут при экспорте событий прохода

Возможна нештатная ситуация, если длина текста экспортируемого события прохода превысит максимальную длину значений заданного атрибута. В этом случае экспорт информации события не произойдет. Для решения подобных ситуаций предусмотрена настройка «Максимальная длина значения атрибута». По умолчанию ограничения выключены и значение настройки равно 0. В случае превышения длины экспортируемый текст будет обрезаться согласно заданным настройкам с многоточием в конце.

6.7 Не работает экспорт персон

Возможна нештатная ситуация, когда при экспорте персон их аккаунты не создаются. Возможной причиной может быть слишком длинное имя аккаунта, превышающее лимит по количеству символов. Или любой другой атрибут сервера LDAP имеет ограничение по количеству символов. В этом случае поможет уменьшение длины мета-переменных для проблемных атрибутов в LDIF-конфиге.

Так же аккаунты могут не создаваться из-за не уникального имени аккаунта, которое формируется при экспорте у конкретной персоны. Для решения данной проблемы можно найти дублирующий аккаунт и удалить его перед повторным экспортом или изменить атрибуты, отвечающие за идентификацию имен аккаунтов, таким образом, чтобы для каждой персоны мог создаться аккаунт с уникальным именем.

6.8 Сервер LDAP недоступен на ОС Linux через TLS

Параметр «Отключить верификацию сертификата сервера» на платформе ОС Linux может работать некорректно. Проверка подключения к серверу LDAP по порту 636 и включенной настройкой «Использовать TLS» возвращает ошибку «The LDAP server is unavailable». В этом случае для процесса *BAgentSvc* системную переменную «*LDAPTLS_REQCERT=never*» необходимо указать в файле «*etc/systemd/system.conf*» для раскомментированного параметра *DefaultEnvironment.* Пример:

«*DefaultEnvironment=LDAPTLS_REQCERT=never*».

Приложения

Приложение 1. История изменений

2024.1 (05.04.2024)

[*] Исправления ошибок импорта и экспорта.

[*] Оптимизирована загрузка большого количества LDAP-аккаунтов.

2023.3 (29.12.2023)

[+] Для поддержки гибкого механизма экспорта реализована возможность настройки форматирования LDIF-запросов.

[+] Отлажена и проверена работа модуля с серверами ALD (AstraLinux), Microsoft Active Directory и OpenLDAP.

2023.1 (03.04.2023)

[+] Первая версия, включена в комплект поставки ПК «Бастион-3».