Бастион-2 – Active Directory. Руководство администратора

Версия 2.1.13

(13.09.2023)

Самара, 2022

Оглавление

1 Общие сведения

Система «Бастион-2 – Active Directory» предназначена для синхронизации пропусков СКУД АПК «Бастион-2» с пользователями Active Directory.

Возможности системы включают:

- Импорт пользователей из Active Directory в АПК «Бастион-2» с созданием заявок на пропуска;
- Возврат пропусков в АПК «Бастион-2» при блокировке в Active Directory владельца пропуска;
- Настройку правил присвоения уровней доступа в АПК «Бастион-2»;
- Настройку соответствий полей *пропуска* и *персоны* в АПК «Бастион-2» полям в Active Directory;
- Экспорт пользователей в Active Directory на основе активных пропусков, созданных и выданных в АПК «Бастион-2»;
- Ручная синхронизация данных пропуска и персоны в АПК «Бастион-2» и полей пользователя в Active Directory;
- Запись настраиваемого текста событий прохода персоны из АПК «Бастион-2» в заданный атрибут этого пользователя в Active Directory;
- Наличие дополнительного модуля, который позволяет блокировать активные сессии пользователей ПК, связанных с персонами в АПК «Бастион-2» при выходе персоны с заданной территории.

Система состоит из модуля расширения сервера системы АПК «Бастион-2» и конфигуратора, как показано на Рис. 1.

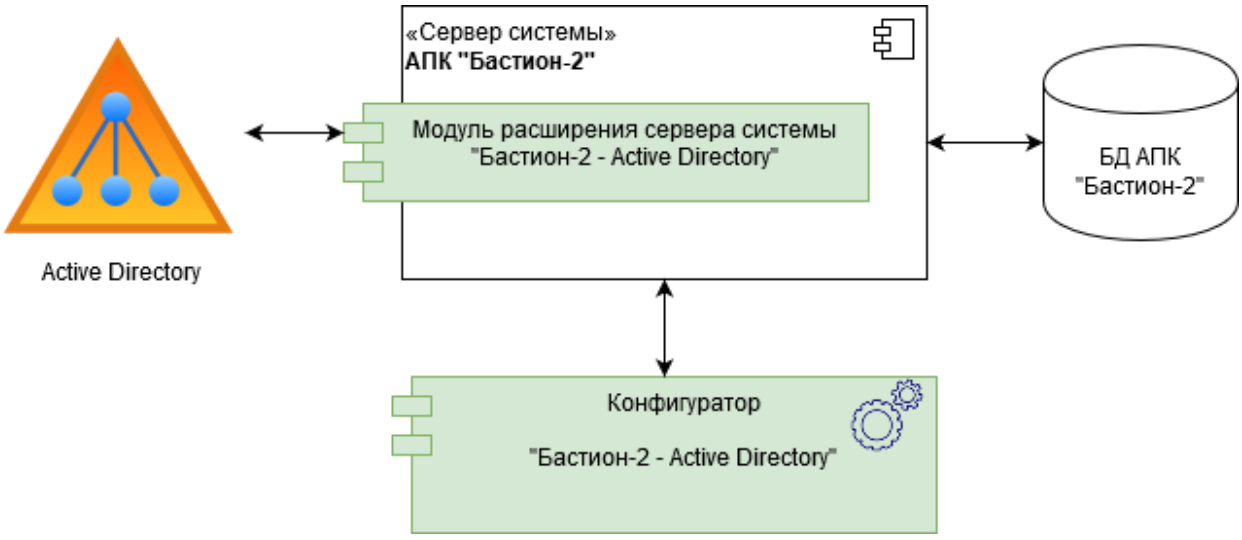

Рис. 1. Структура системы «Бастион-2 – Active Directory»

Для настройки системы пользователь должен обладать знаниями о структуре и администрировании Active Directory, организационной структуре предприятия и администрировании СКУД АПК «Бастион-2».

2 Условия применения

2.1 Требования к совместимости

На модуль «Бастион-2 – Active Directory» распространяются те же требования к аппаратной и программной платформе, что и для АПК «Бастион-2».

Для работы требуется АПК «Бастион-2» версии не ниже 2.1.9.

Технология интеграции подразумевает возможность использования в качестве каталога пользователей не только Active Directory, но и другие серверы LDAP. Тем не менее, следует учитывать, что тестирование системы производилось только с Active Directory.

2.2 Лицензирование системы

Для работы системы требуется наличие в ключе защиты строки активации модуля «Бастион-2 – Active Directory». Модуль не имеет количественных ограничений на объем синхронизируемых данных.

Как видно из схемы на Рис. 1, всегда требуется наличие одного модуля «Бастион-2 – Active Directory» на каждом сервере системы.

3 Установка

Модуль «Бастион-2 – Active Directory» устанавливается в составе АПК «Бастион-2». Для его установки нужно отметить соответствующий флаг в списке устанавливаемых модулей.

4 Настройка

4.1 Основные настройки

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

Настройка модуля осуществляется с помощью приложения «Active Directory – конфигуратор».

Интерфейс конфигуратора 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;

- Обновить – служит для обновления списка OU в узле «Organizational Units» (но и выполняет также функции кнопки «Отменить изменения»);
- Запустить синхронизацию – служит для немедленного запуска процесса синхронизации с Active Directory. После ручного запуска синхронизации следующая итерация будет выполнена после интервала времени, заданного в настройке «Период синхронизации».

2) Дерево настроек – содержит 3 основных узла, это:

- Основные настройки – основные настройки модуля «Бастион-2 – Active Directory»;
- Синхронизация – предоставляет список всех пользователей Active Directory и персон АПК «Бастион-2» с возможностью запуска точечной ручной синхронизации персонала;
- Organizational Units – содержит список OU, существующих на сервере Active Directory, либо один элемент с названием «<ошибка подключения>» если настройки подключения к серверу Active Directory указаны неправильно, либо подключение к серверу невозможно по другим причинам.

3) Область настройки – содержит доступные для редактирования параметры выбранного в дереве настроек узла.

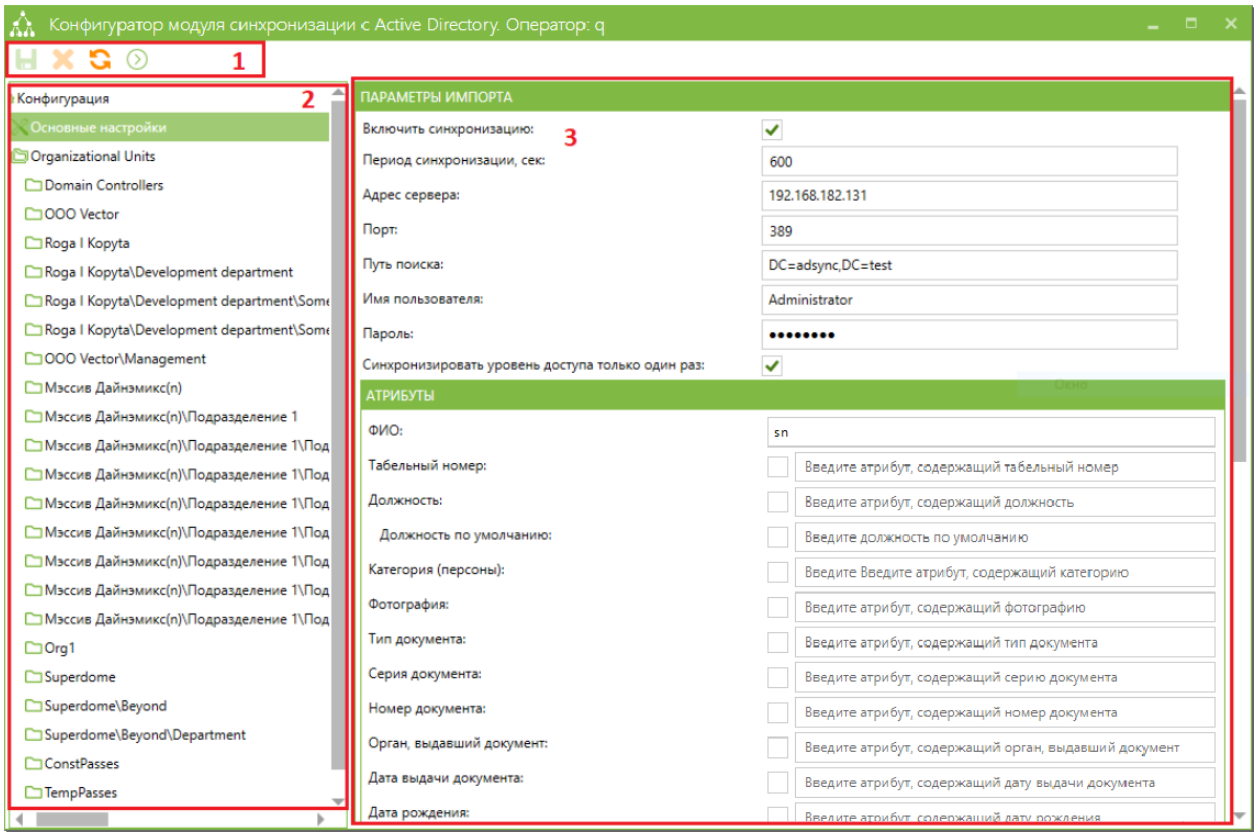

Рис. 2. Active Directory – конфигуратор

Основные настройки изображены на Рис. 2, Рис. 3 и представлены двумя группами – это настройки импорта и настройки экспорта. Группа настроек импорта имеет вложенную группу для настроек

атрибутов импорта. Галочки напротив каждого поля ввода имени атрибута включают импорт данного поля, без включенной галочки атрибут не импортируется.

Настройки импорта содержат следующие пункты:

- *Включить синхронизацию* – при отключенной синхронизации экспорт данных из Active Directory производиться не будет;
- *Период синхронизации, сек.* – временной промежуток в секундах между циклами синхронизации;
- *Адрес сервера* – IP-адрес или доменное имя сервера Active Directory;
- *Порт* – порт сервера Active Directory;
- *Путь поиска* – путь к организационной единице Active Directory (домен или OU), из которой будут загружаться пользователи, оформленный по правилам именования объектов в Active Directory, например, «OU=OrgUnitOne,DC=test,DC=com»;

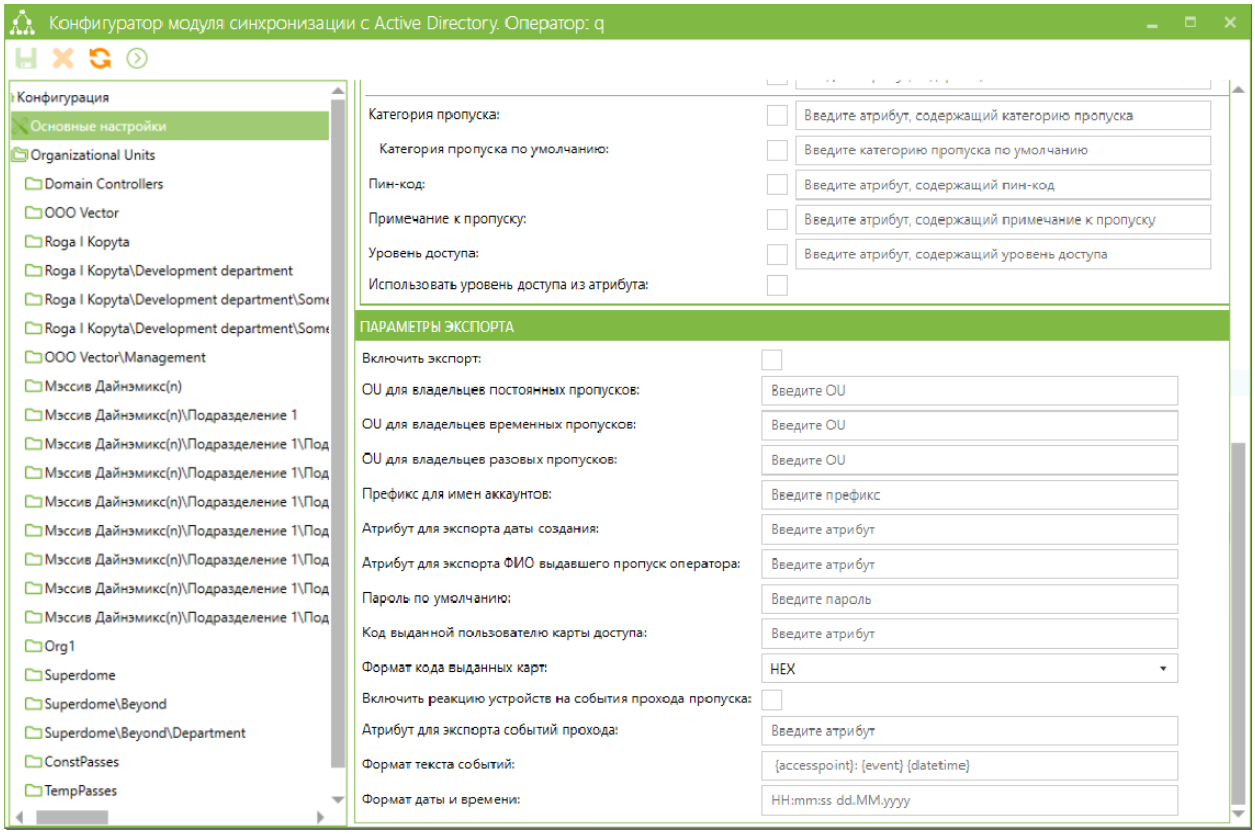

Рис. 3. Active Directory – конфигуратор (часть 2)

- *Имя пользователя* – логин пользователя Active Directory, имеющего права на чтение данных пользователей, включая данные User Account Control (UAC);
- *Пароль* – пароль пользователя Active Directory;
- *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 Active Directory

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;

- *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;
- *Должность по умолчанию* – значение этой настройки будет использоваться в тех случаях, когда у пользователя AD будет пустым значение атрибута, указанного в качестве атрибута для импорта должности;
- *Категория (персоны)* – атрибут, который будет использоваться для чтения категории персоны;
- *Фотография* – атрибут, значение которого будет использоваться для получения фотографии (в формате Base64). Фотография из Active Directory 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;
- *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;
- *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;
- *Подразделение* – атрибут, значение которого будет использоваться для чтения подразделения (если включена настройка «Использовать подразделение из атрибута»). Значение атрибута может содержать несколько вложенных наименований подразделений (где самое старшее наименование является организацией), разделённых символом “\” (например: «ООО Вектор\Отдел кадров»);
- *Использовать подразделение из уровня доступа* – при включении этой настройки подразделение, в котором работает пользователь, будет браться не на основании OU, в котором находится аккаунт пользователя в AD, а на основе значения атрибута.

Настройки экспорта содержат следующие пункты:

- *Включить экспорт* – данная настройка отвечает за включение/выключение экспорта данных из АПК «Бастион-2» в Active Directory;
- *OU для владельцев постоянных пропусков* – от этого параметра зависит, в какую организационную единицу будут экспортироваться владельцы постоянных пропусков. Имя OU должно быть оформлено по правилам именования объектов в Active Directory, таким образом, чтобы строка, сформированная из значения параметра «OU для владельцев постоянных пропусков» и значения параметра «Путь поиска» в формате “<OU>,<Path>”, где “<OU>” – значение параметра «OU для владельцев постоянных пропусков», а «<Path>» - значение параметра «Путь поиска» представляла собой правильное и полное имя OU, в который необходимо экспортировать владельцев постоянных пропусков;

- *OU для владельцев временных пропусков* – от этого параметра зависит, в какую организационную единицу будут экспортироваться владельцы временных пропусков. Имя OU должно быть оформлено по правилам именования объектов в Active Directory, таким образом, чтобы строка, сформированная из значения параметра «OU для владельцев временных пропусков» и значения параметра «Путь поиска» в формате “<OU>,<Path>”, где “<OU>” – значение параметра «OU для владельцев временных пропусков», а «<Path>» - значение параметра «Путь поиска» представляла собой правильное и полное имя OU, в который необходимо экспортировать владельцев временных пропусков;

- *OU для владельцев разовых пропусков* – от этого параметра зависит, в какую организационную единицу будут экспортироваться владельцы разовых пропусков. Имя OU должно быть оформлено по правилам именования объектов в Active Directory, таким образом, чтобы строка, сформированная из значения параметра «OU для владельцев разовых пропусков» и значения параметра «Путь поиска» в формате “<OU>,<Path>”, где “<OU>” – значение параметра «OU для владельцев разовых пропусков», а «<Path>» - значение параметра «Путь поиска» представляла собой правильное и полное имя OU, в который необходимо экспортировать владельцев разовых пропусков;

- *Префикс для имен аккаунтов* – префикс для имени аккаунта экспортируемого пользователя. Имя пользователя в Active Directory будет иметь вид: «<prefix>_<name>», где “<prefix>” – префикс имени аккаунта, а “<name>” – фамилия владельца пропуска, транслитерированная в латинские символы;

- *Атрибут для экспорта даты создания* – атрибут пользователя в Active Directory, в который будет записываться дата выдачи пропуска;

- *Атрибут для экспорта ФИО выдавшего пропуск оператора* – атрибут пользователя Active Directory, в который будет записываться ФИО оператора, выдавшего пропуск (при условии, что к оператору АПК «Бастион-2» привязан его собственный пропуск с ФИО);

- *Пароль по умолчанию* – пароль, который устанавливается для нового пользователя Active Directory пользователя при импорте пропуска из АПК «Бастион-2». Пароль должен удовлетворять требования политик Active Directory. Пароль устанавливается по умолчанию истёкшим, так что пользователю будет необходимо сменить его при первом входе;

- *Код выданной пользователю карты доступа* – атрибут пользователя в Active Directory, в который будет записываться код выданной карты в «АРМ Бюро пропусков»;

- *Формат кода выданной карты* – формат кода выданной карты доступа в «АРМ Бюро пропусков», представленный в двух форматах: шестнадцатеричный (HEX) или десятичный (DEC);

- *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 Active Directory, 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.

4.2 Настройка реакций на события прохода

Передача событий прохода персонала осуществляется при помощи механизма сценариев АПК «Бастион-2». Чтобы создать сценарий передачи события, следует добавить в него действие «Записать информацию в Active Directory» (действия для устройства «Система»). В список событий-триггеров следует добавить события проходов, по которым будет производиться запись текста события в назначенный атрибут Active Directory соответствующей персоны (Рис. 4).

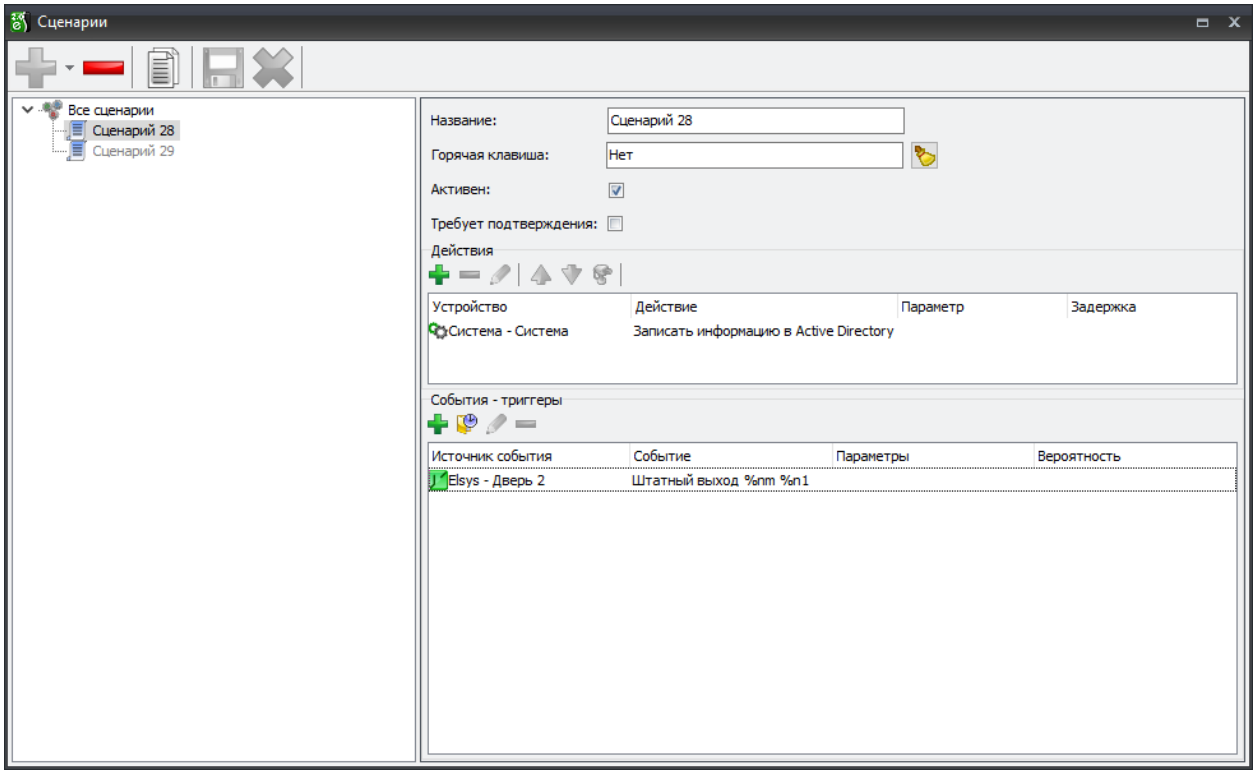

Рис. 4. Настройки сценария

Таким образом, при добавленном триггерном событии, например «Дверь 2: Штатный выход %nm %n1» при проходе через считыватель Двери 2, система передаст в атрибут пользователя Active Directory текст события, согласно настроенному формату.

4.3 Настройка формата текста событий

В конфигураторе «Бастион-2 – Active Directory» есть возможность настроить формат текста событий для записи в атрибут пользователя Active Directory. 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;
- *{access_point}* – имя точки прохода события;
- *{card_code}* – 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 *{accesspoint}* 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_точки_доступа> 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 приложения для блокировки ПК

Блокировку компьютеров производит отдельное приложение-агент: ActiveDirectoryPcAgent.exe. Установщик этого приложения входит в комплект установки АПК «Бастион-2»:

«*Packages**Applications**ActiveDirectory**ActiveDirectoryPcAgentSetup.msi*».

Установщик приложения поддерживает установку отдельно от других компонентов системы.

Установщик приложения поддерживает как установку для всех пользователей компьютера (по умолчанию), так и установку для текущего пользователя. Для установки только для текущего пользователя необходимо передать в параметрах командной строки два аргумента со значениями: **“ALLUSERS=2”** и **“MSIINSTALLPERUSER=1”**.

По умолчанию установка производится в каталог:

«*C:\Program Files(x86)\ES-Prom\Bastion2\Aries\Roles\ActiveDirectory*».

При установке для текущего пользователя установка выполняется в каталог

«C:\Users\<имя_пользователя>\AppData\Local\Programs\ES-Prom\Bastion2\Aries\Roles\ActiveDirectoryPcAgent».

Приложение-агент можно при установке добавить в автозагрузку, для этого необходимо при установке передать в параметрах командной строки аргумент **ADDTOAUTORUN** со значением **1** (“ADDTOAUTORUN=1”).

Файл конфигурации «*config.json*» располагается в каталоге:

«C:\Users\<имя_пользователя>\AppData\Local\ES-prom\Bastion2\ActiveDirectoryPcAgent».

В файле конфигурации задаются основные параметры для работы. Имеется возможность запуска приложения при помощи командной строки с использованием параметров. В этом случае параметры в командной строке переопределят параметры из файла конфигурации.

Параметры конфигурации:

- *Username* – имя пользователя Active Directory или атрибут пользователя «*sAMAccountName*», по которому будет проводится мониторинг атрибутов каталога пользователя. Параметр через cmd «--username=<имя_пользователя>»;
- *AttributeName* – имя атрибута пользователя, в который записывается текст событий прохода. По умолчанию используется атрибут «*userParameters*». Параметр через cmd «--attributename=<атрибут_событий_прохода>»;
- *Condition* – условный текст, при наличии которого в тексте события приложение-агент будет блокировать экран пользовательского компьютера. По умолчанию используется текст «выход». Параметр через cmd «--condition=<условие>»;
- *IsEnabled* – параметр, отвечающий за активность приложения-агента. «1» - приложение-агент начинает мониторинг каталога пользователя в Active Directory после запуска, «0» - после запуска приложения-агента мониторинг не производится. Параметр для запуска через cmd «--username». Параметр через cmd «--isenabled=<включить>»;
- *ClearAttribute* – параметр, включающий очистку атрибута от текста события прохода после блокировки экрана пользовательского компьютера. «1» - очистка включена, «0» - очистка отключена. Параметр через cmd «--clearattribute=<очистить>»;
- *Period* – параметр, определяющий время в секундах, которое должно проходить между итерациями проверки атрибута в Active Directory. Параметр через cmd «--Period=<значение>»;
- *Logging* – параметр, включающий запись сообщений в лог-файл, «1» - включить запись, «0» - выключить. Параметр через cmd «--logging=<включить>».

Установщик приложения-агента поддерживает аргументы командной строки, соответствующие параметрам конфигурации, переданные значения которых будут записаны в файл конфигурации.

После каждого изменения файла конфигуратора рекомендуется перезапускать приложение-агент.

Все свои действия утилита блокировки будет сохранять в лог-файл, который будет располагаться в каталоге:

«C:\Users\<имя_пользователя>\AppData\Local\ES-prom\Bastion2\ActiveDirectoryPcAgent».

4.5 Настройка присвоения уровней доступа

Для каждой организационной единицы (OU) в системе можно задать уровень доступа, который будет установлен для нового пропуска в АПК «Бастион-2».

Внешний вид конфигуратора при выборе OU в дереве настроек представлен на Рис. 5. Здесь доступна одна единственная настройка – «*Уровень доступа*», которая определяет уровень доступа по умолчанию для пропусков всех импортируемых из этого OU пользователей Active Directory.

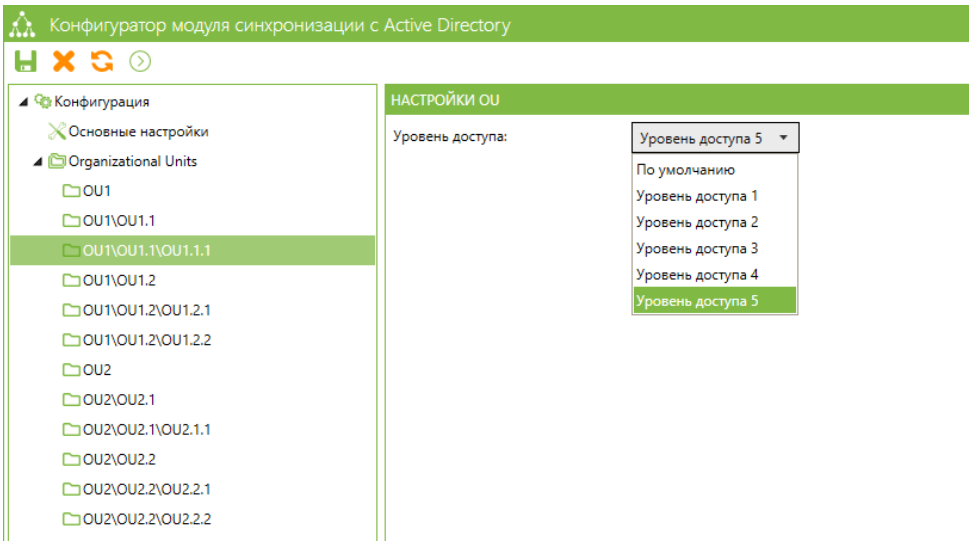

Рис. 5. Настройка связи OU и уровней доступа

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 Active Directory, у которого еще нет активного выданного пропуска или заявки на пропуск в АПК «Бастион-2» 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 АПК «Бастион-2» 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 Active Directory 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 Active Directory аккаунта пользователя выполняется возврат активного пропуска или перенос в архив заявки на пропуск этого пользователя.
- При смене ФИО пользователя Active Directory обновляются его ФИО в АПК «Бастион-2».
- При удалении пользователя в Active Directory в АПК «Бастион-2» не выполняются никакие действия.
- При смене имени OU в Active Directory в АПК «Бастион-2» 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 Active Directory выполняется для активных пропусков, выданных на основании заявок, созданных вручную оператором АПК «Бастион-2».
- 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 для какого-то типа пропуска не задан OU для экспорта, то персоны с *основным* пропуском данного типа экспортироваться не будут.
- При возврате последнего активного пропуска экспортированной из АПК «Бастион-2» персоны, её аккаунт в Active Directory будет заблокирован.
- При появлении у персоны с заблокированным экспортированным аккаунтом Active Directory нового активного пропуска, аккаунт в Active Directory будет разблокирован.
- OU экспортированного из АПК «Бастион-2» 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 АПК «Бастион-2» будет изменено ФИО экспортированного аккаунта в Active Directory.

5.3 Выборочная синхронизация пользователей в АРМ «Бюро пропусков»

В АРМ «Бюро пропусков» имеется возможность ручной синхронизации выбранных атрибутов пользователей. При выборе одного или нескольких пропусков из списка на верхней панели «Основное» из раздела «Управление пропусками» появляется специальная кнопка «Синхронизация с AD». Синхронизировать данные можно через контекстное меню выбранных пропусков. Кнопка инициализирует импорт данных пользователей AD и экспорт данных персон АПК «Бастион-2» в зависимости от того, где были созданы профили пользователей (Рис. 6).

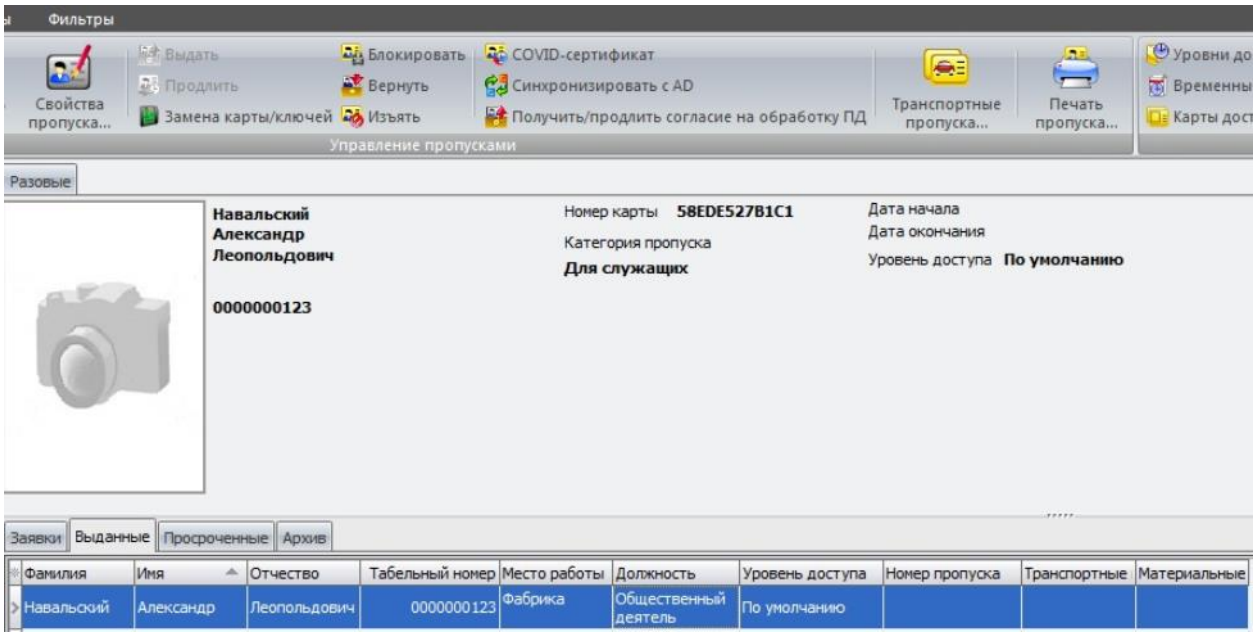

Рис. 6. Выборочная синхронизация персон в АРМ «Бюро пропусков»

Дополнительно имеется возможность синхронизировать персон в меню «Глобального поиска пропусков». Синхронизировать данные можно через контекстное меню выбранных пропусков по нажатию кнопки «Синхронизировать с AD». Данная кнопка будет отображаться только когда глобальный поиск будет вызван из АРМ «Бюро пропусков» (Рис. Рис. 7).

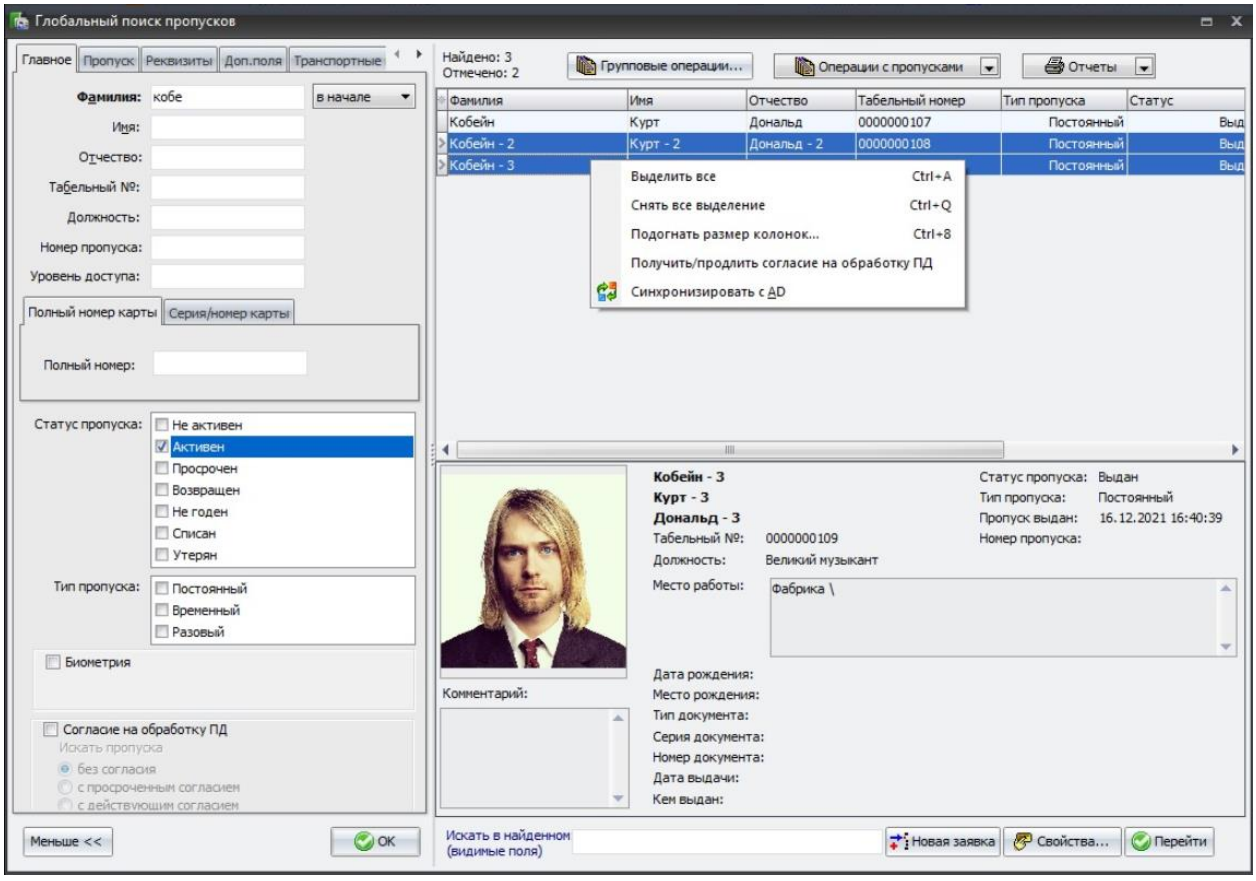

Рис. 7. Синхронизация с AD через «Глобальный поиск пропусков»

6 Нештатные ситуации

6.1 Не работает возврат пропусков

Для работы функции возврата пропусков для пользователей, заблокированных в Active Directory, 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.

6.2 Не работает импорт пользователей из АПК «Бастион-2»

Для импорта пользователей в Active Directory необходимо, чтобы правильно были заданы OU для экспорта из АПК «Бастион-2», а пароль по умолчанию соответствовал политикам, настроенным в Active Directory.