ГАЗИНФОРМ СЕРВИС

ПРОГРАММНЫЙ КОМПЛЕКС «ПЛАТФОРМА РАСШИРЕННОЙ АНАЛИТИКИ БЕЗОПАСНОСТИ ANKEY ASAP» v.2.4.1

Руководство по инсталляции

643.72410666.00071-01 94 01

Листов 76

Содержание

Введение

Настоящее руководство содержит сведения по установке и настройке программного комплекса «Платформа расширенной аналитики безопасности Ankey ASAP» v.2.4.1 643.72410666.00071-01 (далее по тексту – ПК «Ankey ASAP», ПК или комплекс).

При установке и настройке ПК «Ankey ASAP» дополнительно использовать документацию на систему управления базами данных (СУБД) «Jatoba».

1 Общие сведения

1.1 Назначение программного комплекса

Программный комплекс «Платформа расширенной аналитики безопасности Ankey ASAP» v.2.4.1 предназначен для автоматизации работы специалиста информационной безопасности (ИБ) по мониторингу и анализу событий и инцидентов посредством формирования аналитического контента современными методами расширенной аналитики данных от систем управления событиями безопасности.

ПК «Ankey ASAP» является программным комплексом расширенной аналитики событий и инцидентов с функциями поведенческого анализа и может применяться для защиты информации:

– в государственных информационных системах до 2 класса защищенности;

– в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах до 2 класса защищенности;

– в информационных системах значимых объектов критической информационной инфраструктуры Российской Федерации до 2 категории значимости;

– в информационных системах для обеспечения 2, 3 и 4 уровня защищенности персональных данных.

1.2 Структура и описание комплекса

ПК «Ankey ASAP» реализует функции по получению, обработке и визуализации результатов мониторинга и расширенной аналитики данных в виде дашбордов и интерактивных отчетов/графических диаграмм, а также функции администратора по настройке ПК «Ankey ASAP», управлению пользователями ПК «Ankey ASAP» и ведению конфигурационных и справочных данных.

Схема взаимодействия ПК «Ankey ASAP» с внешними компонентами приведена на рисунке 1.1.

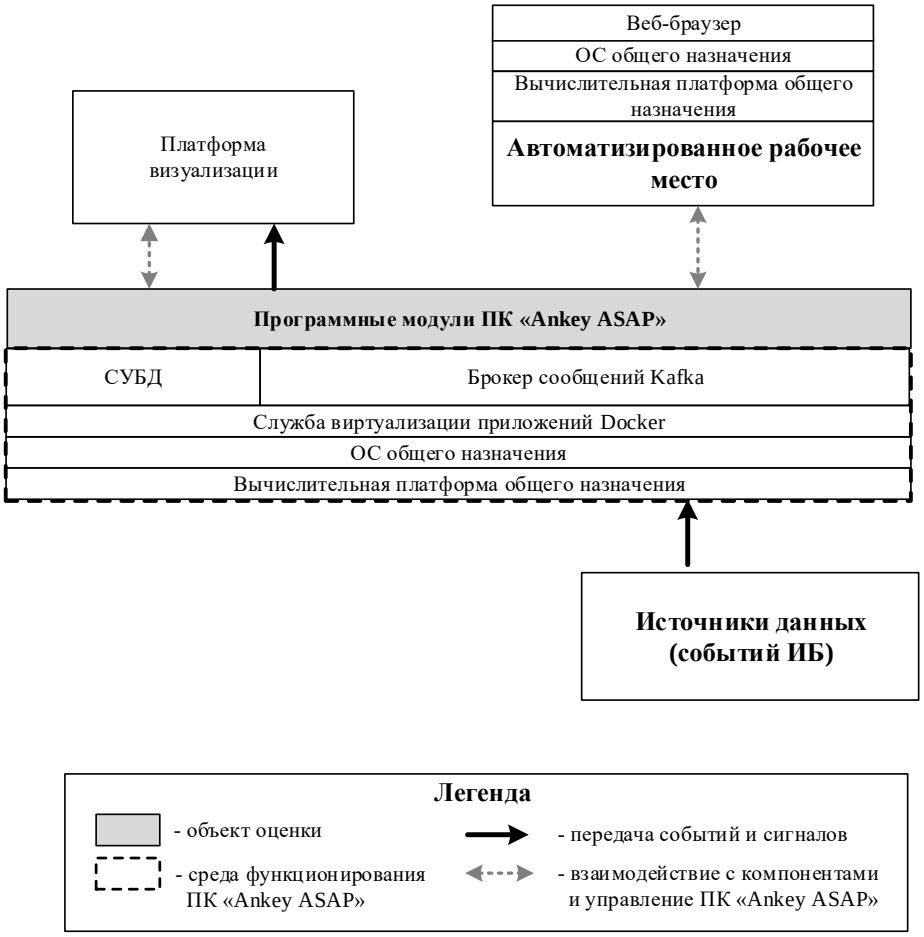


Рисунок 1.1 – Схема взаимодействия ПК «Ankey ASAP» с внешними компонентами

Программные компоненты комплекса функционируют на базе одной из следующих операционных систем (ОС):

– Astra Linux Special Edition 1.7.1 и выше;

– РЕД ОС 7.2 и выше.

Программные модули ПК «Ankey ASAP» обеспечивают выполнение следующих функций:

1. Аутентификация и авторизация пользователей ПК.

2. Администрирование учетных записей пользователей ПК.

3. Получение от внешних систем и обработку следующих категорий данных:

– нормализованные события от системы сбора и управления событиями безопасности Ankey SIEM в формате Common Event Format (CEF);

– инциденты безопасности, регистрируемые в системе сбора и управления событиями безопасности Ankey SIEM;

– активы сетевой модели Ankey SIEM (активы IT-инфраструктуры предприятия);

– события и инциденты безопасности, регистрируемые в системе сбора и управления событиями безопасности Ankey SIEM NG;

– активы сетевой модели Ankey SIEM NG (активы IT-инфраструктуры предприятия);

– информацию об объектах каталога Active Directory (AD) ОС семейства Microsoft Windows.

4. Управление параметрами сбора и обработки событий безопасности в формате CEF и JSON.

5. Настройку интеграции с системой сбора и управления событиями безопасности Ankey SIEM и Ankey SIEM NG с целью получения инцидентов безопасности.

6. Настройку интеграции с контроллерами домена Microsoft Windows посредством Lightweight Directory Access Protocol (LDAP) - для сбора данных о записях в каталогах Active Directory.

7. Формирование аналитических данных по событиям безопасности, получаемых от Ankey SIEM и Ankey SIEM NG.

8. Интеграцию с платформой визуализации для визуализации обработанных данных о событиях и инцидентах ИБ.

9. Передачу данных об инцидентах безопасности во внешнюю систему управления инцидентами.

10. Ведение журнала системных событий ПК, журнала запуска и остановки модулей ПК, журнала операций пользователей ПК.

11. Ведение справочной и конфигурационной информации в ПК.

СУБД ПК «Ankey ASAP» обеспечивают централизованное хранение категорий данных, обрабатываемых в ПК.

Доступ к данным предоставляется только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации.

В качестве системы хранения событий безопасности, полученных ПК «Ankey ASAP» используется защищенная СУБД «Jatoba».

1.3 Сведения о технических и программных средствах, обеспечивающих выполнение функций комплекса

ПК «Ankey ASAP» поставляется в виде ПО для установки на физическом или виртуальном сервере.

1.3.1 Требования к программному и аппаратному обеспечению

Требования к программному и аппаратному обеспечению при развертывании ПК «Ankey ASAP» описаны в таблице 1.1.

Таблица 1.1 – Требования к серверу ПК «Ankey ASAP»

Элемент	**Параметры**		
Тип инсталляции	Низконагруженная (до 3000 событий\сек)	Средненагруженная (до 10000 событий\сек)	Высоконагруженная (выше 10000 событий\сек)
Требования к программному обеспечению			
ОС	Astra Linux Special Edition 1.7.1 и выше, имеющая сертификат соответствия № 2557 (выдан ФСТЭК России выдан 27 января 2012 г., срок действия до 27 января 2026 г.) РЕД ОС 7.3, имеющая сертификат соответствия № 4060 (выдан ФСТЭК России выдан 12 января 2019 г., срок действия до 12 января 2024 г.)		
Поддерживаемые СУБД	Jatoba		
Требования к аппаратному обеспечению			
Процессор (с поддержкой HT и AVX)	От 16 до 24 ядер (от 2.4 GHz)	56 ядер (от 2.4 GHz)	Рассчитывается отдельно
Оперативная память, Гбайт	128	512	
Жесткий диск, Тбайт	Не менее 9 (SSD) RAID 6 + 1 Hot Spare	Не менее 16 (SSD) RAID 6 + 1 Hot Spare	
Дисковая подсистема для ОС, Гбайт	Не менее 480, RAID 1	Не менее 480, RAID 1	Не менее 480, RAID 1
Устройства ввода вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB-интерфейсами	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB-интерфейсами	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB-интерфейсами
Адаптер Ethernet	от 1 Гбит/с	от 10 Гбит/с	от 10 Гбит/с

Требования к ПО автоматизированного рабочего места (АРМ) управления представлены в таблице 1.2. Рекомендуемое разрешение экрана монитора АРМ: 1920 x 1080.

Таблица 1.2 – Требования к программному обеспечению АРМ управления

Элемент	Параметр
Операционная система	Требования не предъявляются
Поддерживаемый браузер	Google Chrome 77, Яндекс.Браузер 19.10 и выше

Для эксплуатации и эффективного применения ПК «Ankey ASAP» необходимо использование на электронно-вычислительных машинах (ЭВМ) лицензионного системного ПО.

Инфраструктура объекта внедрения должна обеспечивать функционирование следующих сервисов:

1. DNS. Связь между компонентами комплекса осуществляется по доменным именам, в связи с этим, на серверах DNS должны быть произведены соответствующие настройки, сервера DNS должны функционировать в штатном режиме.

2. Активное сетевое оборудование (АСО). Обмен данными между компонентами комплекса, а также сбор событий ИБ с подключенных источников, происходит по имеющейся сети передачи данных. Сервер ПК «Ankey ASAP и подключаемые источники должны быть доступны по сети.

3. Межсетевые экраны (МЭ). Обмен данными между компонентами ПК «Ankey ASAP», а также сбор событий ИБ с подключенных источников, происходит по имеющейся сети передачи данных. На МЭ, находящихся между ПК «Ankey ASAP» и источниками событий ИБ должны быть настроены разрешающие правила, МЭ должны функционировать в штатном режиме.

Настройка безопасности среды функционирования (ОС Astra Linux) компонентов ПК «Ankey ASAP» осуществляется автоматически в процессе установки компонентов.

2 Установка и удаление ПК «Ankey ASAP»

2.1 Необходимые действия перед началом установки ПО

Все команды по установке и удалению выполняются от пользователя с правами администратора.

На сервере должна быть предустановлена ОС специального назначения Astra Linux Special Edition 1.7 (1.7.1 и выше) или РЕД ОС 7.2 (и выше).

Рекомендуемые настройки при установке ОС Astra Linux приведены на рисунках 2.1 – 2.4.

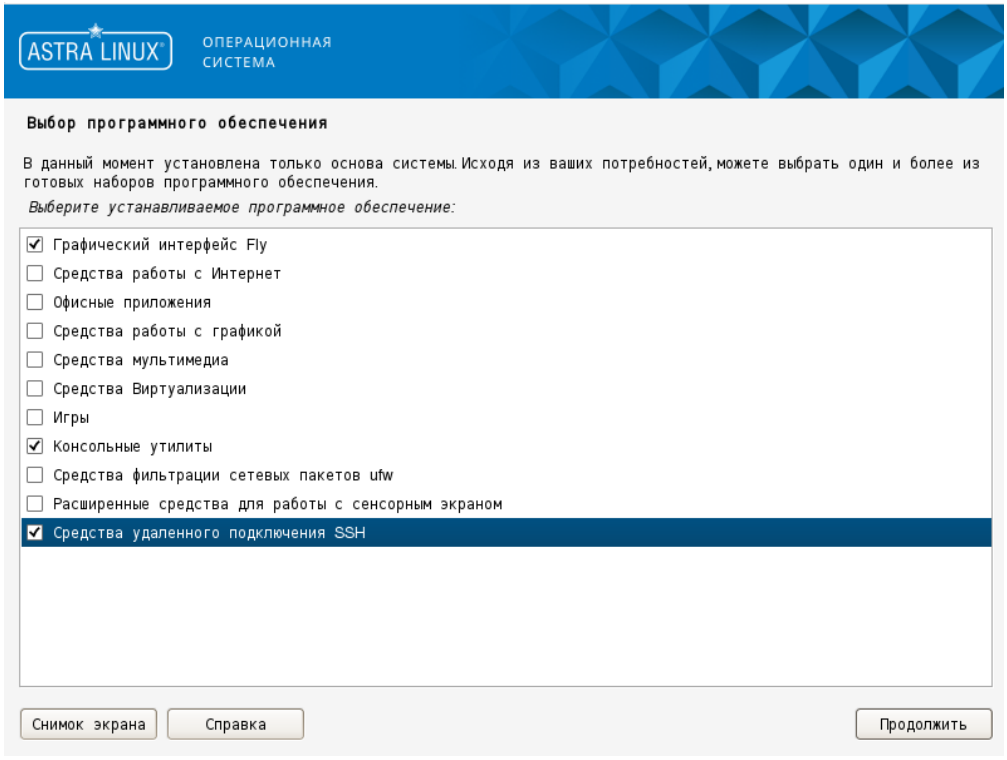


Рисунок 2.1 – Рекомендуемые компоненты для установки Astra Linux

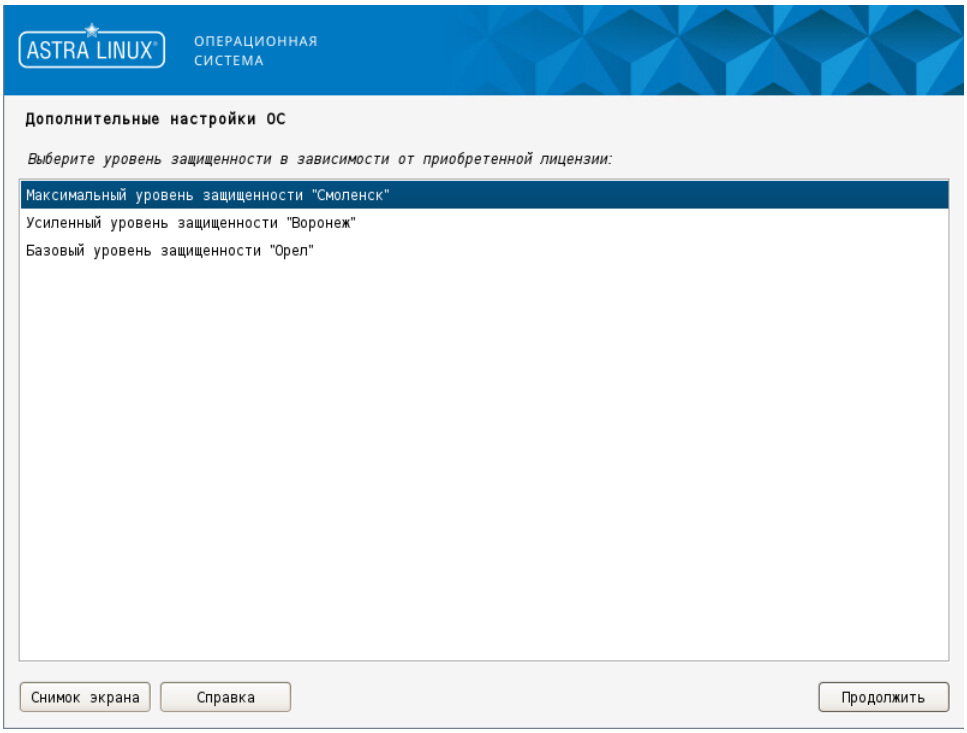


Рисунок 2.2 – Выбор уровня защищенности ОС

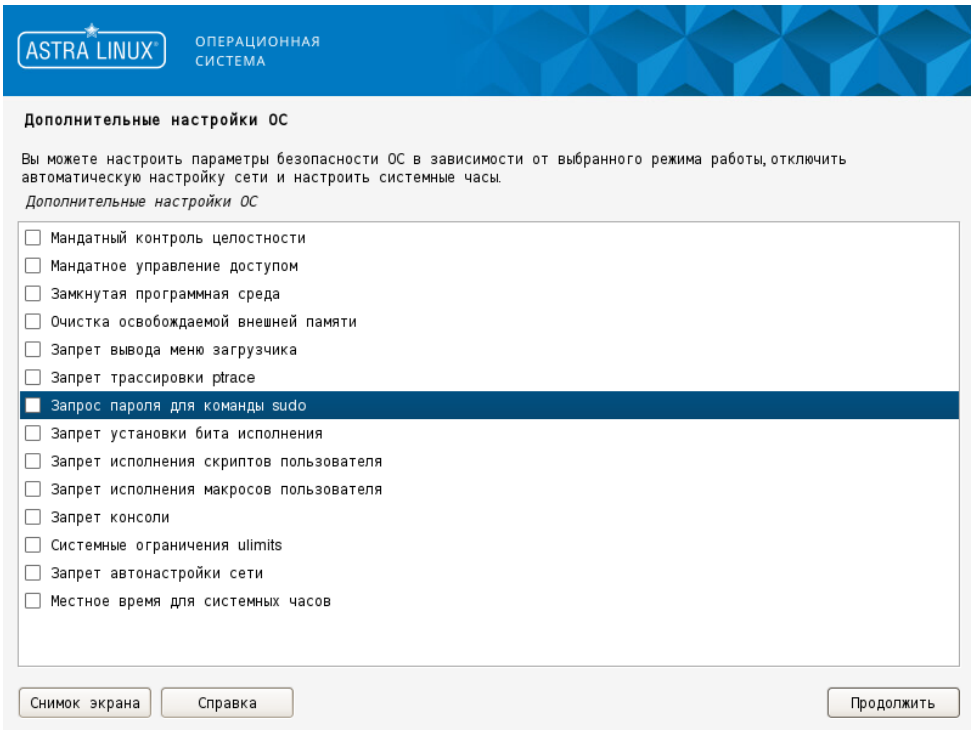


Рисунок 2.3 – Параметры безопасности ОС

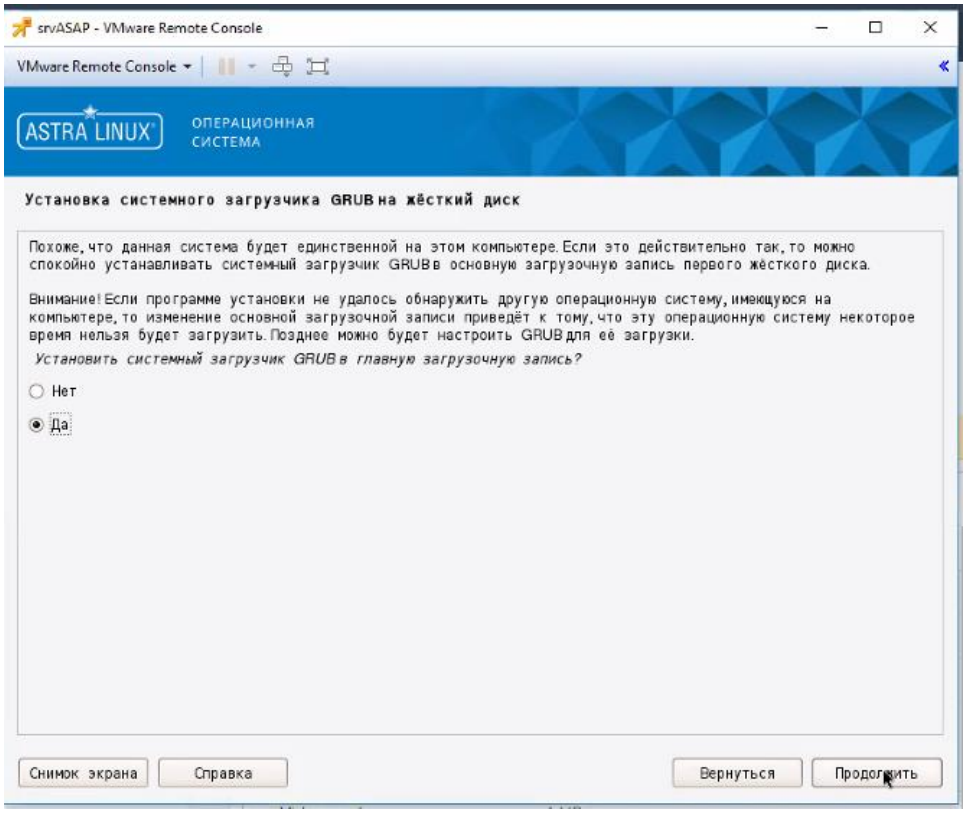


Рисунок 2.4 – Установка системного загрузчика

2.1.2 Рекомендации по организации файловой системы

Перед установкой ПК «Ankey ASAP» рекомендуется произвести организацию файловой системы (ФС) в соответствии с таблицей 2.1.

Таблица 2.1 – Рекомендации по организации файловой системы

Физический уровень	Точка монтирования ФС	Тип ФС	Рекомендованный размер, Гбайт	Примечание
Physical Volume 1 (Primary)	/boot	ext2	1	первичный (загрузочный)
	/	ext4	не менее 231	первичный
	–	swap	8	первичный, раздел подкачки
Physical Volume 2	/mnt/asap	ext4	1/3 от доступного объема	первичный
	/mnt/asap/mongo	ext4	1/3 от доступного объема	Первичный. Использовать SSD-диск под раздел
	/mnt/asap/jatoba	ext4	1/3 от доступного объема	первичный

Примечания:

1. Под раздел «/mnt/asap/mongo» рекомендуется использовать SSD- диск.

2. Разделы mnt/asap, /mnt/asap/mongo и /mnt/asap/jatoba предназначены для хранения данных. Рекомендуется выделять под них достаточное количество ресурсов в соответствии с требованиями к аппаратному обеспечению.

2.1.3 Настройка СУБД Jatoba

2.1.3.1 Действия перед началом установки

Перед установкой СУБД Jatoba выполнить следующие действия из командной строки с правами администратора:

1. Создать в каталоге /mnt/asap папку «jatoba»:

mkdir –p /mnt/asap/jatoba

2. Перейти в каталог /var/lib:

cd /var/lib

3. Создать ссылку на каталог /mnt/asap/jatoba:

ln –s /mnt/asap/jatoba /var/lib/jatoba

Установку СУБД Jatoba производить из каталога /mnt/asap/jatoba в соответствии с документацией на СУБД Jatoba. Помимо обязательных пакетов для установки, необходимо установить дополнительный пакет «jatoba4 pg-task».

2.1.3.2 Инициализация базы данных

После установки СУБД Jatoba выполнить инициализацию базы данных, для чего выполнить следующие действия в командной строке с правами администратора:

1. Установить пароль пользователю «postgres», по умолчанию у этого пользователя пароль пустой:

passwd postgres

2. Под данным пользователем создать директорий для хранения базы, если он отсутствует, и выполнить ее инициализацию:

su -l postgres

mkdir /var/lib/jatoba/4/data

cd /usr/jatoba-4/bin

./initdb -D /var/lib/jatoba/4/data --locale=ru_RU.UTF-8

3. Убедиться, что установлена кодировка UTF-8, выполнив команды.

su - postgres

psql

\l

4. Если необходимо пересоздать базу, то прежде ее необходимо удалить:

*rm –rf /var/lib/jatoba/4/data/**

5. В случае кодировки, отличной от UTF-8, выполнить команды:

sudo -u postgres /usr/jatoba-4/bin/initdb -D /var/lib/jatoba/4/data --locale=ru_RU.UTF-8

sudo chown -R postgres:postgres /mnt/asap/jatoba

sudo ln -s -f /mnt/asap/jatoba /var/lib/jatoba/4/data

2.1.3.3 Активация лицензии

Активацию лицензии производить в соответствии с документацией на СУБД Jatoba.

2.1.3.4 Настройка конфигурационных файлов

Выполнить настройку конфигурационных файлов «postgresql.conf» и «pg_hba.conf», которые находятся в директории базы данных «var/lib/jatoba/4/data».

Для файла «*postgresql.conf*» выполнить следующие действия:

1. В разделе «CONNECTIONS AND AUTHENTICATION» установить доступ к использованию базы данных:

listen_addresses = ''*

2. В разделе «CLIENT CONNECTION DEFAULTS» для параметра «shared_preload_libraries» задать значение «*pg_task*»:

shared_preload_libraries = 'pg_task'

pg_task.json = '[{"data":"asap","user":"postgres", "schema":"public"}]'

3. Убедиться, что в разделе «LICENSER OPTIONS AND PARAMETERS» параметры имеют следующие значения:

lic_product_name = 'Jatoba'

lic_file_path = '/usr/jatoba-4/bin/jatoba.cer'

lic_server_addr = 'https://license.gaz-is.ru'

В файле «*pg_hba.conf*» настроить сетевое взаимодействие, добавив следующие строки в раздел *# IPv4 local connections:*

host all all 0.0.0.0/0 md5

Для вступления в силу изменений настроек конфигурационных файлов, перезапустить службу СУБД:

systemctl restart jatoba-4

2.1.3.5 Добавление в автозапуск службы Jatoba

Для загрузки СУБД Jatoba вместе с ОС, выполнить следующие команды:

systemctl start jatoba-4

systemctl enable jatoba-4

2.1.3.6 Создание пользователя и базы данных

Подключиться к СУБД Jatoba из командной строки с правами администратора:

su – postgres

psql

4. Создать пользователя ASAP:

create role asap encrypted password '<пароль>';

alter role asap superuser;

alter role asap login;

Для проверки создания пользователя использовать команду «*\du*».

5. Создать БД «asap»:

create database asap owner asap;

Для проверки создания БД использовать команду «*\l*».

2.1.3.7 Создание представления в БД

Для просмотра сессий на вовлеченных в инцидент устройствах, необходимо настроить создание представления в БД.

Примечания:

1. Данную настройку необходимо производить после того, как будут настроены и запущены все необходимые плагины, указанные в подразделе 2.6.

2. Таблица будет создана при условии наличия в системе типов событий, перечисленных в конфигурации плагина «Запись потока данных из брокера сообщений в базу данных» (datasaver).

Для создания представления необходимо выполнить следующие действия:

3. Выполнить SQL-скрипт, представленный в файле «*view_create*» из папки «*jatoba_add*», поставляемой вместе с дистрибутивом, выполнив команду:

psql -d asap -U postgres –f <путь к файлу>/view_create.sql

4. Убедиться в создании представления «*seance_vw1*», как показано на рисунке 2.5, для чего:

– подключиться к БД:

psql -d asap -U postgres

– выполнить команду для проверки:

\dv

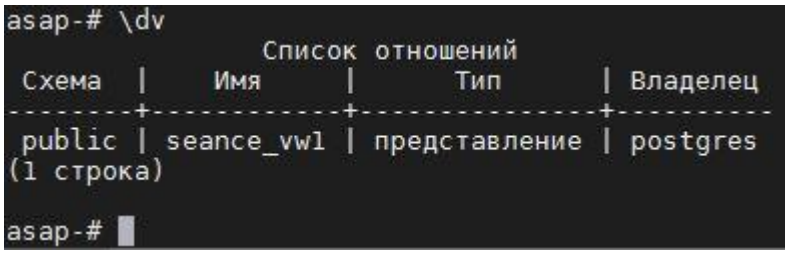


Рисунок 2.5 – Проверка создания представления

2.2 Настройка портов

Для правильного взаимодействия компонентов ПК «Ankey ASAP» необходимо настроить порты и протоколы, приведенные в таблице 2.2. В качестве источника данных для ПК «Ankey ASAP» могут выступать следующие системы:

– Ankey SIEM;

– Ankey SIEM NG;

– контроллер домена (MS Active Directory).

Таблица 2.2 – Перечень портов и протоколов для информационного взаимодействия ПК «Ankey ASAP»

Отправитель	Получатель	Протокол/Порт	Примечание
АРМ пользователя	ПК «Ankey ASAP»	TCP/80, 443, 22	Доступ к Веб и CLI консоли
ПК «Ankey ASAP»	Контроллер домена	TCP/389, 636	Взаимодействие с контроллером домена, получение данных от Active Directory
Система автоматизации процессов обеспечения безопасности (САОБ)	ПК «Ankey ASAP	TCP/443	Передача инцидентов безопасности
Взаимодействие с Ankey SIEM			

Отправитель	Получатель	Протокол/Порт	Примечание
ПК «Ankey ASAP»	Сервер корреляции Ankey SIEM	TCP/8443	Запрос на получение данных от Ankey SIEM (события, сетевая модель)
Сервер корреляции Ankey SIEM	Брокер сообщений ПК «Ankey ASAP»	TCP/9093	Получение данных от Ankey SIEM
ПК «Ankey ASAP»	Сервер сбора событий Ankey SIEM	UDP/514	Передача событий журнала аудита ПК «Ankey ASAP»
Взаимодействие с Ankey SIEM NG			
Сервер Ankey SIEM NG (Event Broker на компоненте Server)	ПК «Ankey ASAP»	TCP/6514	Получение событий и инцидентов ИБ от Ankey SIEM NG [1)]
Сервер Ankey SIEM NG (компонент Server)	ПК «Ankey ASAP»	TCP/5672	Получение событий и инцидентов ИБ от Ankey SIEM NG [2)]
ПК «Ankey ASAP»	Сервер Ankey SIEM NG (компонент Core)	TCP/3334	Выгрузка сетевой модели от Ankey SIEM NG
ПК «Ankey ASAP»	Сервер Ankey SIEM NG (компонент Agent)	UDP/514	Передача событий журнала аудита ПК «Ankey ASAP»
1) В случае передачи данных по syslog с использованием компонента Ankey SIEM NG Event Broker (для ПК «Ankey SIEM NG» v4 и выше) 2) В случае передачи данных через RabbitMQ (для ПК «Ankey SIEM NG» v3)			

2.3 Установка ПО

При установке и настройке ПО команды необходимо вводить от имени суперпользователя root, либо используя программу sudo.

2.3.1 Установка среды функционирования ПК «Ankey ASAP»

Для установки среды функционирования ПК «Ankey ASAP» подключить установочный диск со средой функционирования («asap-runtime_2.4.1»).

В случае установки с компакт-диска:

1. Из консоли выполнить переход на диск.
2. С правами администратора выполнить следующую команду для установки:

   sh install.sh

В случае установки с iso-образа:

1. Произвести монтирование iso-образа в директорию «/media/<любое имя, например iso1>», предварительно создав точку монтирования:

mkdir /media/iso1

mount <наименование образа>/media/iso1

2. Из консоли с правами администратора выполнить переход на диск:

cd /media/iso1

3. Выполнить следующую команду для установки:

sh install.sh

Примечания:

1. При установке может потребоваться установочный диск ОС для разрешения необходимых зависимостей.

2. Во избежание разрыва SSH-сессии во время установки, рекомендуется использовать утилиту «screen» во время установки.

2.3.2 Установка ПК «Ankey ASAP»

Для установки ПК «Ankey ASAP» необходимо подключить установочный диск ПК «Ankey ASAP» («asap_2.4.1»).

В случае установки с компакт-диска:

1. Из консоли выполнить переход на диск.

2. С правами администратора выполнить следующую команду для установки:

sh install.sh

В случае установки с iso-образа:

1. Монтирование iso-образа производить в директорию «/media/<любое имя, например iso2>» по аналогии с приведенным в пункте 2.3.1.

2. Из консоли с правами администратора выполнить переход на диск и выполнить следующую команду:

sh install.sh

При успешной установке на экране появляется сообщение «Successfully installed as /usr/bin/asap.», как показано на рисунке 2.6.

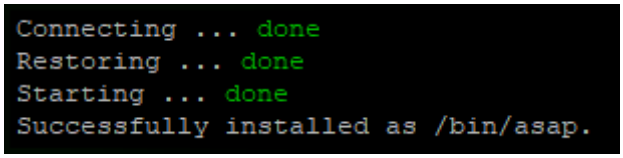


Рисунок 2.6 – Сообщения при успешной установке

При успешной установке на экране должно появиться сообщение «Successfully installed as /usr/bin/asap.».

3. Выполнить команду для проверки успешного запуска ПК «Ankey ASAP»:

asap status

При успешном запуске, выводом команды будет сообщение «asap is running».

Лог установки записывается в файл «install.log» по пути /opt/asap/.

Примечание. Во избежание разрыва SSH-сессии во время установки, рекомендуется использовать утилиту «screen» во время установки.

2.3.3 Установка плагинов ПК «Ankey ASAP»

Для установки плагинов ПК «Ankey ASAP» необходимо подключить установочный диск ПК «Ankey ASAP» («asap-plugins_2.4.1»).

В случае установки с компакт-диска:

1. Из консоли выполнить переход на диск.

2. С правами администратора выполнить следующую команду для установки:

sh install.sh

В случае установки с iso-образа:

1. Монтирование iso-образа производить в директорию «/media/<любое имя, например iso3>» по аналогии с приведенным в пункте 2.3.1.

2. Из консоли с правами администратора выполнить переход на диск и выполнить следующую команду:

sh install.sh

Примечание. Установку отдельных плагинов можно выполнить через веб-интерфейс в соответствии с 2.6.2.

2.3.4 Проверка работоспособности

ПК «Ankey ASAP» запускается автоматически. Для проверки работы ПК «Ankey ASAP» необходимо подключиться к комплексу посредством CLI-интерфейса под учетной записью (УЗ) пользователя ОС «root» и выполнить команду с правами администратора:

asap ps

При правильной работе в графе «*State*» должно быть указано значение «*Up*».

При запуске ПК «Ankey ASAP» службы запускаются автоматически. Для проверки состояния служб выполнить команду с правами администратора:

asap get pods

При штатной работе статус служб должен иметь значение «*Running*».

Для запуска ПК «Ankey ASAP» в ручном режиме необходимо выполнить команду с правами администратора:

asap up

2.4 Настройка ПО

2.4.1 Подключение к веб-интерфейсу ПК «Ankey ASAP»

Для доступа к веб-интерфейсу необходимо:

1. В адресной строке веб-браузера набрать адрес веб-интерфейса ПК «Ankey ASAP» вида «*https://<IP-address>*».

Примечание. Для доступа к веб-интерфейсу по доменному имени, необходимо выполнить настройки, приведенные в 2.4.3.4.

2. При возникновении предупреждения о ненадежности сертификата безопасности, необходимо продолжить открытие веб-сайта, после чего отобразится веб-интерфейс ПК «Ankey ASAP».

3. Ввести учетные данные:

– идентификатор пользователя – «*admin*»;

– пароль – «*admin*».

4. Установить новый пароль при первом входе в систему в открывшемся окне смены пароля.

Будет выполнена автоматическая проверка соответствия пароля заданной в ПК «Ankey ASAP» сложности пароля, по умолчанию пароль должен:

– быть не менее 6 символов;

– содержать хотя бы одну цифру;

– содержать хотя бы одну латинскую букву верхнего регистра;

– содержать хотя бы одну латинскую букву нижнего регистра;

– не совпадать с предыдущими тремя паролями пользователя.

5. После успешной смены пароля вновь открывается страница авторизации пользователя, где администратору необходимо выполнить вход с новым паролем.

Для продолжения работы с комплексом будет предложено выполнить активацию лицензии.

2.4.2 Активация лицензии

Для использования ПК «Ankey ASAP» необходима активация лицензии на право использования продукта.

После первой авторизации под учетной записью администратора появляется уведомление о том, что продукт не активирован (рисунок 2.7) и окно активации лицензии (рисунок 2.8).

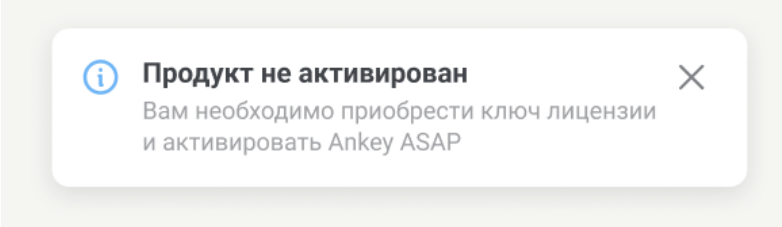


Рисунок 2.7 – Уведомление о необходимости активации лицензии

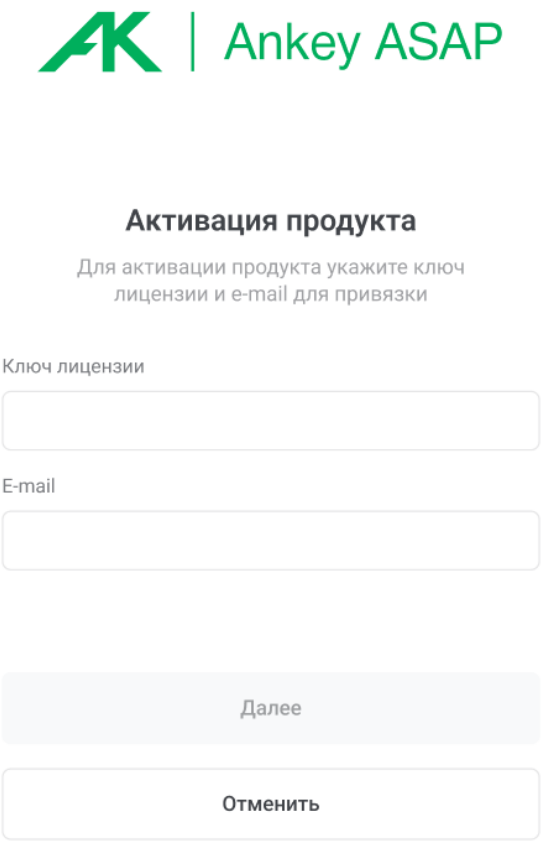


Рисунок 2.8 – Окно активации лицензии

Возможны два варианта произведения активации лицензии:

– онлайн-активация – при наличии подключения к серверу лицензирования;

– офлайн-активация – при отсутствии подключения к серверу лицензирования.

2.4.2.1 Онлайн-активация лицензии

Онлайн-активация комплекса осуществляется при наличии подключения к сети Интернет и возможности подключения к серверу лицензирования ООО «Газинформсервис».

Для активации лицензии выполнить следующие действия:

1. В окне активации лицензии ввести ключ лицензии, полученный при приобретении ПК «Ankey ASAP», и электронную почту для получения ключа активации (рисунок 2.9).

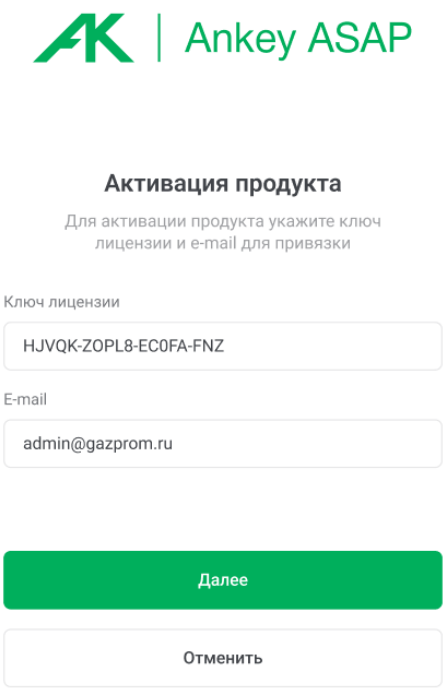


Рисунок 2.9 – Окно ввода ключа лицензии

2. В случае отсутствия сетевого соединения будет предложена офлайн-активация лицензии (2.4.2.2).

3. В открывшееся окно ввести ключ активации, полученный на указанный электронный адрес, и нажать кнопку «Активировать продукт» (рисунок 2.10).

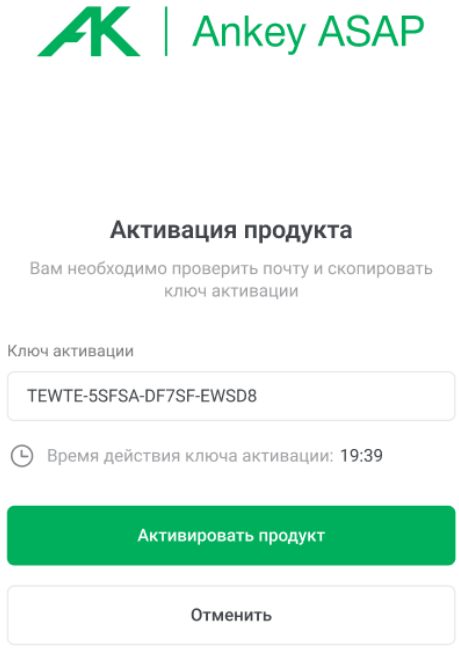


Рисунок 2.10 – Онлайн активация лицензии

4. При успешной активации на электронную почту придёт письмо с вложенным файлом лицензии и контактными данными для обращения в техническую поддержку.

2.4.2.2 Офлайн-активация лицензии

Офлайн-активация производится при отсутствии подключения к сети Интернет и серверу лицензирования ООО «Газинформсервис». Для офлайн-активации выполнить следующие действия:

5. В окне активации лицензии ввести ключ лицензии, полученный при приобретении ПК «Ankey ASAP» (см. рисунок 2.9) и email-адрес.

6. При невозможности подключения к серверу лицензирования будет выведено уведомление о его недоступности (рисунок 2.11).

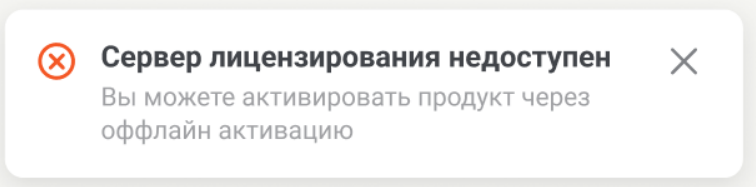


Рисунок 2.11 – Уведомление о недоступности сервера лицензирования

7. Скопировать запрос на активацию, нажав «скопировать» (рисунок 2.12), либо скачать файл с запросом.

Примечание. В случае, если файл лицензии уже был получен ранее, нажать кнопку «Далее» и перейти в пункту 9.

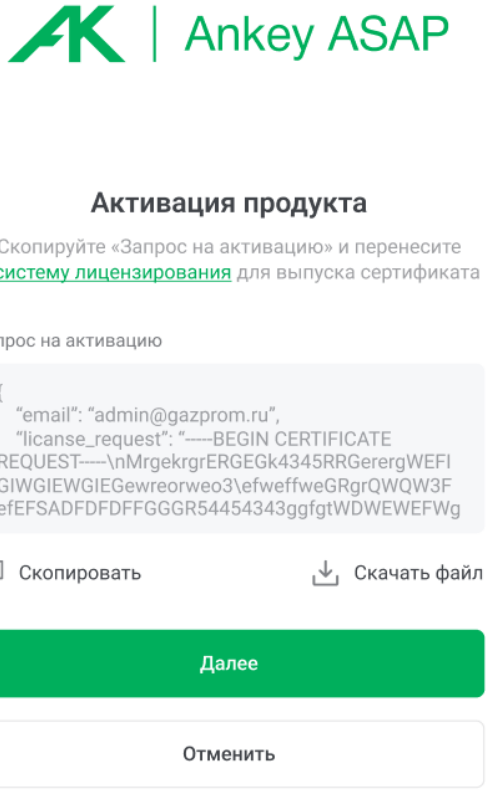


Рисунок 2.12 – Окно с инструкцией по офлайн активации

8. Следующие действия необходимо проводить с рабочей станции, имеющей доступ к сети Интернет:

– перейти на страницу офлайн-активации *https://license.gaz-is.ru/offlineActivate/;*

– ввести скопированный ранее запрос (рисунок 2.13);

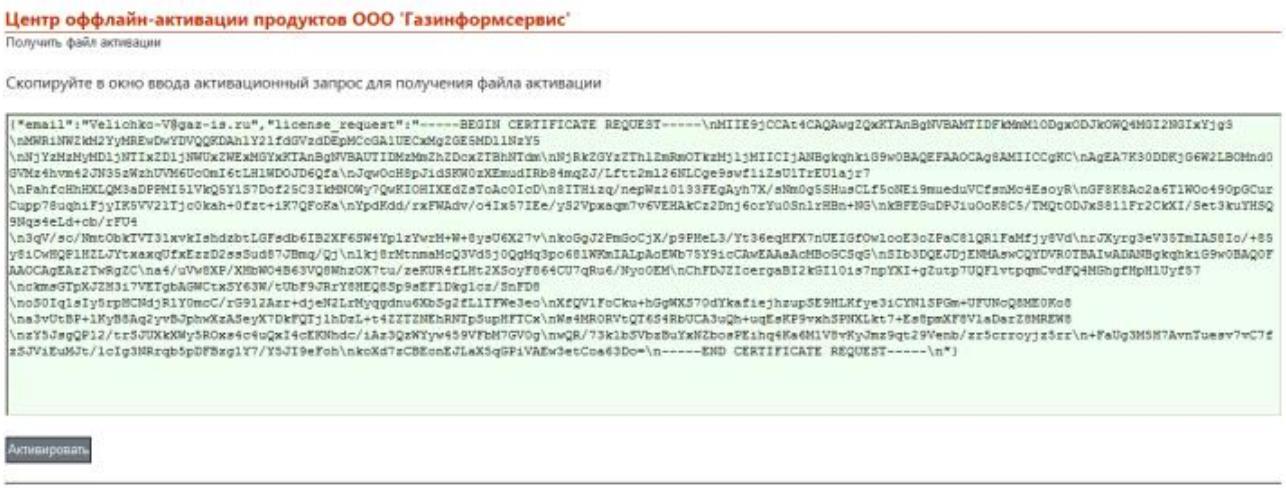


Рисунок 2.13 – Окно активации лицензии

– ввести в окно ключ активации, полученный на электронную почту, указанную в шаге 5 (рисунок 2.14) и нажать кнопку «Активировать»;

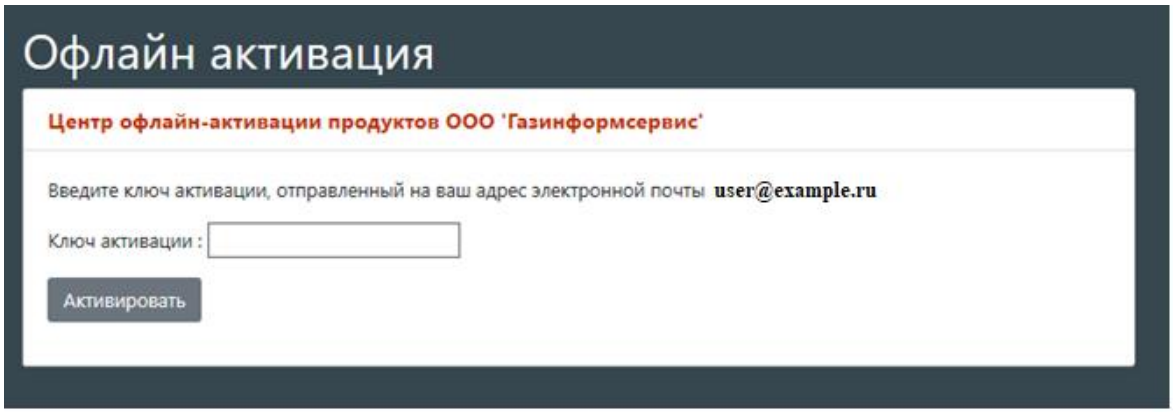


Рисунок 2.14 – Окно ввода ключа активации

– в случае успешного прохождения активации на электронную почту будет отправлено письмо с файлом лицензии и появится сообщение об успешной активации с кодом лицензии в браузере. Можно сохранить код лицензии, нажав на кнопку «Скопировать в буфер обмена» (рисунок 2.15);

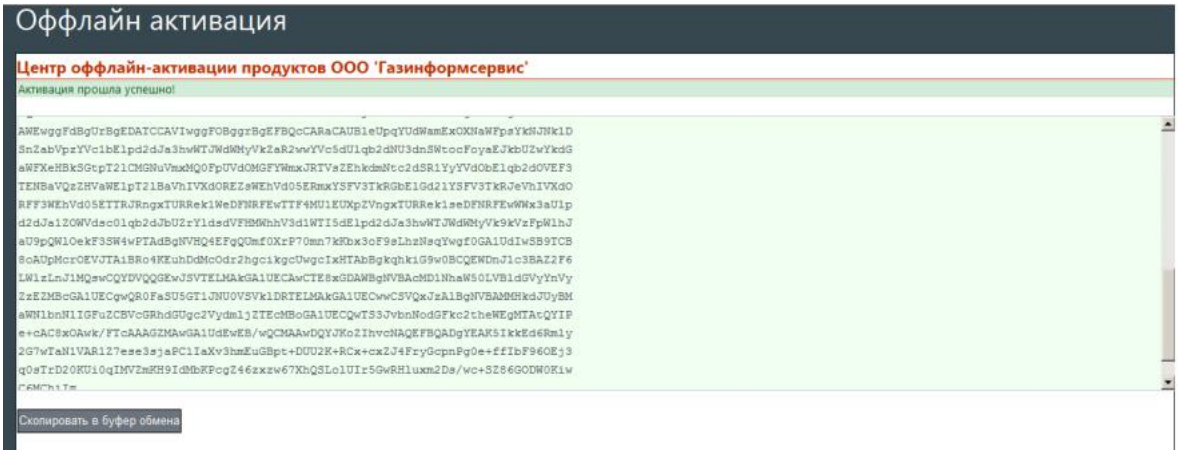


Рисунок 2.15 – Окно с файлом лицензии

9. Вставить полученный код файла лицензии в окно офлайн-активации (рисунок 2.16).

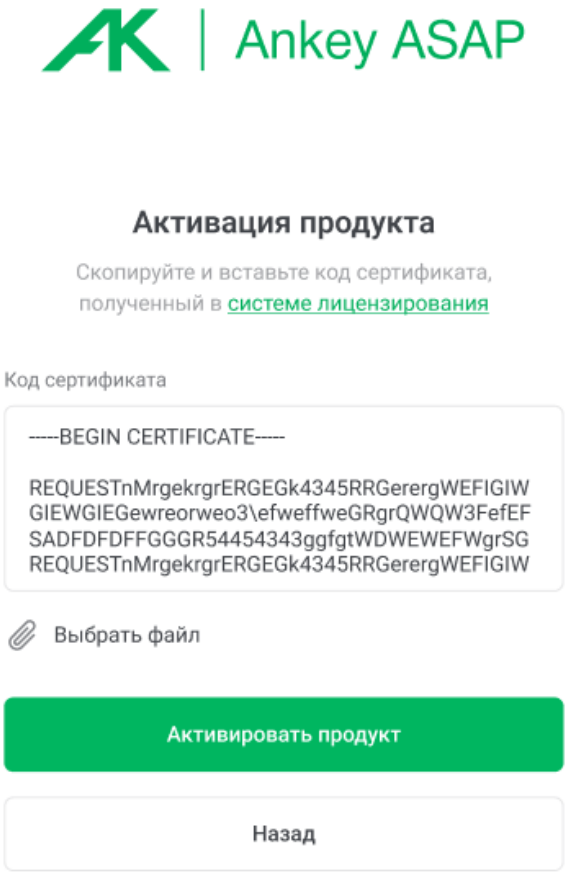


Рисунок 2.16 – Активация лицензии

10. Активировать продукт.

Информацию о лицензии и технической поддержке можно узнать на странице «Администрирование» → «Лицензирование».

2.4.2.3 Реактивация лицензии

При реактивации лицензии, лицензия с текущей инсталляции ПК «Ankey ASAP» переносится на вновь активируемую инсталляцию.

Для осуществлении переноса лицензии в онлайн-режиме, необходимо выполнить действия, указанные в подпункте 2.4.2.1. При этом необходимо вводить адрес электронной почты, используемый для ранее активированной лицензии.

Для осуществления офлайн-переноса лицензии после установки ПК «Ankey ASAP» на другой сервер, необходимо:

1. Выполнить действия 1 – 4 подпункта 2.4.2.2. При этом необходимо вводить адрес электронной почты, используемый для ранее активированной лицензии.

2. При получении на сервисе лицензирования сообщения о реактивации продукта, нажать кнопку «Активировать» (рисунок 2.17). Будет отправлено письмо с ключом активации на ранее введенный адрес электронной почты.

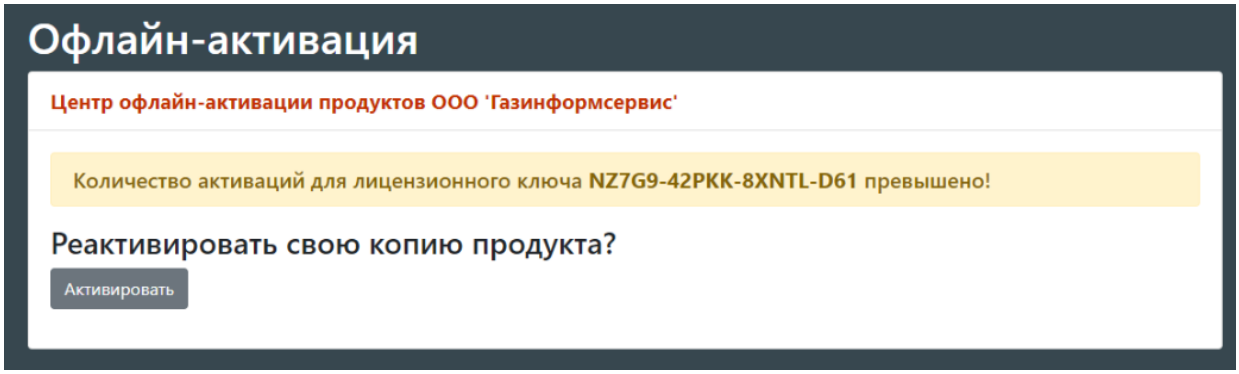


Рисунок 2.17 – Реактивация лицензии

3. Ввести полученный ключ активации в окно ввода и нажать кнопку «Активировать» (рисунок 2.18).

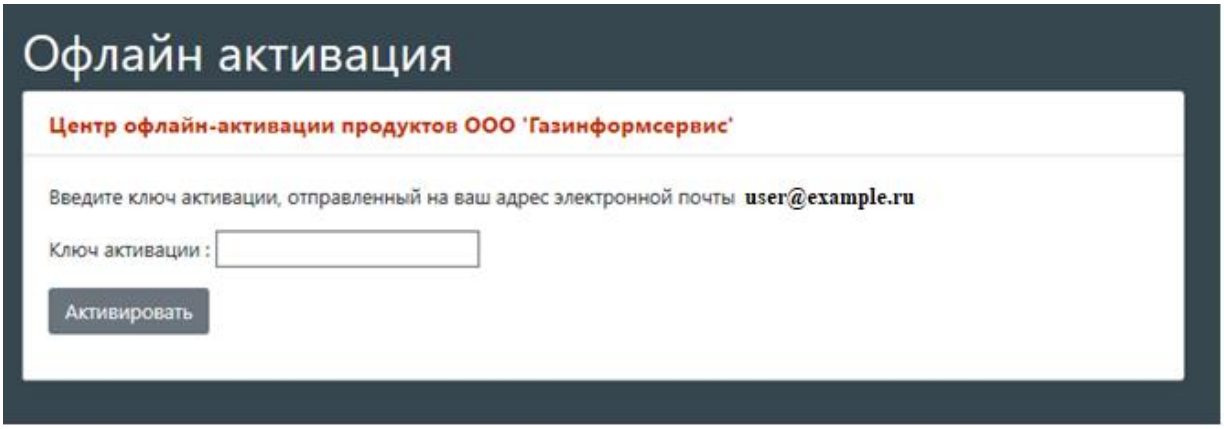


Рисунок 2.18 – Окно для ввода ключа активации

4. В случае успешного прохождения активации на электронную почту будет отправлено письмо с файлом лицензии и появится сообщение об успешной активации с кодом лицензии в браузере.

5. Вставить полученный код файла лицензии в окно офлайн-активации ПК «Ankey ASAP».

В случае, если данный ключ лицензии используется для активации на нескольких инсталляциях, то необходимо выбрать ту инсталляцию, с которой будет осуществлен перенос лицензии. Для этого необходимо будет предоставить код сертификата, который использовался для активации инсталляции, с которой осуществляется перенос, как показано на рисунке 2.19.

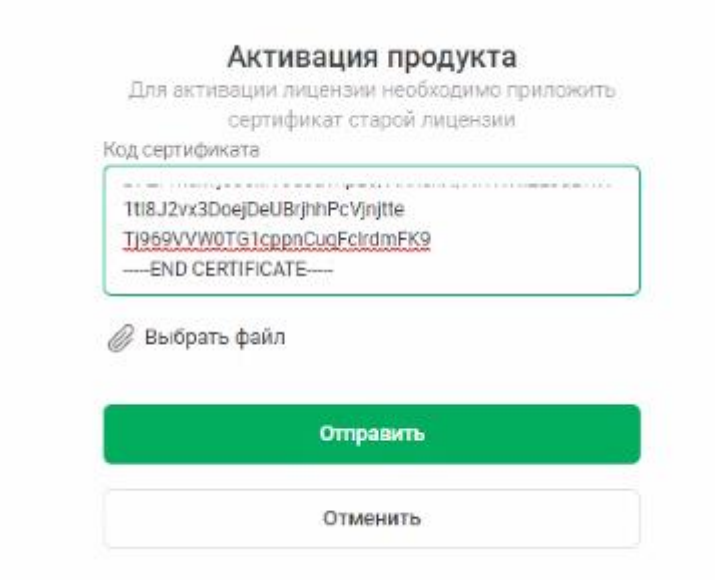


Рисунок 2.19 - Предоставление старого сертификата лицензии

2.4.3 Внесение изменений в настройки

2.4.3.1 Настройки для подключения к БД Jatoba

Для подключения к данным, хранящимся в БД Jatoba, выполнить следующие настройки:

1. В консоли перейти в директорию */opt/asap/manifests/services*.

2. Скопировать файл «backend.yaml» в домашний каталог.

3. Перейти в домашний каталог и открыть скопированный файл «backend.yaml» для изменения.

4. Добавить следующие переменные (env) в файл:

– name: PG_WORK_HOST

value: “<IP-адрес сервер Ankey ASAP>”

– name: PG_WORK_PORT

value: “5432”

– name: PG_WORK_DATABASE

value: “asap”

– name: PG_WORK_USERNAME

value: “asap”

– name: PG_WORK_PASSWORD

value: “<пароль, заданный для пользователя «asap»>”

5. Применить изменения командой

asap apply –f backend.yaml

asap restart backend

Примечание. В случае обновления ПК «Ankey ASAP» до новой версии, выполнить данные настройки еще раз.

2.4.3.2 Настройка времени хранения событий в БД

Примечание. Настройку времени хранения событий в БД производить после того, как будут настроены и запущены все необходимые плагины, указанные в подразделе 2.6.

Для настройки времени хранения событий в БД Jatoba (по умолчанию 30 дней), выполнить следующие действия под пользователем *posgtres*:

1. Скопировать файл «*functions.sql*» из папки «*jatoba_add*», поставляемой вместе с дистрибутивом, на сервер ПК «Ankey ASAP».

2. Применить sql-скрипт «*functions.sql*» и дождаться вывода четырех записей «CREAT FUNCTION»:

su -l postgres

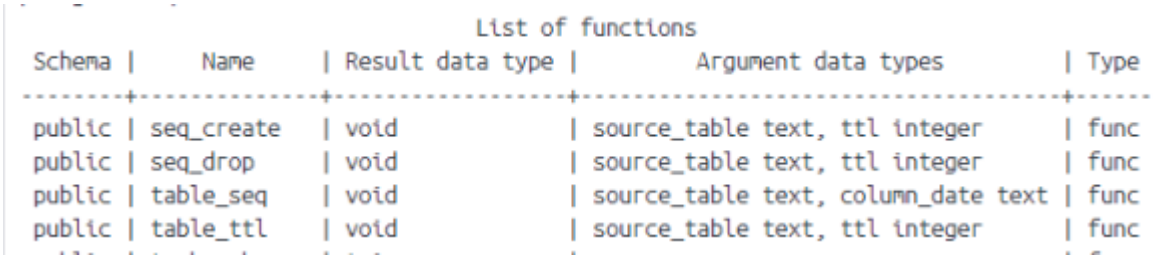
psql -d asap -U postgres -f <путь к файлу>/functions.sql

3. Перейти в БД:

psql -d asap -U asap

4. Проверить наличие функций (рисунок 2.20), выполнив команду:

\df



List of functions

Schema	Name	Result data type	Argument data types	Type
public	seq_create	void	source_table text, ttl integer	func
public	seq_drop	void	source_table text, ttl integer	func
public	table_seq	void	source_table text, column_date text	func
public	table_ttl	void	source_table text, ttl integer	func

Рисунок 2.20 – Список функций

5. Выполнить команду для секционирования таблицы с событиями:

select table_seq('uefa_events', ' "createdAt" ');

6. Удалить таблицу с данными, старше 30 дней, выполнив команду:

drop table uefa_events_old;

2.4.3.3 Изменение порта брокера сообщений

По умолчанию при установке имя хоста равно имени сервера, на котором установлен ПК «Ankey ASAP», порт брокера сообщений – «9093».

Для изменения порта брокера сообщений на доступный для внешних подключений к нему из Ankey SIEM (рисунок 2.21) выполнить команду с правами администратора:

asap configure

В настройке должен быть указан ip-адрес или доменное имя хоста и порт брокера сообщений.

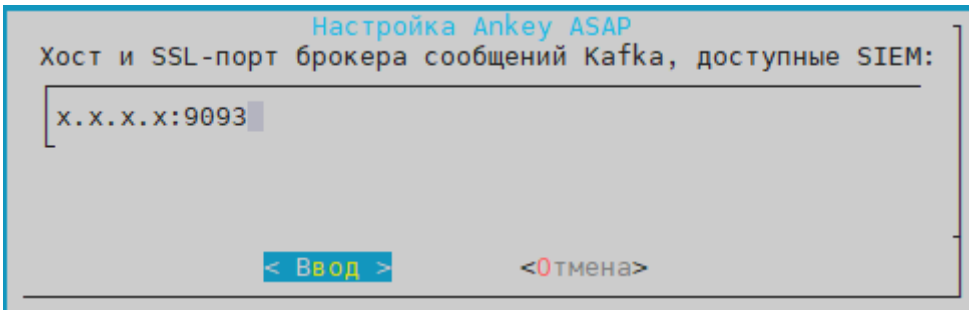


Рисунок 2.21 – Настройка адреса брокера сообщений Kafka

2.4.3.4 Настройка доступа по доменному имени

Для настройки доступа в веб-интерфейс ПК «Ankey ASAP» по доменному имени, необходимо выполнить следующие настройки:

1. Прописать соответствие доменного имени IP-адресу сервера в файле «hosts» на сервере.

2. Выполнить команду с правами администратора:

asap configure

3. Прописать соответствие доменного имени IP-адресу сервера в файле «hosts» на АРМ, откуда осуществляется доступ к веб-интерфейсу ПК «Ankey ASAP».

2.5 Интеграция с источниками данных

Для получения данных необходимо выполнить интеграцию с источниками данных для передачи данных в ПК «Ankey ASAP».

При проведении интеграции необходимо убедиться в том, что время и часовой пояс на сервере ПК «Ankey ASAP» и на сервере, с которым производится интеграция, установлены корректно.

2.5.1 Интеграция с Ankey SIEM

Интеграция с Ankey SIEM выполняется для получения событий и инцидентов безопасности, а также сетевой модели.

После выполнения настроек на стороне Ankey SIEM, приведенных ниже, необходимо настроить плагины, указанные в таблице 2.3 для получения данных, а также плагины, указанные в таблице 2.9 для обработки данных.

Таблица 2.3 – Плагины для получения данных из Ankey SIEM

Наименование	Пункт руководства
Получение объектов из сетевой модели Ankey SIEM	2.6.3.1

Передача данных в ПК «Ankey ASAP» может осуществляться следующими способами:

– через «Transformation Hub»;

– по syslog.

2.5.1.1 Настройка Ankey SIEM для передачи событий безопасности в ПК «Ankey ASAP» через «Transformation Hub»

Перед настройкой коннекторов Ankey SIEM необходимо выполнить перенос ключей шифрования на хост, где установлен коннектор, для чего:

1. С сервера, на котором установлен ПК «Ankey ASAP», скопировать ключи шифрования из директории *opt/asap/configs/kafka* (рисунок 2.22).

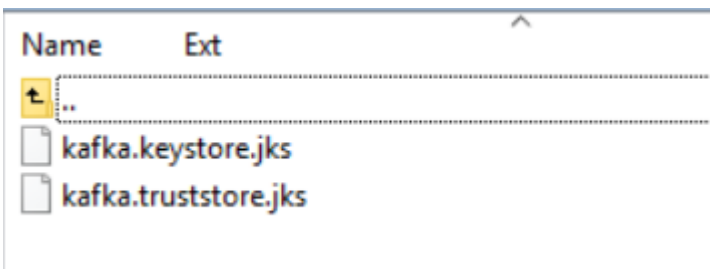


Рисунок 2.22 – Ключи шифрования

2. Учетной записи, под которой работает коннектор Ankey SIEM, выделить права на чтение скопированных файлов с ключами.

Для получения событий безопасности необходимо настроить передачу данных на коннекторах SIEM-системы. Для этого необходимо создать дополнительный адрес назначения на коннекторах Ankey SIEM:

3. Подключиться к веб-интерфейсу Ankey SIEM.

4. Перейти на «Коннекторы» («Управление узлами» → «Обзор всех узлов» → «Коннекторы») и выбрать необходимый коннектор с типом назначения «Kafka».

5. Добавить новое направление отправки событий «Destination».

6. Указать тип направления «Transformation Hub» или «Events Broker», в зависимости от версии коннектора.

7. Заполнить следующие поля для отправки в Ankey ASAP:

– адрес сервера ПК «Ankey ASAP»;

– порт брокера сообщений (по умолчанию – 9093);

– имя топика брокера сообщений: «events». Заданное имя топика используется при настройке конфигурации плагина «Предобработка событий и инцидентов» (2.6.3.7);

– параметры для определения версии SIEM-системы;

– включить шифрование (Use SSL/TLS: true);

– указать путь для скопированного файла с доверенным хранилищем (Trust Store) и название файла;

– указать пароль к нему (Qwerty7);

– включить аутентификацию (Use authentification SSL/TLS);

– указать путь для скопированного файла с ключевым хранилищем (Key Store) и название файла;

– дважды указать пароль (Qwerty7).

2.5.1.2 Настройка Ankey SIEM для передачи событий безопасности в ПК «Ankey ASAP» по syslog

При передаче событий по Syslog, необходимо указать следующие настройки для коннектора:

1. Подключиться к веб-интерфейсу Ankey SIEM.

2. Перейти на «Коннекторы» («Управление узлами» → «Обзор всех узлов» → «Коннекторы») и выбрать необходимый коннектор с типом назначения «Kafka».

3. Добавить новое направление отправки событий «Destination».

4. Указать тип направления «CEF Syslog».

5. Заполнить следующие поля для отправки в Ankey ASAP:

– адрес сервера ПК «Ankey ASAP»;

– порт ПК «Ankey ASAP» (по умолчанию – 6514);

– протокол: «Raw TCP».

Указание топика брокера сообщений и включение шифрования не требуется.

2.5.1.3 Настройка Ankey SIEM для передачи инцидентов безопасности в ПК «Ankey ASAP»

Посредством консоли сервера корреляции SIEM-системы необходимо выполнить следующие действия:

1. Перейти на вкладку «Ресурсы» → «Пользователи» и создать новую настраиваемую группу (Custom User Group) для учётных записей пользователей как показано на рисунке 2.23.

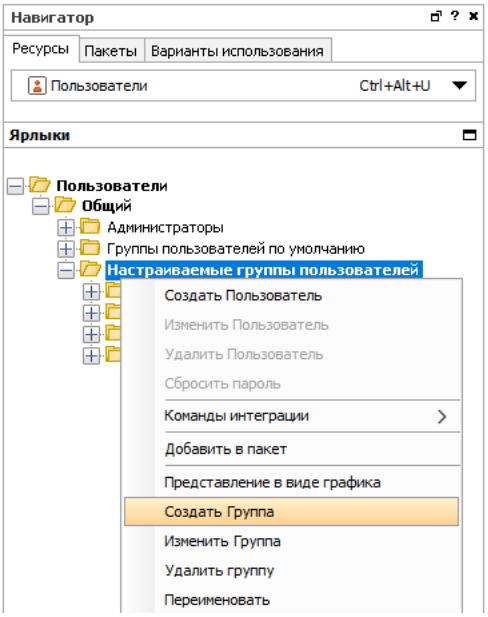


Рисунок 2.23 – Создание новой настраиваемой группы для учетных записей пользователей

2. В группе, созданной на шаге 1, создать новую учетную запись пользователя, как показано на рисунке 2.24.

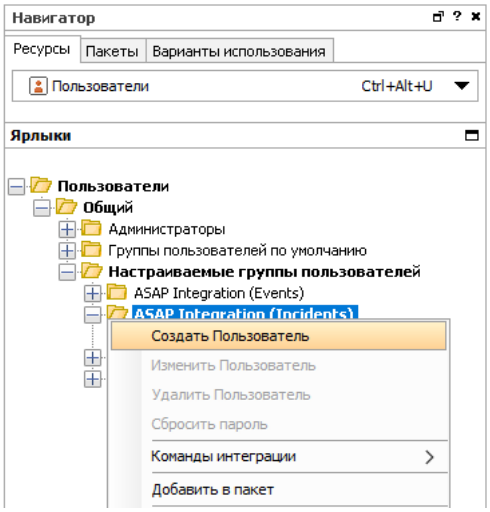


Рисунок 2.24 – Создание новой учетной записи пользователя

3. Сменить тип учетной записи пользователя (User Type), созданной на шаге 2, на «Коннектор выгрузки данных» (Forwarding Connector), как показано на рисунке 2.25.

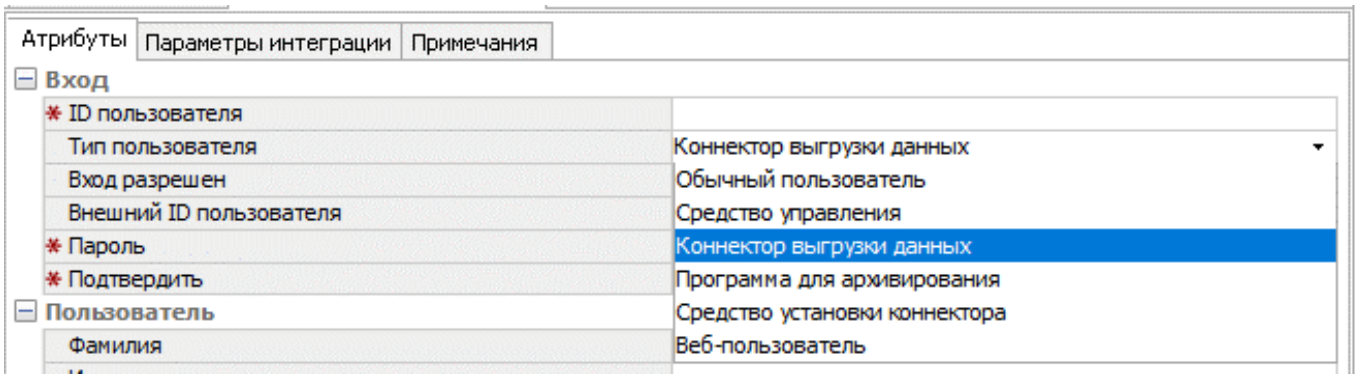


Рисунок 2.25 – Смена типа учетной записи пользователя

4. В ресурсе «Правило» (Rule), срабатывание которого соответствует детектированию инцидентов информационной безопасности, перейти на вкладку «Действия» (Actions). Выбрать триггер (Trigger), выполняемый при срабатывании действия, тип которого подходит конкретному ресурсу «Правило» (Rule) по смыслу и реализации. Открыть контекстное меню триггера и добавить новое действие, выбрав «Указать поле события» (Set Event Field) (рисунок 2.26). В открывшемся окне в поле события «Категория события устройства» (Device Event Category) записать любое опорное значение (например, «/Incident/Correlation»), как показано на рисунке 2.27.

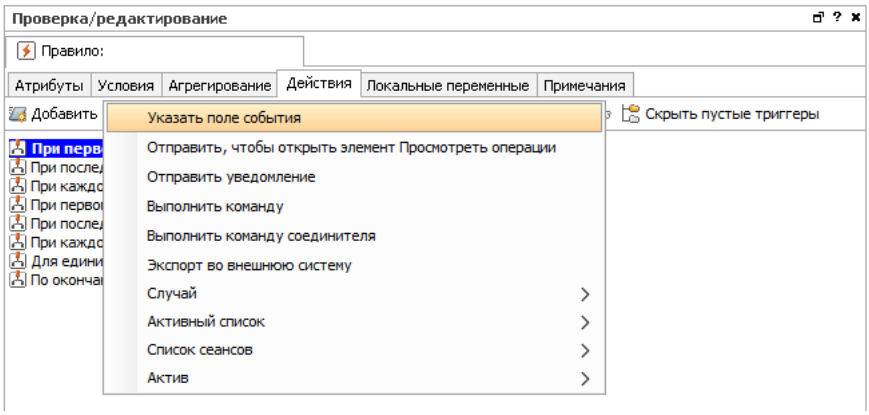


Рисунок 2.26 – Выбор типа действия для триггера при срабатывании правила

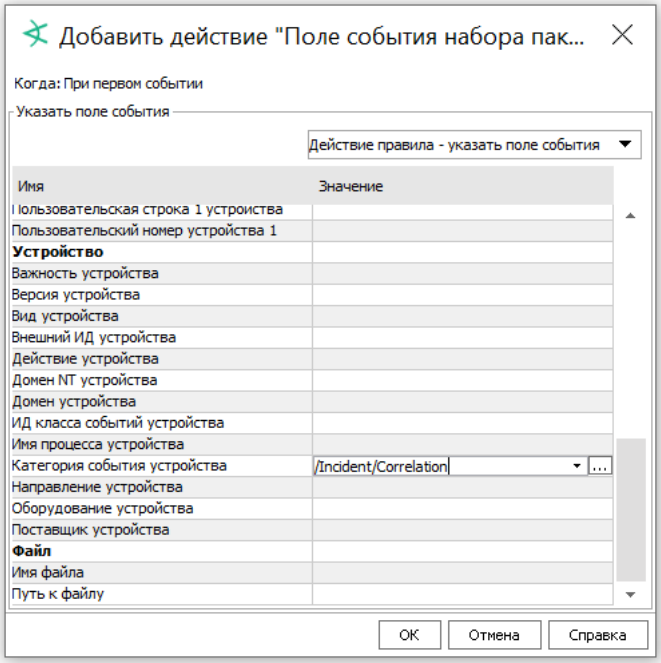


Рисунок 2.27 – Указание опорного значения в поле «Категория события устройства»

5. Убедиться, что триггеры (Trigger), выбранные на шаге 4, активны. Если какой-либо триггер (Trigger) отключен, его необходимо включить, нажав на кнопку «Включить триггер» (Activate Trigger), как показано на рисунке 2.28.

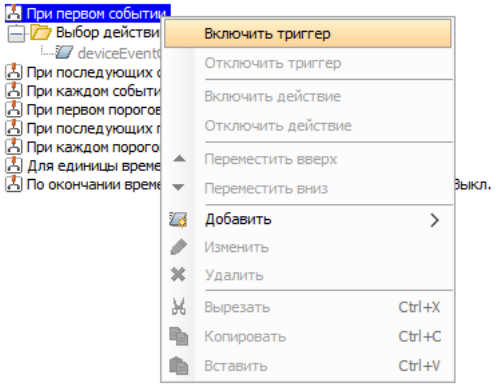


Рисунок 2.28 – Включение триггера

6. Создать ресурс «Фильтр» (Filter) для событий, соответствующих экспортируемым инцидентам ИБ. Рекомендуется построить фильтр на опорном значении, заданном на шаге 4 в поле «Категория события устройства» (Device Event Category), как показано на рисунке 2.29.

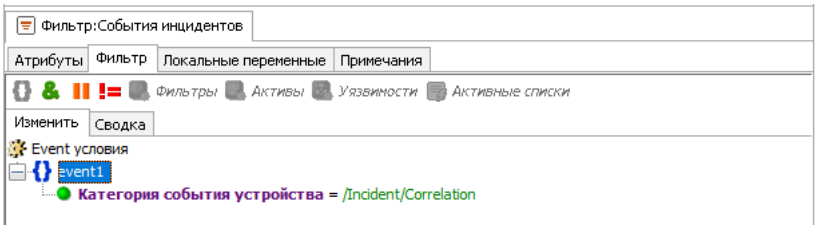


Рисунок 2.29 – Фильтр для экспорта инцидентов

7. В контекстном меню настраиваемой группы пользователей, созданной на шаге 1, выбрать «Изменить права доступа» (Edit Access Control), как показано на рисунке 2.30.

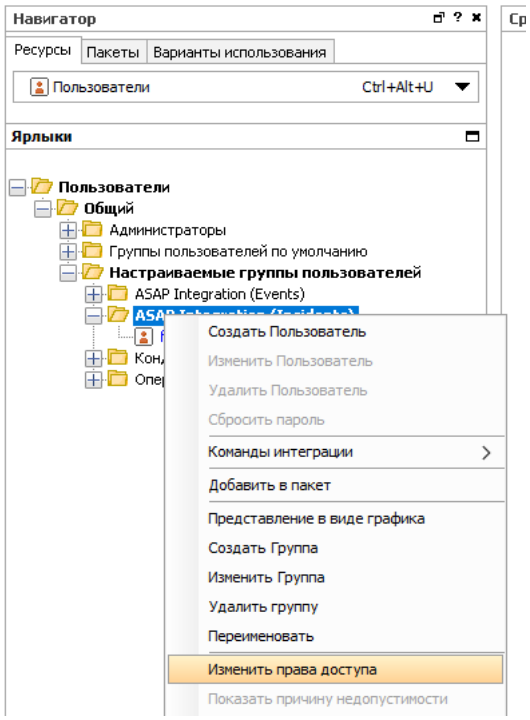


Рисунок 2.30 – Открытие формы изменения прав доступа группы

8. В открывшейся форме изменения прав доступа перейти на вкладку «События» (Events), нажать кнопку «Добавить» (Add) и в открывшемся списке фильтров выбрать фильтр, созданный на шаге 6, как показано на рисунках 2.31, 2.32.

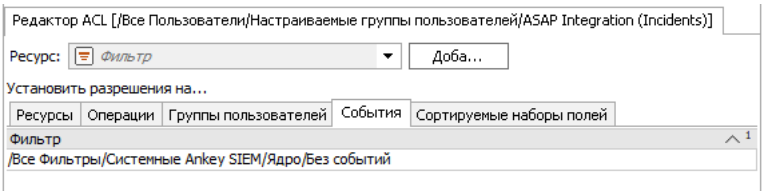


Рисунок 2.31 – Вкладка «События» формы изменения прав доступа

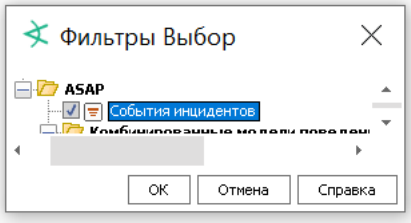


Рисунок 2.32 – Выбор фильтра для экспорта инцидентов

Затем настроить коннектор выгрузки данных в зависимости от выбранного способа:

– через «Transformation Hub», как описано в 2.5.1.3.1;

– по syslog, как описано в 2.5.1.3.2.

Для передачи в ПК «Ankey ASAP» событий, послуживших основанием для детектирования инцидента, выполнить следующие действия:

1. Добавить через редактор в файл конфигурации сервера корреляции SIEM-системы, располагающемуся по пути *«/config/server.properties»*, запись следующего формата:

«eventstream.cfc=<Connector ID>.<User ID>»,

где *<Connector ID>* – идентификатор коннектора выгрузки данных Ankey SIEM,

<User ID> – идентификатор учетной записи, созданной на шаге 2 при взаимодействии с консолью сервера корреляции SIEM-системы.

2. Перезагрузить сервер корреляции SIEM-системы, выполнив следующие команды:

«/etc/init.d/ankey_services stop all»

«/etc/init.d/ankey_services start all»

2.5.1.3.1 Настройка коннектора Ankey SIEM для передачи инцидентов безопасности в ПК «Ankey ASAP» через «Transformation Hub»

Посредством консоли ОС для инсталлированного коннектора выгрузки данных Ankey SIEM установить определенный перечень настроек, выполнив следующие действия:

1. Находясь в директории *«<директория установки>/current/bin/»* запустить скрипт «*runagentsetup.sh*»

2. Выбрать пункт «Add a Connector» введя «0», как показано на рисунке 2.33.

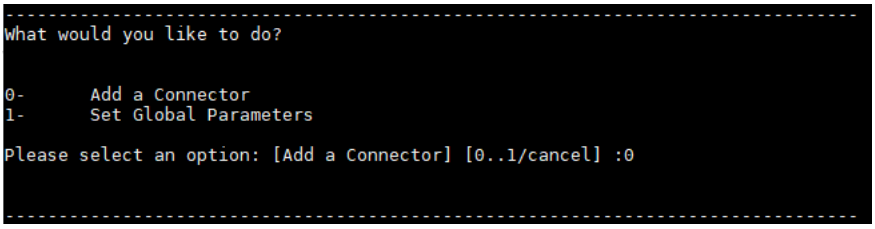


Рисунок 2.33 – Выбор пункта меню «runagentsetup.sh»

3. Выбрать тип «Forwarding Connector (Enhanced)» как показано на рисунке 2.34.

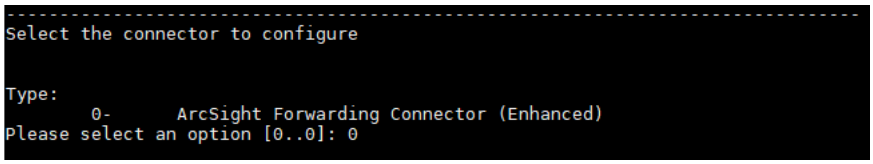


Рисунок 2.34 – Выбор типа конектора, для которого вносятся изменения

4. Менеджер настройки коннектора предложит скрыть вводимые параметры (пара логин-пароль) на следующем этапе настройки. Ввести значение «yes» если скрытие необходимо или «no» если оно не нужно, как показано на рисунке 2.35.

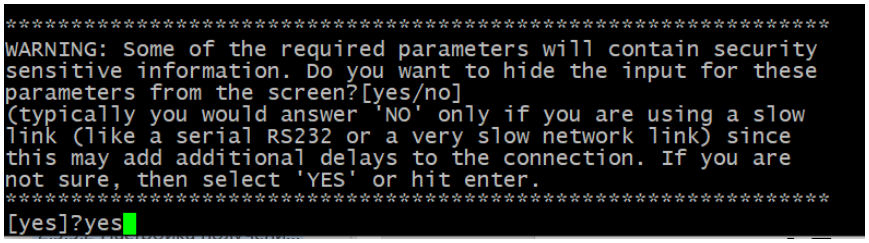


Рисунок 2.35 – Настройка скрытия вводимых данных при настройке коннектора выгрузки данных Ankey SIEM

5. Поочередно ввести следующие данные:

– FQDN устройства сервера корреляции SIEM-системы;

– открытый сетевой порт для взаимодействия с SIEM-системой;

– имя учетной записи, созданной на шаге 2, при взаимодействии с консолью сервера корреляции SIEM-системы (2.5.1.3);

– пароль учетной записи, созданной на шаге 2, при взаимодействии с консолью сервера корреляции SIEM-системы (2.5.1.3).

Подтвердить корректность параметров настройки, введя «yes», как показано на рисунке 2.36.

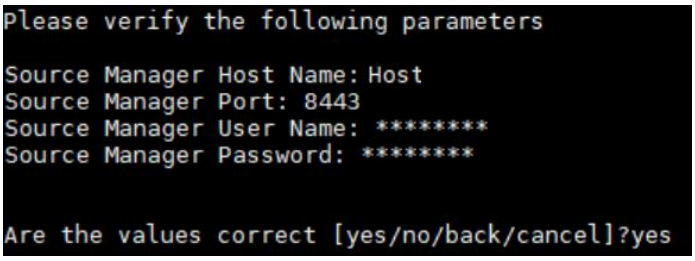


Рисунок 2.36 – Ввод параметров для идентификации сервера корреляции SIEM-системы в менеджере настройки коннектора выгрузки данных Ankey SIEM

6. Импортировать сертификат, если это необходимо, введя «0», как показано на рисунке 2.37.

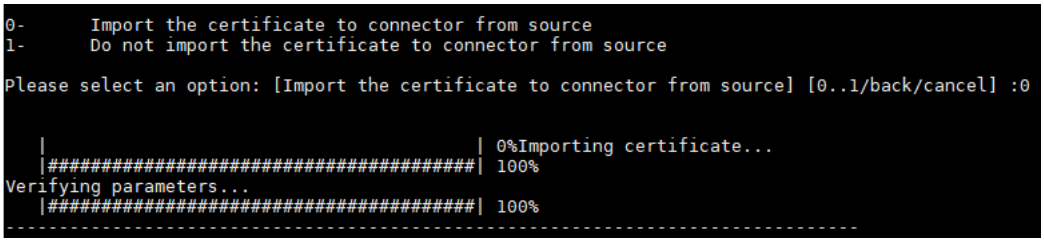


Рисунок 2.37 – Импорт сертификата в менеджере настройки коннектора выгрузки данных Ankey SIEM

7. Выбрать тип места назначения «Transformation Hub» для отправки событий, как показано на рисунке 2.38.

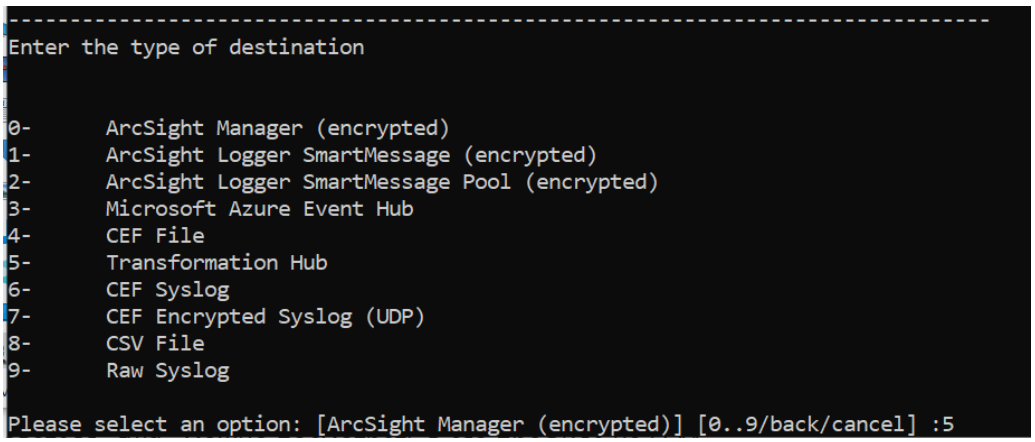


Рисунок 2.38 – Выбор типа места назначения в менеджере настройки коннектора выгрузки данных Ankey SIEM

8. Поочередно ввести следующие данные:

– FQDN сервера ПК «Ankey ASAP» и открытый сетевой порт брокера сообщений ПК «Ankey ASAP» в формате «<FQDN>:<сетевой порт>»;

Примечание. Сетевой порт, заданный командой «asap configure». По умолчанию: 9093;

– наименование топика для событий об инцидентах: «incident».

Примечание. Запомнить заданное имя топика, так как оно используется при настройке плагина «Предобработка событий и инцидентов» (2.6.3.7) в веб-интерфейсе ПК «Ankey ASAP»;

– параметры для определения версии SIEM-системы;

– включить шифрование (Use SSL/TLS: true);

– указать путь для скопированного файла с доверенным хранилищем (Trust Store) и название файла;

– указать пароль к нему (Qwerty7);

– включить аутентификацию (Use authentification SSL/TLS);

– указать путь для скопированного файла с ключевым хранилищем (Key Store) и название файла;

– дважды указать пароль (Qwerty7).

Подтвердить корректность параметров настройки, введя «yes», как показано на рисунке 2.39.

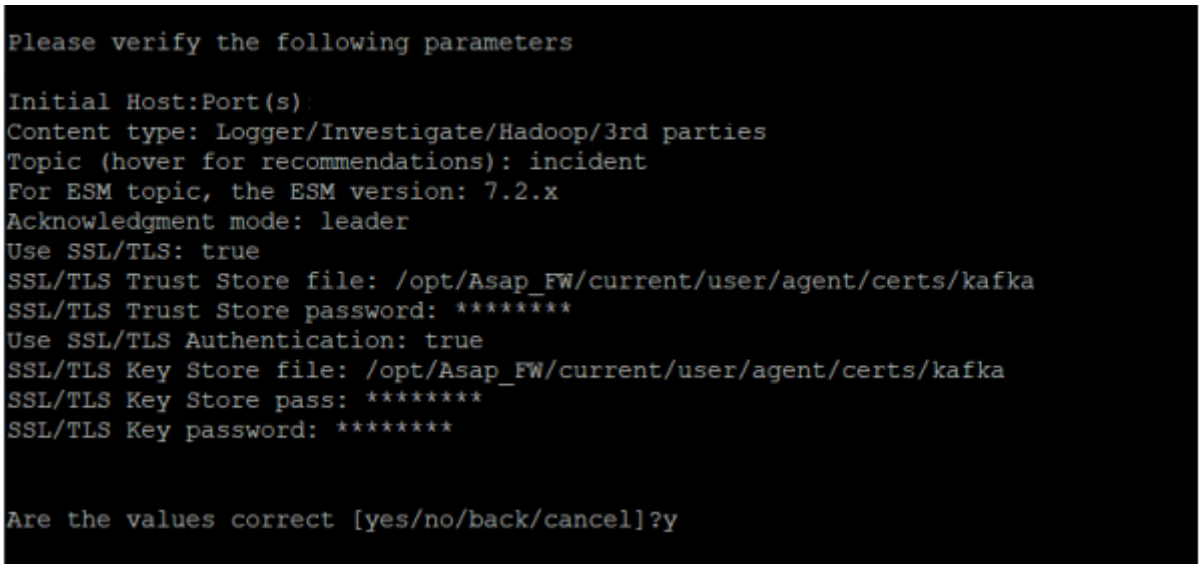


Рисунок 2.39 – Ввод параметров создаваемого места назначения в менеджере настройки коннектора выгрузки данных Ankey SIEM

9. Убедиться в сохранении всех заданных настроек в менеджере настройки коннектора выгрузки данных Ankey SIEM и завершить процесс.

2.5.1.3.2 Настройка коннектора Ankey SIEM для передачи инцидентов безопасности в ПК «Ankey ASAP» по syslog

Для настройки коннектора Ankey SIEM для передачи инцидентов по syslog выполнить следующие действия:

1. Выполнить действия 1 - 6 подпункта 2.5.1.3.1.

2. Выбрать тип места назначения «CEF Syslog» для отправки событий, как показано на рисунке 2.30.

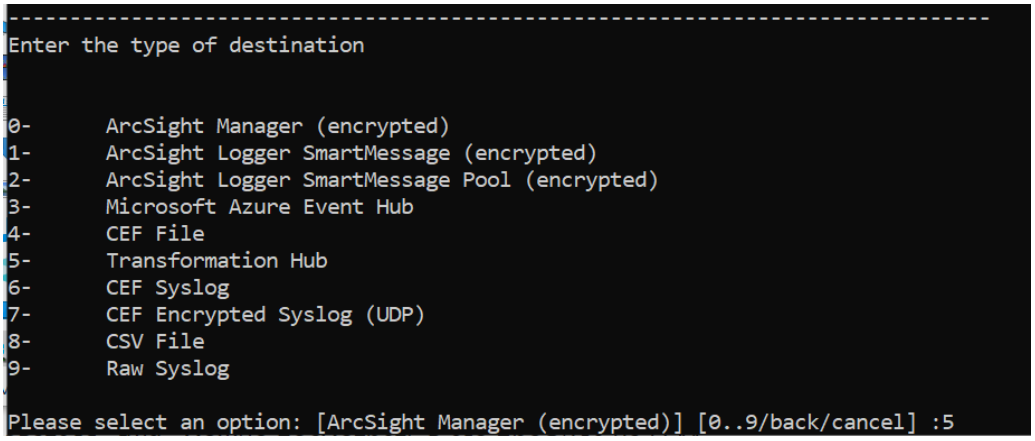


Рисунок 2.40 – Выбор типа места назначения в менеджере настройки коннектора выгрузки данных Ankey SIEM

3. Поочередно ввести следующие данные:

– FQDN сервера ПК «Ankey ASAP» и сетевой порт ПК «Ankey ASAP» в формате «<FQDN>:<сетевой порт>»;

Примечание. Сетевой порт по умолчанию: 6514;

– параметры для определения версии SIEM-системы.

Убедиться в сохранении всех заданных настроек в менеджере настройки коннектора выгрузки данных Ankey SIEM и завершить процесс.

2.5.1.4 Настройка Ankey SIEM для создания пакета ресурсов сетевой модели

Посредством консоли сервера корреляции SIEM-системы необходимо выполнить следующие действия:

1. Создать новую учетную запись пользователя в настраиваемой группе пользователей («Custom User Group») (рисунок 2.41).

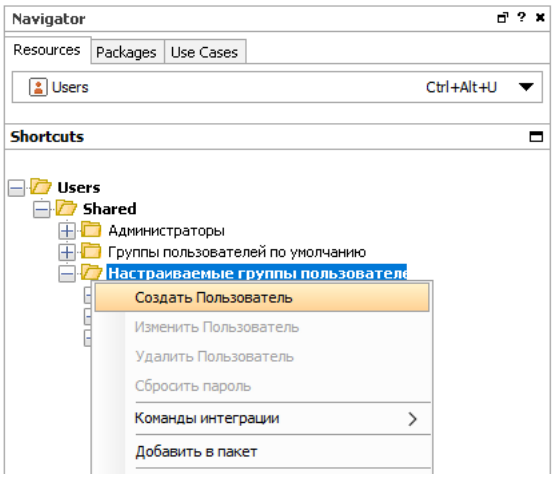


Рисунок 2.41 – Создание новой учетной записи пользователя в настраиваемой группе пользователей

2. Для созданной на шаге 1 учетной записи пользователя сменить ее тип («User Type») на «Веб-пользователя» («Web User») как показано на рисунке 2.42.

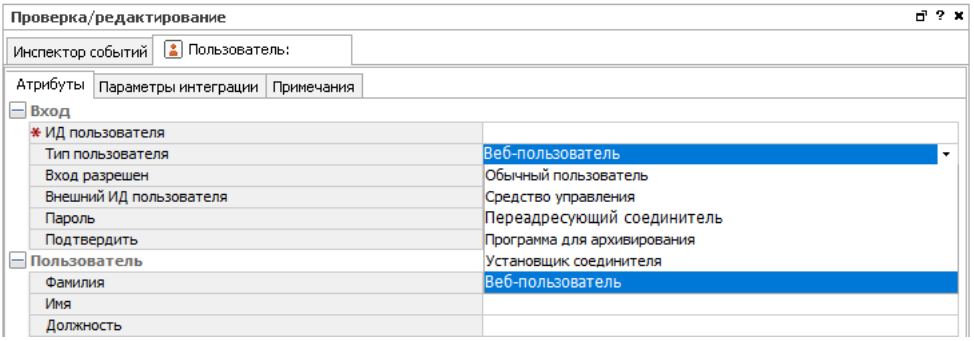


Рисунок 2.42 – Смена типа учетной записи пользователя на «Веб-пользователь» («Web User»)

3. Из ресурсов («Resources») SIEM-системы, информацию о которых необходимо передать в ПК «Ankey ASAP», сформировать пакет ресурсов («Package»), соответствующий сетевой модели. Для добавления ресурсов SIEM-системы в существующий пакет ресурсов, выбрать в контекстном меню пакета пункт «Изменить пакет», как показано на рисунке 2.43. Нажать на кнопку «Add» и выбрать добавляемые ресурсы (рисунок 2.44).

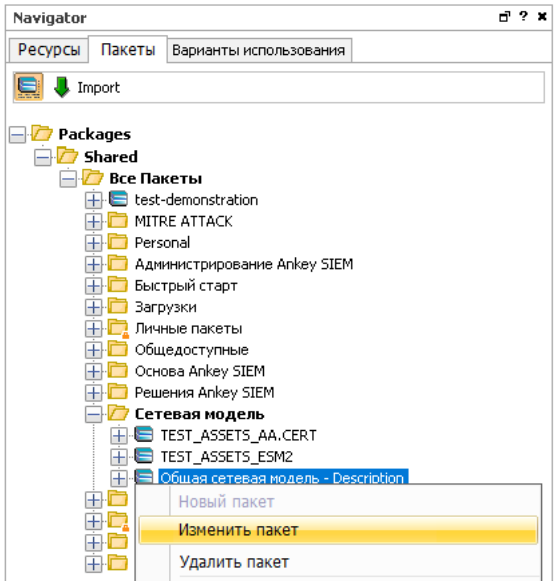


Рисунок 2.43 – Открытие инструмента для изменения пакета ресурсов SIEM-системы

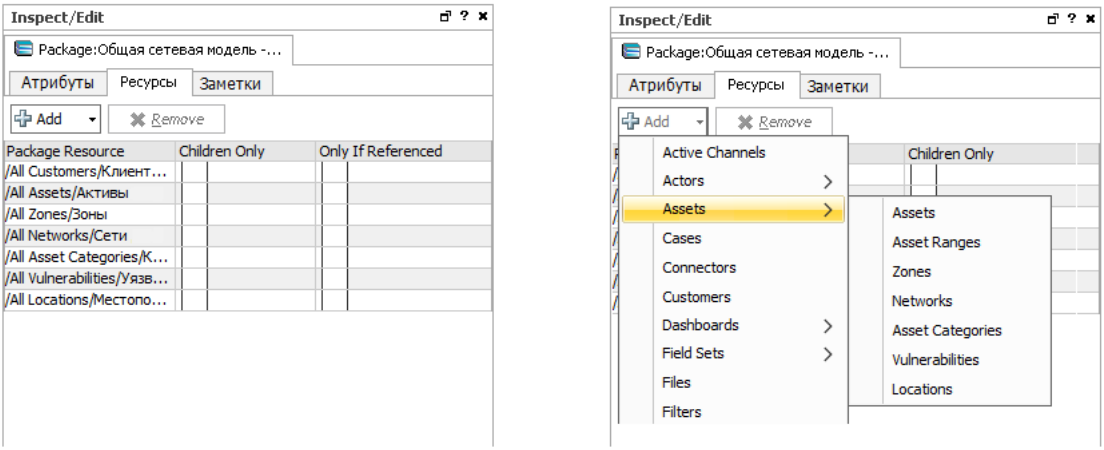


Рисунок 2.44 – Добавление ресурсов в пакет ресурсов SIEM-системы, используя редактирование пакета

Также добавление ресурсов в пакет возможно через дерево каталогов ресурсов. Для этого в контекстном меню требуемого ресурса необходимо выбрать пункт «Добавить в пакет» (Add to Package) и указать пакет, в который нужно добавить ресурс, как показано на рисунках 2.45 и 2.46.

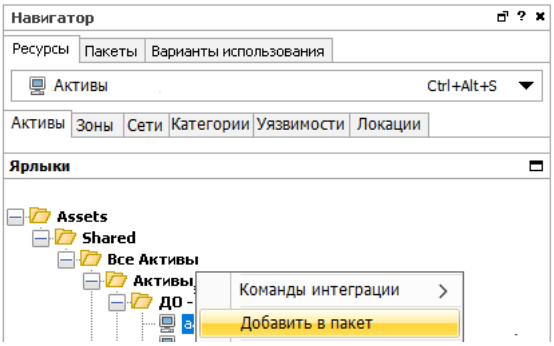


Рисунок 2.45 – Добавление ресурсов в пакет ресурсов SIEM-системы через дерево каталогов.

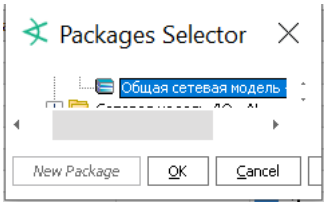


Рисунок 2.46 – Указание пакета, в который необходимо внести ресурс.

Выбрать следующие ресурсы для передачи в ПК «Ankey ASAP»:

– «Активы» (Asset's);

– «Сетевые зоны» (Zone);

– «Сети» (Networks);

– «Категории» (Categories или Asset's Categories);

– «Уязвимости» (Vulnerabilitie's);

– «Локации» или «Территории» (Location's);

– «Клиенты» (Customer's).

Наличие остальных типов ресурсов в пакете ресурсов не влияет на работу ПК «Ankey ASAP», они также могут быть добавлены в пакет ресурсов, соответствующий синхронизируемой сетевой модели.

4. Зафиксировать идентификатор пакета ресурсов («Resource ID»), указанный в атрибутах пакета, рисунок 2.47.

Рисунок 2.47 – Идентификатор пакета ресурсов («Resource ID»)

5. Выполнить экспорт arb-пакета сетевой модели.

6. Настроить планировщик задач на обновление пакета ресурсов сетевой модели в соответствии с документацией на ПК Ankey SIEM.

2.5.2 Интеграция с Ankey SIEM NG

После выполнения настроек на стороне Ankey SIEM NG, приведенных ниже, необходимо настроить плагины, указанные в таблице 2.4 для получения данных, а также плагины, указанные в таблице 2.9 для обработки данных.

Таблица 2.4 – Плагины для получения данных из Ankey SIEM NG

Наименование	Пункт руководства	Примечание
Получение потока событий и инцидентов из Ankey SIEM NG	2.6.3.2	Только при интеграции через RabbitMQ для версии Ankey SIEM NG v3 (отсутствие компонента Event Broker ПК Ankey SIEM NG)
Получение объектов из модели активов Ankey SIEM NG	2.6.3.3	

2.5.2.1 Настройка Ankey SIEM NG для передачи событий и инцидентов безопасности в ПК «Ankey ASAP» через компонент Event Broker

Для выполнения передачи событий и инцидентов безопасности из Ankey SIEM NG v4 и выше в ПК «Ankey ASAP» используется компонент «Ankey SIEM NG Event Broker», установленный на компонент «Ankey SIEM NG Server».

Для настройки пересылки данных из компонента «Ankey SIEM NG Event Broker», необходимо создать файл конфигурации «redirection_rules.json» и внести настройки, указанные в таблице 2.5. Пример файла «redirection_rules.json» приведен в приложении А.

Таблица 2.5 – Настройка компонента Ankey SIEM NG Event Broker

Параметры		Настройка	Описание
"transports":	**Первый транспорт**		
	"id":	"00000000-0000-0000-0000-000000000001"	Уникальный идентификатор транспорта, значение присваивается пользователем
	"qos":	"retain"	Параметр регулирования сообщений в

Параметры		Настройка		Описание
				очереди: удаляет сообщения из очереди, для которых не было получено подтверждение
	"syslog":	"host":	FQDN сервера	FQDN сервера ПК «Ankey ASAP»
		"port":	6514	Номер порта, на который будут передаваться нормализованные события
		"protocol":	"tcp"	Протокол, по которому будут передаваться нормализованные события. Рекомендуется использовать TCP-протокол, так как размер передаваемых пакетов может превышать допустимый размер по протоколу UPD
"rules":	**Правило для первого транспорта**			
	"id":	"00000000-0000-0000-0000-000000000002"		Уникальный идентификатор правила фильтрации событий, значение присваивается пользователем
	"transports":	"00000000-0000-0000-0000-000000000001"		Идентификатор транспорта, к которому принадлежит блок правила
	"event_type":	"norm"		Тип событий: нормализованные события (включает в себя нормализованные и коррелированные события)

Для установки правил фильтрации пересылаемых событий необходимо выполнить следующие действия:

1. Создать файл «redirection_rules.json» на сервере обработки ПК Ankey SIEM NG (компонент «Server»);

2. Выполнить следующую команду:

/opt/siem/bin/siemlight-kb --redirection -u redirection_rules.json --host <FQDN сервера Ankey SIEM NG>

2.5.2.2 Настройка Ankey SIEM NG для передачи событий и инцидентов безопасности в ПК «Ankey ASAP» через очередь RabbitMQ

Другой способ сбора событий и инцидентов безопасности осуществляется с помощью создания очереди в RabbitMQ ПК Ankey SIEM NG (при отсутствии компонента Event Broker):

Примечание. Данный способ не рекомендован к использованию для передачи данных.

1. Подключиться к веб-интерфейсу RabbitMQ ПК Ankey SIEM NG (компонент Server) с использованием логина и пароля (по умолчанию: «localhost:15672»).

2. Перейти на вкладку «Admin» → «Policies» и создать политику на ограничение количества сообщений в очереди (рисунок 2.48). Для этого нажать на кнопку «Add / update a policy» и указать следующие параметры:

– Virtual host: siem

– Name: events_for_asap.events_Size_Policy

– Pattern: ^events_for_ASAP

– Apply to: Exchanges and queues

– Definition: max-length: 4000

Примечание. Параметр «max-length» указать не более 10000.

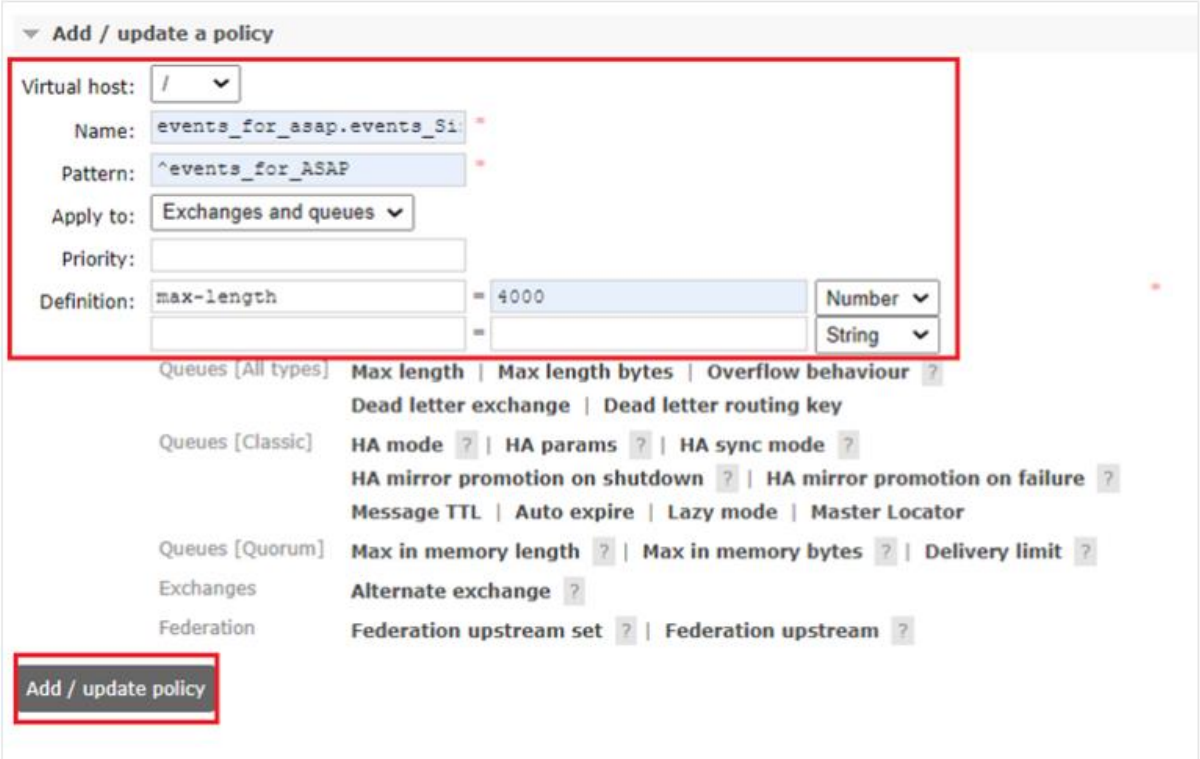


Рисунок 2.48 – Создание политики на ограничение сообщений в очереди

3. На вкладке «Admin» перейти в раздел «Shovel Management».

4. Создать новый «shovel» со следующими параметрами (рисунок 2.49):

– Virtual host: siem

– Name: events_for_ASAP

– Source: AMQP 0.9.1

– URI: amqp://siem@/siem

«ampq://<имя УЗ RabbitMQ Ankey SIEM NG>@/<Virtual host>»

– Queue: events_for_ASAP

– Destination: AMQP 0.9.1

– URI: ссылка на RabbitMQ Ankey ASAP в формате:

«ampq://<имя УЗ RabbitMQ в Ankey ASAP>:<пароль>@<ip-адрес Ankey ASAP>:5672»

– Queue (название очереди, создаваемой в RabbitMQ Ankey ASAP): events_for_ASAP. Данное название очереди используется в конфигурации плагина «Получение потока событий и инцидентов из Ankey SIEM NG» (2.6.3.2).

Примечание. В случае отсутствия вкладки «Shovel», добавить её в настройках RabbitMQ либо воспользоваться консольными утилитами, поставляемыми с RabbitMQ.

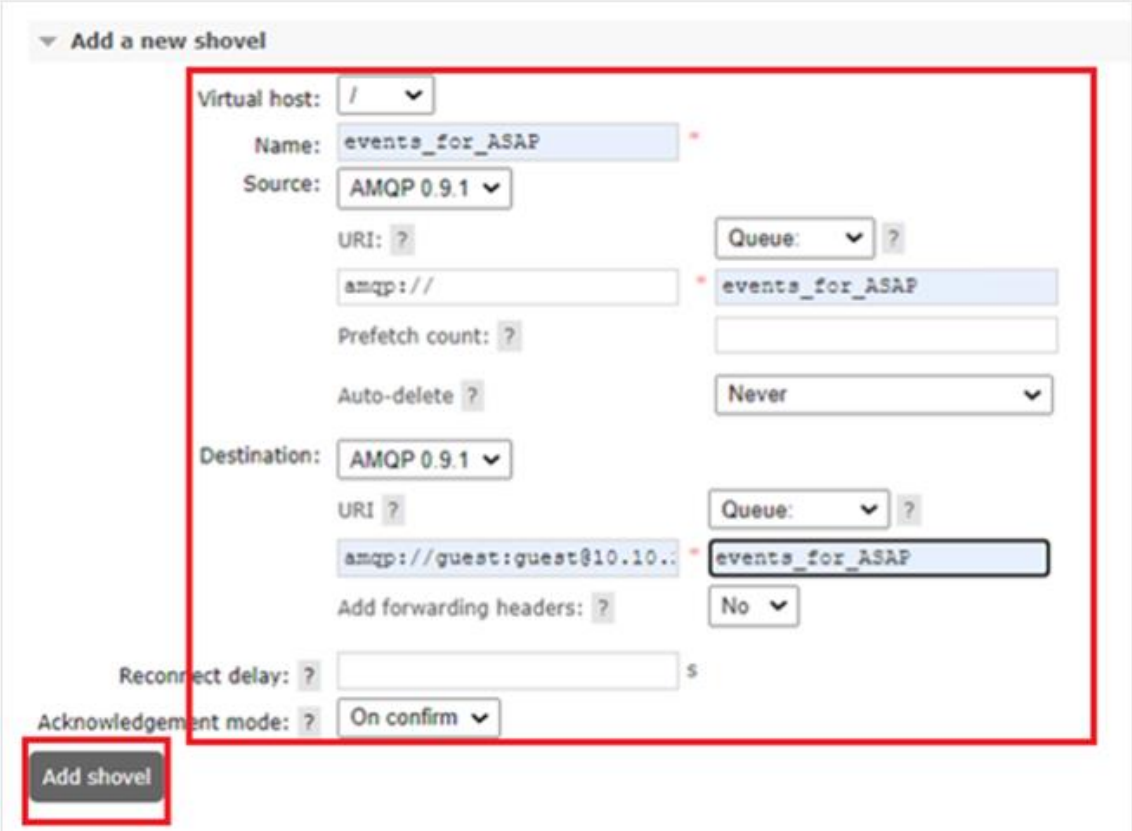


Рисунок 2.49 – Создание Shovel

5. Убедиться, что «Shovel Status» запущен и имеет значение «running».

6. Перейти в «Queues», в созданную очередь (event_for_ASAP). Перейти во вкладку «bindings». Создать bind по следующему шаблону:

– From exchange: events

– Routing key: storageq

7. Выйти из веб-интерфейса RabbitMQ ПК Ankey SIEM NG.

8. В RabbitMQ Ankey ASAP (порт 5903) проверить наличие очереди «events_for_ASAP» в разделе «Queues».

9. Перейти на вкладку «Admin» и создать политику на ограничение количества сообщений в очереди. Для этого нажать на кнопку «Add / update a policy» и указать следующие параметры:

– Virtual host: /

– Name: events_Size_Policy

– Pattern: ^events_for_ASAP

– Definition: max-length: 4000

Примечание. Параметр «max-length» указать не более 10000.

2.5.2.3 Настройка Ankey SIEM NG для получения объектов из модели активов

Для получения объектов из модели активов необходимо создать УЗ с ролью оператора в Ankey SIEM NG.

Примечание. Пароль для создаваемой УЗ не должен содержать символы:

", #, %, \, /, ?

2.5.3 Интеграция с Active Directory

Для синхронизации каталога MS Active Directory (AD) выполняется подключение к LDAP, чтение информации (все записи в каталоге по пользователям, группам, компьютерам).

Для получения данных AD необходимо настроить плагин, указанный в таблице 2.6. Для подключения плагина используется УЗ, созданная в AD, имеющая права на чтение каталога AD.

Таблица 2.6 – Плагины для получения данных из Active Directory

Наименование	Описание	Пункт руководства
Получение объектов из MS Active Directory	Получение записей каталога по пользователям, группам, компьютерам	2.6.3.4

2.5.4 Интеграция с Staffcop Enterprise

Интеграция с программным комплексом Staffcop Enterprise (Staffcop) выполняется для получения событий с рабочих компьютеров сотрудников.

Примечание. Сбор данных из Staffcop Enterprise выполняется при наличии соответствующей лицензии на коннектор сбора данных.

Выгрузка данных производится через прямое подключение к БД PostgreSQL Staffcop Enterprise. Для этого необходимо:

1. Создать УЗ в БД PostgreSQL с правами на чтение либо использовать имеющуюся УЗ.

2. В конфигурационные файлы «*pg_hba.conf*» и *postgresql.conf* внести изменения в соответствии с документацией на Staffcop Enterprise.

3. Для вступления в силу изменений настроек конфигурационных файлов, перезапустить службу СУБД:

service postgresql restart

После выполнения настроек на стороне Ankey SIEM, приведенных ниже, необходимо настроить плагины, указанные в таблице 2.7 для получения данных, а также плагины, указанные в таблице 2.9 для обработки данных.

Таблица 2.7 – Плагины для получения данных из Staffcop Enterprise

Наименование	Пункт руководства
Выгрузка данных из Staffcop	2.6.3.5
Получение объектов из Staffcop	2.6.3.6

2.6 Настройка плагинов

Плагины предназначены для подключения к источникам для сбора данных, а также для вычитки данных, поступивших из источников в брокер сообщений ПК «Ankey ASAP». Экземпляры плагинов выполняют обработку определенных типов данных и записывают данные в базу данных ПК «Ankey ASAP». Перед началом работы плагинов необходимо настроить интеграцию с источниками данных в соответствии с подразделом 2.5.

Добавление и настройка плагинов производится в веб-интерфейсе ПК «Ankey ASAP», на странице «Параметры платформы» → «Плагины» (рисунок 2.50).

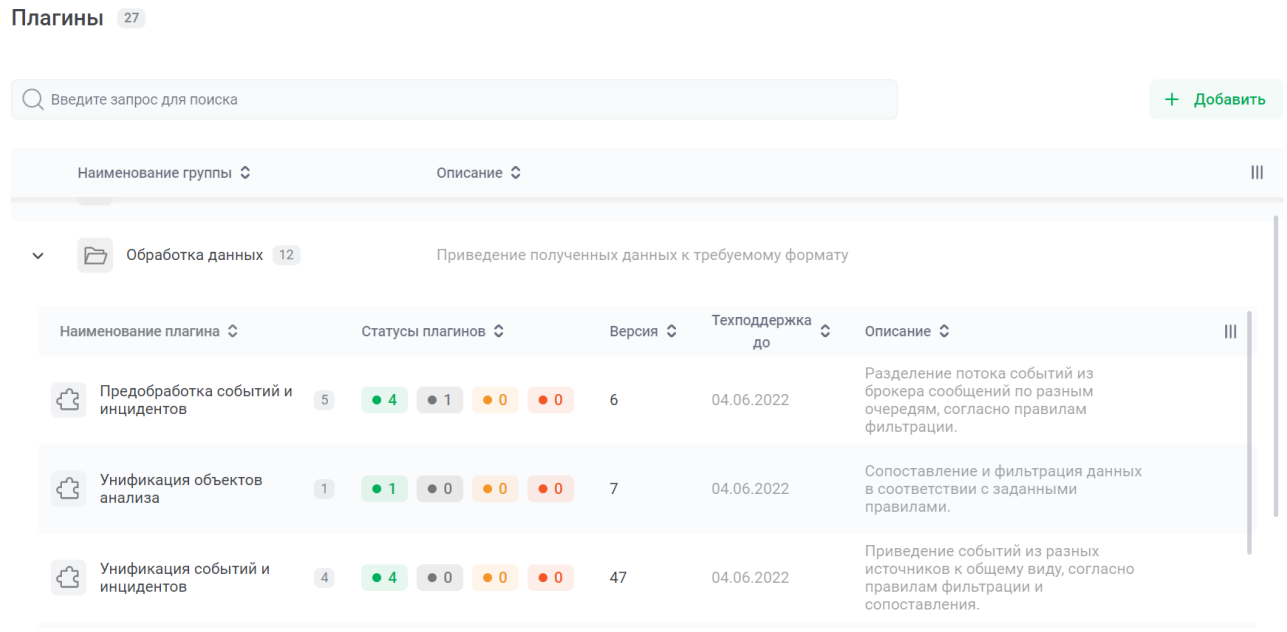


Рисунок 2.50 – Страница «Плагины»

После инсталляции ПК «Ankey ASAP» базовые плагины автоматически установлены без экземпляров и размещаются в папке «*/opt/asap/configs/backend/plugins*» в архивах, имеющих расширение «zip».

После инсталляции доступны базовые плагины для интеграции с источниками, перечисленные в таблице 2.8 и базовые плагины для обработки и сохранения данных, перечисленные в таблице 2.9.

Таблица 2.8 – Плагины ПК «Ankey ASAP» для интеграции с источниками данных

Наименование плагина	Название архива с плагином	Источник	Пункт руководства
Плагины получения данных из внешних источников			
Получение объектов из сетевой модели Ankey SIEM	entitiesaksiem	Ankey SIEM	2.6.3.1
Получение потока событий и инцидентов из Ankey SIEM NG (при отсутствии компонента Event Broker)	eventsaksiemng	Ankey SIEM NG	2.6.3.2
Получение объектов из модели активов Ankey SIEM NG	entitiesaksiemng	Ankey SIEM NG	2.6.3.3
Получение объектов из MS Active Directory	entitiesmsad	Active Directory	2.6.3.4

Таблица 2.9 – Плагины для обработки данных

Наименование плагина	Описание	Название архива с плагином	Пункт руководства	Примечание
Плагины обработки данных				
Предобработка событий и инцидентов	Обработка данных (базовые события из Ankey SIEM) из общего топика kafka в разные очереди согласно правилам фильтрации	eventsformatconverter	2.6.3.7	Только при интеграции с Ankey SIEM
Унификация событий и инцидентов	Категоризация и унификация событий в соответствии с источником событий	eventsunifier	2.6.3.8	
Унификация объектов анализа	Сопоставление и фильтрация данных в соответствии с заданными	entitiesunifier	2.6.3.9	

Наименование плагина	Описание	Название архива с плагином	Пункт руководства	Примечание
	правилами.			
Классификация событий по алертам	Алерты по редким действиям, совершаемым объектами анализа	alerter	2.6.3.10	
Выявление атак LotL	Классификация команд для выявления атак Living off the Land	lotl	2.6.3.11	
Запись потока данных из брокера сообщений в базу данных	Перенос и сохранение в БД потока данных, поступившего в брокер сообщений	datasaver	2.6.3.12	

Добавление плагинов, в случае их отсутствия после инсталляции, описано в 2.6.2.

Также для получения данных необходимо произвести настройки для источника данных. Для получения базовых событий и инцидентов из Ankey SIEM и Ankey SIEM NG необходимо выполнить настройки на стороне Ankey SIEM и Ankey SIEM NG соответственно. Настройки приведены в пункте 2.5.

2.6.2 Добавление плагина

Для добавления плагина необходимо выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины» и нажать кнопку «Добавить» > «Плагин» в правом верхнем углу (см. рисунок 2.50).

2. В открывшемся диалоговом окне выбора файла перейти в папку с плагином, выбрать zip-архив с плагином и нажать кнопку «Открыть».

Откроется окно для инсталляции плагина (рисунок 2.51).

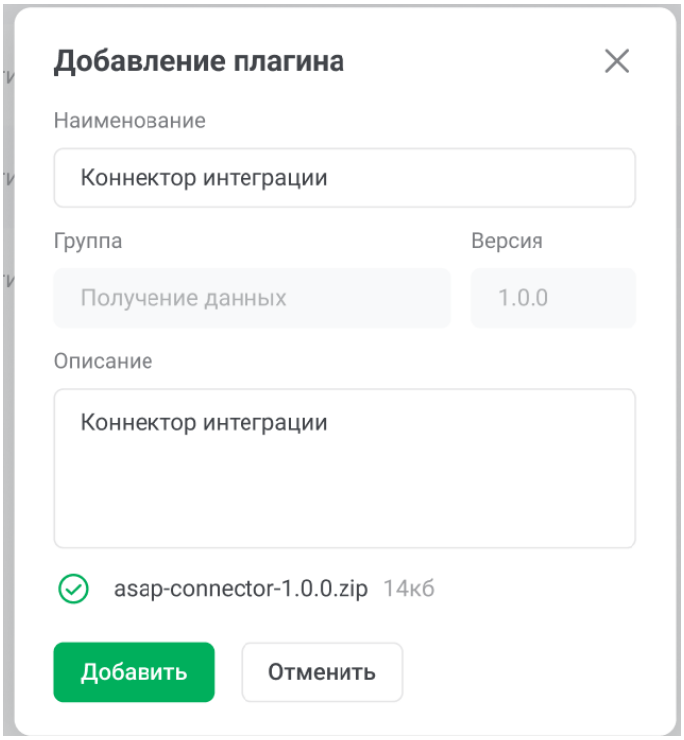


Рисунок 2.51 – Инсталляция плагина

3. В окне инсталляции плагина должны быть заданы следующие поля:

– наименование плагина (заполнено, с возможностью изменения);

– группа (заполнено);

– версия – устанавливаемая версия плагина (заполнено);

– описание (заполнено, с возможностью изменения);

– файл плагина – указывается наименование zip-файла, выбранного при добавлении плагина (заполнено).

4. Нажать кнопку «Добавить».

5. Для работы плагина необходимо выполнить настройку и запуск экземпляров плагина.

Информацию о добавленном плагине и его экземплярах можно просмотреть на странице «Плагины» в соответствующей группе.

2.6.3 Настройка экземпляров плагина

Для просмотра и настройки экземпляров плагина на странице «Параметры платформы» → «Плагины» раскрыть требуемую группу плагинов и нажать на наименование плагина. Откроется окно с перечнем экземпляров плагина (рисунок 2.52).

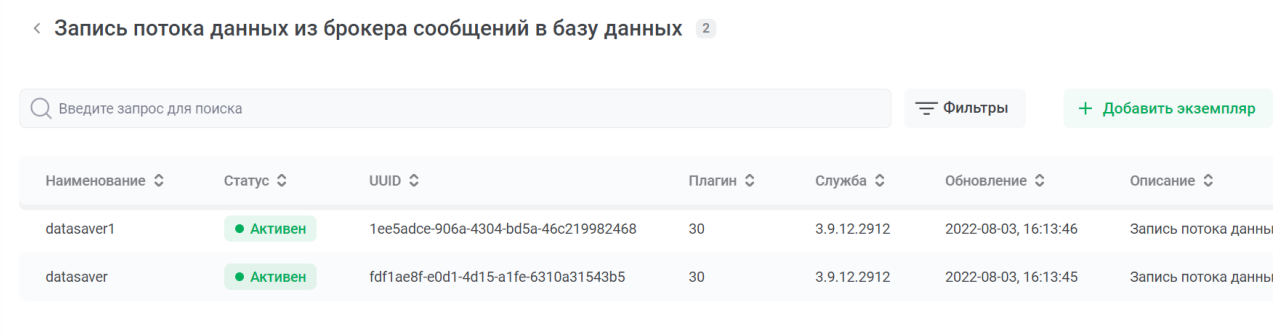


Рисунок 2.52 – Экземпляры плагина

В данном окне можно выполнить запуск, остановку или настройку определенных экземпляров плагина. Подробная настройка плагинов описана в руководстве администратора.

В случае отсутствия экземпляров плагинов, нажать кнопку «Добавить экземпляр». После выполнения создания экземпляра, будет открыто окно с конфигурацией плагина (рисунок 2.53). Конфигурация плагина настраивается для каждого экземпляра плагина согласно подразделу по соответствующему плагину.

Примечание. В случае, если при создании плагина возникает ошибка создания экземпляра, выполнить попытку добавления еще раз. В случае возникновения ошибки больше двух раз подряд, выполнить следующие действия:

1. Выполнить команду в консоли с правами администратора:
   asap reset manager
2. Подтвердить удаление данных.
3. Добавить экземпляр в интерфейсе еще раз.

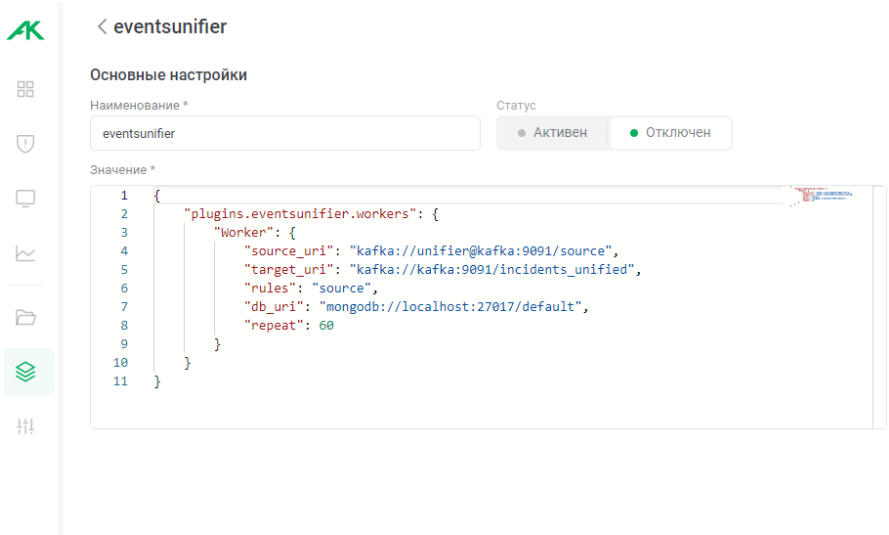


Рисунок 2.53 – Пример конфигурации экземпляра плагина

Запуск экземпляра плагина производится одним из следующих способов:

– установить статус «Активен» и нажать кнопку «Сохранить» в конфигурации плагина;

– на странице с экземплярами плагина нажать пиктограмму «▷» в правой части строки соответствующего экземпляра плагина.

Получение логов плагина возможно следующими способами:

1. В веб-интерфейсе скопировать UUID плагина и найти логи на странице «Журнал аудита», выполнив поиск по UUID.

2. В консоли:

– найти нужный pod, содержащий UUID требуемого плагина, выполнив команду:

sudo asap get deploy

– вывести лог:

asap logs svc/service-<uuid плагина>

2.6.3.1 Настройка получения объектов из сетевой модели Ankey SIEM

Настройка плагина выполняется при интеграции с Ankey SIEM.

Плагин «Получение объектов из сетевой модели Ankey SIEM» предназначен для получения объектов сетевой модели путем подключения к ПК «Ankey SIEM» и записи данных в брокер сообщений ПК «Ankey ASAP».

Для получения объектов сетевой модели необходимо выполнить настройку на стороне Ankey SIEM в соответствии с 2.5.1.4.

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

1. Перейти на страницу настройки экземпляров плагина «Получение объектов из сетевой модели Ankey SIEM», входящего в группу «Сбор данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «EntitiesAKSIEM.zip» в соответствии с 2.6.2.

2. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр».

3. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.10.

Таблица 2.10 – Конфигурация плагина «Получение объектов из сетевой модели Ankey SIEM»

Настройка	Формат	Параметр
plugins.entitiesaksiem.workers		
siem_uri	*siem://<имя УЗ>:<пароль УЗ>@<ip-адрес сервера SIEM>?resourceId=<ID пакета ресурсов >* siem://asap:password@localhost?resourceId=	имя УЗ – имя УЗ, созданной в SIEM
		пароль УЗ[1)] – пароль созданной УЗ в SIEM
		ID пакета ресурсов - Resource ID пакета ресурсов, сформированного в SIEM
repeat	*<периодичность>*	периодичность синхронизации (в секундах)
1) Пароль УЗ не должен содержать следующие символы: ", #, %, \, /, ?		

4. Установить статус плагина «Активен».

5. Нажать кнопку «Сохранить».

2.6.3.2 Настройка получения потока событий и инцидентов из Ankey SIEM NG

Примечание. Настройка плагина выполняется только при интеграции с Ankey SIEM NG через очередь сообщений RabbitMQ в случае отсутствия компонента Event Broker Ankey SIEM NG.

Плагин «Получение потока событий и инцидентов из Ankey SIEM NG» предназначен для подключения к очереди сообщений Ankey SIEM NG и сбора данных о событиях и инцидентах безопасности.

Для сбора данных необходимо выполнить настройку на стороне Ankey SIEM NG в соответствии с 2.5.2.2.

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно настройки экземпляров плагина «Получение потока событий и инцидентов из Ankey SIEM NG», входящего в группу «Сбор данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «eventsaksiemng.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.11.

Таблица 2.11 – Конфигурация плагина «Получение потока событий и инцидентов из Ankey SIEM NG»

Настройка	Формат	Параметр	Значение
plugins.eventsaksiemng.workers			
broker_uri	*amqp://<имя УЗ>:<пароль>@<ip-адрес Ankey ASAP>:<порт>* amqp://guest:*****@ x.x.x.x:5672	Имя УЗ - УЗ в RabbitMQ в Ankey ASAP	
		Пароль[1)] – пароль УЗ RabbitMQ в Ankey ASAP	
		Порт – открытый порт брокера сообщений RabbitMQ Ankey ASAP	5672
transfer: { topic	events_for_ASAP	Очередь – название очереди RabbitMQ Ankey ASAP, заданное при настройках shovel на стороне SIEM NG (параметр “queue”) (2.5.2.1)	events_for_ASAP
rules [2)]	transfer	Перенос событий из очереди RMQ в топик kafka	"enabled": true
1) Пароль УЗ не должен содержать следующие символы: ", #, %, \, /, ? 2) Остальные неуказанные значения rules должны иметь параметр "enabled": false			

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.3 Настройка получения объектов из модели активов Ankey SIEM NG

Настройка плагина выполняется при интеграции с Ankey SIEM NG.

Плагин «Получение объектов из модели активов Ankey SIEM NG» предназначен для подключения к Ankey SIEM NG и сбора данных об активах сетевой модели.

Для сбора данных необходимо выполнить создать учетную запись на стороне Ankey SIEM NG для подключения либо использовать существующую.

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно настройки экземпляров плагина «Получение объектов из модели активов Ankey SIEM NG», входящего в группу «Сбор данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «entitiesaksiemng.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.12.

Таблица 2.12 – Конфигурация плагина «Получение объектов из модели активов Ankey SIEM NG»

Настройка	Формат	Параметр	Значение
plugins.entitiesaksiemng.workers			
siem_uri	*siem://<имя УЗ>:<пароль>@<ip-адрес SIEM NG(компонент Core)>:<порт>*	*имя УЗ в SIEM NG* – имя созданной или существующей УЗ в SIEM NG	
		пароль – пароль УЗ в SIEM NG	
		порт – открытый порт в SIEM NG	3334 (по умолчанию)
db_uri	*mongodb://mongo:27017/asap*		
repeat	*<периодичность>*	периодичность синхронизации (в секундах)	60 (по умолчанию, секунд)
* Пароль УЗ не должен содержать следующие символы: ", #, %, \, /, ?			

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.4 Настройка получения объектов из MS Active Directory

Для синхронизации каталога MS Active Directory плагин выполняет подключение по LDAP, чтение информации (все записи в каталоге по пользователям, группам, компьютерам) и запись в базу данных.

Для добавления и настройки плагина для получения объектов MS AD выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти на страницу настройки экземпляров плагина «Получение объектов из MS Active Directory», входящего в группу «Сбор данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «entitiesmsad.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.13.

Таблица 2.13 – Конфигурация плагина «Получение объектов из MS Active Directory»

Настройка	Формат	Параметр
plugins.entitiesmsad.workers		
ldap_uri	*ldap://<домен AD> \\<имя пользователя>:<пароль>@<имя хоста контроллера домена>* Пример: ldap://DOMAIN\\user:password@domain.lan	домен AD –имя домена AD (FQDN)
		имя пользователя – имя созданной УЗ для подключения к AD
		пароль[1)] – пароль от созданной УЗ
		имя хоста контроллера домена – имя хоста или IP-адрес контроллера домена
repeat	*<периодичность>*	периодичность синхронизации (в секундах)
1) Пароль УЗ не должен содержать следующие символы: ", #, %, \, /, ?		

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.5 Настройка выгрузки данных из Staffcop Enterprise

Для получения данных (событий) из Staffcop, плагин выполняет прямое подключение к БД Staffcop.

Для добавления и настройки плагина для получения данных из Staffcop выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти на страницу настройки экземпляров плагина «Выгрузка данных из Staffcop», входящего в группу «Сбор данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «staffcop.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.14.

Таблица 2.14 – Конфигурация плагина «Выгрузка данных из Staffcop»

Настройка	Формат	Параметр
plugins.staffcop.workers		
"sources": { "staffcop": { "uri"	postgresql://<имя УЗ>:<пароль>@<ip-адрес>:<порт>/<имя БД> Пример:	user – имя УЗ в БД Staffcop
		пароль[1)] – пароль от созданной УЗ
		ip-адрес - ip-адрес сервера Staffcop

Настройка	Формат	Параметр
	postgresql://staffcop:password@x.x.x.x:5432/staffcop	Порт – порт БД PostgreSQL Staffcop (по умолчанию 5432)
		имя БД – имя БД в БД PostgreSQL Staffcop (по умолчанию «staffcop»)
1) Пароль УЗ не должен содержать следующие символы: ", #, %, \, /, ?		

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.6 Настройка получения объектов из Staffcop Enterprise

Для получения объектов из Staffcop, плагин выполняет прямое подключение к БД Staffcop.

Для добавления и настройки плагина для получения данных из Staffcop выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти на страницу настройки экземпляров плагина «Получение объектов из Staffcop», входящего в группу «Сбор данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «entitiesstaffcop.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.15.

Таблица 2.15 – Конфигурация плагина «Получение объектов из Staffcop»

Настройка	Формат	Параметр
plugins.entitiesstaffcop.workers		
"sources": { "staffcop": { "uri"	postgresql://<имя УЗ>:<пароль>@<ip-адрес>:<порт>/<имя БД> Пример: postgresql://staffcop:password@x.x.x.x:5432/staffcop	user – имя УЗ в БД Staffcop
		пароль[1)] – пароль от созданной УЗ
		ip-адрес - ip-адрес сервера Staffcop
		Порт – порт БД PostgreSQL Staffcop (по умолчанию 5432)
1) Пароль УЗ не должен содержать следующие символы: ", #, %, \, /, ?		

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.7 Настройка предобработки событий и инцидентов

Плагин «Предобработка событий и инцидентов» ПК «Ankey ASAP» выполняет разделение потока событий Ankey SIEM из брокера сообщений по разным очередям, согласно правилам фильтрации.

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно добавления и настройки экземпляров плагина «Предобработка событий и инцидентов», входящего в группу «Обработка данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «eventsformatconverter.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр плагина».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.16.

Таблица 2.16 – Конфигурация плагина «Предобработка событий и инцидентов»

Настройка	Формат	Параметр	Значение
plugins.eventsformatconverter.workers			
events: { topic	events	Название топика, заданное при настройке коннектора Ankey SIEM (2.5.1.1)	events
incident: { topic	incident	Название топика, заданное при настройке коннектора Ankey SIEM (2.5.1.3)	incident
rules[1)]	incident	Предобработка инцидентов	"enabled": true
	events	Предобработка событий	"enabled": true
1) Остальные неуказанные значения rules должны иметь параметр "enabled": false			

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.8 Настройка унификации событий и инцидентов

Плагин «Унификация событий и инцидентов» производит категоризацию и унификацию событий в соответствии с источником событий.

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно добавления и настройки экземпляров плагина «Унификация событий и инцидентов», входящего в группу «Обработка данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «eventsunifier.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр плагина».

4. После создания экземпляра выполнить изменение конфигурации плагина в соответствии с таблицей 2.17, для чего:

– выполнить поиск по конфигурации плагина, переведя курсор в область редактора и нажав сочетание клавиш «Ctrl+F». Откроется окно поиска, представленное на рисунке 2.54;

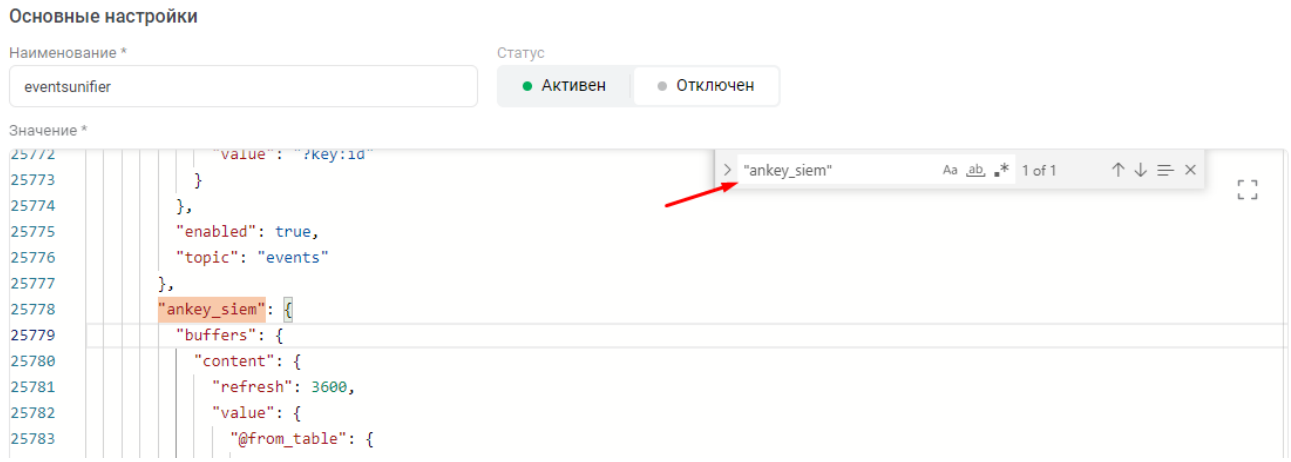


Рисунок 2.54 – Поиск по конфигурации плагина

– изменить в правиле значение поля "*enabled*" на *false*, вместо *true*;

Таблица 2.17 – Конфигурация плагина «Унификация событий и инцидентов»

Настройка	Формат	Параметр	Значение
plugins.eventsunifier.workers			
rules[1)]	“staffcop__<название>”	Обработка данных из Staffcop	"enabled": false
	“ankey_siem__<название>”[2)]	Обработка данных из Ankey SIEM	"enabled": false
	“ankey_siem_ng__<название>[3)]	Обработка данных из Ankey SIEM NG	"enabled": false
broker_uri	kafka://unifier@kafka:9091		
1) Остальные неуказанные значения rules должны иметь параметр "enabled": true (значение по			

Настройка	Формат	Параметр	Значение
умолчанию) 2) В случае, если источником данных является Ankey SIEM NG 3) В случае, если источником данных является Ankey SIEM			

5. Нажать кнопку «Сохранить».

6. Установить статус плагина «Активен».

7. Нажать кнопку «Сохранить».

Примечание. При большом потоке, в случае, если инциденты приходят с задержкой, увеличить количество экземпляров плагина до четырех.

2.6.3.9 Настройка унификации объектов анализа

Плагин «Унификация объектов анализа» ПК «Ankey ASAP» выполняет унификацию всех сущностей.

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно добавления и настройки экземпляров плагина «Унификация объектов анализа», входящего в группу «Обработка данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «entitiesunifier.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр плагина».

4. Запустить экземпляр плагина, установив статус «Активен» и нажав кнопку «Сохранить».

2.6.3.10 Классификация событий по алертам

Плагин «Классификация событий по алертам» позволяет обнаруживать редкие действия пользователей (первые действия за последние 90 дней).

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно добавления и настройки экземпляров плагина «Классификация событий по алертам», входящего в группу «Обработка данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «alerter.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр плагина».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.18.

Таблица 2.18 – Конфигурация плагина «Классификация событий по алертам»

Настройка	Формат	Описание	Значение
plugins.alerter.workers			
db_uri	*postgresql://<имя УЗ>:<пароль>@<IP-адрес сервера Ankey ASAP>:<порт>/<БД>*	Имя УЗ – имя пользователя БД, заданное при настройке СУБД Jatoba в соответствии с 2.1.3	asap
		Пароль – пароль от УЗ пользователя БД	
		Порт – внутренний открытый порт СУБД Jatoba	5432
		БД – база данных, созданная в СУБД Jatoba	asap

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

2.6.3.11 Выявление атак LotL

Плагин «Выявление атак LotL» позволяет обнаруживать деструктивные терминальные команды при использовании легитимных или встроенных системных утилит для выявления атак типа «Living-off-the-land».

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно добавления и настройки экземпляров плагина «Выявление атак LotL», входящего в группу «Обработка данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «lotl.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр плагина».

4. После создания экземпляра плагина установить статус «Активен».

5. Нажать кнопку «Сохранить».

2.6.3.12 Настройка сохранения событий и инцидентов в базу данных

Плагин «Запись потока данных из брокера сообщений в базу данных» выполняет перенос и сохранение в базу данных событий, поступивших в брокер сообщений.

Данные распределяются по следующим БД:

1. Внутренняя СУБД MongoDB:
   – инциденты;
   – редкие действия (алерты);
   – унифицированные базовые события (с ограниченным перечнем полей).
2. СУБД Jatoba:
   – унифицированные базовые события (с расширенным перечнем полей);
   – сессии объектов анализа (на объектах анализа).

Для добавления и настройки плагина выполнить следующие действия:

1. Перейти на страницу «Параметры платформы» → «Плагины».

2. Перейти в окно добавления и настройки экземпляров плагина «Запись потока данных из брокера сообщений в базу данных», входящего в группу «Отправка данных».

Примечание. В случае отсутствия плагина или необходимости обновления плагина вручную, выполнить добавление архива с плагином «datasaver.zip» в соответствии с 2.6.2.

3. Добавить экземпляр плагина, нажав на кнопку «Добавить экземпляр плагина».

4. После создания экземпляра изменить конфигурацию в соответствии с таблицей 2.19 для сохранения инцидентов.

Таблица 2.19 – Конфигурация плагина «Запись потока данных из брокера сообщений в базу данных» для сохранения данных в MongoDB

Настройка	Формат	Описание	Значение
plugins.datasaver.workers			
db_uri	mongodb://mongo:27017/asap		
rules[1)]	incidents	Сохранение унифицированных инцидентов	"enabled": true

Настройка	Формат	Описание	Значение
	alerts	Сохранение редких действий	"enabled": true
	uefa_events_to_mongo	Сохранение унифицированных событий	"enabled": false
	Другие		"enabled": false
1) Остальные неуказанные значения rules должны иметь параметр "enabled": false			

5. Установить статус плагина «Активен».

6. Нажать кнопку «Сохранить».

7. Аналогично создать экземпляр плагина для сохранения базовых событий в соответствии с таблицей 2.20 и выполнить настройки подключения к БД Jatoba в соответствии с 2.4.3.1.

Таблица 2.20 – Конфигурация плагина «Запись потока данных из брокера сообщений в базу данных» для сохранения данных в СУБД Jatoba

Настройка	Формат	Описание	Значение
plugins.datasaver.workers			
db_uri	*postgresql://<имя УЗ>:<пароль>@<IP-адрес сервера Ankey ASAP>:<порт>/<БД>*	Имя УЗ – имя пользователя БД, заданное при настройке СУБД Jatoba в соответствии с 2.1.3	asap
		Пароль – пароль от УЗ пользователя БД	
		Порт – внутренний открытый порт СУБД Jatoba	5432
		БД – база данных, созданная в СУБД Jatoba	asap
rules[1)]	uefa_events_to_postgres	Сохранение унифицированных базовых событий	"enabled": true
	session_events_to_postgres	Сохранение событий, связанных с сессиями	"enabled": true
	Другие		"enabled": false
1) Остальные неуказанные значения rules должны иметь параметр "enabled": false			

8. Установить статус плагина «Активен».

9. Нажать кнопку «Сохранить».

Выполнить создание представления в БД «Jatoba» в соответствии с 2.1.3.7.

2.7 Удаление ПК «Ankey ASAP»

2.7.1 Удаление ПК «Ankey ASAP» для ОС Astra Linux

Для удаления ПК «Ankey ASAP» в ОС Astra Linux необходимо выполнить следующие действия от пользователя с правами администратора:

1. Для остановки контейнеров и удаления исполняемых файлов выполнить команду:

apt remove asap

В случае выполнения данного варианта удаления данные в брокере сообщений Kafka и базах данных сохраняются для последующего использования. После новой установки ПК «Ankey ASAP», необходимо будет реактивировать лицензию, как описано в 2.4.2.3.

2. Для полного удаления ПК «Ankey ASAP» выполнить команду:

apt remove --purge asap

В случае выполнения данного варианта удаления все данные удаляются, и система возвращается к исходному состоянию. В случае новой установки ПК «Ankey ASAP», необходимо будет реактивировать лицензию, как описано в 2.4.2.3.

3. Для удаления служб плагинов выполнить команду:

apt remove asap-plugins

4. Для удаления среды функционирования ПК «Ankey ASAP» выполнить команду:

apt remove asap-runtime

2.7.2 Удаление ПК «Ankey ASAP» для РЕД ОС

Для удаления ПК «Ankey ASAP» в РЕД ОС необходимо:

1. Выполнить следующую команду:

yum remove asap

Пример выполнения команды приведен на рисунке 2.55.

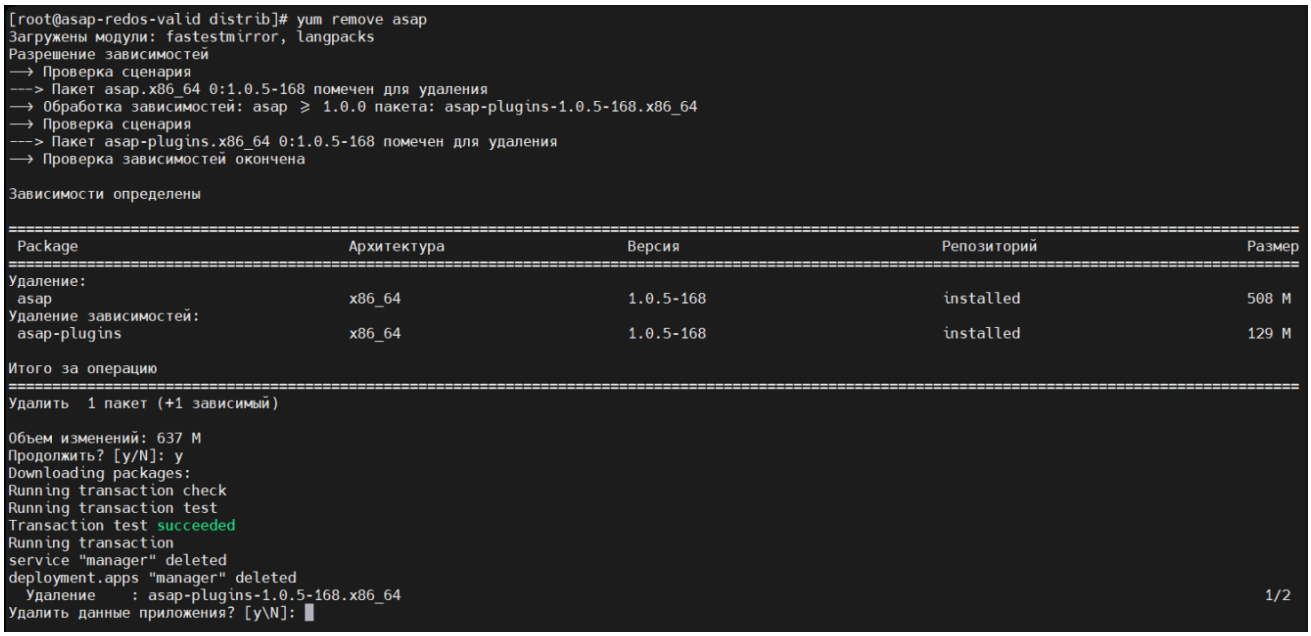


Рисунок 2.55 – Пример команды для удаления Ankey ASAP

2. Выбрать вариант удаления ПК «Ankey ASAP» – полное удаление с данными, либо удаление без данных:

– для сохранения данных и настроек, на вопрос «Удалить данные приложения?», ввести ответ: «N».

– для выполнения полного удаления данных и возврата системы к исходному состоянию, на вопрос «Удалить данные приложения?», ввести ответ: «Y»

Для удаления среды функционирования ПК «Ankey ASAP» выполнить команду:

yum remove asap-runtime

3 Интеграция с системами автоматизации процессов обеспечения безопасности

В систему автоматизации процессов обеспечения безопасности (САОБ) передаются инциденты ИБ и сведения о событиях изменения правил корреляции для дальнейшей работы с инцидентами и проведения расследования.

Интеграция позволяет синхронизировать состояние карточек инцидентов ИБ в ПК «Ankey ASAP» и системах управления инцидентами после внесения в них изменений.

Передача сведений об инцидентах в САОБ происходит посредством API-запросов по протоколу HTTPS в ПК «Ankey ASAP» со стороны САОБ.

Для передачи инцидентов ИБ в САОБ в ПК «Ankey ASAP» используется один из следующих методов:

1. Подключение с помощью логина и пароля.

В ПК «Ankey ASAP» должна быть создана служебная учетная запись для подключения. Для создания служебной учетной записи выполнить следующие действия:

– перейти в «Администрирование» → «Пользователи»;

– нажать на кнопку «Добавить»;

– при заполнении полей отметить поле «Служебная учетная запись»;

– создать учетную запись.

Логин и пароль от созданной учетной записи используется для подключения к ПК «Ankey ASAP» со стороны САОБ.

2. Подключение с помощью API-ключа

В ПК «Ankey ASAP» должна быть создана УЗ, содержащая API-ключ для подключения. Для этого выполнить следующие действия:

– перейти в «Администрирование» → «Пользователи»;

– нажать на кнопку «Добавить»;

– создать УЗ с ролью «Аналитик»;

– выполнить вход в ПК «Ankey ASAP» под созданной УЗ;

– перейти в профиль пользователя (в нижней части левого меню);

– в подразделе «Интеграция» нажать кнопку «Сгенерировать» для генерации API-ключа.

Сгенерированный API-ключ используется для подключения к ПК «Ankey ASAP» со стороны САОБ.

Перечень сокращений

AD	–	Active Directory
CEF	–	Common Event Format
LDAP	–	Lightweight Directory Access Protocol
CLI	–	Command Line Interface
АРМ	–	автоматизированное рабочее место
ИБ	–	информационная безопасность
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
САОБ	–	система автоматизации процессов обеспечения безопасности
СУБД	–	система управления базами данных
УЗ	–	учетная запись
ЭВМ	–	электронно-вычислительная машина

Приложение А
(справочное)
Пример конфигурационного файла для настройки Ankey SIEM NG Event Broker

```
  "transports": [
    {
      "id": "00000000-0000-0000-0000-000000000001",
      "qos": "retain",
      "syslog": {
        "host": "kuu-asap-adm",
        "port": 6514,
        "protocol": "tcp"
        }
    }
  ],
  "rules": [
    {
      "id" : "00000000-0000-0000-0000-000000000001",
      "transports": [
        "00000000-0000-0000-0000-000000000001"
      ],
      "event_type": "norm",
    }
  ]
}
```

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер докум.	Входящий номер сопроводи-тельного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					