GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс

«Система мониторинга и управления событиями безопасности Ankey SIEM Next Generation» v 4.1.2

Руководство оператора

Ankey SIEM NG®

При инсталляции ПК Ankey SIEM NG необходимо ознакомиться с условиями лицензионного соглашения на использование конечным пользователем программы*, согласно которому весь функционал программного комплекса, в том числе отдельные его модули (составляющие)**, носители и документация, предоставляются на условиях «как есть»***.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Дата редакции документа: 3 квартал 2023 года.

* Использование ПК Ankey SIEM NG означает согласие со всеми пунктами лицензионного соглашения.

** ПК Ankey SIEM NG включает в свой состав компоненты платформы, коннекторы (модули сбора и обработки данных) и контент (модули выявления нарушений ИБ (корреляционной обработки данных)).

*** Выполнение основных функций программы (функциональные возможности), предусмотренных (-е) действующей релизной версией. Комплектность, предусмотренная действующей релизной версией изделия. Документация, предусмотренная действующей релизной версией изделия.

Содержание

1 Об этом документе

Руководство оператора содержит пошаговые инструкции и справочную информацию об использовании Ankey SIEM Next Generation (далее также − ПК Ankey SIEM NG) для управления информационными активами организации. В руководстве вы также найдете инструкции по настройке ключевых и дополнительных функций системы для выполнения конкретных задач. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию ПК Ankey SIEM NG.

Руководство адресовано специалистам, ответственным за обеспечение информационной безопасности.

Комплект документации ПК Ankey SIEM NG включает в себя документы, представленные в таблице 1.1.

Таблица 1.1 − Комплект документации ПК Ankey SIEM NG

Каталог	Наименование документа	Описание
Сведения о релизе	Обзор новых возможностей Ankey SIEM NG	Содержит описание изменений между выпускаемой и предыдущей версиями ПК Ankey SIEM NG
Основное	Руководство администратора Ankey SIEM NG	Содержит справочную информацию и инструкции по настройке и администрированию продукта
	Руководство оператора Ankey SIEM NG	Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности
	Руководство по инсталляции Ankey SIEM NG	Содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
	Руководство администрирования Ankey SIEM NG Management and Configuration	Содержит справочную информацию и инструкции по настройке и администрированию компонента Ankey SIEM NG Management and Configuration
	Руководство по настройке Ankey SIEM NG Event Broker	Содержит справочную информацию и инструкции по настройке и администрированию компонента Event Broker
Подключение источников	Руководство по интеграции с источниками Ankey SIEM NG. Описание	Содержит рекомендации по интеграции элементов IT-инфраструктуры организации с ПК Ankey SIEM NG для сбора событий с источников и аудита активов

Каталог	Наименование документа	Описание
	Руководство по интеграции с источниками Ankey SIEM NG. Приложение А	Содержит перечни регистрируемых событий, маппинг событий и результаты обработки для поддерживаемых источников пакета стандартных коннекторов ПК Ankey SIEM NG
	Руководство по интеграции с источниками Ankey SIEM NG. Список изменений	Содержит список изменений пакета стандартных коннекторов ПК Ankey SIEM NG
Настройка корреляции	Пакет общих ресурсов контента <Номер версии пакета>. Описание	Содержит справочную информацию и инструкции по установке и настройке пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет общих ресурсов контента <Номер версии пакета>. Приложение А	Содержит списки применимых правил корреляции из состава пакета общих ресурсов контента ПК Ankey SIEM NG для поддерживаемых источников
	Пакет общих ресурсов контента <Номер версии пакета>. Список изменений	Содержит список изменений пакета общих ресурсов контента ПК Ankey SIEM NG
Дополнительно	Руководство разработчика Ankey SIEM NG	Содержит рекомендации по созданию правил нормализации, корреляции, агрегации и обогащения событий, описание утилит Ankey SIEM NG SDK для их отладки, а также информацию о доступных в Ankey SIEM NG функциях сервиса REST API
	Синтаксис языка запроса PDQL	Содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с Ankey SIEM NG
	PDQL-запросы для анализа активов	Содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в Ankey SIEM NG

В документе приняты условные обозначения.

Таблица 1.2 − Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев,

Пример	Описание
	дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
❖ Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **ОК**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду Stop-Service	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2 О программном комплексе ПК Ankey SIEM NG

Ankey SIEM Next Generation (далее также − Ankey SIEM NG) − это система управления событиями и информацией о безопасности, которая предназначена для сбора, хранения и анализа данных о событиях, которые генерируют различные источники в IT-инфраструктуре организаций. Ankey SIEM NG позволяет обеспечивать мониторинг информационной безопасности как всей инфраструктуры, так и отдельных подразделений, узлов и приложений.

Ankey SIEM NG предоставляет следующие основные возможности:

- **инвентаризация активов**. Система регулярно собирает данные о сетевых узлах и связях между ними;
- **сбор данных о событиях**. В качестве источника событий может выступать любое поддерживаемое оборудование или ПО;
- **анализ событий для выявления инцидентов ИБ**. Набор специальных правил, на основе которых выполняется анализ, постоянно пополняется экспертами ООО «Газинформсервис»;
- **управление инцидентами ИБ**. Система помогает организовать работу по расследованию инцидентов информационной безопасности и устранению их последствий;
- **визуализация данных**. Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.

Ankey SIEM NG предоставляет также дополнительные возможности:

- **пакеты экспертизы.** Использование базы знаний, разработанной экспертами ООО «Газинформсервис». База содержит данные о самых современных тактиках и техниках хакерских атак и помогает выявлять даже сложные нетиповые атаки;
- **автоматизация работы с активами.** Система может автоматически устанавливать значимость активов и сроки актуальности данных об активах, полученных в результате сканирования IT-инфраструктуры;
- **повторная проверка событий.** Ретроспективная корреляция полученных ранее событий после добавления новых правил или обновления данных табличных списков; ретроспективный поиск индикаторов компрометации;
- **отправка уведомлений.** Оповещение ответственных об изменениях в IT-инфраструктурах организаций, о работе задач сбора данных Ankey SIEM NG, собираемых событиях, а также о выявляемых инцидентах ИБ.

3 Вход в ПК Ankey SIEM NG через Ankey SIEM NG MC

Сервис управления пользователями и доступом Ankey SIEM NG Management and Configuration (Ankey SIEM NG MC) обеспечивает механизм единого входа (технология single sign-on) в ПК Ankey SIEM NG.

Перед входом в ПК Ankey SIEM NG запросите у администратора Ankey SIEM NG MC:

- ссылку для входа в интерфейс продукта;
- тип учетной записи (локальная или доменная);
- логин и пароль вашей учетной записи пользователя.

В ПК Ankey SIEM NG реализована ролевая модель управления доступом. Роли определяют доступные для пользователя операции (например, работу с активами), а также объекты (события, активы, инциденты и источники). Подробнее о ролевой модели см. Руководство администратора Ankey SIEM NG 4.1.2.

Перед выполнением инструкции вам нужно убедиться, что в браузере разрешены всплывающие окна.

❖ Чтобы войти в ПК Ankey SIEM NG:

1. В адресной строке браузера введите ссылку для входа в интерфейс ПК Ankey SIEM NG.
   Откроется страница входа в сервис Ankey SIEM NG MC.
2. Выполните одно из следующих действий:
   - если вы входите под локальной учетной записью, то на вкладке **Локальный** укажите логин локальной учетной записи;
   - если вы входите под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи;
3. В поле **Пароль** введите пароль вашей учетной записи.

> **Примечание.** Стандартная сессия пользователя в ПК Ankey SIEM NG длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

Ankey SIEM NG MC проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница со стандартным дашбордом ПК Ankey SIEM NG. Если вы указали неверные данные, отобразится сообщение об ошибке.

4 Интерфейс ПК Ankey SIEM NG

Все действия в Ankey SIEM NG вы можете выполнять с помощью графического пользовательского интерфейса. В этом разделе приводится описание основных элементов интерфейса Ankey SIEM NG, доступных после входа в Ankey SIEM NG.

При входе в ПК Ankey SIEM NG по умолчанию открывается главная страница.

Главная страница содержит главное меню, панель инструментов и рабочую область.

Главное меню обеспечивает доступ к основным функциям ПК Ankey SIEM NG. Главное меню содержит разделы для перехода к страницам ПК Ankey SIEM NG, раздел с данными учетной записи, индикатор состояния ПК Ankey SIEM NG, а также следующие кнопки:

-  – для перехода с любой страницы системы на главную страницу для просмотра статистической информации об активах, уязвимостях, событиях и инцидентах;
-  – для перехода из ПК Ankey SIEM NG в сервис управления пользователями и доступом Ankey SIEM NG Management and Configuration.

На главной странице вам доступна информация, расположенная на виджетах и дашбордах. Виджет − это отдельный графический элемент представления данных, например, гистограмма или таблица. Дашборд − это страница, содержащая набор виджетов. Вы можете:

- просматривать данные на виджетах, сохранять информацию, представленную на диаграммах, в PNG-файл;
- настраивать период времени, за который вам требуется просматривать информацию (по умолчанию каждый виджет содержит статистические данные за последние 24 часа);
- настраивать время автоматического обновления этих данных или обновлять их вручную (по умолчанию время автоматического обновления − 15 минут);
- настраивать виджеты в соответствии с видом представления информации (количественные показатели, диаграммы без распределения данных во времени, диаграммы с распределением данных во времени);
- переходить к просмотру детальной информации, нажимая на элементы виджетов;
- создавать пользовательские дашборды на основе стандартных шаблонов, содержащих разметку для размещения виджетов;
- настраивать состав и расположение пользовательских дашбордов, изменять их названия;
- настраивать состав виджетов на пользовательских дашбордах, выбирая их из библиотеки виджетов;
- менять расположение виджетов на дашборде.

4.1 Главное меню

Главное меню расположено в верхней части страницы и обеспечивает доступ к основным функциям Ankey SIEM NG.

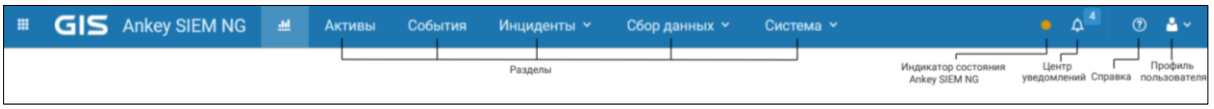

Рисунок 4.1 − Главное меню

Главное меню содержит название системы и следующие элементы:

- кнопку . По кнопке открывается меню для перехода в базу знаний Knowledge Base и в сервис управления пользователями и доступом Ankey SIEM NG Management and Configuration;
- кнопку для перехода на главную страницу с дашбордами;
- разделы для перехода к страницам Ankey SIEM NG. Если раздел объединяет несколько страниц, то у него есть меню. Выбирая пункт меню, вы переходите на нужную страницу;
- индикатор состояния Ankey SIEM NG. По нажатию на индикатор открывается список уведомлений о состоянии системы. Индикатор может показывать следующие состояния:
  – система работает корректно;
  – в системе есть предупреждения;
  – система работает с ошибками;
  – в системе происходит событие, не нарушающее ее работоспособность;
  – не удалось выполнить диагностику системы.
- значок для просмотра сообщений центра уведомлений Ankey SIEM NG. По нажатию на значок открывается список уведомлений. Нажав на уведомление, вы можете открыть окно с подробным описанием. Вы можете удалить одно уведомление или уведомления за день, нажав . Также вы можете очистить список уведомлений, нажав кнопку **Удалить все**, или отключить все уведомления, нажав ;
- кнопку для перехода к справочной информации;
- кнопку . По кнопке открывается меню с именем пользователя Ankey SIEM NG и пунктами **Профиль** для перехода в личный кабинет пользователя в Ankey SIEM NG MC и **Выход** для выхода из системы.

4.2 Панель инструментов

Панель инструментов расположена в верхней части страницы под главным меню. Состав панели инструментов и содержимое рабочей области

зависят от страницы.

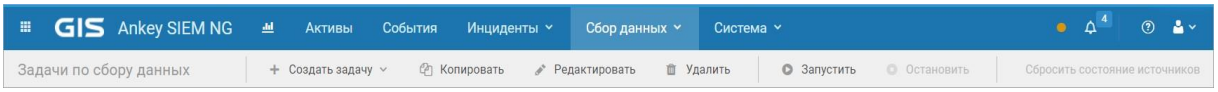

Рисунок 4.2 – Панель инструментов

Панель инструментов содержит кнопки. С их помощью вы можете выполнять действия (в том числе групповые) с данными, представленными в рабочей области. Кнопки могут иметь раскрывающееся меню, объединяющее группу пунктов.

4.3 Рабочая область

Рабочая область расположена на странице под панелью инструментов.

Рабочая область отображает различную информацию о работе системы одним из следующих способов:

- в виде списка. Списки бывают обычные и иерархические. Содержимое некоторых списков вы можете фильтровать;
- в виде таблицы. Например, информация об активах отображается в виде таблицы. Рабочая область может содержать таблицы, в которых вы можете настраивать состав колонок, а также сортировать, группировать и фильтровать записи.

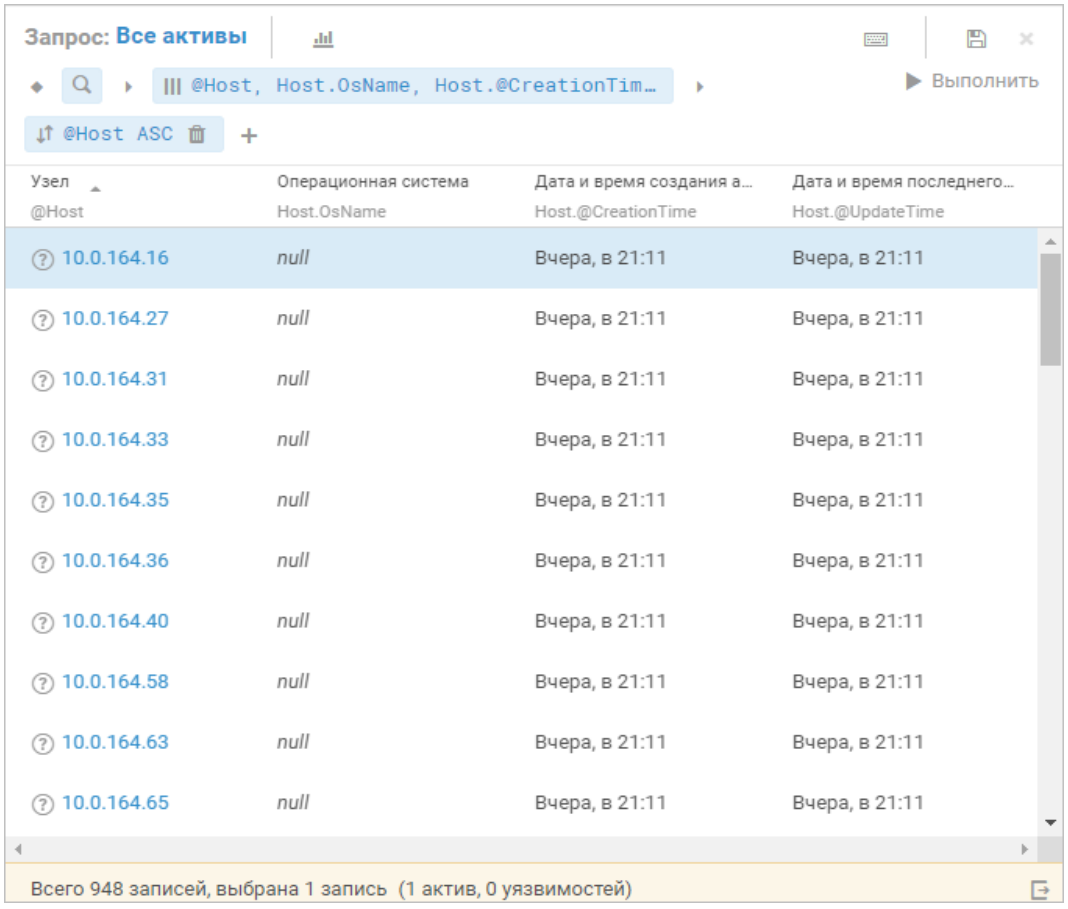

Рисунок 4.3 – Таблица событий

Для дополнительной группировки информации в рабочей области предусмотрены вкладки.

Рабочая область может содержать инструменты, позволяющие настраивать представление информации: панель группировки, панель фильтрации.

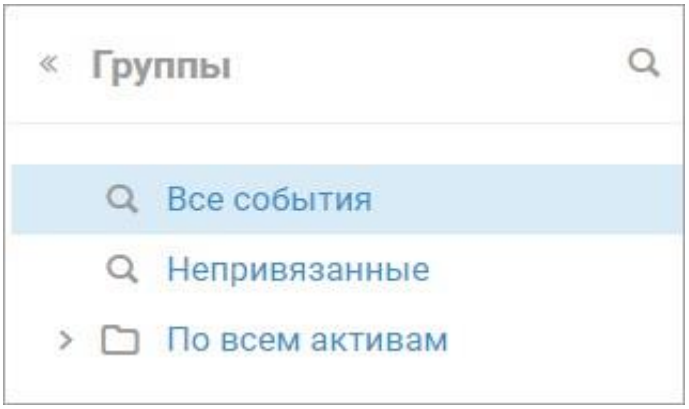

Рисунок 4.4 − Панель группировки событий по активам

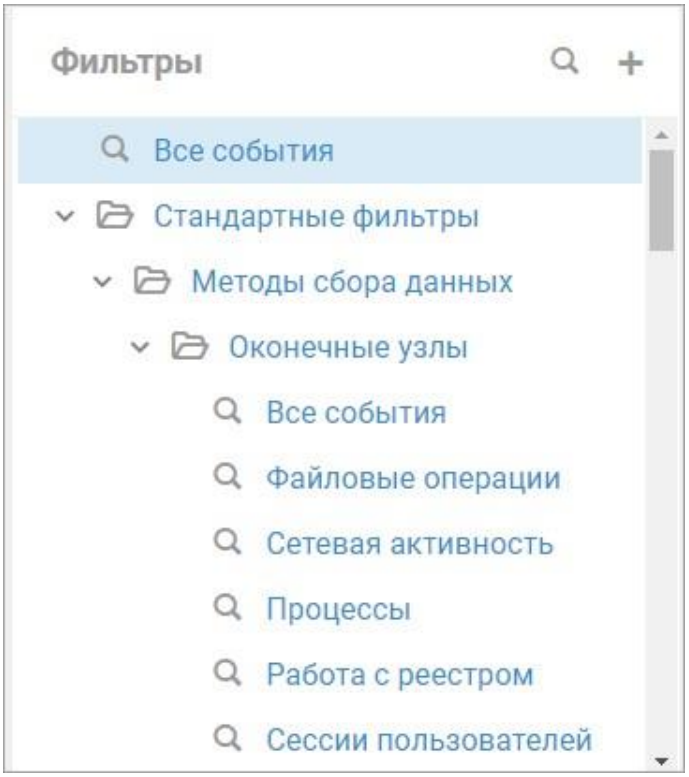

Рисунок 4.5 − Панель **Фильтры**

4.4 Главная страница

При входе в Ankey SIEM NG открывается главная страница.

На главной странице вам доступна информация, расположенная на виджетах и дашбордах. Виджет – это отдельный графический элемент представления данных, например гистограмма или таблица. Дашборд – это страница, содержащая набор виджетов.

Вы можете:

- просматривать данные на виджетах, сохранять информацию, представленную на диаграммах, в PNG-файл;
- настраивать период времени, за который вам требуется просматривать информацию (по умолчанию каждый виджет содержит статистические данные за последние 24 часа);
- настраивать время автоматического обновления этих данных или обновлять их вручную (по умолчанию время автоматического обновления – 15 минут);
- настраивать виджеты в соответствии с видом представления информации (количественные показатели, диаграммы без распределения данных во времени, диаграммы с распределением данных во времени);
- переходить к просмотру детальной информации, нажимая на элементы виджетов;
- создавать пользовательские дашборды на основе стандартных шаблонов, содержащих разметку для размещения виджетов;
- настраивать состав и расположение пользовательских дашбордов, изменять их названия;
- настраивать состав виджетов на пользовательских дашбордах, выбирая их из библиотеки виджетов;
- менять расположение виджетов на дашборде

В рабочей области главной страницы расположен стандартный дашборд **Общая информация**. Он помогает вам отслеживать, сколько активов, событий и инцидентов было в IT-инфраструктуре организации в тот или иной момент. Вы можете просматривать, как менялось их количество и контролировать распространение проблем. Также вы можете ознакомиться с подробной информацией о том, корректно ли настроена система.

Стандартный дашборд **Общая информация** содержит предустановленные виджеты. Вы можете настраивать их, изменять их расположение, перемещать виджеты по дашборду, копировать отдельные виджеты на другой дашборд.

Примечание. При первом входе в систему после установки Ankey SIEM NG виджеты стандартного дашборда будут пустыми, поскольку в системе не зарегистрированы активы и нет информации о собранных событиях и зарегистрированных инцидентах.

Вы можете добавлять дашборды с нужной вам информацией.

Информация на виджетах обновляется автоматически (по умолчанию каждые 15 минут). Также вы можете обновить информацию вручную по кнопке  .

4.5 Страница Активы

На странице **Активы** отображается информация об активах, которые добавлены в систему, а также о группах активов и запросах для фильтрации

активов. По умолчанию отображаются все активы, данные о которых есть в системе, из групп, к которым у вас есть доступ (включая вложенные группы). Данные об активах добавляются в систему с помощью задач по сбору данных.

В рабочей области страницы **Активы** расположены:

- панель **Группы активов** с иерархическим списком групп для категоризации активов. В верхней части панели находятся следующие кнопки:
  - − для создания группы активов;
  - − для просмотра свойств, изменения и удаления группы активов.
- панель **Запросы** со списком PDQL-запросов для фильтрации активов. Список содержит три вида запросов − стандартные, общие и пользовательские. В верхней части панели **Запросы** расположены следующие кнопки:
  - − для поиска запроса по названию;
  - − для создания новой папки с запросами.

Примечание. Вы можете скрывать и раскрывать панели **Группы активов** и **Запросы**, используя « и ».

- панель инструментов над таблицей активов. Вы можете обновить таблицу активов по нажатию или настроить автоматическое обновление таблицы по нажатию . Панель инструментов содержит следующие кнопки:
  - **Добавить актив** − для добавления актива вручную или импорта данных об активе из файла;
  - **Выпустить отчет** − для создания отчетов по активам в формате PDF;
  - **Создать табличный список** − для экспорта данных об активах в табличный список.
- панель фильтрации активов с возможностью формирования PDQL-запроса для фильтрации, сортировки и группировки активов в таблице активов. Вы можете как применять стандартные и общие запросы, так и создавать собственные, сохраняя их для повторного использования.

  Выбрать условия запроса можно по нажатию и .
  Вы можете вручную изменить сохраненный PDQL-запрос. Для выполнения такого запроса нужно нажать кнопку **Выполнить**.
  В панели фильтрации активов также расположены следующие кнопки:
  - − для построения виджета, отображающего собранные данные об активах в виде таблицы, столбчатой диаграммы, графика или круговой диаграммы;
  - − для выбора способа ввода PDQL-запроса (текстом или с помощью графического интерфейса);
  - − для сохранения составленного PDQL-запроса.

– таблица активов, в которой отображаются данные об активах в соответствии с параметрами фильтрации, сортировки и группировки, заданными с помощью PDQL-запроса.
Панель с подробной информацией об активе, который выбран в таблице активов. Панель содержит вкладки **Актив** и **Топология**.
В центре вкладки **Актив** располагается график, отражающий моменты получения новых сведений об активе.
В нижней части располагаются вкладки, которые содержат сводные данные об активе, информацию о программном и аппаратном обеспечении актива, перечень и значения метрик CVSS (Common Vulnerability Scoring System).
В верхней части вкладки **Актив** отображаются сведения о жизненном цикле актива, метрика значимости актива и следующие кнопки:
– для просмотра и изменения расположения актива в группах активов;
– для присвоения активу значимости (не определена, низкая, средняя, высокая);
– для удаления актива из системы;
– для сравнения конфигураций актива, действовавших в разные дни;
– для экспорта истории конфигураций актива в XML-формате;
– для поиска событий, инцидентов и задач по сбору данных;
– для создания задачи по сбору данных;
Расчет достижимости – для расчета достижимости актива (куда есть доступ у актива, откуда есть доступ к активу).
– на вкладке **Топология** отображаются карта сети и связи выбранного актива с другими активами. По кнопке можно выбрать параметры отображения карты сети. На вкладке **Топология** также расположены следующие кнопки:
– для расположения узлов на карте сети по умолчанию;
Расчет достижимости – для расчета достижимости актива (куда есть доступ у актива, откуда есть доступ к активу).

4.6 Страница События

Страница предназначена для работы с событиями, собранными с источников и зарегистрированными ПК Ankey SIEM NG. На странице вы можете искать события по фильтру, анализировать статистику событий и выпускать отчеты по данным событий, регистрировать инциденты по событиям или привязывать события к инцидентам, зарегистрированным ранее.

В таблице событий отображаются следующие типы событий:

– – ненормализованное событие;

– – нормализованное событие;
– – корреляционное событие.

Панель инструментов содержит название страницы, а также ссылки для настройки фильтрации отображаемых на странице событий по периоду регистрации и по группе активов, на которых эти события были зарегистрированы.

В рабочей области страницы расположены:

– панель **Группы** со списком групп активов для поиска событий, которые произошли на активах выбранной группы и вложенных в нее групп. В верхней части панели расположена кнопка для быстрого поиска группы по названию;

> **Примечание.** Вы можете скрыть и открыть панели **Группы** и **Фильтры**, используя « и ».

– панель **Фильтры** со списком стандартных и сохраненных пользовательских фильтров. В верхней части панели расположены кнопки – для быстрого поиска фильтра по названию и – для создания папки для фильтров. При выборе пользовательского фильтра в строке с его названием появляется кнопка . По кнопке раскрывается меню, которое содержит пункты для копирования и удаления фильтра;
– панель с таблицей событий, собранных с источников и зарегистрированных Ankey SIEM NG. В таблице отображаются события, соответствующие всем выбранным условиям фильтрации. Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию – пять минут). В верхней части панели расположены следующие кнопки:
  – **Создать инцидент** – для регистрации инцидента на основании выделенных в таблице событий;
  – **Связать с инцидентом** – для связи выделенных в таблице событий с созданным ранее инцидентом (по его идентификатору);
  – **Выпустить отчет** – для выпуска отчета со статистическими данными о событиях по одному из стандартных шаблонов.
  – **Показать на топологии** – для открытия страницы **Активы** с информацией об активе, на котором зарегистрировано выделенное в таблице событие.

– панель для настройки фильтрации событий. По умолчанию отображаются все события. По ссылке **Все события** вы можете выбрать один из стандартных или пользовательских фильтров, перечисленных в панели **Фильтры**. В панели расположены следующие кнопки:
  – – для выбора предыдущего запроса в списке выполненных запросов.
  – – для выбора следующего запроса в списке выполненных запросов.
  – – для открытия панели История запросов со списком выполненных ранее запросов.

> **Примечание.** В панели **История запросов** вы можете очистить список по кнопке **Очистить историю** или удалить отдельный запрос, нажав в строке запроса. Также вы можете включить отображение только избранных запросов, отмеченных .

  – – для выбора связанных приложений (в случае использования нескольких площадок) и конвейеров обработки событий (если установлено несколько конвейеров);
  – – для перехода к графическому представлению данных из событий;
  – – для настройки фильтрации событий в таблице с помощью запроса на языке PDQL;
  – – для изменения состава колонок таблицы;
  – – для настройки сортировки событий в таблице;
  – – для настройки группировки событий и агрегации данных из событий;
  – – для ограничения количества событий в таблице;
  – **Выполнить** – для применения параметров фильтрации событий;
  – – для сохранения параметров фильтрации как пользовательского фильтра;
  – – для сброса параметров фильтрации событий.
– панель **Сводка** с подробной информацией о событии, которое выбрано в таблице событий. Используя пункты меню, открывающегося при нажатии , вы можете скрывать и раскрывать блоки с полями события. По ссылкам в значениях полей вы можете настраивать фильтры событий.

  Значок показывает, что ПК Ankey SIEM NG скорректировал время события.

Для корреляционного события по ссылке **<Название правила корреляции> из N исходных событий** вы можете открыть страницу с таблицей событий, на основании которых оно было зарегистрировано. Если для правила корреляции настроен механизм обработки ложных срабатываний (и создан шаблон исключений) по ссылке **Добавить исключение** вы можете настроить исключение по данным события.

Для ненормализованного события по кнопке в блоке **Исходное событие** вы можете скопировать исходное событие.

Примечание. Вы можете скрыть и открыть панель **Сводка**, используя « и ».

4.7 Страницы раздела Инциденты

Из раздела **Инциденты** главного меню вы можете открывать страницы для работы с инцидентами:

- **Инциденты** – для просмотра и фильтрации списка инцидентов и подробной информации об инцидентах;
- **Задачи** – для просмотра задач, связанных с инцидентами;
- **Статистика** – для просмотра статистической информации по созданию, закрытию и устранению инцидентов за выбранный отчетный период.

4.7.1 Страница Инциденты

Информация об инцидентах отображается на странице **Инциденты**. На этой странице вы можете:

- создавать, изменять, удалять инциденты;
- экспортировать или импортировать инциденты в унифицированном формате – JSON;
- просматривать на топологии, связанные с выбранным инцидентом активы и сети;
- группировать инциденты.

В рабочей области расположены три панели: **Инциденты**, **Группы и фильтры** и **Сводка**. По умолчанию панели развернуты. Вы можете разворачивать и скрывать панели **Группы и фильтры** и **Сводка**, используя « и ».

Панель **Инциденты** содержит таблицу со списком инцидентов, входящих в выбранную группу, с учетом наложенного фильтра. По умолчанию выбран фильтр **Незакрытые инциденты**.

Для каждого инцидента указан набор параметров:

- **Опасность** – уровень опасности инцидента. Уровень опасности может быть низким, средним или высоким;
- **ID** – идентификационный номер инцидента;
- **Инцидент** – наименование инцидента;

- **Категория** – классификация инцидента по категории. Возможные значения: **Атака**, **Безопасность данных**, **Нарушение политик ИБ**, **Нарушение работоспособности**, **Не определена**, **Неавторизованный доступ**, **Обнаружение вредоносного ПО**, **Управление уязвимостями**;
- **Тип** − классификация инцидента по типу. Тип инцидента зависит от присвоенной ему категории;
- **Статус** − статус инцидента. Возможные значения: **Новый**, **Утвержден**, **Разрешен**, **Закрыт**, **Закрыт (ложное срабатывание)**;
- **Создан** − день и время создания инцидента;
- **Ответственный** − пользователь системы, который назначен ответственным за инцидент.

Панель **Группы и фильтры** делится на две части: **Инциденты** и **Фильтры**.

В части **Инциденты** отображаются варианты группировки инцидентов:

- **Все инциденты**;
- **Непривязанные инциденты**;
- **Мои инциденты**;
- **По группам активов**.

В части **Фильтры** отображаются варианты фильтров, которые позволяют выполнять поиск инцидентов по определенным параметрам:

- **Все инциденты**;
- **Стандартные фильтры**;
- **Пользовательские фильтры**.

Панель **Сводка** содержит подробную информацию о выбранном инциденте, о расположении инцидента на топологии и об истории инцидента.

4.7.2 Страница Задачи

Все задачи, связанные с инцидентами, отображаются на странице **Задачи**. На этой странице вы можете:

- сортировать список задач;
- просматривать подробную информацию по выбранной задаче;
- изменять задачу.

В рабочей области расположены три панели: **Задачи**, **Группы** и **Сводка**. По умолчанию панели развернуты. Вы можете разворачивать и скрывать панели **Задачи** и **Сводка**, используя « и ».

Панель **Задачи** содержит таблицу задач, связанных с инцидентами.

Для каждой задачи указан набор параметров:

- **Название** − наименование задачи;
- **Тип** − тип задачи. Возможные значения: **Расследование**, **Сбор доказательств**, **Восстановление**;
- **Статус** − статус задачи. Возможные значения: **Новая**, **Назначена**, **В работе**, **Закрыта**;
- **Ответственный** − пользователь системы, который назначен ответственным за выполнение задачи;
- **Дедлайн** − дата и время, к которому задача должна быть выполнена.

Панель **Группы** содержит группы задач по инцидентам.

Панель **Сводка** содержит сводную информацию о выбранной задаче:

- ссылку с идентификатором (ID) задачи и ее названием. Идентификатор задачи выглядит следующим образом: **TASK-<порядковый номер, отображающий последовательность создания задач в системе>**. По ссылке с идентификатором и названием задачи доступен переход в карточку задачи;
- параметры задачи − номер и название инцидента, по которому поставлена задача, тип задачи, время, к которому задача должна быть выполнена;
- статус задачи − текущий статус задачи, автор задачи, ответственный по задаче;
- описание задачи − подробное текстовое описание задачи.

4.7.3 Страница Статистика

Статистика по инцидентам отображается на странице **Статистика**. Вы можете просматривать собранную ПК Ankey SIEM NG статистику:

- общее количество новых инцидентов с распределением по времени;
- общее количество закрытых инцидентов с распределением по времени;
- общее количество инцидентов, не закрытых на начало заданного периода;
- общее количество незакрытых инцидентов с распределением по времени и по уровню опасности инцидентов;
- среднее время устранения инцидентов с распределением по времени.

В окне статистики представлены три диаграммы. Каждую диаграмму вы можете рассматривать подробнее по кнопке **Увеличить**, изменять временной интервал диаграммы. Вы можете отсортировать статистические данные для диаграмм:

- по группам, используя фильтр **По группам**;
- за указанный период, используя временной фильтр: по дням, неделям, месяцам или кварталам.

Также вы можете отсортировать статистические данные, настроив на диаграмме период:

- последние 30 дней;
- текущая и предыдущая неделя;
- текущий и предыдущий месяц;
- текущий и прошедший квартал;
- текущий и предыдущий год.

По умолчанию данные на диаграммах обновляются раз в 5 минут.

Диаграмма **Созданные инциденты** показывает количество инцидентов, созданных за указанный период. Чтобы узнать точное количество созданных инцидентов, наведите курсор мыши на одну из областей диаграммы.

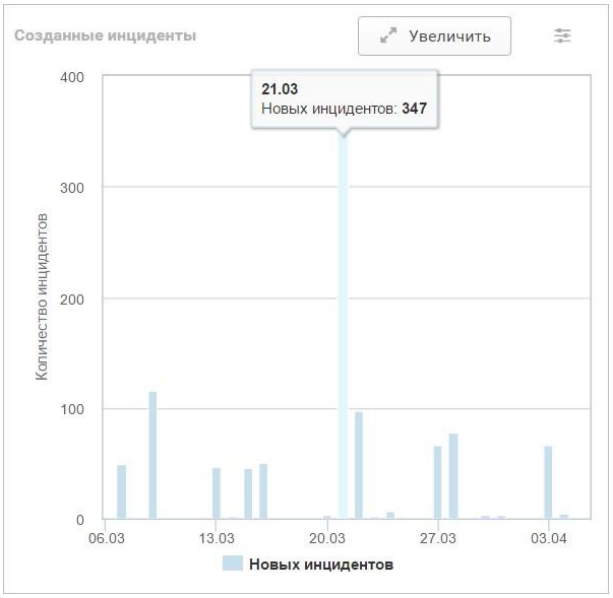

Рисунок 4.6 − Созданные инциденты

Диаграмма **Закрытые инциденты за период** позволяет отслеживать количество инцидентов, не закрытых на начало периода, и количество инцидентов, закрытых за период.

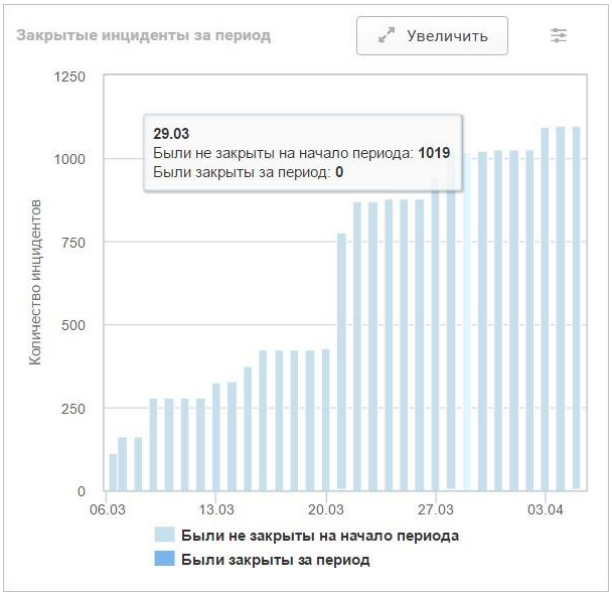

Рисунок 4.7 − Закрытые инциденты за период

Диаграмма **Незакрытые инциденты по уровню опасности** показывает количество незакрытых инцидентов, сгруппированных по уровню опасности. Степень опасности может быть высокой, средней или низкой. Каждая степень обозначена соответствующим цветом: красным, желтым, синим.

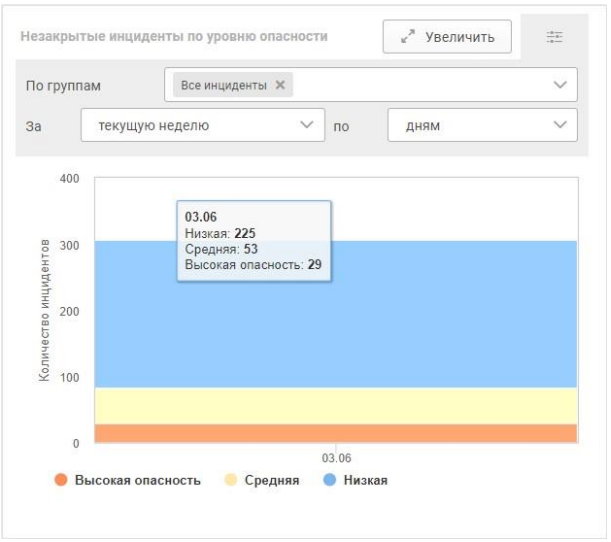

Рисунок 4.8 − Незакрытые инциденты по уровню опасности

На странице **Статистика** отображается среднее время устранения инцидента в выбранном периоде. Период вы можете выбрать по кнопке в панели **Среднее время устранения инцидента**.

4.8 Страницы раздела Сбор данных

Используя пункты раздела **Сбор данных** главного меню, вы можете открывать страницы для настройки сбора событий с источников, аудита активов и тонкой настройки анализа полученных данных.

4.8.1 Страница Задачи по сбору данных

На странице **Задачи по сбору данных** вы можете создавать, копировать, изменять и удалять задачи, запускать и останавливать их выполнение.

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать задачу** − по кнопке раскрывается меню, которое содержит пункты для создания задач по сбору событий и данных об активах, импорта событий из файла журнала и проверки событий;
- **Копировать** − для копирования выбранной задачи;
- **Редактировать** − для изменения параметров выбранной задачи;
- **Удалить** − для удаления выбранной задачи;
- **Запустить** − для запуска выбранного задачи;
- **Остановить** − для остановки выбранной задачи;
- **Сбросить состояние источников** − по кнопке в выбранных задачах все события в журналах источников считаются новыми. Вы можете сбросить состояние источников только для задач по сбору данных из хранилищ со статусом **Завершена**.

В рабочей области страницы расположены:

- панель **Статусы** со списком фильтров по статусам задач;
- панель **Типы задач** со списком фильтров по типу задач;

Примечание. Вы можете скрывать и раскрывать боковые панели, используя с

– панель **Все задачи**, содержит таблицу с задачами.

При нажатии в верхней части панели открывается поле для быстрого поиска задач по названию задачи, агента, учетной записи, транспорта, профиля или модуля; по IP-адресу или FQDN цели задачи.

При нажатии открывается панель для настройки фильтра задач.

Примечание. Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию − пять минут).

В таблице в колонке **Статус** отображается статус задачи. Существуют следующие статусы:

– **Не запускалась**.
  − задача ни разу не запускалась;
– **Подготавливается**. Создается запуск задачи. Создаются подзадачи;
– **Ожидает выполнения**. Отправлен запрос о назначении подзадач на Ankey SIEM NG Agent. Подзадачи будут запущены в порядке очереди.
  − все подзадачи назначены.
  − часть подзадач не назначены.
– **Выполняется**. Хотя бы одна подзадача запущена на Ankey SIEM NG Agent. Идет процесс сбора данных.
  − нет подзадач, завершенных с ошибками.
  − часть подзадач завершены с ошибкой.
– **Завершается**. После остановки задачи вручную пользователем отправлен запрос об остановке подзадач на Ankey SIEM NG Agent.
  − нет подзадач, завершенных с ошибками.
  − часть подзадач завершены с ошибкой.
– **Завершена**. Подзадачи завершены.
  − все подзадачи завершены без ошибок.
  − часть подзадач завершена с ошибками.
  − задача была остановлена или не может быть выполнена.
– панель **<Название задачи>**, содержит информацию о выбранной задаче.
  По ссылке **Перейти** в строке **Собранные события** вы можете просматривать список событий, полученных по этой задаче.
  По ссылке **История запусков** вы можете просматривать историю запусков задачи и журналы подзадач.

4.8.1.1 Страница История запусков <Название задачи>

На странице **История запусков <Название задачи>** вы можете просматривать историю запусков задачи и список подзадач, созданных при каждом запуске.

В рабочей области страницы расположены:

- панель **Сводка** с подробной информацией о задаче;

> **Примечание.** Вы можете скрывать и раскрывать панель, используя « и ».

- панель с историей запусков задачи.
  В верхней части панели расположены кнопки – для выбора даты запуска и – для фильтрации запусков с ошибками;
- панель **Подзадачи**, содержит таблицу с подзадачами, а также следующие кнопки:
  - **найти события** – по кнопке вы можете открыть страницу с событиями, собранными по выбранной подзадаче;
  - **скачать журнал** – по кнопке вы можете скачать файл с журналом выбранной подзадачи;
  - **журнал подзадачи** – по кнопке вы можете открыть страницу журнала выбранной подзадачи.

> **Примечание.** Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию – пять минут).

В таблице в колонке **Статус** отображается статус подзадачи. Существуют следующие статусы:

Создана;

Назначена – назначен Ankey SIEM NG Agent для выполнения;

Ожидает выполнения;

Выполняется;

Завершается;

Завершена – подзадача завершена без ошибок;

Завершена – подзадача завершена с ошибками.

> **Примечание.** Подзадача завершается с ошибкой, если, например, указаны неверные учетные данные, цель сбора данных недоступна или не собрано никаких данных. Более подробная информация доступна в журнале подзадачи (см. раздел 7.4.5).

4.8.1.2 Страница Журнал подзадачи <Время>

На странице **Журнал подзадачи <Время>** вы можете просматривать сообщения и подробную информацию об ошибках подзадачи.

Панель инструментов содержит название страницы, а также следующие кнопку **Остановить задачу** для остановки задачи, для которой создана выбранная подзадача.

Примечание. Вы можете обновить данные на странице нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию − пять минут).

В рабочей области страницы расположены:

- панель **Подзадача** с подробной информацией о выбранной задаче.
  вы можете скрывать и раскрывать боковые панели, используя « и ».;
- панель **Журнал** со списком сообщений об ошибках подзадачи. По кнопке **Скачать журнал** вы можете скачать файл с журналом подзадачи;
- панель **Сводка** с подробной информацией о выбранной ошибке.

4.8.2 Страница Профили

На странице **Профили** вы можете создавать пользовательские профили на базе стандартных, изменять и удалять их.

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать** − по кнопке раскрывается меню, которое содержит пункты для создания пользовательского профиля на базе стандартного и для создания профиля для поиска выбранных уязвимостей;
- **Редактировать** − для изменения параметров выбранного пользовательского профиля;
- **Удалить** − для удаления выбранного пользовательского профиля.

В рабочей области страницы расположены:

- панель **Профили** для фильтрации профилей по собираемым данным или названиям модулей, для которого они созданы;

  Примечание. Вы можете открыть и скрыть панели **Профили** и **Сводка**, используя «и ».

- панель **Список профилей** с таблицей профилей. Для каждого профиля в таблице указаны название, базовый профиль, название модуля и тип (стандартный или пользовательский);

– панель **Сводка**, содержит информацию о выбранном профиле.
По ссылке **Перейти** в строке **Задачи с этим профилем** вы можете просматривать список задач, созданных с выбранным профилем.
По кнопке **Параметры** вы можете просматривать параметры профиля.

4.8.3 Страница Учетные записи

На странице **Учетные записи** вы можете добавлять, изменять и удалять учетные записи (см. раздел 7.1).

Панель инструментов содержит название страницы, а также следующие кнопки:

– **Добавить учетную запись** − по кнопке раскрывается меню, которое содержит пункты для создания учетных записей различных типов («логин−пароль», «пароль» или «сертификат»);
– **Редактировать** − для изменения параметров выбранной учетной записи;
– **Удалить** − для удаления выбранной учетной записи.

В рабочей области страницы расположены:

– панель для выбора учетной записи. Содержит список добавленных учетных записей. Для учетных записей указаны тип и транспорт, для которого она добавлена;
– панель **<Название учетной записи>**. Содержит информацию о выбранной учетной записи;
– по ссылке **Перейти** в строке **Задачи с этой учетной записью** вы можете просматривать список задач, созданных с выбранной учетной записью.

Примечание. Вы можете открыть и скрыть панель, используя « и ».

4.8.4 Страница Справочники

На странице **Справочники** вы можете создавать, изменять и удалять пользовательские справочники (см. раздел 7.2).

Панель инструментов содержит название страницы, а также следующие кнопки:

– **Создать** − для создания пользовательского справочника;
– **Редактировать** − для изменения выбранного пользовательского справочника;
– **Удалить** − для удаления выбранного пользовательского справочника.

В рабочей области страницы расположены:

– панель **Группы справочников**. Содержит список групп справочников;
– панель для выбора справочника. Содержит список справочников в выбранной группе;

– панель **<Название справочника>**. В панели отображается содержимое выбранного справочника.

Примечание. Вы можете открыть и скрыть панели **Группы справочников** и **<Название справочника>**, используя « и ».

4.8.5 Страница Правила корреляции

Страница предназначена для просмотра статистики срабатывания правил корреляции, включения и отключения правил.

Панель инструментов содержит название страницы, а также следующие кнопки:

– **Включить** – для включения выбранного в таблице правила;
– **Отключить** – для отключения выбранного в таблице правила.

В рабочей области страницы расположены:

– Панель **Список правил корреляции**, содержит таблицу с правилами корреляции. Если установлено несколько конвейеров обработки событий, справа от названия панели отображается ссылка для выбора конвейера. После выбора конвейера в таблице появятся установленные в него правила.

Примечание. Вы можете выбрать колонки, отображаемые в таблице, по кнопке в строке заголовков колонок.

Для правил в таблице указаны статус, идентификатор, название, категория регистрируемого события ИБ, тип правила (стандартное или пользовательское) и количество срабатываний за сутки. Кроме того, вы можете добавить в таблицу колонки с количеством собираемых по правилам цепочек событий в памяти Ankey SIEM NG Server и общим числом событий в этих цепочках;

Примечание. Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию – пять минут).

При нажатии в верхней части страницы открывается поле для поиска правила по названию. По ссылке в таблице вы можете открыть страницу в Ankey SIEM NG Knowledge Base с кодом правила.

Существуют следующие статусы правил:

Включено – правило используется для корреляции событий;

Отключается, **Включается** − временные статусы;

Приостановлено − правило автоматически остановлено на основании результатов мониторинга работы правил корреляции ПК Ankey SIEM NG;

Отключено − правило не используется для корреляции событий;

Ошибка валидации − при валидации правила обнаружены ошибки, оно не может использоваться для корреляции событий.

– панель **Сводка**, содержит информацию о выбранном в таблице правиле.

Примечание. Вы можете открыть и скрыть панель, используя « и ».

4.8.6 Страница Правила обогащения

Страница предназначена для включения и отключения правил обогащения.

Панель инструментов содержит название страницы, а также следующие кнопки:

– **Включить** − для включения выбранного в таблице правила;
– **Отключить** − для отключения выбранного в таблице правила.

В рабочей области страницы расположены:

– панель **Список правил обогащения**, содержит таблицу с правилами обогащения. Если установлено несколько конвейеров обработки событий, справа от названия панели отображается ссылка для выбора конвейера. После выбора конвейера в таблице появятся установленные в него правила.

Для каждого правила в таблице указаны статус, идентификатор, название и тип (стандартное или пользовательское). По ссылке в таблице вы можете открыть страницу с кодом правила.

При нажатии в верхней части страницы открывается поле для поиска правила по названию;

Примечание. Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию − пять минут).

Существуют следующие статусы правил:

Включено − правило используется для обогащения событий;

Отключается, **Включается** − временные статусы;

Отключено – правило не используется для обогащения событий;

Ошибка валидации – при валидации правила обнаружены ошибки, оно не может использоваться для обогащения событий.

– панель **Сводка**, содержит информацию о выбранном в таблице правиле.

Примечание. Вы можете открыть и скрыть панель, используя « и ».

4.8.7 Страница Табличные списки

Страница предназначена для просмотра записей табличных списков и работы с записями табличных списков для правил корреляции и обогащения (если такая возможность была предусмотрена при создании табличного списка).

Если установлено несколько конвейеров обработки событий, справа от названия панели отображается ссылка для выбора конвейера. После выбора конвейера на странице появятся установленные в него табличные списки.

В рабочей области страницы расположены:

– панель **Табличные списки**. Содержит доступные табличные списки.

При нажатии в верхней части страницы открывается поле для поиска табличного списка по названию. При нажатии появляется раскрывающийся список для фильтрации табличных списков по назначению;

Примечание. Вы можете открыть и скрыть панель **Табличные списки**, используя « и ».

– панель **<Название табличного списка>**. Содержит параметры выбранного табличного списка и записи табличного списка.

Примечание. Вы можете обновить записи табличного списка нажатием и настроить автоматическое обновление записей в меню, открывающемся при нажатии (по умолчанию – пять минут).

Блок с записями табличного списка содержит кнопку **Экспорт** для сохранения записей в файле формата CSV. Для табличных списков для правил корреляции и обогащения доступны кнопки для работы с записями:

– **Редактировать содержимое** – для добавления, удаления и изменения записей;
– **Очистить табличный список** – для удаления всех записей;

- **Импорт** – для добавления записей из файла формата CSV;
- **Экспорт** – для сохранения записей в файл формата CSV.

Для любого табличного списка вы можете построить табличный виджет по кнопке  .

4.8.8 Страница Мониторинг источников

Источники и форвардеры появляются в системе автоматически, по мере сбора событий с активов и их идентификации. На странице **Мониторинг источников** пользователь системы может просмотреть состояние источников (см. раздел 7.6.1) и параметры потока данных от них или состояние форвардеров (см. раздел 7.6.2) и параметры находящихся в них источников. Ссылка для выбора типа элементов (источников или форвардеров) находится в верхней части рабочей области страницы.

Если вы выбрали по ссылке работу с источниками, рабочая область страницы **Мониторинг источников** содержит:

- панель **Источники** для поиска источников, которые находятся на активах выбранной группы и вложенных в нее групп;
- панель **Фильтры** для фильтрации источников по условию наличия или отсутствия предупреждений;
- панель управления с возможностью экспортировать и обновлять список источников, искать источники в списке;
- центральную панель с таблицей источников, а также со ссылкой для настройки периода отображения (по времени последнего получения данных от источника).

Если вы выбрали по ссылке работу с форвардерами, рабочая область страницы **Мониторинг источников** содержит:

- панель **Форвардеры** для поиска форвардеров, которые содержатся в выбранной группе активов и вложенных в нее группах;
- панель **Фильтры** для фильтрации форвардеров по условию наличия или отсутствия предупреждений;
- панель управления с возможностью экспортировать и обновлять список форвардеров, искать форвардеры в списке;
- центральную панель с таблицей форвардеров, а также со ссылкой для настройки периода отображения (по времени последнего получения данных от форвадера).

Примечание. По умолчанию на странице **Мониторинг источников** отображаются все источники (форвардеры), связанные с группами активов, к которым оператору предоставлен доступ.

4.9 Страницы раздела Система

Используя пункты раздела **Система** главного меню, вы можете открывать страницы для работы со всеми отчетами, созданными в ПК Ankey SIEM NG;

результатами мониторинга обработки событий; списками проверок, позволяющих правильно настроить ПК Ankey SIEM NG; информацию о состоянии ПК Ankey SIEM NG.

4.9.1 Страница Отчеты

Все отчеты, созданные в системе, отображаются на странице **Отчеты** (**Система** → **Отчеты**). На этой странице вы можете:

- создавать, копировать, изменять или удалять задачи по выпуску отчетов;
- выпускать отчеты и настраивать расписание выпуска отчетов;
- скачивать отчеты (см. раздел 12.6).

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать** – для создания задачи по выпуску отчета;
- **Копировать** – для копирования параметров выбранной задачи по выпуску отчета;
- **Редактировать** – для изменения параметров выбранной задачи по выпуску отчета;
- **Удалить** – для удаления выбранной задачи по выпуску отчета;
- **Выпустить** – для выпуска отчета;
- **Расписание** – по кнопке раскрывается меню, которое содержит пункты для управления расписанием выпуска отчета.

Рабочая область страницы **Отчеты** содержит:

- таблицу задач по выпуску отчетов, в которой отображается подробная информация обо всех таких задачах;
- панель **История выпусков**, в которой отображается информация о дате и времени выпуска отчета, а также о доступности отчета для скачивания;
- панель **Сводка** с подробной информацией о задаче по выпуску отчета, которая выбрана в таблице задач по выпуску отчетов.

Вы можете скрывать и раскрывать панель **Сводка**, используя » и «.

4.9.2 Страница Уведомления

Страница **Уведомления** позволяет работать с задачами для отправки уведомлений. В панели инструментов страницы находятся следующие кнопки:

- **Создать** – для создания задачи;
- **Копировать** – для создания задачи на основе существующей задачи (см. раздел 13.9);
- **Редактировать** – для изменения параметров задачи (см. раздел 13.10);
- **Удалить** – для удаления задачи (см. раздел 13.11);
- **Остановить** – для остановки задачи (см. раздел 13.8);
- **Запустить** – для запуска задачи после ее остановки (см. раздел 13.8).

Примечание. После создания задачи она запускается автоматически.

В рабочей области страницы расположены:

- панель **Типы уведомлений**. Содержит перечень разделов по типам объектов, для которых доступно создание задач. При выборе типа в центральной панели отобразятся задачи, созданные для объектов этого типа;
- центральная панель. Содержит таблицу с задачами;
- панель **<Название задачи>**. Содержит данные о выбранной задаче.

4.9.3 Страница Политики

На странице **Политики** вы можете просматривать политики – наборы правил, по которым активы автоматически проверяются и обрабатываются. Политики позволяют указать сроки актуальности данных, полученных при помощи сканирования активов методом аудита или пентеста.

В рабочей области страницы **Политики** отображается:

- панель **Список политик**, содержащая перечень доступных политик. Политика может стать недействующей, если в правилах этой политики появились ошибки. Такое правило в таблице правил будет отмечено значком  ;
- панель инструментов с возможностью создавать, изменять, копировать, удалять, включать и отключать правила;

Примечание. Для настройки политик требуются права администратора.

- панель с таблицей правил выбранной политики. Правила внутри политики применяются согласно установленному порядку. Правила могут быть  стандартными и  пользовательскими;
- панель **Сводка** со сводной информацией о состоянии правила, результатах его применения и о группах активов, для которых установлено правило.

Примечание. Вы можете скрывать и раскрывать боковые панели, используя и  .

4.9.4 Страница Управление системой

На странице **Управление системой** отображается информация о состоянии компонентов Ankey SIEM NG.

Рабочая область страницы **Управление системой** содержит панель **Компоненты** с разделами **О системе**, **Агенты** и **Обработка активов**.

Раздел О системе

В разделе **О системе** вы можете просматривать информацию о лицензии и версии компонента Ankey SIEM NG Core. Для корректной работы Ankey SIEM

NG необходима действующая лицензия.

Раздел Конвейеры

В разделе **Конвейеры** вы можете просматривать информацию о конвейерах Ankey SIEM NG Server, которые обеспечивают обработку событий в системе.

Панель инструментов содержит кнопку **Переименовать** для изменения псевдонима конвейера и кнопку **Удалить** для удаления недоступного конвейера из списка.

В рабочей области страницы отображается таблица со списком конвейеров. Для каждого конвейера в таблице указаны статус, псевдоним, версии установленной системы и схемы полей событий, имя узла, IP-адреса и семейство ОС сервера. Вы можете сортировать список, нажимая на названия колонок таблицы. Нажатием вы можете обновить информацию о конвейерах. При выборе конвейера система отображает подробную информацию о нем в боковой панели с названием конвейера.

Примечание. Вы можете скрывать и раскрывать боковые панели, используя « и ».

В колонке **Статус** отображается статус конвейера:

- **Доступен** − конвейер работает в нормальном режиме;
- **Недоступен** − Ankey SIEM NG Core не получает отклика от конвейера более 10 минут.

Раздел Агенты

В разделе **Агенты** вы можете просматривать информацию о Ankey SIEM NG Agent, который обеспечивает поступление данных в систему.

Панель инструментов содержит кнопку **Обновить версию** для обновления версии агента и кнопку **Удалить** для удаления недоступного агента из списка.

В рабочей области страницы отображается таблица со списком агентов. Для каждого агента в таблице указаны название, версия, статус, роли, а также IP-адреса и семейство ОС сервера. Вы можете сортировать список, нажимая на названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая в правой верхней части таблицы. Для поиска агента в списке вы можете нажать и ввести в поле для поиска параметр агента. При выборе агента система отображает подробную информацию о нем в боковой панели с названием агента.

Примечание. Вы можете скрывать и раскрывать боковые панели, используя » и «.

В колонке **Статус** отображается статус агента:

- **Доступен** – агент работает в нормальном режиме;
- **С ограничениями** – агент работает в режиме ограниченной функциональности по причине нехватки свободного дискового пространства (величина свободного дискового

пространства для каждого агента задается администратором системы);
- **Недоступен** – Ankey SIEM NG Core не получает отклика от агента более 10 минут;
- **Удаляется** – агент удаляется из списка.

Раздел База знаний

В разделе **База знаний** вы можете просматривать информацию о подключенной базе знаний. Панель инструментов содержит кнопку **Обновить** для обновления версии базы знаний.

Настройка компонентов системы описана в Руководстве администратора Ankey SIEM NG 4.1.2.

Раздел Обработка активов

В разделе **Обработка активов** вы можете просматривать информацию о работе служб Ankey SIEM NG Core на различных этапах обработки данных об активах.

Для каждого этапа в таблице указаны название используемой службы, длина очереди, время ожидания обработки, номера пакетов в очереди, номера последних обработанных пакетов и средняя скорость обработки пакетов за 5 минут. Вы можете обновить данные в таблице нажатием и настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию – пять минут).

4.9.5 Страница Чек-лист настройки системы

После установки ПК Ankey SIEM NG на странице **Чек-лист настройки системы** вы можете уточнить, какие параметры необходимо настроить в системе с учетом специфики IT-инфраструктуры вашей организации. Также в процессе работы с ПК Ankey SIEM NG вы можете проверять, корректно ли настроена система.

В рабочей области страницы **Чек-лист настройки системы** отображается:
- панель **Список проверок** со списком и статусом всех проверок, с возможностью искать и фильтровать проверки;
- панель инструментов с возможностью запускать проверку или исключать ее из списка;
- описание отдельной проверки и необходимых шагов по настройке системы.

Для удобства проверки сгруппированы. Напротив каждой группы отображается количество пройденных в этой группе проверок.

5 Интерфейс Ankey SIEM NG Knowledge Base

Раздел содержит описание страниц веб-интерфейса Ankey SIEM NG Knowledge Base.

5.1 Главное меню

Главное меню расположено в верхней части любой страницы Ankey SIEM NG Knowledge Base.

Главное меню содержит следующие кнопки:

- кнопку для перехода в ПК Ankey SIEM NG и в Ankey SIEM NG MC;
- кнопку для перехода на страницу **Статистика**;
- кнопку для перехода на страницу с информацией о версии ядра и веб-интерфейса Ankey SIEM NG Knowledge Base;
- кнопку для выбора языка интерфейса и для выхода из системы.

Главное меню содержит следующие разделы:

- **<Название БД>** – содержит пункт **Базы данных** для перехода на страницу для работы с БД Ankey SIEM NG Knowledge Base и пункты для выбора БД. Пункт стандартной БД всегда отмечен значком, пункт установочной БД – значком;
- **SIEM** – содержит пункты для перехода на страницы для работы с пакетами экспертизы и создания объектов для обработки и анализа данных, для работы с макросами, на страницы для просмотра схемы полей событий и журнала установки объектов в ПК Ankey SIEM NG и на страницу для просмотра используемых версий SDK и выбора версии SDK для валидации объектов.

5.2 Страница Статистика

При входе в веб-интерфейс Ankey SIEM NG Knowledge Base открывается страница **Статистика**, которая предназначена для отслеживания изменения количества объектов в используемой БД.

В верхней части рабочей области страницы расположены ссылки для выбора БД и периода времени для просмотра изменения количества объектов, а также кнопки для включения и отключения линии того или иного типа объектов БД на графике. На каждой кнопке указаны тип объекта, количество объектов в БД на текущий момент и маркер линии для типа объекта на графике.

В нижней части рабочей области страницы расположен график зависимости количества объектов в БД от времени (за указанный период).

5.3 Страница Базы данных

Страница предназначена для работы с БД Ankey SIEM NG Knowledge

Base.

Панель инструментов содержит название страницы, а также следующие кнопки для работы с БД, выбранной в панели **Базы данных**:

- **Создать ветку** − для создания дочерней пользовательской БД;
- **Сделать установочной** − для назначения установочной базы и установки объектов БД в ПК Ankey SIEM NG;
- **Импорт ревизий** − для импорта изменений из родительской БД;
- **Загрузить обновления** − для загрузки обновлений из файла (доступна только для стандартной БД);
- **Управление** − по кнопке раскрывается меню, которое содержит пункты для изменения параметров БД и удаления пользовательской БД.

В рабочей области страницы расположены:

- панель **Базы данных**. Содержит иерархический список БД. Стандартная неизменяемая БД является корневым элементом списка и отмечена значком . Установочная БД отмечена в списке значком . Рядом с названиями БД указано количество ревизий родительской БД, изменения из которых доступны для импорта;

Примечание. Вы можете скрыть и открыть панель **Базы данных**, используя « и ».

- панель для работы с БД. Содержит параметры и список ревизий БД, выбранной в панели **Базы данных**. Для каждой ревизии указаны имя пользователя, который изменил БД, дата и время изменения. При выборе ревизии появляются кнопки **Сравнение по объектам** для сравнения ревизий БД и кнопка **Слияние** для экспорта изменений выбранной БД в родительскую (кнопка недоступна, если родительской является стандартная БД). Рядом с кнопкой **Слияние** отображается количество ревизий, изменения из которых доступны для экспорта в родительскую БД.

Примечание. Администратору Ankey SIEM NG Knowledge Base доступны ревизии БД, созданные всеми пользователями, оператору − только ревизии, созданные им самим.

5.4 Страница Пакеты экспертизы

Страница предназначена для работы с правилами и табличными списками, которые используются для обработки и анализа данных в Ankey SIEM NG.

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать** – для создания пользовательских правил корреляции, обогащения, агрегации, нормализации и табличных списков;
- **Установить в SIEM** – для установки объектов в конвейеры обработки событий;
- **Импорт** – для импорта объектов БД.

В рабочей области страницы расположены:

- панель **Папки**. Содержит доступные пакеты экспертизы и папки, созданные для хранения объектов в БД. При выборе пакета экспертизы (папки) в таблице отображается список объектов, при выборе отдельного объекта – страница объекта.

  По кнопке вы можете настроить отображение в таблице объектов из вложенных папок.

  По кнопке вы можете создать пакет экспертизы (папку) для хранения объектов в БД.

  Примечание. Вы можете скрыть и открыть одновременно обе панели **Папки** и **Наборы для установки**, используя « и ».

  При наведении курсора на пакет экспертизы (папки) в строке с его названием появляется кнопка . По кнопке раскрывается меню, которое содержит пункты для изменения, удаления пользовательского пакета экспертизы (папки) и создания вложенной папки;
- Панель **Наборы для установки**. Содержит наборы для установки объектов в конвейеры обработки событий. При выборе набора в таблице отображается список добавленных в него объектов. По умолчанию в панели находится стандартный набор **Все объекты**.

  По кнопке вы можете создать новый набор. При наведении курсора на строку с названием набора в правой части строки появляется кнопка , по нажатию которой раскрывается меню для изменения, копирования и удаления набора, валидации и экспорта его объектов, а также для создания вложенного набора.

  В строке с названием набора отображается значок статуса валидации его объектов:

  – валидация выполнена успешно;

  – валидация не выполнялась или объекты в наборе были изменены после валидации;

  – при валидации возникли ошибки.

Если в главном меню выбрана установочная БД, в строке с названием набора также отображается значок статуса установки его объектов:

– все объекты установлены;

– некоторые установленные объекты неактуальны, поскольку они обновлены в пакетах экспертизы установочной БД;

– не все объекты установлены;

– ни один объект из набора не установлен – вследствие смены установочной БД или вовсе никогда не устанавливались.

– вкладка **<Название пакета экспертизы (папки)>**, содержит таблицу со списком объектов. В таблице отображаются объекты пакета экспертизы (папки), выбранного в панели **Папки**, которые входят в набор для установки, выбранный в панели **Наборы для установки**.

Примечание. Для выбора в таблице нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов – клавишу Ctrl. Чтобы выбрать все объекты, можно использовать комбинацию клавиш Ctrl+A.

В верхней части панели расположены:

- поле для быстрого поиска объектов в списке. По кнопке вы можете настроить фильтрацию объектов в списке;
- кнопка для изменения выбранного пользовательского объекта;
- кнопка для копирования выбранного объекта;
- кнопка для удаления выбранных пользовательских объектов, не установленных в конвейеры обработки событий;
- кнопка для перемещения выбранных пользовательских объектов между папками или пакетами экспертизы;
- кнопка для добавления выбранных объектов в набор для установки или их удаления из набора;
- кнопка для валидации объектов. При наведении курсора на кнопку во время валидации отображается всплывающая подсказка с индикатором выполнения;
- кнопка для экспорта объектов БД в файл с расширением .kb или в ZIP-архив.

Примечание. По кнопке в строке заголовков колонок вы можете выбрать отображаемые в списке колонки с параметрами объектов.

Для объектов в таблице указаны следующие параметры:

- в колонке **Статус валидации** отображается значок статуса валидации объекта: – валидация объекта не выполнялась или он был изменен после валидации, – валидация выполнена успешно, – при валидации объекта обнаружены ошибки;
- в колонке **Идентификатор** указан код объекта, который формируется автоматически при создании объекта;
- в колонке **Название** указано системное название объекта, которое используется для идентификации объекта. По ссылке в колонке вы можете открыть страницу объекта;
- в колонке **Описание** приводится описание объекта;
- в колонке **Тип** отображается значок типа объекта: – получен из стандартной БД, – создан пользователем. Значок указывает на то, что объект создан в результате копирования другого объекта; при нажатии на значок открывается ссылка на оригинальный объект;
- в колонке указана информация о статусе установки объекта в конвейеры обработки событий:

  – объект успешно установлен;

  – установленный объект неактуален, поскольку он обновлен в пакетах экспертизы установочной БД;

  – объект установлен не во все конвейеры (статус может отображаться только при наличии нескольких конвейеров обработки событий);

  – объект не установлен. Вследствие смены установочной БД или вовсе никогда не устанавливался.

  Если в системе установлено несколько конвейеров обработки событий, справа от значка статуса находится значок с цифрой, указывающей количество конвейеров, в которые установлен объект;
- в колонке **Папка** указана папка, в которой хранится объект в БД. По ссылке в колонке вы можете открыть таблицу со списком всех объектов в этой папке.

– вкладка **О пакете**. Содержит описание выбранного в панели **Папки** пакета экспертизы.

5.5 Страница Макросы

Страница предназначена для настройки макросов (см. раздел 16.13.4).

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать** − для создания пользовательского макроса;
- **Редактировать** − для изменения выбранного пользовательского макроса;
- **Создать копию** − для копирования выбранного макроса;
- **Удалить** − для удаления выбранного пользовательского макроса;
- **Валидация** − для проверки правильности структуры и синтаксиса кода выбранного макроса;
- **Метки** − для добавления меток для выбранного макроса.

В рабочей области страницы расположены:

- панель **Метки**. Содержит список меток, созданных для макросов. По умолчанию в панели создан список, содержащий стандартные метки и группы меток.

  По кнопке + вы можете создавать пользовательские метки и группу меток. Пользовательские метки и группы меток будут добавляться в список **Локальная система**. При выборе пользовательской группы меток в строке с ее появляется кнопка ⋮. По кнопке раскрывается меню, которое содержит пункты для добавления метки, изменения и удаления группы меток. При выборе пользовательской метки в строке с ее названием появляется кнопка ⋮. По кнопке раскрывается меню, которое содержит пункты для изменения и удаления метки;

  Примечание. Вы можете скрыть и открыть панель **Метки**, используя « и ».

- панель с таблицей макросов. Если в панели **Метки** выбран пункт **Все макросы** в таблице отображаются все созданные макросы. Если в панели **Метки** выбрана метка, в таблице отображаются макросы, для которых установлена эта метка, если группа меток − макросы, для которых установлена хотя бы одна метка из выбранной группы.

  В верхней части панели расположено поле для быстрого поиска в таблице по идентификатору, названию или системному названию макроса, указанному в его коде. По кнопке **Переключиться в фильтр** вы можете настроить фильтрацию макросов в таблице.

  Примечание. Вы можете выбрать колонки, отображаемые в таблице, по кнопке ⚙ в строке заголовков колонок.

- в колонках таблицы указаны следующие характеристики макросов:
  - статус валидации макроса: – валидация не выполнялась или макрос был изменен после валидации, – валидация выполнена успешно, – при валидации группы обнаружены ошибки;
  - **Идентификатор** – код макроса, который создается автоматически при его создании;
  - **Название** – название макроса, адаптированное для представления в интерфейсе;
  - **Описание** – текстовый комментарий;
  - **Тип** – отображается значок типа макроса: – получен из стандартной БД, – создан пользователем. Значок указывает на то, что макрос создан в результате копирования другого макроса; при нажатии на значок открывается ссылка на оригинальный макрос.
- панель **<Название макроса>**. Панель содержит информацию о выбранном макросе, установленных для него метках, существующих аргументах и код макроса.

5.6 Страница Схема полей событий

Любое событие ПК Ankey SIEM NG представляет собой совокупность полей, заполненных значениями, определяющими это событие. Схема полей событий содержит перечень всех полей и их допустимых значений. Страница предназначена для просмотра схемы полей событий.

В рабочей области страницы расположены:

- панель **Схема полей событий**. Содержит все доступные поля событий ПК Ankey SIEM NG. Для каждого поля указан поддерживаемый тип данных.
  В верхней части панели расположено поле для быстрого поиска поля события по его названию;
- панель для просмотра информации о выбранном поле события. В панели указаны название, описание, категория, поддерживаемый тип данных поля события и следующие атрибуты, указывающие на вариант использования поля при работе с событиями и составлении PDQL-запроса по событиям:
  - aggregatable – к значениям поля нескольких событий можно применить агрегатные функции;
  - asset_resolution – значение поля используется для идентификации актива;
  - distributable – по значениям поля можно распределить события по времени (time, start_time, recv_time);
  - filterable – по значениям поля можно фильтровать события;
  - groupable – по значениям поля можно группировать события;

  - selectable – можно получить значение поля;
  - sortable – по значениям поля можно сортировать события.
- панель **Допустимые значения свойства Enum**. Открывается при выборе полей событий с типом данных Enum и содержит список значений, которые может принимать выбранное поле.

5.7 Страница Журнал установки

Страница предназначена для просмотра журнала установки объектов в конвейеры обработки событий.

В рабочей области страницы расположены:

- панель для выбора записи журнала. В верхней части панели находятся кнопки **Статус** и **Конвейер** для настройки фильтров по статусу установки и по конвейерам, а также значок  для выбора даты записи;
- панель для просмотра записи. Содержит информацию о выбранной записи;
- панель для просмотра ошибок. Если при установке объектов возникла ошибка, в панели отображается ее подробное описание.

5.8 Страница Настройка инструментария для разработки правил SIEM

Страница предназначена для выбора версии ПК Ankey SIEM NG SDK для валидации объектов БД.

Панель инструментов содержит название страницы, а также кнопку **Установить SDK для валидации** или **Восстановить SDK для валидации**.

В рабочей области страницы расположены:

- панель для просмотра информации об используемых версиях SDK и схемы полей событий, а также об установленных версиях конвейеров обработки событий. Версии SDK могут различаться:
  - SDK для валидации – SDK, с помощью которого валидируются объекты БД (версию можно выбрать);
  - SDK системного контента – SDK объектов в стандартной БД.
- панель для выбора версии SDK. Содержит список доступных для установки версий SDK. В верхней части панели расположено поле для поиска SDK по номеру версии;
- панель для просмотра информации о версиях утилит, входящих в выбранный SDK.

6 Актуализация IT-инфраструктуры предприятия. Работа с активами

Работа с системой начинается со сбора сведений об активах. Это позволяет получить представление об информационной инфраструктуре предприятия.

Вы можете анализировать данные об активах и связях между ними, чтобы принимать решения по управлению IT-инфраструктурой.

6.1 Инвентаризация активов

Актив в ПК Ankey SIEM NG − информация или оборудование, имеющие ценность для предприятия и подлежащие защите от киберугроз.

Основные типы активов − сетевой узел и служба каталогов Microsoft Active Directory.

Служба каталогов Microsoft Active Directory является хранилищем для логинов, паролей и групп пользователей, персональной и организационной информации. Количество служб зависит от количества инфраструктур, но в большинстве случаев на предприятии такая служба одна. Службу каталогов Microsoft Active Directory можно добавить в ПК Ankey SIEM NG только с помощью задачи на сбор данных, вручную это сделать невозможно.

Внимание! Активы такого типа доступны в таблице активов после создания динамической группы активов (см. раздел 6.1.3.1) с фильтром ActiveDirectory.

Сведения, собранные об активе, составляют модель актива.

При сканировании IT-инфраструктуры предприятия, сборе и анализе данных о событиях безопасности ПК Ankey SIEM NG обнаруживает активы и создает о них записи. Вы также можете добавлять активы вручную, импортировать из файла (см. раздел 6.1.2.2) или из MP8. Удаляется актив либо вручную, либо автоматически − при его устаревании.

Вы можете объединять активы в группы (см. раздел 6.1.3) для удобства работы с системой: для отображения в системе организационной структуры предприятия, планирования задач на сканирование узлов, генерации отчетов.

Кроме того, группы активов позволяют фильтровать данные для других операций и создавать связи между событиями, инцидентами и пользователями.

6.1.1 Идентификация активов

ПК Ankey SIEM NG обнаруживает активы при сканировании сети предприятия, а также при сборе и анализе событий. Обнаруженные активы необходимо идентифицировать, при этом различается обнаружение активов и привязка существующих активов к событиям.

Степень полноты идентифицирующих данных, достаточных для создания записи о новом или обновления существующей записи об активе, зависит от контекста, например от метода сканирования актива, роли актива в событии, источника событий.

Привязка активов к событиям не влияет на состояние базы данных активов и ограничивается попыткой найти наилучшее соответствие между активами в базе данных и идентификаторами, содержащимися в событии.

Алгоритм идентификации при привязке активов к событиям отличается от алгоритма идентификации при обнаружении активов.

Идентификация активов − это сравнение отдельных атрибутов актива (его идентификаторов) с атрибутами существующих активов, о которых есть записи в базе данных. В случае идентификации при обнаружении активов по итогам сравнения либо создается запись о новом активе, либо обновляются записи о существующих активах. Если идентифицируется актив, участвующий в событии, то в случае успешной идентификации актива создается запись о связи актива с событием.

У актива могут быть следующие идентификаторы:

- Type − тип операционной системы;
- VMID − уникальный ключ виртуальной машины в контексте конкретной виртуальной инфраструктуры;
- IsVirtual − признак виртуальности узла;
- SystemId − уникальный идентификатор системы (способ формирования зависит от конкретной операционной системы);
- Hostname − имя узла, заданное на самом узле;
- FQDN − полное имя узла (значение, которое будет отображаться при аудите узла в режиме белого ящика, безотносительно внешних серверов имен);
- MAC − список доступных MAC-адресов (исключая виртуальные, такие как MAC-адреса протоколов отказоустойчивости);
- IP − список доступных IP-адресов (только маршрутизируемых за пределы сегмента); − Failover − список серийных номеров участников failover-группы (для Cisco ASA).

6.1.1.1 Обнаружение активов

Под обнаружением актива подразумевается получение набора данных, идентифицирующих актив, достаточного для создания новой или обновления существующей записи об активе. Для составления и поддержания полного и актуального представления об IT инфраструктуре предприятия в системе используются методы как непосредственного обнаружения − путем сканирования самого актива, так и косвенного обнаружения активов − при анализе информации о других активах, которую содержит сканируемый актив, и при анализе событий.

К непосредственным методам обнаружения активов относятся сканирование сетевых узлов в режимах белого ящика (модулем audit) и черного ящика (модулем pentest), добавление активов вручную и импорт активов из файла.

Активы также могут быть импортированы из MP8. Подробнее см. Руководство по интеграции с источниками Ankey SIEM NG 4.1.2.

Результаты сканирования активов получает служба управления сканированием (Core Scanning), эта же служба получает результаты ручного ввода и импорта активов.

К косвенным методам обнаружения активов относятся обнаружение на основе данных других активов и обнаружение на основе данных о событиях. В обоих случаях обнаруженные активы поступают на вход службы управления

сканированием. Таким образом, независимо от метода обнаружения активов их дальнейшая обработка происходит единообразно.

На основе данных других активов, полученных сканированием в режиме белого ящика, могут быть обнаружены следующие активы:

- при сканировании контроллера домена Active Directory обнаруживаются активы-участники домена с операционной системой Windows;
- при сканировании сервера Microsoft System Center Configuration Manager (SCCM) обнаруживаются активы-клиенты SCCM с операционной системой Windows, информацией о сетевых интерфейсах и установленном программном обеспечении;
- при сканировании сервера Kaspersky Security Center обнаруживаются активы-клиенты с операционной системой Windows;
- при сканировании гипервизоров VMware ESXi и Microsoft Hyper-V обнаруживаются активные виртуальные машины, если гипервизор предоставляет достаточную информацию об их сетевых интерфейсах и установленной операционной системе (полнота информации, доступной гипервизору, зависит от гостевой операционной системы и наличия установленного набора утилит VMware Tools).
- при сканировании сетевых устройств анализируется полученная по протоколам CDP и LLDP информация о соседних устройствах, их типе, IP-адресах и операционной системе и обнаруживаются соответствующие активы;
- при сканировании сетевых устройств анализируется полученная информация об актуальных связках «MAC-адрес − IP-адрес» в базе DHCP snooping и обнаруживаются активы − сетевые узлы с данными адресами;
- при сканировании актива на основе динамических записей из его ARP-таблицы обнаруживаются активы − сетевые узлы (за исключением записей proxy ARP, local proxy ARP и записей с виртуальными MAC-адресами);
- при сканировании актива на основе информации о шлюзах, полученной из его таблицы маршрутизации, обнаруживаются активы с указанным IP-адресом и ролью «маршрутизатор».

Обнаружение активов на основе данных другого актива производится не на этапе сканирования, а на этапе обработки данных исходного актива агрегатором (исключение − обнаружение клиентских активов SCCM, которое производится на этапе сканирования SCCM).

Обнаружение активов на основе данных о событиях осуществляется путем анализа нормализованных событий. Поскольку в потоке нормализованных событий может происходить большое количество однотипных событий в единицу времени, на основании которых многократно может быть принято решение о создании записи об одном и том же активе, на этом же этапе производится предварительное объединение обнаруженных активов с полностью одинаковыми наборами идентификаторов. Активы с уникальными наборами идентификаторов поступают на вход службы управления сканированием.

На основе данных о событиях могут быть обнаружены следующие активы:

- актив − клиентский узел − из событий назначения IP-адреса;
- актив − сетевое устройство с IP-адресом источника события (для сетевых устройств Cisco и CheckPoint GAiA);
- актив − сетевое устройство с SystemId источника события (для устройств Fortinet FortiGate);
- актив с FQDN источника события (для источников Microsoft Windows и VMware ESXi);
- актив-клиент с установленной операционной системой Microsoft Windows, указанными FQDN и IP-адресом − из событий сервера Kaspersky Security Center;
- актив-маршрутизатор − из события неудачной аутентификации FHRP от сетевых устройств Cisco;
- актив-сервер syslog − из события начала журналирования от сетевых устройств Cisco IOS;
- актив-сервер доступа к сети (NAS) − из событий от серверов AAA;
- актив − клиентский узел − из событий выполнения команды, успешного и неуспешного входа в систему и выхода из системы от различных сетевых устройств (только для локальных адресов, соответствующих документам RFC 1918 и RFC 4193);
- актив-сервер NTP − из события выбора сервера от сетевых устройств Huawei VRP (только для локальных адресов, соответствующих документам RFC 1918 и RFC 4193);
- актив − сетевое устройство и актив-клиент SNMP − из события неудачной аутентификации SNMP от сетевых устройств Juniper Junos OS (клиент обнаруживается, только если его локальный адрес соответствует документам RFC 1918 и RFC 4193);
- актив − сетевое устройство и актив-сервер LDAP − из события успешного подключения к серверу LDAP от сетевых устройств Palo Alto.

6.1.1.2 Алгоритмы идентификации активов

При анализе событий безопасности, а также при сканировании сетевых узлов площадки требуется правильно идентифицировать активы. Сканирование одним агентом сетевых сегментов, активы в которых имеют одни и те же IP-адреса, может привести к неверной агрегации активов: вместо нескольких активов система может идентифицировать один актив. Также наличие в списке активов с одинаковым IP-адресом может затруднить поиск необходимого актива. При наличии в составе площадки таких сегментов сети для каждого из них создается отдельная инфраструктура. В задаче сканирования указывается инфраструктура (если их несколько), соответственно для сканирования разных инфраструктур создаются разные задачи.

Примечание. После развертывания ПК Ankey SIEM NG имеет одну инфраструктуру **Инфраструктура** по умолчанию. Подробнее о работе с инфраструктурами см. Руководство администратора Ankey SIEM 4.1.2.

Псевдонимы параметров инфраструктур, к которым принадлежат активы, вы можете использовать для фильтрации, настройки представления данных в таблице активов и для создания динамических групп активов.

Алгоритм идентификации при обнаружении активов

При обнаружении активов идентификация происходит следующим образом: обнаруженные активы поступают в службу управления сканированием от одного из источников (модулей сканирования, ручного ввода, импорта из файла, обнаружения на основе данных о событиях). Затем в системе сравниваются идентификаторы просканированных активов (в первую очередь идентификатор Type) с идентификаторами существующих в инфраструктуре активов. В зависимости от результатов происходит обновление базы данных активов по одному из сценариев:

- если совпадений нет − создается новая запись об активе, в которую заносятся входящие модельные данные;
- если входящему набору идентификаторов соответствует один существующий актив − входящие модельные данные заносятся в существующую запись об активе;
- если входящему набору идентификаторов соответствует несколько существующих активов − совпавшие записи объединяются в одну, и в эту запись заносятся входящие модельные данные.

Алгоритм идентификации при привязке активов к событиям

Система анализирует все события, произошедшие в IT-инфраструктуре предприятия, для определения участвующих в них активов. Этот процесс происходит независимо от процесса обнаружения активов на основе данных о событиях. Один и тот же набор идентификаторов в событии может служить входными данными для обоих процессов.

При привязке активов к событиям идентификация актива происходит следующим образом: в системе происходит сбор событий с источников, все события приводятся к нормализованному виду. Затем система для каждого события определяет участвующие в нем активы. Далее сравниваются идентификаторы участвующих активов (в первую очередь идентификатор Type) с идентификаторами активов из базы данных. В зависимости от результатов выбирается один из сценариев привязки актива к событию:

- если совпадений нет − изменения в событие не вносятся;
- если актив совпал с одним активом из базы данных − в событие добавляется ссылка на актив из базы данных;
- если актив совпал с несколькими активами из базы данных − в событие добавляется ссылка на тот актив из базы данных, который более актуален (обновлен последним).

6.1.2 Добавление активов в систему

Система обнаруживает активы при сканировании сети предприятия, а

также при сборе и анализе событий. Вы также можете добавлять активы вручную или импортировать из CSV файла. При импорте из файла вы можете задавать пользовательские поля активов и их значения, которые необходимы вам для их идентификации.

Кроме того, при добавлении активов вы можете задавать время, в течение которого данные об активе будут считаться актуальными, для сканирования модулем audit (режим белого ящика) и модулем pentest (режим черного ящика). Это поможет вам контролировать устаревание активов (см. раздел 6.1.4).

6.1.2.1 Добавление актива вручную

❖ Чтобы добавить актив в систему:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.

   Примечание. Если это первый запуск ПК Ankey SIEM NG, то вам необходимо создать пользовательскую группу активов.

2. В панели инструментов нажмите + и в раскрывшемся меню выберите пункт **Добавить актив**.
   Откроется окно **Создание актива**.
3. В раскрывающемся списке **Расположение** выберите группу, в которую будет помещен актив.
4. Если вы знаете название операционной системы, установленной на активе, в раскрывающемся списке **ОС** выберите тип операционной системы и в поле **OsName** введите ее название.
5. Укажите идентификаторы актива:
   - если вы выбрали тип операционной системы Windows, в поле **FQDN** введите полное доменное имя актива;
   - если вы выбрали тип операционной системы Cisco IOS, в поле **FQDN** введите полное доменное имя актива или в поле **Hostname** введите имя узла актива;
   - если вы не выбрали тип операционной системы или выбрали другой тип, в поле **Hostname** введите имя узла актива.
6. В поле **IP-адрес** введите IP-адрес актива.
7. Если вы указали название операционной системы, установленной на активе, нажмите кнопку **Далее**.
   Откроется страница с блоком параметров **Программное обеспечение**.

   Примечание. С помощью раскрывающегося списка **Название ПО** вы можете выбрать название программного обеспечения, установленного на активе.

8. Если требуется, в блоке **Статусы актуальности данных** настройте время, в течение которого данные об активе будут считаться актуальными, отдельно для сканирования в режимах черного и белого ящика.

Примечание. Вы можете выбрать время в раскрывающемся списке или ввести его с помощью языка PDQL.

9. Нажмите кнопку **Сохранить**.

Актив добавлен в указанную группу активов.

6.1.2.2 Импорт активов из файла

Вы можете импортировать в ПК Ankey SIEM NG данные об активах типа Host из файла формата CSV. Имя файла может быть любым, файл должен быть представлен в кодировке UTF-8 с BOM.

В первой строке файла должны содержаться названия полей в порядке, в котором во второй и последующих строках будут содержаться их значения. Вторая и последующие строки описывают импортируемые активы (одна строка должна соответствовать одному активу). Значения текстовых полей должны быть заключены в кавычки (" "). Значения полей должны быть разделены точкой с запятой (;).

Примечание. Вы можете скачать пример файла в окне импорта активов по кнопке **?**.

В состав полей должны входить обязательные поля, необходимые для идентификации актива:

- TypeAlias − псевдоним;
- FQDN − для активов, на которых развернута операционная система семейства Windows или ESXi;
- FQDN или Hostname − для активов, на которых развернута операционная система семейства Cisco IOS;
- Hostname − для прочих активов;
- IP-адрес. Поле может содержать несколько значений, которые должны быть разделены вертикальной чертой (|).

Вы можете также добавить в файл необязательные поля: поле MAC, содержащее список доступных через сеть MAC-адресов актива, и поле IsVirtual (признак виртуальности узла). Значения поля MAC должны быть разделены вертикальной чертой (|). Кроме того, вы можете добавить в файл пользовательские поля, которые необходимы вам для работы с активами (см. Руководство администратора Ankey SIEM NG 4.1.2).

Примечание. Если в двух классах активов есть одинаковые по названию и разные по типу поля, вам необходимо указать в списке полей в файле оба поля, предваряя их названием класса с точкой. Например, для инвентаризационных номеров активов, на которых установлены операционные системы семейств Windows и Linux, укажите поля WindowsHost.UF_InvNum и LinuxHost.UF_InvNum.

❖ Чтобы импортировать из файла данные об активах:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели инструментов нажмите + и в раскрывшемся меню выберите пункт **Импортировать данные**.
   Откроется окно **Импорт активов**.

3. В раскрывающемся списке **Инфраструктура** выберите инфраструктуру, к которой будут привязаны активы.

Примечание. Список отображается, если в системе создано более одной инфраструктуры.

4. В раскрывающемся списке **Расположение** выберите группу, в которую будут помещены активы.
5. Перетащите или выберите файл в формате CSV.
6. Нажмите кнопку **Импортировать**.

Данные об активах импортированы.

6.1.3 Группы активов

Пользователь может объединять активы в группы для удобства работы с системой: для отображения в системе организационной структуры предприятия, планирования задач на сканирование узлов, генерации отчетов. Группировка активов также используется:

- при фильтрации данных для отчетов, графиков, отображения данных;
- привязке событий;
- привязке инцидентов;
- привязке ролей пользователей (назначении пользователю определенных полномочий на выполнение тех или иных действий в рамках группы, назначении роли пользователя в группе; подробнее о ролях пользователей см. Руководство администратора Ankey SIEM NG 4.1.2);
- сборе данных.

Группа может содержать активы и другие группы. Отображение групп и содержащихся в этих группах активов зависит от роли пользователя, который авторизован в ПК Ankey SIEM NG. Пользователь не может настраивать или удалять вложенные группы активов, если у него нет прав на родительскую группу.

Группы активов бывают пользовательскими и стандартными. Стандартные группы предустановлены в ПК Ankey SIEM NG, их невозможно изменить или удалить.

По умолчанию ПК Ankey SIEM NG имеет две стандартные группы:

- группа **Все активы** − в ней выводятся все активы, которые доступны роли пользователя;
- группа **Unmanaged hosts** − в ней выводятся все активы, не привязанные ни к одной из групп (расположение этих активов не указано).

Пользовательские группы делятся на динамические и статические. В динамическую группу ПК Ankey SIEM NG добавляет актив автоматически, если он удовлетворяет определенному условию − запросу на языке PDQL.

Примечание. Динамические группы наполняются всеми подходящими под PDQL-запрос активами, независимо от расположения и уровня вложенности этих групп.

Сложные PDQL-запросы могут обрабатываться долго. В списке групп

медленные динамические группы отмечаются специальным значком.

Пользователь, у которого нет доступа ко всем активам, не может создавать динамические группы или изменять в динамической группе запрос для фильтрации активов. В статической группе располагаются активы, которые вручную выбирает пользователь.

Для группы активов пользователь может выпустить отчет, построить статистику, просмотреть карту сети. Также пользователь может по нажатию кнопки мыши просматривать во всплывающей подсказке полный путь к группе, если роль пользователя предполагает доступ к нескольких группам с одинаковыми названиями, а доступ к родительским группам отсутствует.

Группы иерархически связаны друг с другом и отображаются в интерфейсе системы в виде дерева. На иерархию групп накладываются следующие ограничения:

- возможны не более 9 уровней вложенности;
- каждая создаваемая группа должна быть привязана к какой-либо другой группе;
- группа не может быть для другой группы одновременно родительской и вложенной в нее (например, если Группа 3 входит в Группу 1, то Группа 1 не может входить в Группу 3);
- динамическая группа не может содержать в себе вложенные группы.

6.1.3.1 Создание группы активов

❖ Чтобы создать группу активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Группы активов** нажмите +.
   Откроется страница **Создание группы**.
3. В поле **Название** введите название группы активов.
4. В раскрывающемся списке **Расположение** выберите группу активов, в которую войдет новая группа.
5. Выберите тип группы активов.

> **Примечание.** Если у вас нет доступа ко всем активам, вы не сможете создать динамическую группу.

6. Если вы выбрали тип группы активов **Динамическая**, в поле **Фильтр** введите запрос для фильтрации активов на языке PDQL.

> **Примечание.** Вы также можете настроить метрики CVSS. Описание метрик CVSS см. на сайте first.org.

7. Нажмите кнопку **Сохранить**.

Группа активов создана.

6.1.3.2 Создание группы активов из карточки актива

Вы можете создавать группы активов из карточки актива.

❖ Чтобы создать группу активов из карточки актива:

1. В главном меню выберите раздел **Активы**.

Откроется страница **Активы**.
2. В панели **Активы** выберите актив.
3. На карточке актива выберите вкладку **Актив**.
4. Во всплывающем окне выберите условие фильтрации.
Условие будет добавлено в PDQL-запрос в нижней части карточки актива.

Примечание. Вы можете выбрать несколько условий фильтрации.

5. В правом нижнем углу страницы нажмите **Перейти к созданию группы**.
Откроется страница **Создание группы**. Сформированный PDQL-запрос будет автоматически добавлен в поле **Фильтр**.

Примечание. Вы можете сформировать PDQL-запрос вручную.

6. В поле **Название** введите название группы активов.
7. В раскрывающемся списке **Расположение** выберите группу активов, в которую войдет новая группа.
8. Выберите тип группы активов.

Примечание. Вы также можете настроить метрики CVSS. Описание метрик CVSS см. на сайте first.org.

9. Нажмите кнопку **Сохранить**.

Группа активов создана.

6.1.3.3 Настройка группы активов

❖ Чтобы настроить группу активов:

1. В главном меню выберите раздел **Активы**.
Откроется страница **Активы**.
2. В панели **Группы активов** выберите группу активов.
3. В панели **Группы активов** нажмите ⋮ и в раскрывшемся меню выберите пункт **Редактировать**.
Откроется страница **Редактирование группы <Название группы>**.
4. Внесите необходимые изменения.

Примечание. Вы можете изменить тип группы. Если сделать группу динамической, из нее поначалу будут удалены все активы. Если группа содержит вложенные группы, сделать ее динамической невозможно. Если сделать группу статической, все активы, которые соответствуют фильтру, будут привязаны к ней.

Примечание. Если у вас нет доступа ко всем активам, вы не сможете изменить запрос для фильтрации активов.

5. Нажмите кнопку **Сохранить**.

Группа активов настроена.

6.1.3.4 Удаление группы активов

Вы можете удалять группы активов, при этом будут удалены все вложенные группы. Вы не можете удалять стандартные группы активов.

❖ Чтобы удалить группу активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Группы активов** выберите группу активов.

> **Примечание.** Вы можете выбрать несколько групп, удерживая клавишу Ctrl.

3. В панели **Группы активов** нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Выбранная группа активов удалена.

6.1.4 Устаревание актива

Сведения об активах со временем устаревают и приводят к ошибкам при выполнении задач. Чтобы не допускать таких ошибок, система выявляет и удаляет устаревшие активы. За это отвечает служба идентификации активов. Она принимает решение о том, что актив устарел и затем создает событие о его удалении.

Устаревшим считается актив, после последнего обновления которого прошло определенное время. Время устаревания для всех активов устанавливает администратор.

О том, когда ожидается устаревание конкретного актива, вы можете узнать в карточке актива.

Актив не устареет, если:

- от него будет получен ответ при сканировании сети;
- он будет обновлен при анализе событий;
- данные о нем будут обновлены вручную;
- данные о нем будут обновлены при импорте из файла (см. раздел 6.1.2.2).

6.1.5 Карточка актива

Карточка актива содержит полную информацию об активе. Перейти в карточку можно из таблицы активов, щелкнув по названию актива. Также вам доступен быстрый просмотр карточки в боковой панели Актив.

Под именем актива располагаются сведения о его жизненном цикле, а также указаны интегральная уязвимость и метрика значимости актива (низкая, средняя, высокая или не определена). Вы можете вручную установить значимость для актива из таблицы (см. раздел 6.1.8) или из его карточки (см. раздел 6.1.7).

График отражает моменты, когда были получены новые данные об активе. Новые данные поступают после завершения задач на сканирование, а также если внести изменения в конфигурацию актива вручную.

По умолчанию на графике отображается история актива за последние 7 дней. Вы можете изменить период для просмотра истории актива по кнопке 🗓.

Под графиком расположены вкладки **Сводка**, **Конфигурация** и **Метрики CVSS**.

Сводка. В карточке актива типа "сетевой узел" отображается краткая информация об аппаратном и программном обеспечении актива и сетевая конфигурация.

Конфигурация. Вкладка содержит подробную информацию об аппаратном и программном обеспечении актива.

Метрики CVSS. На вкладке отображаются контекстные метрики CVSS. Описание метрик CVSS см. на сайте first.org.

Вы можете устанавливать и изменять значения для метрик, в том числе при настройке группы, в которую входит актив. Эффективное значение определяется автоматически и является максимальным для данной метрики из всех установленных значений (для актива и групп, в которые входит актив). Максимальные значения метрик наследуются от родительской группы к вложенной группе и от вложенной группы к активу.

Кроме того, в карточке актива могут отображаться пользовательские поля, добавленные в модель актива, и их значения.

6.1.6 Мини-карточка актива

В мини-карточке актива вы можете получать базовую информацию об активе, статистику его участия в инцидентах. Мини-карточка позволяет переходить к созданию задачи на сбор данных с актива, а также к просмотру:

- актива на карте сети;
- событий с участием актива;
- инцидентов с участием актива;
- детальной информации об активе.

Открыть мини-карточку актива вы можете по ссылке с названием актива.

В верхней части мини-карточки содержится название актива. Под названием актива находятся вкладки **Сводка**, **Интерфейсы** и **Инциденты**.

Примечание. Вкладка **Интерфейсы** доступна только при работе с мини-карточкой актива на карте сети.

На вкладке **Сводка** отображаются краткая информация о программном обеспечении актива, роли, указатель метрики значимости, дата последнего обновления, а также признак виртуальности (если есть).

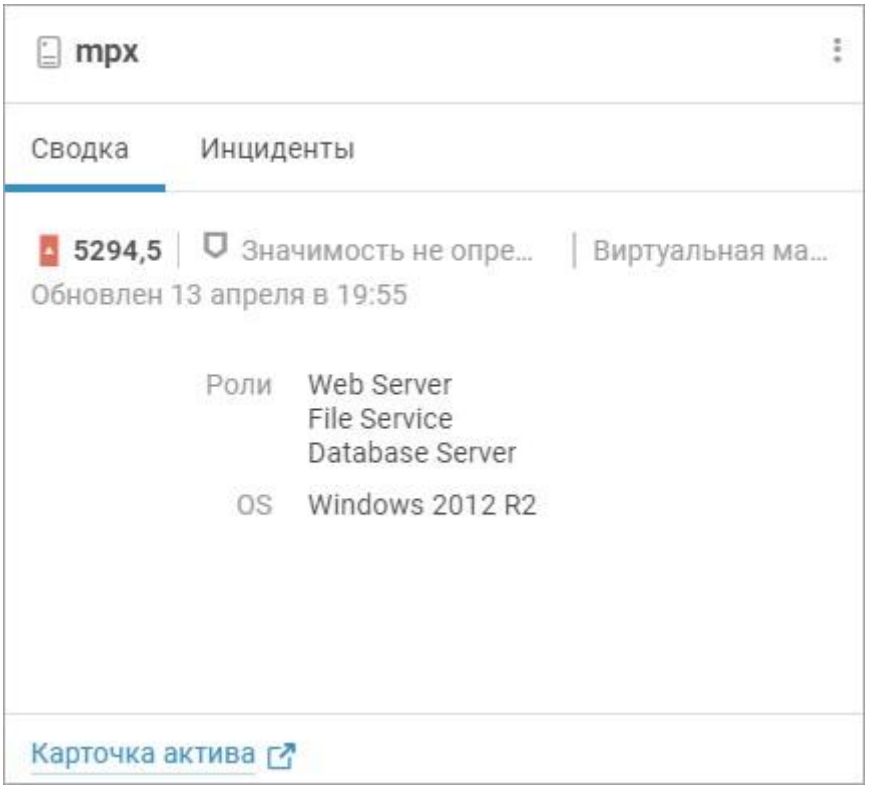

Рисунок 6.1 − Просмотр сводной информации об активе

На вкладке **Инциденты** находится диаграмма. Диаграмма отображает распределение инцидентов, в которые вовлечен актив, по опасности или по роли актива в инцидентах.

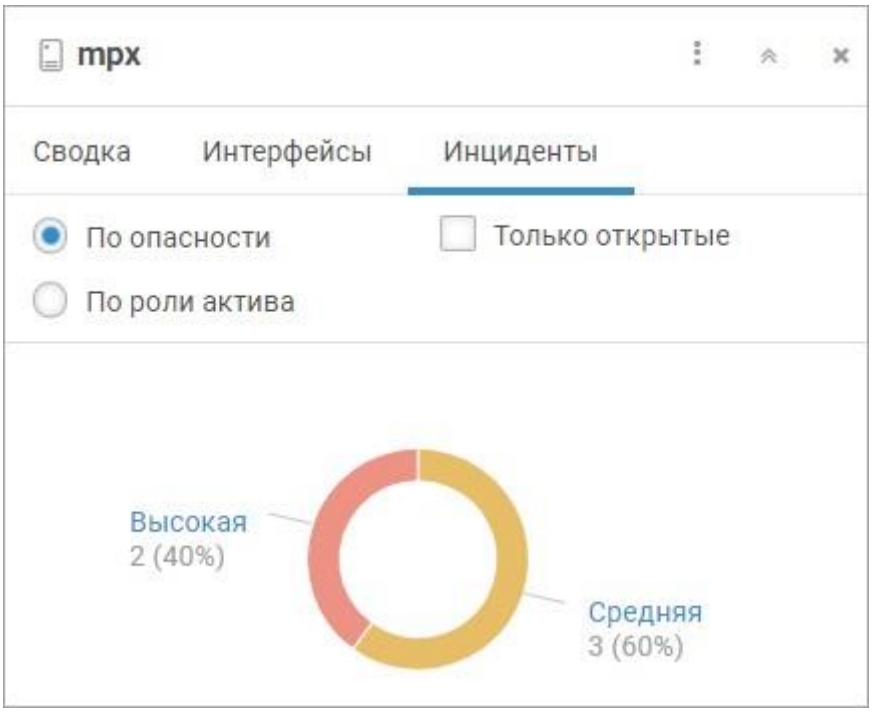

Рисунок 6.2 − Просмотр статистики участия актива в инцидентах

Вкладка **Интерфейсы** содержит список интерфейсов актива с их IP- и MAC-адресами.

Рисунок 6.3 − Просмотр интерфейсов актива

6.1.7 Изменение информации об активах

При сканировании сети предприятия система обновляет информацию об активах. Вы также можете изменять информацию об активах вручную. Например, если на активе была установлена новая версия операционной системы или новое программное обеспечение.

Примечание. Вы не можете изменить ранее заданную операционную систему на систему другого семейства. Также вы не можете изменять дополнительные сведения одновременно для нескольких активов.

❖ Чтобы изменить информацию об одном или о нескольких активах:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В таблице активов выберите один или несколько активов.
3. В панели инструментов нажмите и в раскрывшемся меню выберите один из пунктов:
   – если вы хотите изменить данные паспорта одного или нескольких активов, выберите пункт **Паспорт**;
   – если вы хотите изменить другую информацию (например, значения пользовательских полей) об одном активе, выберите пункт **Дополнительные сведения**.
4. Измените информацию об активах.
5. Нажмите кнопку **Сохранить**.

Информация изменена.

Также вы можете изменить информацию об одном активе из его карточки по кнопке **Редактировать**.

6.1.8 Присвоение значимости активам

В ПК Ankey SIEM NG для новых активов уровень значимости не определяется автоматически. Вы можете вручную присвоить активу значимость (низкую, среднюю или высокую), например чтобы расставить приоритеты во время устранения уязвимостей или при разборе инцидентов.

❖ Чтобы присвоить активам уровень значимости:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите .
   Откроется окно **Изменение значимости <N> активов**.
4. В раскрывающемся списке выберите уровень значимости.
5. Нажмите кнопку **Применить**.

Активам присвоен уровень значимости.

Также вы можете перейти к присвоению уровня значимости одному активу из его карточки по кнопке **Установить значимость** или по кнопке **Редактировать** → **Паспорт**.

6.1.9 Удаление активов

При работе с системой может возникнуть ситуация, когда вы выявили неактуальные активы (например, была неправильно настроена задача сбора данных).

❖ Чтобы удалить активы:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите и подтвердите удаление.
4. Выбранные активы удалены.

Также вы можете удалить один актив из его карточки по кнопке **Удалить**.

6.2 Аналитика по активам

По умолчанию на странице **Активы** отображаются все активы, данные о которых есть в системе, из групп, к которым у вас есть доступ (включая вложенные группы).

Информация об активах в системе представлена в виде модели активов, то есть структурированной совокупности всех атрибутов активов. В модель актива также могут быть добавлены пользовательские поля. Для удобства работы вы можете использовать табличное представление данных об активах и любых их атрибутах. В этом случае поля модели активов преобразуются в поля таблицы активов, а атрибуты активов − в значения. В таблице активов вы можете:

- фильтровать записи;
- изменять состав колонок;
- группировать записи;
- анализировать данные;
- ограничивать количество записей;
- отображать только уникальные записи;
- выбирать порядок сортировки.

После группировки вы можете анализировать данные об активах с помощью математических операций.

Вы можете изменять список отображаемых данных об активах с помощью панели фильтрации − последовательно выбирая операции, а также с помощью поля поиска − указав название актива, его описание, MAC- или IP-адрес. Способы фильтрации сочетаются друг с другом: ввод значения в поле поиска дает возможность перейти к созданию запроса на языке PDQL по кнопке .

6.2.1 Фильтрация активов по группе

Вы можете использовать стандартные и пользовательские группы активов, чтобы фильтровать активы. Иерархический список групп активов отображается на странице **Активы** в панели **Группы активов**.

❖ Чтобы отфильтровать активы по группе:

1. В главном меню выберите раздел **Активы**.

Откроется страница **Активы**.

2. В панели **Группы активов** выберите группу активов.

Активы отфильтрованы.

Для удобства анализа вы можете настроить отображение не всех активов из выбранных, а только их части, фильтруя активы с помощью запросов на языке PDQL.

Кроме того, вы можете настроить представление данных в таблице активов. Например, чтобы отсортировать записи об активах в таблице.

6.2.2 Фильтрация активов с помощью PDQL-запроса

Вы можете использовать запросы на языке PDQL, чтобы фильтровать активы.

❖ Чтобы отфильтровать активы с помощью PDQL-запроса:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Фильтрация**.
   Откроется окно PDQL-запроса.
3. В поле **Условие фильтрации** введите запрос на языке PDQL.
4. Нажмите кнопку **Применить**.

Активы отфильтрованы.

Кроме того, вы можете перейти к созданию и изменению PDQL-запроса по нажатию на значок .

В открывшемся окне вы можете настроить представление данных в таблице активов.

Если вы хотите регулярно фильтровать данные по заданному набору атрибутов и их значений, вы можете сохранить этот набор как запрос.

6.2.3 Представление данных об активах

По умолчанию на странице **Активы** представлены все активы, к которым у вас есть доступ.

Для каждого актива в таблице отображаются:

- название и графическое обозначение его типа;
- значение метрики интегральной уязвимости;
- время последнего изменения данных.

Вы можете изменить состав колонок таблицы и настроить отображение данных в ней:

- ограничить количество записей;
- отобразить только уникальные записи;
- выбрать порядок сортировки.

Кроме того, вы можете сгруппировать данные об активах и проанализировать их с помощью математических функций.

Если вы хотите регулярно настраивать представление данных в таблице с помощью набора атрибутов и их значений, вы можете сохранить этот набор как запрос.

6.2.3.1 Выбор колонок для таблицы активов

❖ Чтобы выбрать колонки для таблицы активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Выбор полей**.
3. В открывшемся окне **Выбор полей** выберите колонки для таблицы активов.
   Если требуется, включите отображение только уникальных записей в таблице.

> **Примечание.** Вы можете отобразить только уникальные записи в таблице позднее (см. раздел 6.2.3.3).

4. Нажмите кнопку **Применить**.

В таблице активов отображены выбранные колонки с данными.

6.2.3.2 Ограничение количества записей в таблице активов

❖ Чтобы ограничить количество записей в таблице активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Ограничение**.
3. В открывшемся окне в поле **Максимальное количество строк** введите количество строк таблицы.
4. Если требуется, включите отображение всех записей.
5. Нажмите кнопку **Применить**.

Количество записей в таблице активов ограничено.

6.2.3.3 Отображение уникальных записей в таблице активов

❖ Чтобы отобразить уникальные записи в таблице активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Уникальность**.

В таблице активов отображены уникальные записи.

Кроме того, вы можете включить отображение только уникальных записей в таблице при выборе колонок для таблицы активов (см. раздел 6.2.3.1).

6.2.3.4 Сортировка записей в таблице активов

❖ Чтобы отсортировать данные в таблице активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Сортировка**.
3. В открывшемся окне в поле **Сортировка по полям** укажите колонки таблицы активов.
4. Если требуется, измените направление сортировки.
5. Нажмите кнопку **Применить**.

Данные в таблице активов отсортированы.

6.2.4 Группировка и анализ данных об активах с помощью математических операций

Вы можете анализировать сгруппированные данные об активах с помощью математических операций над данными в таблице активов. Для выполнения операций используются функции (см. приложение Б).

❖ Чтобы сгруппировать и проанализировать данные об активах:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Группировка и агрегация**.
   Откроется окно группировки и анализа данных.
3. В раскрывающемся списке **Группировка** выберите поля, по которым требуется сгруппировать активы.

   Примечание. Вы можете выбрать не более десяти полей.

4. В раскрывающемся списке выберите функцию.
5. В раскрывающемся списке выберите название колонки таблицы, над данными которой требуется выполнить математическую операцию.
6. Если требуется, укажите псевдоним.
   Вы можете проанализировать данные об активах, выбрав несколько математических операций по нажатию +.
   Вы можете удалять математические операции по нажатию в строке операции.
7. Нажмите кнопку **Применить**.

В таблице отображены результаты группировки и анализа данных об активах.

Вы также можете выполнить группировку и анализ данных отдельно.

Если вы хотите регулярно группировать и анализировать данные в таблице с помощью набора атрибутов и их значений, вы можете сохранить этот набор как запрос (см. раздел 6.2.6).

6.2.5 Фильтрация активов с помощью объединения запросов

Для подготовки аналитики по активам часто требуется получать данные об их атрибутах, которые связаны между собой, но находятся на разных уровнях иерархии в модели активов или относятся к активам разных типов. Чтобы получать все эти данные в одной таблице, вы можете объединять результат ранее выполненного PDQL-запроса с результатом выполнения другого PDQL-запроса.

Избежать повторения названий колонок таблиц при объединении запросов можно с помощью псевдонимов. В качестве псевдонима для PDQL-запроса вы можете использовать один или несколько символов, которые будут добавлены к названиям всех колонок в таблице с результатами объединения запроса. Например, при использовании псевдонима A колонки таблицы будут иметь названия 1, 2, …, n, A.1, A2, …, A.n.

❖ Чтобы объединить результат выполненного запроса с результатом выполнения другого запроса:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Введите запрос на языке PDQL.
3. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Объединение**.
   Откроется окно **Объединение с результатом другого запроса**.
4. В поле **Запрос** введите запрос на языке PDQL.
   С результатом выполнения этого запроса будет объединен результат ранее выполненного PDQL-запроса.

   Примечание. Вы можете скопировать условие фильтрации, нажав ссылку **Вставить условие из сохраненного запроса** и выбрав условие из списка.

5. Если требуется, в поле **Псевдоним запроса** введите псевдоним.

   Примечание. Псевдоним запроса может содержать латинские и русские буквы, цифры, знак подчеркивания и дефис; не может начинаться с дефиса.

   В списке **Колонки, доступные для объединения** отобразятся названия всех колонок таблиц.
6. В поле **Условие объединения запроса** введите условие объединения.
   Для создания условия надо использовать только названия колонок таблиц из списка **Колонки, доступные для объединения**.
7. Нажмите кнопку **Применить**.

Запросы объединены, результат отобразится в таблице активов.

Если вы хотите регулярно искать и анализировать данных об активах с помощью двух запросов, вы можете сохранить объединенный запрос.

6.2.6 Работа с пользовательскими и общими запросами

Вы можете фильтровать активы в ПК Ankey SIEM NG с помощью запросов на языке PDQL.

В системе предусмотрены готовые запросы для фильтрации активов и настройки представления данных о них в таблице. Эти запросы расположены в папках, вложенных в стандартную папку **Стандартные запросы**.

Примечание. Вы не можете изменять или удалять стандартные папки и запросы.

Для решения рабочих задач вы можете создавать свои пользовательские запросы и папки и помещать их в стандартную папку **Пользовательские запросы**. К пользовательским запросам и папкам не имеет доступа никто, кроме их создателя. Кроме того, вы можете создавать в стандартной папке **Общие запросы** вложенные папки (или перемещать туда пользовательские папки) и запросы, к которым будут иметь доступ все пользователи системы.

На странице **Активы** вы можете работать с пользовательскими и общими

вложенными папками и запросами (см. раздел 4.5).

6.2.6.1 Создание папки запросов

Для удобства работы вы можете создавать папки, чтобы помещать туда запросы для фильтрации активов по выбранным критериям.

❖ Чтобы создать папку запросов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** нажмите +.
   Откроется окно **Новая папка**.
3. В поле **Название** введите название папки запросов.
4. В раскрывающемся списке **Расположение** выберите папку, внутри которой требуется создать папку запросов.
   По умолчанию папка создается внутри папки **Пользовательские запросы**.
5. Нажмите кнопку **Создать**.

Папка запросов создана.

Кроме того, вы можете перейти к созданию папки внутри уже созданной папки запросов, наведя курсор на созданную папку и нажав ⋮.

6.2.6.2 Изменение папки запросов

Вы можете изменять названия папок запросов или перемещать их в другие папки.

❖ Чтобы изменить папку запросов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** наведите курсор на папку, нажмите ⋮ и в раскрывшемся меню выберите пункт **Переместить или переименовать**.
   Откроется окно **<Название папки>**.
3. В поле **Новое название** введите название папки запросов.
4. В раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить папку запросов.
5. Нажмите кнопку **Сохранить**.

Папка запросов изменена.

6.2.6.3 Удаление папки запросов

Вы можете удалять папки запросов. При удалении папки все вложенные папки и запросы также будут удалены.

❖ Чтобы удалить папку запросов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** наведите курсор на папку, нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить папку** и при необходимости подтвердите удаление.

Папка запросов удалена.

6.2.6.4 Сохранение запроса

Вы можете сохранять условия запросов для фильтрации активов, чтобы использовать их повторно.

Условие запроса может включать в себя:

- условие фильтрации активов на языке PDQL (см. раздел 6.2.2);
- настроенное представление данных об активах в таблице (см. раздел 6.2.3);
- условие группировки данных об активах и параметры их анализа с помощью математических функций (см. раздел 6.2.4).

❖ Чтобы сохранить условие запроса:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Добавьте условие запроса в панель фильтрации.
3. В панели фильтрации нажмите ⋮ и в раскрывшемся меню выберите пункт **Сохранить как новый**.
   Откроется окно **Новый запрос**.
4. В поле **Название** введите название пользовательского запроса.
   Если требуется, в раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить этот запрос.
5. Нажмите кнопку **Сохранить**.

Условие запроса сохранено.

6.2.6.5 Создание запроса на основе существующего

Вы можете создавать новые запросы на основе имеющихся запросов − стандартных, общих или пользовательских.

❖ Чтобы создать запрос на основе имеющегося:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** наведите курсор на запрос, нажмите ⋮ и в раскрывшемся меню выберите пункт **Сохранить как новый**.
   Откроется окно **Новый запрос**.
3. В поле **Название** введите название пользовательского запроса.
4. Если требуется, в раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить этот запрос.
5. Нажмите кнопку **Сохранить**.

Запрос создан.

6.2.6.6 Изменение условия запроса

❖ Чтобы изменить условие запроса:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** выберите запрос.
   Условие запроса будет добавлено в панель фильтрации.
3. Измените условие запроса.
4. В панели фильтрации нажмите ⋮ и в раскрывшемся меню выберите пункт **Сохранить**.

Условие запроса изменено.

6.2.6.7 Изменение названия и расположения запроса

Вы можете изменять названия запросов или перемещать их в другие папки.

Примечание. После перемещения пользовательского запроса в папку **Общие запросы** другие пользователи смогут изменять, перемещать или удалить его.

❖ Чтобы изменить запрос:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** наведите курсор на запрос, нажмите ⋮.
3. В раскрывшемся меню выберите пункт **Переместить или переименовать**.
   Откроется окно **<Название запроса>**.
4. В поле **Новое название** введите название запроса.
5. В раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить запрос.
6. Нажмите кнопку **Сохранить**.

Запрос изменен.

Кроме того, вы можете перемещать запросы, нажав ⋮ и в раскрывшемся меню выбрав пункт **Перенести в общие** или **Перенести в личные**.

6.2.6.8 Удаление запроса

❖ Чтобы удалить запрос:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Запросы** наведите курсор на запрос, нажмите ⋮.
3. В раскрывшемся меню выберите пункт **Удалить запрос** и подтвердите удаление.

Запрос удален.

6.2.7 Экспорт данных об активах в табличный список

Вы можете сохранить данные об активах в табличном списке для последующего использования в правилах корреляции и обогащения. При изменении данных об активах записи табличного списка автоматически обновляются.

❖ Чтобы экспортировать данные об активах в табличный список:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели **Группы активов** выберите одну или несколько групп, по активам которых формируется табличный список.

   Примечание. Для выбора нескольких групп используйте клавишу Ctrl.

3. В панели фильтрации настройте PDQL-запрос данных об активах, например:
   Select(@<Название поля 1>,@<Название поля 2>,...)| Sort(@<Название поля для сортировки>)
4. В панели инструментов нажмите кнопку **Создать табличный список**.

В новой вкладке браузера откроется веб-интерфейс Ankey SIEM NG Knowledge Base на странице **Новый табличный список**.

5. В поле **Название** введите название табличного списка.

> **Примечание.** В поле **Описание** вы можете ввести любой текстовый комментарий.

6. В раскрывающемся списке **Группы** установите флажки у групп Ankey SIEM NG Knowledge Base, в которые будет добавлен табличный список.
7. В раскрывающемся списке **Назначение** выберите **Данные об активах**.
8. Если нужно изменить список групп (по активам которых формируется табличный список), в раскрывающемся списке **Группы активов** установите флажки напротив названий этих групп.
9. Если нужно добавить активы из вложенных групп, установите флажок **Включать вложенные группы**.
10. В поле **PDQL-запрос** измените запрос к модели активов, указав названия колонок табличного списка, в виде:
    Select(@<Название поля 1> as <Название колонки 1>,@<Название поля 2> as <Название колонки 2>,...)| Sort(@<Название колонки для сортировки>)
11. Нажмите кнопку **Обновить схему**.
12. Нажмите кнопку **Создать**.
13. На странице **Табличные списки** в панели **Доступные списки** выберите созданный табличный список.
14. В панели инструментов нажмите кнопку **Установить в SIEM**.

Данные об активах экспортированы.

6.2.8 Экспорт данных об активах в CSV-файл

Данные об активах в системе могут быть представлены в виде таблицы. Вы можете экспортировать отфильтрованные и сгруппированные данные об активах из таблицы в файл формата CSV для последующего анализа.

❖ Чтобы экспортировать данные об активах в файл:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Выберите записи об активах.
3. Внизу таблицы активов в сообщении о количестве выбранных записей нажмите  .

Система сформирует CSV-файл и выгрузит его в локальную папку, указанную в свойствах браузера.

6.3 Работа с конфигурацией актива

В ряде случаев (например, при расследовании инцидентов или при анализе результатов сканирования) вам нужно видеть, различались ли конфигурации выбранного актива в два разных момента времени. Также вам может потребоваться история изменений, произошедших с активом, чтобы найти

в заданном промежутке времени опасные, подозрительные или интересные изменения актива.

6.3.1 Экспорт истории конфигурации актива

В ряде случаев (например, при расследовании инцидентов или при анализе результатов сканирования) вам может потребоваться история изменений, произошедших с активом.

Примечание. Вы можете экспортировать историю изменений только одного актива.

❖ Чтобы экспортировать историю изменений актива:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В таблице активов выберите актив.
3. В панели инструментов нажмите  и в раскрывшемся меню выберите пункт **Экспортировать историю конфигурации**.
   Откроется окно Параметры для экспорта.
4. Выберите период времени, за который вы хотите получить историю изменений конфигурации актива.
5. Установите флажки для нужных вам параметров конфигурации актива.
6. Нажмите кнопку **Экспортировать**.

Система сформировала XML-файл и выгрузила его в локальную папку, указанную в свойствах браузера. Файл содержит структурированное представление истории изменений, произошедших с активом за выбранный период времени, с учетом выбранных параметров конфигурации актива.

6.3.2 Сравнение конфигураций актива

В ряде случаев (например, при расследовании инцидентов или при анализе результатов сканирования) вам может потребоваться информация о том, различались ли конфигурации одного или нескольких выбранных активов в два разных момента времени.

Примечание. Если на любой из выбранных вами моментов времени актив не существовал, то система будет считать, что в этот момент времени актив не содержал ни одного элемента.

❖ Чтобы сравнить конфигурации одного или нескольких активов:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите ⇄.
   Откроется окно **Сравнение конфигураций для <N> активов**.
4. Выберите моменты времени, на которые будет производиться сравнение конфигураций.
5. Нажмите кнопку **Сравнить**.
   Откроется страница со списком активов. На ней отображаются интегральная уязвимость каждого актива, дата и время его создания, дата и время последнего обновления и дата удаления.

6. Если требуется, в панели инструментов включите **Только изменения**, чтобы исключить из просмотра те активы, по которым не было изменений.

Примечание. Вы можете просмотреть подробный результат сравнения конфигураций, выбрав интересующий вас актив.

Примечание. Также вы можете экспортировать в XML-файл результаты сравнения конфигураций по кнопке **Экспорт**.

6.4 Топология сети. Работа с картой сети

Реальные связи между активами в сети представлены в виде карты сети. Она строится на основе информации об активе или группе активов. Топология сети отображается на странице **Активы** на вкладке **Топология**. Вершинами графа являются активы сети, а ребрами − связи между ними.

Связи между активами отображаются на карте на основе данных об активе, полученных при сканировании сети в режиме белого ящика (модулем audit). Если данные актива изменились, то после сканирования карта обновится.

С помощью карты сети вы можете выявлять:

- связи между активами;
- отсутствие необходимых связей между активами;
- ошибки настройки активов (например, объединенные в кластер маршрутизаторы имеют разные параметры);
- проблемы архитектуры сети (например, активы из одной сети имеют разные сетевые маски);
- постороннее оборудование, подключенное к внутренним сетям.

Для удобства каждый тип актива на карте сети имеет свое графическое обозначение.

Таблица 6.1 − Графические обозначения активов на карте сети

Тип актива	Графическое обозначение
Рабочая станция	
Сервер	
Маршрутизатор	
Сетевой коммутатор	
Межсетевой экран	
Точка доступа	
Неизвестное сетевое устройство	
Сетевой принтер	
Узел	
Сеть	

Тип актива	Графическое обозначение
Служба каталогов Microsoft Active Directory	
Гипервизор	
Контроллер удаленного управления сервером (iDRAC или iLO)	

6.4.1 Настройка отображения активов на карте сети

На вкладке **Топология** вы можете:

- изменять число активов в сети, отображаемых на карте сети;
- изменять отображение карты сети в рабочей области;
- отображать или скрывать названия активов на карте сети.

Вы можете настраивать отображение активов на карте сети для одной или нескольких групп активов. Для удобства работы с системой вид карты сети сохраняется для каждой учетной записи пользователя.

Кроме того, вы можете изменять расположение активов на карте сети курсором мыши.

❖ Чтобы вернуть вид карты сети по умолчанию, в панели инструментов нажмите кнопку  **Расположить узлы по умолчанию**.

Выбор количества активов

По умолчанию на карте сети отображаются не более 20 активов, входящих в одну сеть. Вы можете изменить это максимальное число активов. Например, если необходимо просмотреть все активы, входящие в сеть.

❖ Чтобы выбрать максимальное число активов, отображаемых для одной сети:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели инструментов выберите вкладку **Топология**.
   Отобразится карта сети.
3. В панели инструментов нажмите .
   Откроется окно настройки вида карты сети.
4. Укажите число активов в поле **Уменьшать узлы в сетях больше <число> узлов**.

На карте для каждой сети отображено выбранное число активов.

Выбор отображения карты сети

Вы можете выбрать отображения карты сети в рабочей области − с прокруткой или без прокрутки.

Если выбран вариант без прокрутки, то на карте сети вы видите все активы и связи между ними. Карта сети занимает всю рабочую область, ее масштаб зависит от количества активов.

Если выбран вариант с прокруткой, то масштаб отображения активов на карте сети увеличивается. Карта сети выходит за пределы рабочей области.

❖ Чтобы выбрать отображение карты сети в рабочей области:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.

2. В панели инструментов выберите вкладку **Топология**.
   Отобразится карта сети.
3. В панели инструментов нажмите ⋮.
   Откроется окно настройки вида карты сети.
4. Выберите один из вариантов:
   - если вы хотите видеть сразу все активы на карте сети, выключите прокрутку;
   - если вы хотите увеличить масштаб отображения активов на карте сети, включите прокрутку.

Карта сети отображается в рабочей области в соответствии с выбранным вариантом.

Выключение отображения названий активов

По умолчанию на карте сети отображаются названия активов. Вы можете выключить отображение названий активов. Например, если на экране слишком много активов и их названия затрудняют восприятие информации и работу с картой сети.

❖ Чтобы выключить отображение названий активов на карте:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели инструментов выберите вкладку **Топология**.
   Отобразится карта сети.
3. В панели инструментов нажмите ⋮.
   Откроется окно настройки вида карты сети.
4. Выключите отображение названий узлов и сетей.

Отображение названий активов на карте выключено.

6.4.2 Просмотр информации об активе

На карте сети отображаются активы, удовлетворяющие условиям фильтра. Вы можете выбрать любой актив или связь между активами, чтобы просмотреть подробную информацию о них.

Активы, удовлетворяющие условиям фильтра, но не выбранные на карте, не изменяют цвет. Активы, выбранные на карте, выделены синим цветом. Активы и связи между активами, не удовлетворяющими условиям фильтра, изменяют цвет на серый.

Кнопки ↗↙ и ↙↗ позволяют сворачивать и разворачивать содержимое активов типа «Сеть».

По нажатию на актив открывается окно с базовой информацией о нем − мини-карточка актива. По ссылке **Карточка актива** вы можете перейти к просмотру состояния актива.

Для актива типа **«Сеть»** в окне с информацией на вкладке **Свойства** отображаются параметры, а на вкладке **Активы** − список активов.

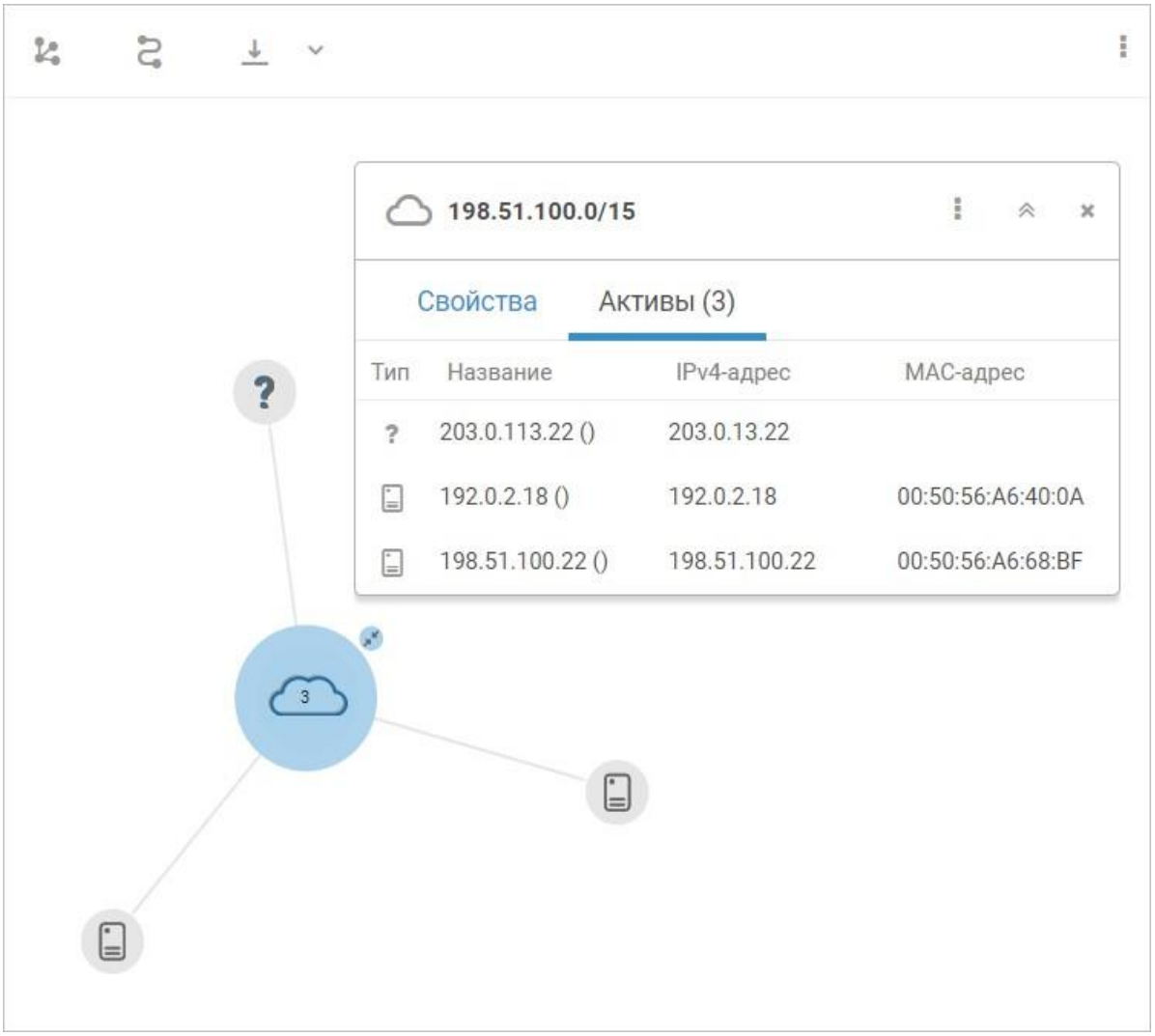

Рисунок 6.4 − Просмотр списка активов для актива типа **«Сеть»**

По нажатию на связь между активами открывается окно с информацией о типе активов, их параметрах и о связи между ними.

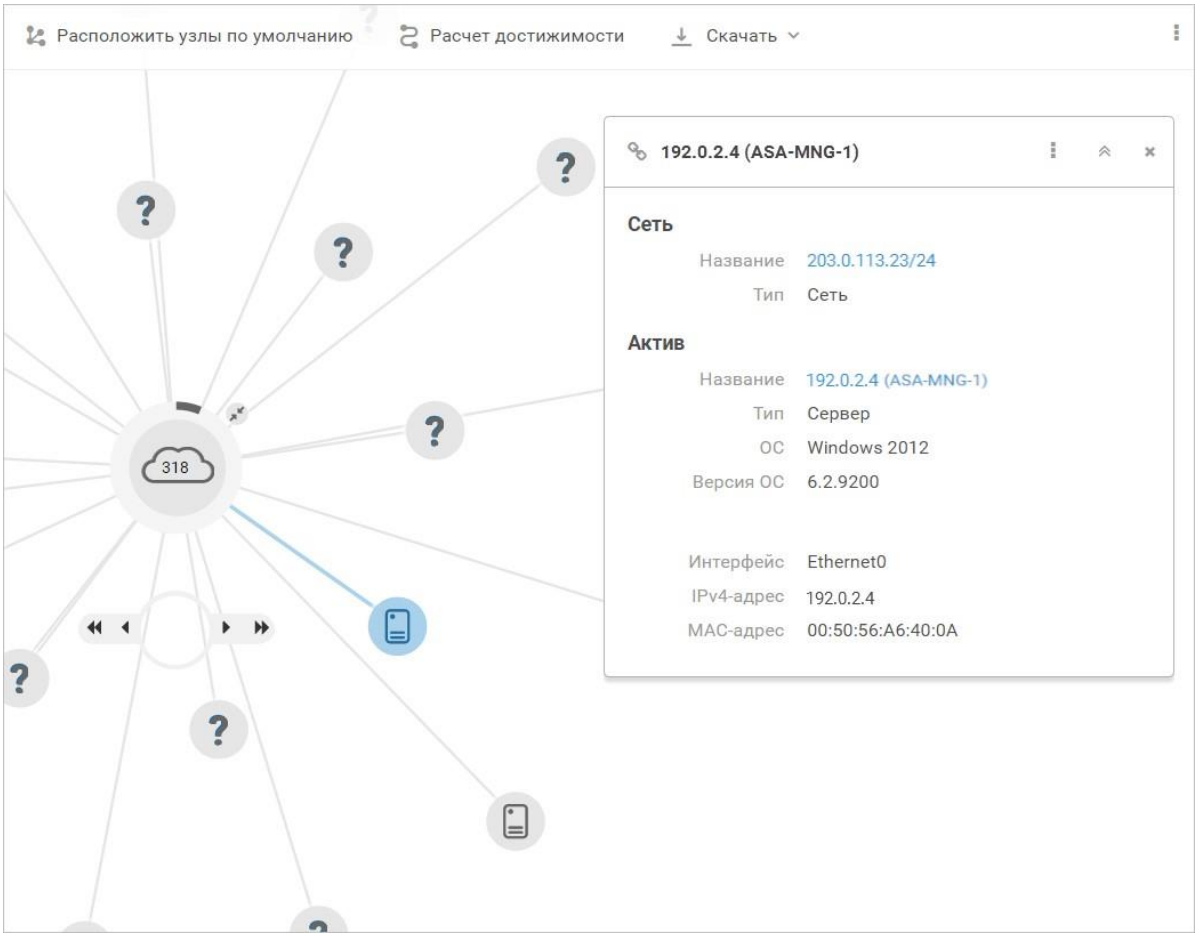

Рисунок 6.5 − Просмотр информации о связи между активами

❖ Чтобы свернуть окно с информацией об активе или связи между активами, нажмите ⌃⌃.

❖ Чтобы закрыть окно с информацией об активе или связи между активами, нажмите ✖.

6.4.3 Достижимость между активами

Достижимость − это свойство актива и группы активов, означающее возможность их взаимодействия с другими активами и группами активов в сети. Путь между достижимыми активами и группами активов (маршрут) определяется выбранными параметрами достижимости.

С помощью расчета достижимости вы можете:

- контролировать доступность активов и групп активов в сети;
- проверять правильность установки и настройки сетевых устройств;
- проверять работу политик доступа к активам и группам активов;
- уточнять список активов и групп активов, которые нужно проанализировать во время аудита;
- выявлять активы и группы активов, представляющие угрозу ИБ, и их связи с другими активами и группами активов.

Вы можете рассчитать достижимость от одного актива и (или) группы

активов или всех активов и сетевых адресов к активу и (или) группе активов, сетевому адресу, диапазону сетевых адресов.

Вы можете перейти к расчету достижимости по кнопке **Расчет достижимости** в панели инструментов.

6.4.3.1 Расчет достижимости от актива

Вы можете рассчитать достижимость от выбранного актива и (или) группы активов к другому активу и (или) группе активов, сетевому адресу, диапазону сетевых адресов.

❖ Чтобы рассчитать достижимость от актива:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите кнопку **Расчет достижимости** и в раскрывшемся меню выберите пункт **Куда открыт доступ**.
   В новой вкладке браузера откроется страница **Активы**, в таблице активов будут отображаться выбранные активы. В панели **Топология** откроется окно **Расчет достижимости**.
4. Активы, от которых рассчитывается достижимость, указаны в блоке параметров **Источники**.
5. В блоке параметров **Цели** выберите конечные точки маршрутов.
   Если требуется, укажите дополнительную информацию о протоколах и портах цели по ссылке **Уточнить протоколы и порты цели**.
6. Нажмите кнопку **Рассчитать маршруты**.
   Система сформирует списки доступных целей и маршрутов к ним.
7. Доступные сетевые адреса и маршруты к ним отобразятся на вкладке **Доступные**.
   Если требуется, по кнопке выберите способ группировки маршрутов.
8. Выберите конечную точку маршрута.

В раскрывающемся блоке отображаются маршруты достижимости выбранной цели, сгруппированные по парам «протокол – порт». Для маршрутов также могут отображаться правила маршрутизации, трансляции сетевых адресов (NAT) и списков управления доступом (ACL).

Маршрут достижимости отображается также на карте сети.

Кроме того, вы можете перейти к расчету достижимости по кнопке **Расчет достижимости** на вкладке **Топология**.

6.4.3.2 Расчет достижимости к активу

Вы можете рассчитать достижимость от актива и (или) группы активов или всех активов и сетевых адресов к выбранному активу и (или) группе активов.

❖ Чтобы рассчитать достижимость к активу:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите кнопку **Расчет достижимости** и в раскрывшемся меню выберите пункт **Откуда открыт доступ**.

В новой вкладке браузера откроется страница **Активы**, в таблице активов будут отображаться выбранные активы. В панели **Топология** откроется окно **Расчет достижимости**.

4. Активы, от которых рассчитывается достижимость, указаны в блоке параметров **Цели**.
   Если требуется, укажите дополнительную информацию о протоколах и портах цели по ссылке **Уточнить протоколы и порты цели**.
5. В блоке параметров **Источники** выберите начальные точки маршрутов. Начальными точками маршрутов могут быть активы, группы активов или все активы и сетевые адреса.
6. Нажмите кнопку **Рассчитать маршруты**.
   Система сформирует списки доступных источников и маршрутов к выбранным активам.
7. Если требуется, по кнопке выберите способ группировки маршрутов.
8. Выберите начальную точку маршрута.

В раскрывающемся блоке отображаются маршруты достижимости выбранной цели, сгруппированные по парам «протокол – порт». Для маршрутов также могут отображаться правила маршрутизации, трансляции сетевых адресов (NAT) и списков управления доступом (ACL).

Маршрут достижимости отображается также на карте сети.

Кроме того, вы можете перейти к расчету достижимости по кнопке **Расчет достижимости** на вкладке **Топология**.

6.4.4 Переход к работе с событиями и инцидентами из таблицы активов

Из таблицы активов вы можете перейти к работе с событиями и инцидентами, связанными с выбранными активами, а также найти задачи по сбору данных.

❖ Чтобы перейти из таблицы активов к работе с событиями:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В таблице активов выберите актив.
3. В панели инструментов выберите кнопку **Найти** и в раскрывшемся списке выберите пункт **Найти события**.

Откроется страница **События**. В рабочей области отобразится список событий, связанных с выбранным активом.

Также вы можете искать инциденты и задачи по сбору данных, связанные с выбранным активом.

6.4.5 Переход к работе с событиями и инцидентами с карты сети

Из карты сети вы можете перейти к работе с событиями и инцидентами, связанными с выбранным активом.

❖ Чтобы перейти к работе с событиями из карты сети:

1. В главном меню выберите раздел **Активы**. Откроется страница **Активы**.
2. В панели инструментов выберите вкладку **Топология**. Отобразится карта сети.

3. Выберите актив на карте сети.
   Откроется окно с информацией об активе.
4. Нажмите кнопку ⋮ и в раскрывшемся меню выберите пункт **Найти события**. Откроется страница **События**. В рабочей области отобразится список событий, связанных с выбранным активом.

Кроме того, из окна с информацией об активе вы можете перейти к работе с инцидентами, выбрав в меню ⋮ пункт **Найти инциденты**.

6.4.6 Экспорт топологии активов

ПК Ankey SIEM NG собирает информацию об активах в сети и представляет ее в виде карты. Вы можете экспортировать настроенную топологию сети в виде графического файла для последующего анализа.

❖ Чтобы экспортировать топологию сети:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели инструментов выберите вкладку **Топология**.
   Отобразится карта сети.
3. В панели инструментов нажмите кнопку **Скачать** и в раскрывшемся меню выберите формат графического файла: PNG или SVG.

Топология сети экспортирована.

6.4.7 Создание задачи на сбор событий с актива из таблицы активов

Вы можете получать информацию о событиях, произошедших на активах. Для этого требуется создать задачу на сбор событий с выбранного актива. Вы можете создать такую задачу из таблицы активов.

❖ Чтобы создать задачу на сбор событий с актива:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В таблице активов выберите актив.
3. В панели инструментов нажмите .

Откроется страница **Создание задачи на сбор данных**. Выбранный актив указан в панели **Цели сбора данных** в поле **Активы**.

6.4.8 Создание задачи на сбор событий с актива

Вы можете получать информацию о событиях, произошедших на активах. Для этого требуется создать задачу на сбор событий с выбранного актива. Вы можете перейти к созданию такой задачи из карты сети.

❖ Чтобы перейти к созданию задачи на сбор событий с актива:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели инструментов выберите вкладку **Топология**.
   Отобразится карта сети.
3. Выберите актив на карте сети.
4. Нажмите ⋮ и в раскрывшемся меню выберите пункт **Создать задачу по сбору данных**.

Откроется страница **Создание задачи на сбор данных**. Выбранный актив указан в панели **Цели сбора данных** в поле **Активы**.

7 Сбор данных

Примечание. Ankey SIEM NG Agent может одновременно собирать события не более чем с 1000 клиентских компьютеров или не более чем с 500 серверов.

Сбор событий с источников выполняется компонентом Ankey SIEM NG Agent. Компонент имеет модульную структуру и, в зависимости от используемых модулей, может выполнять различные задачи по сбору данных из IT-инфраструктуры организации. Модули можно разделить по типам собираемых данных на следующие группы:

- модули аудита − предназначены для поиска активов и сбора информации о них;
- пассивного сбора событий − предназначены для приема событий, отправляемых источниками;
- мониторинга − предназначены для сбора событий сразу после регистрации их на источниках;
- модули для периодического сбора событий, сохраненных на источниках.

Для настройки модуля и указания особенностей сбора событий с конкретного источника или сбора информации об активе для модулей создаются шаблоны настройки − профили. В зависимости от способа хранения событий на источнике (сетевая папка, журнал ОС, СУБД) или способа сбора информации об активах (сетевой протокол, API) используются специализированные алгоритмы сбора данных − транспорты. Для доступа к источнику или активу в параметрах транспорта можно указать данные учетной записи.

7.1 Работа с учетными записями

Учетные записи используются для авторизации и повышения привилегий на источнике событий или активе. При создании учетной записи вы можете указать один или нескольких транспортов, в которых она может использоваться.

Добавлять, изменять и удалять учетные записи вы можете на странице **Учетные записи**.

7.1.1 Добавление учетной записи типа «логин−пароль»

❖ Чтобы добавить учетную запись типа «логин−пароль»:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.
   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин-пароль**.
   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.
5. В поле **Логин** введите логин учетной записи.
6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

> **Примечание.** При вводе различаются заглавные и строчные буквы.

7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.1.2 Добавление учетной записи типа «пароль»

❖ Чтобы добавить учетную запись типа «пароль»:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.
   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.
   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

> **Примечание.** В поле **Описание** вы можете ввести любой текстовый комментарий.

4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.
5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

> **Примечание.** При вводе различаются заглавные и строчные буквы.

6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.1.3 Добавление учетной записи типа «сертификат»

❖ Чтобы добавить учетную запись типа «сертификат»:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.
   Откроется страница **Учетные записи**.
2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Сертификат**.
   Откроется страница **Добавление учетной записи**.
3. В поле **Название** введите название учетной записи.

Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.
5. В поле **Сертификат** введите путь к файлу сертификата.
   Вы можете указать расположение файла сертификата по ссылке **Выбрать** или перетащить файл в поле **Сертификат**.

Внимание! Размер файла сертификата должен быть меньше 100 КБ.

6. Если требуется, в поле **Логин** введите логин учетной записи.
7. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

Примечание. При вводе различаются заглавные и строчные буквы.

8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.1.4 Изменение учетной записи

❖ Чтобы изменить учетную запись:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.
   Откроется страница **Учетные записи**.
2. Выберите учетную запись.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. Измените параметры учетной записи.
5. Нажмите кнопку **Сохранить**.

Учетная запись изменена.

7.1.5 Удаление учетной записи

❖ Чтобы удалить учетную запись:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.
   Откроется страница **Учетные записи**.
2. В левой панели выберите учетную запись.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Учетная запись удалена.

7.2 Работа со справочниками

В справочниках могут храниться дополнительные данные и сценарии, необходимые для работы модулей. Например, справочники example_collect_process_changes, example_collect_tabular, example_collect_text содержат сценарии на языке программирования Python.

Справочники бывают стандартные и пользовательские. Стандартные справочники предустановлены, вы не можете их изменять и удалять. Создавать, изменять и удалять пользовательские справочники вы можете на странице **Справочники**.

7.2.1 Создание справочника

❖ Чтобы создать справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.
   Откроется страница **Справочники**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание справочника**.
3. В поле **Название** введите название справочника.
4. В поле **Содержимое** введите текст для справочника.
   Для деления текста на колонки вы можете использовать табуляцию (комбинация клавиш Alt+009). Вы также можете написать текст в любом текстовом редакторе и скопировать в поле **Содержание**.
5. Нажмите кнопку **Сохранить**.

Справочник создан.

7.2.2 Копирование справочника

❖ Чтобы скопировать справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.
   Откроется страница **Справочники**.
2. Выберите справочник.
3. В панели инструментов нажмите кнопку **Копировать**.
   Откроется окно **Создание справочника**.
4. Если нужно, измените справочник.
5. Нажмите кнопку **Сохранить**.

Справочник скопирован.

7.2.3 Изменение пользовательского справочника

❖ Чтобы изменить пользовательский справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.
   Откроется страница **Справочники**.
2. Выберите пользовательский справочник.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется страница **Редактирование справочника**.
4. В поле **Название** измените название справочника.
5. В поле **Содержимое** измените содержимое справочника.
6. Нажмите кнопку **Сохранить**.

Пользовательский справочник изменен.

7.2.4 Удаление справочника

❖ Чтобы удалить пользовательский справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.
   Откроется страница **Справочники**.

2. Выберите пользовательский справочник.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Пользовательский справочник удален.

7.3 Работа с профилями

Профиль − шаблон настройки модуля, описывающий особенности сбора событий с источников или аудита активов.

Профили используются для сохранения параметров модулей. Профили бывают стандартные и пользовательские. Стандартные профили предустановлены, вы не можете их изменять и удалять. На базе стандартных вы можете создавать пользовательские профили и настраивать параметры сбора данных. Создавать, изменять и удалять пользовательские профили вы можете на странице **Профили**.

7.3.1 Создание пользовательского профиля на базе стандартного

❖ Чтобы создать пользовательский профиль на базе стандартного:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
   Откроется страница **Профили**.
2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **На базе выбранного профиля**.
   Откроется страница **Новый профиль**.
4. В поле **Название** введите название профиля.
5. Если требуется, в панели **Параметры профиля** в раскрывающемся списке **Учетная запись** выберите учетную запись для сбора данных.
   В зависимости от профиля для выбора учетной записи вам может потребоваться указать другие параметры профиля или выбрать другой пункт в иерархическом списке.

   Примечание. В раскрывающемся списке **Учетная запись** отображаются учетные записи, при добавлении которых была выбрана метка используемого профилем метода сбора данных или не было выбрано никаких меток.

6. Если требуется, настройте другие параметры профиля.

   Примечание. Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

7. Нажмите кнопку **Сохранить**.

Пользовательский профиль создан.

7.3.2 Изменение пользовательского профиля

❖ Чтобы изменить пользовательский профиль:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
   Откроется страница **Профили**.
2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется страница **Профили / <Название профиля>**.
4. Измените параметры профиля.

> **Примечание.** Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

5. Нажмите кнопку **Сохранить**.

Пользовательский профиль изменен.

7.3.3 Экспорт параметров профиля

При экспорте параметров пользовательского профиля в файле формата JSON сохраняются название и GUID стандартного профиля, на базе которого создан пользовательский профиль, и параметры, отличающиеся от указанных по умолчанию.

❖ Чтобы экспортировать параметры пользовательского профиля:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
   Откроется страница **Профили**.
2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. В панели **Параметры профиля** нажмите кнопку **Экспорт**.

> **Примечание.** Кнопка **Экспорт** доступна, если параметры пользовательского профиля отличаются от параметров стандартного профиля, на базе которого он создан.

Параметры пользовательского профиля экспортированы и сохранены в файле <Название профиля>_<Дата и время экспорта>.json.

7.3.4 Удаление пользовательского профиля

❖ Чтобы удалить пользовательский профиль:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
   Откроется страница **Профили**.
2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Пользовательский профиль удален.

7.4 Работа с задачами

Для получения данных с IT-инфраструктуры организации в

ПК Ankey SIEM NG необходимо создать задачу. В задаче необходимо указать цели, с которых нужно получить данные, например IP-адреса или добавленные в систему активы (группы активов). Вы можете запускать задачу вручную или настроить запуск по расписанию. В рамках задачи система создает подзадачи, которые выполняются автоматически. В зависимости от выбранного в задаче профиля с помощью компонента Ankey SIEM NG Agent запускается соответствующий модуль для сбора данных. Задачи могут использоваться для:

- обнаружения узлов. Система вносит информацию обо всех обнаруженных в IT-инфраструктуре организации активах в хранилище активов;
- сканирования активов методом черного ящика. Система обнаруживает открытые порты и сетевые сервисы на этих портах. Затем обнаруживает уязвимости на сетевых сервисах;
- аудита активов методом белого ящика. Система определяет детальную конфигурацию операционной системы, установленной на активе, перечень установленного на активе программного обеспечения, список открытых портов, перечень пользователей, которые зарегистрированы на активе. Формирует перечень уязвимостей и карту сети;
- сканирования веб-приложения. Система обнаруживает параметры веб-приложения, выявляет уязвимые параметры, формирует перечень уязвимых библиотек;
- сбора событий с источников. Система собирает события журналирования и привязывает их к активам, на которых они обнаружены. На основе собранных событий система обнаруживает события, связанные с рисками информационной безопасности, и регистрирует инциденты;
- поиска уязвимостей на активах в режиме пентест. Система выполнит поиск на активах уязвимостей с указанными CVE-идентификаторами;
- поиска индикаторов компрометации в событиях. Система выполнит проверку полученных ранее событий на наличие в них индикаторов компрометации по данным табличных списков;
- ретроспективной корреляции событий. Система выполнит повторную проверку полученных ранее событий по выбранным правилам корреляции;
- Импорта офлайн-журналов событий.

Вы можете создавать, изменять, удалять, запускать и останавливать задачи на странице **Задачи по сбору данных**. Кроме того, вы можете перейти к просмотру истории запусков подзадач по ссылке **История запусков**.

7.4.1 Создание задачи на сбор данных

❖ Чтобы создать задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.
   Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите профиль.
5. Если требуется, в раскрывающемся списке **Учетная запись** выберите учетную запись для сбора данных.
   В зависимости от профиля для выбора учетной записи вам может потребоваться указать другие параметры профиля или выбрать другой пункт в иерархическом списке.

> **Примечание.** В раскрывающемся списке **Учетная запись** отображаются учетные записи, при добавлении которых была выбрана метка используемого профилем метода сбора данных или не было выбрано никаких меток. По умолчанию выбрана учетная запись, указанная в профиле.

6. Если требуется, настройте другие параметры профиля.

> **Примечание.** Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

7. Если требуется, в раскрывающемся списке **Агент** выберите Ankey SIEM NG Agent для сбора данных.
8. Если в системе заведено больше одной инфраструктуры, в раскрывающемся списке **Инфраструктура** выберите инфраструктуру.
9. В панели **Цели сбора данных** на вкладке **Включить** укажите цели:
   - если вы хотите сканировать группу активов, укажите ее в поле **Группы активов**;
   - если вы хотите сканировать отдельные активы, укажите их в поле **Активы**;
   - если вы хотите сканировать конкретные сетевые узлы, укажите их IP-адреса, FQDN или маски подсетей в поле **Сетевые адреса**.

> **Примечание.** Вы также можете изменить приоритетный способ подключения к активам − по полному доменному имени (FQDN) или по IP-адресу. По умолчанию выбран приоритет подключения по FQDN актива, так как вероятность его изменения ниже, чем у IP-адреса. Подключение по FQDN позволяет увеличить согласованность результатов сбора данных и реализовать поддержку протокола Kerberos. При невозможности подключения к активу по FQDN используется подключение по IP-адресу, и наоборот.

Примечание. В поле **Сетевые адреса** вы также можете указывать локальные сетевые адреса, например localhost, 127.0.0.1, ::1. Это может потребоваться для использования модуля RemoteExecutor.

10. Если требуется, установите флажок **Выполнить обнаружение узлов до начала сбора данных**.
    Обнаружение узлов до начала сбора данных позволяет сократить общее время сканирования.
11. Если требуется исключить отдельные цели сбора данных, укажите их на вкладке **Исключить**.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

12. Выполните одно из следующих действий:
    - если вы хотите запустить задачу сразу после создания, нажмите кнопку **Сохранить и запустить**;
    - если вы хотите запустить задачу позднее, нажмите кнопку **Сохранить**.

Задача создана.

7.4.2 Создание задачи на поиск уязвимостей

❖ Чтобы создать задачу на поиск уязвимостей в режиме пентест:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
   Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Поиск уязвимостей в режиме пентеста**.
   Откроется окно **Создание задачи на поиск уязвимостей**.
3. В поле **CVE уязвимостей** укажите CVE-идентификаторы уязвимостей.

Примечание. Вы можете просмотреть полный список CVE-идентификаторов уязвимостей, для которых доступны проверки в Ankey SIEM NG, выполнив на странице **Активы** запрос `select(@VulnerPassport, VulnerPassport.HasPentestCheck, VulnerPassport.CVEs) | filter(VulnerPassport.HasPentestCheck = true and VulnerPassport.CVEs).`

4. Нажмите кнопку **Создать**.
   Откроется страница **Создание задачи на поиск уязвимостей**.
5. Если необходимо, в поле **Название** измените название задачи.
6. Если требуется, в раскрывающемся списке **Агент** выберите Ankey SIEM NG Agent для сбора данных.
7. В панели **Цели сбора данных** на вкладке **Включить** укажите цели:
   - если вы хотите сканировать группу активов, укажите ее в поле **Группы активов**;

– если вы хотите сканировать отдельные активы, укажите их в поле **Активы**.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

8. Выполните одно из следующих действий:
   – если вы хотите запустить задачу сразу после создания, нажмите кнопку **Сохранить и запустить**;
   – если вы хотите запустить задачу позднее, нажмите кнопку **Сохранить**.

Задача создана.

7.4.3 Создание задачи на импорт событий из файла журнала

❖ Чтобы создать задачу на импорт событий из файла журнала:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Импорт журнала**. Откроется страница **Создание задачи на сбор данных**.
3. В поле **Название** введите название задачи.
4. Если требуется, в раскрывающемся списке **Профиль** выберите пользовательский профиль, созданный на базе профиля FileImporter.
5. В раскрывающемся списке **Протокол подключения** выберите протокол.
6. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.
7. В иерархическом списке выберите пункт **Обработка событий** → **<Папка не указана>**.
8. В поле **Папка журнала** введите имя общей папки с файлами журнала на источнике.

Примечание. Если файлы журнала расположены во вложенной папке, при вводе пути используйте \.

9. Если требуется, в раскрывающемся списке **Агент** выберите Ankey SIEM NG Agent для сбора данных.
10. Если в системе добавлено больше одной инфраструктуры, в раскрывающемся списке **Инфраструктура** выберите инфраструктуру.
11. В панели **Цели сбора данных** на вкладке **Включить** в поле **Сетевые адреса** введите IP-адрес источника событий.

Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.

12. Выполните одно из следующих действий:
    - если вы хотите запустить задачу сразу после создания, нажмите кнопку **Сохранить и запустить**;
    - если вы хотите запустить задачу позднее, нажмите кнопку **Сохранить**.

Задача на импорт событий создана.

7.4.4 Поиск и фильтрация задач

Вы можете настроить фильтр по статусам задач, их целям, используемым в них модулям, профилям, транспортам и учетным записям; по агентам, которые выполняют задачи или инфраструктурам (если их несколько).

❖ Чтобы настроить фильтр задач:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
   Откроется страница **Задачи по сбору данных**.
2. В панели **Все задачи** нажмите кнопку .
   Откроется панель фильтрации.
3. Нажмите кнопку с названием параметра задачи.
   Откроется окно для выбора значений параметра.
4. Если вы настраиваете фильтр по агентам, модулям, профилям, статусам задач, транспортам, учетным записям или инфраструктурам, в открывшемся окне установите флажки напротив значений параметров.

   Примечание. Вы можете использовать поле поиска в верхней части окна для поиска значения параметра.

5. Если вы настраиваете фильтр по целям задачи, укажите цели следующими способами:
   - в раскрывающемся списке **Группы активов** установите флажки напротив групп активов;
   - в поле **Активы** укажите один или несколько активов;
   - в поле **Сетевые адреса** введите IP-адрес, диапазон IP-адресов, маску подсети или FQDN.
6. Нажмите кнопку с названием параметра задачи.

   Примечание. Вы можете очистить значения для одного параметра задачи, нажав рядом с его названием , или очистить фильтры, нажав в панели фильтрации.

Задачи отфильтрованы в соответствии с условием.

7.4.5 Запуск задачи вручную

❖ Чтобы запустить задачу вручную:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
   Откроется страница **Задачи по сбору данных**.
2. В списке выберите задачу.
3. В панели инструментов нажмите кнопку **Запустить**.

Задача запущена.

7.4.6 Остановка задачи

Вы можете останавливать задачи, например чтобы снизить нагрузку на оборудование в сети.

❖ Чтобы остановить задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.
2. В списке выберите задачу.
3. В панели инструментов нажмите кнопку **Остановить**.

Задача остановлена.

7.4.7 Просмотр истории запусков задачи

При каждом запуске задачи (по расписанию или вручную) автоматически создается подзадача.

❖ Чтобы просмотреть историю запусков задачи:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.
2. В панели **Все задачи** выберите задачу.
3. По ссылке **История запусков** откройте страницу **История запусков <Название задачи>**.

В панели **Подзадачи** отображается история запусков задачи.

Примечание. Вы можете настроить период для просмотра запусков задачи, указав его по ссылке **за все время**, или настроить фильтр (по статусам подзадач, их целям или по агентам, которые выполняют подзадачи), нажав в панели **Подзадачи**.

Вы можете просмотреть журнал подзадачи по кнопке **Журнал подзадачи** или экспортировать его в текстовый файл по кнопке **Скачать журнал**.

7.4.8 Просмотр журнала подзадачи

❖ Чтобы просмотреть журнал подзадачи:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.
2. В панели **Все задачи** выберите задачу.
3. По ссылке **История запусков** откройте страницу **История запусков <Название задачи>**.
4. В панели **Подзадачи** выберите подзадачу.

Примечание. Вы можете настроить фильтр подзадач, нажав .

5. Нажмите кнопку **Журнал подзадачи**.

Откроется страница **Журнал подзадачи от <Период журнала>**.

Вы можете экспортировать журнал подзадачи в текстовый файл по кнопке **Скачать журнал**.

7.4.9 Копирование задачи

❖ Чтобы скопировать задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.

2. В списке выберите задачу.
3. В панели инструментов нажмите кнопку **Копировать**.
   Откроется окно **Создание задачи на сбор данных**.
4. Если нужно, измените параметры задачи.
5. Нажмите кнопку **Сохранить**.

Задача скопирована.

7.4.10 Настройка задачи

❖ Чтобы настроить задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
   Откроется страница **Задачи по сбору данных**.
2. В списке выберите задачу.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется страница **Задачи / <Название задачи>**.
4. Измените параметры задачи и выбранного профиля.

> **Примечание.** Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

5. Нажмите кнопку **Сохранить**.

Задача настроена.

7.4.11 Экспорт параметров профиля

Вы можете экспортировать измененные параметры профиля, выбранного в задаче. При экспорте параметров в файле формата JSON сохраняются название и GUID стандартного профиля и параметры, отличающиеся от указанных по умолчанию.

❖ Чтобы экспортировать параметры профиля, выбранного в задаче:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
   Откроется страница **Задачи по сбору данных**.
2. В панели **Все задачи** выберите задачу.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется страница **Задачи / <Название задачи>**.
4. В панели **Параметры сбора данных** нажмите кнопку **Экспорт**.

> **Примечание.** Кнопка **Экспорт** доступна, если профиль отличается от стандартного.

Параметры профиля экспортированы и сохранены в файле <Название задачи>_<Дата и время экспорта>.json.

7.4.12 Удаление задачи

❖ Чтобы удалить задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
   Откроется страница **Задачи по сбору данных**.
2. В списке выберите задачу.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача удалена.

7.5 Мониторинг доступности активов

Ankey SIEM NG осуществляет мониторинг доступности активов. Эта функция реализована в виде набора профилей, специфичных для каждой информационной системы. При запуске задачи с выбранным профилем происходит сканирование целевой системы на наличие возможных проблем. В случае обнаружения неисправности или незапланированного отключения актива Ankey SIEM NG информирует пользователя: создается событие, на основе которого формируется инцидент.

Вы можете настроить отправку соответствующих уведомлений по электронной почте (см. Руководство администратора Ankey SIEM NG 4.1.2).

Для сбора данных необходимо создать задачу, параметры сканирования которой будут определяться профилем. В зависимости от ситуации необходимо использовать определенный профиль, чтобы выявить неисправность. Большинство стандартных профилей не требуют настройки для мониторинга и готовы к использованию. Однако вы можете внести изменения в стандартный профиль (например, изменить протокол или порты). Результатом сканирования является созданное в системе событие. Выберите его из списка событий, чтобы просмотреть детали.

Таблица 7.1 − Рекомендуемые профили

Ситуация	Рекомендуемые профили
Сбои в работе ПО сетевого оборудования	Service Availability Monitoring, Monitoring Linux Services, Monitoring Unix Services
Отключение или перезагрузка сетевого оборудования	Host Availability Monitoring
Сбои в работе операционных систем	Service Availability Monitoring, Host Availability Monitoring
Проблемы с доступностью серверов, входящих в состав сети	Host Availability Monitoring, Monitoring Windows CPU Load, Monitoring Linux CPU Load, Monitoring Unix CPU Load
Проблемы с наличием свободного места на жестком диске и загрузкой оперативной памяти на серверах, входящих в состав сети	Monitoring Windows HDD Free Space, Monitoring Windows RAM Load, Monitoring Linux HDD Free Space, Monitoring Linux RAM Load, Monitoring Unix HDD Free Space, Monitoring Unix RAM Load
Остановка, отключение или перезагрузка операционных систем	Monitoring Windows CPU Load, Monitoring Windows RAM Load, Monitoring Linux CPU Load, Monitoring Linux RAM Load, Monitoring Unix CPU Load, Monitoring Unix RAM Load
Проблемы с доступностью и работоспособностью служб и сервисов информационной сети	Monitoring Linux Services, Monitoring Unix Services, Service Availability Monitoring
Сбои и отказы в работе средств защиты информации	Monitoring Linux Services, Monitoring Unix Services, Service Availability Monitoring
Отключение или перезагрузка средств защиты информации	Monitoring Linux Services, Monitoring Unix Services,

Ситуация	Рекомендуемые профили
	Service Availability Monitoring

7.6 Мониторинг источников событий

Для уменьшения вероятности пропуска инцидентов ИБ необходимо своевременно отслеживать состояние источников событий и потока данных от них. Качество и непрерывность сбора данных с источников влияют на оперативность выявления инцидентов и принятия решений.

Данные от источников передаются в ПК Ankey SIEM NG напрямую (без посредников) или через промежуточный актив − форвардер (например, через контроллер домена). Форвардер, кроме пересылки данных от других активов, также может отправлять данные от находящихся в нем источников.

Источники и форвардеры появляются в системе автоматически, по мере сбора событий с активов и их идентификации. На странице **Мониторинг источников** пользователь системы может просмотреть состояние источников и параметры потока данных от них или состояние форвардеров и параметры находящихся в них источников. Ссылка для выбора типа элементов (источников или форвардеров) находится в верхней части рабочей области страницы.

7.6.1 Просмотр списка источников и списка потоков событий от источника

❖ Чтобы просмотреть список источников:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите пункт **ПК Ankey SIEM NG**.
   Откроется главная страница.
2. В главном меню в разделе **Сбор данных** выберите пункт **Мониторинг источников**.
   Откроется страница **Мониторинг источников**.

В центральной панели отображена таблица со списком источников.

Для каждого источника в таблице указаны значения параметров. Вы можете сортировать список, нажимая на название колонки (параметра). Нажимая ⚙ в правом верхнем углу страницы, вы можете отображать и скрывать колонки таблицы.

Примечание. Срок хранения данных, полученных от источника, 30 дней.

Для автоматизации мониторинга потока событий от источников или форвардеров администратор системы создает предупреждения для отслеживания наличия событий, средней скорости потока событий и задержки в получении события агентом. Состояние предупреждения отображается в колонке **Контроль** соответствующим значком:

- ✔ − параметры потока событий находятся в пределах допустимых значений;
- ⓘ − параметры потока событий вышли за пределы допустимых значений;
- ⊘ − предупреждение отключено.

При наведении курсора мыши на значок предупреждения во

всплывающем окне отображается информация об отслеживаемых параметрах потока событий.

Примечание. Источник автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Также удаляются данные, полученные от источника.

❖ Чтобы просмотреть список потоков событий от источника, откройте страницу со списком потоков событий двойным щелчком мыши на строке с названием источника.

7.6.2 Просмотр списка форвардеров и списка источников форвардера

❖ Чтобы просмотреть список форвардеров:

1. В главном меню нажмите ☰ и в раскрывшемся меню выберите пункт **ПК Ankey SIEM NG**.
   Откроется главная страница.
2. В главном меню в разделе **Сбор данных** выберите пункт **Мониторинг источников**.
   Откроется страница Мониторинг источников.

В центральной панели отображена таблица со списком форвардеров.

Для каждого форвардера в таблице указаны значения параметров. Вы можете сортировать список, нажимая на название колонки (параметра). Нажимая ⚙ в правом верхнем углу страницы, вы можете отображать и скрывать колонки таблицы.

Примечание. Срок хранения данных, полученных от форвардера, 30 дней.

Для автоматизации мониторинга потока событий от источников или форвардеров администратор системы создает предупреждения для отслеживания наличия событий, средней скорости потока событий и задержки в получении события агентом. Состояние предупреждения отображается в колонке Контроль соответствующим значком:

- − параметры потока событий находятся в пределах допустимых значений;
- − параметры потока событий вышли за пределы допустимых значений;
- − предупреждение отключено.

При наведении курсора мыши на значок предупреждения во всплывающем окне отображается информация об отслеживаемых параметрах потока событий.

Примечание. Форвардер автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Также удаляются данные, полученные от форвардера.

❖ Чтобы просмотреть список источников форвардера, откройте страницу со списком источников двойным щелчком мыши на строке с названием форвадера.

8 Работа с событиями

ПК Ankey SIEM NG обеспечивает:

- сбор событий, произошедших на активах;
- фильтрацию событий;
- создание инцидентов по событиям, связанным с информационной безопасностью;
- различное представление данных о событиях;
- привязку событий к инцидентам.

Вы можете управлять событиями на странице **События**. По умолчанию на ней отображаются все события, связанные с группами активов, к которым вам предоставлен доступ.

Кроме того, пользователь с ролью администратора ПК Ankey SIEM NG может настраивать автоматическую отправку на адрес электронной почты уведомлений о появлении событий и отчетов (см. раздел 12.8).

8.1 Фильтрация и группировка событий

По умолчанию на странице **События** в таблице отображаются все события, созданные ПК Ankey SIEM NG за последний час и связанные с активами из групп, к которым у вас есть доступ (включая вложенные группы).

Для удобства анализа и для выпуска отчетов вы можете фильтровать события с помощью стандартных и пользовательских фильтров.

Вы можете отобразить события:

- произошедшие в выбранный период;

> **Примечание.** Если интервал между временем регистрации события на источнике и временем сбора события Ankey SIEM NG Agent превышает 24 часа (и при сборе событие не было отмечено как устаревшее), то событие попадет в период, включающий дату и время сбора события.

- связанные с выбранной группой активов;
- отвечающие условиям стандартных или пользовательских фильтров;
- отвечающие условиям запроса на языке PDQL;
- хранящиеся на других площадках;
- принадлежащие тем или иным конвейерам обработки событий.

Кроме того, с помощью PDQL-запроса вы можете изменить состав колонок таблицы событий, а также указать порядок сортировки записей. Для удобства анализа вы можете сгруппировать события.

Также вы можете ограничить количество событий в таблице, например для получения графиков вида «топ-10» в виджетах.

Если вы хотите регулярно настраивать представление данных в таблице с помощью набора полей событий и их значений, вы можете сохранить этот набор как фильтр.

Примечание. В приложении В «Фильтрация событий агентом ПК Ankey SIEM NG» представлены настройки профилей сбора для отбрасывания лишних событий.

8.1.1 Фильтрация событий по периоду

Вы можете фильтровать события в таблице по периоду. По умолчанию в рабочей области на странице **События** отображаются события за последний час.

❖ Чтобы отфильтровать события по периоду:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. Нажмите и во всплывающем окне укажите период.
3. Нажмите кнопку **Применить**.

События отфильтрованы.

8.1.2 Фильтрация событий по группе активов

Вы можете использовать группы активов, чтобы фильтровать события в таблице событий.

Иерархический список групп активов отображается на странице **События** в панели **Группы**.

❖ Чтобы отфильтровать события по группе активов:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Группы** выберите группу активов.

События отфильтрованы.

8.1.3 Фильтрация событий с помощью сохраненных фильтров

Вы можете использовать стандартные и сохраненные пользовательские фильтры, чтобы фильтровать события в таблице событий. Иерархический список фильтров отображается на странице **События** в панели **Фильтры**.

❖ Чтобы отфильтровать события с помощью фильтра:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** выберите фильтр.

События отфильтрованы.

8.1.4 Использование для фильтрации событий выполненного ранее запроса

Чтобы отфильтровать события с помощью выполненного ранее запроса:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите .
   Откроется панель **История запросов**.
3. Выберите запрос.

Примечание. Вы можете отметить часто используемые запросы, нажав ☆ в строке запроса.

События отфильтрованы.

8.1.5 Фильтрация событий с помощью PDQL-запроса

Вы можете использовать запросы на языке PDQL, чтобы фильтровать события в таблице событий.

❖ Чтобы отфильтровать события с помощью PDQL-запроса:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите .
   Откроется окно PDQL-запроса.
3. Выполните одно из следующих действий:
   – если вы хотите добавить введенное условие в запрос для фильтрации событий, нажмите кнопку **Добавить**;
   – если вы хотите отправить PDQL-запрос на получение событий с введенными параметрами, нажмите кнопку **Выполнить (Ctrl + Enter)**.

События в таблице отфильтрованы в соответствии с условием PDQL-запроса.

Если вы планируете далее работать с этим фильтром, вы можете сохранить его в папку (см. раздел 8.2.4).

8.1.6 Выбор конвейеров для фильтрации событий

По умолчанию для фильтрации доступны события всех конвейеров локального приложения. Если требуется ограничить количество событий, вы можете выбрать нужные вам конвейеры. Для фильтрации станут доступны события только выбранных конвейеров.

❖ Чтобы выбрать конвейеры:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите .
3. Во всплывающем окне выберите конвейеры обработки событий.
4. Нажмите кнопку **Добавить**.

Конвейеры выбраны.

Вы можете сохранить фильтр (см. раздел 8.2) по событиям выбранных конвейеров. Вместе с тем необходимо учитывать ряд ограничений при работе с такими фильтрами. Если конвейер недоступен, при использовании фильтра появятся сообщения об ошибках в виджете на дашборде или в отчете, созданном в конструкторе, а также при выпуске отчета.

Также сообщение об ошибке будет содержать уведомление о событиях, созданное с таким фильтром.

8.1.7 Выбор связанных приложений для фильтрации событий

При развертывании Ankey SIEM NG на нескольких площадках администратор системы может настроить связи между приложениями Ankey SIEM NG и предоставить тому или иному пользователю права доступа к распределенному поиску событий. В этом случае пользователь сможет работать (см. раздел 8.1) в интерфейсе одного приложения со всеми событиями, собранными как на локальной площадке, так и на площадках связанных приложений, независимо от прав доступа к событиям, установленным для его

ролей.

❖ Чтобы выбрать связанные приложения:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите .
3. Во всплывающем окне выберите приложения.
4. Нажмите кнопку **Добавить**.

Связанные приложения выбраны. Их события доступны для фильтрации.

Вы можете сохранить фильтр (см. раздел 8.2) событий связанных приложений. Вместе с тем необходимо учитывать ряд ограничений при работе с такими фильтрами. Если пользователь не имеет прав доступа к распределенному поиску событий:

- при выборе таких фильтров он не может создавать или изменять отчеты по шаблону, а также выпускать их вручную;
- в виджетах, использующих такие фильтры, будет отображаться сообщение об ошибке (на дашборде или в отчете, созданном в конструкторе).

Также при выборе подобных фильтров невозможно будет создать уведомление о задачах сбора данных.

8.1.8 Выбор колонок для таблицы событий

По умолчанию в таблице событий отображаются дата и время, когда произошло событие, информация об активе, на котором произошло событие, а также описание события. Заголовки колонок таблицы соответствуют названиям полей событий. Вы можете изменять состав колонок таблицы с помощью операции выбора полей. Кроме того, вы можете использовать псевдонимы, чтобы переименовывать колонки таблицы событий для удобства представления информации.

В качестве псевдонима вы можете использовать один или несколько символов, которые заменят название поля события. Например, для поля «count» вы можете указать псевдоним «Количество событий».

Примечание. Псевдоним для поля, указанный при операции выбора колонок, сохраняется для всей последовательности операций в рамках одного запроса для фильтрации событий. Для результатов операций группировки и агрегации вы можете указать другие псевдонимы.

❖ Чтобы выбрать колонки для таблицы событий:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите .
3. В открывшемся окне **Выбор полей** выберите колонки для таблицы событий.
4. Если требуется переименовать колонку, нажмите на ее заголовок, в открывшемся окне укажите псевдоним и нажмите .
5. Выполните одно из следующих действий:
   - если вы хотите добавить выбор полей в запрос для фильтрации событий, нажмите кнопку **Добавить**;

– если вы хотите отправить запрос на отображение выбранных колонок в таблице событий, нажмите кнопку **Выполнить (Ctrl + Enter)**.

В таблице событий отображены выбранные колонки с данными.

Если вы планируете далее работать с этим выбором колонок, вы можете сохранить его в папку (см. раздел 8.2.4).

8.1.9 Сортировка записей в таблице событий

❖ Чтобы отсортировать данные в таблице событий:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите ⇵.
3. В открывшемся окне **Сортировка по полям** укажите колонки таблицы событий, по которым требуется выполнить сортировку.
4. Если требуется, измените направление сортировки.
5. Выполните одно из следующих действий:
   – если вы хотите добавить условие сортировки в запрос для фильтрации событий, нажмите кнопку **Добавить**;
   – если вы хотите отправить запрос на сортировку событий, нажмите кнопку **Выполнить (Ctrl + Enter)**.

Данные в таблице событий отсортированы.

8.1.10 Группировка и анализ данных о событиях с помощью математических операций

Для подготовки аналитической информации вы можете группировать и агрегировать (выполнять математические операции над сгруппированными данными (см. приложение Б)) данные о событиях. Для удобства просмотра результатов анализа (например, на виджетах) вы можете указывать псевдонимы для групп событий, полученных в результате выполнения операции группировки, и для результатов выполнения операции агрегации событий.

В качестве псевдонима вы можете использовать один или несколько символов, которые заменят название поля события, по которому была выполнена операция. Например, при группировке по полю «action» вы можете указать для результата псевдоним «Действие».

❖ Чтобы сгруппировать и проанализировать данные о событиях:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите ⋮≡.
   Откроется окно группировки и анализа данных.
3. В раскрывающемся списке **Группировка** выберите поля, по которым требуется сгруппировать события.
4. Если требуется, укажите псевдоним для результата группировки.
5. В раскрывающемся списке **Агрегация** выберите функцию.
6. В раскрывающемся списке выберите название колонки таблицы, над данными которой требуется выполнить математическую операцию.
7. В раскрывающемся списке выберите аргумент функции.
8. Если требуется, укажите псевдоним для результата агрегации.
9. Выберите интервалы времени, по которым требуется распределить результаты анализа.

Примечание. Вы можете удалять математические операции по нажатию в строке операции.

10. Выполните одно из следующих действий:
    - если вы хотите добавить условия группировки и агрегации в запрос для фильтрации событий, нажмите кнопку **Добавить**;
    - если вы хотите отправить запрос на выполнение операций, нажмите кнопку **Выполнить (Ctrl + Enter)**.

События в таблице сгруппированы и проанализированы в соответствии с условиями.

- Чтобы скрыть колонки с условиями группировки, нажмите .
- Чтобы отобразить колонки с условиями группировки, нажмите .

8.1.11 Ограничение количества событий в таблице событий

- Чтобы ограничить количество событий в таблице событий:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации нажмите .
3. В открывшемся окне снимите флажок **Показать все строки** и в поле **Максимальное количество строк** введите количество строк таблицы.
4. Выполните одно из следующих действий:
   - если вы хотите добавить введенное ограничение в запрос для фильтрации событий, нажмите кнопку **Добавить**;
   - если вы хотите отправить запрос на ограничение количества событий в таблице, нажмите кнопку **Выполнить (Ctrl + Enter)**.

Количество событий в таблице ограничено.

8.2 Работа с сохраненными фильтрами

В ПК Ankey SIEM NG предусмотрены стандартные фильтры для событий. Эти фильтры расположены в папках, вложенных в папку **Стандартные фильтры**.

Примечание. Вы не можете изменять или удалять стандартные папки и фильтры.

Для решения рабочих задач вы можете создавать в папке **Пользовательские фильтры** вложенные папки и помещать туда пользовательские фильтры. Кроме того, вы можете делать фильтры доступными для других пользователей. Для этого фильтр требуется поместить в папку **Общие фильтры**.

Вы можете работать с фильтрами событий на странице **События**.

8.2.1 Создание папки фильтров

Для удобства работы вы можете создавать папки, чтобы помещать туда

фильтры для поиска событий по выбранным критериям.

❖ Чтобы создать папку фильтров:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** нажмите кнопку +.
   Откроется окно **Новая папка фильтров**.
3. В поле **Название** введите название папки фильтров.
4. В раскрывающемся списке **Внутри папки** выберите папку, внутри которой требуется создать папку фильтров.
   По умолчанию папка создается внутри папки **Пользовательские фильтры**.
5. Нажмите кнопку **Создать**.

Папка фильтров создана.

Кроме того, вы можете перейти к созданию папки внутри уже созданной папки фильтров, наведя курсор на созданную папку и нажав ⋮.

8.2.2 Изменение папки фильтров

Вы можете изменить название пользовательской папки фильтров или переместить ее в другую папку.

❖ Чтобы изменить папку фильтров:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** наведите курсор на пользовательскую папку, нажмите ⋮ и в раскрывшемся меню выберите пункт **Редактировать**.
   Откроется окно **Редактирование папки фильтров**.
3. В поле **Название** измените название папки фильтров.
4. В раскрывающемся списке **Внутри папки** выберите папку, в которую требуется переместить папку фильтров.
5. Нажмите кнопку **Сохранить**.

Папка фильтров изменена.

8.2.3 Удаление папки фильтров

Вы можете удалить пользовательскую папку фильтров. При удалении папки все вложенные папки и фильтры также будут удалены.

❖ Чтобы удалить папку фильтров:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** наведите курсор на пользовательскую папку, нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и при необходимости подтвердите удаление.

Папка фильтров удалена.

8.2.4 Сохранение пользовательского фильтра

Для удобства работы вы можете сохранить пользовательский фильтр событий.

❖ Чтобы сохранить пользовательский фильтр:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. Отфильтруйте события с помощью PDQL-запроса.

Условие фильтра будет добавлено в PDQL-запрос над таблицей событий.

3. В панели фильтрации нажмите  и в раскрывшемся меню выберите пункт **Сохранить как**.
   Откроется окно **Новый фильтр**.
4. В поле **Название** введите название пользовательского фильтра.
5. Если требуется, в раскрывающемся списке **Внутри папки** выберите папку, в которую требуется переместить этот фильтр.
6. Нажмите кнопку **Сохранить**.

Фильтр сохранен.

8.2.5 Создание пользовательского фильтра на основе существующего фильтра

Вы можете создать пользовательский фильтр на основе имеющегося фильтра − стандартного или пользовательского.

❖ Чтобы создать фильтр на основе имеющегося:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** выберите фильтр.
   Условие фильтра будет добавлено в PDQL-запрос над таблицей событий.
3. Нажмите на условие фильтра.
   Откроется окно PDQL-запроса.
4. Измените условие фильтра на языке запроса PDQL.
5. Нажмите кнопку **Применить**.
6. В панели фильтрации нажмите  и в раскрывшемся меню выберите пункт **Сохранить как**.
   Откроется окно **Новый фильтр**.
7. В поле **Название** введите название пользовательского фильтра.
8. Если требуется, в раскрывающемся списке **Внутри папки** выберите папку, в которую требуется переместить этот фильтр.
9. Нажмите кнопку **Сохранить**.

Фильтр создан.

8.2.6 Создание копии пользовательского фильтра

Вы можете создать копию пользовательского фильтра событий, например чтобы на ее основе создать новый пользовательский фильтр (см. раздел 8.2.5).

❖ Чтобы создать копию пользовательского фильтра:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** наведите курсор на пользовательский фильтр, нажмите и в раскрывшемся меню выберите пункт **Сделать копию**.

Копия фильтра создана в той же папке, в которой расположен исходный фильтр. К названию исходного пользовательского фильтра прибавляется слово «_Копия».

8.2.7 Изменение условия пользовательского фильтра

Вы можете изменить сохраненный пользовательский фильтр. Например,

в условии фильтрации на языке PDQL вы можете изменить порядок сортировки отфильтрованных событий в таблице.

❖ Чтобы изменить пользовательский фильтр:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** выберите пользовательский фильтр.
   Условие фильтра будет добавлено в PDQL-запрос над таблицей событий.
3. Нажмите на условие фильтра.
   Откроется окно PDQL-запроса.
4. Измените условие фильтра на языке запроса PDQL.
5. Нажмите кнопку **Применить**.
6. В панели фильтрации нажмите  и в раскрывшемся меню выберите пункт **Сохранить**.
   Откроется окно **Редактирование фильтра**.
7. Нажмите кнопку **Сохранить**.

Условие пользовательского фильтра изменено.

8.2.8 Удаление пользовательского фильтра

❖ Чтобы удалить пользовательский фильтр:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели **Фильтры** наведите курсор на пользовательский фильтр, нажмите  , в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Пользовательский фильтр удален.

8.3 Создание исключения на основе данных события ИБ

Для многих правил корреляции в системе предусмотрен механизм обработки ложных срабатываний, реализованный на основе табличных списков для исключений. При выявлении ложного срабатывания в один из таких табличных списков необходимо внести данные, указанные в корреляционном событии (например, имя узла, на котором зарегистрировано событие, или идентификатор учетной записи, с которой связана подозрительная активность). Выбор табличного списка зависит от правила. После добавления данных в табличный список события с таким же данными не будут регистрироваться правилом корреляции.

Добавлять данные для исключений в табличный список вы можете вручную из Ankey SIEM NG Knowledge Base (согласно описанию пакета экспертизы, в который входит правило) или автоматически по ссылке из сводки о корреляционном событии.

Внимание! Автоматическое добавление данных для исключений доступно только в табличные списки, для которых создан шаблон исключений (см. раздел 16.13.1.2).

❖ Чтобы создать исключение на основе данных корреляционного события:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В таблице событий выберите корреляционное событие.

> **Примечание.** Для поиска корреляционных событий вы можете использовать PDQL-запрос correlation_name != null и группировку по полю события correlation_name.

3. В панели **Сводка** по ссылке **Добавить исключение** откройте всплывающее окно для работы с исключениями.
   В окне расположены блок с уже созданными исключениями, ссылки для создания исключений разных типов и ссылка на табличный список, в который вносятся исключения.

> **Примечание.** Вы можете удалить созданное ранее исключение по кнопке  .

4. В блоке **Добавить исключение** по ссылке с типом исключения откройте окно для выбора исключения по данным события.
   Справа от каждой ссылки указаны количество событий, подпадающих под это исключение, и ссылка на таблицу с этими событиями.
5. По ссылке с данными события добавьте исключение.

Исключение на основе данных корреляционного события создано.

8.4 Настройка представления и экспорт результатов анализа данных о событиях

В ПК Ankey SIEM NG вы можете изменять представление результатов анализа данных о событиях. Вы также можете экспортировать результаты из системы в виде файла формата PNG.

Перед настройкой представления данных о событиях вам нужно их отфильтровать, сгруппировать и проанализировать.

❖ Чтобы настроить представление результатов анализа данных о событиях:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели инструментов нажмите  .
   Откроется страница настройки представления данных.
3. В блоке представления данных выберите тип представления – **Таблица**, **Столбчатая диаграмма**, **График** или **Круговая диаграмма**.
4. Если требуется, настройте легенду: выберите отображение и расположение маркеров.
5. Если требуется, включите и настройте отображение подписей значений на графике.

Примечание. При установленном флажке **Разрешить наложение** на представлении будут отображаться подписи всех значений, даже если они будут перекрывать друг друга.

6. Если требуется, включите подписи осей и в полях **X** и **Y** введите наименования осей.
7. Если требуется, настройте отображение подписей значений на оси X.

Примечание. При установленном флажке **Разрешить поворот** подписи значений, если они не помещаются горизонтально, будут повернуты.

Представление результатов анализа данных о событиях настроено.

При выборе элемента (например, столбца диаграммы) открывается страница веб-интерфейса системы с подробной информацией.

Настроенное представление результатов вы можете сохранить в виде виджета по кнопке **Сохранить в библиотеку виджетов**.

По кнопке **Назад к списку событий** вы можете вернуться к отображению результатов анализа данных в виде таблицы событий.

8.5 Ошибки при просмотре событий

При возникновении в ПК Ankey SIEM NG проблем в работе с событиями в рабочей области страницы **События** отображаются сообщения об ошибках. Одновременно отображаются не более трех ошибок.

В зависимости от типа учетной записи сообщение об ошибке содержит текст разного уровня детализации. Для пользователя отображаются код ошибки, ее описание и наименование компонента, в работе которого произошел сбой. Для пользователя с ролью администратора дополнительно приводится более детальная информация об источнике ошибки (например, сетевой адрес).

Если с ошибкой связаны другие ошибки, вы можете просмотреть информацию о них по ссылке **Показать вложенные ошибки**.

Вы можете скопировать текст ошибки, чтобы передать его администратору системы или в службу технической поддержки.

- Чтобы скопировать текст ошибки, в блоке с текстом ошибки нажмите .

Текст ошибки (вместе с описанием вложенных ошибок) будет скопирован в буфер обмена.

9 Работа с инцидентами

ПК Ankey SIEM NG помогает вам выявлять и расследовать инциденты информационной безопасности.

Инцидент информационной безопасности (также инцидент) − это одно или несколько нежелательных или неожиданных событий, которые могут повлиять на информационную безопасность организации.

Примерами инцидентов ИБ могут служить:

- несанкционированное изменение данных;
- установка запрещенного ПО;
- обнаружение вируса;
- сканирование сети;
- спам;
- утечка данных.

ПК Ankey SIEM NG предназначен для выявления инцидентов и помогает анализировать и расследовать инциденты, а также хранить информацию о них.

ПК Ankey SIEM NG сканирует IT-инфраструктуру организации с помощью модулей и собирает информацию, на основе которой формирует внутреннюю модель активов.

На основе анализа событий ПК Ankey SIEM NG автоматически или вы вручную можете регистрировать инциденты информационной безопасности.

ПК Ankey SIEM NG помогает вам точно и быстро реагировать на инциденты, что позволит в кратчайшие сроки восстановить работоспособность IT-инфраструктуры организации и свести к минимуму неблагоприятное влияние инцидентов на IT-инфраструктуру организации.

Процесс работы с инцидентами в ПК Ankey SIEM NG состоит из следующих этапов:

1. Выявление инцидентов.
2. Приоритизация инцидентов.
3. Анализ инцидента.
4. Расследование инцидента.

Выявление инцидентов

Цель этапа: узнать о появлении инцидента (если он создан автоматически) или, если вы обнаружили его самостоятельно, внести информацию о нем в ПК Ankey SIEM NG.

Если инцидент был создан автоматически, вы можете узнать об этом из уведомления, пришедшего на вашу электронную почту. Статус созданного инцидента в системе – **Новый**.

Инциденты со статусом **Новый** переходят на следующий этап жизненного цикла в системе − этап приоритизации инцидентов.

Приоритизация инцидентов

Цель этапа: выбрать инциденты, которые вам нужно взять в работу в первую очередь.

Ваши действия:

1. Отсортировать и отфильтровать инциденты с помощью встроенных в ПК Ankey SIEM NG инструментов − сортировки и фильтрации:
   - сортировка инцидентов. Вы можете сортировать инциденты по параметрам: по времени создания, по степени опасности, по статусу;
   - фильтрация инцидентов. Вы можете использовать стандартные, временные или свои настроенные (пользовательские) фильтры, чтобы быстро найти нужный вам инцидент или группу инцидентов по заданным параметрам.
2. Выполнить диагностику инцидента. В ходе диагностики вы должны принять решение о том, нужен ли дальнейший анализ и расследование инцидента:
   - если инцидент является ложным срабатыванием, вы должны изменить его статус с **Новый** на **Закрыт**. Инцидент будет храниться в системе со статусом **Закрыт (ложное срабатывание)**, изменение этого статуса невозможно;
   - если инцидент является истинным (не ложным срабатыванием), вы должны изменить его статус с **Новый** на **Утвержден**. Утвержденный инцидент переходит на следующий этап жизненного цикла инцидента в системе − этап анализа.

Анализ инцидента

Цель этапа: расширить контекст инцидента и принять решение, нужно ли дальнейшее расследование.

Ваши действия:

1. Проанализировать связи инцидента; события и активы, привязанные к инциденту; данные из карточки.
2. Принять решение, нужно ли дальнейшее расследование или инцидент был разрешен без вашего участия:
   - если инцидент был разрешен без вашего участия (например, был создан инцидент **Обнаружение вируса**, но к этапу анализа антивирус уже успел удалить вредоносное ПО), вы должны изменить статус инцидента с **Утвержден** на **Закрыт**;
   - если нужно дальнейшее расследование, вы должны изменить статус инцидента с **Утвержден** на **В работе**. Инцидент со статусом **В работе** переходит на следующий этап жизненного цикла в системе − этап расследования.

Примечание. На этапе расследования изменение названия и описания статуса инцидента становится недоступным.

Расследование инцидента

Цель этапа: определить источник угроз, выявить обстоятельства, которые привели к возникновению инцидента, собрать доказательства инцидента, дать рекомендации по устранению инцидента и закрыть инцидент.

Ваши действия:

1. Категоризировать инцидент. Вы должны оценить ситуацию и предварительно присвоить инциденту категорию на основе информации, доступной вам на момент выявления инцидента: например, **Установка запрещенного ПО** или **Утечка данных**.
2. Локализовать инцидент. Вы должны просмотреть топологию инцидента и достижимости, чтобы определить, какие активы вовлечены в инцидент.
3. Поставить задачи по инциденту. Вы можете поставить задачу на другого сотрудника, чтобы привлечь его к расследованию инцидента, сбору доказательств по инциденту или восстановлению работоспособности системы. В рамках расследования каждого инцидента вы можете создавать несколько задач.
4. Разработать план и принять меры по инциденту. После того, как вы исследовали все обстоятельства инцидента, вам нужно разработать планы и дать рекомендации вовлеченным в инцидент сотрудникам, чтобы предотвратить повторное возникновение выявленного инцидента. Затем вы должны изменить статус инцидента с **В работе** на **Разрешен**.
5. Проконтролировать исполнение рекомендаций (опционально):
   - если ваши рекомендации выполнены, а инцидент и последствия устранены, вы должны изменить статус инцидента с **Разрешен** на **Закрыт**. Принятые меры по инциденту вам нужно зафиксировать в карточке инцидента.
   - если ваши рекомендации не выполнены либо принятых мер оказалось недостаточно и инцидент возникает повторно, вы должны изменить статус инцидента с **Разрешен** на **В работе**.

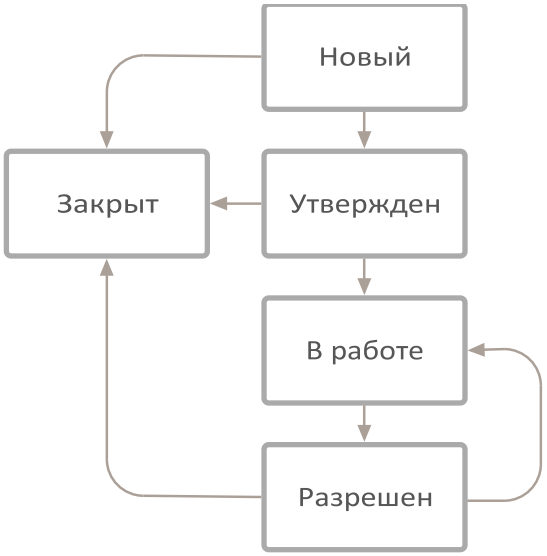

Рисунок 9.1 – Статусы инцидента

В любой момент работы с инцидентами вы можете экспортировать их в унифицированном формате обмена для последующего импорта в другие системы.

Также вы можете просматривать ключевые показатели работы по инцидентам, например отслеживать динамику появления инцидентов, как быстро они обрабатываются, сколько времени в среднем тратится на устранение инцидента.

На странице Инциденты вы можете просматривать таблицу инцидентов и выполнять типовые действия с инцидентами.

9.1 Выявление инцидентов

На этапе выявления инцидентов ваша цель − узнать о появлении инцидента (если он создан автоматически) или, если вы обнаружили его самостоятельно, внести информацию о нем в ПК Ankey SIEM NG.

Инциденты выявляются в ПК Ankey SIEM NG следующими способами:

- ПК Ankey SIEM NG создает инцидент и отправляет вам на электронную почту уведомление об инциденте;
- вы создаете инцидент вручную;
- вы импортируете инциденты из ПК Ankey SIEM NG, относящегося к IT-инфраструктуре сети другого филиала, или из других систем управления событиями безопасности.

Автоматическое уведомление об инциденте

При возникновении события, которое может нарушить работу сети, ПК Ankey SIEM NG создает инцидент автоматически. Также событие может быть агрегировано с несколькими уже существующими инцидентами.

Агрегация необходима для того, чтобы вы могли накопить информацию, необходимую для первичной оценки инцидента, в рамках одного инцидента и при этом уменьшить количество повторяющихся однотипных инцидентов.

ПК Ankey SIEM NG может сообщать пользователям по электронной почте об изменении состава группы активов, о событиях и состоянии инцидентов.

Для отправки уведомлений по электронной почте необходимо настроить ПК Ankey SIEM NG.

Создание инцидента вручную

Если вы обнаружили, что в системе сработало правило корреляции, или заметили подозрительное поведение системы, вы можете:

- создать инцидент на странице **Инциденты**;
- создать инцидент из списка событий;
- привязать к ранее созданному инциденту одно или несколько событий.

Импорт инцидентов

Вы можете импортировать инциденты (см. раздел 9.6.2) из территориально распределенного ПК Ankey SIEM NG или из других систем управления событиями IT-безопасности в унифицированном формате обмена − JSON.

Подробная информация об автоматических уведомлениях содержится в Руководстве администратора Ankey SIEM NG 4.1.2.

9.1.1 Создание инцидента вручную

При возникновении события, которое может нарушить работу IT-инфраструктуры сети, ПК Ankey SIEM NG создает инцидент автоматически. Вы можете создать инцидент вручную в следующих случаях:

- инцидент был выявлен другими людьми (например, сотрудник другого подразделения сообщил об атаке);
- инцидент был выявлен вами на основе вашей экспертной оценки.

❖ Чтобы создать инцидент:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется страница создания нового инцидента.
3. Заполните блок параметров **Параметры**:
   - в поле **Название** введите название инцидента, которое позволит определить характер инцидента;

     Примечание. Ограничение на ввод – 200 символов.

   - если требуется, в поле **Описание** введите подробное текстовое описание инцидента, указав все необходимые для его обработки сведения;

     Примечание. Ограничение на ввод – 2000 символов.

   - в раскрывающемся списке **Расположение** выберите все группы активов, связанные с инцидентом;
   - если требуется, в поле **Обнаружен** укажите дату и время обнаружения инцидента вручную или с помощью значков ^ и v;

Примечание. Дата и время обнаружения инцидента не могут быть больше текущей даты и времени.

- в раскрывающемся списке **Категория и тип** выберите категорию и тип инцидента;
- в раскрывающемся списке **Влияние** выберите, какое воздействие оказывает инцидент на активы.

4. Заполните блок **Статус**:
   - в раскрывающемся списке **Опасность** выберите степень опасности создаваемого инцидента – высокую, среднюю или низкую;
   - если требуется, в раскрывающемся списке **Ответственный** выберите пользователя системы, который назначается ответственным за создаваемый инцидент.

Примечание. Если вы оставите поле **Ответственный** незаполненным, то в карточке инцидента после сохранения будет отображаться значение **Не назначен**.

5. Если требуется, заполните блок параметров **Активы и сети**:
   - в раскрывающемся списке **Группы активов** выберите одну или несколько атакованных групп активов;
   - в раскрывающемся списке **Активы** выберите один или несколько атакованных активов;
   - в раскрывающемся списке **Сети** выберите один или несколько IP-адресов атакованных сетей;
   - в поле **Сетевые адреса** введите один или несколько DNS-адресов атакованных сетей;
   - если требуется, в поле **Прочие активы и сети** введите один или несколько активов, или IP-адресов сетей, или DNS-адресов сетей, связанных с атакованными активами.

Примечание. В этом поле вы можете указать информацию по атакованным активам и сетям, которые еще не зарегистрированы в системе.

6. Если требуется, заполните блок параметров **Атакующие активы**, указав информацию об атакующих активах и сетях.
7. Нажмите кнопку **Сохранить**.

Инцидент создан. Созданный инцидент отображается в таблице инцидентов.

9.1.2 Создание инцидента с привязкой к событию

Если вы обнаружили, что событие информационной безопасности в ПК Ankey SIEM NG сигнализирует о возможном сбое в работе актива, вы можете создать инцидент с привязкой к событию.

❖ Чтобы создать инцидент с привязкой к событию:

1. В главном меню выберите раздел События.
2. В таблице событий укажите одно или несколько событий и в панели инструментов нажмите кнопку **Создать инцидент**.

Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.

Откроется окно Создание инцидента.

3. В поле **Название** введите название инцидента, которое позволит определить характер инцидента.

Примечание. Ограничение на ввод – 200 символов.

4. Если требуется, в поле **Описание** введите подробное текстовое описание инцидента, указав все необходимые для его обработки сведения.

Примечание. Ограничение на ввод – 2000 символов.

5. В поле **Группы** выберите группы активов, которые задействованы в инциденте.
6. В раскрывающемся списке **Категория и тип** выберите категорию и тип инцидента.

Примечание. Набор полей после раскрывающегося списка **Категория и тип** будет зависеть от выбранных вами категории и типа инцидента.

7. В раскрывающемся списке **Опасность** выберите степень опасности создаваемого инцидента – высокую, среднюю или низкую.
8. В поле **Обнаружен**:
   - в календаре выберите дату обнаружения инцидента или введите эту дату вручную;
   - выберите с помощью стрелок ^ и v время обнаружения инцидента.
9. Если требуется, в раскрывающемся списке **Ответственный** выберите пользователя системы, которого вы назначаете ответственным за инцидент.
10. В раскрывающемся списке **Влияние** выберите, какое воздействие оказывает инцидент на активы.
11. Нажмите кнопку **Сохранить**.

Инцидент создан. На странице **События** отображается сообщение о создании инцидента со ссылкой на этот инцидент.

9.1.3 Обновление списка инцидентов

Вы можете обновлять список инцидентов вручную или настроить автоматическое обновление списка.

❖ Чтобы обновить список инцидентов:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.

2. Выберите желаемый вариант обновления списка инцидентов:
   - если вы хотите обновить список инцидентов вручную, нажмите ;
   - если вы хотите, чтобы список инцидентов обновлялся автоматически, нажмите , установите флажок **Автоматически обновлять** и выберите нужный вам период обновления.

9.2 Приоритизация инцидентов

В процессе выявления инцидентов может быть создано множество инцидентов. Одновременно взять все инциденты в работу невозможно, поэтому вы должны приоритизировать инциденты − распределить их по срочности и важности реакции на них.

Чтобы расставить приоритеты в работе с инцидентами, используйте фильтрацию и сортировку инцидентов.

Фильтрация инцидентов

Фильтры инцидентов бывают стандартными и пользовательскими.

Стандартные фильтры являются предустановленными, у вас нет возможности их изменять или удалять. В стандартном временном фильтре вы можете выбирать из предустановленных значений временной интервал инцидентов (по умолчанию установлено значение **за последние 7 дней**).

Пользовательские фильтры инцидентов вы можете создавать самостоятельно. Также для группировки и быстрого поиска созданных фильтров вы можете добавлять пользовательские папки фильтров.

Сортировка инцидентов

Вы можете сортировать инциденты по времени создания, по статусу, по уровню опасности. Сортировка инцидентов по умолчанию является многоуровневой. Это означает, что вы можете отсортировать инциденты по нескольким полям. Сортировка производится в том порядке, в котором указаны поля для сортировки. Для каждого поля сортировки вы можете указать направление сортировки.

9.2.1 Фильтрация инцидентов по периоду

Вы можете фильтровать инциденты по периоду, используя стандартный временной фильтр. По умолчанию на странице **Инциденты** в таблице инцидентов отображаются незакрытые инциденты за последние 7 дней.

❖ Чтобы отфильтровать список инцидентов по периоду:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. Нажмите и во всплывающем окне укажите период.

Примечание. Если выбран вариант **текущий квартал (текущий год)**, в таблице инцидентов отображаются инциденты за период от начала текущего квартала (текущего года) до настоящего момента.

3. Нажмите кнопку **Применить**.

В таблице инцидентов отображаются инциденты за выбранный период.

9.2.2 Фильтрация инцидентов по группе активов

В инцидентах участвуют активы, входящие в стандартные и пользовательские группы активов. Вы можете фильтровать инциденты по принадлежности к группам активов. Иерархический список групп активов отображается на странице **Инциденты**. Инциденты из вложенных групп отображаются по умолчанию.

Примечание. Инциденты, которые не привязаны к активам (группа «Непривязанные инциденты»), доступны только пользователю с ролью администратора.

❖ Чтобы отфильтровать инциденты в таблице инцидентов по группе активов:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. Если необходимо, настройте отображение групп активов требуемого типа в панели **Инциденты** по кнопке .
3. В панели **Инциденты** выберите группу активов.
   Название группы активов отобразится над таблицей инцидентов.
   В таблице инцидентов отобразятся инциденты, произошедшие на активах из выбранной группы.
4. Если требуется скрыть инциденты из вложенных групп, в панели **Инциденты** по кнопке под раскрывающимся списком **Тип группы** снимите флажок **Показывать инциденты из вложенных групп**.

9.2.3 Фильтрация инцидентов с помощью стандартных или пользовательских фильтров

Вы можете использовать стандартные или сохраненные пользовательские фильтры, чтобы фильтровать инциденты в таблице инцидентов. Иерархический список фильтров отображается на странице **Инциденты** в панели **Фильтры**.

Примечание. Вы можете отфильтровать список инцидентов только по одному фильтру.

❖ Чтобы отфильтровать инциденты в таблице инцидентов с помощью стандартного или пользовательского фильтра:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** выберите фильтр.
   Название фильтра отображается над таблицей инцидентов.

В таблице инцидентов отображаются инциденты, удовлетворяющие условиям фильтрации.

9.2.4 Фильтрация инцидентов с помощью PDQL-запроса

Вы можете использовать запросы на языке PDQL, чтобы фильтровать инциденты в таблице инцидентов. Запросы вы можете создавать из атрибутов инцидента или вручную.

❖ Чтобы отфильтровать инциденты по атрибутам инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В таблице инцидентов выберите атрибут инцидента (например, статус инцидента).
3. Во всплывающем окне выберите условие фильтрации.
4. Условие добавлено в PDQL-запрос над таблицей инцидентов.

Инциденты в таблице отфильтрованы в соответствии с условиями PDQL-запроса.

Вы также можете указать PDQL-запрос для фильтрации инцидентов вручную.

❖ Чтобы отфильтровать инциденты с помощью PDQL-запроса:

1. Над таблицей инцидентов нажмите **<Название фильтра инцидентов>**.
   Откроется всплывающее окно с PDQL-запросом.
2. Нажмите кнопку **Применить**.

Инциденты в таблице отфильтрованы в соответствии с условиями PDQL-запроса.

9.2.5 Работа с пользовательскими фильтрами инцидентов

ПК Ankey SIEM NG позволяет создавать пользовательские фильтры инцидентов. Пользовательские фильтры помогают быстро находить и брать в работу инциденты, соответствующие вашим критериям, и сохранять параметры поиска. Для группировки и быстрого поиска созданных фильтров вы можете добавлять пользовательские папки фильтров. В этом разделе содержатся инструкции по работе с пользовательскими фильтрами и пользовательскими папками фильтров.

Вы можете работать с фильтрами по инцидентам на странице **Инциденты**.

9.2.5.1 Создание пользовательской папки фильтров инцидентов

Для удобства работы вы можете создавать папки, чтобы помещать туда фильтры для поиска инцидентов по выбранным вами критериям.

Существуют следующие ограничения на создание папок для пользовательских фильтров:

- имена папок должны быть уникальными на одном уровне. Если вы попробуете сохранить или перенести фильтр в папку, которая уже содержит фильтр с таким названием, ПК Ankey SIEM NG выведет сообщение об ошибке;
- максимальный уровень вложенности − 30 папок;
- максимальная длина имени фильтра − 256 символов;
- максимальная длина строки условия − 4000 символов.

❖ Чтобы создать пользовательскую папку фильтров:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** нажмите кнопку +.
   Откроется окно **Новая папка фильтров**.
3. В поле **Название** укажите название папки.
4. Если требуется, в раскрывающемся списке **Внутри папки** выберите расположение папки.
   По умолчанию папка создается внутри папки **Пользовательские фильтры**.
5. Нажмите кнопку **Создать**.

Созданная папка отображается в списке пользовательских фильтров инцидентов.

9.2.5.2 Изменение пользовательской папки фильтров инцидентов

Вы можете изменить название пользовательской папки фильтров или переместить ее в другую папку.

❖ Чтобы изменить пользовательскую папку:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** наведите курсор на пользовательскую папку, нажмите ⋮ и в раскрывшемся меню выберите пункт **Редактировать**.
   Откроется окно **Редактирование папки фильтров**.
3. В поле **Название** измените название папки фильтров.
4. В раскрывающемся списке **Внутри папки** выберите папку, в которую требуется переместить пользовательскую папку фильтров.
5. Нажмите кнопку **Сохранить**.

Пользовательская папка фильтров изменена.

9.2.5.3 Удаление пользовательской папки фильтров инцидентов

Вы можете удалить пользовательскую папку фильтров.

Внимание! При удалении папки все вложенные папки и фильтры также будут удалены.

❖ Чтобы удалить пользовательскую папку фильтров:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** наведите курсор на пользовательскую папку, нажмите ⋮ и в раскрывшемся меню выберите пункт **Удалить**.

Пользовательская папка фильтров удалена.

9.2.5.4 Создание пользовательского фильтра инцидентов

❖ Чтобы создать пользовательский фильтр:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Инциденты** выберите группу активов.
3. В таблице инцидентов по ссылке с пунктирным подчеркиванием выберите атрибут инцидента (например, статус).
4. Во всплывающем окне выберите условие фильтрации.
   Условие будет добавлено в PDQL-запрос над таблицей инцидентов.

   Примечание. Вы можете выбрать несколько условий фильтрации.

5. Нажмите ссылку с PDQL-запросом.
   Откроется всплывающее окно с PDQL-запросом.

   Примечание. Вы также можете указать запрос для фильтрации инцидентов вручную.

6. Нажмите кнопку **Сохранить**.
   Откроется окно **Новый фильтр**.
7. В поле **Название** введите название пользовательского фильтра.
8. В поле **Папка** укажите папку, в которой будет сохранен пользовательский фильтр.
9. Нажмите кнопку **Сохранить**.

Созданный пользовательский фильтр отображается в списке фильтров инцидентов.

9.2.5.5 Создание пользовательского фильтра инцидентов на основе существующего фильтра

Вы можете создать пользовательский фильтр на основе существующего фильтра − стандартного или пользовательского.

❖ Чтобы создать фильтр на основе существующего:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** выберите фильтр.
   Условие фильтра будет добавлено в PDQL-запрос над таблицей инцидентов.
3. Нажмите на условие фильтра.
   Откроется окно PDQL-запроса.
4. Измените условие фильтра на языке запроса PDQL.
5. Нажмите кнопку **Сохранить**.
   Откроется окно **Новый фильтр**.
6. В поле **Название** введите название пользовательского фильтра.
7. Если требуется, в раскрывающемся списке **Папка** выберите папку, в которую требуется поместить этот фильтр.
8. Нажмите кнопку **Сохранить**.

Пользовательский фильтр инцидентов на основе существующего фильтра создан.

9.2.5.6 Создание копии пользовательского фильтра инцидентов

Вы можете создать копию пользовательского фильтра инцидентов, чтобы использовать ее как основу для создания нового пользовательского фильтра (см. раздел 9.2.5.4).

❖ Чтобы создать копию пользовательского фильтра:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** наведите курсор на пользовательский фильтр, нажмите ⋮ и в раскрывшемся меню выберите пункт **Сделать копию**.

Копия фильтра создана в той же папке, в которой расположен исходный фильтр. К названию исходного пользовательского фильтра прибавляется слово «_Копия».

9.2.5.7 Изменение условия пользовательского фильтра инцидентов

Вы можете изменить сохраненный пользовательский фильтр: например, в условии фильтрации на языке PDQL изменить порядок сортировки отфильтрованных инцидентов в таблице.

❖ Чтобы изменить пользовательский фильтр:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** выберите пользовательский фильтр.
   Условие фильтра будет добавлено в PDQL-запрос над таблицей инцидентов.
3. Нажмите на условие фильтра.
   Откроется окно PDQL-запроса.
4. Измените условие фильтра на языке запроса PDQL.
5. Нажмите кнопку **Сохранить**.
   Откроется окно **Редактирование фильтра**.
6. Нажмите кнопку **Сохранить**.

Условие пользовательского фильтра изменено.

9.2.5.8 Удаление пользовательского фильтра инцидентов

❖ Чтобы удалить пользовательский фильтр:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели **Фильтры** наведите курсор на пользовательский фильтр, нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Пользовательский фильтр удален.

9.2.6 Сортировка инцидентов

По умолчанию все инциденты в таблице инцидентов отсортированы:

1. По времени создания: от новых к старым.
2. По статусу: **Новые**, **Утвержденные**, **В работе**, **Разрешенные**, **Закрытые**.
3. По уровню опасности: **Высокая**, **Средняя**, **Низкая**.

В таблице инцидентов порядок сортировки колонок по умолчанию обозначен цифрами 1−3, располагающимися рядом со значками ▼ и ▲.

Вы можете менять порядок сортировки двумя способами: в таблице инцидентов или с помощью PDQL-запроса.

Сортировка инцидентов в таблице инцидентов

❖ Чтобы отсортировать инциденты:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. Нажмите на заголовок колонки, по содержанию которой вы хотите отсортировать инциденты.

> **Примечание.** Вы можете сортировать инциденты по одной из следующих колонок: **Создан**; **Статус**; **Опасность**; **ID**; **Инцидент**; **Категория**; **Тип**; **Ответственный**.

   Справа от названия этой колонки появится значок ▲.
   Значения в этой колонке будут упорядочены по возрастанию (А−Я, A−Z, 0−9).
3. Чтобы упорядочить значения в этой же колонке по убыванию (Я−А, Z−A, 9−0), еще раз нажмите на ее заголовок.
   Справа от названия колонки появится значок ▼.
   Значения в этой колонке будут упорядочены по убыванию (Я−А, Z−A, 9−0).

Инциденты отсортированы.

❖ Чтобы сбросить сортировку по колонке, выполните одно из следующих действий:

- нажмите на заголовок этой колонки один раз, если в заголовке отображается значок ▼, или два раза, если ▲;
- настройте сортировку инцидентов по любой другой колонке.

Значок ▼ или ▲ справа от названия колонки пропадет. Сортировка по колонке сброшена.

Сортировка инцидентов с помощью PDQL-запроса

❖ Чтобы отсортировать инциденты в таблице инцидентов с помощью PDQL-запроса:

1. Нажмите на строку PDQL-запроса под временным фильтром.
   Откроется окно PDQL-запроса.

> **Примечание.** Порядок колонок в поле **ORDER BY** определяет порядок сортировки. По умолчанию отображаются следующие колонки для сортировки: **Создан**, **Статус**, **Опасность**.

2. В поле **ORDER BY** нажмите один раз на нужное вам название колонки, чтобы изменить направление сортировки.
3. Если требуется, установите курсор после названия предустановленной колонки и в раскрывающемся списке выберите название колонки, которое вы хотите добавить для сортировки.
4. Нажмите кнопку **Применить**.

Инциденты отсортированы.

Примечание. Если вы удалите все названия колонок в поле **ORDER BY** и нажмете кнопку **Применить**, то инциденты в таблице инцидентов будут отсортированы по умолчанию.

9.2.7 Сброс всех условий фильтрации

Вы можете вернуть для таблицы инцидентов значения фильтров по умолчанию, сбросив все условия фильтрации.

❖ Чтобы сбросить все условия фильтрации:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели инструментов нажмите кнопку **Сбросить фильтр**.

Текущие условия фильтрации сброшены. К таблице инцидентов применен фильтр по умолчанию: все незакрытые инциденты за последние 7 дней.

9.3 Анализ инцидента

На этапе анализа ваша цель − расширить контекст инцидента и принять решение, нужно ли дальнейшее расследование. Вам необходимо:

1. Открыть карточку инцидента и просмотреть описание инцидента, его статус и параметры.
2. В карточке инцидента проанализировать список привязанных к инциденту событий и активов.
3. В карточке инцидента просмотреть на топологии вовлеченные в инцидент активы.
4. Принять решение, нужно ли дальнейшее расследование или инцидент был разрешен без вашего участия:
   - если инцидент был разрешен без вашего участия, вы закрываете инцидент (см. раздел 9.4.4);
   - если полученной в результате анализа информации недостаточно, вы берете инцидент в работу и переходите на этап расследования инцидента (см. раздел 9.4).

9.3.1 Просмотр карточки инцидента

В процессе работы с инцидентом ваше основное рабочее пространство – карточка инцидента. В карточке инцидента отображается информация о произошедшем событии информационной безопасности: название и описание инцидента, параметры и статус инцидента, связанные с инцидентом задачи, события, активы, а также комментарии об инциденте.

В карточке инцидента вы можете:

- просматривать информацию об инциденте;
- менять статусы инцидента;
- ставить задачи другим пользователям;
- описывать принятые по инциденту меры.

❖ Чтобы просмотреть карточку инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. По ссылке с названием инцидента перейдите в карточку инцидента.

Карточка инцидента состоит из панели инструментов и рабочей области страницы. Рабочая область страницы состоит из двух панелей – верхней и нижней.

Верхняя панель содержит подробную информацию об инциденте, его статусе и параметрах. Нижняя панель содержит набор вкладок. На вкладках вы можете просматривать и изменять информацию о связанных с инцидентом задачах, событиях, активах, а также оставлять комментарии об инциденте.

9.3.2 Просмотр списка событий, привязанных к инциденту

❖ Чтобы просмотреть список привязанных к инциденту событий:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. По ссылке с названием инцидента перейдите в карточку инцидента.
3. Выберите вкладку **События**.
   На вкладке отобразятся 5 последних событий, привязанных к инциденту.
4. Если требуется отобразить на вкладке все события, привязанные к инциденту, нажмите кнопку **Показать все <количество> событий**.
   Отобразится полный список событий.
5. Если требуется, отвяжите событие от инцидента, нажав .
6. Если требуется, нажмите кнопку **Открыть «События»**.
   Откроется страница **События**. В таблице событий отобразится полный список событий, привязанных к инциденту.

Вы просмотрели события, привязанные к инциденту.

9.3.3 Просмотр на топологии активов, вовлеченных в инцидент

❖ Чтобы просмотреть на топологии вовлеченные в инцидент активы:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. По ссылке с названием инцидента перейдите в карточку инцидента.
3. В панели инструментов в раскрывающемся списке **Показать на топологии** выберите один из вариантов: **Активы и сети**, **Атакующие активы**, **Все связанные активы**.

Открылась страница **Активы**. В таблице активов отображается подробная информация о выбранном виде активов. На вкладке **Топология** отображается карта активов.

9.4 Расследование инцидента

После того как вы проанализировали инцидент и подтвердили, что это не ложное срабатывание, вы должны начать расследование инцидента.

В процессе расследования инцидента вам необходимо:

1. Определить источник угрозы.
2. Выявить обстоятельства, которые привели к возникновению инцидента.
3. Собрать доказательства инцидента.
4. Выработать рекомендации, что и кому нужно сделать, чтобы устранить последствия инцидента.

Чем быстрее вы расследуете инцидент, тем меньше будет риск нанесения значительного ущерба IT-инфраструктуре сети. Чтобы ускорить расследование, вы можете привлекать к расследованию сотрудников, зарегистрированных в ПК Ankey SIEM NG.

Когда расследование инцидента завершено, опишите принятые меры по инциденту в карточке инцидента и укажите, почему вы считаете, что дальнейшие работы не требуются.

9.4.1 Создание задачи по инциденту

Вы можете привлекать к расследованию других пользователей, чтобы ускорить расследование инцидента. Для этого вам нужно создать по инциденту одну или несколько задач и назначить ответственных за выполнение этих задач.

❖ Чтобы создать задачу по инциденту:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. По ссылке с названием инцидента перейдите в карточку инцидента.
3. В нижней панели на вкладке **Задачи** нажмите кнопку **Поставить задачу**.
   Откроется страница **Создание задачи**.
4. В раскрывающемся списке **Тип** выберите тип задачи:
   - **Расследование** – выявление причин инцидента и способов предотвратить его повторное возникновение;
   - **Сбор доказательств** − выявление объектов атаки, сбор и хранение доказательств атаки;
   - **Восстановление** − восстановление работоспособности IT-инфраструктуры сети.
5. В поле **Дедлайн** укажите дату, к которой задача должна быть выполнена.
6. В раскрывающемся списке **Ответственный** укажите ответственного за выполнение задачи.

Примечание. Ответственным вы можете указать только пользователя, чья учетная запись заведена в ПК Ankey SIEM NG.

7. Если требуется, в поле **Описание** введите подробное описание задачи, указав все необходимые для ее обработки детали.
8. Нажмите кнопку **Сохранить**.

Задача создана.

ПК Ankey SIEM NG отправил пользователю, ответственному за выполнение задачи, уведомление на электронную почту.

Все задачи, относящиеся к инциденту, отображаются в карточке инцидента.

9.4.2 Изменение статуса инцидента

Статус инцидента отображает информацию о том, на каком этапе в текущий момент находится расследование инцидента.

При переходе от одного этапа расследования инцидента к другому (например, от **В работе** к **Разрешен**) вам нужно в карточке инцидента изменять статус инцидента.

❖ Чтобы изменить статус инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В таблице инцидентов нажмите название инцидента.
   Откроется карточка инцидента.
3. В панели инструментов нажмите кнопку **Изменить статус**.
   Откроется окно **Сменить статус инцидента <Название инцидента>**.
4. В раскрывающемся списке **<Текущий статус инцидента>** выберите новый статус инцидента.

   Примечание. Доступный для выбора статус зависит от текущего этапа расследования инцидента (см. раздел 9.4).

5. Если требуется, в поле **Принятые меры** укажите, что было сделано в ходе анализа или в ходе расследования инцидента.
6. Если требуется, в поле **Комментарий** укажите причину смены статуса инцидента или другую информацию, касающуюся обработки инцидента.
7. Нажмите кнопку **Сменить статус**.

Статус инцидента изменен. Новый статус инцидента отображается в таблице инцидентов и в карточке инцидента.

Учетная запись автора изменений сохранена в карточке инцидента.

Вы можете сортировать инциденты по присвоенным им статусам или формировать на основе статусов инцидентов статистику по инцидентам.

9.4.3 Привязка событий к инциденту

Вы можете управлять событиями на странице **События**. По умолчанию на ней отображаются все события, связанные с группами активов, к которым вам предоставлен доступ.

В результате расследования инцидента вы можете выявить связь инцидента с одним или несколькими событиями. Такие события вам нужно привязать к инциденту.

❖ Чтобы привязать одно или несколько событий к инциденту:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. Найдите нужный вам инцидент и скопируйте из колонки ID его идентификатор.
3. В главном меню выберите раздел **События**.
   Откроется страница **События**.
4. Укажите одно или несколько событий в списке событий и нажмите кнопку **Связать с инцидентом**.

   Примечание. Чтобы выбрать несколько событий одновременно, удерживайте клавишу Ctrl.

   Откроется окно **Идентификатор инцидента**.
5. Введите в окне **Идентификатор инцидента** скопированный идентификатор инцидента и нажмите кнопку **Связать**.

Одно или несколько событий привязаны к инциденту.

9.4.4 Закрытие инцидента

После того, как вы завершили расследование инцидента и убедились, что последствия инцидента устранены и рекомендованные вами меры по устранению инцидента приняты, вам нужно закрыть инцидент. При этом очень важно, чтобы вы сохранили информацию о принятых мерах по инциденту в карточке инцидента. В дальнейшем эта информация позволит предотвратить появление подобных инцидентов или ускорить реагирование на подобные инциденты.

❖ Чтобы закрыть инцидент:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. Выберите инцидент в таблице.
3. По ссылке с названием инцидента перейдите в карточку инцидента.
4. В панели инструментов нажмите кнопку **Изменить статус**.
   Откроется окно **Сменить статус инцидента <Номер инцидента>**.
5. В раскрывающемся списке смены статуса выберите **Закрытый**.
6. В поле **Принятые меры** перечислите, какие действия были выполнены во время обработки инцидента.
7. Если требуется, в поле **Комментарий** укажите причину смены статуса инцидента или другую информацию, касающуюся обработки инцидента.
8. Нажмите кнопку **Сменить статус**.

Инцидент закрыт.

9.5 Просмотр статистики по инцидентам

Для оценки эффективности работы по инцидентам вам необходимы измеряемые ключевые показатели. Эти ключевые показатели помогают вам

оценить, успеваете ли вы обрабатывать инциденты, быстро ли вы обрабатываете инциденты, растет или снижается количество незакрытых опасных инцидентов.

ПК Ankey SIEM NG сохраняет ключевые показатели работы по инцидентам и отображает статистику по ним в виде диаграмм на странице **Статистика** в разделе **Инциденты**.

К ключевым показателям относятся:

- динамика количества новых инцидентов (диаграмма **Созданные инциденты**);
- скорость обработки инцидентов за период времени (диаграмма **Закрытые инциденты за период**);
- количество незакрытых инцидентов разной степени опасности (диаграмма **Незакрытые инциденты по уровню опасности**);
- среднее время устранения инцидента (панель **Среднее время устранения инцидента**).

❖ Чтобы просмотреть диаграммы с ключевыми показателями:

1. В главном меню в разделе **Инциденты** выберите пункт **Статистика**.
   Откроется страница **Статистика**.
2. Выберите интересующий вас ключевой показатель работы по инцидентам и на соответствующей диаграмме нажмите .
   Над диаграммой отобразятся фильтры инцидентов по группам и по временному периоду.
3. В раскрывающемся списке **По группам** выберите интересующие вас группы инцидентов.
4. Если требуется, в раскрывающемся списке временного фильтра выберите нужное значение периода.

На диаграмме отобразилась динамика количества инцидентов определенного типа в выбранном периоде.

Если вы заметили необычную динамику по какому-либо ключевому показателю за выбранный период (например, значительный рост или падение количества инцидентов, скачкообразные изменения количества инцидентов), вы можете увеличить соответствующую диаграмму для удобства просмотра данных.

❖ Чтобы увеличить интересующую вас диаграмму:

1. На диаграмме нажмите кнопку **Увеличить**.
   В новом окне откроется увеличенная диаграмма.
2. Если требуется, измените значения фильтров, нажав в левом верхнем углу диаграммы кнопку .
3. На временной шкале диаграммы курсором мыши выделите период, который нужно просмотреть более детально. Масштаб диаграммы увеличится.
4. Нажмите кнопку **Сбросить масштаб**, чтобы вернуться к исходному масштабу диаграммы.
   Масштаб диаграммы вернется к исходному.
5. Нажмите кнопку **Закрыть** на увеличенной диаграмме, чтобы вернуться к странице **Статистика**.

Открылась страница **Статистика**.

Для оценки эффективности процесса управления инцидентами вы

можете посмотреть, сколько в среднем времени тратится на устранение инцидента.

❖ Чтобы посмотреть среднее время устранения инцидента за период:

1. В главном меню в разделе **Инциденты** выберите пункт **Статистика**.
2. Выберите панель **Среднее время устранения инцидента**.
3. Нажмите .
4. В раскрывающемся списке временного фильтра выберите нужное вам значение периода.

Отобразилось среднее время устранения инцидента за заданный период.

9.6 Экспорт и импорт инцидентов

ПК Ankey SIEM NG предоставляет вам возможность обмениваться информацией об инцидентах. Обмен информацией об инцидентах может происходить внутри территориально распределенных систем (например, ПК Ankey SIEM NG головной организации и ПК Ankey SIEM NG, относящийся к IT-инфраструктуре сети филиалов организации) или между ПК Ankey SIEM NG и другими системами управления событиями IT-безопасности. Такой обмен позволяет консолидировать данные по инцидентам и извлекать аналитическую информацию.

Например, оператор ПК Ankey SIEM NG в филиале может экспортировать инциденты и отправлять в головное подразделение, чтобы получить консультацию более опытных специалистов, как расследовать сложные инциденты. Операторы ПК Ankey SIEM NG в головном подразделении могут импортировать инциденты из филиалов, чтобы сформировать общее представление об инцидентах в организации.

9.6.1 Экспорт инцидентов

Вы можете экспортировать инциденты из ПК Ankey SIEM NG в унифицированном формате обмена JSON для последующего импорта этих инцидентов в другие системы.

Примечание. В один файл можно экспортировать не более 10 000 инцидентов. Если вы выбрали более 10 000 инцидентов, то будут экспортированы первые 10 000 инцидентов.

❖ Чтобы экспортировать инциденты:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. Если требуется, в таблице инцидентов выберите отдельные инциденты, удерживая нажатой клавишу Ctrl.

   Примечание. Вы также можете отфильтровать инциденты.

3. В панели инструментов нажмите кнопку **Экспорт**.
   Откроется окно **Экспорт инцидентов**.
4. Выберите один из вариантов − все инциденты за указанный период или выбранные вами инциденты.

5. Нажмите кнопку **Экспортировать**.

Система сформирует JSON-файл и выгрузит его в локальную папку, указанную в свойствах браузера.

Примечание. ПК Ankey SIEM NG формирует имя файла с инцидентами в зависимости от системного языка по одному из двух шаблонов: Инциденты_YYYY-MM-DD hh-mmssZ.json или Incidents_YYYY-MM-DD hh-mm-ssZ.json, где YYYY – год, MM – месяц, DD – день, hh – часы, mm – минуты, ss – секунды, Z – зона UTC. Время формирования отчета hh_mm_ssZ указано в нулевом часовом поясе (GMT+0).

Инциденты экспортированы и сохранены в файл формата JSON.

9.6.2 Импорт инцидентов

Вы можете импортировать в ПК Ankey SIEM NG инциденты в унифицированном формате обмена − JSON.

❖ Чтобы импортировать инциденты:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели инструментов нажмите кнопку **Импорт**.
   Откроется окно **Импорт инцидентов**.
3. В раскрывающемся списке **Расположение** выберите группы активов, где необходимо расположить инциденты.
4. Если требуется, установите флажок **перезаписать существующие инциденты**.

   Примечание. Если флажок снят, инциденты с совпадающим идентификатором (параметром identification.source.id), экспортированные из разных систем, будут пропущены в процессе импорта.

5. Загрузите файл с инцидентами одним из двух способов:
   – перетащите файл в поле;
   – нажмите **выбрать** и добавьте файл.

   Примечание. Если у импортируемого файла инцидентов идентификатор формата отличается от JSON или формат данных этого файла некорректный, то ПК Ankey SIEM NG отобразит в окне импорта инцидентов ошибку валидации и выделит невалидный файл красным цветом. Кнопка Импортировать будет недоступна до тех пор, пока вы не удалите невалидные файлы. Максимальный объем одного импортируемого файла − 512 МБ.

6. Нажмите кнопку **Импортировать**.
   Начнется импорт инцидентов. По завершении импорта в окне **Импорт инцидентов** отобразится информация о результатах импорта инцидентов.

Примечание. Окно **Импорт инцидентов** содержит записи о каждом импортированном файле, включая результат импорта и количество импортированных инцидентов. В случае возникновения ошибки при импорте инцидентов такие инциденты пропускаются. В колонке **Импортировано инцидентов** отображается количество успешно импортированных инцидентов и общее количество инцидентов в файле. В нижней части окна отображается общий итог импорта: количество импортированных файлов, количество импортированных и пропущенных инцидентов.

7. Нажмите кнопку **Закрыть**.
   Инциденты импортированы в ПК Ankey SIEM NG. Импортированные инциденты отображаются на странице **Инциденты** в таблице инцидентов по фильтру **Импортированные из файла**.

Общая папка фильтров для всех импортируемых инцидентов − **Инциденты по источнику импорта**. Для импортированных инцидентов в поле **Источник** появится значок .

9.7 Удаление инцидентов

При развертывании и запуске ПК Ankey SIEM NG могут быть автоматически созданы ложные инциденты. Также при анализе и расследовании инцидентов вы можете обнаружить, что инциденты дублируются или были заведены в системе ошибочно, например, в результате некорректно сработавшего правила корреляции. Такие инциденты вы можете удалять − по одному или группой.

❖ Чтобы удалить инцидент или группу инцидентов:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В таблице инцидентов выберите один или несколько инцидентов.

Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.

   Также вы можете применить к таблице инцидентов фильтр, чтобы быстро выбрать и удалить группу инцидентов.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Примечание. Также вы можете удалить инцидент из его карточки по кнопке **Удалить**.

Инцидент или группа инцидентов удалены.

Удалены все связанные с инцидентом или группой инцидентов дочерние задачи.

Удалены все связи инцидента или группы инцидентов с другими

сущностями (сами сущности при этом не удаляются).

Удаленный инцидент или группа инцидентов исключены из статистики и больше не отображаются на дашбордах.

10 Оперативная настройка анализа данных

По результатам расследования инцидентов оператор может внести изменения в табличные списки, запустить, остановить правила корреляции или обогащения.

10.1 Работа с табличными списками

Табличный список − двумерный массив данных, хранящийся в памяти ПК Ankey SIEM NG и доступный для использования в правилах корреляции и правилах обогащения.

Рекомендации по заполнению табличных списков представлены в Приложении Д.

Ключевая колонка − это колонка, значения в которой являются идентификаторами записей табличного списка. Если ключевых колонок несколько, то запись идентифицируется по совокупности значений всех ключевых колонок.

Работать с табличными списками вы можете на странице **Табличные списки**. В зависимости от назначения существуют следующие типы табличных списков:

- данные об активах − предназначены для хранения информацией об активах, используемой в правилах обогащения и корреляции. Заполняются данными из модели активов и автоматически обновляются при изменении состояния активов;
- заполняются правилами корреляции − предназначены для хранения данных, используемых в правилах обогащения и корреляции. Заполняются автоматически при выполнении правил корреляции. Вы можете вручную добавить или изменить записи в табличных списках, выполнить импорт данных из файла формата CSV или очистить табличный список;
- заполняются правилами обогащения − предназначены для хранения данных, используемых в правилах обогащения и корреляции. Заполняются автоматически при выполнении правил обогащения. Вы можете вручную добавить или изменить записи в табличных списках, выполнить импорт данных из файла формата CSV или очистить табличный список;
- справочник − предназначены для хранения справочной информации, используемой в правилах обогащения и корреляции. Через веб-интерфейс Ankey SIEM NG Knowledge Base вы можете вручную добавить или изменить записи в табличных списках, выполнить импорт данных из файла формата CSV или очистить табличный список.

Вы можете выполнить экспорт данных из любого табличного списка в файл формата CSV.

10.1.1 Поиск записей с помощью PDQL-запроса

Вы можете использовать запросы на языке PDQL, чтобы искать записи в табличных списках. Запросы можно создавать с помощью данных из ячеек табличных списков и вручную.

❖ Чтобы найти записи в табличном списке с помощью данных из ячеек:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список.
4. Выберите вкладку **Записи**.
   Откроется табличный список.
5. В табличном списке по ссылке с подчеркиванием выберите значение в ячейке (например, тип шифрования).
6. Во всплывающем окне выберите условие поиска.
   Условие поиска будет добавлено в PDQL-запрос над табличным списком.

В табличном списке отображаются записи, соответствующие условию PDQL-запроса.

❖ Чтобы вручную изменить существующее условие поиска записей в табличном списке:

1. Над табличным списком нажмите **<Условие PDQL-запроса>**.
   Откроется всплывающее окно с PDQL-запросом. В поле **SELECT** указаны колонки табличного списка.
2. Если требуется, в раскрывающемся списке **ORDER BY** выберите колонку, по которой будет отсортирован результат выполнения запроса, и по ссылке с подчеркиванием выберите направление сортировки.
3. По умолчанию записи в табличном списке отсортированы по времени последнего изменения от новых к старым.
4. Нажмите кнопку **Применить**.

Условие поиска записей в табличном списке изменено. Записи табличного списка найдены и отсортированы в соответствии с условиями PDQL-запроса.

10.1.2 Экспорт данных в файл формата CSV

❖ Чтобы выполнить экспорт данных из табличного списка:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список.
4. Выберите вкладку **Записи**.
5. Если нужно экспортировать отдельные записи табличного списка, выберите строки с этими записями.

Примечание. Для выбора нескольких строк подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных строк − клавишу Ctrl.

6. В панели **<Название табличного списка>** нажмите кнопку **Экспорт**.
7. В открывшемся окне выберите один из вариантов:
   - **Все <Количество строк табличного списка> записей** − для экспорта всего табличного списка;
   - **Первые <Количество>** − для экспорта указанного количества строк;
   - **Выбранные <Количество выбранных строк табличного списка>** − для экспорта выделенных в рабочей области строк.
8. Нажмите кнопку **Экспортировать** и укажите папку для сохранения файла.

Данные экспортированы и сохранены в файл формата CSV. Имя файла содержит имя табличного списка и дату импорта. В первой строке файла указаны имена колонок табличного списка, в качестве разделителя используется точка с запятой (;). Строки отсортированы по ключевым колонкам.

10.1.3 Импорт данных из файла формата CSV

Поддерживается импорт данных из файлов формата CSV в кодировке UTF-8. В первой строке файла нужно указать наименования колонок, в качестве разделителя данных в строке нужно использовать точку с запятой (;).

Файл для импорта должен содержать значения для ключевых колонок табличного списка. Значения ячеек должны удовлетворять требованиям: для типа данных DateTime − дата должна находиться в интервале от 1970-01-01 00:00:00 до 2106-02-07 06:28:15; для Number − число должно находиться в интервале от −9223372036854775807 до 9223372036854775807; для String − длина строки не должна превышать 16 382 символов (65 531 байт).

❖ Чтобы выполнить импорт данных в табличный список для правил корреляции или обогащения:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
4. Выберите вкладку **Записи**.
5. Нажмите кнопку **Импорт**.
6. В открывшемся окне по ссылке **выбрать** укажите расположение файла с данными для импорта.

Примечание. Для выбора файла с данными вы можете перетащить его в окно **Импорт табличного списка** в область **Загрузить файл CSV**.

7. Нажмите кнопку **Импортировать**.

8. При появлении сообщения об окончании процедуры импорта нажмите кнопку **Закрыть**.

Данные импортированы. Строки с уникальным значением ключевых колонок добавлены в конец табличного списка. Строки с существующими в табличном списке значениями ключевых колонок перезаписаны.

10.1.4 Добавление записи в табличный список

❖ Чтобы добавить запись в табличный список для правил обогащения или корреляции:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
4. Выберите вкладку **Записи**.
5. Нажмите кнопку **Редактировать содержимое**.
6. В открывшемся окне выберите вариант **Приостановить все связанные правила** и нажмите кнопку **Далее**.
7. В панели инструментов вкладки нажмите кнопку **Добавить**.
8. В добавленной строке заполните ячейки в соответствии с типом данных колонок табличного списка и нажмите ✓.
9. В нижней части вкладки нажмите кнопку **Закончить редактирование**.

Запись добавлена в табличный список.

10.1.5 Удаление записей из табличного списка

❖ Чтобы удалить записи из табличного списка для правил корреляции или обогащения:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
4. Выберите вкладку **Записи**.
5. Нажмите кнопку **Редактировать содержимое**.
6. В открывшемся окне выберите вариант **Приостановить все связанные правила** и нажмите кнопку **Далее**.
7. Выберите одну или несколько записей.

> **Примечание.** Для выбора нескольких строк подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных строк − клавишу Ctrl.

8. Нажмите кнопку **Удалить** и подтвердите удаление.
9. В нижней части вкладки нажмите кнопку **Закончить редактирование**.

Записи удалены из табличного списка.

10.1.6 Очистка табличного списка

❖ Чтобы удалить все записи из табличного списка для правил обогащения или корреляции:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
4. Выберите вкладку **Записи**.
5. Нажмите кнопку **Очистить табличный список** и подтвердите очистку.

Все записи удалены из табличного списка.

10.2 Включение и отключение правил корреляции и обогащения событий

Корреляция событий − это процесс обнаружения событий информационной безопасности путем анализа потока нормализованных событий. При обнаружении в потоке событий такой их последовательности, которая указана в условии одного из заранее настроенных правил корреляции, регистрируется корреляционное событие.

Обогащение событий − заполнение полей нормализованных, агрегированных и корреляционных событий согласно правилам обогащения. Поля заполняются данными, указанными в правиле обогащения или полученными из табличных списков.

На странице **Правила корреляции** вы можете включать и отключать правила корреляции событий, на странице **Правила обогащения** − правила обогащения событий.

10.2.1 Отключение правила корреляции

Вы можете отключать правила корреляции со статусами «Включено» и «Приостановлено».

❖ Чтобы отключить правило корреляции:

1. В главном меню в разделе **Сбор данных** выберите пункт **Правила корреляции**.
   Откроется страница **Правила корреляции**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Список правил корреляции** выберите одно или несколько правил.

> **Примечание.** Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил − клавишу Ctrl.

4. В панели инструментов нажмите кнопку **Отключить**.

Правило корреляции отключено, конвейер не будет использовать его для корреляции событий.

10.2.2 Включение правила корреляции

Вы можете включать правила корреляции со статусом «Отключено» и «Приостановлено».

❖ Чтобы включить правило корреляции:

1. В главном меню в разделе **Сбор данных** выберите пункт **Правила корреляции**.
   Откроется страница **Правила корреляции**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Список правил корреляции** выберите одно или несколько правил.

> **Примечание.** Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил − клавишу Ctrl.

4. В панели инструментов нажмите кнопку **Включить**.

Правило корреляции включено, конвейер начнет использовать его для корреляции событий.

10.2.3 Отключение правила обогащения

Вы можете отключать правила обогащения со статусом «Включено».

❖ Чтобы отключить правило обогащения:

1. В главном меню в разделе **Сбор данных** выберите пункт **Правила обогащения**.
   Откроется страница **Правила обогащения**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Список правил обогащения** выберите одно или несколько правил.

> **Примечание.** Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил − клавишу Ctrl.

4. В панели инструментов нажмите кнопку **Отключить**.

Правило обогащения отключено, конвейер не будет использовать его для обогащения событий.

10.2.4 Включение правила обогащения

Вы можете включать правила обогащения со статусом «Отключено».

❖ Чтобы включить правило обогащения:

1. В главном меню в разделе **Сбор данных** выберите пункт **Правила обогащения**.
   Откроется страница **Правила обогащения**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

3. В панели **Список правил обогащения** выберите одно или несколько правил.

> **Примечание.** Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил − клавишу Ctrl.

4. В панели инструментов нажмите кнопку **Включить**.

Правило обогащения включено, конвейер начнет использовать его для обогащения событий.

10.3 Поиск индикаторов компрометации в событиях

В ПК Ankey SIEM NG предусмотрена возможность проверки полученных ранее событий на наличие в них индикаторов компрометации по данным табличных списков.

Индикатор компрометации − это признак подозрительной активности или вредоносного объекта в IT-инфраструктуре организации; такие признаки могут указывать на развитие злоумышленниками атаки. Индикаторами компрометации могут выступать, например, IP-адрес или доменное имя узла, на котором зарегистрирована подозрительная активность, хеш-сумма вредоносного файла.

Для поиска индикаторов компрометации в событиях нужно создать задачу на проверку событий с одним из профилей модуля batcheventsearch.

10.3.1 Создание задачи на проверку событий

❖ Чтобы создать задачу на проверку событий для поиска индикаторов компрометации:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Проверка событий на IOC**. Откроется страница **Создание задачи на проверку событий**.
3. В поле **Название** введите название задачи.
4. Если нужно настроить профиль, нажмите  , в открывшемся окне измените параметры профиля и нажмите кнопку **Сохранить**.
5. В раскрывающемся списке **Агент** выберите агент для работы задачи.
6. Если нужно настроить периодический запуск задачи, в блоке параметров **Расписание** включите и настройте расписание.
7. Нажмите кнопку **Сохранить**.

Задача создана.

10.3.2 Параметры модуля batcheventsearch

Модуль предназначен для проверки полученных ранее событий на наличие в них индикаторов компрометации, указанных в одном из табличных списков. При выполнении проверки модуль отбирает новые события (и события, полученные за указанный период), соответствующие указанному PDQL-запросу. Для каждого отобранного события модуль проверяет условие соответствия данных в полях события данным указанного табличного списка и при выполнении

условия регистрирует одно или несколько корреляционных событий.

Параметры модуля сохраняются в профилях. Вы можете изменять параметры профиля при создании пользовательского профиля или задачи на проверку событий. Для настройки профиля в окне **Параметры профиля** доступны следующие элементы:

- **Конвейер обработки событий** − раскрывающийся список для выбора конвейера, события которого необходимо проверить;
- **Фильтр событий** − поле ввода PDQL-запроса;

> **Примечание.** По ссылке **Вставить условие из сохраненного запроса** вы можете выбрать запрос, сохраненный ранее на странице **События**.

- **Глубина проверки** − по ссылке открывается окно для настройки периода, за который были получены проверяемые события;

> **Примечание.** Проверяются все новые события, полученные с момента предыдущей проверки, и повторно проверяются события, полученные за указанный период до момента предыдущей проверки. Если проверка ранее не производилась, проверяются события за указанный период.

- **Табличный список** − раскрывающийся список для выбора табличного списка;
- **Использовать только часть табличного списка** − при установке флажка открывается поле ввода PDQL-запроса для фильтрации записей табличного списка;
- **Поля события** − поле для ввода полей события, для которых проверяется условие соответствия;
- **Колонки табличного списка** − поле для ввода названий колонок табличного списка, для которых проверяется условие соответствия;
- **Условие соответствия** − раскрывающийся список для выбора условия регистрации корреляционного события, содержит значения:
  - **По умолчанию (совпадение значений)** − условие выполняется при совпадении значения любого поля, указанного в **Поля события**, со значением в любой из колонок, указанных в **Колонки табличного списка** (для каждого совпадения регистрируется отдельное корреляционное событие);
  - **Задать для всех строк** − при выборе значения открывается поле для ввода выражения (из таблицы

ниже)[1], указывающего на вариант совпадения значения поля события с маской. Условие выполняется, если в соответствии с выбранным вариантом совпадают значения любого поля, указанного в **Поля события** с значением маски в любой из колонок, указанных в **Колонки табличного списка**;

- **<Название колонки>** − при выборе значения из колонки табличного списка считывается выражение (из таблицы ниже)[1], указывающее на вариант совпадения значения поля события с маской. Условие выполняется, если в соответствии со считанным вариантом совпадают значения любого поля, указанного в **Поля события**, с значением маски в любой из колонок, указанных в **Колонки табличного списка**;

- **Время** − позволяет выбрать время регистрации корреляционного события;
- Раскрывающиеся списки для полей корреляционного события позволяют выбрать данные для заполнения полей. Значение поля можно ввести вручную, заполнить данными из поля исходного события или из указанной колонки табличного списка;
- **Добавить параметр** − по кнопке вы можете добавить дополнительные поля корреляционного события.

Таблица 10.1 − Выражения для вариантов совпадения с маской

Вариант совпадения с маской	Выражение для	
	URL	FQDN
Домен, все его поддомены и их содержимое	u:hAS	h:dAS
Адрес с папками	u:hAS,dAS	−
Сценарий с конкретными параметрами	u:hAS,pEX	−
Адрес с параметрами	u:hAS,pSW	−
Адрес с последовательностью символов	u:hAS,pTM	−
Домен третьего уровня	u:hEX	h:dEX
Домен с папкой или файлом, но без вложенных папок	u:hEX,dEX	−

10.4 Ретроспективная корреляция событий

В ПК Ankey SIEM NG предусмотрена возможность повторной проверки полученных ранее событий по выбранным правилам корреляции. Вы можете указать способ наполнения табличных списков, используемых правилами при

[1] Для составления условия, кроме указанных в таблице выражений, вы можете использовать регулярные выражения, поддерживаемые службой Elasticsearch. Регулярные выражения нужно вводить с префиксом "re:".

проверке. Записи табличных списков могут быть получены из файла формата CSV, из Ankey SIEM NG Knowledge Base или из ПК Ankey SIEM NG. По результатам проверки регистрируются события ИБ, которые могут быть сохранены в файл или в ПК Ankey SIEM NG. На основании событий ИБ в ПК Ankey SIEM NG могут быть зарегистрированы инциденты.

Ретроспективную корреляцию событий можно использовать в следующих случаях:

- для проверки событий после добавления в Ankey SIEM NG Knowledge Base новых правил корреляции (при установке нового пакета экспертизы или при создании пользовательского правила);
- для проверки событий после обновления данных табличных списков;
- для поиска угроз в режиме threat hunting;
- для проверки событий по правилам, работа которых была автоматически приостановлена.

Для ретроспективной корреляции событий нужно создать задачу с одним из профилей модуля retrocorrelator (входит в состав компонента Ankey SIEM NG RC). Для модуля создан стандартный профиль Retrospective Correlation, на базе которого вы можете создавать пользовательские профили (см. раздел 7.4).

10.4.1 Создание задачи для ретроспективной корреляции

Перед созданием задачи ретроспективной корреляции нужно через веб-интерфейс Ankey SIEM NG Knowledge Base создать набор для установки (см. раздел 16.6) и добавить в него правила, по которым нужно проверить события.

❖ Чтобы создать задачу для ретроспективной корреляции событий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**. Откроется страница **Задачи по сбору данных**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Ретроспективная корреляция событий**.
   Откроется страница **Создание задачи на ретроспективную корреляцию событий**.
3. В поле **Название** введите название задачи.
4. Если нужно настроить профиль, нажмите ⚙, в открывшемся окне измените параметры профиля и нажмите кнопку **Сохранить**.
5. В раскрывающемся списке **Агент** выберите агент с модулем retrocorrelator.

> **Примечание.** Один агент с модулем retrocorrelator может одновременно выполнять только одну задачу ретроспективной корреляции событий.

6. Нажмите кнопку **Сохранить**.

Задача создана.

После запуска и выполнения задачи вы можете скачать архив с результатами проверки на странице **История запусков <Название задачи>** по кнопке **Скачать журнал и результаты**; также по кнопке **Найти события** вы

можете открыть страницу с событиями, зарегистрированными при выполнении задачи.

10.4.2 Параметры модуля retrocorrelator

Модуль предназначен для повторной проверки полученных ранее событий по выбранным правилам корреляции.

Параметры модуля сохраняются в профилях. Вы можете изменять параметры профиля при создании пользовательского профиля или задачи на проверку событий. Для настройки профиля в окне **Параметры профиля** доступны следующие блоки параметров:

Входящие данные

- **Конвейер обработки событий** − раскрывающийся список для выбора конвейеров, события которых необходимо проверить;
- **Созданные** − по ссылке открывается окно для настройки периода времени регистрации событий, которые нужно проверить;
- **Фильтр событий** − поле ввода PDQL-запроса для дополнительной фильтрации событий;

> **Примечание.** По ссылке **Вставить условие из сохраненного запроса** вы можете выбрать запрос, сохраненный ранее на странице **События**.

- **База данных** − раскрывающийся список для выбора базы данных Ankey SIEM NG Knowledge Base с правилами корреляции для проверки;
- **Набор для установки** − раскрывающийся список для выбора набора для установки объектов БД в ПК Ankey SIEM NG с правилами корреляции для проверки;

> **Примечание.** По ссылке **Настроить набор для установки** вы можете открыть вебинтерфейс в Ankey SIEM NG Knowledge Base и настроить набор для установки.

- **Настройка табличных списков** − раскрывающиеся списки для выбора способа наполнения табличных списков, используемых правилами при проверке событий. Перечень табличных списков формируется автоматически по выбранным правилам корреляции. Вы можете указать способ наполнения для всех списков одного типа или для каждого списка в отдельности (перечень табличных списков одного типа открывается по кнопке ›). Возможны следующие способы наполнения табличных списков:
  - **Не загружать** − использовать пустые списки;
  - **Загрузить из Ankey SIEM NG Knowledge Base** − наполнить записями из выбранной базы данных Ankey SIEM NG Knowledge Base;

- **Загрузить из SIEM** − наполнить записями актуальных табличных списков из конвейера, к которому подключен агент задачи ретроспективной корреляции;
- **Загрузить из CSV-файла** − импортировать записи табличных списков из файла формата CSV. Для каждого табличного списка нужно указать расположение файла с записями.
  Поддерживается импорт записей из файлов формата CSV в кодировке UTF-8. В первой строке файла нужно указать наименования колонок, в качестве разделителя данных в строке нужно использовать точку с запятой (;).
  Файл для импорта должен содержать значения для ключевых колонок табличного списка. Значения ячеек должны удовлетворять требованиям: для типа данных DateTime − дата должна находиться в интервале от 1970-01-01 00:00:00 до 2106-02-07 06:28:15; для Number − число должно находиться в интервале от −9223372036854775807 до 9223372036854775807; для String − длина строки не должна превышать 16 382 символов (65 531 байт).

Примечание. По ссылке **Добавить фильтр PDQL** вы можете ввести PDQL-запрос для дополнительной фильтрации записей табличных списков.

Выполнение задачи

- **Продолжительность** − ограничение максимального времени выполнения задачи. По умолчанию время не ограничено, по ссылке открывается блок параметров для ввода максимального времени выполнения. Если задача не будет выполнена до окончания указанного времени, она будет остановлена с ошибкой;
- **Входной поток событий** − ограничение максимального потока событий, поступающих на проверку. По умолчанию установлен максимальный поток 1000 событий в секунду. Можно снять это ограничение или указать по ссылке другое значение;
- **Срабатывание правил корреляции** − ограничение максимального числа регистрируемых событий ИБ. По умолчанию установлено ограничение в 10 000 событий. Можно снять это ограничение или указать по ссылке другое значение (число событий отслеживается с точностью до удвоенного значения входного потока событий). При достижении указанного значения задача будет остановлена с ошибкой.

Примечание. По ссылке **указать исключения** вы можете через запятую указать системные названия правил корреляции: события, регистрируемые по этим правилам, не будут учитываться при подсчете общего числа событий. Можно указать шаблон для названий правил, используя звездочку (*) для различающихся частей названий.

Сохранение результатов

- **Новые корреляционные события** − раскрывающиеся списки для выбора варианта сохранения зарегистрированных в результате проверки событий ИБ. Возможные варианты:
  - **Не сохранять** − не сохранять события;
  - **Сохранять в SIEM** − сохранить события в ПК Ankey SIEM NG;
  - **Сохранять в файл** − сохранить события в файл формата JSON (по умолчанию).
- **Новые инциденты** − раскрывающиеся списки для включения регистрации инцидентов по результатам проверки. Возможные варианты:
  - **Не сохранять** − не регистрировать инциденты (по умолчанию);
  - **Сохранять в SIEM** − регистрировать инциденты**.**
- **Агрегация инцидентов** − раскрывающиеся списки для настройки группировки (агрегации) инцидентов, регистрируемых по результатам проверки. Возможные варианты:
  - **Не связывать** − не группировать инциденты;
  - **Только в рамках задачи** − группировать только с другими инцидентами, зарегистрированными по результатам проверки (по умолчанию);
  - **Связывать всегда** − группировать со всеми инцидентами ПК Ankey SIEM NG.
- **Изменения табличных списков** − раскрывающиеся списки для выбора варианта сохранения записей табличных списков для правил корреляции и обогащения, добавленных по результатам проверки. Возможные варианты:
  - **Не сохранять** − не сохранять записи (по умолчанию);
  - **Сохранять в файл** − сохранять записи в файл формата CSV.

11 Работа с дашбордами и виджетами

На главной странице ПК Ankey SIEM NG на дашбордах представлены данные, полученные в процессе мониторинга информационной безопасности. Вы можете:

1. Просматривать статистическую информацию на дашбордах. Стандартные виджеты отображают информацию об активах, входящих в группы активов, а также о тех уязвимостях, событиях и инцидентах, которые связаны с активами из групп активов. Пользовательские виджеты отображают информацию о событиях.

   Примечание. Вы не можете менять состав и расположение виджетов стандартного дашборда **Стартовая страница**.

2. Создавать, переименовывать, изменять, перемещать и удалять пользовательские дашборды.
3. Создавать, изменять, перемещать и удалять виджеты.
4. Выгружать данные с виджетов в PNG- или CSV-файл.

11.1 Виджеты по активам

Набор стандартных виджетов по активам показывает, сколько активов есть в системе, как изменялось их количество за выбранный период, сколько в системе есть активов без указанной значимости и актуальны ли данные сканирования активов. Эти виджеты отображаются на стартовом дашборде.

Количество активов

Виджет **Количество активов** представляет собой тренд и число. Число означает количество активов в системе. Если выбрана точная дата, то отображается количество активов на эту дату. Если выбран период, то отображается количество активов на конец периода. Тренд показывает, как менялось это количество.

Значимость активов

Виджет **Значимость активов** представляет собой числа и график. Первое число означает количество активов, для которых не указана значимость. Второе число означает общее количество активов в системе. Если выбрана точная дата, то отображается количество активов на эту дату. Если выбран период, то отображается количество активов на конец периода. График показывает, как менялось количество всех активов.

Уязвимости по уровню

Виджет **Уязвимости по уровню** представляет собой график распределения уязвимостей по уровням опасности. Вы можете включать или отключать отображение уязвимостей по уровням опасности с помощью фильтров **Низкий**, **Средний**, **Высокий**, **Критический**.

По умолчанию эти фильтры отключены (отображаются все данные). При наведении курсора на линию графика отображается количество уязвимостей для выбранного уровня опасности на заданную дату и время. Для графика вы можете

дополнительно настраивать отображение легенды и подписей значений на графике, названия для осей X и Y; включить отображение данных, которые отличаются между собой существенно (на порядки), в виде логарифмической шкалы.

Актуальность данных об активах

Виджет представляет собой график, отображающий количество активов и состояние данных сканирования (например, данные отсутствуют, неактуальны, сканирование не проводилось). Под графиком отображается количество активов, у которых не определена операционная система.

Топ-10 уязвимых активов

Виджет **Топ-10 уязвимых активов** представляет собой гистограмму, которая отражает 10 самых уязвимых активов.

При наведении курсора на линию гистограммы отображается распределение уязвимостей по уровням опасности. Вы можете включать или отключать отображение уровней опасности с помощью фильтров **Низкий**, **Средний**, **Высокий**, **Критический**.

По нажатию на FQDN (например, на **192.168.0.1 (siem.example)**) отображается мини-карточка актива (см. раздел 6.1.6). Также вы можете перейти из виджета на страницу **Активы**, чтобы ознакомиться с детальной информацией об уязвимостях актива.

11.2 Виджеты по событиям

Набор стандартных виджетов для событий отображает общее количество событий за период времени, динамику появления событий и распределение во времени уязвимостей по уровню опасности.

Виджеты **Средний поток событий** и **Распределение среднего потока событий** отображаются на дашборде **Стартовая страница**.

Количество событий

Виджет **Количество событий** представляет собой график. График содержит информацию о количестве событий за выбранный период. При наведении курсора на линию графика отображается количество событий на заданную дату и время. Для графика вы можете дополнительно настраивать отображение легенды и подписей значений, названия для осей X и Y.

Средний поток событий

Виджет **Средний поток событий** представляет собой тренд и число. Число означает среднее количество событий, направленных в хранилище системы за одну секунду. Тренд позволяет отслеживать динамику этого показателя за период времени. Вы можете настраивать детализацию данных.

Также вы можете перейти из виджета на страницу **Мониторинг обработки событий**, чтобы ознакомиться с данными о собранных событиях.

Распределение среднего потока событий

Виджет **Распределение среднего потока событий** представляет собой график. График содержит распределение среднего количества событий, направленных в хранилище системы за одну секунду, за период времени. При наведении курсора на линию графика отображается количество событий на

заданную дату и время. Вы можете дополнительно настраивать отображение легенды и подписей значений, названия для осей X и Y.

Также вы можете перейти из виджета на страницу **Мониторинг обработки событий**, чтобы ознакомиться с данными о собранных событиях.

События по категории с распределением по важности

Виджет **События по категории с распределением по важности** представляет собой график. График содержит распределение событий по трем уровням важности. Вы можете включать или отключать отображение уровней важности с помощью фильтров **Низкая**, **Средняя**, **Высокая**. По умолчанию эти фильтры отключены (отображаются все данные).

11.3 Виджеты по инцидентам

Набор виджетов для инцидентов отображает общее количество открытых инцидентов за период времени, распределение во времени открытых инцидентов по категории и уровню опасности. Эти виджеты отображаются на дашборде **Стартовая страница**.

Количество инцидентов

Виджет **Количество инцидентов** представляет собой тренд и число. Тренд показывает тенденции изменения количества открытых инцидентов во времени. Число означает количество открытых инцидентов, зарегистрированных в системе за указанный период времени.

Инциденты по уровню опасности

Виджет Инциденты по уровню опасности представляет собой график, на котором отображается количество открытых инцидентов высокого, среднего и низкого уровня опасности за период времени. При наведении курсора на линию графика отображается количество инцидентов на заданную дату и время. Вы можете дополнительно настраивать отображение легенды и подписей значений, названия для осей X и Y, представить данные в виде гистограммы с накоплением или логарифмической шкалы. Также вы можете перейти из виджета на страницу Инциденты, чтобы ознакомиться с данными об открытых инцидентах.

Инциденты по категории

Виджет **Инциденты по категории** представляет собой круговую диаграмму, которая отражает распределение открытых инцидентов по статусам.

Вы можете объединять сегменты диаграммы в один. Такой сегмент будет называться **Другое**. Вы можете объединять сегменты, доля которых на диаграмме меньше заданного процента; сегменты, значение которых меньше заданного числа; все сегменты кроме нескольких первых. Также вы можете просматривать детализированную информацию только по объединенным сегментам, перейдя в сегмент **Другое**.

11.4 Виджет по проверкам

Виджет **Проверки по чек-листу** представляет собой список групп включенных проверок системы (см. раздел 14) с индикаторами состояния.

Вы можете настраивать период обновления данных. Также вы можете перейти из виджета на страницу **Чек-лист настройки системы**, чтобы

ознакомиться с подробной информацией о проверках и действиях, которые необходимо выполнить, чтобы настроить систему.

11.5 Создание дашборда

На главной странице Ankey SIEM NG на дашбордах представлены данные, полученные в процессе мониторинга информационной безопасности. При первом запуске Ankey SIEM NG стандартный дашборд формируется автоматически и содержит предустановленный набор виджетов. Вы можете создавать дашборды и добавлять на них виджеты самостоятельно. При создании дашборда можно использовать как стандартные шаблоны, так и шаблоны, созданные другими пользователями.

Примечание. Дашборд, созданный по шаблону, сохраняет с ним связь. Это означает, что если изменяется шаблон, изменяются и все дашборды, созданные на его основе.

❖ Чтобы создать дашборд:

1. На главной странице в панели инструментов нажмите +. Откроется окно **Создание дашборда**.
2. В поле **Название** введите название дашборда.
3. Выберите вариант сетки, по которой будут располагаться виджеты.
4. Нажмите кнопку **Создать**.

Дашборд создан.

❖ Чтобы создать дашборд на основе шаблона:

1. На главной странице в панели инструментов нажмите +.
2. Откроется окно **Создание дашборда**.
3. Выберите одну из вкладок с шаблонами и щелкните левой кнопкой мыши по полю с описанием шаблона.
4. Отобразятся параметры дашборда.

Примечание. Вы можете изменить название дашборда или отвязать его от шаблона.

5. Нажмите кнопку **Создать**.

Дашборд создан.

По умолчанию новый дашборд отображается справа от уже существующих, но вы можете его перетащить.

11.6 Создание шаблона дашборда

В Ankey SIEM NG вы можете создавать шаблоны дашбордов и хранить их в базе шаблонов. При этом можно использовать стандартные шаблоны и шаблоны, созданные другими пользователями. Дашборд, созданный по шаблону, сохраняет с ним связь. Это означает, что если изменяется шаблон, изменяются и все дашборды, созданные на его основе.

❖ Чтобы создать шаблон дашборда:

1. На главной странице выберите дашборд.

2. В панели инструментов нажмите  и в раскрывшемся меню нажмите кнопку **Сохранить как новый шаблон**.
   Откроется окно создания шаблона дашборда.
3. В поле **Название** введите название шаблона.
4. Если требуется, в поле **Описание** введите информацию о шаблоне.

> **Примечание.** Дополнительная информация может помочь другим пользователям выбрать наиболее удобный и полезный для них шаблон.

5. Нажмите кнопку **Сохранить**.

Шаблон дашборда создан.

11.7 Изменение дашборда

❖ Чтобы изменить название пользовательского дашборда:

1. На главной странице выберите пользовательский дашборд.
2. В панели инструментов нажмите  и в открывшемся окне введите новое название дашборда.
3. Нажмите кнопку **Сохранить**.

Название пользовательского дашборда изменено.

Также вы можете отвязать дашборд от шаблона по кнопке **Сохранить** и отвязать от шаблона.

11.8 Удаление дашборда

❖ Чтобы удалить пользовательский дашборд:

1. На главной странице выберите пользовательский дашборд.
2. В панели инструментов нажмите  и подтвердите удаление дашборда.

Дашборд удален.

11.9 Создание виджета по событиям

Вы можете создавать виджеты, выбирая графическое представление исходя из решаемых вами задач.

❖ Чтобы создать виджет по отфильтрованным событиям:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации **Все события** нажмите  .
3. Отфильтруйте события с помощью PDQL-запроса.
4. В панели инструментов нажмите  .
5. Выберите и настройте графическое представление виджета – таблицу, столбчатую диаграмму, график, круговую диаграмму.
6. В панели инструментов нажмите кнопку  **Сохранить в библиотеку виджетов**.
7. В открывшемся окне введите название виджета и название фильтра.

8. Укажите папку фильтра и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

❖ Чтобы создать табличный виджет по сгруппированным и агрегированным событиям:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели фильтрации **Все события** нажмите .
3. Выполните группировку событий.
   В таблице отобразятся колонки с условиями группировки событий.
4. В панели фильтрации **Все события** нажмите .
5. Проанализируйте данные о событиях.
   В таблице отобразятся результаты анализа данных о событиях.
6. В панели инструментов нажмите .
7. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.
8. В открывшемся окне введите название виджета и название фильтра.
9. Укажите папку фильтра и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

11.10 Создание табличного виджета по событиям

Вы можете создавать табличные виджеты, построенные на основе данных обо всей совокупности событий, представленной в таблице событий.

❖ Чтобы создать табличный виджет по событиям:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. В панели инструментов нажмите .
3. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.
4. В открывшемся окне введите название виджета и название фильтра.
5. Укажите папку фильтра и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

11.11 Создание виджета по активам

Вы можете создавать виджеты по отфильтрованным активам.

❖ Чтобы создать виджет по отфильтрованным активам:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. Сгруппируйте и проанализируйте данные об активах (см. раздел 6.2.4).
3. В панели инструментов нажмите .
4. Выберите и настройте графическое представление виджета – таблицу, столбчатую диаграмму, график, круговую диаграмму.
5. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.

6. В открывшемся окне введите название виджета и название запроса.
7. Укажите папку запроса и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

11.12 Создание табличного виджета по активам

Вы можете создавать табличные виджеты, построенные на основе данных обо всей совокупности активов, представленной в таблице активов.

❖ Чтобы создать табличный виджет по активам:

1. В главном меню выберите раздел **Активы**.
   Откроется страница **Активы**.
2. В панели инструментов нажмите .
3. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.
4. В открывшемся окне введите название виджета и название запроса.
5. Укажите папку запроса и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

11.13 Создание табличного виджета по данным из табличного списка

Вы можете создавать табличные виджеты на основе данных из табличных списков.

❖ Чтобы создать табличный виджет на основе данных из табличного списка:

1. В главном меню в разделе **Сбор данных** выберите пункт **Табличные списки**.
   Откроется страница **Табличные списки**.
2. В панели **Табличные списки** выберите табличный список.
3. В панели инструментов нажмите .
   В рабочей области появится построенный виджет. В панели **Данные для виджета** вы можете отфильтровать и отсортировать записи, а также задать их количество.
4. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.

Виджет создан и сохранен в библиотеку виджетов.

11.14 Добавление виджета на дашборд

Вы можете добавлять виджеты только в пустые ячейки пользовательских дашбордов. Если пустых ячеек на дашборде нет, необходимо сначала удалить один виджет, затем добавить другой.

Для поиска виджета с необходимой статистической информацией в библиотеке предусмотрена фильтрация виджетов.

❖ Чтобы добавить виджет на дашборд:

1. На главной странице выберите пользовательский дашборд.
2. В свободной ячейке нажмите кнопку **Добавить виджет**.

Откроется окно **Добавить виджет**.

3. В окне выберите хотя бы один виджет.
4. Нажмите кнопку **Добавить**.

Виджет добавлен на дашборд.

11.15 Изменение виджета на дашборде

В процессе работы со статистическими данными, представленными на виджетах, вы можете изменять виджеты с учетом решаемых задач.

❖ Чтобы изменить виджет:

1. На главной странице выберите дашборд.
2. В панели инструментов виджета нажмите ⋮ и в раскрывшемся меню выберите пункт **Настроить**.
   Откроется страница **Настройка виджета**.
3. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Виджет изменен.

11.16 Удаление виджета с дашборда

❖ Чтобы удалить виджет с дашборда:

1. На главной странице выберите пользовательский дашборд.
2. В панели инструментов виджета нажмите ⋮ и в раскрывшемся меню выберите пункт **Удалить**.

Виджет удален с дашборда.

11.17 Экспорт статистических данных

Информация о текущем состоянии информационной инфраструктуры организации может быть вам полезна при проведении аудитов и формировании отчетности. Вы можете экспортировать статистические данные с графического виджета в файл формата PNG или с табличного виджета в файл формата CSV.

❖ Чтобы экспортировать данные с графического виджета:

1. На главной странице выберите дашборд.
2. В панели инструментов графического виджета нажмите ⋮, в раскрывшемся меню выберите пункт **Скачать в PNG** и подтвердите сохранение.

Файл сохранен на ваш компьютер.

❖ Чтобы экспортировать записи с табличного виджета:

1. На главной странице выберите дашборд.
2. В панели инструментов табличного виджета нажмите ⋮ и в раскрывшемся меню выберите один из вариантов:
   - если вы хотите экспортировать только выбранные записи – **Экспортировать выбранные записи в CSV-файл**;
   - если вы хотите экспортировать все отображаемые записи – **Экспортировать отображаемые записи в CSV-файл**.
3. Подтвердите сохранение.

Файл сохранен на ваш компьютер.

12 Работа с отчетами

При работе с большим количеством данных необходимо, чтобы они были хорошо организованы и наглядно представлены. Данные, полученные в процессе мониторинга информационной безопасности и представленные на дашбордах на главной странице ПК Ankey SIEM NG, вы можете выгружать в PDF-файлы. Такие файлы называются отчетами и дают вам возможность:

- исследовать данные об активах, событиях или инцидентах (например, определить, какие активы чаще всего участвуют в инцидентах);
- изучить данные об уязвимостях различного типа, обнаруженных в системе (например, динамику среднего времени жизни важных уязвимостей);
- оценить процесс управления уязвимостями в организации (например, соотношение количества важных уязвимостей, обрабатываемых автоматически на основе политик, и обрабатываемых вручную);
- определить наиболее значимые данные (например, в каком регионе инциденты вызвали самый большой ущерб);
- находить в данных закономерности и аномалии, которые невозможно выявить при ручном анализе (например, понять, как защита периметра сети влияет на защищенность конкретного узла).

Вы можете управлять отчетами на странице **Отчеты** (**Система** → **Отчеты**).

Рабочая область страницы **Отчеты** содержит:

- таблицу задач по выпуску отчетов, в которой отображается подробная информация обо всех таких задачах;
- панель **История выпусков**, в которой отображается информация о дате и времени выпуска отчета, а также о доступности отчета для скачивания;
- панель **Сводка** с подробной информацией о задаче по выпуску отчета, которая выбрана в таблице задач по выпуску отчетов.

Вы можете создавать отчеты самостоятельно или использовать отчеты с предустановленными параметрами; копировать, изменять и удалять отчеты. Также вы можете настроить выпуск отчетов по расписанию или выпускать отчеты вручную.

12.1 Создание задачи по выпуску пользовательского отчета

При создании задачи по выпуску пользовательского отчета вы можете:

- задавать последовательность объектов (текстов, изображений, виджетов), из которых будет состоять отчет;
- выбирать для отчета различные типы визуализации, например диаграммы, графики или гистограммы;

– настраивать внешний вид отчета: добавить колонтитулы, легенды и подписи для диаграмм.

❖ Чтобы создать задачу по выпуску пользовательского отчета:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание задачи**.
3. В списке шаблонов отчетов выберите пункт **Без шаблона** и нажмите кнопку **Далее**.
   Откроется страница **Редактирование задачи <Название отчета>**.
4. В панели **Настройка задачи** на вкладке **Параметры отчета** настройте внешний вид отчета.

Примечание. Вы можете изменить название задачи по выпуску отчета, если требуется, а также настроить отображение информации в \колонтитулах.

5. Выберите вкладку **Параметры выпуска**.
6. Настройте формат и частоту выпуска отчета, укажите получателя отчета.
7. В рабочей области нажмите  и выберите объект.
   На страницу отчета добавится новый объект.

Примечание. Вы можете добавить несколько объектов.

8. Выберите объект.
   Откроется панель настройки объекта.
9. Настройте выбранный объект.
10. Нажмите кнопку **Сохранить** и в раскрывшемся меню выберите пункт **Сохранить задачу**.
11. Нажмите кнопку **Обновить**.
12. Нажмите кнопку **Закрыть**.

Задача по выпуску пользовательского отчета создана и отображается в таблице задач по выпуску отчетов.

12.2 Создание задачи по выпуску отчета на основе шаблона

Отчеты удобнее всего создавать на основе шаблонов. Шаблоны – это готовые типовые отчеты, в совокупности предоставляющие наиболее полную информацию о состоянии безопасности системы. Они позволяют провести инвентаризацию операционной системы, программного или аппаратного обеспечения, собрать структурированную информацию о событиях и зарегистрированных инцидентах для последующего анализа. С их помощью вы можете понять, насколько хорошо выстроен процесс обработки уязвимостей.

❖ Чтобы создать задачу на выпуск отчета на основе шаблона:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.

Откроется окно **Создание задачи**.

3. Выберите шаблон отчета из списка и нажмите кнопку **Далее**.
   Откроется окно **Создание задачи** с описанием выбранного шаблона и информацией о расписании его запуска.
4. Нажмите кнопку **Далее**.
   Откроется страница **Редактирование задачи <Название отчета>**.
5. В панели **Настройка задачи** на вкладке **Параметры отчета** настройте внешний вид отчета.

> **Примечание.** Вы можете изменить название задачи по выпуску отчета, если требуется, а также настроить отображение информации в колонтитулах.

6. Выберите вкладку **Параметры выпуска**.
7. Настройте формат и частоту выпуска отчета, укажите получателя отчета.

❖ Чтобы добавить дополнительные объекты в отчет, если это необходимо:

1. В рабочей области нажмите  и выберите объект.
   На страницу отчета добавится новый объект.

> **Примечание.** Вы можете добавить несколько объектов.

2. Выберите объект.
   Откроется панель настройки объекта.
3. Настройте выбранный объект.
4. Нажмите кнопку **Сохранить** и в раскрывшемся меню выберите пункт **Сохранить задачу**.

Задача по выпуску отчета на основе шаблона создана и отображается в таблице задач по выпуску отчетов.

12.2.1 Создание задачи по выпуску отчета по активам

❖ Чтобы создать задачу по выпуску отчета по активам:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно Создание задачи.
3. В списке шаблонов выберите **Отчеты по активам, событиям и инцидентам**.
   Откроется окно **Создание задачи**.
4. В поле **Название** введите название отчета.
5. В раскрывающемся списке **Источник** выберите **Активы**.
6. В раскрывающемся списке **В группе** выберите группы активов, данные о которых должны войти в отчет.
7. Если вы хотите, чтобы в отчет попадали также данные об активах из вложенных групп, установите флажок **Включая вложенные**.
8. В раскрывающемся списке **Отчет** выберите шаблон отчета.

9. Настройте расписание, в соответствии с которым отчет будет автоматически выпускаться в указанное время с заданной периодичностью.
10. Если требуется, в поле **Кому** укажите адрес электронной почты для доставки отчета.

> **Примечание.** Для скачивания доступны только два последних отчета.

11. Нажмите кнопку **Сохранить**.

Задача по выпуску отчета по активам создана.

12.2.2 Создание задачи по выпуску отчета по событиям

❖ Чтобы создать задачу по выпуску отчета по событиям:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание задачи**.
3. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание задачи**.
4. В списке шаблонов выберите **Отчеты по активам, событиям и инцидентам**.
   Откроется окно **Создание задачи**.
5. В поле **Название** введите название отчета.
6. В раскрывающемся списке **Источник** выберите **События**.
7. В раскрывающемся списке **В группе** выберите группы активов, данные о событиях в которых должны войти в отчет.
8. Если вы хотите, чтобы в отчет попадали также данные о событиях в активах из вложенных групп, установите флажок **Включая вложенные**.
9. В раскрывающемся списке **Фильтр** выберите фильтр событий.
10. В раскрывающемся списке **Отчет** выберите шаблон отчета.
11. Настройте расписание, в соответствии с которым отчет будет автоматически выпускаться в указанное время с заданной периодичностью.
12. Если требуется, в поле **Кому** укажите адрес электронной почты для доставки отчета.

> **Примечание.** Для скачивания доступны только два последних отчета.

13. Нажмите кнопку **Сохранить**.

Задача по выпуску отчета по событиям создана.

12.2.3 Создание задачи по выпуску отчета по инцидентам

❖ Чтобы создать задачу по выпуску отчета по инцидентам:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание задачи**.

3. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Создание задачи**.
4. В списке шаблонов выберите **Отчеты по активам, событиям и инцидентам**.
   Откроется окно **Создание задачи**.
5. В поле **Название** введите название отчета.
6. В раскрывающемся списке **Источник** выберите **Инциденты**.
7. В раскрывающемся списке **В группах** выберите группы активов, данные об инцидентах в которых должны войти в отчет.
8. Если вы хотите, чтобы в отчет попадали также данные об инцидентах в активах из вложенных групп, установите флажок **Включая вложенные**.
9. В раскрывающемся списке **Фильтр** выберите фильтр инцидентов.
10. В раскрывающемся списке **Отчет** выберите шаблон отчета.
11. Настройте расписание, в соответствии с которым отчет будет автоматически выпускаться в указанное время с заданной периодичностью.
12. Если требуется, в поле **Кому** укажите адрес электронной почты для доставки отчета.

> **Примечание.** Для скачивания доступны только два последних отчета.

13. Нажмите кнопку **Сохранить**.

Задача по выпуску отчета по инцидентам создана.

12.3 Создание задачи по выпуску отчета на основе существующей

Если вам необходимы несколько похожих задач по выпуску отчета, вы можете создать их на основе существующей задачи, изменив отдельные параметры.

Вы не можете изменить источник данных для отчета (например, на основе задачи по выпуску отчета по активам вы не можете создать задачу по выпуску отчета по инцидентам).

❖ Чтобы создать задачу по выпуску отчета на основе существующей:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
   Откроется страница **Отчеты**.
2. Выберите задачу по выпуску отчета.
3. В панели инструментов нажмите кнопку **Копировать**.
   Откроется страница **Редактирование задачи <Название отчета> (копия)**.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Задача по выпуску отчета создана.

12.4 Изменение задачи по выпуску отчета

❖ Чтобы изменить задачу по выпуску отчета:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

Откроется страница **Отчеты**.
2. Выберите задачу по выпуску отчета.
3. В панели инструментов нажмите кнопку **Редактировать**.
Откроется страница с параметрами задачи по выпуску отчета.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Примечание. Вы не можете изменить источник данных для отчета (например, вы не можете изменить отчет по активам на отчет по инцидентам).

Задача по выпуску отчета изменена.

12.5 Удаление задачи по выпуску отчета

❖ Чтобы удалить задачу по выпуску отчета:
1. В главном меню в разделе **Система** выберите пункт **Отчеты**.
Откроется страница **Отчеты**.
2. Выберите задачу по выпуску отчета.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача по выпуску отчета удалена.

12.6 Управление выпуском отчетов

В ПК Ankey SIEM NG на странице **Отчеты** вы можете настроить автоматический выпуск отчетов по расписанию или выпустить отдельный отчет вручную. При выпуске отчета по расписанию ПК Ankey SIEM NG отправляет указанным адресатам электронное письмо с выпущенным отчетом во вложении.

ПК Ankey SIEM NG хранит последние два файла отчета. Вы можете скачать их в панели **История выпусков**.

Выпуск отчетов осуществляется поочередно. Это означает, что пока ПК Ankey SIEM NG не завершит выпуск одного отчета, вы не сможете выпустить еще один отчет.

12.7 Выпуск отчета по активам

❖ Чтобы выпустить отчет по выбранной группе активов:
1. В главном меню выберите раздел **Активы**.
Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите кнопку **Выпустить отчет**.
Откроется окно **Выпуск отчета**.
4. Выберите шаблоны отчетов по активам или уязвимостям.
5. В поле **Формат** выберите формат отчета.
6. Нажмите кнопку **Выпустить отчет**.

Отчеты по активам используются для инвентаризации операционной системы, программного или аппаратного обеспечения.

Отчет состоит из нескольких разделов:

– **Параметры отчета** – список активов, на основании которых сформирован отчет;

- **Общая статистика** − отображение информации отчета в виде таблицы или графической диаграммы;
- **Свойства объектов** − более подробное описание параметров каждого из объектов (только для отчетов по активам).

12.8 Выпуск отчета по событиям

Отчеты по событиям используются для сбора структурированной информации о событиях для последующего анализа и выявления потенциальных атак на уязвимые объекты.

Для выпуска доступны следующие две группы отчетов.

Детальные отчеты по событиям

Детальные отчеты по событиям собираются на основе отображаемых данных о событиях в соответствии с выбранными фильтрами.

Детальные отчеты по событиям поддерживают форматы XLSX, CSV.

Примечание. Количество событий, доступных для единоразового отчета, ограничено одним миллионом для обоих форматов. При попытке создания отчета по большему количеству событий будет сформирован файл с одним миллионом записей, остальные записи включены в отчет не будут.

Детальный отчет по событиям представляет собой таблицу:

- **Заголовок** содержит колонки, отображаемые в соответствии с выбранным фильтром.
- **Информация о событиях** содержит: в случае отчета по всем событиям – множество событий формируется в соответствии с пунктами из секции «Исходные данные». Если пользовательский фильтр был изменен, но не был сохранен, то в отчете он будет отражен в виде PDQL-строки; в случае отчета по выбранным событиям – множество событий, выбранных пользователем.

Для каждого события выгружаются поля, отображаемые в соответствии с выбранным фильтром. Сортировка событий также осуществляется в соответствии с выбранным фильтром.

Отчеты по статистике событий

Отчеты по статистике событий собираются на основе данных о распределении количества событий в зависимости от отдельных источников, пользователей, зарегистрированных исходящих или входящих подключений.

Отчеты по статистике событий поддерживают форматы PDF, MHT, DOCX и состоят из нескольких разделов:

- **Параметры отчета** – раздел отображает название выбранного отчета, выбранную группу активов или все активы, а также выбранный временной интервал и фильтр;
- **Распределение событий по времени** – диаграмма, отображающая количество событий по дате, часам и минутам в зависимости от выбранного интервала времени. В случае отчетов по "Статистике событий по

пользователям" данный раздел содержит следующие подразделы: **Действия пользователей**, **Действия над пользователями**, **Пользовательские взаимодействия**. Первые два раздела содержат диаграммы по пользователям и количеству их событий и табличное представление. Третий раздел – табличное представление пользователей с указанием общего количества действий, произведенных ими в системе. Данные разделы заполняются в том случае, если значения полей subject.name и object.name равны account.

Выпуск отчета

❖ Чтобы получить отчеты по событиям:

1. В главном меню выберите раздел **События**.
   Откроется страница **События**.
2. Выберите группу событий по активам.
3. Откройте временной фильтр и установите интервал, за который необходимо построить отчет.

> Внимание! В детальном отчете по всем событиям и в детальном отчете по выбранным событиям время соответствует часовому поясу UTC+0.

4. Нажмите кнопку **Выпустить отчет**.
   Откроется окно, в котором вы можете выбрать один из шаблонов отчетов.
5. Выберите шаблон отчета.
   После выбора шаблона появится поле **Формат**.
6. Выберите формат отчета.
7. Нажмите кнопку **Выпустить**.

12.9 Выпуск отчета об инцидентах

Отчет о зарегистрированных в ПК Ankey SIEM NG инцидентах нужен, чтобы вы могли:

- узнать количество инцидентов и вид инцидентов в заданном периоде;
- использовать полученные данные при анализе инцидента или в расследовании инцидента;
- формировать статистику по инцидентам.

❖ Чтобы выпустить отчет об инцидентах:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
   Откроется страница **Инциденты**.
2. В панели инструментов нажмите кнопку **Выпустить отчет**.
   Откроется окно **Выпуск отчета**.
3. В раскрывающемся списке **Отчет** выберите вид отчета:
   - **Открытые**. В отчете будут отражены инциденты, зарегистрированные в заданный промежуток времени и еще не расследованные. Формат файла отчета – PDF;

- **Завершенные**. В отчете будут отражены расследованные инциденты, зарегистрированные в заданный промежуток времени и сгруппированные по типу. Формат файла отчета – PDF;
- **Общие**. В отчете будут отражены все зарегистрированные инциденты; новые, еще не расследованные инциденты, зарегистрированные в заданный промежуток времени и сгруппированные по участникам. Формат файла отчета – XLXS.

Примечание. В поле **Формат** ПК Ankey SIEM NG на основании выбранного вида отчета автоматически проставит формат файла отчета.

4. В раскрывающемся списке **Период** выберите период времени, за который вы хотите сформировать отчет (по умолчанию установлено значение **За последние 7 дней**).
5. Нажмите кнопку **Выпустить отчет**.

Примечание. ПК Ankey SIEM NG формирует имя файла отчета по шаблону: Перечень инцидентов_<ГГГГ-ММ-ДД> ЧЧ_ММ_ССZ, где ГГГГ – год, ММ – месяц, ДД – день, ЧЧ – час, ММ – минуты, СС – секунды, Z – зона UTC. Пример: **Перечень инцидентов_2018-05-23 06_18_08Z**. Время формирования отчета ЧЧ_ММ_ССZ указано в нулевом часовом поясе (GMT+0).

Отчет по заданным параметрам сформирован в локальной папке, указанной в свойствах браузера.

13 Работа с уведомлениями

Уведомления Ankey SIEM NG содержат информацию об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных, собираемых событиях и параметрах потока событий, а также о выявляемых инцидентах ИБ и состоянии системы.

Вы можете автоматизировать отправку уведомлений, создавая задачи на странице **Уведомления**.

13.1 Создание задачи для отправки уведомления об изменении общего числа активов

❖ Чтобы создать задачу для отправки уведомления об изменении общего числа активов:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об изменении общего числа активов**.
5. Если необходимо, снимите флажок **Создание активов** или **Удаление активов**.
6. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления;
   - если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса;
7. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
8. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об изменении общего числа активов создана.

13.2 Создание задачи для отправки уведомления об изменениях в группах активов

❖ Чтобы создать задачу для отправки уведомления об изменениях в группах активов:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об изменениях в группах активов**.
5. Если необходимо, снимите флажок **Добавление активов в группу** или **Исключение активов из группы**.
6. В раскрывающемся списке **В группах** выберите те группы активов, об изменениях которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об изменениях в группах активов создана.

13.3 Создание задачи для отправки уведомления об инцидентах

❖ Чтобы создать задачу для отправки уведомления об инцидентах:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **О состоянии инцидентов**.

5. В раскрывающемся списке **В группах** выберите те группы активов, об инцидентах которых система будет отправлять уведомление.
6. В раскрывающемся списке **Фильтр** выберите фильтр инцидентов.
7. В блоке параметров **Уведомление при срабатывании** в поле **Кому** укажите адреса электронной почты получателей уведомления.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об инцидентах создана.

13.4 Создание задачи для отправки уведомления о событиях

❖ Чтобы создать задачу для отправки уведомления о событиях:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **О событиях**.
5. В раскрывающемся списке **В группах** выберите те группы активов, о событиях которых система будет отправлять уведомление.
6. В раскрывающемся списке **Фильтр** выберите фильтр событий.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления;
   - если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о событиях создана.

13.5 Создание задачи для отправки уведомления о выходе параметров потока событий за пределы допустимых значений

Созданная задача уведомит получателей о выходе параметров потока событий от источника или форвардера за пределы допустимых значений, заданных в предупреждении для отслеживания потока событий (см. раздел 7.6).

❖ Чтобы создать задачу для отправки уведомления о выходе параметров потока событий за пределы допустимых значений:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об источниках событий**.
5. Укажите, какие уведомления необходимо отправлять получателю:
   - если необходимо отправлять уведомление о задержке поступления события от источника (форвардера) к агенту, установите флажок **Контроль задержки**;
   - если необходимо отправлять уведомление о наличии событий от источника (форвардера), установите флажок **Контроль отправки**;
   - если необходимо отправлять уведомление о выходе за пределы допустимых значений средней скорости потока событий, установите флажок **Контроль потока событий**.
6. В раскрывающемся списке **В группах** выберите те группы активов, об изменении источников которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления;
   - если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о выходе параметров потока событий за пределы допустимых значений создана.

13.6 Создание задачи для отправки уведомления о состоянии Ankey SIEM NG

❖ Чтобы создать задачу для отправки уведомления о состоянии Ankey SIEM NG:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся блоке **Сообщать** выберите **О состоянии системы**.
5. В раскрывающемся списке **Опасность** выберите тип сообщений, отправляемых системой самодиагностики.
6. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
7. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
8. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о состоянии системы создана.

13.7 Создание задачи для отправки уведомления о выполнении задач сбора данных

❖ Чтобы создать задачу для отправки уведомления о выполнении задач сбора данных:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.
   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **О задачах сбора данных**.
5. Если необходимо, снимите флажок **О начале выполнения** или **О завершении**.

6. В раскрывающемся списке **Задачи** выберите те задачи сбора данных, о начале и (или) завершении которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о выполнении задач сбора данных создана.

13.8 Остановка и повторный запуск задачи для отправки уведомления

❖ Чтобы остановить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Остановить**.

Задача для отправки уведомления остановлена.

❖ Чтобы запустить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Запустить**.

Задача для отправки уведомления запущена.

13.9 Создание новой задачи на основе существующей задачи

❖ Чтобы создать новую задачу на основе существующей:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Копировать**.
   Откроется окно **Новое уведомление**.

4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Новая задача создана на основе существующей.

13.10 Изменение задачи для отправки уведомления

❖ Чтобы изменить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется окно **Редактировать уведомление**.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Задача для отправки уведомлений изменена.

13.11 Удаление задачи для отправки уведомления

❖ Чтобы удалить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.
   Откроется страница **Уведомления**.
2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача для отправки уведомлений удалена.

14 Мониторинг обработки событий

Мониторинг обработки событий − это сбор данных о различных типах событий, зарегистрированных ПК Ankey SIEM NG, и представление их в графическом виде. Вы можете просматривать результаты мониторинга на странице **Система** → **Мониторинг обработки событий**.

Если установлено несколько конвейеров обработки событий, справа от названия страницы отображается ссылка для выбора конвейера. После выбора конвейера на странице появится статистика обработки событий этим конвейером.

Результаты мониторинга представлены на трех вкладках по типам событий: входящие события, события нормализатора и события коррелятора.

Диаграммы отображают количество событий определенного типа, зафиксированных системой в указанное время. При наведении курсора мыши на диаграмму во всплывающем сообщении отображается информация о дате и количестве зафиксированных событий. Некоторые диаграммы имеют фильтр. Вы можете увеличить диаграмму по кнопке **Увеличить**. На увеличенной диаграмме вы можете выделить область курсором мыши для более детального просмотра данных. Вы можете вернуться к увеличенной диаграмме по кнопке **Сбросить масштаб** или к странице **Мониторинг обработки событий** по кнопке **Закрыть**.

По умолчанию данные на диаграммах обновляются раз в 5 минут. Вы можете изменить частоту обновления данных в панели инструментов, нажав .

14.1 Мониторинг данных о собранных событиях

Данные о входящих событиях представлены на четырех диаграммах на вкладке **Сбор** страницы **Мониторинг обработки событий**.

Диаграмма **По источникам** отображает количество событий, полученных от различных источников. Вы можете выбрать источники в раскрывающемся списке.

Вы также можете выпускать отчеты о собранных событиях по кнопке **Выпустить отчет**.

Диаграмма **По модулям сбора** отображает количество событий, полученных от различных модулей сбора данных. Вы можете выбрать модули в раскрывающемся списке.

Диаграмма **По агентам** отображает количество событий, полученных от различных агентов. Если используется несколько агентов Ankey SIEM NG, вы можете выбрать нужные вам агенты в раскрывающемся списке.

Диаграмма **Направлены в хранилище** отображает количество собранных событий, направленных в хранилище.

14.2 Мониторинг данных о событиях нормализатора

Данные о нормализованных и ненормализованных событиях представлены на двух диаграммах на вкладке **Нормализация** страницы **Мониторинг обработки событий**.

На диаграмме **Работа службы нормализации** представлено количество

пришедших в нормализатор событий, а также нормализованных и ненормализованных событий. Вы можете выпускать отчеты по нормализованным событиям по кнопке **Выпустить отчет**.

Диаграмма **Нормализованы и направлены в хранилище** отображает количество нормализованных событий, направленных в хранилище.

14.3 Мониторинг данных о событиях коррелятора

Данные о входящих и корреляционных событиях и статистика срабатывания правил корреляции представлены на диаграммах на вкладке **Корреляция** страницы **Мониторинг обработки событий**.

На диаграмме **Работа службы корреляции** представлено количество событий, поступивших в коррелятор, и корреляционных событий.

Диаграмма **Срабатывание правил** отображает суммарное количество срабатываний правил корреляции. Вы можете перейти к выбору отдельных правил по кнопке  .

Гистограмма **Наиболее частые корреляции за 24 часа** показывает 20 правил корреляции, которые чаще других срабатывали за последние сутки.

15 Чек-лист настройки системы

После установки ПК Ankey SIEM NG необходимо его настроить, поскольку часть параметров зависит от специфики IT-инфраструктуры организации. Также в процессе работы часть параметров может изменяться, поэтому возникает необходимость периодически проверять, корректно ли настроен ПК Ankey SIEM NG. Для решения этих задач вы можете использовать чек-лист (**Система** → **Чек-лист настройки системы**), который содержит список проверок, помогающих вам правильно выполнить необходимые действия.

Для удобства проверки сгруппированы. Напротив каждой группы отображается количество пройденных в этой группе проверок. Для каждой проверки дано краткое описание, объясняющее, что именно и почему требуется настроить и какие шаги необходимо выполнить. Вы можете исключить те проверки, которые не являются для вас важными.

Отдельные параметры проверок можно изменять с помощью файла конфигурации. Подробнее о параметрах проверок см. Руководство администратора Ankey SIEM NG 4.1.2.

Для некоторых проверок приведены примеры PDQL-запросов. Такие запросы составлены с учетом значений по умолчанию параметров проверки. Если параметры проверки были изменены, вам необходимо будет внести изменения и в PDQL-запрос.

Кроме того, в ПК Ankey SIEM NG реализованы уведомления о непройденных проверках.

16 Тонкая настройка анализа данных

Тонкая настройка ПК Ankey SIEM NG для обработки и анализа данных выполняется в Ankey SIEM NG Knowledge Base. Для этого в Ankey SIEM NG Knowledge Base используются следующие объекты: правила нормализации, агрегации, обогащения, корреляции и локализации, к объектам-справочникам относятся справочник полей событий и табличные списки. Все объекты хранятся в БД.

В общем случае тонкая настройка обработки и анализа данных включает следующие шаги:

1. Вход в Ankey SIEM NG Knowledge Base.
2. Создание пользовательской БД.
3. Создание пакета экспертизы или структуры папок для пользовательских объектов.
4. Создание набора для установки объектов в конвейеры обработки событий.
5. Выбор версии SDK для валидации объектов.
6. Настройка объектов-справочников.
7. Настройка объектов для обработки и анализа событий.
8. Выбор пользовательской БД в качестве установочной.
9. Валидация объектов набора для установки.
10. Установка объектов в конвейеры обработки событий.
11. Просмотр журнала установки.

16.1 Этапы обработки событий

ПК Ankey SIEM NG выполняет непрерывный мониторинг информационной безопасности IT-инфраструктуры организации. Мониторинг осуществляется путем сбора событий с источников и отслеживания состояния активов.

Для обнаружения событий информационной безопасности используется метод rule-based reasoning. Специалисты по информационной безопасности заранее создают правила, описывающие признаки события. Событие информационной безопасности фиксируется, если в потоке событий от источников появляется событие (или последовательность событий), указанное в одном из правил, или фиксируется изменение состояния актива, описанное в одном из правил.

Нормализация событий

Для событий, собранных с разных источников, могут отличаться формат (TXT, XML, JSON) и стандарт записи. Для анализа потока событий требуется преобразовать все события к единому виду.

Нормализация события − процедура приведения необработанного события к нормализованному виду в соответствии с заранее заданным для источника и типа события правилом нормализации.

Нормализованное событие − событие представляет собой совокупность полей, заполненных данными из необработанного события согласно правилу нормализации.

Примечание. Для записи событий (нормализованных, агрегированных, корреляционных) в ПК Ankey SIEM NG используется внутренний стандарт, разработанный на основе стандарта Common Event Expression (его описание см. на сайте mitre.org).

Агрегация событий

Поток событий может содержать однотипные события, отличающиеся значением одного или нескольких полей (например, временем регистрации). Для сокращения количества таких событий выполняется агрегация событий.

Агрегация событий − это процесс отбора (в потоке нормализованных и корреляционных событий) событий, которые удовлетворяют условию заранее настроенного правила агрегации, и объединения их в одно агрегированное событие.

Обогащение событий

Обогащение событий − заполнение полей нормализованных, агрегированных и корреляционных событий согласно правилам обогащения. Поля заполняются данными, указанными в правиле обогащения или полученными из табличных списков.

Табличный список − двумерный массив данных, хранящийся в памяти ПК Ankey SIEM NG и доступный для использования в правилах корреляции и правилах обогащения.

Корреляция событий

Корреляция событий − это процесс обнаружения событий информационной безопасности путем анализа потока нормализованных событий. При обнаружении в потоке событий такой их последовательности, которая указана в условии одного из заранее настроенных правил корреляции, регистрируется корреляционное событие.

Корреляционное событие − событие информационной безопасности, представляющее собой совокупность полей, заполненных данными о возможном нарушении согласно правилам, указанным в правиле корреляции.

Инцидент − корреляционное событие, связанное с нарушением информационной безопасности. Сведения об инцидентах оперативно передаются оператору ПК Ankey SIEM NG.

Локализация событий

При регистрации нормализованного, агрегированного или корреляционного события в веб-интерфейсе ПК Ankey SIEM NG с ним может быть связано описание на русском или английском языке (в зависимости от языка интерфейса). Сопоставление описаний с регистрируемыми событиями выполняется согласно заранее настроенным правилам локализации.

16.2 Вход в Ankey SIEM NG Knowledge Base

Внимание! Для входа необходима учетная запись с правом доступа в Ankey SIEM NG Knowledge Base.

❖ Чтобы войти в Ankey SIEM NG Knowledge Base, в главном меню

ПК Ankey SIEM NG нажмите кнопку и в раскрывшемся меню выберите пункт Knowledge Base.

Откроется веб-интерфейс Ankey SIEM NG Knowledge Base на странице **Статистика**.

16.3 Работа с базами данных

По умолчанию в Ankey SIEM NG Knowledge Base используется стандартная БД **GIS_DB**, она содержит все объекты, необходимые ПК Ankey SIEM NG на всех этапах обработки и анализа данных. Вы не можете создавать, изменять и удалять объекты в стандартной БД или удалить саму БД.

Для работы со стандартными ресурсами создается ветка стандартной БД данных **Customer_Data**.

Внимание! Установка стандартной БД **GIS_DB** и создание ветки **Customer_Data** описаны в документе «Руководство по инсталляции Ankey SIEM NG 4.1.2».

На основе стандартной БД вы можете создавать пользовательские БД. Все БД в Ankey SIEM NG Knowledge Base связаны иерархически как «предок – потомок» (по принципу «один ко многим»). При создании пользовательской БД в нее копируются все объекты из родительской БД. В качестве родительской может выступать стандартная или другая пользовательская БД. Вы можете создавать, изменять и удалять объекты в пользовательской БД, удалять пользовательские БД.

Примечание. Создавать, изменять и удалять пользовательские БД могут только пользователи с правами администратора в Ankey SIEM NG Knowledge Base.

В Ankey SIEM NG Knowledge Base сохраняется история изменений всех БД. При изменении любого объекта в БД создается новая ревизия (версия) БД. Вы можете выполнить экспорт измененных объектов БД в родительскую БД или импорт из родительской БД. Для отслеживания изменения БД реализована функция сравнения ревизий.

Любая БД имеет следующие параметры:

- имя;
- идентификатор (его нельзя изменить после создания БД);
- разрешение для пользователей на просмотр объектов в БД;
- разрешение на изменение объектов в БД;
- разрешение на изменение параметров БД;
- разрешение на импорт объектов из родительской БД (слияние).

Примечание. Если не выдано ни одного разрешения, БД недоступна другим пользователям Ankey SIEM NG Knowledge Base.

Одна из БД должна быть выбрана в качестве установочной. Объекты установочной БД используются ПК Ankey SIEM NG при обработке и анализе данных. В качестве установочной вы можете выбрать пользовательскую БД.

16.3.1 Создание пользовательской БД

❖ Чтобы создать пользовательскую БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите родительскую БД.
3. В панели инструментов нажмите кнопку **Создать ветку**.
4. В открывшемся окне в поле **Имя** введите название БД.
5. В поле **Идентификатор** введите идентификатор БД.
6. В блоке параметров **Модификаторы доступа** настройте параметры БД.
7. Нажмите кнопку **Сохранить**.

Начнется процесс создания пользовательской БД. По завершении БД будет доступна для выбора.

16.3.2 Выбор установочной БД

❖ Чтобы выбрать установочную БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.
3. В панели инструментов нажмите кнопку **Сделать установочной** и подтвердите смену установочной БД.

Установочная БД выбрана. Рядом с названием БД в панели **Базы данных** появится значок  .

16.3.3 Изменение параметров БД

❖ Чтобы изменить параметры БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.
3. В панели инструментов нажмите кнопку **Управление** и в раскрывшемся меню выберите пункт **Редактировать**.
   Откроется окно **Редактирование базы данных**.
4. В поле **Имя** измените имя БД.
5. В блоке параметров **Модификаторы доступа** измените параметры БД.
6. Нажмите кнопку **Сохранить**.

Параметры БД изменены.

16.3.4 Удаление пользовательской БД

Вы не можете удалить установочную БД.

❖ Чтобы удалить пользовательскую БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.

3. В панели инструментов нажмите кнопку **Управление**, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Пользовательская БД удалена.

16.3.5 Сравнение ревизий БД

❖ Чтобы сравнить ревизии БД и просмотреть изменения объектов в БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.
   В панели для работы с БД появится список ревизий выбранной БД.
3. Наведите курсор на строку ревизии, в правой части строки нажмите кнопку **Сравнение по объектам** и в раскрывшемся меню выберите пункт **Выбрать ревизию для сравнения**.
4. Наведите курсор на ревизию для сравнения, в правой части строки нажмите кнопку **Сравнить по объектам выбранные версии**.
   Откроется страница **Сравнение ревизий**.
5. Выберите тип объектов.
   Появится список измененных объектов выбранного типа.

> **Примечание.** В списке объектов вы можете отфильтровать объекты по статусу изменения, установив флажки в меню, открывающемся по .

6. Выберите объект для просмотра изменений.
   Появится иерархический список свойств выбранного объекта. Изменения каждого свойства между выбранными ревизиями отображаются в колонках **Было** и **Стало**. Добавленные свойства отмечены зеленым цветом, измененные − оранжевым, удаленные − красным.

> **Примечание.** В иерархическом списке вы можете раскрывать или скрывать списки свойств объекта, нажав или .

16.3.6 Отмена изменений в БД

❖ Чтобы отменить изменения объектов в БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.
   В панели для работы с БД появится список ревизий выбранной БД.
3. Наведите курсор на строку ревизии, в правой части строки нажмите кнопку **Сравнение по объектам** и в раскрывшемся меню выберите пункт **Выбрать ревизию для сравнения**.

4. Наведите курсор на строку ревизии с измененными объектами, в правой части строки нажмите кнопку **Сравнить по объектам выбранные версии**.
   Откроется страница **Сравнение ревизий**.
5. Выберите тип объектов.
   Появится список измененных объектов выбранного типа.

> **Примечание.** В списке объектов вы можете отфильтровать объекты по статусу изменения, установив флажки в меню, открывающемся по .

6. Наведите курсор на строку объекта, изменения в котором нужно отменить, и в правой части строки нажмите .
7. Если нужно, аналогичным образом выберите другие объекты для отмены изменений.
8. В панели для выбора типов объектов выберите строку **Отмена изменений**.
   Отобразится список объектов, выбранных для отмены изменений.

> **Примечание.** Если требуется удалить объект из списка для отмены изменений, в правой части строки объекта нажмите .

9. В центральной панели нажмите кнопку **Отменить <N> объектов** и подтвердите отмену изменений.
   Откроется страница **Базы данных / <Название БД>**, начнется процесс отмены изменений. По завершении процесса в рабочей области страницы появится соответствующее сообщение.
10. Нажмите кнопку **Завершить**.

Отменены изменения объектов в БД.

16.3.7 Экспорт ревизий в родительскую БД

Вы не можете выполнить экспорт изменений в стандартную БД.

❖ Чтобы выполнить экспорт изменений в родительскую БД:

1. В главном меню в разделе **<Название БД>** выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.
3. Наведите курсор на строку ревизии, изменения которой нужно экспортировать, и нажмите появившуюся кнопку **Слияние**.
   Начнется экспорт данных, появится индикатор выполнения. По завершении экспорта появится сообщение «Слияние выполнено».

> **Примечание.** Вы можете остановить экспорт, нажав кнопку **Отменить**.

4. В строке сообщения нажмите кнопку **Завершить**.

Выполнен экспорт изменений в родительскую БД.

16.3.8 Импорт ревизий из родительской БД

❖ Чтобы выполнить импорт изменений из родительской БД:

1. В главном меню в разделе <**Название БД**> выберите пункт **Базы данных**.
   Откроется страница **Базы данных / <Название БД>**.
2. В панели **Базы данных** выберите БД.
3. В панели инструментов нажмите кнопку **Импорт ревизий**.
   Начнется импорт ревизий, появится индикатор выполнения. По завершении импорта появится сообщение «Импорт выполнен».

> **Примечание.** Вы можете остановить импорт, нажав кнопку **Отменить**.

4. В строке сообщения нажмите кнопку **Завершить**.

Выполнен импорт изменений из родительской БД.

16.4 Работа с ресурсами в ветке Customer_Data

16.4.1 Корректировки стандартных ресурсов в ветке Customer_Data

❖ Для корректировки стандартных ресурсов в ветке **Customer_Data** необходимо выполнить следующие действия:

1. В главном меню в разделе **<Название БД>** выберите пункт **Customer_Data**.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. В панели инструментов нажмите кнопку **Создать копию**.
   Откроется редактор кода.
5. В открывшемся редакторе кода необходимо внести требуемые корректировки. Наименование ресурса автоматически изменится. Система добавит окончание **_copy** к названию ресурса.

> Внимание! Если в названии исходного правила присутствует слово **«copy»**, то при копировании название будет обрезано до этого слова.

Пример названия скопированного ресурса:
<Наименование ресурса>_copy
А также изменяются все соответствующие имена в самом коде (correlation name, директива rule, правила локализации).

6. Можно задать собственное имя, изменив его в поле **Системное название**. Система внесет эти изменения автоматически при нажатии на соответствующую подсказку: **Обновить системное название в тексте правила и правилах локализации**.

> Внимание! Если предварительно копировались макросы или табличные списки, необходимо вручную поменять все зависимости в копируемом ресурсе. Например, в правиле **<Наименование_правила>** используется табличный список **<Наименование_табличного_списка>** и макрос **<Наименование_макроса>**, в случае, если они были изменены (скопированы) и получили соответствующие новые имена, при необходимости использования их в правиле **<Наименование_правила>_copy**, необходимо поменять исходные имена на новые в коде данного правила. При этом измененный ресурс может иметь зависимости на стандартные ресурсы без каких-либо ограничений.

7. Нажмите кнопку **Сохранить**.
После сохранения изменений, новый ресурс появляется в самом низу иерархии, вне пакетов экспертизы, как показано на рисунке 16.1.

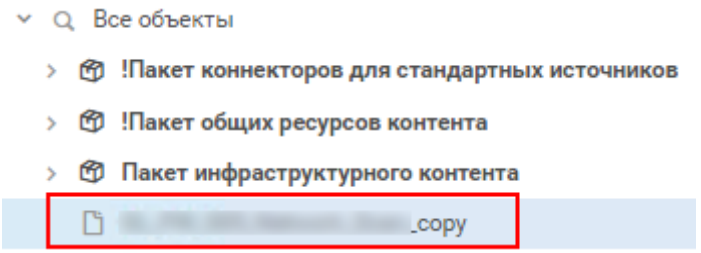

Рисунок 16.1 – Копия ресурса в панели **Папки**

8. Можно создать удобную иерархическую структуру из папок для пользовательских ресурсов. Для этого в панели **Папки** нажмите + и в раскрывшемся меню выберите пункт **Создать папку** (подробнее см. раздел 16.5.4).

После копирования изменится описание вновь созданного ресурса (см. рисунок 16.2):

- идентификатор LOC, вместо родительского GIS;
- тип − пользовательский, следовательно, ресурс доступен для дальнейшего редактирования, удаления и экспорта;
- поставщик − локальная система, вместо родительского Газинформсервис;
- дополнительное свойство **Основано на** сохраняет связь с родительским объектом в виде ссылки на него.

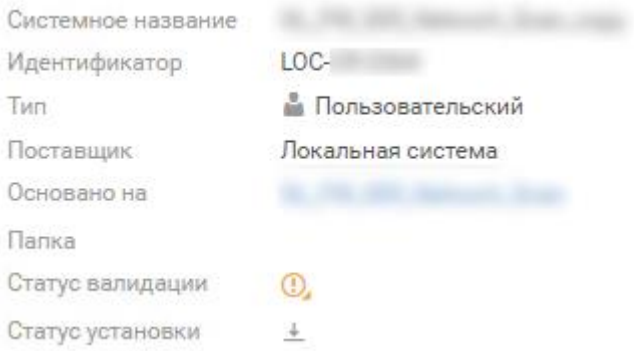

Рисунок 16.2 – Описание скопированного ресурса

16.4.2 Установка ресурсов из Knowledge Base в Server

После того, как все необходимые ресурсы в **Knowledge Base** были настроены, следует установить их в компонент **Server**. Те ресурсы, которые не были изменены, могут быть установлены в своем исходном виде, т.е. в том числе и стандартные ресурсы[2].

В ПК Ankey SIEM NG не следует одновременно устанавливать оригинальные ресурсы совместно с модифицированными. Для разделения ресурсов по признаку их востребованности используется функционал **Наборов для установки** (подробнее см. раздел 16.6).

❖ Чтобы корректно установить все необходимые ресурсы в компонент **Server** необходимо:

1. В главном меню в разделе **<Название базы данных>** выберите **Customer_Data**.
2. В главном меню в разделе **SIEM** выберите **Пакеты экспертизы**. Откроется страница **Пакеты экспертизы**.
3. В панели **Наборы для установки** нажмите +. Откроется окно **Создание набора для установки**.
4. В поле **Системное название** введите название набора. Рекомендуется указать системное название на латинице.
5. В поле **Название (русский)** возможно внести любое значение, оно будет отображаться в веб-интерфейсе. Например, «Ресурсы для конвейера в администрации».
6. В поле **Входит в набор** возможно выбрать **Все объекты** или любой другой корректно сформированный набор для установки.
7. В поле **Устанавливать в конвейер** выберите один или несколько конвейеров, в который будут установлены ресурсы из набора установки. Выбрать конвейеры для установки возможно только в том случае, если корректно выполнена установка всех основных компонентов Ankey SIEM NG.

[2] Тип ресурсов не влияет на их работу.

Примечание. Наборы установки для конвейеров следует формировать с учетом того, что при установке новых ресурсов из приложения Knowledge Base в компонент Server ресурсы, которые были установлены ранее автоматически и принудительно удаляются, а новые устанавливаются. Т.е. набор установки для конвейеров должен содержать все необходимые правила нормализации, правила корреляции, правила обогащения, правила агрегации и табличные списки.

8. Нажмите кнопку **Создать**.
   Набор для установки создан.
9. В панели **Наборы для установки** выберите **Все объекты**.
10. В панели **Папки** выберите пакет экспертизы (или папку). Появится список объектов пакета экспертизы (папки).

Примечание. Вы можете использовать фильтрацию, чтобы изменить список объектов

11. Выберите объекты.

Примечание. Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов − клавишу Ctrl. Чтобы выбрать все объекты, можно использовать комбинацию клавиш Ctrl+A.

12. Нажмите  .
    Откроется окно **Наборы для установки**.
13. Установите флажки напротив названий наборов для установки, в которые нужно добавить объекты.

Примечание. Место ресурса в иерархической структуре не поменяется, наборы для установки представляют собой группы, которые объединяет объекты по некоторому признаку.

14. Нажмите кнопку **Сохранить**.
    Объекты добавлены в набор для установки.
15. Из набора установки необходимо удалить все родительские ресурсы, с которых были созданы копии в ветке **Customer_Data** чтобы не было конфликтов в работе SIEM-системы после установки. Найти родительский ресурс, выделив скопированный, возможно, перейдя к нему по ссылке из описания скопированного ресурса.

Внимание! При любых изменениях в наборе для установки, его статус валидации меняется, даже если статус ресурсов внутри него остался прежним. Т.е. все ресурсы могут иметь статус успешной валидации, но при изменении состава набора, его статус валидации изменится.

16. Выполните валидацию, нажав **Валидация**.
    Откроется окно **Валидировать**.
17. Нажмите кнопку **Запустить валидацию**.

> Внимание! Ветка **Customer_Data** является установочной БД, ресурсы, расположенные в родительской **GIS_DB** доступны только для валидации и не устанавливаются в систему.

18. Выполните установку, нажав **Установить в SIEM**.
    Откроется окно **Установить в SIEM**.
19. В окне установки необходимо выбрать конвейер, в который будет выполнена установка всех требуемых ресурсов из актуального набора установки.
20. Нажмите кнопку **Запустить установку**.

Начнется установка объектов в ПК Ankey SIEM NG. По завершении установки в рабочей области появится соответствующее сообщение.

16.5 Работа с пакетами экспертизы

Пакет экспертизы представляет собой совокупность правил корреляции или других объектов, объединенных одной темой, например, предназначенных для выявления атак на некоторую систему или использующих определенную тактику.

Работать с пакетами экспертизы вы можете в разделе **SIEM → Пакеты экспертизы** в панели **Папки**. В Ankey SIEM NG Knowledge Base пакет экспертизы представляет собой папку в узле **<Все объекты>**, к которой могут быть добавлены описание и любые файлы, содержащие информацию о пакете или используемые при его настройке. Пакет экспертизы может содержать вложенную структуру папок для удобства хранения и систематизации объектов.

Пакеты экспертизы бывают стандартными и пользовательскими. Стандартные пакеты экспертизы разработаны специалистами по информационной безопасности ООО «Газинформсервис» и не могут быть изменены. Вы можете копировать объекты из стандартных пакетов. Также вы можете создавать, изменять и удалять пользовательские пакеты экспертизы и объекты.

16.5.1 Создание пакета экспертизы

❖ Чтобы создать пакет экспертизы:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** нажмите + и в раскрывшемся меню выберите пункт **Создать пакет экспертизы**.
   Откроется окно **Новый пакет экспертизы**.
4. В поле **Название (русский)** введите название.

5. Если в пакет нужно добавить файл, перетащите его в область **Вложения** или по ссылке **выберите** укажите расположение файла.
   Размер файла не должен превышать 100 МБ.
6. Если нужно изменить название добавленного файла, в строке с названием нажмите , измените название и нажмите .

Примечание. Вы можете удалить добавленный файл, нажав в строке с его названием.

7. Если нужно, в панели **Описание пакета (русский)** добавьте описание.

Примечание. При описании пакета вы можете использовать язык разметки Markdown.

8. Нажмите кнопку **Создать**.

Пакет экспертизы создан.

После создания пакета экспертизы вы можете создать структуру папок для хранения объектов пакета.

16.5.2 Изменение пакета экспертизы

❖ Чтобы изменить пакет экспертизы:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите пакет экспертизы.
3. В строке с названием папки нажмите и в раскрывшемся меню выберите пункт **Редактировать**.
   Откроется страница **Редактирование пакета экспертизы <Название пакета>**.
4. Если нужно, измените название и описание пакета, добавьте или удалите файлы, измените их названия.
5. Нажмите кнопку **Сохранить**.

Пакет экспертизы изменен.

16.5.3 Удаление пакета экспертизы

Вы можете удалить пакет экспертизы, если ни один из входящих в него объектов не установлен в ПК Ankey SIEM NG.

❖ Чтобы удалить пакет экспертизы:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите пакет экспертизы.
3. В строке с названием пакета экспертизы нажмите , в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Пакет экспертизы удален.

16.5.4 Создание папки

Вы можете создавать папки в узле **<Все объекты>** в пакете экспертизы или в другой папке.

❖ Чтобы создать папку:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** нажмите + и в раскрывшемся меню выберите пункт **Создать папку**.
   Откроется окно **Новая папка**.
4. В поле **Название** введите название папки.
5. Если нужно создать вложенную папку в пакете экспертизы или в другой папке, в раскрывающемся списке **Расположение** выберите куда поместить папку.
6. Нажмите кнопку **Создать**.

Папка создана.

16.5.5 Изменение папки

❖ Чтобы изменить папку:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите папку.
3. В строке с названием папки нажмите ⋮ и в раскрывшемся меню выберите пункт **Редактировать**.
   Откроется окно **Редактирование папки**.
4. Если требуется изменить название папки, в поле **Название** измените его.
5. Если требуется перенести папку, в раскрывающемся списке **Расположение** выберите папку.
6. Нажмите кнопку **Сохранить**.

Папка изменена.

16.5.6 Удаление папки

Вы можете удалить папку, если ни один из расположенных в ней объектов не установлен в ПК Ankey SIEM NG.

❖ Чтобы удалить папку:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите папку.
3. В строке с названием папки нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Папка удалена.

16.5.7 Фильтрация объектов

Вы можете фильтровать объекты по типу, источнику (стандартные или

пользовательские), статусу установки в Ankey SIEM NG или статусу валидации. Также вы можете фильтровать правила, применяя регулярные выражения к коду правил.

Примечание. Для поиска объекта по его названию, идентификатору или описанию вы можете использовать поле быстрого поиска.

❖ Чтобы отфильтровать объекты:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите **Все объекты**.
3. В панели **Наборы для установки** выберите **Все объекты**.
4. В панели со списком объектов нажмите .
   Появится строка с названиями фильтров.
5. По ссылке с названием нужного фильтра откройте окно с его параметрами.
6. Настройте параметры фильтра и повторно нажмите на ссылку.

Примечание. Вы можете очистить параметры фильтра, нажав справа от названия фильтра. Вы можете очистить параметры всех фильтров, нажав в строке с названиями фильтров.

Объекты в списке отфильтрованы в соответствии с условием.

16.5.8 Перемещение объектов

Вы можете перемещать пользовательские объекты между пользовательскими папками или пакетами экспертизы.

❖ Чтобы переместить объекты:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.

   Примечание. Вы можете использовать фильтрацию, чтобы сформировать список объектов.

2. Выберите объекты.

   Примечание. Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов − клавишу Ctrl. Чтобы выбрать все объекты, можно использовать комбинацию клавиш Ctrl+A.

3. Нажмите .
4. Откроется окно **Перемещение объектов в папку**.
5. В раскрывающемся списке **Расположение** выберите папку или пакет экспертизы.
6. Нажмите кнопку **Переместить**.

Объекты перемещены.

16.5.9 Удаление объектов

Вы можете удалять пользовательские объекты, не установленные в Ankey SIEM NG.

❖ Чтобы удалить объекты:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.

   Примечание. Вы можете использовать фильтрацию, чтобы сформировать список объектов.

2. Выберите объекты.

   Примечание. Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов − клавишу Ctrl. Чтобы выбрать все объекты, можно использовать комбинацию клавиш Ctrl+A.

3. Нажмите и подтвердите удаление объектов.

Объекты удалены.

16.5.10 Экспорт объектов

Вы можете экспортировать объекты в файл с расширением .kb для последующего импорта в Knowledge Base, а также в ZIP-архив − для добавления объектов в «SIEM на агенте».

В файл архива экспортируются правила нормализации, агрегации, обогащения и корреляции, схема полей событий, макросы (без меток) и табличные списки с записями и шаблонами исключений. При экспорте в файл с расширением .kb также экспортируются метки макросов и описания пакетов экспертизы.

❖ Чтобы экспортировать объекты:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. Выберите вариант экспорта:
   - если нужно экспортировать все объекты Knowledge Base − нажмите ;
   - если один или несколько объектов − выберите их в таблице и нажмите ;
   - если нужно экспортировать все объекты набора для установки − в строке с названием набора нажмите и в раскрывшемся меню выберите пункт **Экспортировать**.

   Откроется окно **Экспорт объектов**.
3. Выберите формат экспорта.
4. Нажмите кнопку **Экспортировать**.
   Браузер сохранит объекты в файле knowledgebase_<Дата экспорта>.kb или knowledgebase_<Дата экспорта>.zip в папке загрузки.

Объекты экспортированы.

16.5.11 Импорт объектов

Вы можете импортировать объекты только из файла с расширением .kb и только в пользовательскую БД. Схема полей событий не импортируется.

Если в файле с объектами только стандартные объекты, разработанные GIS, все объекты импортируются в БД как пользовательские. Уже существующие в БД стандартные объекты заменяются объектами из файла (в том числе − записи табличных списков), новые объекты добавляются в БД.

Если в файле есть пользовательские объекты или объекты, разработанные другими поставщиками, доступны следующие режимы импорта:

- **Добавить и обновить объекты из файла** − все объекты импортируются в БД как пользовательские. Новые объекты добавляются в БД, уже существующие в БД пользовательские объекты заменяются объектами из файла (в том числе − записи табличных списков);
- **Добавить объекты <Поставщик> как стандартные** − импортируются только объекты, разработанные сторонними поставщиками. Все объекты импортируются в БД как стандартные. Новые объекты добавляются в БД, уже существующие в БД объекты этого поставщика заменяются объектами из файла;
- **Синхронизировать объекты <Поставщик> с содержимым файла** − импортируются только объекты, разработанные сторонними поставщиками. Все объекты импортируются в БД как стандартные. Если в БД и в файле есть объекты, разработанные одним и тем же поставщиком, все такие объекты заменяются в БД объектами из файла. Таким образом, новые объекты добавляются в БД, уже существующие в БД объекты заменяются объектами из файла, отсутствующие в файле объекты удаляются из БД.

❖ Чтобы импортировать объекты:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели инструментов нажмите кнопку **Импорт**.
   Откроется окно **Импорт объектов**.
3. По ссылке **выберите** укажите расположение файла с объектами.
4. Если требуется, выберите режим импорта.
5. Если требуется, установите флажок **Импортировать макросы**.
6. Нажмите кнопку **Импортировать**.

Объекты импортированы.

16.5.12 Выбор версии SDK для валидации

Для валидации объектов нужно выбрать версию SDK. В SDK входят утилиты для отладки правил нормализации, агрегации, обогащения и корреляции. Вы можете выбрать разные версии SDK для валидации разных пользовательских БД. Версии SDK объектов в стандартной БД, пользовательских БД и установленных в Ankey SIEM NG могут отличаться. Для

исключения ошибок совместимости версия SDK для валидации не должна быть выше версии SDK, используемой в Ankey SIEM NG. Выбрать версию SDK для валидации вы можете на странице **Настройка инструментария для разработки правил SIEM**.

❖ Чтобы выбрать версию SDK для валидации:

1. В главном меню в разделе **SIEM** выберите пункт **Выбор версии SDK**.
   Откроется страница **Настройка инструментария для разработки правил SIEM**.
2. В центральной панели выберите версию SDK.
3. В панели инструментов нажмите кнопку **Установить SDK для валидации**.
   Откроется окно **Обновление SDK**.
4. Нажмите кнопку **Обновить**.

Версия SDK выбрана.

16.5.13 Валидация объектов

Перед установкой объектов вы можете выполнить валидацию одного или нескольких объектов, а также валидацию всех объектов из набора для установки. При валидации отдельных объектов выполняется проверка структуры объекта, его синтаксиса и однозначности указанных условий. При валидации набора дополнительно проверяются согласованность объектов и непротиворечивость указанных в них условий. Например, если правило корреляции, включенное в набор, использует табличный список, он также должен быть включен в этот набор.

❖ Чтобы выполнить валидацию объектов:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Наборы для установки** выберите набор.
3. Выберите вариант валидации:
   - если нужно выполнить валидацию всех объектов из набора – в строке с названием набора нажмите ⋮ и в раскрывшемся меню выберите пункт **Валидировать**;
   - если одного или нескольких объектов – выберите их в таблице и нажмите ☑.

   Откроется окно **Валидировать**.
4. Нажмите кнопку **Запустить валидацию**.

По завершении валидации в рабочей области появится сообщение.

16.6 Работа с наборами для установки

Для удобства работы с объектами, быстрой валидации и установки объектов в ПК Ankey SIEM NG вы можете группировать объекты в наборы для установки. В набор могут входить любые стандартные и пользовательские объекты из разных пакетов экспертизы и папок. Один и тот же объект может входить одновременно в несколько наборов для установки. Наборы для установки можно использовать, например, если в ПК Ankey SIEM NG нужно установить объекты из одного или нескольких пакетов экспертизы, а не все

объекты БД.

Работать с наборами для установки вы можете в разделе **SIEM** → **Пакеты экспертизы** в панели **Наборы для установки**. Вы можете создавать, изменять и удалять наборы для установки.

16.6.1 Создание набора для установки

❖ Чтобы создать набор для установки:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Наборы для установки** нажмите +.
   Откроется окно **Новый набор для установки**.
4. В поле **Системное название** введите название набора.
5. Если набор нужно добавить в другой пользовательский набор, в раскрывающемся списке **Входит в набор** выберите этот пользовательский набор.

> **Примечание.** Создаваемый набор должен входить в тот или иной уже созданный набор. По умолчанию все создаваемые наборы входят в стандартный набор **Все наборы**.

6. Если в главном меню выбрана установочная БД, в раскрывающемся списке **Устанавливать в конвейер** выберите конвейеры, в которые будут устанавливаться объекты набора.
7. Нажмите кнопку **Создать**.

Набор для установки создан.

16.6.2 Создание набора на основе существующего

❖ Чтобы создать набор на основе существующего:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Наборы для установки** выберите набор.
3. В строке с названием набора нажмите ⋮ и в раскрывшемся меню выберите пункт **Создать копию**.
   Откроется окно **Создать копию**.
4. Если необходимо изменить название набора, в поле **Системное название** введите название.
5. Если набор нужно добавить в другой пользовательский набор, в раскрывающемся списке **Входит в набор** выберите этот пользовательский набор.

> **Примечание.** Создаваемый набор должен входить в тот или иной уже созданный набор. По умолчанию все создаваемые наборы входят в стандартный набор **Все наборы**.

6. Если в главном меню выбрана установочная БД, в раскрывающемся списке **Устанавливать в конвейер** выберите конвейеры, в которые будут устанавливаться объекты набора.
7. Нажмите кнопку **Создать**.

Набор создан.

16.6.3 Изменение набора для установки

❖ Чтобы изменить набор для установки:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Наборы для установки** выберите набор.
3. В строке с названием набора нажмите ⋮ и в раскрывшемся меню выберите пункт **Редактировать**.
   Откроется окно **Редактирование набора для установки**.
4. Внесите изменения.
5. Нажмите кнопку **Сохранить**.

Набор для установки изменен.

16.6.4 Удаление набора для установки

❖ Чтобы удалить набор для установки:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Наборы для установки** выберите набор.
3. В строке с названием набора нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Набор для установки удален.

16.6.5 Добавление объектов в набор для установки

❖ Чтобы добавить объекты в набор для установки:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Наборы для установки** выберите **Все объекты**.
3. В панели **Папки** выберите пакет экспертизы (или папку).
   Появится список объектов пакета экспертизы (папки).

> **Примечание.** Вы можете использовать фильтрацию, чтобы изменить список объектов

4. Выберите объекты.

> **Примечание.** Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов − клавишу Ctrl. Чтобы выбрать все объекты, можно использовать комбинацию клавиш Ctrl+A.

5. Нажмите .

Откроется окно **Наборы для установки**.

6. Установите флажки напротив названий наборов для установки, в которые нужно добавить объекты.
7. Нажмите кнопку **Сохранить**.

Объекты добавлены в набор для установки.

16.6.6 Удаление объектов из набора для установки

❖ Чтобы удалить объекты из набора для установки:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите **Все объекты**.
3. В панели **Наборы для установки** выберите набор для установки.
   Появится список объектов, входящих в набор для установки.

> **Примечание.** Вы можете использовать фильтрацию, чтобы изменить список объектов.

4. Выберите объекты в списке.

> **Примечание.** Для выбора нескольких объектов подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных объектов − клавишу Ctrl.

5. Нажмите  .
   Откроется окно **Наборы для установки**.
6. Снимите флажки напротив названий наборов для установки, из которых нужно удалить объекты.
7. Нажмите кнопку **Сохранить**.

Объекты удалены из набора для установки.

16.7 Установка объектов в конвейеры обработки событий

Чтобы использовать для обработки событий правила и табличные списки, созданные в Knowledge Base, их необходимо установить в конвейеры обработки событий. Записи об установке сохраняются в журнале на странице.

16.7.1 Установка объектов

❖ Чтобы установить объекты:

1. В главном меню в разделе **<Название БД>** выберите пункт с установочной БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Наборы для установки** выберите набор.
4. Нажмите кнопку **Установить в SIEM**.
   Откроется окно **Установка в SIEM**.

5. Если не нужно устанавливать объекты в некоторые конвейеры, снимите флажки с названиями этих конвейеров.
6. Нажмите кнопку **Запустить установку**.
   Начнется установка объектов.

Примечание. При наведении курсора на кнопку **Установить в SIEM** во всплывающей подсказке отображается ход установки.

По завершении установки в рабочей области появится сообщение «Установка успешно завершена». Объекты установлены.

16.7.2 Просмотр записей журнала установки

❖ Чтобы просмотреть записи журнала установки:

1. В главном меню в разделе **SIEM** выберите пункт **Журнал установки**.
   Откроется страница **Журнал установки**.
2. Если необходимо, отфильтруйте записи по статусу, по конвейеру или по дате.
3. Выберите запись.

В рабочей области отобразится информация об установке объектов.

16.8 Настройка нормализации событий

Нормализация событий от источников для последующей обработки и анализа выполняется по созданным заранее правилам. Специальные правила создаются для каждого источника и типа события.

Правила нормализации бывают стандартными и пользовательскими. Стандартные правила нормализации разработаны специалистами по информационной безопасности ООО «Газинформсервис» и не могут быть изменены. Вы можете копировать стандартные правила нормализации для создания пользовательских правил. Пользовательские правила нормализации вы можете создавать, изменять, копировать и удалять.

Правило нормализации имеет следующие параметры:

- системное название − может состоять из букв латинского алфавита, цифр и знака подчеркивания, должно начинаться с прописной буквы или цифры;
- папка − папка или пакет экспертизы для хранения правила в БД;
- набор для установки − набор объектов, в составе которого правило будет устанавливаться в ПК Ankey SIEM NG (правило может быть добавлено одновременно в несколько наборов);
- может иметь описание на русском или английском языке;
- правило локализации − правило, согласно которому с событиями, нормализованными по правилу нормализации, в веб-интерфейсе ПК Ankey SIEM NG связывается определенное описание на русском или английском языке.

16.8.1 Создание правила нормализации

❖ Чтобы создать правило нормализации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Правило нормализации**.
   Откроется страница **Новое правило нормализации**.
4. Введите код правила.
5. В поле **Системное название** введите системное название правила.
6. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения правила в БД.

> **Примечание.** Вы можете добавить правило в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**, а также ввести любой текстовый комментарий в поле **Описание (русский)**.

7. Если нужно, по кнопке **Добавить** создайте правила локализации.
8. Нажмите кнопку **Сохранить**.

Правило нормализации создано.

16.8.2 Копирование правила нормализации

❖ Чтобы скопировать правило нормализации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Новое правило нормализации (на основе <Название оригинального правила>)**.
5. Если нужно, измените параметры правила.
6. Нажмите кнопку **Сохранить**.

Правило нормализации скопировано.

16.8.3 Изменение правила нормализации

❖ Чтобы изменить пользовательское правило нормализации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.

2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

Примечание. Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование правила нормализации: <Название правила>**.
5. Измените код правила.
6. Если нужно, измените параметры правила.
7. Нажмите кнопку **Сохранить**.

Правило нормализации изменено.

16.9 Настройка агрегации событий

Агрегация событий для объединения однотипных нормализованных или корреляционных событий в одно агрегированное событие выполняется по созданным заранее правилам.

Правила агрегации бывают стандартными и пользовательскими. Стандартные правила агрегации разработаны специалистами по информационной безопасности ООО «Газинформсервис» и не могут быть изменены. Вы можете просматривать стандартные правила агрегации и копировать их для создания пользовательских правил. Пользовательские правила агрегации вы можете создавать, изменять, копировать и удалять.

Правило агрегации имеет следующие параметры:

- системное название − должно совпадать с названием, указанным в коде правила в директиве aggregate, и будет совпадать с названием файла правила (может состоять из букв латинского алфавита, цифр, знаков подчеркивания и точки, должно начинаться с прописной буквы);
- папка − папка или пакет экспертизы для хранения правила в БД;
- набор для установки − набор объектов, в составе которого правило будет устанавливаться в ПК Ankey SIEM NG (правило может быть добавлено одновременно в несколько наборов);
- может иметь описание на русском или английском языке;
- правило локализации − правило, согласно которому с событиями, агрегированными по правилу, в веб-интерфейсе ПК Ankey SIEM NG связывается определенное описание на русском или английском языке.

16.9.1 Создание правила агрегации

❖ Чтобы создать новое правило агрегации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.

2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Правило агрегации**.
   Откроется страница **Новое правило агрегации**.
4. Введите код правила.
5. В поле **Системное название** введите системное название правила.
6. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения правила в БД.

> **Примечание.** Вы можете добавить правило в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**, а также ввести любой текстовый комментарий в поле **Описание (русский)**.

7. Если нужно, по кнопке **Добавить** создайте правила локализации.
8. Нажмите кнопку **Сохранить**.

Правило агрегации создано.

16.9.2 Копирование правила агрегации

❖ Чтобы скопировать правило агрегации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите  .
   Откроется страница **Новое правило агрегации (на основе <Название оригинального правила>)**.
5. Если нужно, измените параметры правила.
6. Нажмите кнопку **Сохранить**.

Правило агрегации скопировано.

16.9.3 Изменение правила агрегации

❖ Чтобы изменить пользовательское правило агрегации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

Примечание. Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование правила агрегации**: **<Название правила>**.
5. Измените код правила.
6. Если нужно, измените параметры правила.
7. Нажмите кнопку **Сохранить**.

Правило агрегации изменено.

16.10 Настройка обогащения событий

Обогащение событий выполняется по созданным заранее правилам. При обогащении поля нормализованных, агрегированных и корреляционных событий заполняются данными, указанными в правиле обогащения или полученными из табличных списков.

Правила обогащения бывают стандартными и пользовательскими. Стандартные правила обогащения разработаны специалистами по информационной безопасности ООО «Газинформсервис» и не могут быть изменены. Вы можете просматривать стандартные правила обогащения и копировать их для создания пользовательских правил. Пользовательские правила вы можете создавать, изменять, копировать и удалять. Правило обогащения имеет следующие параметры:

- системное название − должно совпадать с названием, указанным в коде правила в директиве enrichment, и будет совпадать с названием файла правила (может состоять из букв латинского алфавита, цифр, знаков подчеркивания и точки, должно начинаться с прописной буквы);
- папка − папка или пакет экспертизы для хранения правила в БД;
- набор для установки − набор объектов, в составе которого правило будет устанавливаться в ПК Ankey SIEM NG (правило может быть добавлено одновременно в несколько наборов);
- может иметь описание на русском или английском языке.

16.10.1 Создание правила обогащения

❖ Чтобы создать правило обогащения:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Правило обогащения**.
   Откроется страница **Новое правило обогащения**.
4. Введите код правила.

5. В поле **Системное название** введите системное название правила.
6. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения правила в БД.

> **Примечание.** Вы можете добавить правило в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**, а также ввести любой текстовый комментарий в поле **Описание (русский)**.

7. Нажмите кнопку **Сохранить**.

Правило обогащения создано.

16.10.2 Копирование правила обогащения

❖ Чтобы скопировать правило обогащения:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите  .
   Откроется страница **Новое правило обогащения (на основе <Название оригинального правила>)**.
5. Если нужно, измените параметры правила.
6. Нажмите кнопку **Сохранить**.

Правило обогащения скопировано.

16.10.3 Изменение правила обогащения

❖ Чтобы изменить пользовательское правило обогащения:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите  .
   Откроется страница **Редактирование правила обогащения: <Название правила>**.
5. Измените код правила.

6. Если нужно, измените параметры правила.
7. Нажмите кнопку **Сохранить**.

Правило обогащения изменено.

16.11 Настройка корреляции событий

Корреляция событий выполняется по созданным заранее правилам. В условии правила корреляции указывается последовательность событий, которая является признаком события информационной безопасности. При обнаружении в потоке событий такой последовательности регистрируется корреляционное событие.

Правила корреляции бывают стандартными и пользовательскими. Стандартные правила корреляции разработаны специалистами по информационной безопасности ООО «Газинформсервис» и не могут быть изменены. Вы можете просматривать стандартные правила корреляции и копировать их для создания пользовательских правил. Пользовательские правила корреляции вы можете создавать, изменять, копировать и удалять.

Правило корреляции имеет следующие параметры:

- системное название − должно совпадать с названием, указанным в коде правила в директиве rule, и будет совпадать с названием файла правила (может состоять из букв латинского алфавита, цифр, знаков подчеркивания и точки, должно начинаться с прописной буквы);
- папка − папка или пакет экспертизы для хранения правила в БД;
- набор для установки − набор объектов, в составе которого правило будет устанавливаться в ПК Ankey SIEM NG (правило может быть добавлено одновременно в несколько наборов);
- может иметь описание на русском или английском языке;
- правило локализации − правило, согласно которому с корреляционными событиями, зарегистрированными по правилу, в веб-интерфейсе ПК Ankey SIEM NG связывается определенное описание на русском или английском языке.

16.11.1 Создание правила корреляции

❖ Чтобы создать правило корреляции:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Правило корреляции**.
   Откроется страница **Новое правило корреляции**.
4. Настройте параметры правила корреляции.
5. Настройте условие корреляции.
6. Если нужно, настройте корреляционное событие.
7. Если нужно, настройте дополнительные действия.

Примечание. По кнопке **Предварительный просмотр** вы можете посмотреть код получившегося правила корреляции.

8. Нажмите кнопку **Создать**.

Начнется процесс валидации. По завершении валидации будет создано новое правило корреляции.

16.11.1.1 Настройка параметров правила корреляции

❖ Чтобы при создании правила корреляции настроить его параметры:

1. В левой части окна выберите **Параметры правила корреляции**.
2. В поле **Название** введите название правила.

Примечание. В поле **Описание** вы можете добавить любой текстовый комментарий на русском и английском языках.

3. Если по правилу корреляции регистрируется инцидент, выберите тип корреляционного события − **incident**.
4. Если нужно, измените важность корреляционного события.
5. Если нужно, выберите другую папку или пакет экспертизы для хранения правила в раскрывающемся списке **Папка**.

Примечание. Вы можете указать набор для установки, в которые нужно добавить правило, установив флажки в раскрывающемся списке **Наборы для установки**.

6. Если нужно, в панели **Категоризация** с помощью раскрывающихся списков **category.generic**, **category.high**, **category.low** укажите категории корреляционного события.
   Вы можете выбирать рекомендованные значения из списков или вводить произвольные значения.

После настройки параметров правила нужно настроить условие корреляции.

16.11.1.2 Настройка условия корреляции

При создании правила корреляции вам нужно настроить условие, при выполнении которого по правилу корреляции будет регистрироваться корреляционное событие. Условие корреляции состоит из последовательности событий и интервала времени, за который эти события должны быть получены ПК Ankey SIEM NG. Для составления последовательности событий нужно указать типы событий (**A**, **B**, **C**…), из которых она состоит, и порядок поступления их в ПК Ankey SIEM NG. Тип события определяется условием отбора событий среди из всех событий, поступающих в ПК Ankey SIEM NG, и требованием о появлении этого события в последовательности.

❖ Чтобы при создании правила корреляции настроить условие корреляции:

1. В левой части страницы выберите **Условие корреляции**.
2. В поле справа от заголовка типа события введите название события.

3. В раскрывающемся списке выберите требование о появлении этого типа событий в последовательности:
   - если события не должны появляться в последовательности – **Не должно произойти**;
   - если события должны появиться в последовательности – **Должно произойти** (в поле справа от списка введите число появлений событий подряд).
   - если события должно появиться в последовательности определенное число раз, но с разными значениями указанного поля – **Должно произойти с разными значениями полей** (в поле справа от списка введите число появлений событий подряд, в раскрывающемся списке выберите поля, значения которых должны различаться в событиях).
4. Настройте условие отбора для типа событий (см. ниже).
   Условие отбора события может состоять из нескольких условий, объединенных логическими операторами И, ИЛИ.

Примечание. Вы можете удалить условие (или блок условий), нажав справа от него ⋮ и выбрав в раскрывшемся меню пункт **Удалить**.

5. Если нужно, добавьте события других типов по ссылке **Добавить событие**.
6. Если нужно изменить время регистрации последовательности событий, измените его по ссылке в блоке параметров **Условие корреляции**.
7. Если нужно изменить требование к типам событий последовательности (если в последовательности указаны несколько типов событий), выберите нужное требование в списке, раскрывающемся по ссылке.

Примечание. Вы можете менять порядок событий разных типов в последовательности, нажав справа от заголовка события ⋮ и выбрав в раскрывшемся меню пункт **Переместить вверх** или **Переместить вниз**.

8. В блоке параметров **Условия объединения событий** для всех добавленных типов событий в раскрывающихся списках выберите поля, по значениям которых события будут объединяться в группы.
   События с одинаковыми значениями указанных при сопоставлении полей объединяются в группы, внутри которых составляются последовательности событий условия корреляции.
9. Если нужно, добавьте сопоставление полей событий по кнопке **Добавить**.

Настройка условия отбора событий с помощью макроса

❖ Чтобы использовать готовое условие отбора событий из макроса:

1. Добавьте блок параметров для настройки условия отбора:
   - если нужно добавить условие с логическим оператором И, по ссылке **Добавить условие для события** в раскрывающемся списке выберите **Макрос**;
   - если нужно добавить первое условие или условие с логическим оператором ИЛИ, нажмите кнопку **Добавить блок условий для события** и в раскрывшемся списке выберите **Макрос**.
2. В появившемся поле нажмите ⌄.
3. В открывшемся окне в левой колонке выберите метку или группу меток макросов.
   В центральной колонке появятся макросы, для которых установлена выбранная метка или одна из меток в выбранной группе.
4. В центральной колонке выберите макрос.
5. Нажмите кнопку **Выбрать**.

Настройка запроса в табличный список

❖ Чтобы использовать в условии отбора событий запрос в табличный список:

1. Добавьте блок параметров для настройки условия отбора:
   - если нужно добавить условие с логическим оператором И, по ссылке **Добавить условие для события** в раскрывающемся списке выберите **Запрос в табличный список**;
   - если нужно добавить первое условие или условие с логическим оператором ИЛИ, нажмите кнопку **Добавить блок условий для события** и в раскрывшемся списке выберите **Запрос в табличный список**.
2. В раскрывающемся списке выберите табличный список.
3. По ссылке выберите в раскрывающемся списке требование к условиям запроса.
4. В раскрывающемся списке **Колонка табличного списка** выберите название колонки.
5. В появившемся раскрывающемся списке выберите логический оператор.
6. Укажите источник значения для сравнения со значением в колонке:
   - если нужно указать значение для сравнения, введите его в поле, появляющееся по ссылке **Значение**;
   - если нужно сравнить с значением поля полученного события, выберите это поле в раскрывающемся списке, появляющемуся по ссылке **Значение из поля**.
7. Если нужно указать условие для другой колонки, в раскрывающемся списке **Колонка табличного списка** выберите эту колонку.

Настройка условия из сравнения полей

❖ Чтобы настроить условие отбора из полей полученного события:

1. Добавьте блок параметров для настройки условия отбора:
   - если нужно добавить условие с логическим оператором И, по ссылке **Добавить условие для события** в раскрывающемся списке выберите **Сравнение полей**;
   - если нужно добавить первое условие или условие с логическим оператором ИЛИ, нажмите кнопку **Добавить блок условий для события** и в раскрывшемся списке выберите **Сравнение полей**.
2. В раскрывающемся списке **Поле события** выберите поле события.

> **Примечание.** Вы можете настроить обработку значения поля события (изменить регистр, применить регулярное выражение) по кнопке ⚙.

3. В появившемся раскрывающемся списке выберите логический оператор.
4. Укажите источник значения для сравнения со значением в поле:
   - если нужно указать значение, введите его в поле, появляющемся по ссылке **Значение**;
   - если нужно сравнить значение с значением поля события, выберите это поле в раскрывающемся списке, появляющемся по ссылке **Значение из поля**.

Настройка условия из кода

❖ Чтобы настроить условие отбора событий, используя блок кода:

1. Добавьте блок параметров для настройки условия отбора:
   - если нужно добавить условие с логическим оператором И, по ссылке **Добавить условие для события** в раскрывающемся списке выберите **Блок кода**;
   - если нужно добавить первое условие или условие с логическим оператором ИЛИ, нажмите кнопку **Добавить блок условий для события** и в раскрывшемся списке выберите **Блок кода**.
2. В открывшееся поле введите блок кода условия.

16.11.1.3 Настройка корреляционного события

При создании правила корреляции вы можете настроить правила заполнения необязательных полей корреляционного события и правило локализации корреляционного события.

❖ Чтобы при создании правила корреляции настроить правила заполнения полей корреляционного события:

1. В левой части окна выберите **Корреляционное событие**.
2. В блоке параметров **Корреляционное событие** в раскрывающемся списке выберите поле корреляционного события.
3. Укажите источник значения для заполнения поля (см. ниже).

Примечание. Вы можете настроить правило заполнения поля корреляционного события в зависимости от типа поступившего события, нажав справа от поля ⋮ и выбрав в раскрывшемся меню пункт **Настроить в зависимости от события**.

4. Если нужно, настройте заполнение других полей корреляционного события.
5. В блоке параметров **Описание корреляционного события** в поле введите описание на русском языке.

В тексте описания события вы можете использовать значения полей корреляционного события, указав эти поля в фигурных скобках. Например, при использовании {event_src.host} в описании события будет указан IP-адрес источника события.

Примечание. Вы можете добавить описание корреляционного события на английском языке по ссылке **Добавить вариант на английском языке**.

Настройка ввода значения поля

❖ Чтобы ввести значение поля корреляционного события:

1. По ссылке **Значение** откройте поле для ввода.
2. Введите значение поля.

Настройка заполнения поля данными из полученного события

❖ Чтобы заполнить поле корреляционного события данными из полученного события:

1. По ссылке **Значение из поля** откройте блок параметров.
2. В центральном раскрывающемся списке выберите тип события, данными из которого будет заполняться поле.
3. В правом раскрывающемся списке выберите поле полученного события, данными из которого будет заполняться поле.

Примечание. Вы можете настроить обработку значения поля события (изменить регистр, применить регулярное выражение) по кнопке ⚙.

Настройка заполнения поля данными из табличного списка

Для получения данных из табличного списка нужно настроить запрос. Если для записи табличного списка условие выполняется, поле корреляционного события заполняется данными этой записи из указанной колонки.

❖ Чтобы заполнить поле корреляционного события данными из табличного списка:

1. По ссылке **Значение из табличного списка** откройте блок параметров.
2. В раскрывающемся списке выберите табличный список.
3. По ссылке выберите в раскрывающемся списке требование к условиям запроса.
4. В раскрывающемся списке **Колонка табличного списка** выберите название колонки.

5. В появившемся раскрывающемся списке выберите логический оператор.
6. Укажите источник значения для сравнения со значением в колонке:
   - если нужно указать значение для сравнения, введите его в поле, появляющееся по ссылке **Значение**;
   - если нужно сравнить с значением поля полученного события, выберите это поле в раскрывающемся списке, появляющемуся по ссылке **Значение из поля**.
7. В раскрывающемся списке **Колонка табличного списка** выберите название колонки, данными из которой будет заполнено поле корреляционного события.

16.11.1.4 Настройка дополнительных действий

При создании правила корреляции вы можете настроить добавление записей в табличный список, удаление записей или очистку табличного списка при выполнении условия корреляции; выполнение блока кода при получении событий какого-либо типа или при выполнении условия корреляции.

Добавить запись в табличный список при выполнении условия корреляции

❖ Чтобы настроить запись в табличный список при выполнении условия корреляции:

1. В левой части окна выберите **Дополнительные действия**.
2. В блоке параметров **Действия при регистрации корреляционного события** нажмите кнопку **Добавить** и в раскрывшемся списке выберите **Вставка записи в табличный список**.
3. В раскрывающемся списке выберите табличный список.
4. Для каждой колонки укажите источник значения для вставки:
   - если нужно указать значение, введите его в поле, открывающееся по ссылке **Значение**;
   - если нужно вставить значение из поля события, выберите это поле в списке, раскрывающемся по ссылке **Значение из поля**.

Удалить записи из табличного списка при выполнении условия корреляции

❖ Чтобы настроить удаление записей, соответствующих указанному условию, из табличного списка при выполнении условия корреляции:

1. В левой части окна выберите **Дополнительные действия**.
2. В блоке параметров **Действия при регистрации корреляционного события** нажмите кнопку **Добавить** и в раскрывшемся списке выберите **Удаление записей из табличного списка**.
3. В раскрывающемся списке выберите табличный список.
4. Если требуется, измените требование к условиям в списке, раскрывающемся по ссылке **выполняется хотя бы одно из условий**.
5. В раскрывающемся списке **Колонка табличного списка** выберите колонку.

Очистить табличный список при выполнении условия корреляции

❖ Чтобы настроить удаление всех записей из табличного списка при выполнении условия корреляции:

1. В левой части окна выберите **Дополнительные действия**, нажмите кнопку **Добавить** и в раскрывшемся списке выберите **Очистка табличного списка**.
2. В раскрывающемся списке выберите табличный список.

Выполнить блок кода при получении одного из отобранных событий

❖ Чтобы настроить выполнение блока кода при получении одного из отобранных событий:

1. В левой части окна выберите **Дополнительные действия**.
2. В блоке параметров **Действия при появлении события <Название события>** нажмите кнопку **Добавить**.
3. В открывшееся поле введите блок кода.

Выполнить блок кода при выполнении условия корреляции

❖ Чтобы настроить выполнение блока кода при выполнении условия корреляции:

1. В левой части окна выберите **Дополнительные действия** нажмите кнопку **Добавить** и в раскрывшемся списке выберите **Блок кода**.
2. В открывшееся поле введите блок кода.

16.11.2 Создание правила корреляции в редакторе кода

❖ Чтобы создать правило корреляции:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите **Правило корреляции (в редакторе кода)**.
   Откроется страница **Новое правило корреляции**.
4. Введите код правила.
5. В поле **Системное название** введите системное название правила.
6. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения правила в БД.

> **Примечание.** Вы можете добавить правило в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**, а также ввести любой текстовый комментарий в поле **Описание (русский)**.

7. Если нужно, по кнопке **Добавить** создайте правила локализации.
8. Нажмите кнопку **Сохранить**.

Правило корреляции создано.

16.11.3 Копирование правила корреляции

❖ Чтобы скопировать правило нормализации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Новое правило нормализации (на основе <Название оригинального правила>)**.
5. Если нужно, измените параметры правила.
6. Нажмите кнопку **Сохранить**.

Правило нормализации скопировано.

16.11.4 Изменение правила корреляции

❖ Чтобы изменить пользовательское правило нормализации:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

> **Примечание.** Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование правила нормализации: <Название правила>**.
5. Измените код правила.
6. Если нужно, измените параметры правила.
7. Нажмите кнопку **Сохранить**.

Правило нормализации изменено.

16.12 Настройка правил локализации

При регистрации нормализованного, агрегированного или корреляционного события в веб-интерфейсе ПК Ankey SIEM NG с ним может быть связано описание на русском или английском языке (в зависимости от языка интерфейса). Сопоставление описаний с регистрируемыми событиями выполняется согласно заранее созданным правилам локализации. Для

нормализованного события правила локализации создаются для правила нормализации, по которой выполняется нормализация этого события, для агрегированного или корреляционного события − для правила агрегации или корреляции, по которому регистрируется событие.

Для одного события может быть создано несколько правил локализации, в зависимости от указанного критерия. Например, вы можете создать, одно правило локализации для события выхода из системы и два правила локализации для события входа в систему, указав в качестве критерия результат входа − успешный или неуспешный.

Правило локализации должно содержать:

- критерий − условие, по которому регистрируемому событию ставится в соответствие определенное описание. Условие может состоять из одного или нескольких предикатов вида: <Поле события><Оператор><Значение> или <Поле 1 события><Оператор><Поле 2 события>. В предикате вы можете использовать логические операторы равенства (=) и неравенства (!=). Между предикатами можно использовать операторы and или or. В условии можно использовать круглые скобки;

  Примечание. В условии вы также можете использовать предикаты вида: <Поле события> и not <Поле события> (альтернативная запись !<Поле события>). Значение первого предиката будет true, если значение поля события отличается от null, второго − если значение равно null или false.

  Пример: id = "PT_Kaspersky_Security_Center_odbc_KLPRCI_TaskState" and reason != null

- значение − описание события на английском или русском языке. В тексте описания события вы можете использовать значения полей события, указав эти поля в фигурных скобках. Например, при использовании {event_src.host} в описании события будет указан IP-адрес источника события.

16.12.1 Создание правила локализации

Вы можете создавать правила локализации для пользовательских правил нормализации, агрегации и корреляции.

❖ Чтобы создать правило локализации для пользовательского правила:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

Примечание. Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование правила <Назначение правила>: <Название правила>**.
5. Нажмите кнопку **Добавить**.
   Откроется блок параметров нового правила локализации.
6. В поле **Критерии** введите условие применения правила локализации.
7. В полях **Значение** введите описание события на русском языке.

Примечание. Вы можете скопировать или удалить правило локализации, нажав справа от блока параметров правила и выбрав в раскрывшемся меню соответствующий пункт.

8. Если нужно, аналогичным образом добавьте другие правила локализации.
9. Нажмите кнопку **Сохранить**.

Правило локализации создано.

16.12.2 Изменение правила локализации

❖ Чтобы изменить правило локализации для пользовательского объекта:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите правило.
   Откроется страница правила.

Примечание. Для поиска правила вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование правила <Назначение правила>: <Название правила>**.
5. В блоке параметров **Правила локализации** измените параметры правила.
6. Нажмите кнопку **Сохранить**.

Правило локализации изменено.

16.13 Настройка справочников для обработки событий

Объекты-справочники предназначены для хранения информации, используемой при обработке и анализе данных в ПК Ankey SIEM NG. К объектам-справочникам относятся схема полей событий, табличные списки и макросы.

В одной базе данных в Ankey SIEM NG Knowledge Base могут храниться

не более 1024 табличных списков типа «справочник» и для данных об активах, не более 1024 табличных списков для правил обогащения и не более 1024 − для правил корреляции. Общее число индексируемых колонок в табличных списках каждой из этих групп (вместе с числом самих списков) не должно превышать 4096.

16.13.1 Настройка табличных списков типа «справочник»

Табличные списки типа «справочник» предназначены для хранения данных, используемых в правилах обогащения и корреляции (но не могут заполнятся из правил). Вы можете работать с табличными списками типа «справочник» на странице **Пакеты экспертизы**.

Табличные списки типа «справочник» могут быть стандартными и пользовательскими. Стандартные табличные списки настроены специалистами по информационной безопасности ООО «Газинформсервис» их параметры не могут быть изменены. Вы можете просматривать стандартные табличные списки и копировать их для создания пользовательских списков. Пользовательские табличные списки вы можете создавать, изменять, копировать и удалять. Вы можете вручную добавлять и изменять записи в стандартных и пользовательских табличных списках, если это предусмотрено при их создании.

Параметры табличного списка

Табличный список типа «справочник» обладает следующими особенностями:

- предназначен для создания справочника;
- должен иметь название, которое может состоять из букв латинского алфавита, цифр, знаков подчеркивания и точек, должно начинаться с прописной буквы;
- может иметь описание на русском или английском языке;
- может иметь стандартный или пользовательский шаблон исключений для автоматического заполнения данными по ссылкам из корреляционных событий;
- может иметь разрешение на изменение записей пользователями;
- позволяет активировать и деактивировать записи (деактивированные записи не используются в правилах корреляции и обогащения);
- располагается в папке или пакете экспертизы для хранения в БД;
- может входить в наборы для установки объектов в ПК Ankey SIEM NG.

Параметры колонок табличного списка

Ключевая колонка − это колонка, значения в которой являются идентификаторами записей табличного списка. Если ключевых колонок несколько, то запись идентифицируется по совокупности значений всех ключевых колонок.

Колонки табличного списка обладают следующими особенностями:

- должны иметь название, которое может состоять из букв латинского алфавита, цифр, знака подчеркивания и точки, должно начинаться с прописной буквы;

– могут содержать данные типов DateTime, Number, String или Perl-совместимые регулярные выражения (PCRE);

> **Примечание.** Вы можете использовать колонки с типом данных String для хранения IPадресов в виде: a.b.c.d/<Маска>.

– могут быть ключевыми. Значения всех ключевых колонок индексируются и не могут быть пустыми (null). По умолчанию ключевой является первая колонка;
– могут индексироваться. Использование индексируемых колонок повышает скорость поиска по записям табличного списка. По умолчанию для индексирования используется первая ключевая колонка;
– могут явно допускать значение null. В табличный список может добавляться запись, в которой какое-то из полей отсутствует. Если соответствующая колонка табличного списка не может заполняться пустым значением, то добавление такой записи не производится. По умолчанию все колонки табличного списка кроме ключевых могут заполняться пустыми значениями.

16.13.1.1 Создание табличного списка типа «справочник»

❖ Чтобы создать табличный список типа «справочник»:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Табличный список**.
   Откроется страница **Новый табличный список**.
4. В поле **Название** введите название табличного списка.

> **Примечание.** В поле **Описание** вы можете ввести любой текстовый комментарий.

5. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения табличного списка в БД.

> **Примечание.** Вы можете добавить табличный список в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**.

6. В раскрывающемся списке **Назначение** выберите **Справочник**.
7. Если нужно, установите флажок **Разрешить пользователям других инсталляций Ankey SIEM NG Knowledge Base редактировать контент**.
8. В блоке параметров **Колонки** по ссылке **Добавить колонку** добавьте колонки в табличный список.

Примечание. Вы можете изменить порядок колонок с помощью значка и удалить колонку по кнопке .

9. В поле **Название** введите название колонки.
10. В раскрывающемся списке **Тип данных** выберите тип данных для колонки.
11. Если колонка является ключевой, установите флажок **Ключевое поле**.

Примечание. Табличный список должен содержать хотя бы одну ключевую колонку. По умолчанию ключевой является первая колонка табличного списка.

12. Если требуется индексировать содержимое колонки, установите для нее флажок **Индексируемое**.
13. Если колонка может заполняться пустыми значениями, установите флажок **Может содержать null**.
14. Нажмите кнопку **Создать**.

Табличный список создан.

16.13.1.2 Создание шаблона исключений

После создания шаблона исключений для табличного списка вы сможете по ссылкам из сводок о корреляционных событиях, зарегистрированных в Ankey SIEM NG, автоматически добавлять исключения в белый список или удалять исключения из черного списка.

Шаблон исключений состоит из кода, описывающего правила создания исключений, и текстов исключений. При регистрации корреляционного события для правила корреляции, по которому регистрируется это событие, выполняется поиск шаблонов исключений, созданных для табличных списков, которые используются в этом правиле корреляции в качестве белых или черных списков. Если данные события удовлетворяют одному из условий исключений, указанных в коде найденных шаблонов исключений, в интерфейсе ПК Ankey SIEM NG в сводке о корреляционном событии отображается ссылка для создания исключения с текстом исключения.

❖ Чтобы создать шаблон исключений для табличного списка:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

Примечание. Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование шаблона исключений <Название табличного списка>**.

5. Если для табличного списка создан стандартный шаблон исключений, выберите вкладку **Локальная система**.
6. Введите код шаблона исключений.
7. В панели **Тексты исключений** по ссылке **Добавить тексты исключений** добавьте блок параметров для текстов исключений.
8. В поле **Название** введите название для типа исключений.

> **Примечание.** В названии и тексте исключения вы можете использовать значения полей события, указав эти поля в фигурных скобках. Например, при использовании {event_src.host} в тексте будет указан IP-адрес источника события.

9. В раскрывающемся списке **Приоритет** выберите приоритет этого типа исключений при отображении в списке исключений.
10. В поле **Ключ** введите ключ описания исключения, указанный в коде шаблона.
11. В поле **Значение** введите текст исключения, который будет отображаться в интерфейсе ПК Ankey SIEM NG для корреляционного события.
12. Если нужно добавить еще один текст для исключения такого же типа, добавьте условие исключения по ссылке **Добавить условие**.
13. Если нужно добавить тексты для исключений другого типа, добавьте блок параметров для текстов исключений по ссылке **Добавить тексты исключений**.
14. Нажмите кнопку **Сохранить**.

Шаблон исключений для табличного списка создан.

16.13.1.3 Фильтрация записей табличного списка

❖ Чтобы отфильтровать записи в табличном списке:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. В блоке параметров табличного списка нажмите  .
   Появится строка фильтров с названиями колонок.
4. По ссылке с названием фильтра откройте окно с параметрами фильтра и в поле с названием колонки введите шаблон поиска.
5. Если нужно, аналогичным образом настройте другие фильтры.

> **Примечание.** Вы можете очистить параметры фильтра, нажав ✖ справа от названия фильтра. Вы можете очистить параметры всех фильтров, нажав ✖ в строке фильтров.

Записи в табличном списке отфильтрованы в соответствии с условием.

16.13.1.4 Добавление записи в табличный список

Вы можете добавлять записи в стандартные табличные списки типа «справочник», если при их создании был установлен флажок **Разрешить пользователям других инсталляций Ankey SIEM NG Knowledge Base редактировать контент**. Также вы можете добавлять записи в пользовательские табличные списки типа «справочник».

❖ Чтобы добавить запись в табличный список:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. Нажмите кнопку **Добавить запись**.
4. В соответствии с типом данных колонок заполните ячейки записи и нажмите ✔.

Запись добавлена в табличный список.

16.13.1.5 Изменение записи в табличном списке

Вы можете изменять записи в стандартных табличных списках типа «справочник», если эти списки содержат хотя бы одну неключевую колонку и при их создании был установлен флажок **Разрешить пользователям других инсталляций Ankey SIEM NG Knowledge Base редактировать контент**. Также вы можете изменять записи в пользовательских табличных списках типа «справочник».

> **Примечание.** При изменении стандартной записи (в стандартном табличном списке) она заменяется пользовательской записью с теми же значениями ключевых колонок, в строке с такой записью отображается значок ↪. При необходимости вы можете восстановить стандартную запись, удалив пользовательскую.

❖ Чтобы изменить запись в табличном списке:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. Выберите запись.
4. Нажмите кнопку **Редактировать**.
5. Измените запись и нажмите ✔.

Запись табличного списка изменена.

16.13.1.6 Активация и деактивация записи

Если запись из стандартного табличного списка типа «справочник» перестала быть актуальной или если вы хотите временно приостановить использование записи из пользовательского табличного списка типа «справочник», вы можете ее деактивировать.

Деактивированные записи не используются в правилах корреляции и обогащения. Деактивированную ранее запись вы можете активировать.

❖ Чтобы деактивировать (активировать) запись:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. Выберите запись.

> **Примечание.** Для выбора нескольких записей подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных записей − клавишу Ctrl.

4. Нажмите кнопку **Деактивировать** (**Активировать**).

Запись деактивирована (активирована).

16.13.1.7 Удаление записей из табличного списка

❖ Чтобы удалить записи из табличного списка:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. Выберите записи.

> **Примечание.** Для выбора нескольких записей подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных записей − клавишу Ctrl.

4. Нажмите кнопку **Удалить** и подтвердите удаление.

> **Примечание.** Вы можете удалить все записи по кнопке **Очистить табличный список**.

Записи удалены из табличного списка.

16.13.1.8 Импорт записей из файла формата CSV

Вы можете импортировать записи в стандартные и пользовательские табличные списки типа «справочник», если при их создании был установлен флажок **Разрешить пользователям других инсталляций Ankey SIEM NG Knowledge Base редактировать контент**. Поддерживается импорт записей из файлов формата CSV в кодировке UTF-8. В первой строке файла нужно указать наименования колонок, в качестве разделителя данных в строке нужно использовать точку с запятой (;).

Файл для импорта должен содержать значения для ключевых колонок табличного списка. Значения ячеек должны удовлетворять требованиям: для типа данных DateTime − дата должна находиться в интервале от 1970-01-01 00:00:00 до 2106-02-07 06:28:15; для Number − число должно находиться в интервале от −9223372036854775807 до 9223372036854775807; для String − длина строки не должна превышать 16 382 символов (65 531 байт).

❖ Чтобы импортировать записи в табличный список:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. В блоке параметров табличного списка нажмите кнопку **Импорт**.
   Откроется окно **Импорт табличного списка**.
4. По ссылке **выбрать** укажите расположение файла с записями.

> **Примечание.** Вы можете указать файл с записями для импорта, перетащив его в область **Загрузить CSV-файл**.

5. Нажмите кнопку **Импортировать**.
6. При появлении сообщения об окончании процедуры импорта нажмите кнопку **Закрыть**.

Записи импортированы. Записи с уникальными значениями ключевых колонок добавлены в конец табличного списка. Записи с существующими в табличном списке значениями ключевых колонок перезаписаны.

16.13.1.9 Экспорт записей в файл формата CSV

❖ Чтобы экспортировать записи из табличного списка:

1. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
2. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

3. Выберите записи.

Примечание. Для выбора нескольких записей подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных записей − клавишу Ctrl.

4. Нажмите кнопку **Экспорт**.
   Откроется окно Экспорт табличного списка.
5. Выберите вариант экспорта Выбранные <N>.

Примечание. Вы можете экспортировать все записи, выбрав вариант экспорта **Все <M> записей**.

6. Нажмите кнопку **Экспортировать** и укажите папку для сохранения файла.

Записи экспортированы и сохранены в файл формата CSV. Имя файла содержит имя табличного списка и дату импорта. В первой строке файла указаны имена колонок табличного списка, в качестве разделителя используется точка с запятой (;). Записи отсортированы по ключевым колонкам.

16.13.1.10 Копирование табличного списка

❖ Чтобы скопировать табличный список:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

Примечание. Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Новый табличный список (на основе <Название табличного списка>)**.
5. В поле **Название** введите название табличного списка.
6. Нажмите кнопку **Создать**.

Табличный список скопирован.

16.13.1.11 Изменение табличного списка

Записи табличного списка сохранятся, если вы измените название или описание табличного списка, добавите колонки, которые могут содержать null (колонки могут быть ключевыми), или измените порядок колонок. В иных случаях после изменения табличного списка все записи будут удалены.

Внимание! Если для табличного списка создан шаблон исключений, после изменения состава или типа данных колонок необходимо также изменить правила заполнения этих колонок в шаблоне.

❖ Чтобы изменить параметры пользовательского табличного списка:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование табличного списка**.
5. Измените параметры табличного списка.
6. Нажмите кнопку **Сохранить**.

Параметры табличного списка изменены.

16.13.1.12 Удаление табличного списка

❖ Чтобы удалить пользовательский табличный список:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите и подтвердите удаление.

Табличный список удален.

16.13.2 Настройка табличных списков для данных об активах

Табличные списки для данных об активах заполняются информацией об активах и автоматически обновляются при изменении состояния активов. Данные из списков могут использоваться в правилах обогащения и корреляции. Вы не можете вручную добавлять или изменять записи в табличных списках для данных об активах. Вы можете создавать, изменять, копировать и удалять пользовательские табличные списки для данных об активах на странице **Пакеты экспертизы**.

Табличный список для данных об активах обладает следующими особенностями:

- должен иметь название, которое может состоять из букв латинского алфавита, цифр, знаков подчеркивания и точек, должно начинаться с прописной буквы;
- может иметь описание на русском или английском языке;

- располагается в папке или пакете экспертизы для хранения в БД;
- может входить в наборы для установки объектов в ПК Ankey SIEM NG;
- предназначен для сохранения проекции модели активов;
- заполняется данными об активах из указанных групп;
- заполняется данными на основании PDQL-запроса к модели активов (по запросу формируется перечень колонок табличного списка, соответствующих указанным полям модели).

16.13.2.1 Создание табличного списка для данных об активах

Примечание. Вы можете создать табличный список для данных об активах (см. раздел 6.2.7) в веб-интерфейсе ПК Ankey SIEM NG на странице **Активы**.

❖ Чтобы создать табличный список для данных об активах:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Табличный список**.
   Откроется страница **Новый табличный список**.
4. В поле **Название** введите название табличного списка.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

5. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения табличного списка в БД.

   Примечание. Вы можете добавить табличный список в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**.

6. В раскрывающемся списке **Назначение** выберите **Данные об активах**.
7. Если нужно отслеживать состояние активов во вложенных группах, установите флажок **Включать вложенные группы**.
8. В поле **PDQL-запрос** введите запрос к модели активов, на основе которого будет сформирован табличный список, в виде:
   Select(@<Название поля 1> as <Название колонки 1>,@<Название поля 2> as <Название колонки 2>,...)| Sort(@<Название поля для сортировки>)
9. Нажмите кнопку **Создать**.

Табличный список создан

16.13.2.2 Копирование табличного списка

❖ Чтобы скопировать табличный список:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите  .
   Откроется страница **Новый табличный список (на основе <Название табличного списка>)**.
5. В поле **Название** введите название табличного списка.
6. Нажмите кнопку **Создать**.

Табличный список скопирован.

16.13.2.3 Изменение табличного списка

❖ Чтобы изменить параметры пользовательского табличного списка:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите  .
   Откроется страница **Редактирование табличного списка**.
5. Измените параметры табличного списка.
6. Нажмите кнопку **Сохранить**.

Параметры табличного списка изменены.

16.13.2.4 Удаление табличного списка

❖ Чтобы удалить пользовательский табличный список:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

Примечание. Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите и подтвердите удаление.

Табличный список удален.

16.13.3 Настройка табличных списков для правил обогащения и корреляции

Табличные списки для правил обогащения и корреляции предназначены для хранения данных, используемых в правилах обогащения и корреляции. Табличные списки для правил корреляции заполняются автоматически при выполнении правил корреляции, табличные списки для правил обогащения − при выполнении правил обогащения. Оба типа табличных списков доступны для чтения из правил корреляции и правил обогащения. Вы можете работать с табличными списками для правил обогащения и корреляции на странице **Пакеты экспертизы**.

Табличные списки для правил обогащения и корреляции бывают стандартными и пользовательскими. Стандартные табличные списки настроены специалистами по информационной безопасности ООО «Газинформсервис» и не могут быть изменены или удалены. Вы можете просматривать стандартные табличные списки и копировать их для создания пользовательских списков. Пользовательские табличные списки вы можете создавать, изменять, копировать и удалять. Вы можете вручную добавлять и изменять записи в стандартных и пользовательских табличных списках через интерфейс ПК Ankey SIEM NG.

Параметры табличного списка

Табличный список для правил обогащения или корреляции обладает следующими особенностями:

- должен иметь название, которое может состоять из букв латинского алфавита, цифр, знаков подчеркивания и точек, должно начинаться с прописной буквы;
- может иметь описание на русском или английском языке;
- располагается в папке или пакете экспертизы для хранения в БД;
- может входить в наборы для установки объектов в ПК Ankey SIEM NG;
- предназначен для хранения данных, полученных при выполнении правил корреляции или обогащения;
- содержит записи, количество которых близко к указанному типичному размеру табличного списка (по умолчанию 80 000);
- содержит записи, количество которых не может превышать указанного максимального размера табличного списка (по умолчанию 100 000). При превышении этого значения наиболее старые записи будут автоматически удалены и количество записей будет сокращено до типичного размера;
- может иметь ограничение на время жизни записей (по умолчанию − один день). По окончании указанного времени

после добавления записи в табличный список, она будет автоматически удалена.

Параметры колонок табличного списка

Ключевая колонка − это колонка, значения в которой являются идентификаторами записей табличного списка. Если ключевых колонок несколько, то запись идентифицируется по совокупности значений всех ключевых колонок.

Колонки табличного списка обладают следующими особенностями:

- должны иметь название, которое может состоять из букв латинского алфавита, цифр, знака подчеркивания и точки, должно начинаться с прописной буквы;
- могут содержать данные одного из типов: DateTime, Number, String;

> **Примечание.** Вы можете использовать колонки с типом данных String для хранения IP-адресов в виде: a.b.c.d/<Маска>.

- могут быть ключевыми. Значения всех ключевых колонок индексируются и не могут быть пустыми (null). По умолчанию ключевой является первая колонка;
- могут индексироваться. Использование индексируемых колонок повышает скорость поиска по записям табличного списка. По умолчанию для индексирования используется первая ключевая колонка;
- могут явно допускать значение null. В табличный список может добавляться запись, в которой какое-то из полей отсутствует. Если соответствующая колонка табличного списка не может заполняться пустым значением, то добавление такой записи не производится. По умолчанию все колонки табличного списка кроме ключевых могут заполняться пустыми значениями.

16.13.3.1 Создание табличного списка для правил обогащения и корреляции

❖ Чтобы создать табличный список для правил обогащения или корреляции:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Табличный список**.
   Откроется страница **Новый табличный список**.
4. В поле **Название** введите название табличного списка.

> **Примечание.** В поле **Описание** вы можете ввести любой текстовый комментарий.

5. В раскрывающемся списке **Папка** выберите папку или пакет экспертизы для хранения табличного списка в БД.

> **Примечание.** Вы можете добавить табличный список в наборы для установки, установив флажки напротив названий наборов в раскрывающемся списке **Наборы для установки**.

6. В раскрывающемся списке **Назначение** выберите назначение табличного списка.
7. В поле **Типичный размер** укажите количество записей табличного списка, которое рекомендуется не превышать.
8. В поле **Максимальный размер** укажите максимальное количество записей табличного списка.
9. В поле **Ограничить время жизни записи** укажите время или выключите ограничение времени жизни записей.
10. В блоке параметров **Колонки** по ссылке **Добавить колонку** добавьте колонки в табличный список.

> **Примечание.** Вы можете изменить порядок колонок с помощью значка ⋮ и удалить колонку по кнопке 🗑.

11. В поле **Название** введите название колонки.
12. В раскрывающемся списке **Тип данных** выберите тип данных для колонки.
13. Если колонка является ключевой, установите флажок **Ключевое поле**.

> **Примечание.** Табличный список должен содержать хотя бы одну ключевую колонку. По умолчанию ключевой является первая колонка табличного списка.

14. Если требуется индексировать содержимое колонки, установите для нее флажок **Индексируемое**.
15. Если колонка может заполняться пустыми значениями, установите флажок **Может содержать null**.
16. Нажмите кнопку **Создать**.

Табличный список создан.

16.13.3.2 Копирование табличного списка

❖ Чтобы скопировать табличный список:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Новый табличный список (на основе <Название табличного списка>)**.
5. В поле **Название** введите название табличного списка.
6. Нажмите кнопку **Создать**.

Табличный список скопирован.

16.13.3.3 Изменение параметров табличного списка

❖ Чтобы изменить параметры пользовательского табличного списка:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите .
   Откроется страница **Редактирование табличного списка**.
5. Измените параметры табличного списка.
6. Нажмите кнопку **Сохранить**.

Параметры табличного списка изменены.

16.13.3.4 Удаление табличного списка

❖ Чтобы удалить пользовательский табличный список:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Пакеты экспертизы**.
   Откроется страница **Пакеты экспертизы**.
3. В панели **Папки** выберите табличный список.
   Откроется страница табличного списка.

> **Примечание.** Для поиска табличного списка вы можете использовать фильтрацию объектов.

4. Нажмите и подтвердите удаление.

Табличный список удален.

16.13.4 Настройка макросов

Макрос представляет собой фрагмент кода, содержащий условие для отбора событий. Макросы могут использоваться при создании правил корреляции. Вы можете работать с макросами на странице **Макросы**.

Макросы бывают стандартными и пользовательскими. Стандартные макросы предустановлены и не могут быть изменены. Вы можете просматривать стандартные макросы и копировать их для создания пользовательских макросов. Пользовательские макросы вы можете создавать, изменять, копировать и

удалять.

Макрос имеет следующие параметры:

- название − название на русском или английском языке, адаптированное для представления в интерфейсе (стандартное название макроса указано в его коде в директиве filter);
- описание − текстовый комментарий на русском или английском языке с информацией об условии отбора событий;
- метки − одна или несколько меток для указания особенностей событий, которые макрос позволяет отбирать;
- устанавливать название события при выборе этого макроса − при создании правила корреляции в названии события автоматически будет указано название макроса, который выбран в качестве условия отбора этого события;
- аргументы − параметры, которые используются в коде макроса при составлении условия для отбора событий; для каждого аргумента макроса могут быть указаны значение по умолчанию и текстовый комментарий на русском или английском языке.

16.13.4.1 Настройка меток макросов

Метка − короткий текст, указывающий на общую особенность событий, которые макрос позволяет отбирать. Для одного макроса можно установить несколько меток. Метки можно объединять в группы.

Метки и группы меток бывают стандартными и пользовательскими. Вы можете создавать, изменять и удалять пользовательские метки и группы меток.

❖ Чтобы настроить метки макросов:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Макросы**.
   Откроется страница **Макросы**.
3. В панели **Метки** нажмите + и в раскрывшемся меню выберите пункт **Создать группу меток**.
   Откроется окно **Новая группа меток**.
4. В поле **Название (русский)** введите название группы на русском языке.
5. Если нужно, по ссылке **Добавить название на английском языке** откройте поле **Название (английский)** и введите название группы на английском языке.
6. Нажмите кнопку **Создать**.
   В списке **Локальная система** появится группа меток с указанным названием.

> **Примечание.** Вы можете изменять и удалить группу меток, используя пункты меню, раскрывающегося при нажатии в строке группы ⋮.

7. Если нужно, аналогичным образом создайте другие группы меток.

8. В строке с названием группы меток нажмите ⋮ и в раскрывшемся меню выберите пункт **Добавить метку**.
   Откроется окно **Новая метка**.
9. В поле **Название (русский)** введите название метки на русском языке.
10. Если нужно, по ссылке **Добавить название на английском языке** откройте поле **Название (английский)** и введите название метки на английском языке.
11. Нажмите кнопку **Создать**.

    В списке **Локальная система** → **<Название группы меток>** появится метка с указанным названием.

> **Примечание.** Вы можете изменить и удалить метку, используя пункты меню, раскрывающегося при нажатии в строке метки ⋮.

12. Если нужно, аналогичным образом создайте другие метки.

Метки макросов настроены.

16.13.4.2 Создание макроса

❖ Чтобы создать пользовательский макрос:

1. В главном меню в разделе **<Название базы данных>** выберите пункт с пользовательской БД.
2. В главном меню в разделе **SIEM** выберите пункт **Макросы**.
   Откроется страница **Макросы**.
3. В панели инструментов нажмите кнопку **Создать**.
   Откроется страница **Новый макрос**.
4. Введите код макроса.

> **Примечание.** Вы можете выполнить валидацию макроса по кнопке **Валидация**.

5. В поле **Название (русский)** введите название на русском языке.
6. Если требуется, по ссылке **Добавить название на английском языке** откройте поле **Название (английский)** и введите название на английском языке.

> **Примечание.** В поле **Описание (русский)** вы можете ввести любой текстовый комментарий на русском языке. Также по ссылке **Добавить описание на английском языке** вы можете открыть поле **Описание (английский)** и ввести любой текстовый комментарий на английском языке.

7. Если требуется, в раскрывающемся списке **Метки** установите флажки напротив меток, которые нужно установить для макроса.

> **Примечание.** Вы можете создать метку или группу меток, используя пункты **Создать метку** и **Создать группу меток**.

8. Если требуется, установите флажок **Устанавливать название события при выборе этого макроса**.
9. Нажмите кнопку **Создать**.

Начнется процесс валидации. По завершении валидации в таблице будет создан новый макрос.

16.13.4.3 Копирование макроса

Записи табличного списка сохранятся, если вы измените название, описание, типичный или максимальный размер табличного списка или время жизни записи. В иных случаях после изменения табличного списка все записи будут удалены.

❖ Чтобы скопировать макрос:

1. В главном меню в разделе **SIEM** выберите пункт **Макросы**.
   Откроется страница **Макросы**.
2. В панели инструментов нажмите кнопку **Создать копию**.
   Откроется страница **Новый макрос на основе <Название оригинального макроса>**.
3. В коде макроса измените название макроса, указанное в инструкции filter.
4. Если нужно, в поле **Название (русский)** измените название макроса.
5. Если нужно, измените другие параметры макроса.
6. Нажмите кнопку **Создать**.

Начнется процесс валидации. По завершении валидации в таблице будет сохранен скопированный макрос.

16.13.4.4 Изменение макроса

❖ Чтобы изменить пользовательский макрос:

1. В главном меню в разделе **SIEM** выберите пункт **Макросы**.
   Откроется страница **Макросы**.
2. В таблице выберите пользовательский макрос.
3. В панели инструментов нажмите кнопку **Редактировать**.
   Откроется страница **Редактирование макроса <Название макроса>**.
4. Измените код макроса.

> **Примечание.** Вы можете выполнить валидацию макроса по кнопке **Валидация**.

5. Если нужно, в поле **Название (русский)** измените название макроса.
6. Если нужно, измените другие параметры макроса.
7. Нажмите кнопку **Сохранить**.

Начнется процесс валидации. По завершении валидации в таблице будет сохранен измененный макрос.

16.13.4.5 Удаление макроса

❖ Чтобы удалить пользовательский макрос:

1. В главном меню в разделе **SIEM** выберите пункт **Макросы**.
   Откроется страница **Макросы**.
2. В таблице выберите пользовательский макрос.

3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Макрос удален.

16.13.4.6 Установка меток макроса

❖ Чтобы установить метки одного или нескольких макросов:

1. В главном меню в разделе **SIEM** выберите пункт **Макросы**. Откроется страница **Макросы**.
2. Выберите макросы в таблице.

> **Примечание.** Для выбора в таблице нескольких строк подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных строк − клавишу Ctrl.

3. В панели инструментов нажмите кнопку **Метки**.
4. В открывшемся меню установите флажки напротив меток, которые нужно установить для макросов и выберите пункт **Применить**.

Метки макросов установлены.

16.13.4.7 Валидация макросов

❖ Чтобы выполнить валидацию макросов:

1. В главном меню в разделе **SIEM** выберите пункт **Макросы**. Откроется страница **Макросы**.
2. Выберите макросы в таблице.

> **Примечание.** Для выбора в таблице нескольких строк подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных строк − клавишу Ctrl.

3. В панели инструментов нажмите кнопку **Валидация**. Откроется окно **Валидировать**.
4. Выберите вариант **Выбранные <Число выбранных макросов> объектов**.
5. Нажмите кнопку **Запустить валидацию**.

Валидация выполнена.

17 Диагностика и решение проблем

Инструкции по диагностике и решению проблем, возникающих при работе с ПК Ankey SIEM NG, представлены в документе «Руководство администратора Ankey SIEM NG 4.1.2».

Если выполнение указанных в документе шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис».

Примечание. Порядок обращения в службу технической поддержки, а также особенности и ограничения услуг технической поддержки представлены в документе «Руководство администратора Ankey SIEM NG 4.1.2».

Перечень сокращений

AAA	–	Authentication, Authorization, Accounting − общее название процессов, связанных с обеспечением защиты данных в информационных системах, включая обеспечение аутентификации, авторизации и аудита, но без обеспечения доступности данных
ACL	–	Access Control List – список управления доступом, который определяет, кто или что может получать доступ к объекту
API	–	Application Programming Interface – протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого
ARP	–	Таблица Address Resolution Protocol – хранится в памяти операционной системы и содержит записи для каждого известного ей узла сети
BOM	–	Byte Order Mark − маркер последовательности байтов
CDP	–	Cisco Discovery Protocol – проприетарный протокол второго уровня, разработанный компанией Cisco Systems
CIDR	–	Classless Inter-Domain Routing – бесклассовая адресация
CPU	−	Central processing unit – центральный процессор
CSV	–	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
CVE	−	Common Vulnerabilities and Exposures − список известных уязвимостей и дефектов безопасности
CVSS	−	Common Vulnerability Scoring System − открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью понять приоритет её исправления
DHCP	–	Dynamic Host Configuration Protocol – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
DNS	–	Domain Name System – компьютерная распределённая система для получения информации о доменах

DOCX	–	Расширение имени файла, используемое для файлов, представляющих текст
EB	–	Модуль Ankey SIEM Next Generation Event Broker
ES	–	Компонент Ankey SIEM Next Generation Events Storage
FHRP	–	First Hop Redundancy Protocol − семейство протоколов, предназначенных для создания избыточности шлюза по умолчанию
FQDN	–	Fully Qualified Domain Name − имя домена, не имеющее неоднозначностей в определении
GUID	–	Globally Unique Identifier − статистически уникальный 128-битный идентификатор
HDD	–	Hard disk drive – запоминающее устройство
IP	–	Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP
IPS	–	Intrusion Prevention System − система предотвращения вторжений
JSON	–	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
KB	–	Knowledge Base – это единая база знаний ПК Ankey SIEM NG
LDAP	–	Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP
LLDP	–	Link Layer Discovery Protocol − протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети
MAC	–	Media Access Control – уникальный идентификатор, присваиваемый каждой единице сетевого оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet
MC	–	Компонент Ankey SIEM NG Management and Configuration
MHT	−	Архивный формат веб-страниц
NAS	–	Network Attached Storage − сервер для хранения данных на файловом уровне

NAT	–	Network Address Translation − механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов
NTP	–	Network Time Protocol − сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
PCRE	–	Perl Compatible Regular Expressions − библиотека, реализующая работу регулярных выражений
PDF	–	Portable Document Format − открытый формат электронных документов
PDQL	–	Язык, разработанный для написания запросов в процессе обработки событий, инцидентов, динамических групп активов и табличных списков в ПК Ankey SIEM NG
PNG	–	Portable network graphics − растровый формат хранения графической информации
RFC	−	Request for Comments − документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети
SIEM	–	Security information and event management – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности
SNMP	–	Simple Network Management Protocol – протокол сетевого управления
SVG	–	Scalable Vector Graphics – язык разметки масштабируемой векторной графики
TXT	–	Компьютерный файл, содержащий текстовые данные
URL	–	Uniform Resource Locator − унифицированный указатель ресурса
UTF-8	–	Unicode Transformation Format, 8-bit − стандарт кодирования символов
XLSX	–	Формат электронной таблицы
XML	–	Xtensible Markup Language – расширяемый язык разметки
БД	–	База данных
ИБ	–	Информационная безопасность

ОС	–	Операционная система
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных

Приложение А
Типы событий, собираемых с активов под управлением Windows

В таблице описаны типы событий, собираемых с активов под управлением Windows.

Таблица А.1 −Типы собираемых событий

Тип события	Описание
Категория filesystem − операции с объектами файловой системы	
FileCreated	Создан файл или папка
FileOverwritten	Перезаписан файл или папка
FileDeleted	Удален файл или папка
FileRenamed	Переименован файл или папка
FileLinkCreate	Создана жесткая ссылка на файл или папку
FileDataModified	Изменено содержимое файла или папки
FileDataPagingModified	Изменен объект отображения в память содержимого файла
FileAttributesModified	Изменены атрибуты файла или папки
FileBasicAttributesModified	Изменены базовые атрибуты файла или папки
FileCreationTimeModified	Изменено время создания файла или папки
FileOpened	Открыт файл или папка
FileDataRead	Прочитаны данные файла
FileAttributesRead	Прочитаны атрибуты файла или папки
FileClosed	Закрыт файл или папка
FileMappingCreated	Создан объект отображения в память содержимого файла
FileDirectoryListed	Получен список файлов папки
Категория registry − события системного реестра	
RegistrySetValue	Присвоено значение ключу реестра
RegistryDeleteValueKey	Удалено значение ключа реестра
Категория network − события сетевой активности	
NetworkPortOpened	Открыт порт на узле
NetworkPortClosed	Закрыт порт на узле
NetworkConnectionEstablished	Установлено соединение с узлом
NetworkConnectionClosed	Закрыто соединение с узлом
Категория other − события системной и пользовательской активностей	
ProcessStarted	Запущен процесс

Тип события	Описание
ProcessStopped	Остановлен процесс
ProcessOpened	Процесс получил доступ к другому процессу
ProcessDriverLoaded	Система загрузила драйвер
ProcessModuleLoaded	Процесс загрузил модуль
ProcessRemoteThreadOpened	Процесс получил доступ к потоку обработки другого процесса
ProcessRemoteThreadCreated	Процесс создал поток в адресном пространстве другого процесса
LogonCreated	Пользователь вошел в систему
LogonTerminated	Пользователь вышел из системы
SessionConnected	Пользователь подключен к сессии
SessionCreated	Пользователь создал сессию
SessionDisconnected	Пользователь отключен от сессии
SessionDisconnectedLoggedOn	Пользователь обновил сессию
SessionLoggedOn	Пользователь вошел в сессию
SessionLoggedOff	Пользователь вышел из сессии
SessionTerminated	Прекращена сессия пользователя
VolumeArrived	Подключен том на узле
VolumeRemoved	Отключен том на узле

Приложение Б
Математические функции для работы с данными в системе

В ПК Ankey SIEM NG вы можете использовать математические функции для анализа данных.

Функция Avg

Функция с аргументом All используется для подсчета среднего значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select [Поле 1], …, [Поле N] Avg ([All] [Поле 1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Compact

Функция используется для компактного представления данных о выбранном объекте. Применяется к данным любого типа. Возвращает для каждой группы единственную строку с указанием значения объекта [Поле 2] (тип данных String) и количества (тип данных Number).

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select ([Поле 1], Compact [Поле 2]) Where [Условие фильтрации]

Функция Compactunique

Функция используется для компактного представления данных о выбранном объекте. Применяется к данным любого типа. Возвращает для каждой группы единственную строку с указанием уникального значения объекта (тип данных String) и количества (тип данных Number).

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select [Поле 1], (Compactunique [Поле 2]) Where [Условие фильтрации]

Функция Count

Функция используется для подсчета количества значений за указанный период. Применяется к данным любого типа. Возвращает для каждой группы единственное значение с типом данных Number.

Функция с аргументом All используется для подсчета количества всех значений с любым типом данных, кроме Null, в выбранной колонке [Поле 1] за указанный период.

Синтаксис:

Select [Поле 1], …, [Поле N] Count ([All] [Поле 1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция с аргументом Distinct используется для подсчета количества уникальных значений с любым типом данных, кроме Null, в выбранной колонке [Поле 1] за указанный период.

Синтаксис:

Select [Поле 1], …, [Поле N] Count ([Distinct] [Поле 1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Count (*) используется для подсчета количества всех значений (в том числе повторяющихся и с типом данных Null) в таблице.

Синтаксис:

Select [Поле 1], …, [Поле N] Count (*) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Countunique

Функция используется для подсчета количества уникальных значений в выбранной колонке [Поле 1] за указанный период. Также функция может использоваться для подсчета количества уникальных записей исходной таблицы, сформированных из указанных колонок [Поле 1], …, [Поле N]. Применяется к данным любого типа. Возвращает для каждой группы единственное значение с типом данных Number.

Синтаксис:

Select [Поле 1], …, [Поле N] Countunique ([Поле 1], …, [Поле N]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Sum

Функция с аргументом All используется для подсчета суммы всех значений в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select [Поле 1], …, [Поле N] Sum ([All] [Поле 1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Min

Функция с аргументом All используется для поиска минимального значения в выбранной колонке [Поле 1] за указанный период. Применяется к

данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select [Поле 1], …, [Поле N] Min ([All] [Поле 1]) WHERE [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Max

Функция с аргументом All используется для поиска максимального значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select [Поле 1], …, [Поле N] Max ([All] [Поле1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Функция Median

Функция с аргументом All используется для поиска медианного значения в выбранной колонке [Поле 1] за указанный период. Данные в колонке сортируются. Для наборов с нечетным числом элементов медианным считается значение центрального элемента, а для наборов с четным числом элементов − среднее значение двух центральных элементов. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

Примечание. При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

Select [Поле 1], …, [Поле N] Median ([All] [Поле1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]

Пример

Запрос Select time, event_src.host, text Count (*) Where importance = high Group by event_src.host Over time (10 минут) позволяет сгруппировать все события с высоким уровнем опасности по узлу-источнику. Для каждого узла-источника в таблице будет указано количество событий в каждом 10-минутном интервале от времени первого события до момента запроса.

Приложение В
Фильтрация событий агентом ПК Ankey SIEM NG

Фильтрация событий позволяет отбросить лишние события на уровне агента, в следствии чего данные события не будут переданы в службу normalizer[3].

Настройка фильтрации доступна для следующих модулей сбора:

- WmiLog;
- WinEeventLog;
- Syslog;
- FileMonitor;
- FileImporter.

Примечание. Для остальных модулей сбора нет возможности настроить фильтрацию событий на уровне профиля сбора из-за отсутствия данного функционала.

B.1 Фильтрация событий для модуля сбора WmiLog

❖ Чтобы настроить фильтрацию событий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
2. Выберите пользовательский профиль, где нужно настроить фильтрацию событий.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. В секции **Каналы журнала** выберите канал, где нужно настроить фильтрацию.
5. В поле **Фильтр для WQL-запроса** введите необходимый фильтр событий на основе WQL-запроса, примеры WQL-запросов приведены в таблице B.1.

Таблица B.1 – Примеры WQL-запросов

WQL-запрос	Описание
EventCode<>'7036' AND EventCode<>'7034'	Исключить из сбора события с EventCode 7036 и 7034
EventCode != '7036' AND NOT EventCode = '7034'	Исключить из сбора события с EventCode 7036 и 7034
User IS NOT NULL	Исключает из сбора события, где поле User является пустым
User LIKE '%ankey%'	Собирает события, где поле User удовлетворяет шаблону, слово "ankey" находится в любом месте строки

Для разработки собственных WQL-запросов для фильтрации событий могут помочь таблица B.2 с описанием ключевых слов и таблица 0 с описанием операторов. Более подробную информацию по WQL-запросам смотрите на официальном портале Microsoft.

[3] Подробнее про службу normalizer см. в документе Руководство разработчика Ankey SIEM NG.

Таблица B.2 – Ключевые слова WQL

Ключевые слова WQL	Описание
AND	Объединяет два логических выражений и возвращает TRUE, если оба выражения имеют значение TRUE
NOT	Логический оператор отрицания
OR	Логическое ИЛИ
LIKE	Оператор, который определяет, соответствует ли строка заданному шаблону
IS	Оператор сравнения с NULL. Синтаксис этого оператора следующий: IS [NOT] NULL (Где NOT не является обязательным)
NULL	Указывает объект, который не имеет явно заданной величины NULL не эквивалентен нулю (0) или пустому значению

Таблица B.3 – Операторы WQL

Операторы WQL	Описание
=	Равно
<	Меньше
>	Больше
<=	Меньше или равно
>=	Больше или равно
!=	Не равно
<>	Не равно

B.2 Фильтрация событий для модуля сбора WinEventLog

❖ Чтобы настроить фильтрацию событий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
2. Выберите пользовательский профиль, где нужно настроить фильтрацию событий.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. В секции **Каналы журнала** выберите канал, где нужно настроить фильтрацию.
5. В поле **Запрос для дополнительной фильтрации событий** введите запрос на языке XPath 1.0 для фильтрации событий. Удовлетворяющие этому запросу события отбрасываются.
6. В таблице B.4 приведены примеры XPath 1.0 запросов.

Таблица B.4 – Примеры XPath запросов

XPath запрос	Описание
*[System[Level=2]]	Запрос для получение событий со всеми уровнями важности кроме Error2
*[EventData[Data and (Data!='Administrator' or Data!='Администратор')]]	Запрос для получения событий, связанных с действиями пользователей Administrator или «Администратор»

XPath запрос	Описание
*[EventData[Data[@Name='SubjectUserName'] and (Data='Administrator' or Data='Администратор')]]	Запрос для получения событий, у которых в параметре SubjectUserName не указано значение Administrator или «Администратор»

Более подробную информацию по XPath-запросам смотрите на официальном портале Microsoft.

B.3 Фильтрация событий для модуля сбора Syslog

❖ Чтобы настроить фильтрацию событий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
2. Выберите пользовательский профиль, где нужно настроить фильтрацию событий.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. Активируйте чек-бокс **Показать дополнительные параметры**.
5. Перейти в секцию **Обработка событий**, секция содержит различные параметры для сбора событий от нескольких источников, по кнопке **Добавить** вы можете добавить отдельную секцию параметров для каждого источника. Секция содержит следующие параметры для настройки фильтрации и предварительной обработки полученных от источника событий:
   - **Приоритет событий от источника** − поле для ввода приоритета, который задается целым неотрицательным числом. Чем меньше число, тем выше приоритет, максимальный приоритет − **0**. По умолчанию приоритет не задан, это соответствует самому низкому приоритету;
   - **Регулярное выражение для фильтрации событий** − дополнительное поле для ввода регулярного выражения для фильтрации событий от источника. Если событие удовлетворяет регулярному выражению (и в параметре **Режим фильтрации событий** указано **Allow**), событие принимается, если нет − отбрасывается. По умолчанию для параметра указана пустая строка, от источника принимаются все события. Поддерживается синтаксис регулярных выражений PCRE;
   - **Режим фильтрации событий** − раскрывающийся список для выбора действия с получаемыми от источника событиями: **Allow** − принимать, **Deny** – отбрасывать;

Примечание. Чтобы настроить с помощью этого параметра фильтрацию событий, нужно создать для источника две секции параметров и с помощью параметра **Регулярное выражение для фильтрации событий** указать в них регулярные выражения для принимаемых и отбрасываемых событий.

– **Маски IP-адресов** – по кнопке **Добавить** вы можете добавить поле для ввода IP-адреса или маски узлов (в формате CIDR), например **192.168.4.1** или **192.168.0.1/24**. Если в параметре **Режим фильтрации событий** указано **Allow**, события принимаются только от указанных узлов. События от других узлов отбрасываются.

В качестве примера ниже представлен алгоритм действий для создания фильтра для отбрасывания событий с наличием слова **ankey** приходящих из подсети **10.10.217.0/24**:

1. Добавьте новый источник, как на рисунке В.1.

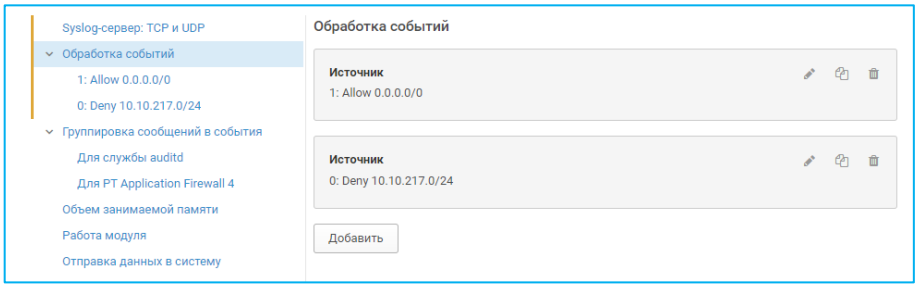

Рисунок В.1 – Создание источника

2. Для источника с режимом фильтрации событий **Allow** в поле **Приоритет событий от источника** укажите значение **1**, как показано на рисунке В.2.

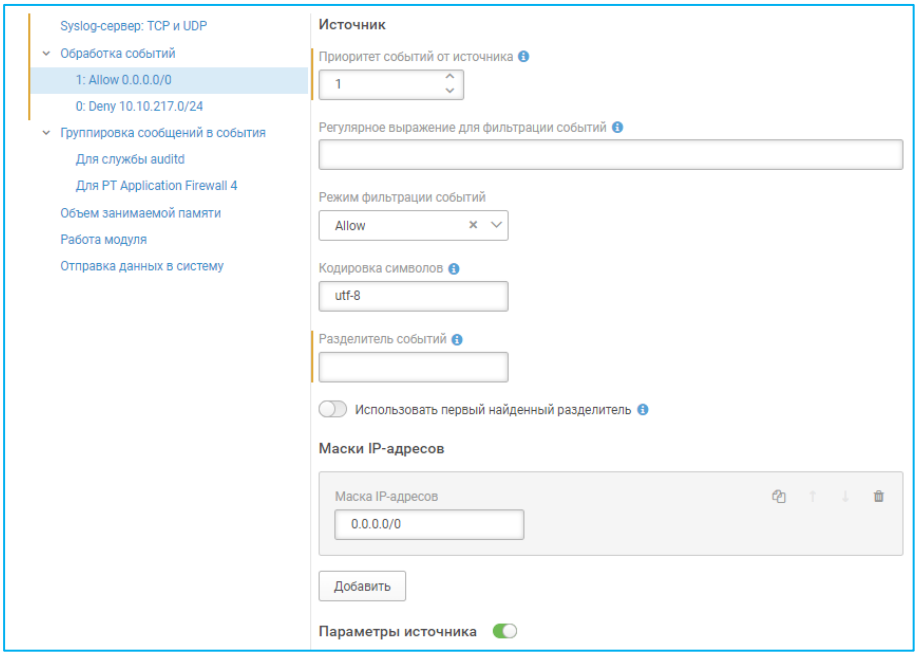

Рисунок В.2 – Настройка источника Allow

3. Для нового источника выполните следующие настройки:
   – в поле **Режим фильтрации событий** необходимо выбрать **Deny**;
   – в поле **Приоритет событий от источника** необходимо ввести значение **0**;

– в поле **Регулярное выражение для фильтрации событий** прописать **.*ankey.***;
– в поле **Маска IP-адресов** прописать **10.10.217.0/24**.

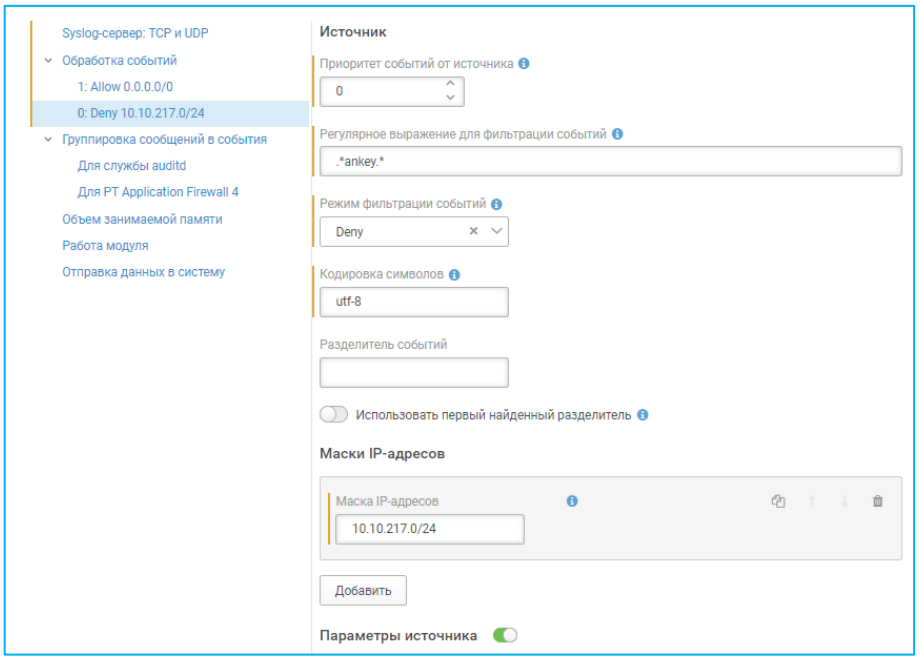

Рисунок В.3 − Настройка источника Deny

В.4 Фильтрация событий для модулей сбора FileMonitor и FileImporter

❖ Чтобы настроить фильтрацию событий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
2. Выберите пользовательский профиль, где нужно настроить фильтрацию событий.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. Активировать чек-бокс **Показать дополнительные параметры**.
5. В секции **Обработка событий** выберите источник, где нужно настроить фильтрацию.
6. В секции **Обработка данных** в поле **Регулярное выражение для отбрасываемых строк** введите регулярное выражение для отбрасываемых строк.
   Поддерживается синтаксис регулярных выражений PCRE.

В качестве примера создадим фильтр для отбрасывания событий с наличием слова **ankey**, для этого в поле **Регулярное выражение для отбрасываемых строк** пропишите **.*ankey.***, как показано на рисунке В.4.

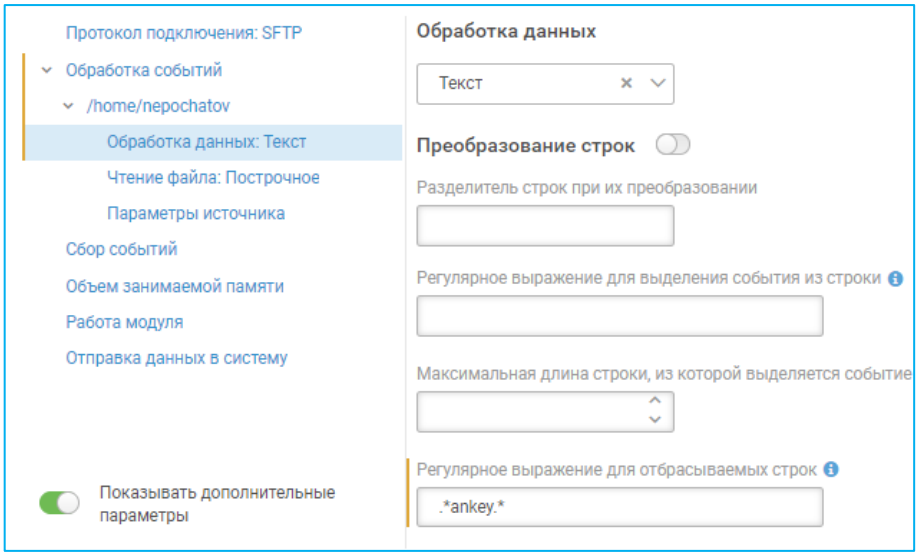

Рисунок В.4 – Регулярное выражение для отбрасывания строки

Данный модуль также позволяет настроить фильтрацию с приоритизацией, для этого:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.
2. Выберите пользовательский профиль, где нужно настроить фильтрацию событий.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. Активировать чек-бокс **Показать дополнительные параметры**.
5. В секции **Чтение данных** в разделе **Фильтры строк** доступны следующие параметры:
   - **Режим фильтрации по умолчанию** – раскрывающийся список для выбора действия со строкой, которая не соответствует ни одному из регулярных выражений, указанных в добавленных фильтрах. **Allow** – строка принимается, **Deny** – строка отбрасывается;
   - **Фильтры строк** – по кнопке **Добавить** вы можете добавить разделы параметров для настройки фильтров строк. Фильтры применяются в порядке, указанном в параметре **Приоритет фильтра**.
     Каждый раздел содержит параметры:
     - **Приоритет фильтра** – поле для ввода приоритета фильтра. Задается целым неотрицательным числом. Чем меньше число, тем раньше применяется фильтр (максимальный приоритет – **0**);
     - **Режим фильтрации** – раскрывающийся список для выбора действия со строкой. **Allow** – строка принимается, **Deny** – строка отбрасывается;
     - **Тип регулярного выражения** – раскрывающийся список для выбора типа регулярного выражения для поиска строк. **Match** – поиск полного совпадения, **Search** – поиск частичного совпадения;

– **Регулярное выражение** – поле для ввода регулярного выражения. Поддерживается синтаксис PCRE.

6. В качестве примера создадим два **Регулярных выражения**, как на рисунке В.5.

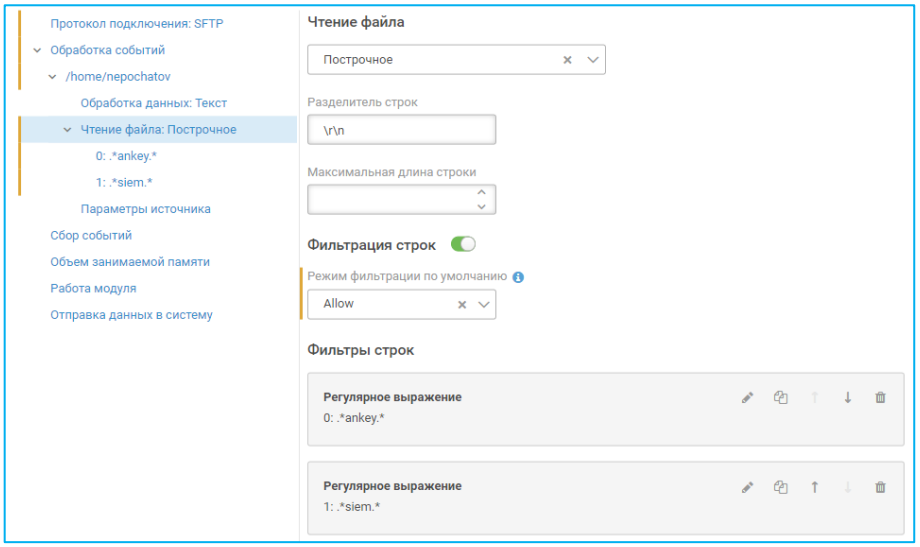

Рисунок В.5 – Фильтрация строк

7. Первое регулярное выражение с приоритетом **0** будет принимать все события, в которых есть полное совпадение со словом **ankey**. Настройки регулярного выражения показаны на рисунке В.6.

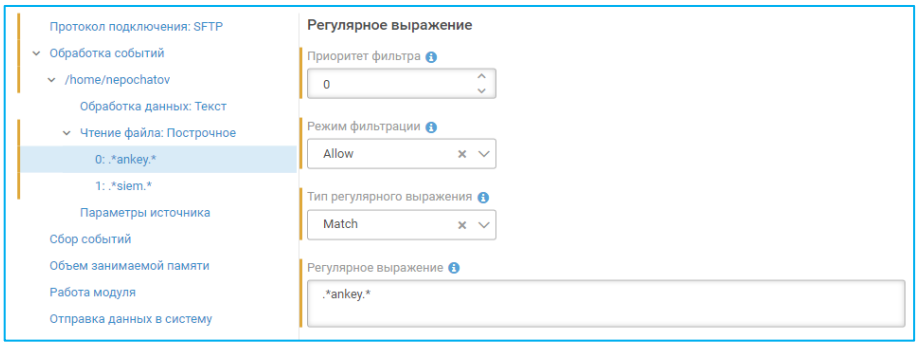

Рисунок В.6 – Регулярное выражение

8. Второе регулярное выражение с приоритетом **1** будет отбрасывать все события, в которых есть полное совпадение со словом **siem**. Настройки регулярного выражения показаны на рисунке В.7.

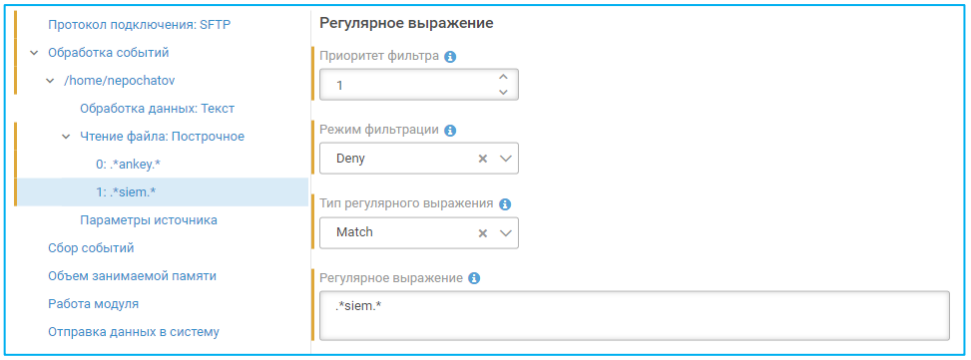

Рисунок В.7 − Регулярное выражение

Логика работы добавленных регулярных выражений следующая:

При обнаружении в событии двух ключевых слов **ankey** и **siem** событие будет пропущено. Отброшено оно будет только в том случае, если в событии присутствует ключевое слово **siem** без ключевого слова **ankey**.

Приложение Г
Клавиши и комбинации клавиш для работы в интерфейсе

Для удобства работы в интерфейсе ПК Ankey SIEM NG вы можете использовать клавиши и их комбинации.

Таблица Г.1 − Клавиши и их комбинации для работы в интерфейсе ПК Ankey SIEM NG

Функция	Клавиши и их комбинации
Общие	
Войти в систему со страницы входа	Enter
Переключаться между разделами главного меню, кнопками, полями ввода	Tab
Переместиться на первую строку	Home
Переместиться на первую строку на странице	PgUp
Переместиться на последнюю строку	End
Переместиться на последнюю строку на странице	PgDn
Переместиться на предыдущую строку	↑
Переместиться на предыдущую строку с сохранением уже выделенных строк	Shift+↑
Переместиться на следующую строку	↓
Переместиться на следующую строку с сохранением уже выделенных строк	Shift+↓
Переключаться между разделами главного меню, кнопками в обратном порядке	Shift+Tab
Выбрать вариант	↓ и ↑
Установить или снять флажок	Space
Таблица событий, таблица инцидентов, табличные списки	
Выделить все строки	Ctrl+A
Выделить несколько строк	Ctrl + щелчок
Выделить несколько строк подряд	Shift + щелчок
Копировать выделенные строки в буфер обмена	Ctrl+C
Табличные списки	
Создать запись в табличном списке	Ctrl+Enter
Удалить запись из табличного списка	Delete
Выполнить множественную сортировку	Shift + щелчок левой кнопкой мыши по названию колонки

Функция	Клавиши и их комбинации
Динамические группы активов	
Узнать количество активов, соответствующих условию PDQLзапроса, при создании динамической группы активов в поле **Фильтр**	Ctrl+Enter
Группы и фильтры	
Развернуть группу, папку фильтров или запросов	* на цифровой клавиатуре
Развернуть группу, папку фильтров или запросов до следующего уровня вложенности	→
Свернуть группу, папку фильтров или запросов	←
Свернуть группу, папку фильтров или запросов	− на цифровой клавиатуре
Свернуть или развернуть панель **Группы и запросы**	[
Свернуть или развернуть панель **Сводка**	]
Меню выбора периода	
Переместиться на предыдущий вариант	←, ↑
Переместиться на следующий вариант	→, ↓
Панель фильтрации событий	
Выполнить запрос	Ctrl+Enter
Конструктор шаблонов отчетов: текстовые объекты	
Отменить (для Windows)	Ctrl+Z
Отменить (для Mac)	Control-Z
Вернуть изменения	Ctrl+Y
Присоединить содержимое элемента списка к элементу списка выше	Alt+↑
Присоединить содержимое элемента списка к элементу списка ниже	Alt+↓
Выделить параграф	Esc
Выделить полужирным	Ctrl+B
Выделить курсивом	Ctrl+I
Увеличить уровень вложенности списка	Ctrl+]
Уменьшить уровень вложенности списка	Ctrl+[

Приложение Д
Рекомендации по заполнению табличных списков

Табличный список – двумерный массив данных, хранящийся в памяти Ankey SIEM NG.

Для работы с табличными списками необходимо в приложении **«Knowledge Base»** перейти на вкладку **«SIEM»** и выбрать в выпадающем списке **«Пакет экспертизы»**, как представлено на рисунке Д.1.

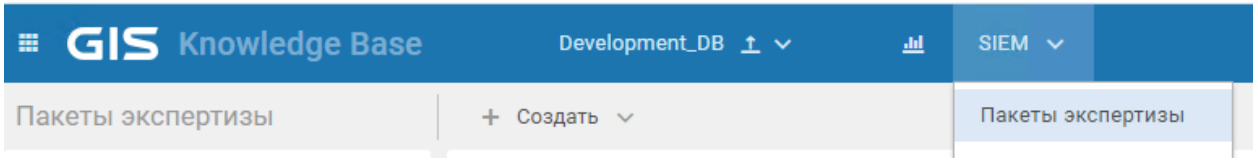

Рисунок Д.1 – Графическая кнопка **«Пакеты экспертизы»**

Для редактирования наполнения табличного списка выберете необходимый табличный список типа **«Справочник»** из списка объектов слева.

Для удобства также можно воспользоваться фильтром (Объекты: Табличные списки) и поиском, как представлено на рисунке Д.2.

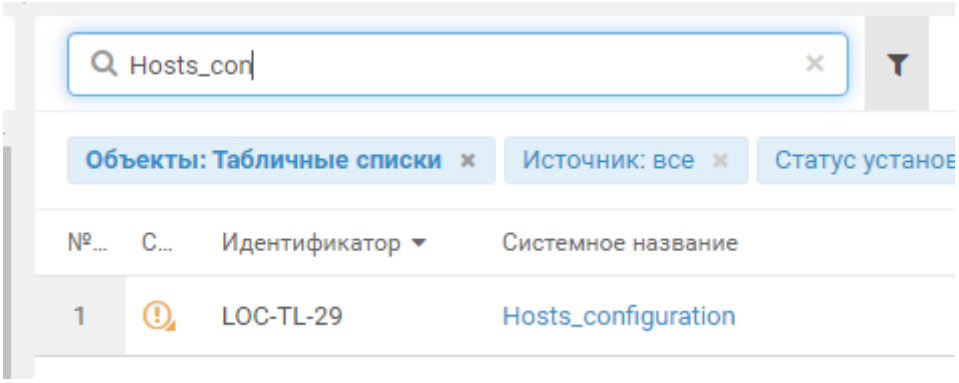

Рисунок Д.2 – Фильтр по объектам

Есть несколько кнопок для работы со справочником, как представлено на рисунке Д.3:

- для редактирования записи нажмите **«Редактировать»**;
- для удаления записи нажмите **«Удалить»**;
- для добавления новых записей нажмите **«Добавить запись»**.

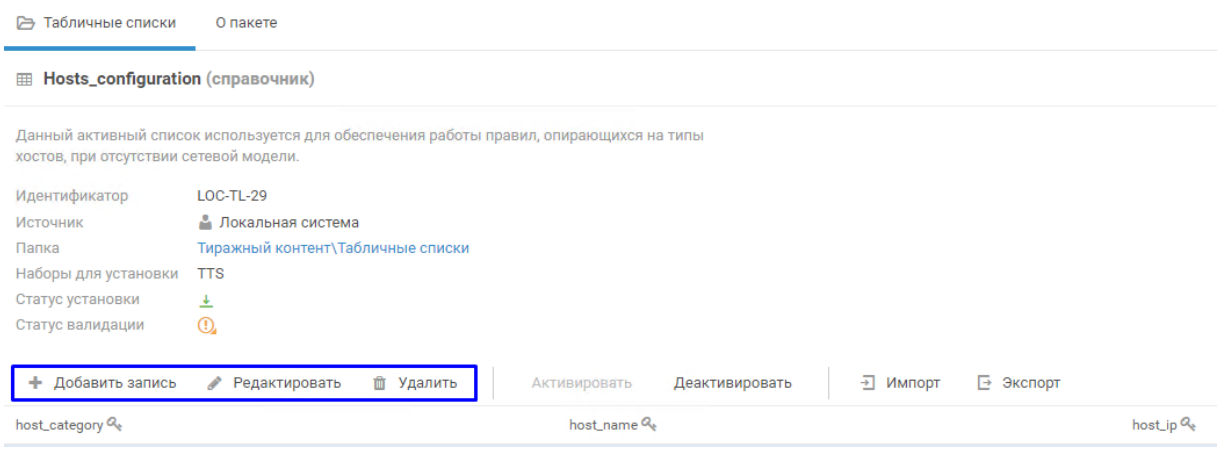

Рисунок Д.3 – Графические кнопки для работы со справочником

Поля можно заполнить значениями разных типов:

1. Поля типа **«number»** заполняются целыми числами от −223372036854775808 до 9223372036854775807.
2. Поля типа **«datetime»** заполняются значениями формата «dd.mm.yyyy». Например, 19.05.2022.
3. Поля с типом **«string»** заполняются символами:
   - IP-адресами (например, 107.24.13.1);
   - подсетями в формате CIDR (например, 107.24.0.0/16);
   - именем хоста;
   - значением «ANY», если поле поддерживает это значение.

Значение **«ANY»** используется в том случае, когда любое значение поля события будет подходить под условия записи в табличном списке.

Рассмотрим пример. Есть следующая запись в табличном списке:

- vendor = Microsoft;
- title = Windows;
- event_src_host = ANY.

Под это условие будут подпадать все события с ОС Windows вне зависимости от источника.

Внимание! Значения «ANY» следует всегда заполнять внимательно.

Рассмотрим пример. Есть следующая запись в табличном списке:

- vendor = ANY;
- title = ANY;
- event_src_host = ANY.

Под это условие будут подпадать события от всех источников со всех хостов, то есть вообще все события. Неосторожное применение значения **«ANY»** может привести к ошибкам корреляции.

Значение **«ANY»** поддерживается не всеми полями табличных списков. Проверить поддерживаемость этого значения можно в описании к справочнику.

Также записи в справочник можно импортировать и экспортировать из него в csv-формате, как представлено на рисунке Д.4.

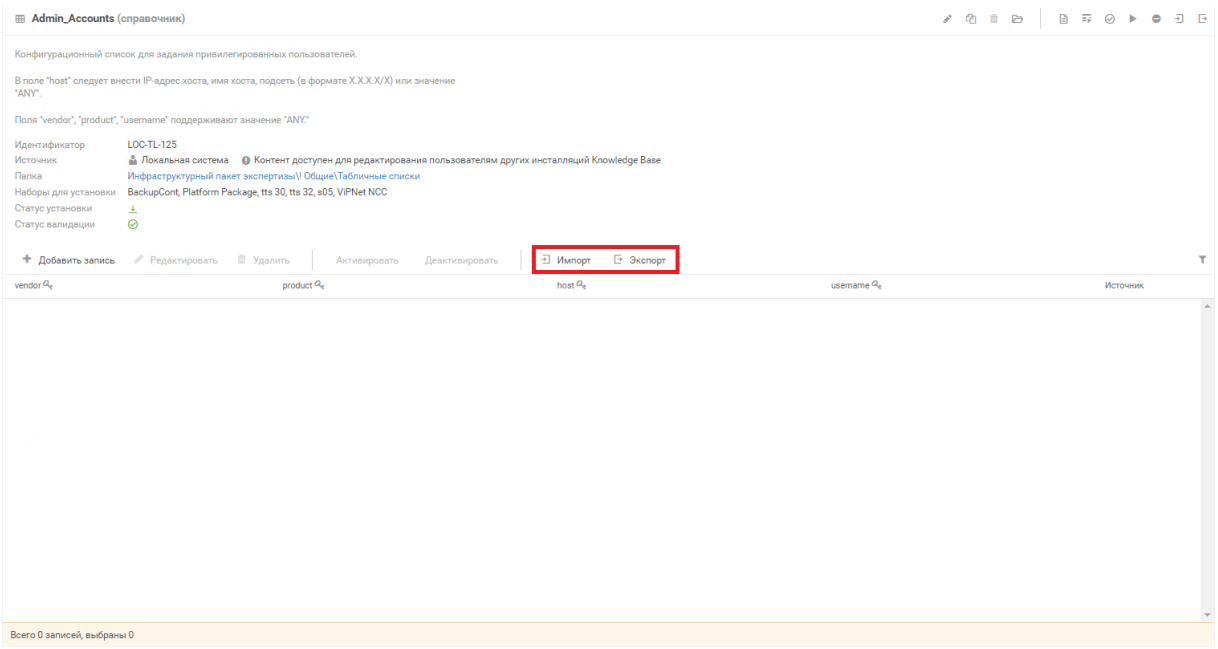

Рисунок Д.4 – Графические кнопки импорта и экспорта записей табличного списка

При экспорте просто выгружается файл csv с составным названием: имя табличного списка, дата и время.

При импорте загружаются все записи, находящиеся в csv-файле, как на рисунке Д.5.

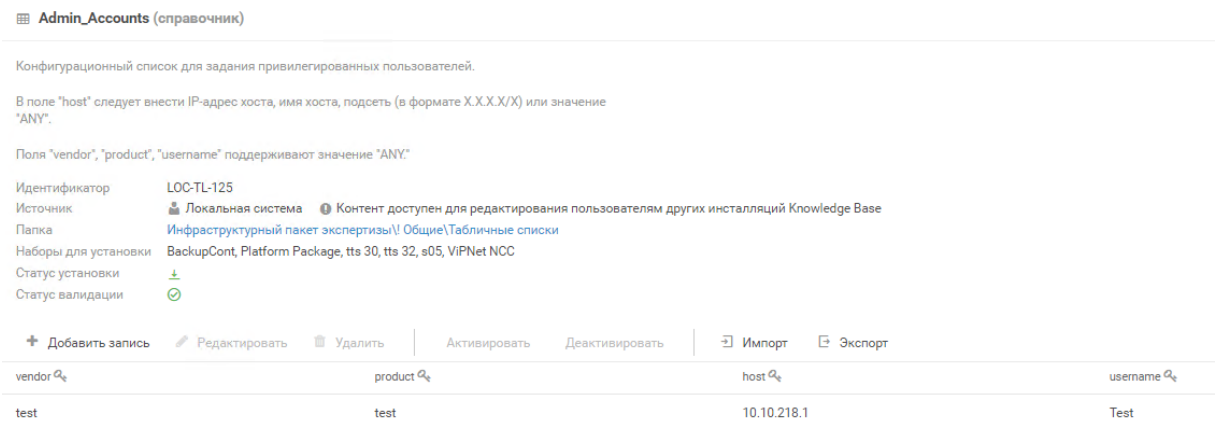

Рисунок Д.5 – Табличный список после импорта записей