ГАЗИНФОРМ СЕРВИС

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

Руководство оператора

643.72410666.00071-01 34 01

Листов 67

Содержание

Введение

Данный документ является руководством оператора для программного комплекса «Платформа расширенной аналитики безопасности Ankey ASAP» v.2.4.1 643.72410666.00071-01 (далее по тексту – ПК «Ankey ASAP», ПК или комплекс).

Руководство предназначено для аналитиков комплекса и описывает назначение, условия и порядок функционирования программного комплекса.

1 Общие сведения

1.1 Назначение программного комплекса

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

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

– в государственных информационных системах до 2 класса защищенности;

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

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

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

1.2 Структура и описание комплекса

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

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

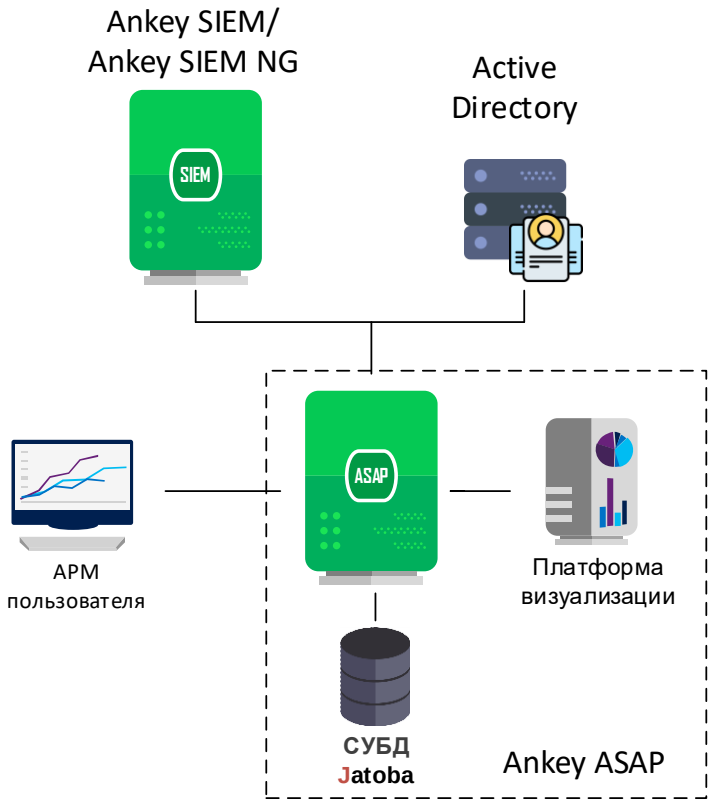


Рисунок 1.1 – Схема взаимодействия ПК «Ankey ASAP» с внешними компонентами

Для выполнения функций по визуализации расширенной аналитики данных о событиях и инцидентах, поступающих в ПК, должна быть использована внешняя платформа визуализации.

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

1. Аутентификация и авторизация пользователей ПК.

2. Администрирование учетных записей пользователей ПК.

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

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

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

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

– активы сетевой модели Ankey SIEM;

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

– активы сетевой модели Ankey SIEM NG.

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

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

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

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

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

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

10. Ведение журнала системных событий ПК, журнала запуска и остановки плагинов (служб) ПК, журнала операций пользователей ПК.

11. Ведение справочной и конфигурационной информации в ПК.

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

1.3 Режимы работы ПК «Ankey ASAP»

Для ПК «Ankey ASAP» установлены следующие режимы функционирования:

– штатный режим;

– регламентный режим;

– режим восстановления (восстановления после сбоев).

Основным режимом функционирования ПК «Ankey ASAP» является штатный режим. В данном режиме обеспечивается выполнение всех функций ПК. Для обеспечения штатного режима функционирования ПК необходимо выполнять

требования и выдерживать условия эксплуатации программного обеспечения и комплекса технических средств ПК, указанные в соответствующих технических документах (техническая документация, эксплуатационная документация и т.д.).

Режим регламентного технического обслуживания должен применяться для осуществления профилактических работ по обслуживанию компонентов системы. В данном режиме допускается остановка отдельных программно-технических средств без нарушения работоспособности системы в целом (выполнение обновления компонентов ПК, создание резервных копий компонентов ПК, перенастройка конфигурации ПК и т.д.).

Режим восстановления является аварийным режимом и характеризуется отказом (сбоем в работе) одного или нескольких компонентов ПК, как в части программного обеспечения, так и в части комплекса технических средств. При переходе ПК в режим восстановления выполняется комплекс мероприятий по устранению причины перехода ПК в данный режим и последующего возвращения в штатный режим работы ПК.

2 Условия выполнения программы

2.1 Аппаратные и программные требования

Требования к ПО автоматизированного рабочего места (АРМ) управления представлены в таблице 2.1. Рекомендуемое разрешение экрана монитора АРМ: 1920 x 1080.

Таблица 2.1 – Требования к программному обеспечению АРМ управления

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

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

2.2 Принципы безопасной работы средства

Для поддержания необходимого уровня защищенности ПК «Ankey ASAP» и его эффективного использования требуется выполнение следующих организационно-технических мероприятий:

– наличие администратора безопасности, отвечающего за правильную эксплуатацию ПК «Ankey ASAP»;

– соблюдение принципа минимизации привилегий пользователей ПК «Ankey ASAP», при котором пользователям предоставляются только те права доступа, которые необходимы им для выполнения служебных обязанностей;

– хранение в секрете идентификаторов (имен), паролей (кодов) администратора и пользователей комплекса;

– периодическая смена паролей пользователей и администратора безопасности ПК «Ankey ASAP»;

– обеспечение физической сохранности (целостности) технических средств, на которых развернут ПК «Ankey ASAP», наличие физической охраны помещения, в котором эксплуатируется программный комплекс и исключение возможности несанкционированного доступа к ПК «Ankey ASAP» посторонних лиц;

– организация защиты каналов управления ЭВМ с установленным ПК «Ankey ASAP», путем прокладки кабельной системы в пределах контролируемой зоны, и защиты её организационно-техническими мерами;

– организация защиты каналов управления ЭВМ с установленным ПК «Ankey ASAP», выходящих за пределы контролируемой зоны, путём применения методов и средств, устойчивых к пассивному и/или активному прослушиванию сети и сертифицированных в установленном порядке или обеспечение запрета удалённого доступа для администрирования ЭВМ с установленным ПК «Ankey ASAP» по незащищённым каналам связи;

– выполнение периодической проверки ЭВМ с установленным ПК «Ankey ASAP» на отсутствие уязвимостей с использованием средств анализа защищённости;

– организация защиты каналов подключения пользовательских АРМ к ЭВМ с установленным ПК «Ankey ASAP» путем применения средств защиты информации, сертифицированных в установленном порядке.

На АРМ управления и пользователя ПК «Ankey ASAP» необходимо обеспечить обязательное выполнение следующих условий эксплуатации:

– обеспечение физической сохранности (целостности), наличие физической охраны помещения, в котором эксплуатируется ЭВМ и исключение возможности несанкционированного доступа к ЭВМ посторонних лиц;

– ежедневная проверка программной среды ЭВМ, использующейся в качестве административной консоли, на наличие вредоносного программного обеспечения;

– периодическая диагностика ЭВМ, использующейся в качестве административной консоли с целью проверки её общей работоспособности.

При эксплуатации ПК «Ankey ASAP» на объектах информатизации необходимо принять следующие основные меры, направленные на исключение возможности эксплуатации выявленных уязвимостей:

– обеспечить защиту от несанкционированного физического доступа к аппаратным компонентам ЭВМ с установленным ПК «Ankey ASAP»;

– исключить каналы связи, обеспечивающие доступ к ЭВМ с установленным ПК «Ankey ASAP» (их программному обеспечению и настройкам) в обход заданных

правил управления доступом, а также правил контроля и фильтрации информационных потоков;

– произвести отключение механизма Intel Active Management Technology (Intel AMT) удаленного управления ЭВМ с установленным ПК «Ankey ASAP» путём применения соответствующих настроек базовой системы ввода-вывода;

– обеспечить защиту настроек базовой системы ввода-вывода от несанкционированного доступа путём применения паролей;

– обеспечить защиту от несанкционированного использования USB-портов ЭВМ с установленным ПК «Ankey ASAP», в том числе при помощи их опечатывания, а также отключения путём применения соответствующих настроек базовой системы ввода-вывода;

– обеспечить ограничение установки (инсталляции) и исполнения в операционной системе программ в части установления возможности установки (инсталляции) и исполнения только программного обеспечения и (или) его компонентов в соответствии с разрешительными атрибутами безопасности на ЭВМ с установленным ПК «Ankey ASAP»;

– обеспечить автоматизированное обнаружение действий в информационных системах, направленных на преднамеренный несанкционированный доступ к информации и специальные воздействия на неё, путём применения систем обнаружения вторжений уровня сети и уровня узла.

3 Выполнение программы

3.1 Подготовка к работе

Перед началом работы пользователю необходимо получить параметры авторизации, с которыми он в дальнейшем будет работать.

Если учетная запись не была создана, то необходимо обратиться к администратору.

3.2 Начало работы

Для управления ПК «Ankey ASAP» используется веб-интерфейс. Для начала работы пользователю необходимо авторизоваться в системе. Для подключения необходимо использовать браузер версии, не ниже указанной в таблице 2.1.

Для запуска веб-интерфейса необходимо:

1. В адресной строке веб-браузера набрать адрес веб-интерфейса сервера «https://<IP-адрес>». Откроется окно авторизации (рисунок 3.1).

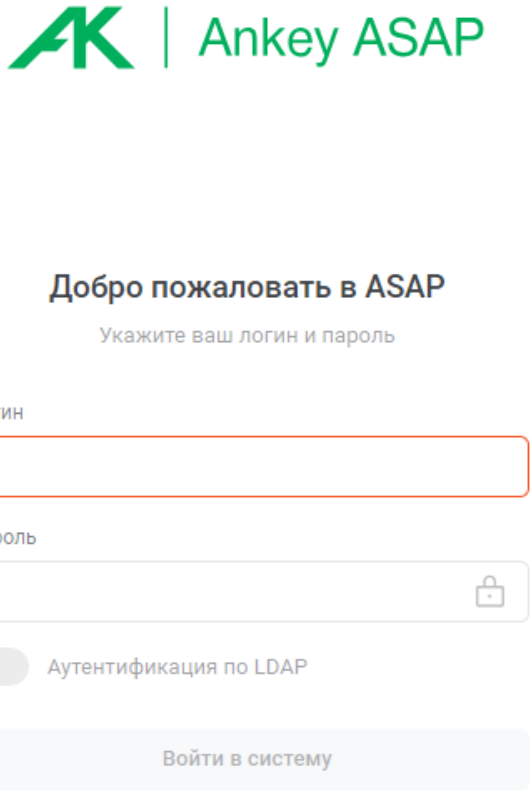


Рисунок 3.1 – Окно авторизации

2. Ввести учетные данные в поля «Логин» и «Пароль».

Примечание. Логин является регистрозависимым.

3. При подключении с использованием доменной учетной записи (через внешний механизм аутентификации (LDAP)) перевести переключатель «Аутентификация по LDAP» в положение «включено».

На странице авторизации пользователю необходимо ввести следующие данные:

– имя доменной учетной записи (без указания домена);

– пароль от доменной учетной записи.

Примечание. Подключение с использование доменной учетной записи должно быть предварительно настроено администратором системы.

4. Нажать кнопку «Войти в вистему» либо клавишу «Enter».

Примечание. При первом входе в систему под локальной учетной записью может потребоваться смена пароля.

После успешной авторизации открывается страница «Мониторинг», представленная на рисунке 3.2. Настройка страницы «Мониторинг» осуществляется в соответствии с пунктом 4.2.1.

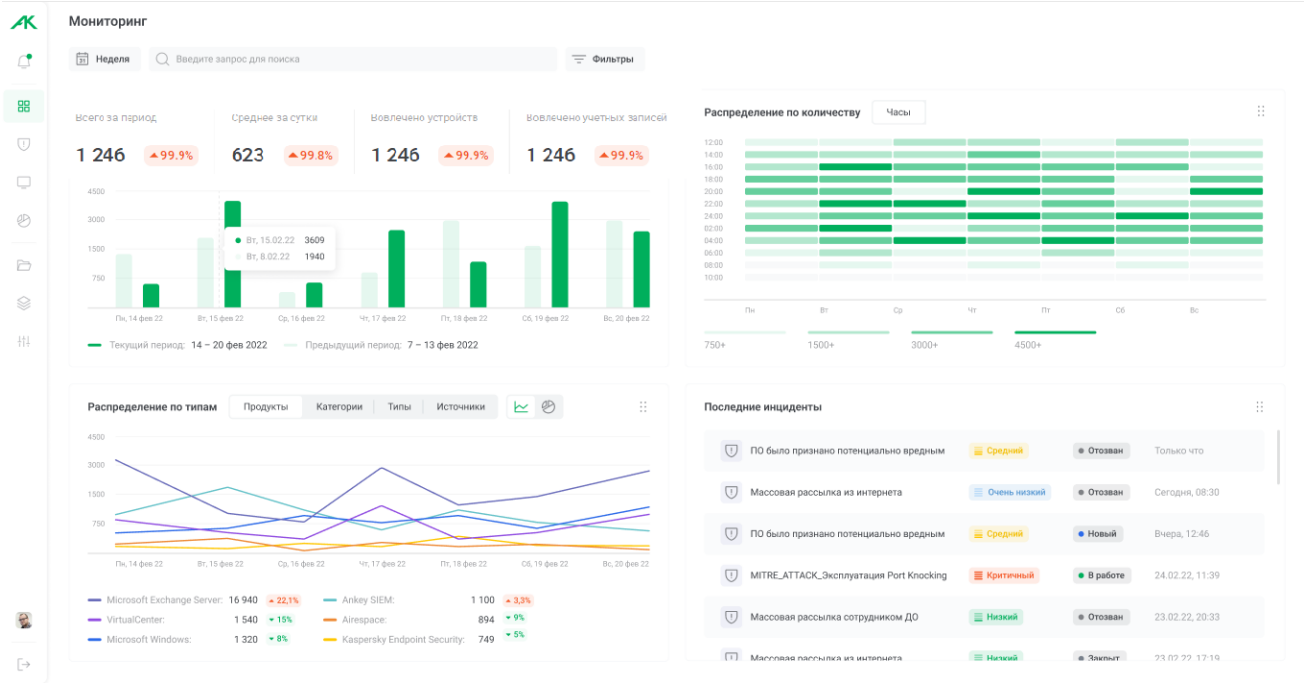


Рисунок 3.2 – Страница «Мониторинг»

Для выхода из системы в левом меню нажать «Выход из системы» под профилем пользователя (рисунок 3.3).

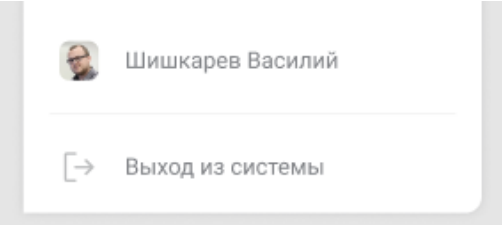


Рисунок 3.3 – Выход из системы

3.3 Веб-интерфейс управления ПК «Ankey ASAP»

В левой части страницы находится панель меню. С помощью панели меню можно получить доступ к следующим ресурсам:

1. Центр уведомлений. Настройка уведомлений об инцидентах и отображение списка уведомлений.

2. Мониторинг. Отображение сводки по инцидентам, алертам и объектам анализа в виде ключевых показателей в виде графиков и диаграмм (пункт 4.2.1).

3. Инциденты. Для просмотра списка инцидентов (пункт 4.4.1) и перехода в карточку инцидента (пункт 4.4.2).

4. Алерты. Для просмотра списка алертов (пункт 4.5.1) и подробной информации о выбранном алерте (пункт 4.5.2).

5. MITRE ATT&CK. Для просмотра таблицы техник и тактик зафиксированных в алертах по системе Mitre (пункт 4.6).

6. Объекты анализа (пункт 4.7). Для просмотра информации об объектах (устройствах и/или учетных записях).

7. Центр аналитики (пункт 4.8) для просмотра аналитических панелей (дашбордов) и проведения визуального анализа данных.

8. Справочники (пункт 4.9). Для ведения (формирования, изменения) справочной информации, используемой для работы платформы и аналитических приложений.

9. Параметры платформы (пункт 4.10):

– Организации. Для просмотра имеющихся в системе организаций.

– Правила регистрации инцидентов. Для просмотра существующих правил регистрации инцидентов, создания и изменения правил.

10. Администрирование → Настройки интеграции (пункт 4.11). Используется для настройки интеграции с платформой визуализации.

В нижней части меню расположен доступ в личный кабинет (профиль) пользователя (пункт 4.12).

4 Описание действий аналитика

4.1 Функции аналитика ПК «Ankey ASAP»

Функции аналитика предназначены для специалиста информационной безопасности и включают в себя мониторинг и анализ событий и инцидентов. Задачи, выполняемые аналитиком, включают в себя действия, перечисленные в таблице 4.1.

Таблица 4.1 – Функции аналитика ПК «Ankey ASAP»

Функции	Операции
Мониторинг событий	Мониторинг событий, поступающих в ПК «Ankey ASAP»
Работа с инцидентами	Работа с карточкой инцидента ИБ Проведение анализа инцидентов
Работа с алертами	Просмотр подробной информации по алертам Проведение анализа алертов
Контроль ресурсов сетевой модели и учетных записей	Контроль учетных записей и устройств Контроль ресурсов сетевой модели Выявление аномального поведения и подозрительных действий объектов
Анализ данных	Проведение визуального анализа данных о событиях и инцидентах с помощью аналитических приложений

4.2 Мониторинг

Страница «Мониторинг» предназначена для проведения мониторинга и анализа данных по графикам и ключевым показателям (KPI), расположенным на странице. Информационные панели (дашборды) можно настраивать и создавать новые.

Примечание. После установки системы настроенные информационные панели отсутствуют.

4.2.1 Создание информационных панелей

Создание информационной панели, при их отсутствии на странице «Мониторинг», осуществляется с помощью кнопки «Добавить» (рисунок 4.1).

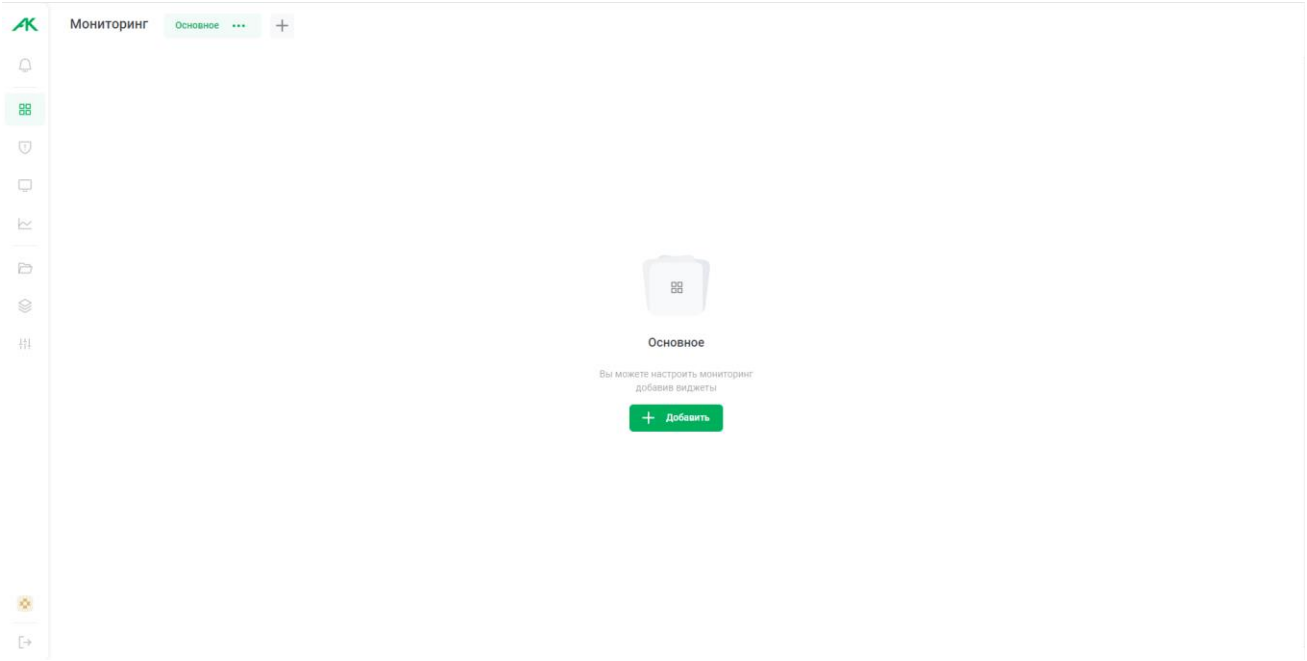


Рисунок 4.1 – Добавление информационной панели

Добавление виджетов на страницу производится из библиотеки виджетов (рисунок 4.2). Для добавления виджетов на страницу выбрать необходимые виджеты из библиотеки и нажать кнопку «Добавить». Виджеты добавляются на текущую вкладку (информационную панель). При сформированной информационной панели, виджеты на нее можно добавить нажав на кнопку «Библиотека виджетов» в правом верхнем углу.

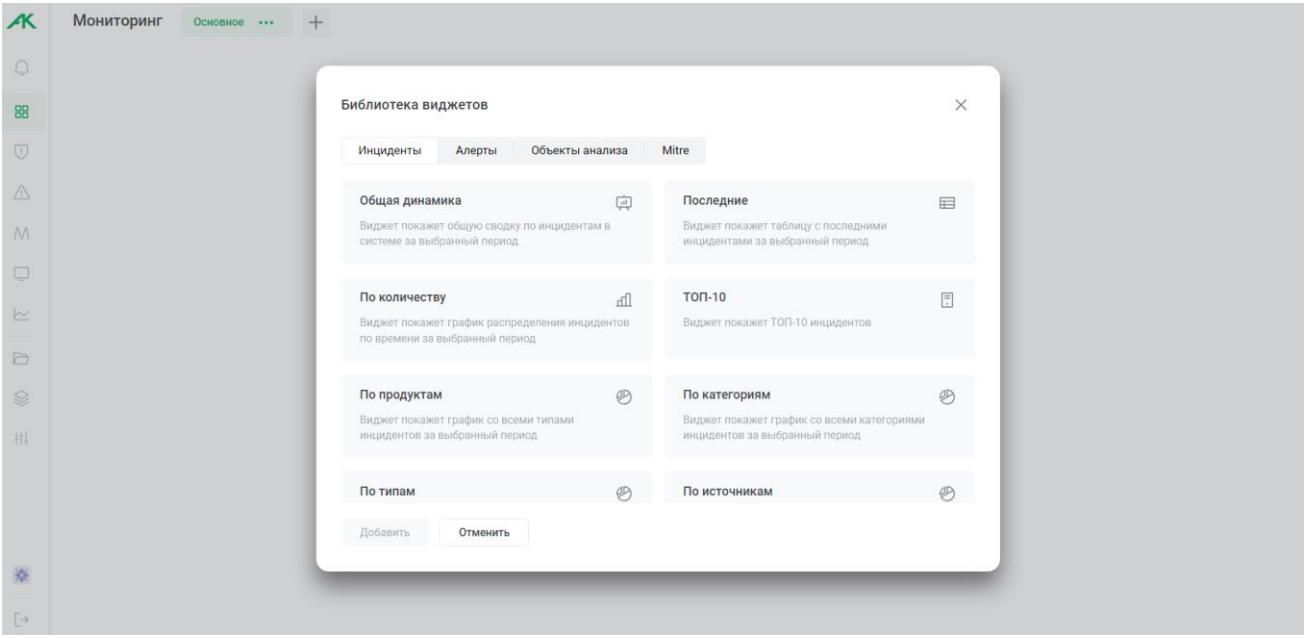


Рисунок 4.2 – Библиотека виджетов

Виджеты на странице можно перемещать или удалять. Для удаления виджета навести курсор на виджет и нажать на пиктограмму «» в правом верхнем углу. Для перемещения виджета необходимо навести курсор на виджет, нажать на пиктограмму «» и, удерживая курсор, переместить виджет в необходимое место на странице.

Для добавления новой вкладки с информационной панелью нажать на пиктограмму «» в верхней части страницы (рисунок 4.3). Ввести наименование вкладки и нажать кнопку «Добавить».

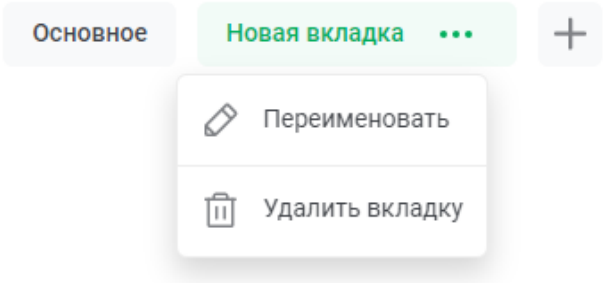


Рисунок 4.3 – Вкладки страницы «Мониторинг»

Для переименования или удаления информационной панели целиком выбрать интересующую вкладку и нажать на «…» справа от наименования.

Пример информационной панели представлен на рисунке 4.4.

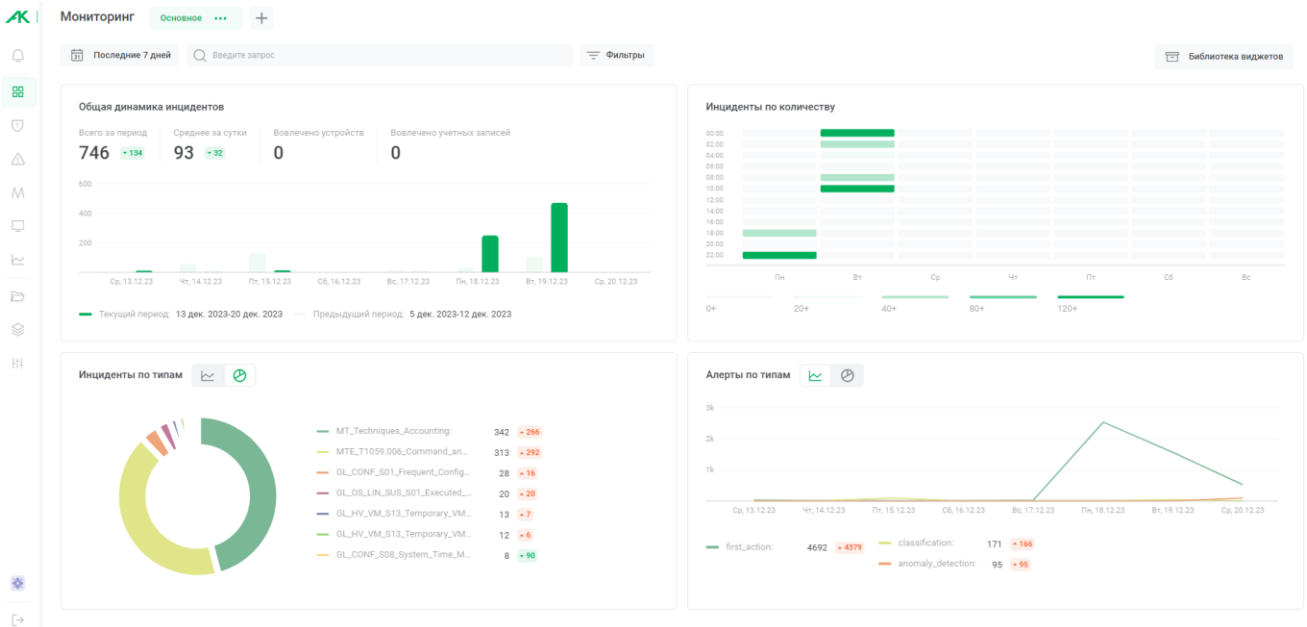


Рисунок 4.4 – Пример информационной панели

На информационную панель могут быть добавлены следующие виджеты:

1. Инциденты:

– общая динамика (сводка по инцидентам в системе за выбранный период);

– последние инциденты (таблица с последними инцидентами за выбранный период);

– по количеству (распределение инцидентов по времени за выбранный период);

– ТОП-10 (10 наиболее часто встречающихся инцидентов);

– по продуктам (график распределения инцидентов по средствам, зафиксировавшим инцидент);

– по категориям (график распределения инцидентов по категориям);

– по типам (график распределения инцидентов по типам);

– по источникам (график распределения инцидентов по источникам, откуда инцидент поступил в систему).

Вид графиков можно изменить, нажав пиктограмму «  » для линейного представления и пиктограмму «  » для круговой диаграммы.

2. Алерты. Статистика по редким действиям объектов (учетных записей и устройств):

– общая динамика (сводка по алертам в системе за выбранный период);

– последние (таблица с последними алертами за выбранный период);

– по количеству (распределение алертов по времени за выбранный период);

– ТОП-10 (10 наиболее часто встречающихся алертов);

– по продуктам (график распределения алертов по средствам, по информации от которых был зафиксирован алерт);

– по моделям поведения (график распределения алертов по видам потенциально опасных действий);

– по типам (график распределения алертов по типам потенциально опасный действий);

– по типам анализаторов (столбчатая диаграмма распределения алертов по типам анализаторов, зафиксировавших алерт).

3. Объекты анализа. Объекты анализа (активы) присутствующие в системе:

– общая динамика (количество устройств и учетных записей в системе);

– ТОП-10 устройств с высоким риском;

– ТОП-10 учетных записей с высоким риском.

4. Mitre. Система мониторинга событий по системе Mitre ATT&CK.

– средний виджет Mitre ATT&CK (вложенный список с событиями классифицированными по системе Mitre);

– маленький виджет Mitre ATT&CK (вложенный список с событиями классифицированными по системе Mitre).

4.2.2 Работа с информационными панелями

Данные, представленные на информационной панели, можно отфильтровать с помощью следующих фильтров:

1. По дате или периоду (рисунок 4.5). Для фильтрации по дате или периоду нажать на «» выбрать период или задать свой период. Ввести или выбрать в выпадающем календаре дату и ввести время начала/конца периода.

2. По данным (рисунок 4.5):

– учетные записи;

– устройства;

– статус инцидента;

– уровень угрозы;

– источник;

– продукт;

– тип.

Для установки фильтров по данным нажать на «Фильтры», ввести или выбрать в выпадающем списке необходимые фильтры. На наличие выбранных фильтров указывает зеленая точка над пиктограммой фильтра «».

3. Поиск по инцидентам, алертам, учетным записям или устройствам. Для поиска ввести запрос в строку поиска и нажать клавишу Enter.

Рисунок 4.5 – Настройка информационных панелей

4.3 Настройка уведомлений об инцидентах и алертах

Настройка уведомлений производится в разделе меню «Центр уведомлений» (пиктограмма «»). При наличии непрочитанных уведомлений рядом с пиктограммой отображается зеленый индикатор «». При переходе в раздел открывается окно с

непрочитанными уведомлениями. Уведомления можно отфильтровать по дате или периоду (пиктограмма «31»).

При нажатии на пиктограмму « ••• », в правом верхнем углу, открывается меню центра уведомлений (рисунок 4.6) в котором доступно выолнение следующих действий:

– включить бесшумный режим (отключение звука и всплывающих уведомлений об инцидентах);

– отметить все прочитанным (все уведомления будут отмечены как прочитанные);

– удалить все уведомления;

– перейти к настройкам уведомлений.

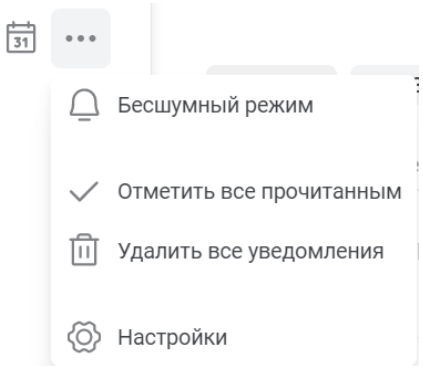


Рисунок 4.6 – Настройки уведомлений

В настройках выполняется управление уведомлениями (рисунок 4.7):

– Бесшумный режим - включение бесшумного режима (отключение всплывающих уведомлений и звука);

– Источник центра уведомлений - настройка фильтрации уведомлений о инцидентах и алертах, в центре уведомлений (рисунок 4.8);

– Источник почтовых уведомлений - настройка фильтрации уведомлений о инцидентах и алертах, на почтовый ящик (рисунок 4.9).

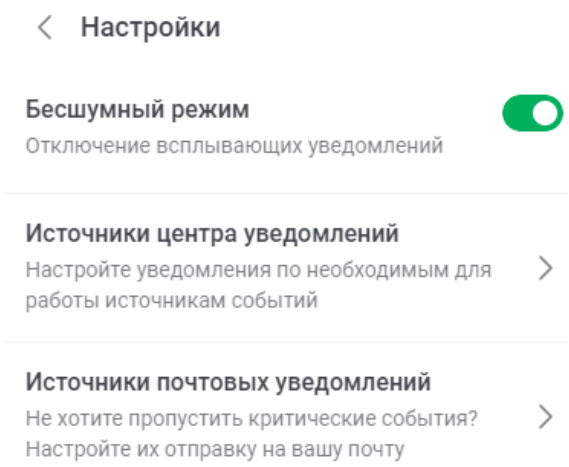


Рисунок 4.7 – Настройки фильрации уведомлений

Для настройки уведомлений по инцидентам установить чекбокс «Инциденты», выбрать необходимы уровень угрозы и источник инцидентов.

Для настройки уведомлений по алертам установить чекбокс «Алерты», выбрать уровень риска.

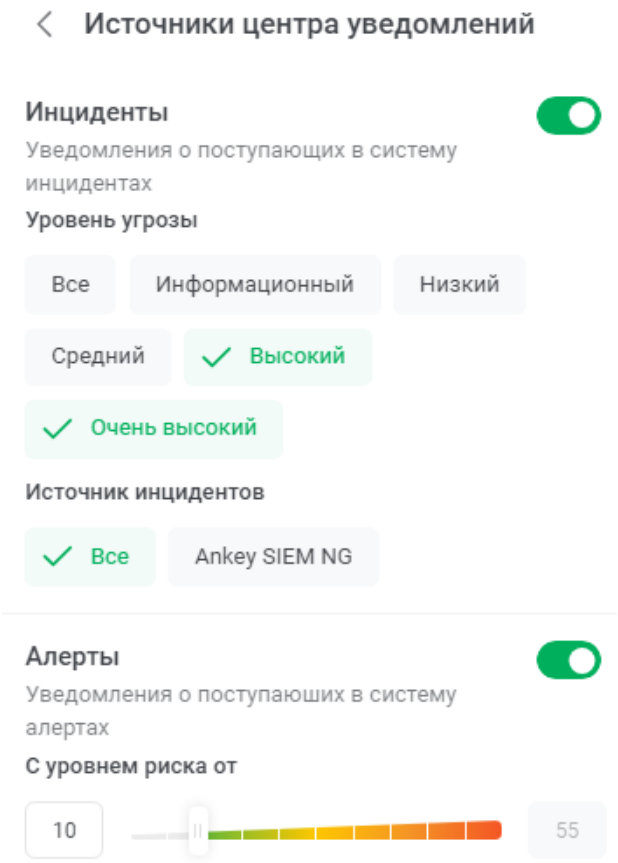


Рисунок 4.8 – Настройки уведомлений об алертах и инцидентах

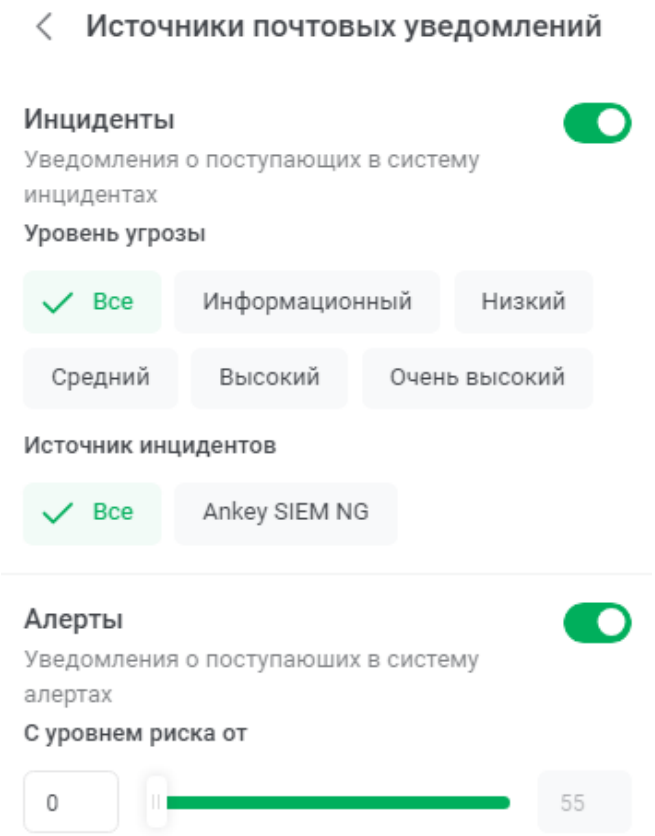


Рисунок 4.9 – Настройки источников почтовых уведомлений

Примечание. Для получения почтовых уведомлений в учетной записи пользователя должен быть введен адрес электронной почты (E-mail).

4.4 Работа с инцидентами

4.4.1 Инциденты

Данные о произошедших инцидентах представлены на странице «Инциденты» (рисунок 4.10).

Примечание. Данные об инцидентах по умолчанию хранятся в системе в течение 365 дней.

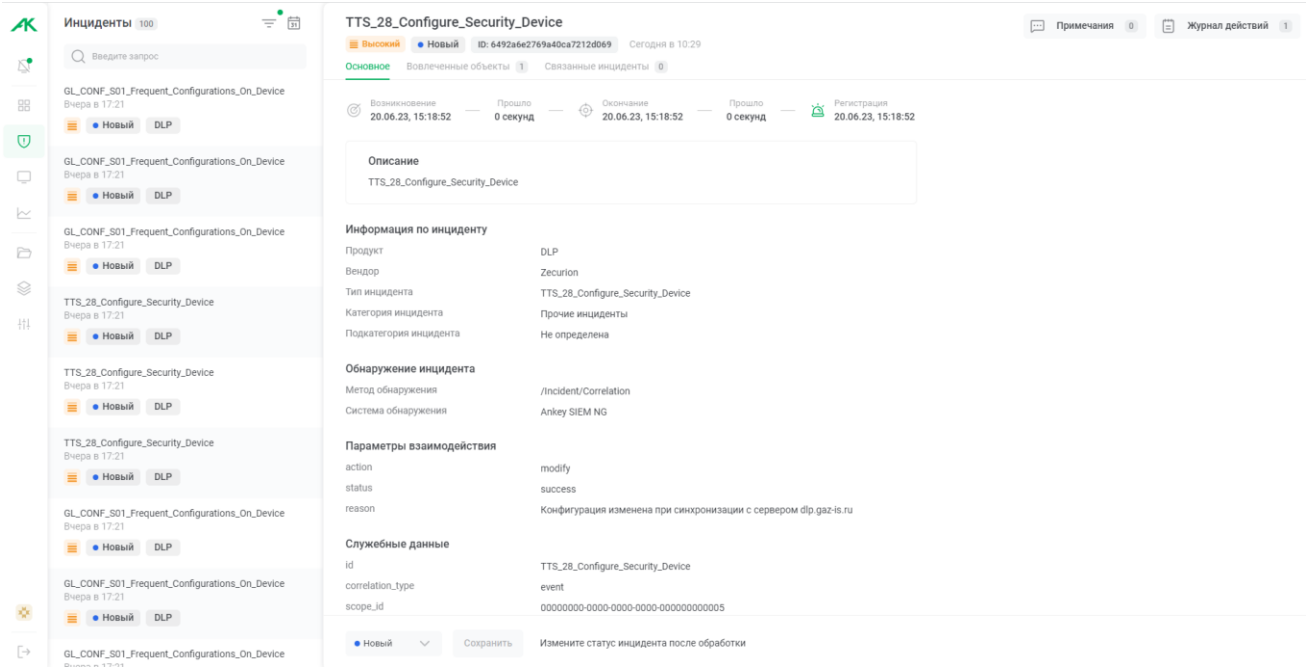


Рисунок 4.10 – Страница инцидентов

На странице показана следующая информация:

1. Список инцидентов.

Перечень инцидентов представлен в левой части страницы в виде списка (рисунок 4.11). По умолчанию в списке отображаются инциденты со статусом «Новый». Для каждого инцидента в списке приводится следующая информация:

– название инцидента;

– дата и время фиксации инцидента;

– иконка, соответствующая уровню угрозы;

– статус инцидента;

– средство, зафиксировавшее инцидент;

– количество комментариев в карточке инцидента (при их наличии);

– количество связанных инцидентов (при наличии связи).

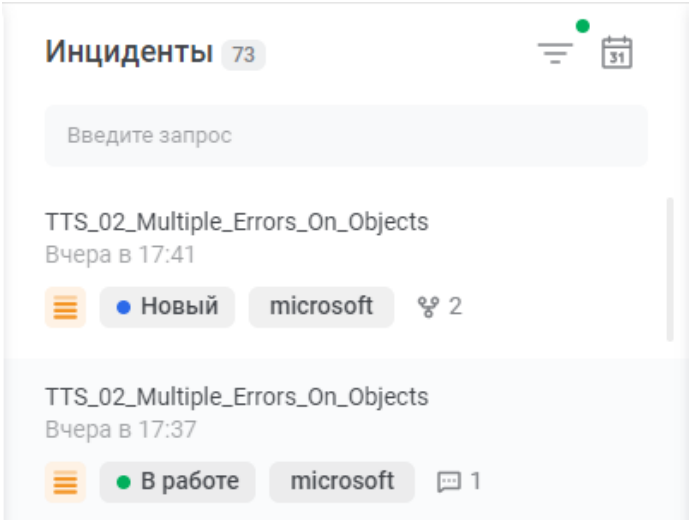


Рисунок 4.11 – Список инцидентов

Список инцидентов обновляется в режиме реального времени, в соответствии с установленным фильтром по дате (за исключением фильтра по заданному периоду). При этом в правой части страницы остается карточка последнего поступившего инцидента на момент открытия страницы «Инциденты». В списке инцидент с открытой карточкой подсвечивается зеленым цветом.

Примечание. При поступлении инцидентов в режиме реального времени не производится завершение сессии пользователя при неактивности, в случае открытой страницы «Инциденты».

2. Фильтры.

К списку инцидентов можно применить фильтры (рисунок 4.12) указанные в таблице 4.2. На наличие выбранных фильтров указывает зеленая точка над пиктограммой фильтра «» или «» (рисунок 4.12).

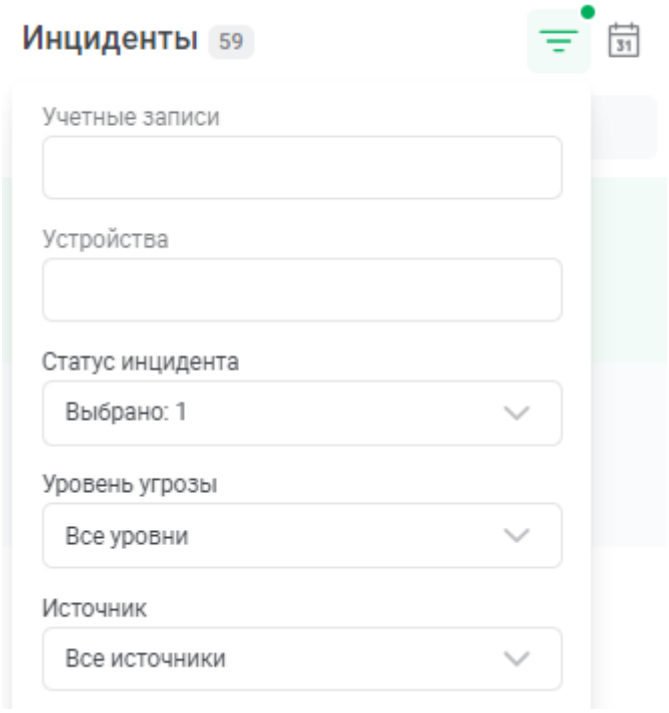


Рисунок 4.12 - Фильтры для списка инцидентов

Таблица 4.2 – Фильтры для списка инцидентов

Фильтр	Описание
Учетные записи	Поиск инцидентов по учетным записям, задействованным в инцидентах
Устройства	Поиск инцидентов по устройствам, задействованным в инцидентах
Статус инцидента	Выбор статуса инцидента из следующих: – новый; – в работе; – закрыт; – отозван. По умолчанию в списке отображаются инциденты со статусом «Новый».
Уровень угрозы	Выбор инцидентов с определенным уровнем угрозы из списка. По умолчанию в списке отображаются инциденты с любым уровнем угрозы.
Источник	Выбор источника инцидентов для Ankey ASAP, в случае, если подключено несколько источников
Период	Выбор периода или задание своего периода из выпадающего календаря и ввод времени начала/конца периода, за который необходимо вывести инциденты

Установленные фильтры закрепляются за пользователем и действуют при следующем входе в систему.

Для поиска по списку инцидентов необходимо ввести запрос в поисковую строку и нажать клавишу Enter.

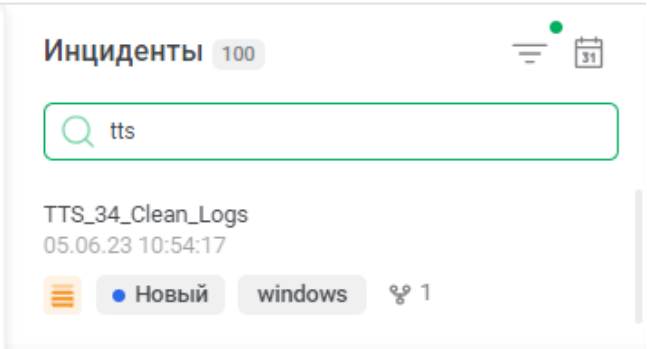


Рисунок 4.13 – Поиск по инцидентам

3. Карточка инцидента

Справа от списка инцидентов отображается карточка с подробной информацией об инциденте. По умолчанию при открытии страницы с инцидентами отображается карточка последнего поступившего инцидента.

4.4.2 Карточка инцидента

На странице «Инциденты» справа от списка инцидентов открывается карточка последнего поступившего инцидента. Пример карточки инцидента (КИ) показан на рисунке 4.14.

Для отображения другой КИ необходимо выбрать инцидент из списка слева.

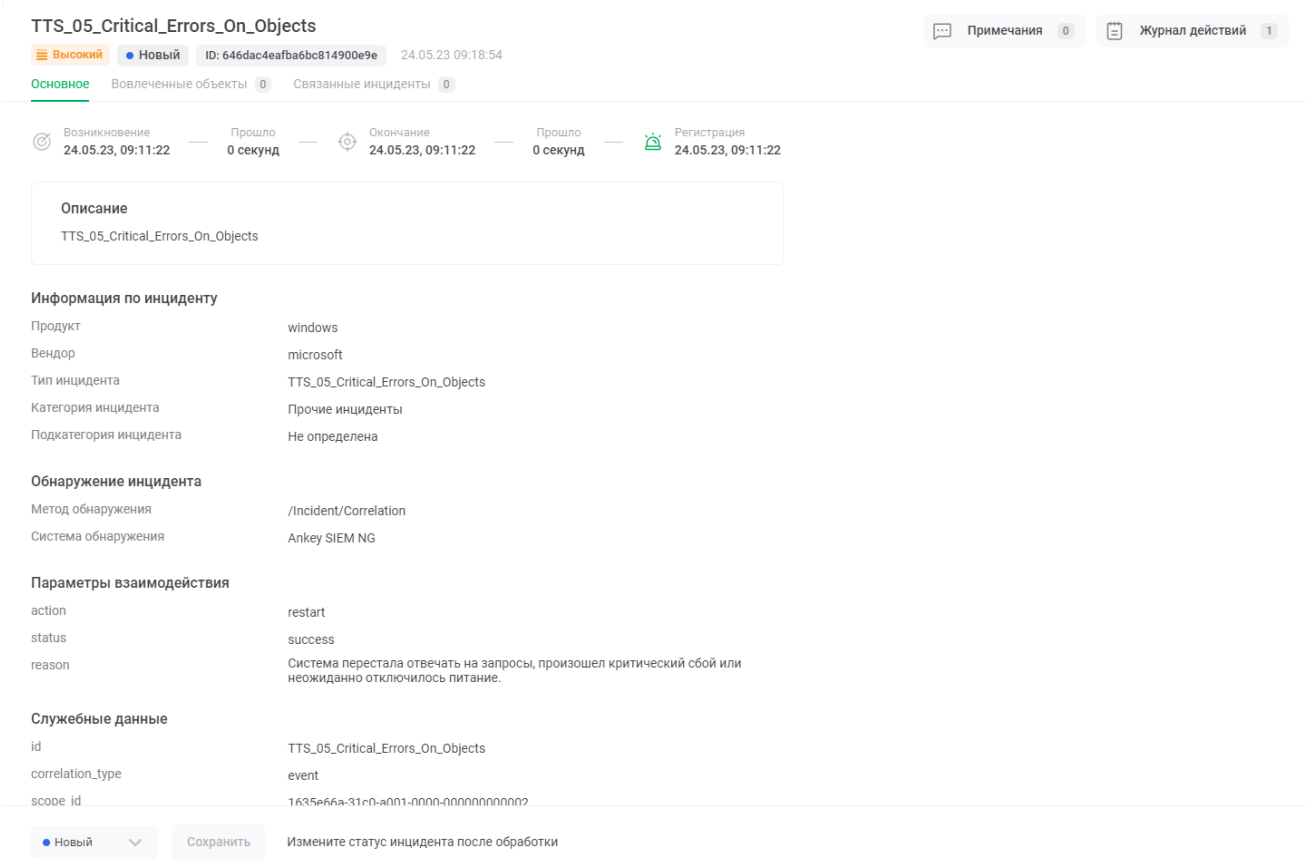


Рисунок 4.14 – Просмотр инцидента

Справа в карточке инцидента есть раздел «Примечания». Раздел предназначен для добавления комментариев по инциденту и прикрепления файлов.

В разделе «Журнал действий» отображаются действия, произведенные с карточкой инцидента, такие как:

– изменение статуса инцидента;

– добавление связи с другим инцидентом.

Для изменения статуса инцидента необходимо выбрать статус из предложенных в нижней части страницы и нажать кнопку «Сохранить». Возможны следующие статусы инцидентов:

– новый;

– в работе;

– закрыт;

– отозван.

Карточка инцидента и произведенные в ней изменения доступны для просмотра всем пользователям Ankey ASAP, ведущим работу с инцидентами.

В карточке инцидента доступны следующие вкладки:

– Основное;

– Вовлеченные объекты;

– Связанные инциденты.

4.4.2.1 Основное

Во вкладке «Основное» показана основная информация об инциденте:

– уровень угрозы;

– дата и время возникновения первого события инцидента;

– период времени между первым и последним событием;

– дата и время окончания (последнее событие);

– дата и время регистрации инцидента (события корреляции);

– описание инцидента (при его наличии);

– информация о средстве, на котором был обнаружен инцидент (вендор и продукт);

– тип инцидента;

– категория и подкатегория инцидента (заполняется в соответствии со справочником «Категоризация инцидентов на основе типа» (4.9.1.3);

– информация о системе, обнаружившей инцидент;

– другие данные.

Поля, поступившие из SIEM-системы по данному инциденту, распределены по группам. При необходимости можно изменять группировку полей или их наименование с помощью справочника «Наименование информационных блоков карточки инцидента» (4.9.1.4).

Все поля события в формате данных SIEM-системы доступны по нажатию кнопки «Подробная информация» в нижней части карточки инцидента (вложенность «invRes»).

4.4.2.2 Вовлеченные объекты

На вкладке представлена информация об объектах (устройствах и учетных записях), задействованных в инциденте (рисунок 4.15).

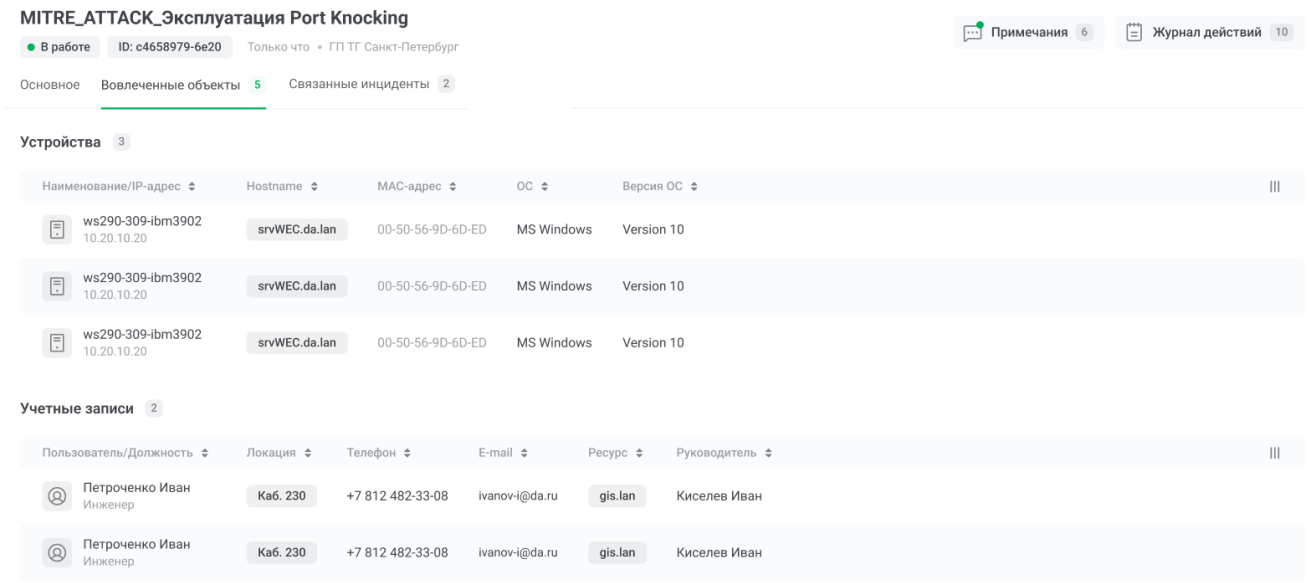


Рисунок 4.15 – Вовлеченные объекты

При нажатии на пиктограмму «›», слева от наименования объекта, откроется диаграмма (таймлайн) с сессиями и сеансами на данном объекте (устройстве) (рисунок 4.16).

Сессия – временной интервал, который начинается с события входа и завершается событием выхода пользователя. Сессии обозначены серым цветом. Сеанс – промежуток времени в рамках сессии, когда пользователь имеет доступ к интерфейсу операционной системы. Обозначены цветными интервалами в рамках сессий.

Период представления информации – одна неделя до возникновения инцидента и один день после. Красной вертикальной полосой обозначен момент, когда был зафиксирован инцидент. Для каждой сессии выводится информация о типе подключения (удаленный, локальный) и длительности сеансов.

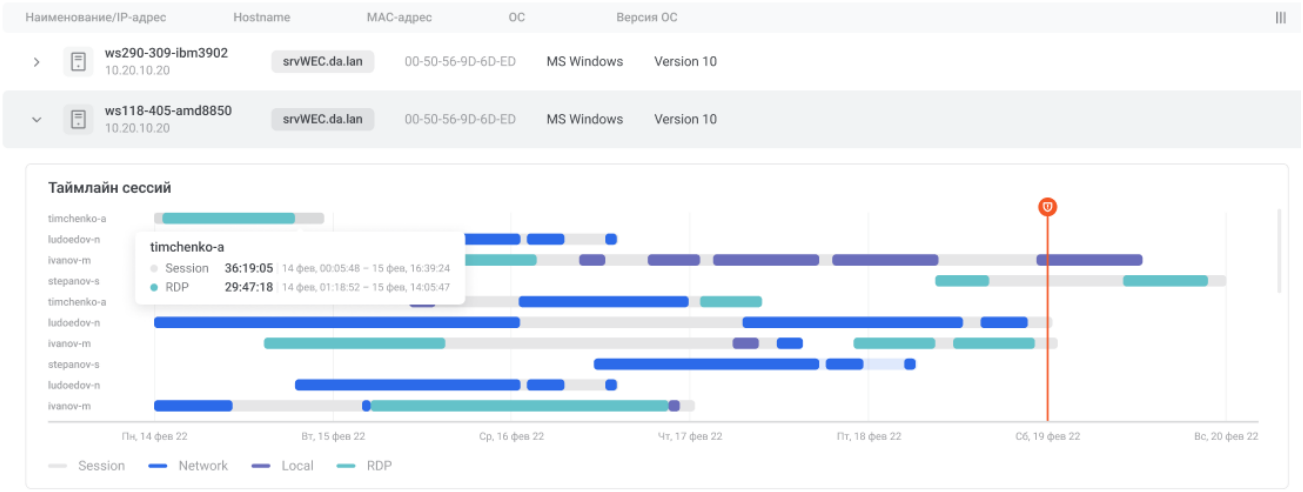


Рисунок 4.16 – Вовлеченные объекты

При нажатии на наименование объекта произойдет переход к карточке данного объекта.

4.4.2.3 Связанные инциденты

На вкладке отображаются инциденты, связанные с текущим инцидентом. Для добавления связи с другим инцидентом нажать кнопку «Добавить», в правом верхнем углу, отметить инциденты, с которыми необходимо добавить связь и нажать кнопку «Сделать связку» (рисунок 4.17).

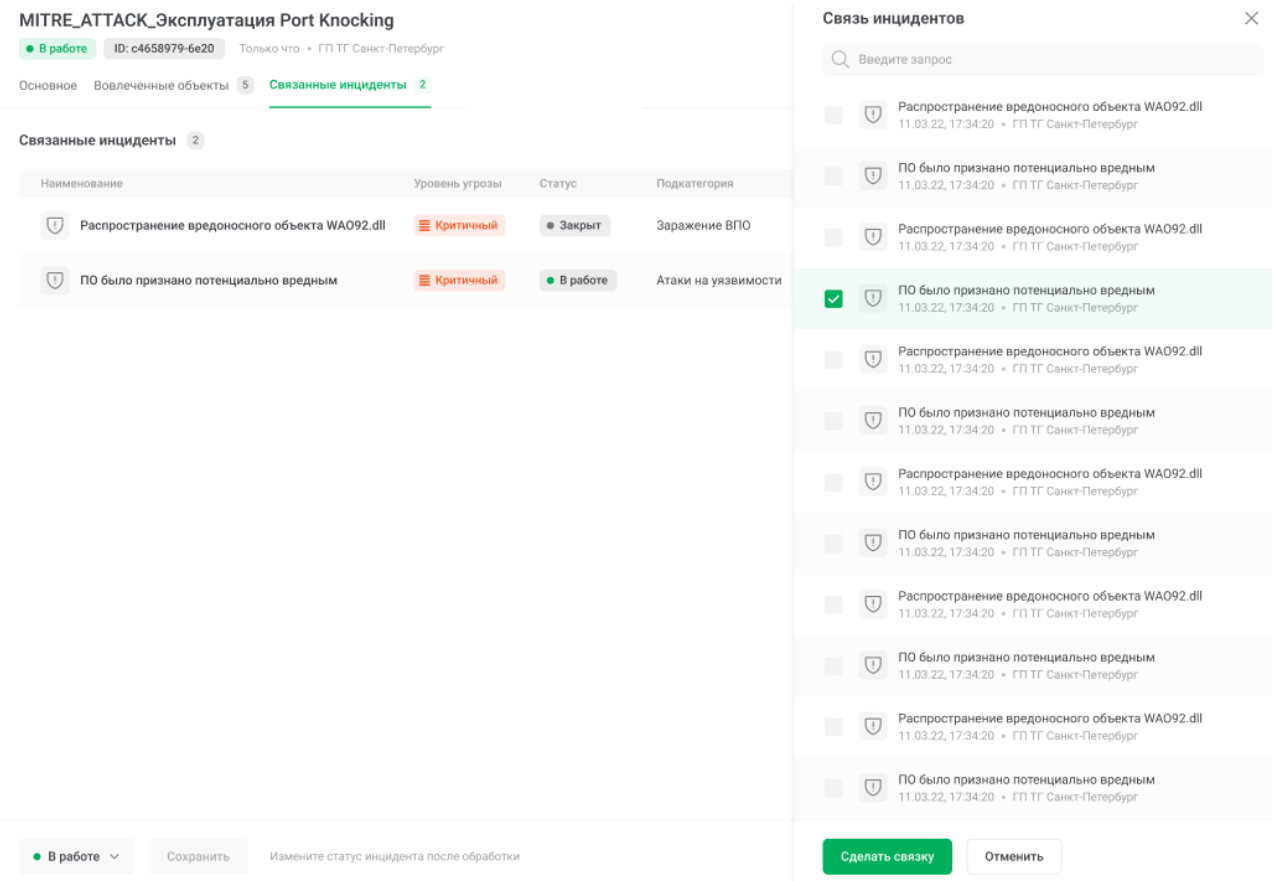


Рисунок 4.17 – Связанные инциденты

При нажатии на наименование связанного инцидента в таблице, осуществляется переход к карточке выбранного инцидента.

4.5 Работа с алертами

4.5.1 Алерты

Страница «Алерты» предназначена для оперативного просмотра информации о возникающих событиях, подозрительного (нетипичного) поведения, зафиксированного программными анализаторами Ankey ASA. Представляет собой список с информацией о зафиксированных алертах, набор фильтров и информационные панели с общими данными (рисунок 4.18).

Примечание. Данные об алертах по умолчанию хранятся в системе в течение 90 дней.

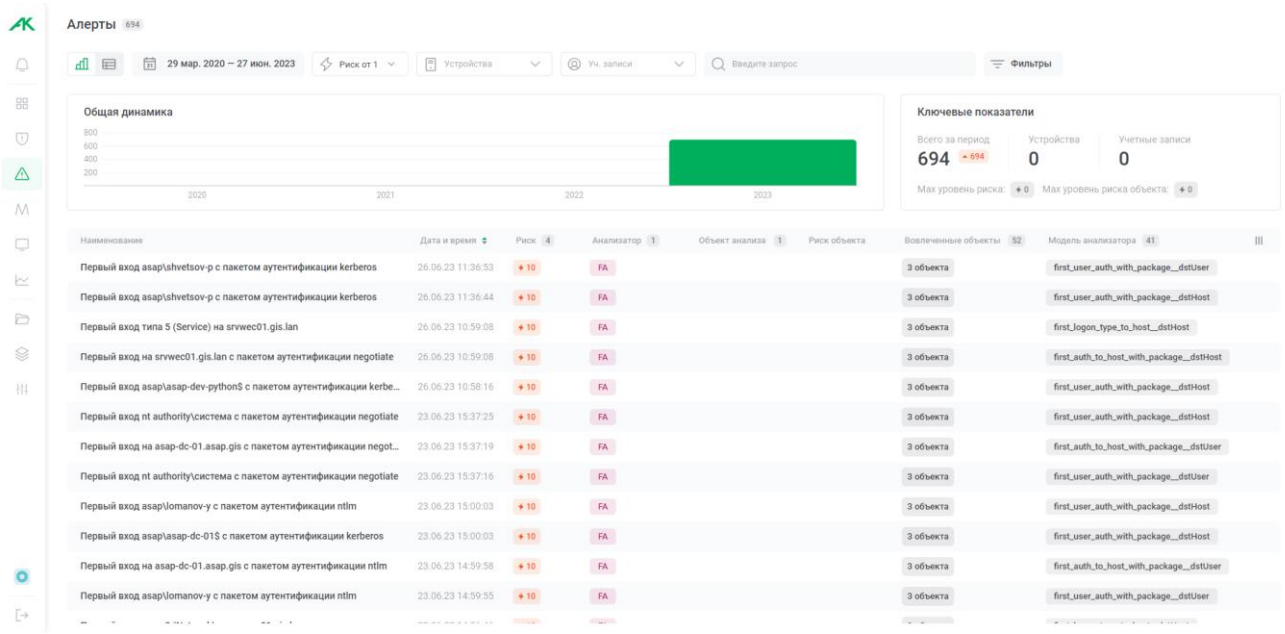


Рисунок 4.18 – Страница алертов

На странице показана следующая информация:

1. Информационные виджеты:

– общая динамика (столбчатая диаграмма, отображающая количество зафиксированных алертов за выбранный период) (рисунок 4.19);

– ключевые показатели (информационная панель, отображающая основные показатели) (рисунок 4.19).

Рисунок 4.19 – Виджеты на странице «Алерты»

Виджеты могут быть отключены, для этого нажать на пиктограмму « ».

2. Список алертов.

Перечень алертов представлен в виде списка, по умолчанию, отсортированных по дате фиксирования (рисунок 4.20).

Для каждого алерта в списке приводится следующая информация:

– наименование;

– дата и время фиксации алерта;

– уровень риска (отображает уровень риска, закрепленный за алертом данного типа);

– анализатор (сокращенной наименование анализатора, зафиксировавшего алерт). При наведении на поле отображается полное наименование анализатора;

– объект анализа (на котором был зафиксирован алерт). При наведении на поле, доступны функции «Добавить фильтр», нажав на пиктограмму « », для добавления фильтра, отображающего алерты, связанные с данным объектом, и «Перейти в карточку объекта», нажав на пиктограмму « »;

– риск объекта (сумма уровня рисков всех алертов, в которых был задействован данный объект);

– вовлеченные объекты. При наведении на поле отображаются наименования вовлеченных объектов;

– модель анализатора (развернутое наименование анализатора, зафиксировавшего алерт).

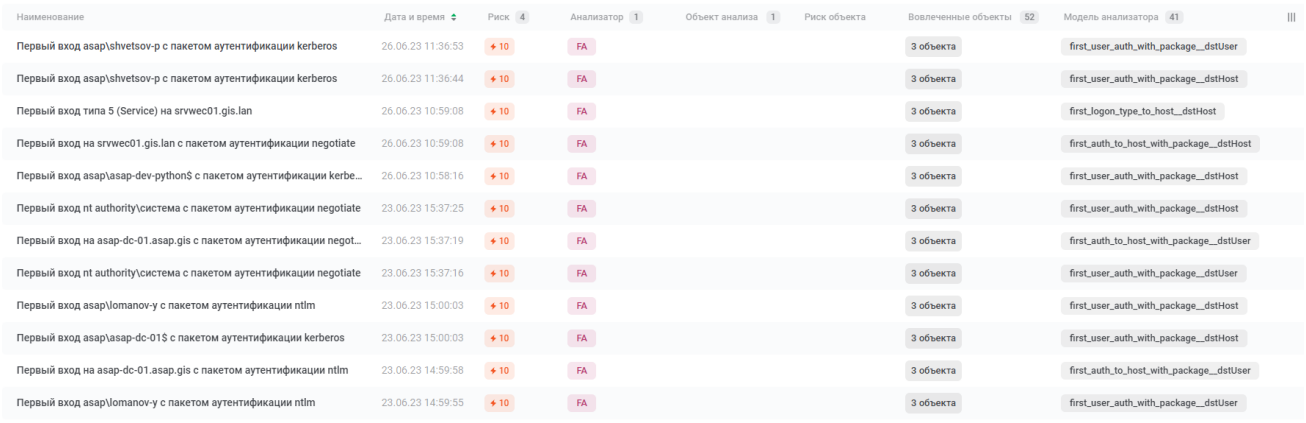


Рисунок 4.20 – Список алертов

Список алертов обновляется в режиме реального времени, в соответствии с установленным фильтром по дате (за исключением фильтра по заданному периоду).

Справа от названия столбцов может располагаться переключатель сортировки « », при нажатии на который, алерты будут отсортированы по значениям данного столбца (в этом случае, данные перестанут актуализироваться, до отключения соритровки).

Справа от названия столбцов может распологаться счетчик « 34 », отображающий количество значений в этом столбце. При наведении на него появляется окно (рисунок 4.21), предостовляющее информацию о 10 наиболее часто встречающихся значениях в порядке убывания.

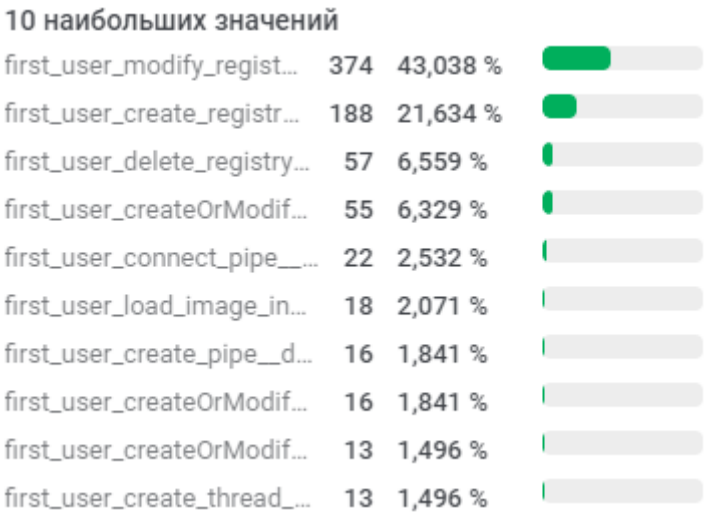


Рисунок 4.21 – 10 наибольших значений

Доступна возможность изменения перечня столбцов в таблице, для этого необходимо нажать на пиктограмму «» и в появившемся окне скрыть или отобразить значения, нажатием на пиктограмму «» справа от названия.

Примечание. При поступлении алертов в режиме реального времени не производится завершение сессии пользователя при неактивности, в случае открытой страницы «Алерты».

3. Фильтры

К списку алертов можно применить фильтры по анализаторам указанным в Таблица 4.3. На наличие выбранных фильтров указывает зеленая точка над пиктограммой фильтра «» или «», как показано на рисунке 4.22.

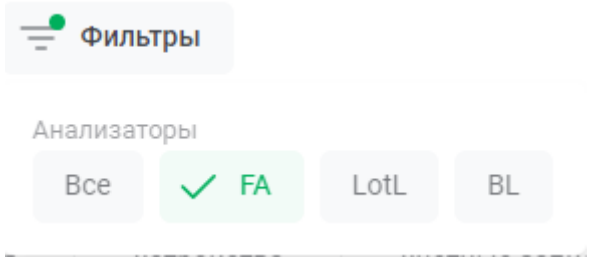


Рисунок 4.22 - Фильтры для списка алертов

Таблица 4.3 – Фильтры для списка алертов

Фильтр	Описание
Все	Отображение всех алертов
FA	Отображение алертов, обнаруженных при помощи анализатора первого действия
LotL	Отображение алертов, обнаруженных при помощи анализатора lotL (подозрительное поведение легитимных программ и функций системы)

Фильтр	Описание
BL	Отображение алертов, обнаруженных при помощи анализатора отклонения от базовой линии

Установленные фильтры закрепляются за пользователем и действуют при следующем входе в систему.

Также в списке алертов можно выполнять поиск по другим параметрам (рисунок 4.23):

– заданным временным рамкам фиксации алерта;

– уровень риска выше заданного значения (диапазон значений от 0 до 55);

– конкретным устройствам в меню выбора;

– конкретным учетным записям в меню выбора;

– наименованию алерта в поисковой строке.

Рисунок 4.23 – Поиск по алертам

4. Информация по алерту.

Для выбора алерта необходимо кликнуть на его название в списке. В правой части страницы отобразится панель с подробной информацией об алерте.

4.5.2 Информация по алерту

На странице «Алерты» доступен просмотр подробных сведений о каждом зафиксированном алерте. Для просмотра необходимо нажать на один из них (рисунок 4.24).

Для отображения информации по другому алерту, необходимо выбрать следующий алерт из списка.

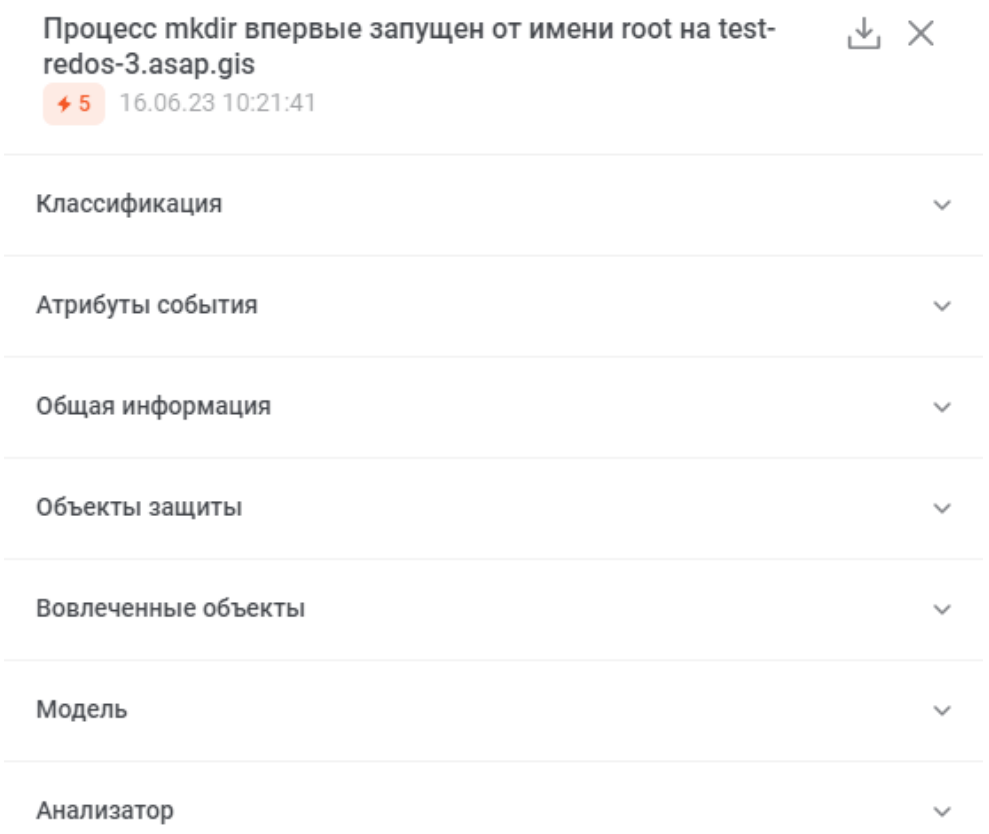


Рисунок 4.24 – Просмотр алерта

Панель с информацией об алерте состоит из заголовка панели и 7 вкладок, содержащих в себе различные перечни подпунктов, в зависимости от разновидности выбранного алерта:

1. Заголовок панели - предоставляет основную информацию об алерте – название, уровень риска и дату фиксации.

2. Классификация - раздел предоставляет информацию об классификации алерта, по различным метрикам и методам обнаружения.

3. Атрибуты события – раздел предоставляет информацию о свойствах и характеристиках алерта.

4. Общая информация – раздел предоставляет базовую информацию об алерте – id, сроки алерта и его фиксации и тд.

5. Объекты защиты – раздел предоставляет информацию об устройстве и учетной записи, на которых был зафиксирован алерт.

6. Вовлеченные объекты – раздел предоставляет информацию об устройствах, учетных записях, файлах и процессах, вовлеченных в алерт.

7. Модель – модель предоставляет информацию о модели поведения и уровне риска алерта.

8. Анализатор – раздел предоставляет информацию об анализаторе, зафиксировавшем алерт.

Для скачивания информации по алерту в формате JSON, нажать на пиктограмму «  ».

Для закрытия информации по алерту нажать на пиктограмму «  ».

4.6 Работа с Mitre ATT&CK

4.6.1 Общая информация Mitre ATT&CK

Страница «Mitre ATT&CK» (рисунок 4.25) предназначена для мониторинга алертов, сгруппированных по моделям возможных атак, для оперативного анализа и прогнозирования действий. На странице отображается список техник и тактик по системе классификации Mitre ATT&CK в табличном виде и набор фильтров и настроек для нее.

Техники расположены в таблице согласно базе знаний и системе классификаций действий злоумышленников. В названии столбцов указано название тактики и количество ее зафиксированных реализаций. В содержании столбцов указаны конкретные техники и количество их зафиксированных реализаций. В зависимости от количества зафиксированных реализаций блоки с техниками и тактиками меняют цвет в сторону красного.

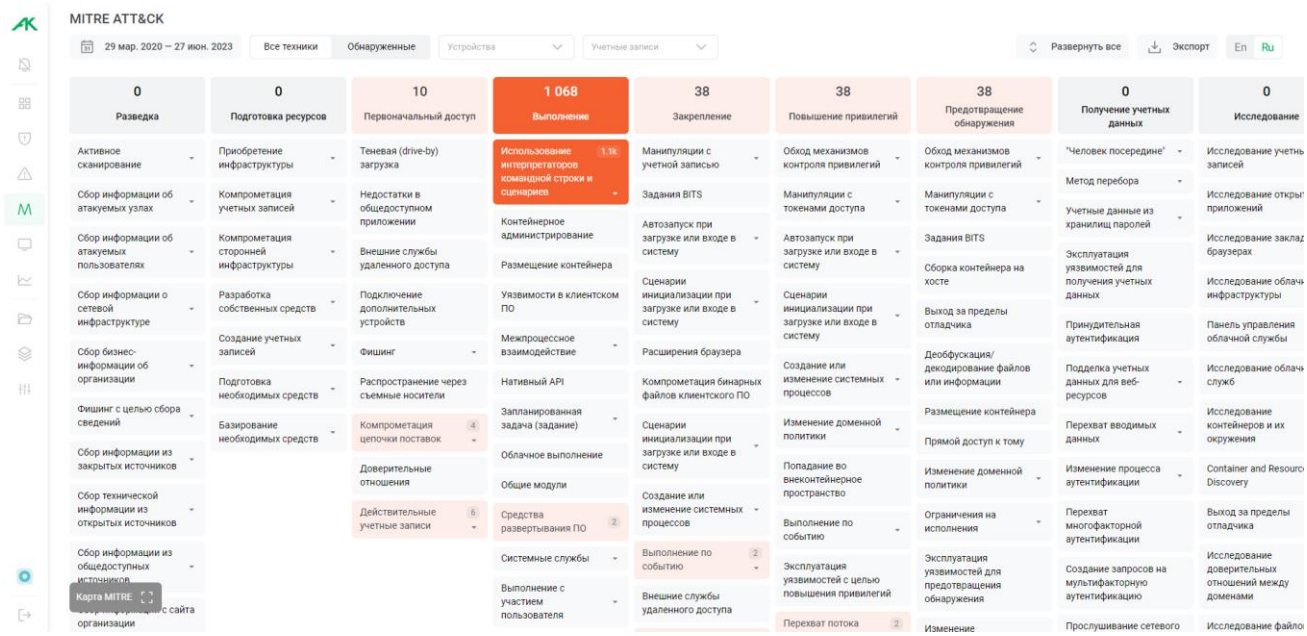


Рисунок 4.25 – Страница Mitre ATT&CK

4.6.2 Фильтрация по таблице техник

К таблице техник могут быть применены следующие фильтры (рисунок 4.26):

– фильтр по дате. Можно выбрать временной промежуток из стандартного перечня или задать свой период;

– фильтр по обнаружению техники. Доступен выбор между вариантами «Все техники», отображающей все возможные техники и «Обнаруженные», отображающей только техники с зафиксированными реализациями;

– фильтр по устройству. Можно выбрать «Все устройства» для отображения информации о всех доступных устройствах или отметить только необходимые, поставив галочку слева от наименования в выпадающем списке. Также доступен поиск по устройствам при помощи ввода запроса в строку поиска. Поиск начинается как только вводится первый символ запроса.

– фильтр по учетной записи. Можно выбрать «Все учетные записи» для отображения информации о всех доступных учетных записях или отметить только необходимые, поставив галочку слева от наименования. Также доступен поиск по учетным записям при помощи ввода запроса в строку поиска. Поиск начинается как только вводится первый символ запроса.

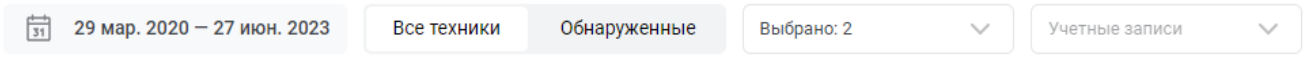


Рисунок 4.26 – Фильтры Mitre ATT&CK

4.6.3 Действия с таблицей техник

Техники могут содержать тематически связанные техники. Для сворачивания или разворачивания блоков со связанными техниками, нажать на кнопку «Развернуть все» / «Свернуть все».

Таблицу с техниками можно сохранить в формате PNG. Для этого нажать на пиктограмму « 

».

Для отображения таблицы техник на другом языке (доступны русский и английский) нажать на переключатель « 

».

В левом нижнем углу страницы расположена кнопка «Карта Mitre» (рисунок 4.27), при нажатии на которую разворачивается окно (рисунок 4.28) для более удобной и быстрой навигации по таблице техник.

Рисунок 4.27 – Карта Mitre ATT&CK (свернутая)

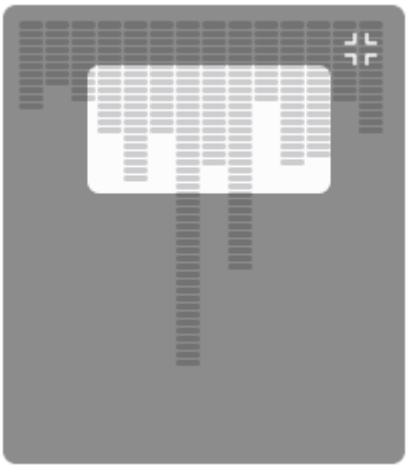


Рисунок 4.28 – Карта Mitre ATT&CK (развернутая)

4.6.4 Карточка техники

При нажатии на блок с техникой в таблице открывается ее карточка. В верхней части карточки указано название техники, ее id идентификатор (подразделы техник, имеют id, разделенный точкой), дата создания, последнего изменения и 4 вкладки:

– алерты. Отображает алерты, отнесенные к данной технике, карточка предоставляет информацию о наименовании, уровне риска, объекте анализа и времени фиксации.;

– учетные записи. Отображает устройства, отнесенные к данной технике, карточка предоставляет информацию о наименовании, уровне риска, локации, телефоне, почте и домене;

– устройства. Отображает устройства, отнесенные к данной технике, карточка предоставляет информацию о наименовании/ip-адресе, уровне риска, hostname, Mac-адрес, ОС и версии ОС;

– описание. Отображает смысл выбранной техники и информацию о ней. Доступна ссылка для перехода на сайт «https://attack.mitre.org/», на страницу данной техники, для более подробного ознакомления.

Для вкладок «Алерты», «Учетные записи» и «Устройства», доступна возможность с помощью пиктограммы «  » зайти в настройки и отключить или включитть отображение выбранных пунктов, при нажатии на пиктограмму «  » справа. Также доступна возможность сортировки по выбранному столбцу, нажатием на пиктограмму «  » (при наличии).

4.7 Просмотр объектов анализа

4.7.1 Общая информация об объектах анализа

В разделе «Объекты анализа» (рисунок 4.29) представлена информация об устройствах и учетных записях (активах), полученных из сетевой модели Ankey SIEM либо Ankey SIEM NG и Active Directory.

На странице «Объекты анализа» показана следующая информация:

1. Информационные виджеты:

– количество активных объектов анализа за последние 7 дней;

– типы устройств (линейчатая диаграмма, отображающая количество устройств по типам);

– должности сотрудников (линейчатая диаграмма, отображающая количество сотрудников по должностям);

– департаменты (линейчатая диаграмма, отображающая количество объектов анализа по департаментам).

Для скрытия или отображения параметра на линейчатой диаграмме необходимо нажать на его название.

Виджеты могут быть отключены, для этого нажать на пиктограмму «  ».

2. Список объектов анализа.

Перечень объектов анализа приведен в виде списка и содержит следующую информацию:

– уровень риска;

– наименование объекта;

– динамика риска в графическом отображении;

– инциденты – количество инцидентов (при их наличии). При наведении отображается количество инцидентов по типам и уровню угрозы;

– алерты – количество алертов для объекта (при их наличии). При наведении отображаются алерты, отсортированные по уровню риска;

– роль;

– отметка административных объектов;

– IP-адрес объекта анализа;

– MAC-адрес объекта анализа;

– электронная почта;

– телефон;

– ответственный;

– организация.

Справа от названия столбца «Уровень риска» располагается переключатель сортировки «  », при нажатии на который, объекты будут отсортированы по уровню риска.

Доступна возможность изменения перечня столбцов в таблице, для этого, необходимо нажать на пиктограмму «  » и в появившемся окне, скрыть или отобразить значения, при нажатии на пиктограмму «  », справа от названия.

3. Фильтры.

По умолчанию отображаются все объекты анализа, которые при необходимости можно отфильтровать, для этого выбрать «Учетные записи» или «Устройства».

Для поиска по объектам анализа необходимо ввести запрос в строку поиска и нажать клавишу Enter.

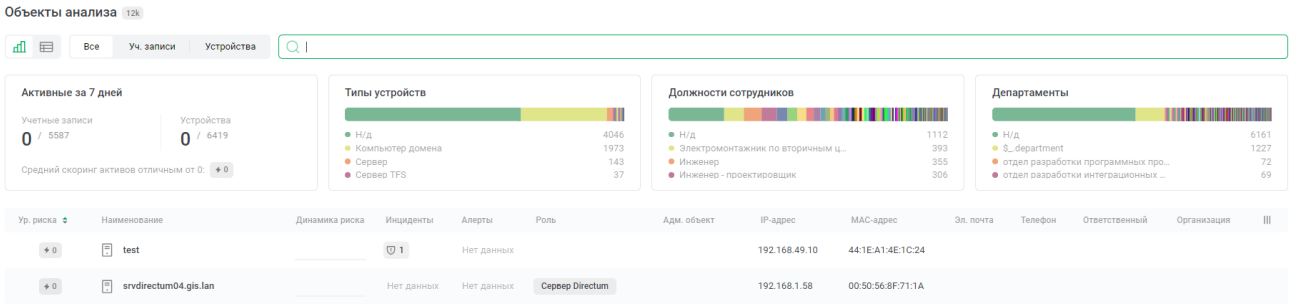


Рисунок 4.29 – Объекты анализа

4.7.2 Карточка объекта анализа

Для перехода к карточке объекта анализа необходимо выбрать интересующий актив из списка.

Примечание. Срок хранения объектов анализа с момента их последнего обновления составляет 365 дней.

Карточка устройства содержит следующие вкладки:

– сводка;

– информация (доступно только на вкладке «Учетные записи»);

– основные (доступно только на вкладке «Устройства»);

– инциденты;

– таймлайн;

– отчеты EfrosCI (доступно только на вкладке «Устройства»);

– уязвимости (доступно только на вкладке «Устройства»).

Примечание. Данные во вкладке «Отчеты EfrosCI» и «Уязвимости» отображаются только при интеграции с Efros CI и Ankey SIEM VM соответственно и наличия соответствующих лицензий.

В верхней части карточки показана основная информация об объекте анализа – название, статус (при наличии), уровень риска и ip адрес (устройства) или id идентификатор (учетной записи).

Для вкладок «Инциденты» и «Уязвимости», доступна возможность с помощью пиктограммы «» зайти в настройки и отключить или включить отображение выбранных пунктов, путем нажатия на пиктограмму «» справа. Также доступна возможность сортировки по выбранному столбцу, нажатием на пиктограмму «» (при наличии).

4.7.2.1 Сводка

На вкладке «Сводка» (рисунок 4.30) могут располагаться виджеты:

– Внешний риск. Отображает схему вектора внешнего риска и значение ключевых показателей, по которым она составлена.

– График со скорингом. Отображает уровень риска, инциденты и алерты, на протяжении выбранного промежутка времени «5 сент. 2020 – 14 сент. 2023». Настройка графика скоринга и установка пороговых значений осуществляется в соответствии с пунктом 4.9.1.5.

– Важные события. Инциденты (пиктограмма «») и алерты (пиктограмма «»), в которых был задействован объект анализа. Разделение списка событий идет по временным промежуткам, каждое событие имеет наименование, время фиксации и уровень угрозы. Для просмотра подробной информации, необходимо нажать на строку инцидента или алерта, которая появится в правой части страницы. Информацию можно сохранить в формате «json», нажав на пиктограмму «».

– Внутренний риск. Отображает схему вектора внутреннего риска и значение ключевых показателей, по которым она составлена.

– ТОП-10 (10 наиболее часто встречающихся алертов).

Создание виджетов, при их отсутствии на вкладке «Сводка», осуществляется с помощью кнопки «Добавить». Для добавления виджетов на сводку нажать на кнопку «Библиотека виджетов» в правом верхнем углу, выбрать виджеты и нажать «Добавить».

Для удаления виджета навести курсор на виджет и нажать на пиктограмму «» в правом верхнем углу. Для перемещения виджета навести курсор на виджет, нажать на пиктограмму «» и, удерживая курсор, переместить виджет в другое место на странице.

Примечание. Набор виджетов и период, выбранный для одного объекта, отображается во вкладке «Сводка» для всех объектов анализа.

Рисунок 4.30 – Сводка объекта анализа

4.7.2.2 Информация

На вкладке «Информация» показана информация об объекте анализа. Вкладка доступна только при выборе объекта анализа – «Учетная запись».

Поле с информацией можно скопировать, для этого необходимо навески на поле и нажать пиктограмму « ».

4.7.2.3 Основное

На вкладке «Основные» показана общая и системная информация об устройстве. Вкладка доступна только при выборе объекта анализа – «Устройство».

Поле с информацией можно скопировать, для этого необходимо навески на поле и нажать пиктограмму « ».

4.7.2.4 Инциденты

На вкладке «Инциденты» представлена таблица с перечнем инцидентов, в которых был задействован объект анализа (рисунок 4.31). Для того, чтобы перейти к карточке инцидента, необходимо нажать на наименование инцидента (пункт 4.4.2).

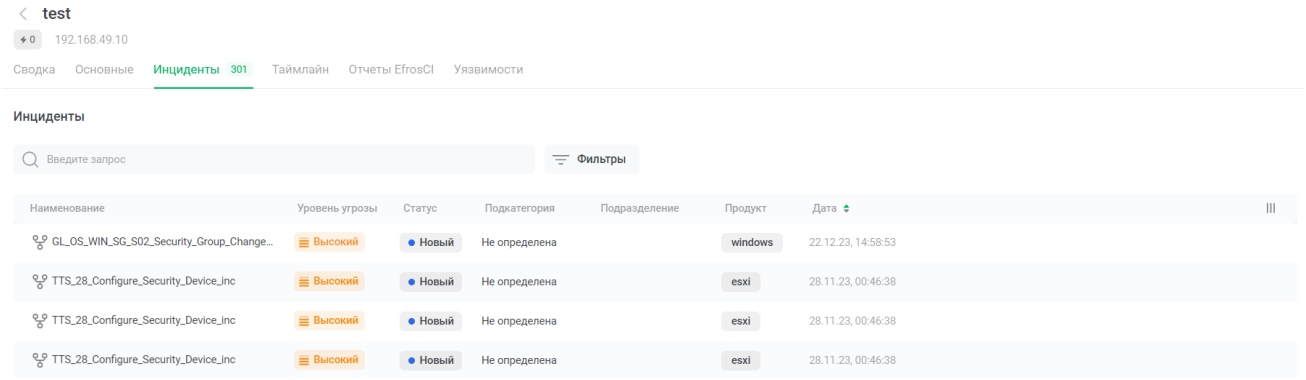


Рисунок 4.31 – Инциденты устройства

4.7.2.5 Таймлайн

Вкладка «Таймлайн» содержит график, где показаны инциденты (пиктограмма «»), алерты (редкие действия объекта или на объекте, пиктограмма «») и базовые события (пиктограмма «») (рисунок 4.32). Под графиком данная информация отображена в хронологическом порядке в виде записей.

Инциденты обозначены отметками зеленого цвета, алерты – отметками серого цвета на шкале под графиком. Базовые события представлены областью серого цвета на графике.

Примечание. По умолчанию данные о базовых событиях хранятся в системе 30 дней, данные об алертах – 90 дней.

Для фильтрации записей можно использовать боковые ползунки, расположенные по бокам от графика. Отображаемая область с данными окрашена зеленым цветом. Также для фильтрации по дате можно использовать календарь над графиком. Для фильтрации событий по категориям предназначен фильтр над графиком.

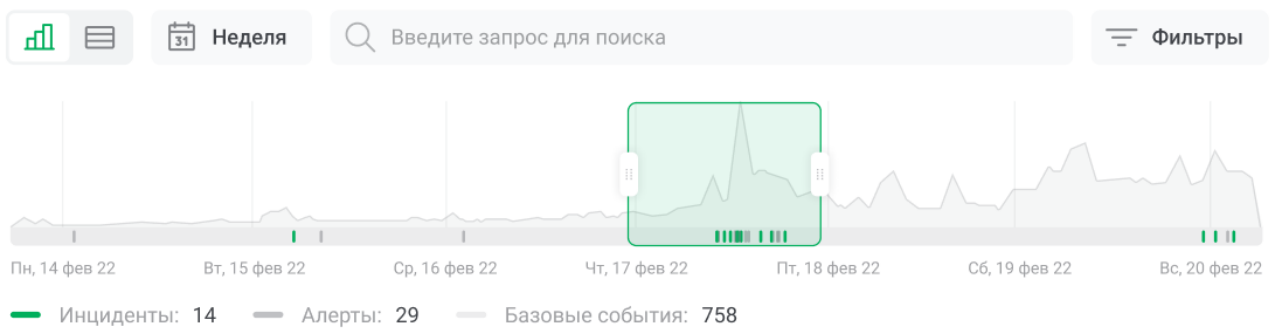


Рисунок 4.32 – График на вкладке «Таймлайн»

Для просмотра подробной информации, необходимо нажать на строку с записью о событии. Информация будет показана в правой части страницы.

4.7.2.6 Отчеты EfrosCI

Вкладка «Отчеты EfrosCI» предоставляет функционал просмотров отчетов из системы EfrosCI. Если отчеты на странице отсутствуют, необходимо нажать на кнопку « 

».

4.7.2.7 Уязвимости

Вкладка «Уязвимости» предоставляет информацию о возможных уязвимостях устройства. На странице представлена таблица (рисунок 4.35) со следующими колонками:

– наименования/описание. Представляет собой наименование уязвимости, под ним, идет краткой описание. При наведении на поле, можно прочитать описание целиком;

– CVSS. Представляет собой количественную оценку уязвимости, по системе открытого стандарта Common Vulnerability Scoring System version 3 (рисунок 4.33), в диапазоне о 0 до 10;

– уровень опасности. Отображает уровень опасности уязвимости, в соответствии с количественной оценкой по системе CVSSv3;

Не определено	0
Низкий	0.1-3.9
Средний	4.0-6.9
Высокий	7.0-8.9
Критический	9.0-10.0

Рисунок 4.33 – Шкала CVSS

– статус. Отражает статус уязвимости, в зависимости от ее давности;

– идентификаторы. Предоставляет идентификатор уязвимости в базе общеизвестных уязвимостей информационной безопасности (CVE). При нажатии на поле, будет открыт сайт NVD, с подробным описанием рассматриваемой уязвимости;

– вектор. Предоставляет информацию (при наличии) о параметрах расчета базовой оценки уязвимости по системе CVSSv3. При наведении на поле, появляется

окно с визуальным отображением, в виде схемы, вектора атак и значением ключевых показателей, по которым она составлена (рисунок 4.34).

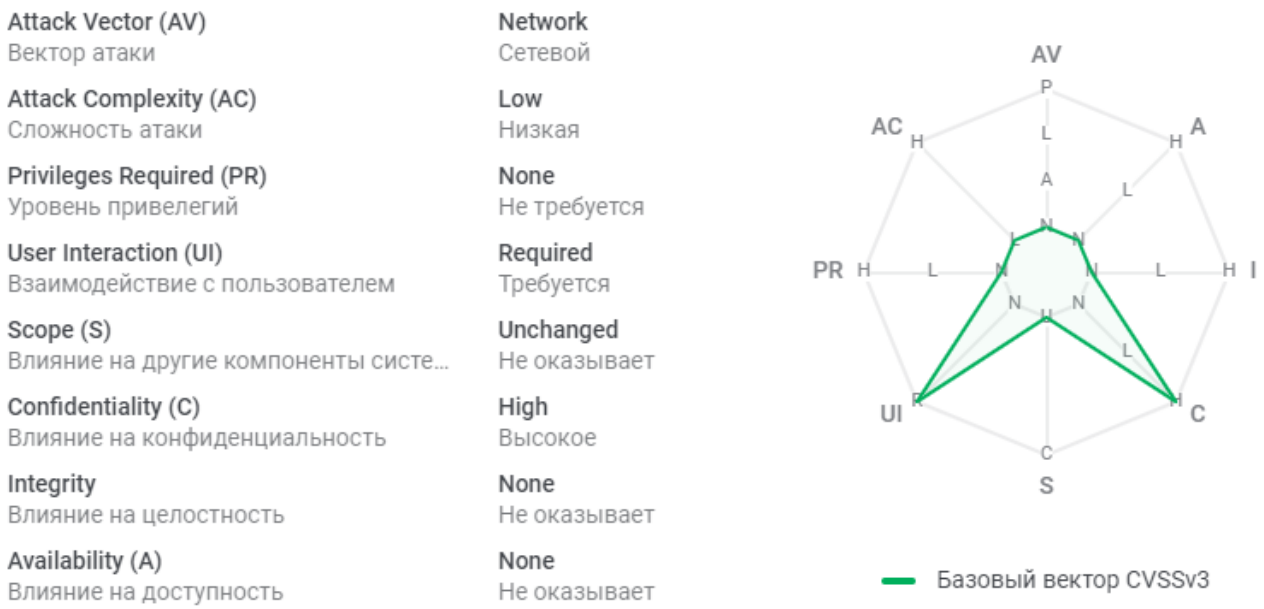


Рисунок 4.34 – Вектор атаки

– дата обнаружения.

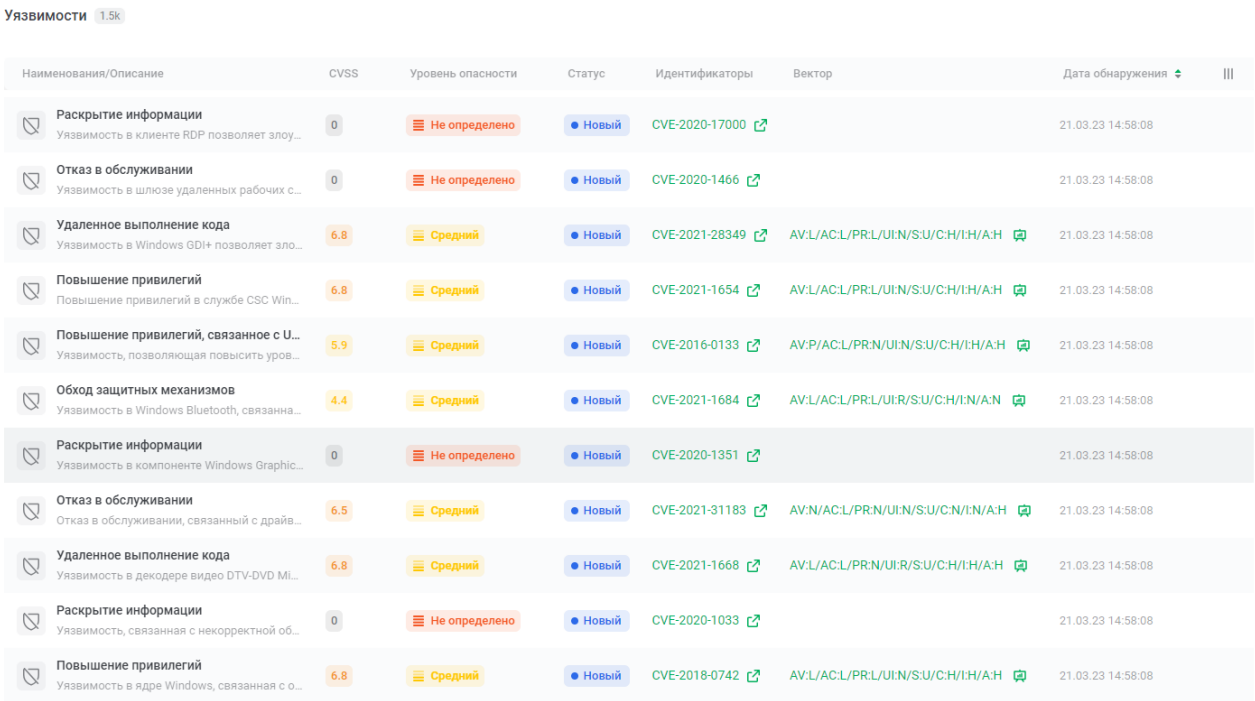


Рисунок 4.35 – Вкладка «Уязвимости»

Для выбора уязвимости необходимо кликнуть на ее название в списке. В правой части страницы отобразится карточка с подробной информацией об уязвимости.

При нажатии на поле «Идентификаторы» откроется сайт NVD, с подробным описанием рассматриваемой уязвимости.

Карточка уязвимости может содержать информацию (при наличии) о параметрах расчета оценки уязвимости по системе CVSSv2 и CVSSv3. При наведении на поле, появляется окно с визуальным отображением, в виде схемы, вектора атак и значением ключевых показателей, по которым она составлена

4.8 Центр аналитики

На вкладках раздела «Центр аналитики» представлены страницы с аналитическими панелями (дашбордами) для проведения визуального анализа данных.

Содержимое страниц состоит из объектов визуализации и фильтров. Отфильтровать данные можно также с помощью нажатия на объект визуализации.

4.9 Работа со справочниками

Справочники предназначены для ведения (формирования, изменения) справочной информации, используемой для настройки представления данных в системе.

Работа со справочниками производится на странице «Справочники» (рисунок 4.36). Справочники объединены в группы. Для просмотра справочников группы нажать на пиктограмму «›» слева от названия группы.

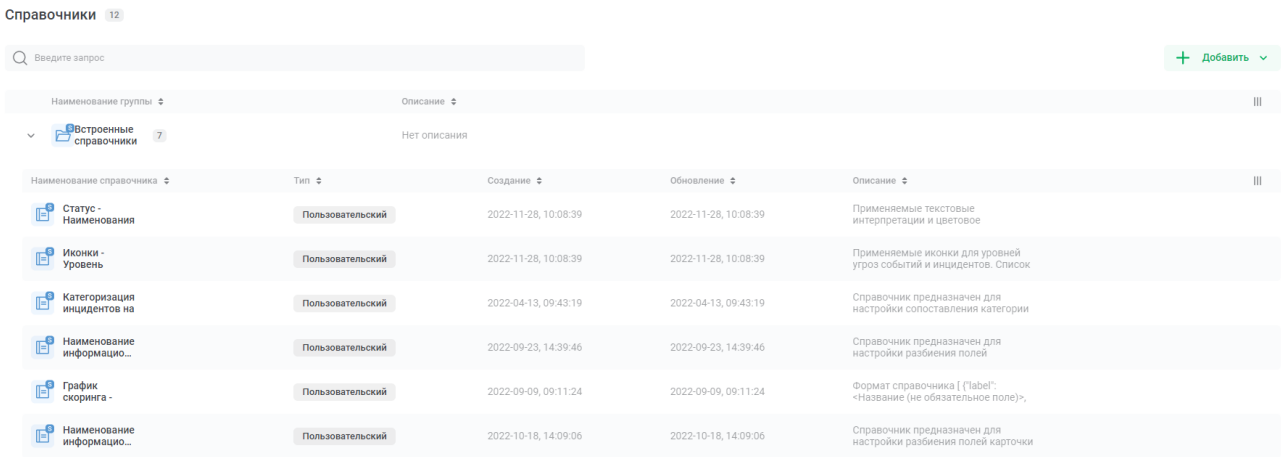


Рисунок 4.36 - Страница «Справочники»

Встроенные справочники и группы обозначены синим цветом, их удаление или переименование невозможно. Описание встроенных справочников приведено в 4.9.1.

Помимо встроенных справочников есть возможность создания собственных справочников.

Предусмотрены следующие форматы справочников (рисунок 4.37):

– список;

– ключ – значение;

– ключ – массив;

– пользовательский. Предназначен для создания справочника в пользовательском формате «JSON».

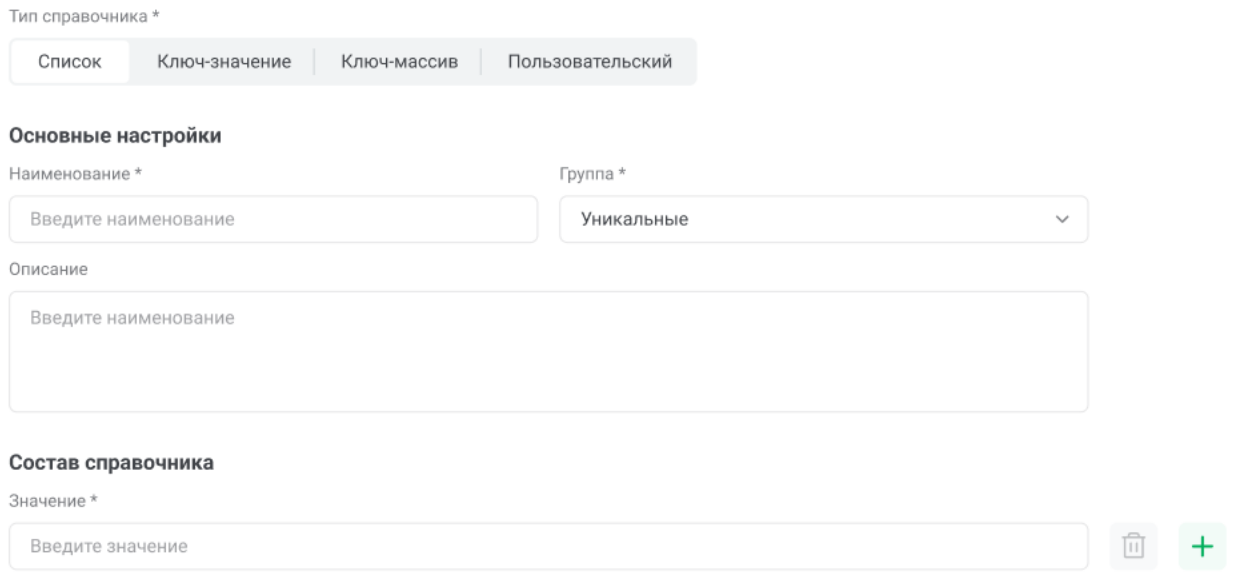


Рисунок 4.37 – Типы справочников

4.9.1 Встроенные справочники

В системе предусмотрены следующие встроенные справочники:

1. Статус - Наименования и цвет.

2. Иконки – Уровень угрозы.

3. Категоризация инцидентов на основе типа.

4. Наименование информационных блоков карточки инцидента.

5. График скоринга – вспомогательная линия, масштабирование и цвет (не используется в модуле Мониторинга).

6. Наименование информационных блоков карточки учетной записи.

7. Наименование информационных блоков карточки устройства.

4.9.1.1 Справочник «Статус - Наименования и цвет»

Справочник «Статус - Наименования и цвет» предназначен для настройки текстового и цветового представления статусов инцидентов (рисунок 4.38). В поле «Описание» справочника приведен используемый формат.

Формат справочника:

```
[
 {
  "key": "<Статус>",
  "value": "<Текстовая интерпретация>",
  "color": "<Цвет в HEX>"
 },
  ... ,
 {
  "key": "<Статус>",
  "value": "<Текстовая интерпретация>",
  "color": "<Цвет в HEX>"
 }
]
```

Значение поля «key» используется в системе и не должно быть изменено.

Значение поля «value» определяет название статуса инцидента, отображаемого в списке на странице «Инциденты» (рисунок 4.38) и в шапке карточки инцидента.

Значение поля «color» определяет цвет маркера для статуса в формате HEX.

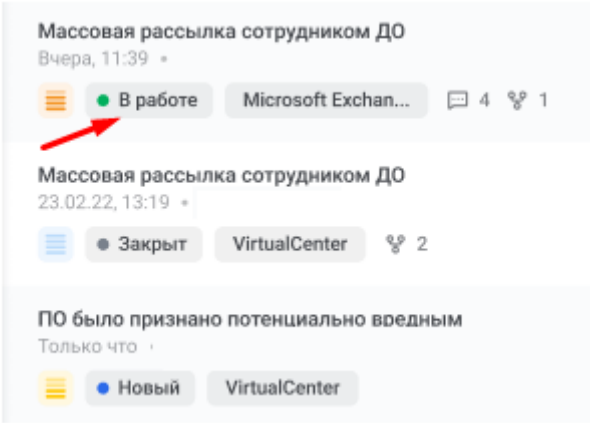


Рисунок 4.38 – Список инцидентов

В разделе «Состав справочника» приведены значения, используемые по умолчанию. При необходимости, значения для «value» и «color» могут быть изменены.

4.9.1.2 Справочник «Иконки - Уровень угрозы»

Справочник «Иконки - Уровень угрозы» используется для настройки наименования уровня угрозы и соответствующего графического изображения (рисунок 4.39).

В поле «Описание» справочника приведен используемый формат.

Формат справочника:

```
[
  "<Уровень угрозы>": {
          "label": "<Название>",
          "icon": "<Иконка>",
          },
   ... ,
  "<Уровень угрозы>": {
          "label": "<Название>",
          "icon": "<Иконка>",
          },
]
```

Значение «Уровень угрозы» совпадает со значением, поступающим в событии из SIEM-системы.

Значение поля «label» определяет название уровня угрозы, отображаемое в системе. Может быть изменено.

Значение поля «icon» определяет графическое изображение.

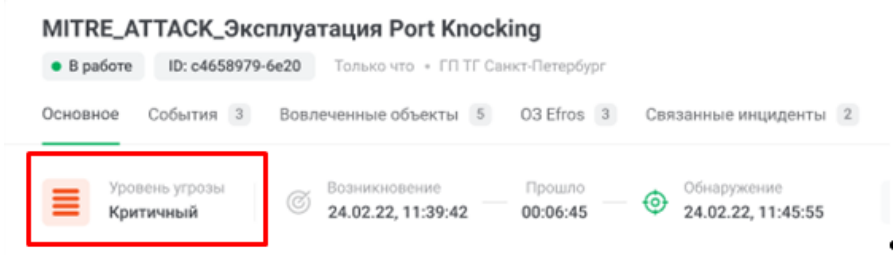


Рисунок 4.39 – Уровень угрозы

В разделе «Состав справочника» приведены значения, используемые по умолчанию. При необходимости, значения для «label» могут быть изменены.

4.9.1.3 Справочник «Категоризация инцидентов на основе типа»

Справочник «Категоризация инцидентов на основе типа» предназначен для настройки сопоставления категории и подкатегории инцидента на основе его типа, получаемого из SIEM-системы. Категория и подкатегория инцидента отображается в

карточке инцидента, в соответствующих полях в разделе «Информация по инциденту» (рисунок 4.40).

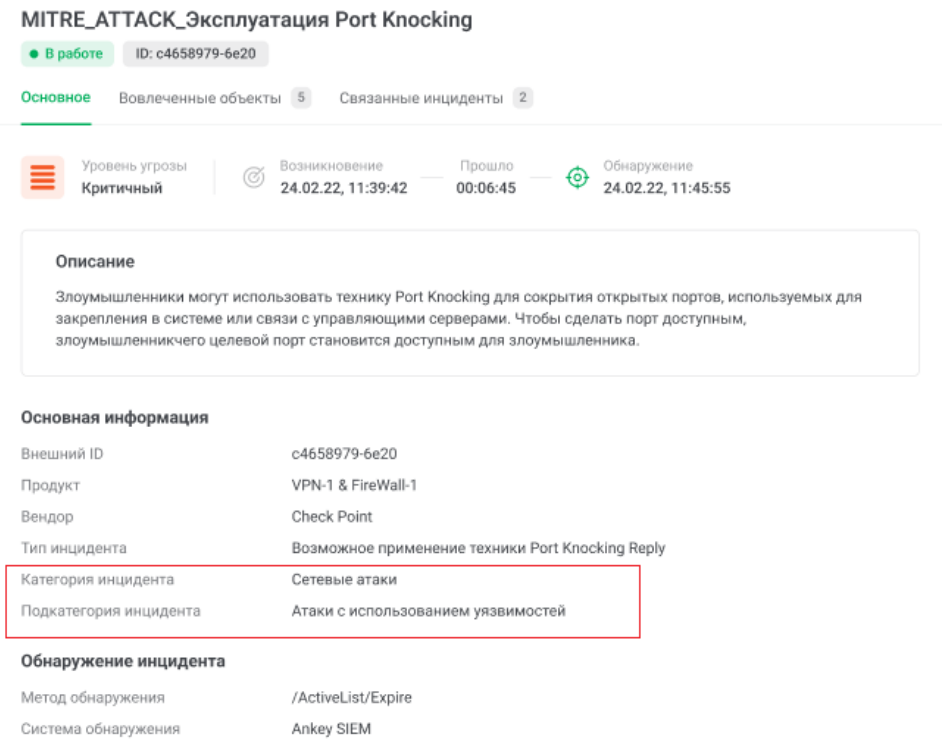


Рисунок 4.40 – Карточка инцидента

Формат справочника:

```
[
  {
   "category":<Наименование категории>,
   "subcategories": [
  {
   "subcategory": <Наименование подкатегории>,
   "types": [
     <Перечисление типов>    ]
  }
 ]
  },
   ...
]
```

Значение поля «category» устанавливает категорию для перечисленных типов.

Значение поля «subcategory» устанавливает подкатегорию для перечисленных типов.

Значения поля «types» определяют типы событий SIEM-системы, относящиеся к данной подкатегории.

В разделе «Состав справочника» приведены значения, используемые по умолчанию. В случае, если после внесения изменений в состав справочника, они не были применены на вновь поступивших инцидентах, может потребоваться перезапуск плагина «Унификация событий и инцидентов» в соответствии с руководством администратора.

4.9.1.4 Справочник «Наименование информационных блоков карточки инцидента»

Справочник «Наименование информационных блоков карточки инцидента» предназначен для настройки разбиения полей карточки инцидента на блоки.

Формат справочника:

```
[
{
"source": "<Наименование системы>",
        "groups": [
                {
                "name": "Наименование информационного блока",
                "fields": [
                        {
                        "label": "Наименование поля",
                        "value": "Ключ поля"
                        }
                ]
        }
]
},
...
]
```

Значение поля «source» устанавливает систему, из которой ПК «Ankey ASAP» получает инциденты («Ankey SIEM» или «Ankey SIEM NG»).

Значение поля «name» определяет наименование информационного блока, куда входят поля (рисунок 4.41).

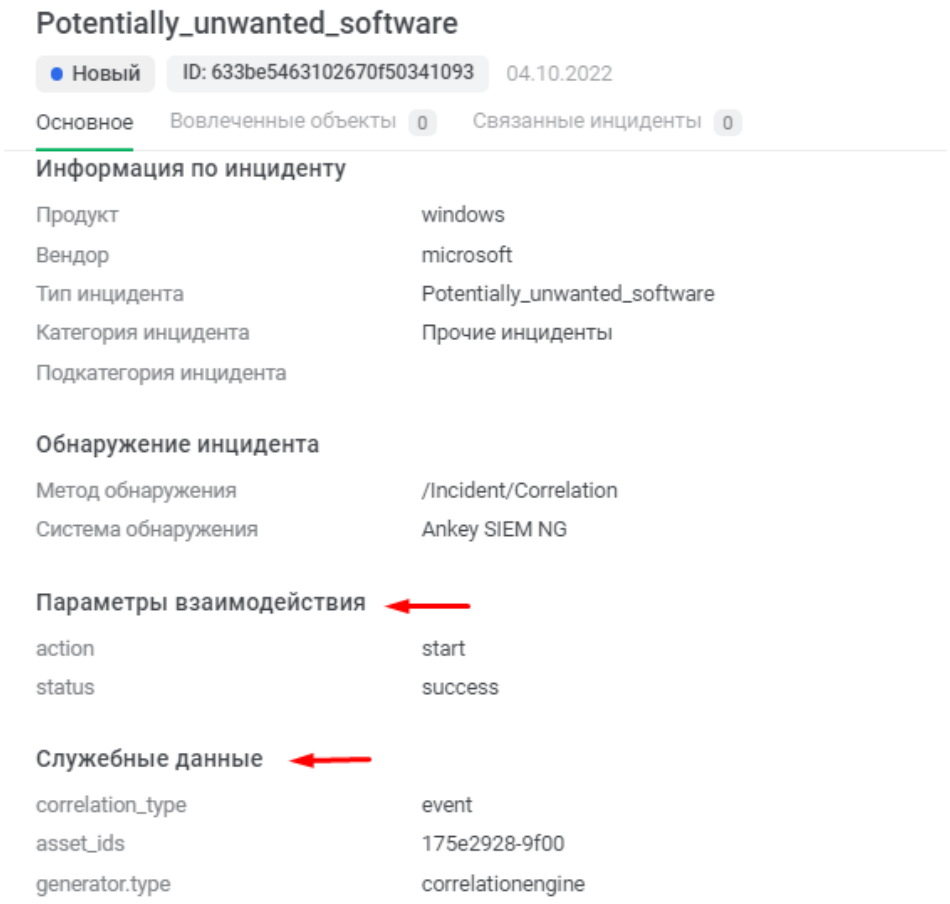


Рисунок 4.41 – Распределение полей в карточке инцидента

Значение поля «label» устанавливает отображаемое наименование поля события в карточке инцидента.

Значение поля «value» определяет поле события, поступившего из SIEM-системы.

В разделе «Состав справочника» приведены значения, используемые по умолчанию. При необходимости, значения для «label» могут быть изменены (столбец слева на рисунке 4.41).

4.9.1.5 Справочник «График скоринга – вспомогательная линия, масштабирование и цвет»

Справочник «График скоринга – вспомогательная линия, масштабирование и цвет» предназначен для настройки графика скоринга и установки пороговых значений.

Формат справочника:

```
[
 {
  "label": " Наименование поля ",
  "value": <Ключ поля>,
```

```
    "color": "Цвет в HEX",
    "type": " Текстовая интерпретация"
  },
  {
    "label": "Наименование поля",
    "value": <Ключ поля>
  }
]
```

Первое значение поля «label», задает название линии на графике (рисунок 4.42). Не является обязательным.

Значение поля «value», задает расположение линии на графике (рисунок 4.42).

Значение поля «color», задает цвет линии на графике (рисунок 4.42). Не является обязательным. В случае, если значение не задано – линия будет прозрачная.

Значение поля «type», задает тип линии на графике (рисунок 4.42). Доступно 3 значения:

– solid, сплошная линия, если значение не задано, является типом по умолчанию;

– dased,

– dotted, пунктирная линия.

Рисунок 4.42 – График скоринга со вспомогательной линией

В разделе «Состав справочника» приведены значения, используемые по умолчанию. При необходимости, значения для «value», «color», «type» могут быть изменены.

4.9.1.6 Справочники «Наименование информационных блоков карточки учетной записи», «Наименование информационных блоков карточки устройства»

Справочники «Наименование информационных блоков карточки учетной записи» и «Наименование информационных блоков карточки устройства» предназначен для настройки разбиения полей карточки объекта анализа (учетной записи и устройства) на блоки.

Формат справочника:

```
[
 {
        "name": "Наименование информационного блока",
        "fields": [
                {
                        "label": "Наименование поля",
                        "value": "Ключ поля"
                }
        ]
 },
 …
 ]
```

Значение поля «name» определяет наименование информационного блока на вкладке «Информация», куда входят поля (рисунок 4.43).

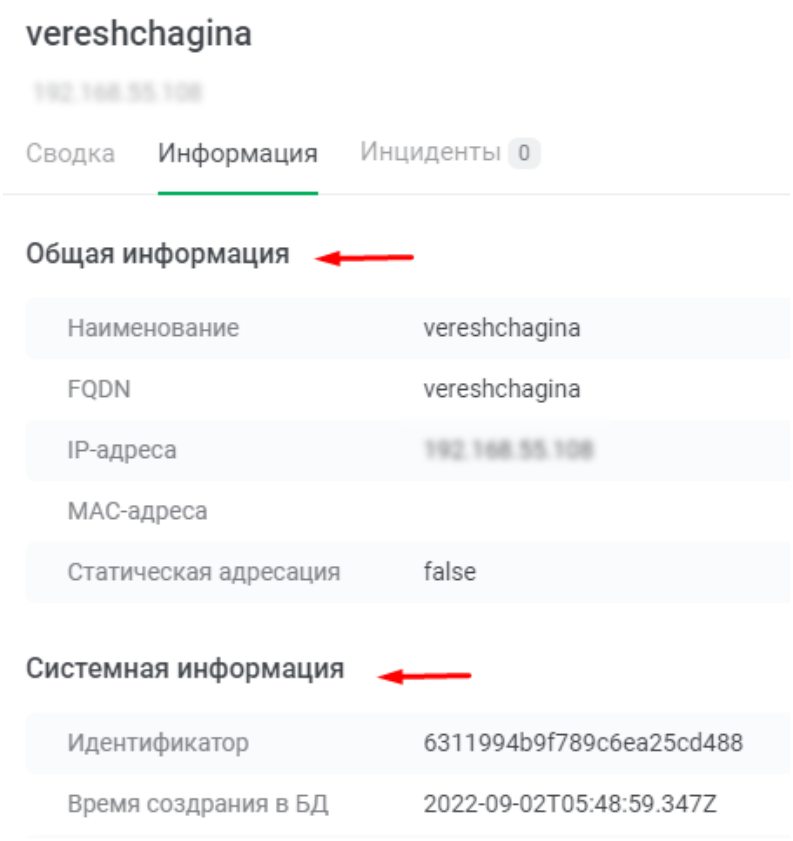


Рисунок 4.43 – Распределение полей в карточке инцидента

Значение поля «label» устанавливает отображаемое наименование поля события в карточке инцидента.

Значение поля «value» определяет поле события, поступившего из SIEM-системы.

В разделе «Состав справочника» приведены значения, используемые по умолчанию. При необходимости, значения для «label» могут быть изменены (столбец слева на рисунке 4.43).

4.9.2 Действия с группой справочников

Для создания группы справочников нажать на кнопку «Добавить» в правом верхнем углу страницы и выбрать «Группу». В открывшемся окне ввести наименование группы (должно быть уникальным) и описание (необязательное поле) группы и нажать кнопку «Добавить» (рисунок 4.44).

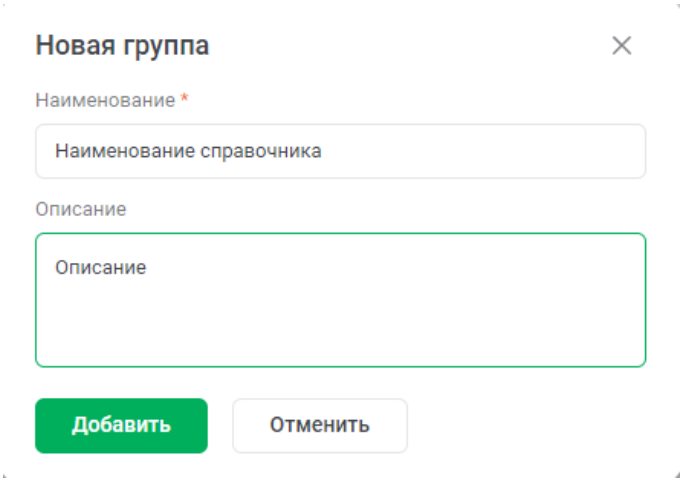


Рисунок 4.44 – Создание группы справочников

Доступны следующие действия с группой справочников, приведенные в таблице 4.4. Действия становятся доступны при наведении на строку с наименованием группы справочников.

Таблица 4.4 – Действия с группой справочников

Действие	Описание
Изменить группу	Изменение наименования или описания группы. Нажать на наименование группы или на пиктограмму «»
Удалить группу	Удаление группы вместе с входящими в группу справочниками. Нажать на пиктограмму «»
Добавить справочник	Добавление справочника в данную группу. Нажать на пиктограмму «»

4.9.3 Создание справочника

Создание справочника возможно следующими способами:

1. На странице «Справочники» нажать кнопку «Добавить» в правом верхнем углу и выбрать «Справочник».

2. При наведении на группу справочников нажать пиктограмму «». Справочник создастся с предопределенной группой.

При создании справочника заполняются поля, указанные в таблице 4.5.

Таблица 4.5 – Поля справочника

Поле	Описание
Основные настройки	
Тип справочника*	– список – ключ-значение

Поле	Описание
	– ключ – массив – пользовательский
Наименование*	Наименование справочника. Должно быть уникальным
Группа*	Выбор группы из имеющихся
Описание	Описание справочника
Состав справочника	
Ключ*	Наименование (ключ) записи для справочников с типами: – ключ-значение – ключ-массив
Значение*	Значение записи (для всех типов справочников)
* - поля, обязательные к заполнению, при их наличии	

Для добавления записи в справочник нажать на пиктограмму «+».

4.9.4 Редактирование и удаление справочника

Для просмотра и редактирования справочника нажать на наименование справочника. В открывшемся окне справочника отображаются поля справочника и журнал действий, которые были проведены со справочником (рисунок 4.45).

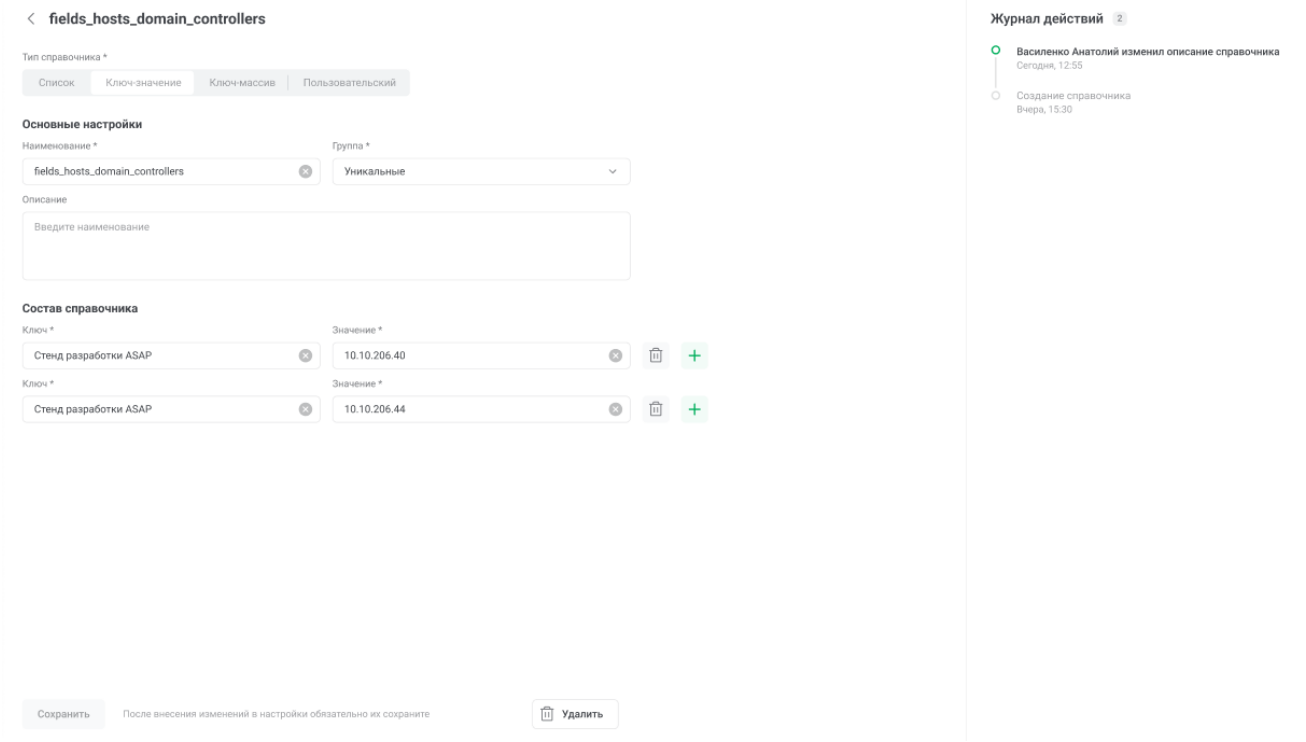


Рисунок 4.45 – Просмотр и редактирование справочника

При редактировании справочника невозможно изменение типа справочника.

После внесения изменений в справочник становится доступна кнопка «Сохранить». Запись об изменении справочника заносится в Журнал действий в правой части страницы.

Для удаления справочника нажать кнопку «Удалить» и подтвердить удаление.

4.10 Параметры платформы

4.10.1 Просмотр организаций

Для просмотра информация об имеющихся в системе организациях и их иерархической структуре необходимо выбрать «Параметры платформы» → «Организации».

4.10.2 Правила регистрации инцидентов

Для просмотра существующих правил регистрации инцидентов необходимо выбрать «Параметры платформы» → «Правила регистрации инцидентов».

На странице показана следующая информация:

– наименование правила;

– уровень угрозы;

– описание;

– дата и время создания правила;

– дата и время последнего обновления правила.

Доступна возможность изменения перечня столбцов в таблице, для этого необходимо нажать на пиктограмму «» и в появившемся окне скрыть или отобразить значения при нажатии на пиктограмму «», справа от названия.

Для изменения настроек одного из правил необходимо нажать на пиктограмму «», справа от нужной записи.

Для удаления одного из правил необходимо нажать пиктограмму «», справа от нужной записи.

4.10.2.1 Создание правила регистрации инцидентов

Для создания нового правила регистрации инцидентов необходимо нажать на кнопку «Добавить», в правом верхнем углу страницы, после чего, откроется окно, доступное для заполнения (рисунок 4.46).

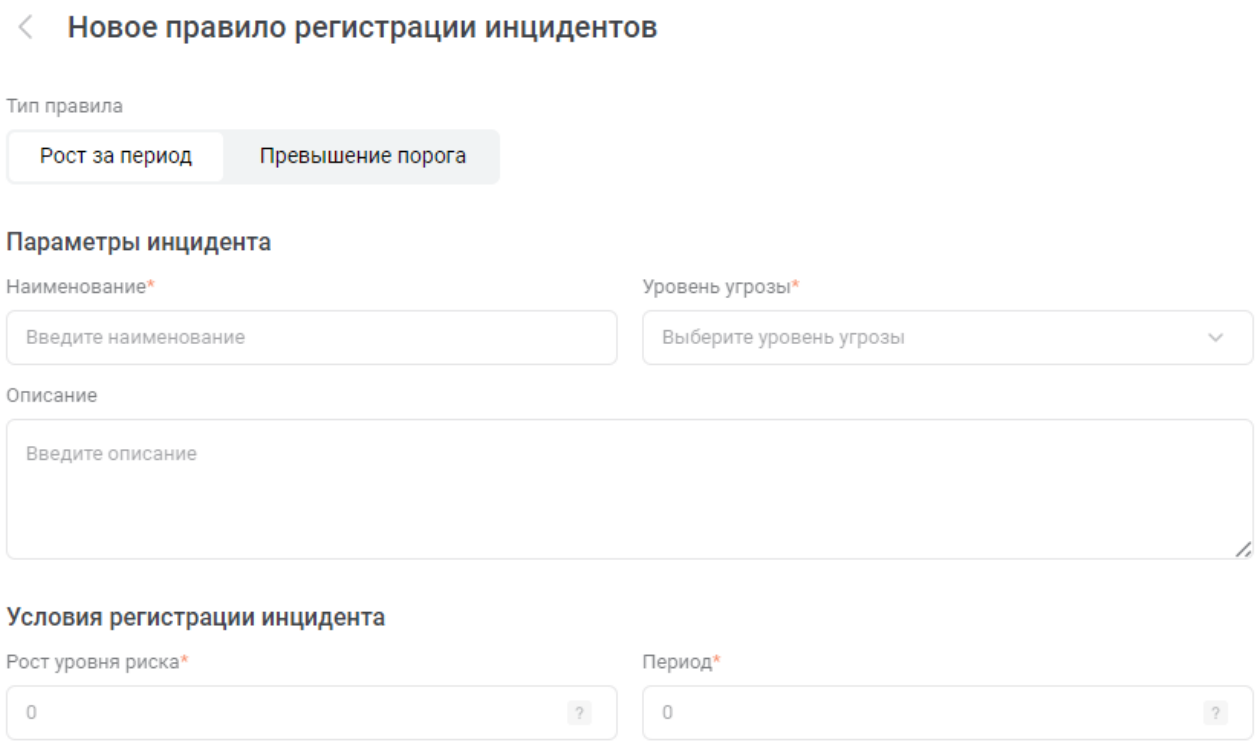


Рисунок 4.46 – Новое правило регистрации инцидентов

Правила регистрации инцидентов включают в себя параметры инцидента, состоящие из:

– наименования. Обязательное для заполнения поле;

– уровень угрозы. Для выбора доступно 5 вариантов в меню выбора (рисунок 4.47), имеющих соответствующие названия и визуальные отображения. Обязательное для заполнения поле;

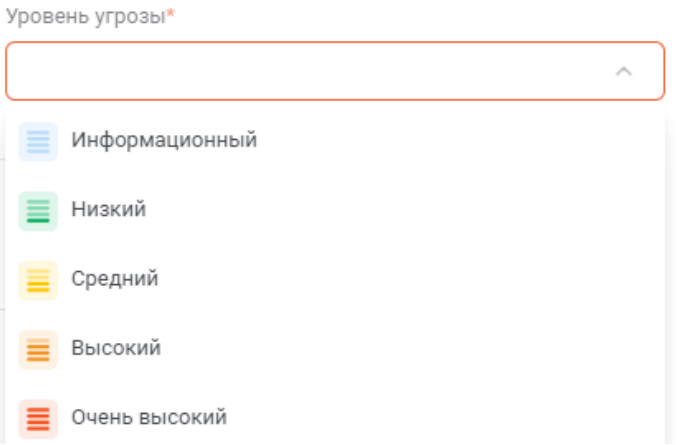


Рисунок 4.47 – Окно выбора уровня угрозы

– описания.

Для выбора доступен тип правила из двух вариантов:

1. Рост за период (значение по умолчанию). Необходимо заполнить два обязательных поля условий регистрации инцидента:

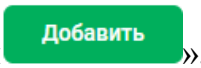
– рост уровня риска - насколько должен увеличиться уровень риска объекта анализа за указанный период, чтобы зарегистрировался инцидент;

– период – за сколько секунд должен увеличиться уровень риска объекта анализа на указанное значение, чтобы зарегистрировался инцидент.

2. Превышение порога. Необходимо заполнить два обязательных поля условий регистрации инцидента:

– уровень риска – значение, при достижении которого, будет зарегистрирован инцидент;

– период повторной регистрации инцидента – через сколько секунд произойдет повторная попытка регистрации инцидента для рассматриваемого объекта анализа.

После заполнения полей, нажать кнопку « 

», в нижней части страницы.

4.11 Администрирование

Для настройки интеграции с платформой визуализации необходимо перейти Администрирование → Настройки интеграции. В открывшемся окне ввести «Наименование» – желаемое название панели визуализации в разделе «Центр аналитики» в основном меню. В поле «Ссылка» добавить ссылку, скопированную ранее в интерфейсе платформы визуализации. При необходимости нажать на пиктограмму «+» и добавить ссылки на другие панели визуализации. Нажать кнопку «Сохранить».

Для удаления элемента (название и ссылку) нажать на пиктограмму «🗑», справа от ссылки на страницу, и нажать кнопку «Сохранить».

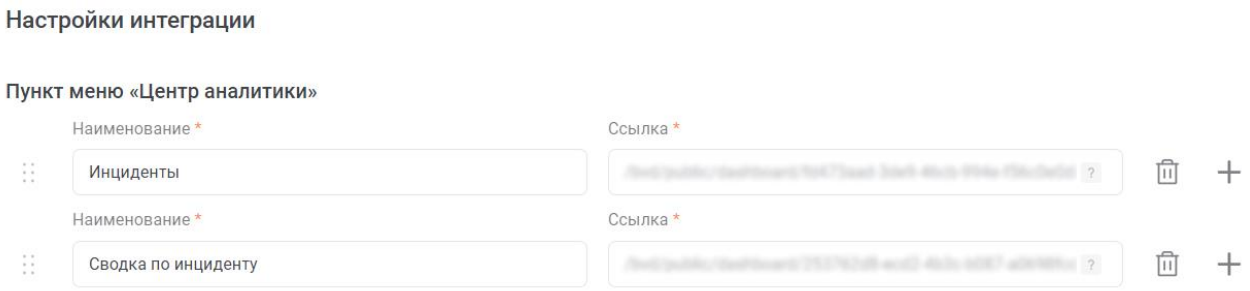


Рисунок 4.48 – Окно «Настройки интеграции»

4.12 Профиль пользователя

4.12.1 Редактирование собственных учетных данных

Редактирование собственных учетных данных или изменение пароля производится в профиле пользователя (рисунок 4.49). Для перехода в профиль пользователя, нажать на имя пользователя (логин) в нижней части меню. Для редактирования доступны следующие данные:

– изображение пользователя;

– имя пользователя в поле «ФИО»;

– e-mail пользователя;

– телефон;

– должность;

– подразделение;

– руководитель.

Для смены изображения выбрать иконку из представленных либо загрузить собственной изображение, нажав на кнопку «Загрузить фото».

Для сохранения внесенных изменений нажать кнопку «Сохранить».

Для изменения пароля нажать кнопку «Изменить пароль», ввести старый пароль, новый пароль, подтверждение и нажать кнопку «Сохранить».

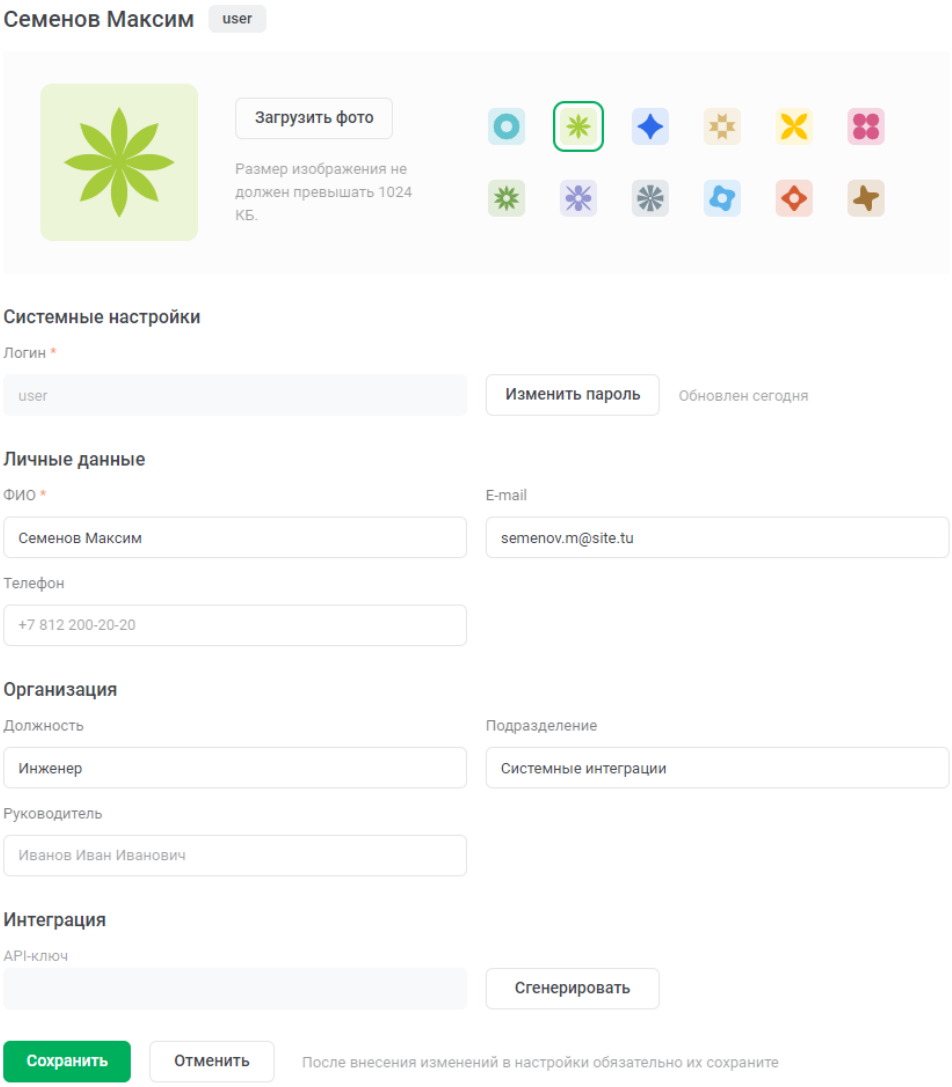


Рисунок 4.49 – Редактирования профиля пользователя

4.12.2 Интеграция с другими системами по API

Раздел «Интеграция» предназначен для учетных записей, использующихся для подключения сторонних систем к ПК «Ankey ASAP» через API.

Для подключения используется API-ключ, для генерации которого необходимо нажать кнопку «Сгенерировать».

4.13 Действия после сбоев и ошибок эксплуатации

Действия после сбоев и ошибок эксплуатации выполняются администратором или системным инженером ПК «Ankey ASAP». Описание действия приведено в руководстве администратора 643.72410666.00071-01 95 01.

Перечень сокращений

AD	–	Active Directory
CEF	–	Common Event Format
LDAP	–	Lightweight Directory Access Protocol
LEF	–	файла активации лицензии
АРМ	–	автоматизированное рабочее место
ИБ	–	информационная безопасность
КИ	–	карточка инцидента
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СУБД	–	система управления базами данных
ЭВМ	–	электронно-вычислительная машина

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