Руководство пользователя по эксплуатации

версия 47 ред. от 02.12.2025

Листов 180

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. Таблица «Термины и сокращения»).

Таблица «Термины и сокращения»

Термины и сокращения	Значение
АРМ	Автоматизированное рабочее место
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
ИБ	Информационная безопасность
ЛКМ	Левая кнопка мыши
МЭ	Межсетевой экран
ОС	Операционная система
ПЛК	Программируемый логический контроллер
ПО	Программное обеспечение
СЗИ	Средства защиты информации
СОВ	Система обнаружения вторжений
ТТУ	Тактики и техники угроз
УЗ	Учётная запись
API	Application Programming Interface, программный интерфейс приложения
ARMA FW	InfoWatch ARMA Firewall
ARMA IE	InfoWatch ARMA Industrial Endpoint
ARMA MC	InfoWatch ARMA Management Console
BACnet	Building Automation and Control network, сетевой протокол, применяемый в системах автоматизации зданий и сетях управления
DNS	Domain Name System, система доменных имён – компьютерная распределённая система для получения информации о доменах
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных

HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IEC104	Промышленный протокол, используемый для передачи данных через сети TCP/IP
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
Modbus	Открытый коммуникационный протокол, основанный на архитектуре ведущий – ведомый, используемый для передачи данных через сети TCP/IP
OMRON	Открытый протокол связи поддерживаемый большинством контроллеров и сетей разработки
OPCDA	Open Platform Communications Data Access – стандарт OPC
OPCUA	Open Platform Communications Unified Architecture – стандарт OPC
S7comm	Протокол, предназначенный для обмена данными с контроллерами Siemens S7 и любым другим оборудованием, поддерживающим данный протокол
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDPB
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
TLS	Transport layer security – протокол защиты транспортного уровня
UDP	User Datagram Protocol, сетевой протокол транспортного уровня, используемый для установления соединений с низкой задержкой и устойчивостью к потерям между приложениями в режиме онлайн

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Management Console v.2.1**.

ARMA MC является единым центром управления системой защиты, агрегирует информацию с подключённых средств защиты и позволяет оперативно оценить текущую защищённость объектов.

ARMA MC выполняет следующие функции:

- централизованно обновляет СЗИ и собирает с них события;
- визуализирует события и выявляет инциденты ИБ;
- позволяет не допустить распространение инцидента ИБ по инфраструктуре организации;
- позволяет осуществить связь с центром ГосСОПКА через личный кабинет.

Настоящее руководство пользователя по эксплуатации содержит описание:

- принципов работы **ARMA MC**;
- веб-интерфейса **ARMA MC**;
- настройки и использования доступных функций **ARMA MC**.

Пользователю **ARMA MC** необходимо изучить настоящее руководство перед эксплуатацией.

В настоящем руководстве использованы ссылки на документы, представленные в таблице (см. Таблица «Смежные документы»).

Таблица «Смежные документы»

Сокращенное наименование	Полное наименование
Руководство администратора ARMA MC	Руководство администратора InfoWatch ARMA Management Console
Руководство администратора ARMA Стена	Руководство администратора InfoWatch ARMA Стена
Руководство пользователя ARMA Стена	Руководство пользователя по эксплуатации InfoWatch ARMA Стена
Руководство администратора ARMA FW	Руководство администратора InfoWatch ARMA Firewall
Руководство пользователя ARMA FW	Руководство пользователя по эксплуатации InfoWatch ARMA Firewall

Руководство пользователя ARMA IE	Руководство пользователя по эксплуатации InfoWatch ARMA Industrial Endpoint

1 СЦЕНАРИИ НАСТРОЙКИ И ЭКСПЛУАТАЦИИ

Сценарий по настройке и использованию программного продукта предназначен для моделирования и проектирования взаимодействия пользователя с **ARMA MC** в рамках выполнения одного или нескольких сценариев работы при эксплуатации **ARMA MC** для достижения конкретных целей.

При первоначальной настройке **ARMA MC** рекомендуется придерживаться следующего сценария эксплуатации:

- ознакомление с информацией о лицензии (см. Лицензии);
- осуществление необходимых изменений в системные настройки продукта (см. Настройки);
- редактирование информации профиля, добавление УЗ и назначение ролей (см. Пользователи);
- добавление СЗИ, источников событий для последующей их эксплуатации (см. Источники событий);
- добавление организации и установка текстового канала связи с НКЦКИ (см. ГосСОПКА);
- настройка обзорной панели для оперативного получения информации из интересующих виджетов (см. Обзорная панель);
- осуществление необходимых настроек правил корреляции (см. Правила корреляции);
- расследование инцидентов, просмотр информации об инцидентах (см. Инциденты);
- просмотр журнала событий, поиск событий (см. События);
- просмотр устройств и активов сети (см. Активы);
- настройка карты сети для анализа взаимодействия сетевых устройств и их связей (см. Карта сети);
- просмотр хранилища архивов собранных инцидентов и событий (см. Хранилище).

2 ВЕБ-ИНТЕРФЕЙС, ОПИСАНИЕ И РАБОТА

В настоящем разделе представлено описание набора элементов, позволяющих пользователю взаимодействовать с веб-интерфейсом **ARMA MC**.

Общий вид веб-интерфейса **ARMA MC** представлен на рисунке (см. Рисунок – Веб-интерфейс ARMA MC).

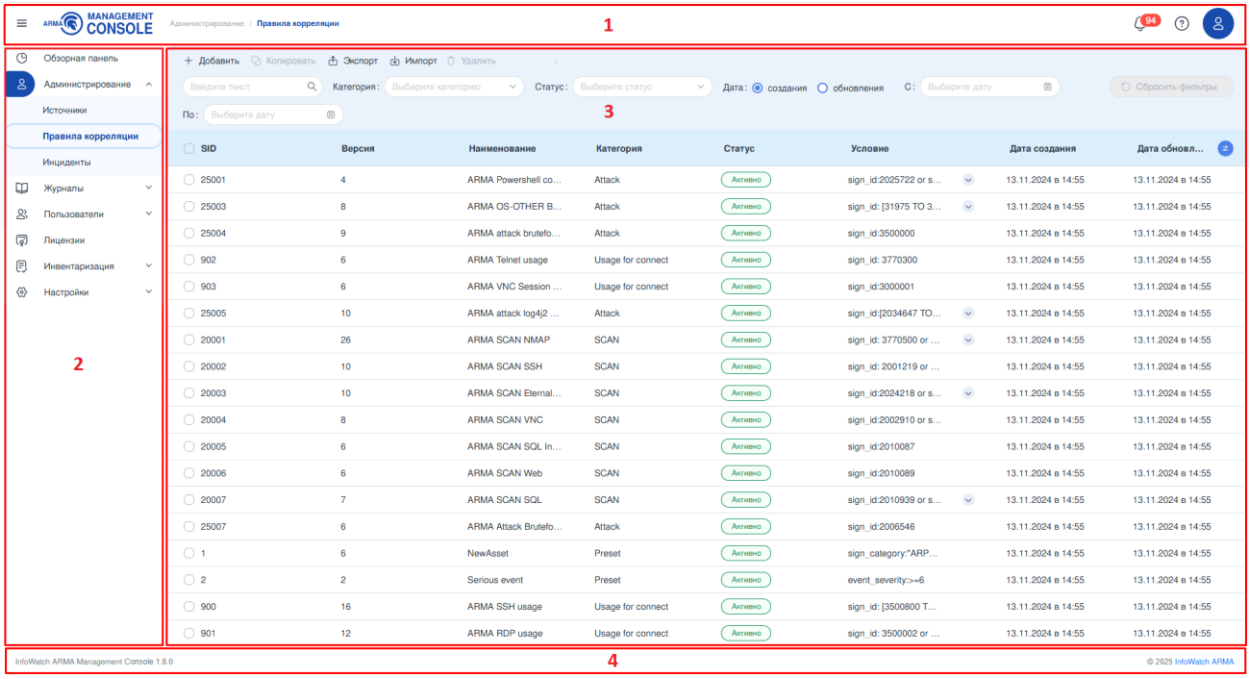


Рисунок – Веб-интерфейс ARMA MC

Основные разделы веб-интерфейса:

- область навигации (**1**);
- область меню (**2**);
- форма раздела меню (**3**);
- служебная информация (**4**).

2.1 Область навигации

Область быстрой навигации **ARMA MC** представлена на рисунке (см. Рисунок – Область навигации).

Рисунок – Область навигации

Область быстрой навигации доступна в любом разделе веб-интерфейса и содержит:

- кнопку сворачивания/разворачивания меню (**1**);
- логотип **ARMA MC** (**2**);

- навигационную цепочку (**3**);
- уведомления (**4**);
- кнопку вызова документации (**5**);
- профиль пользователя (**6**).

Для того чтобы свернуть или развернуть меню необходимо нажать кнопку  .

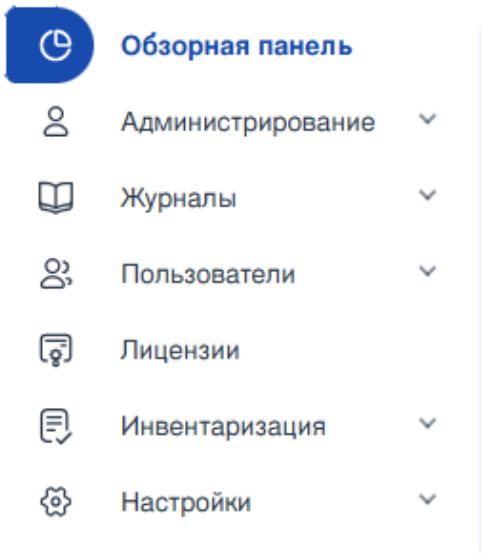


Рисунок – Вид меню в стандартном состоянии

Рисунок – Вид меню в свёрнутом состоянии

При нажатии на логотип **ARMA MC** в любом разделе интерфейса происходит переход в раздел меню **«Обзорная панель»** (см. Обзорная панель настоящего руководства).

Навигационная цепочка отображает путь от раздела меню до подраздела, который в данный момент просматривает пользователь.

Работа с уведомлениями описана в разделе Уведомления настоящего руководства.

При нажатии на кнопку вызова документации произойдёт открытие руководств по эксплуатации **ARMA MC** на новой вкладке.

Работа с профилем описана в разделе Профиль текущего пользователя настоящего руководства.

2.2 Область меню

Область меню предназначена для осуществления доступа к различным функциям **ARMA MC**. В меню существуют следующие уровни вложенности:

- **«раздел»**;
- **«подраздел»** – присутствует не во всех вкладках.

Пример уровней вложенности представлен на рисунке (см. Рисунок – Пример уровней вложенности):

- **«Администрирование»** – раздел;
- **«Источники»/«Правила корреляции»/«Инциденты»** – подраздел.

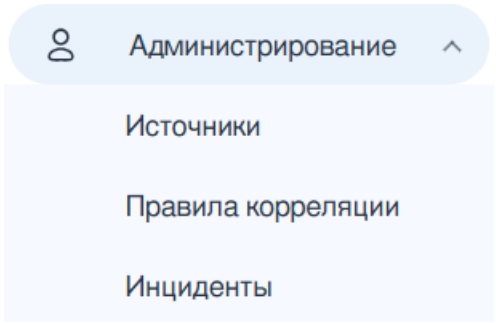


Рисунок – Пример уровней вложенности

2.3 Форма раздела меню. Таблица

В значительной части разделов меню **ARMA MC** информация представлена в формате таблицы. В качестве примера приведена организация информации в табличном формате в подразделе меню **«Правила корреляции»** (см. Рисунок – Подраздел «Правила корреляции» в формате таблицы).

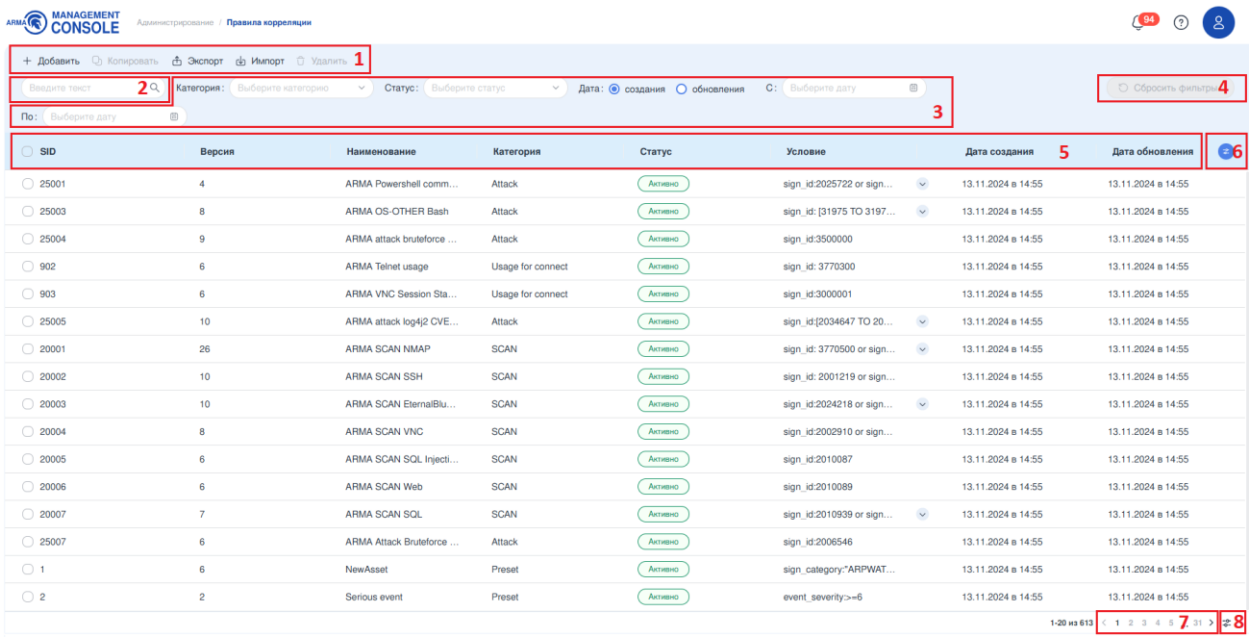


Рисунок – Подраздел «Правила корреляции» в формате таблицы

В разделах меню существуют следующие возможности:

- действия с элементами (**1**);
- поиск по полям таблицы (**2**);
- фильтрация элементов (**3**);
- сброс фильтров (**4**);
- сортировка элементов по столбцам (**5**);
- выбор отображаемых столбцов (**6**);
- работа с карточками;
- переход к предыдущей или следующей странице с записями (**7**);
- выбор количества отображаемых записей (**8**).

2.3.1 Действия с элементами

На панели инструментов расположены кнопки действий с элементами отображаемого списка. Набор кнопок отличается в зависимости от раздела меню.

В качестве примера представлено действие удаления элемента. Для удаления элемента или нескольких элементов из отображаемого списка необходимо выполнить следующие действия:

1. Выбрать необходимый элемент или элементы списка, установив флажок в чек-боксе слева от каждого необходимого элемента.
2. Нажать кнопку **«Удалить»** на панели инструментов.

3. Подтвердить удаление, нажав кнопку **«Удалить»** в открывшемся уведомлении (см. Рисунок – Удаление элемента).

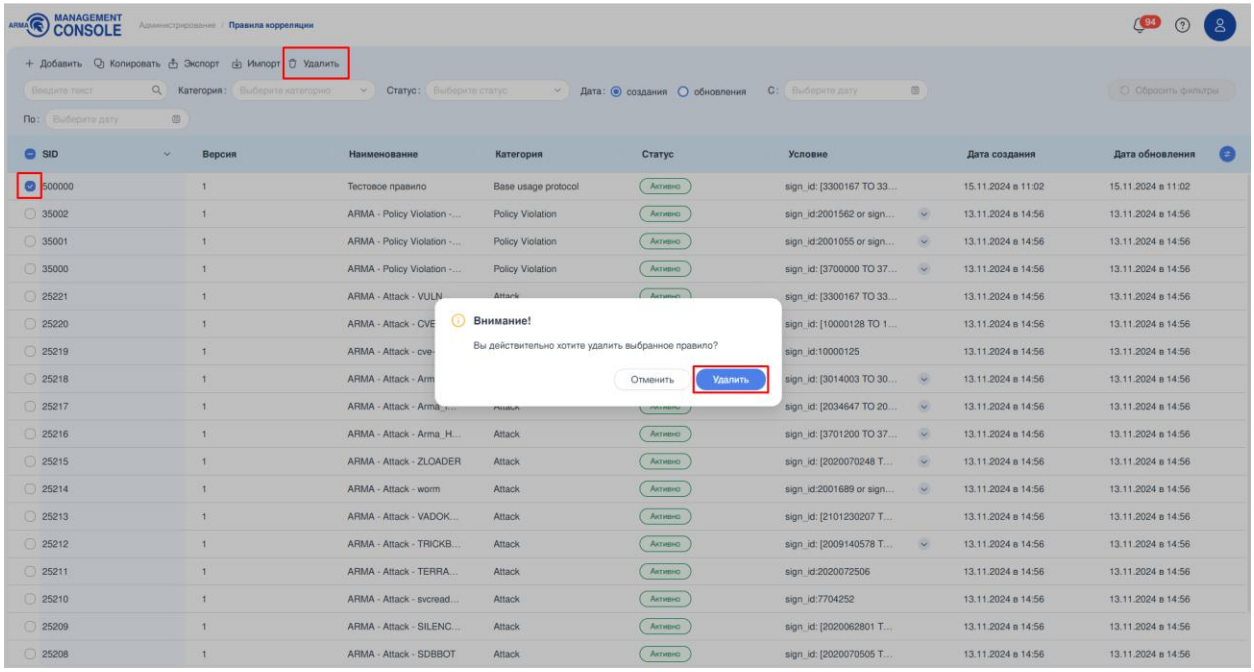


Рисунок – Удаление элемента

Примечание:

Текст окна подтверждения удаления может отличаться в зависимости от элемента.

2.3.2 Поиск по полям таблицы

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»** (см. Рисунок – Подраздел «Правила корреляции» в формате таблицы).

В зависимости от раздела меню поиск осуществляется по различному количеству столбцов таблицы.

2.3.3 Фильтрация элементов

На панели инструментов расположен блок фильтрации, содержащий набор полей для фильтрации элементов отображаемого списка. Набор полей отличается в зависимости от раздела меню.

Для осуществления фильтрации необходимо выбрать значение из выпадающего списка необходимого поля фильтрации. В качестве примера приведена фильтрация правил корреляции по полю **«Категория»** со значением **«SCAN»** (см. Рисунок – Пример фильтрации по полю «Категория»).

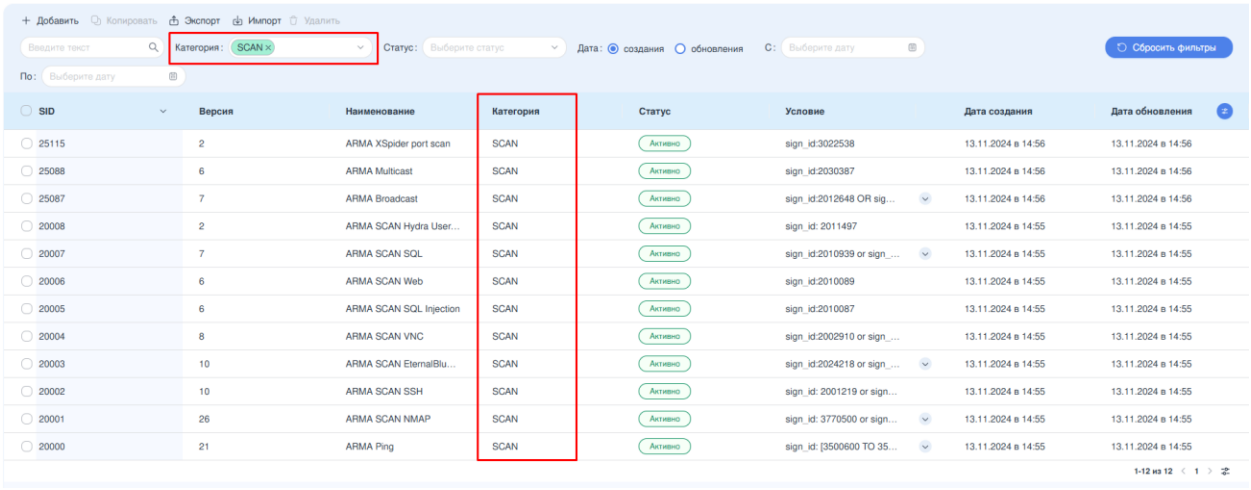


Рисунок – Пример фильтрации по полю «Категория»

2.3.4 Сброс фильтров

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**, находящейся в правой верхней части блока фильтрации (см. Рисунок – Кнопка «Сбросить фильтры»).

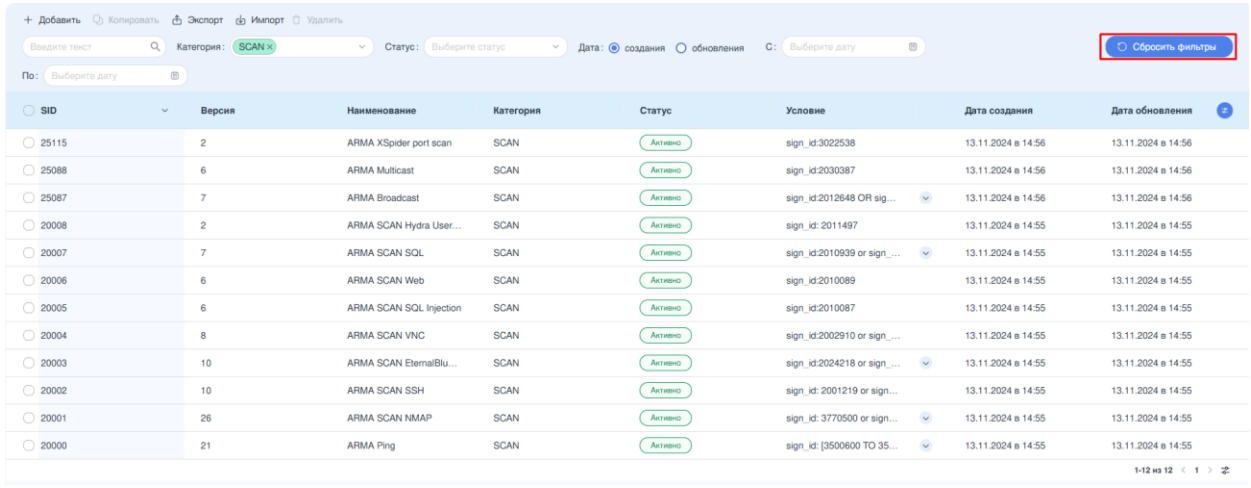


Рисунок – Кнопка «Сбросить фильтры»

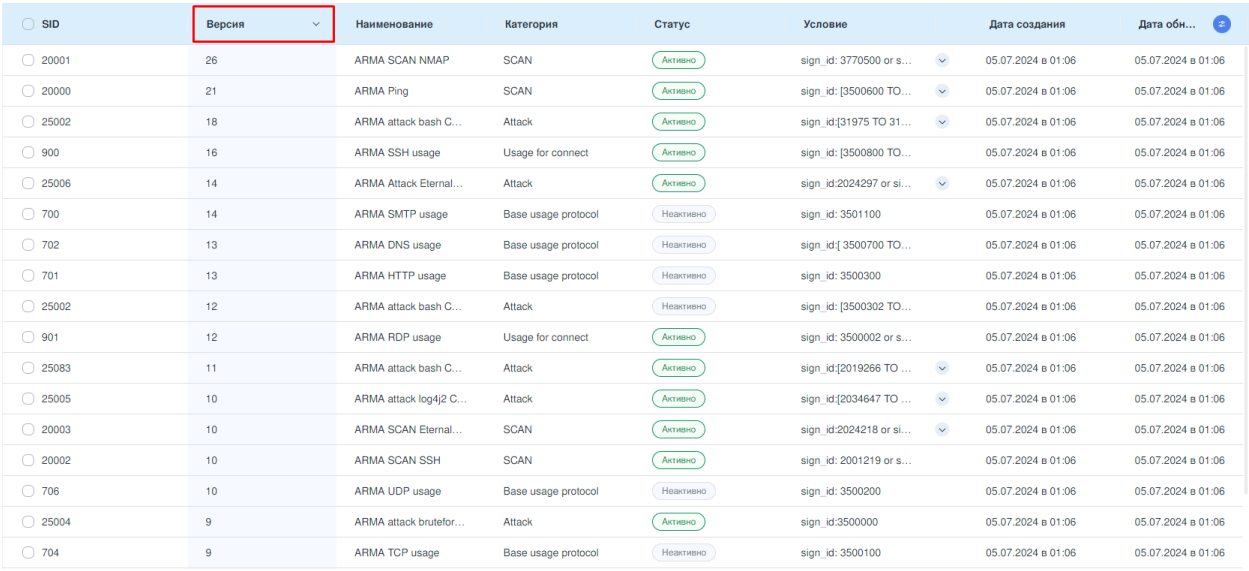
2.3.5 Сортировка элементов по столбцам

Для сортировки списка по определённому столбцу достаточно нажать на заголовок столбца. Наличие « » правее заголовка показывает, что столбец отсортирован по возрастанию, а « » показывает сортировку по убыванию. Если сортировка не применена, вышеупомянутые значки не отображаются.

Примечание:

Сортировка по столбцам **«Группа»** и **«Роль»** не производится.

В качестве примера приведена сортировка правил корреляции по убыванию по столбцу **«Версия»** (см. Рисунок – Пример сортировки по полю «Версия»).



SID	Версия	Наименование	Категория	Статус	Условие	Дата создания	Дата обн...
20001	26	ARMA SCAN NMAP	SCAN	Активно	sign_id: 3770500 or s...	05.07.2024 в 01:06	05.07.2024 в 01:06
20000	21	ARMA Ping	SCAN	Активно	sign_id: [3500600 TO...	05.07.2024 в 01:06	05.07.2024 в 01:06
25002	18	ARMA attack bash C...	Attack	Активно	sign_id:[31975 TO 31...	05.07.2024 в 01:06	05.07.2024 в 01:06
900	16	ARMA SSH usage	Usage for connect	Активно	sign_id: [3500800 TO...	05.07.2024 в 01:06	05.07.2024 в 01:06
25006	14	ARMA Attack Eternal...	Attack	Активно	sign_id:2024297 or si...	05.07.2024 в 01:06	05.07.2024 в 01:06
700	14	ARMA SMTP usage	Base usage protocol	Неактивно	sign_id: 3501100	05.07.2024 в 01:06	05.07.2024 в 01:06
702	13	ARMA DNS usage	Base usage protocol	Неактивно	sign_id:[3500700 TO...	05.07.2024 в 01:06	05.07.2024 в 01:06
701	13	ARMA HTTP usage	Base usage protocol	Неактивно	sign_id: 3500300	05.07.2024 в 01:06	05.07.2024 в 01:06
25002	12	ARMA attack bash C...	Attack	Неактивно	sign_id: [3500302 TO...	05.07.2024 в 01:06	05.07.2024 в 01:06
901	12	ARMA RDP usage	Usage for connect	Активно	sign_id: 3500002 or s...	05.07.2024 в 01:06	05.07.2024 в 01:06
25083	11	ARMA attack bash C...	Attack	Активно	sign_id:[2019266 TO ...	05.07.2024 в 01:06	05.07.2024 в 01:06
25005	10	ARMA attack log4j2 C...	Attack	Активно	sign_id:[2034647 TO ...	05.07.2024 в 01:06	05.07.2024 в 01:06
20003	10	ARMA SCAN Eternal...	SCAN	Активно	sign_id:2024218 or si...	05.07.2024 в 01:06	05.07.2024 в 01:06
20002	10	ARMA SCAN SSH	SCAN	Активно	sign_id: 2001219 or s...	05.07.2024 в 01:06	05.07.2024 в 01:06
706	10	ARMA UDP usage	Base usage protocol	Неактивно	sign_id: 3500200	05.07.2024 в 01:06	05.07.2024 в 01:06
25004	9	ARMA attack brutefor...	Attack	Активно	sign_id:3500000	05.07.2024 в 01:06	05.07.2024 в 01:06
704	9	ARMA TCP usage	Base usage protocol	Неактивно	sign_id: 3500100	05.07.2024 в 01:06	05.07.2024 в 01:06

Рисунок – Пример сортировки по полю «Версия»

2.3.6 Выбор отображаемых столбцов

Настройка отображаемых столбцов осуществляется с помощью кнопки **«Настройка столбцов»** и последующим выбором в выпадающем списке отображаемых столбцов (см. Рисунок – Выбор отображаемых столбцов).

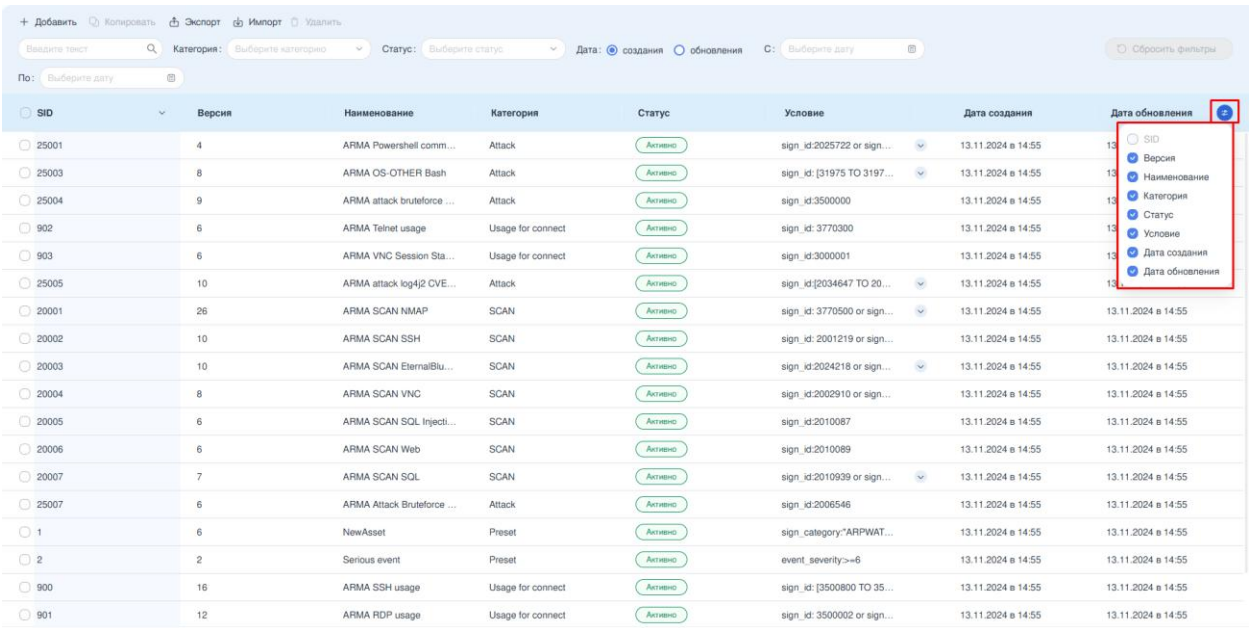


Рисунок – Выбор отображаемых столбцов

2.3.7 Работа с карточками

Карточки предоставляют пользователю расширенную информацию о выбранном элементе, в некоторых случаях с возможностью редактирования данных.

Работа с карточками доступна в двух вариантах:

- в стандартном;

- в полноэкранном режиме.

При нажатии на строку элемента производится стандартное открытие карточки в правой части экрана (см. Рисунок – Карточка, стандартный режим).

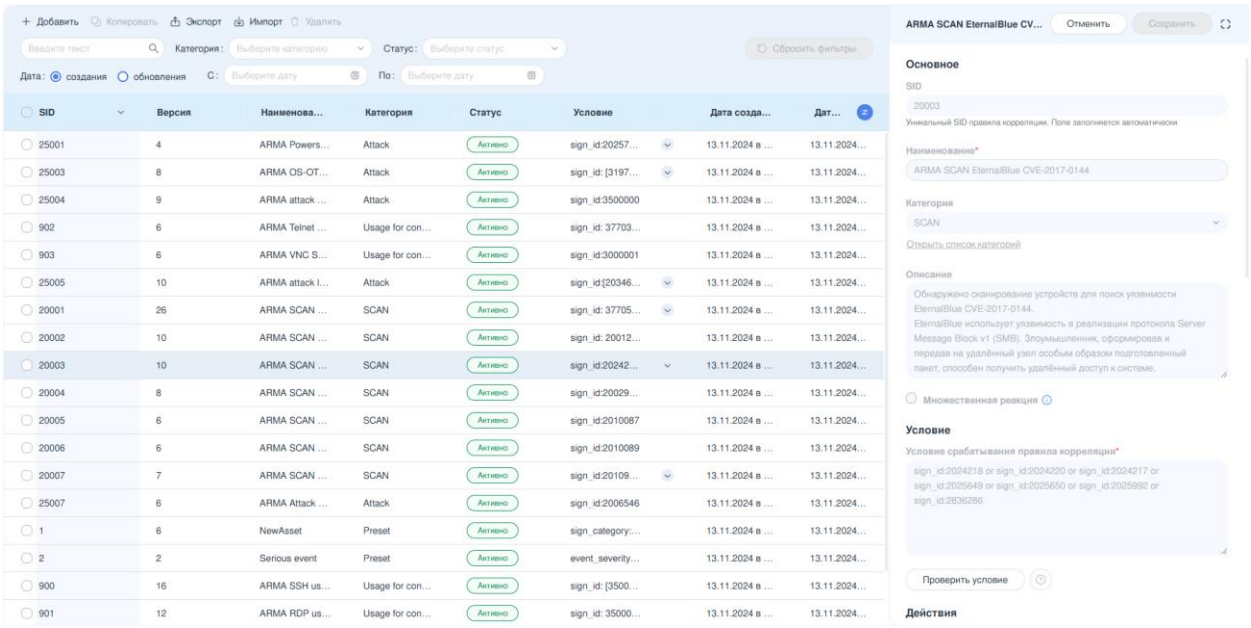


Рисунок – Карточка, стандартный режим

При нажатии кнопки « » в правом верхнем углу карточки производится открытие карточки в полноэкранном режиме (см. Рисунок – Карточка, полноэкранный режим).

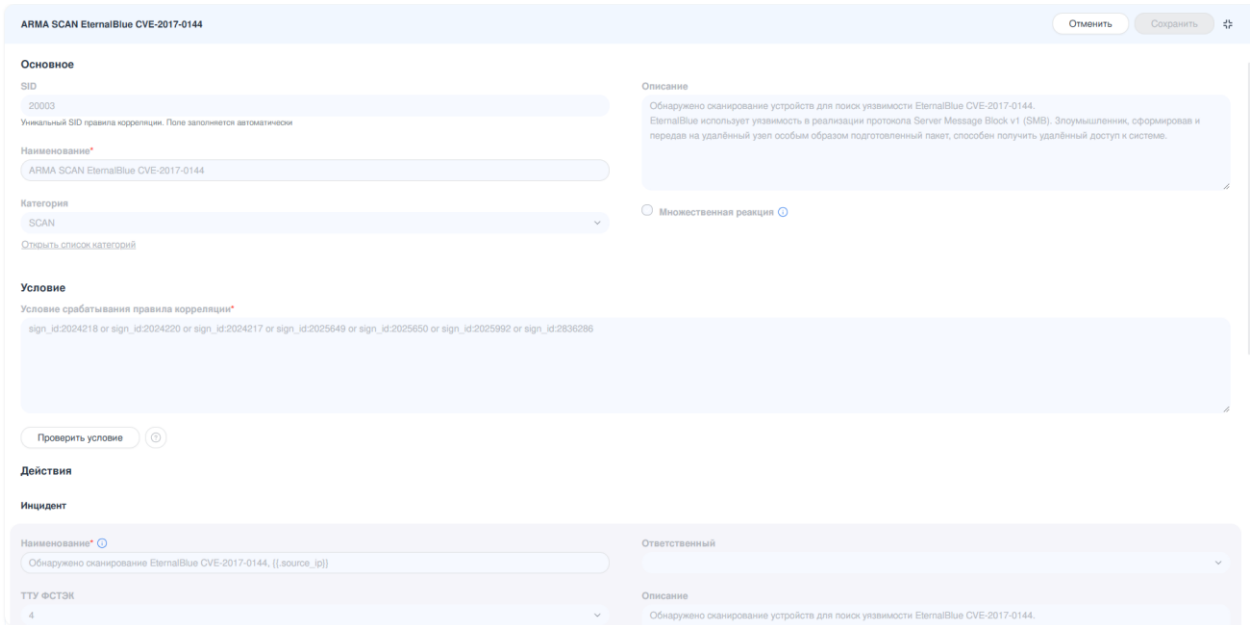


Рисунок – Карточка, полноэкранный режим

Для возврата к свёрнутой карточке необходимо нажать кнопку « » в правом верхнем углу экрана.

2.3.8 Переход к предыдущим и следующим страницам

Для перехода к предыдущей или следующей странице с записями необходимо нажать кнопки « < » и « > » соответственно. Порядковый номер текущей страницы отображён между данными кнопками (см. Рисунок – Порядковый номер текущей страницы).

Рисунок – Порядковый номер текущей страницы

2.3.9 Выбор количества отображаемых записей

Для выбора количества отображаемых записей в таблице необходимо нажать кнопку « » в правом нижнем углу экрана и указать количество записей в открывшемся выпадающем списке (см. Рисунок – Выбор количества отображаемых записей).

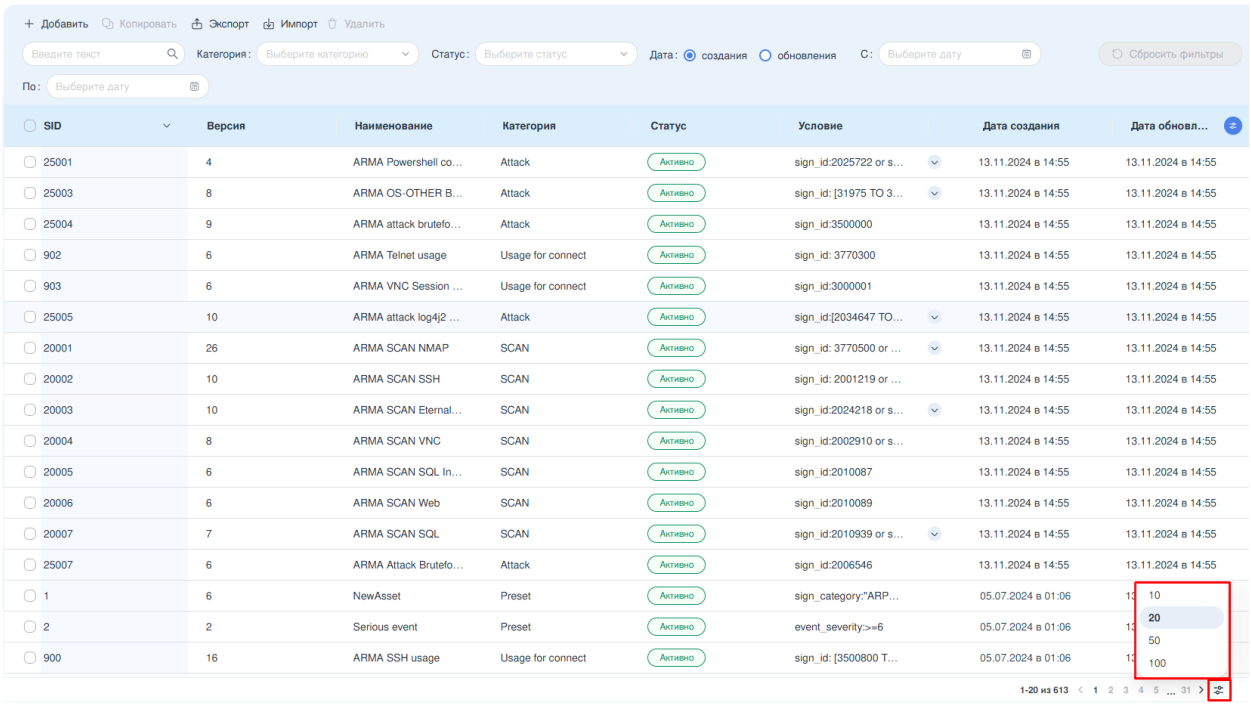


Рисунок – Выбор количества отображаемых записей

3 УВЕДОМЛЕНИЯ

В настоящем разделе представлено описание раздела меню **«Уведомления»**, позволяющего пользователю просматривать список уведомлений от **ARMA MC**.

Раздел меню **«Уведомления»** доступен пользователю с любой страницы системы. Для перехода в раздел меню необходимо нажать на иконку « » в правом верхнем углу страницы (см. Рисунок – Уведомления).

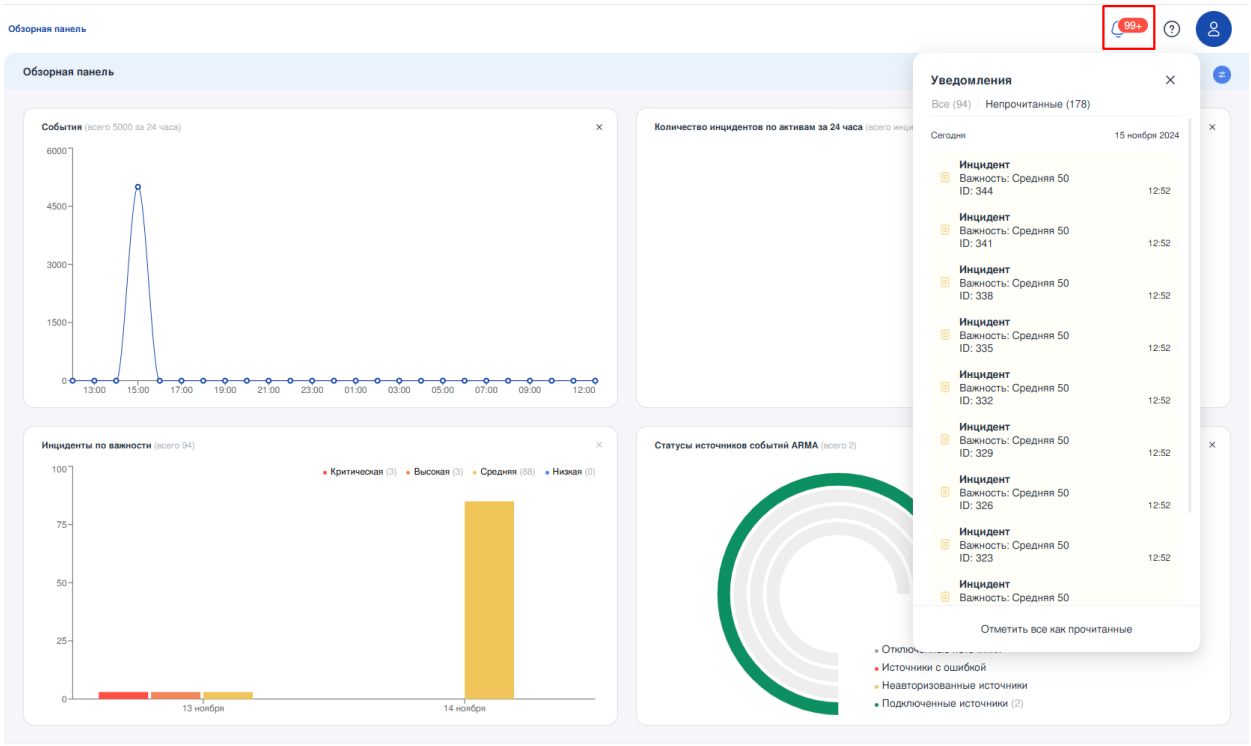


Рисунок – Уведомления

Иконка « » отображает количество активных уведомлений. В случае, если активных уведомлений больше 99, на иконке отобразится значение **«99+»**.

Информация об уведомлениях отображается в режиме реального времени. В момент появления нового уведомления слева от иконки « » появляется сообщение (см. Рисунок – Новое уведомление).

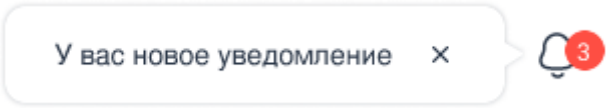


Рисунок – Новое уведомление

Уведомление отображается до тех пор, пока пользователь не откроет его или не удалит. Для удаления уведомления необходимо нажать кнопку « » в правой части необходимого уведомления (см. Рисунок – Удаление уведомления).

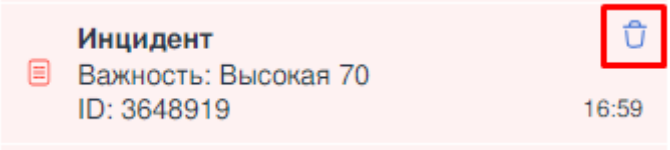


Рисунок – Удаление уведомления

Примечание:

Уведомления автоматически удаляются из системы через 30 дней, независимо от того, были они прочитаны или нет.

Для того чтобы скрыть все уведомления, необходимо нажать кнопку **«Отметить все как прочитанные»** (см. Рисунок – Кнопка «Отметить все как прочитанные»).

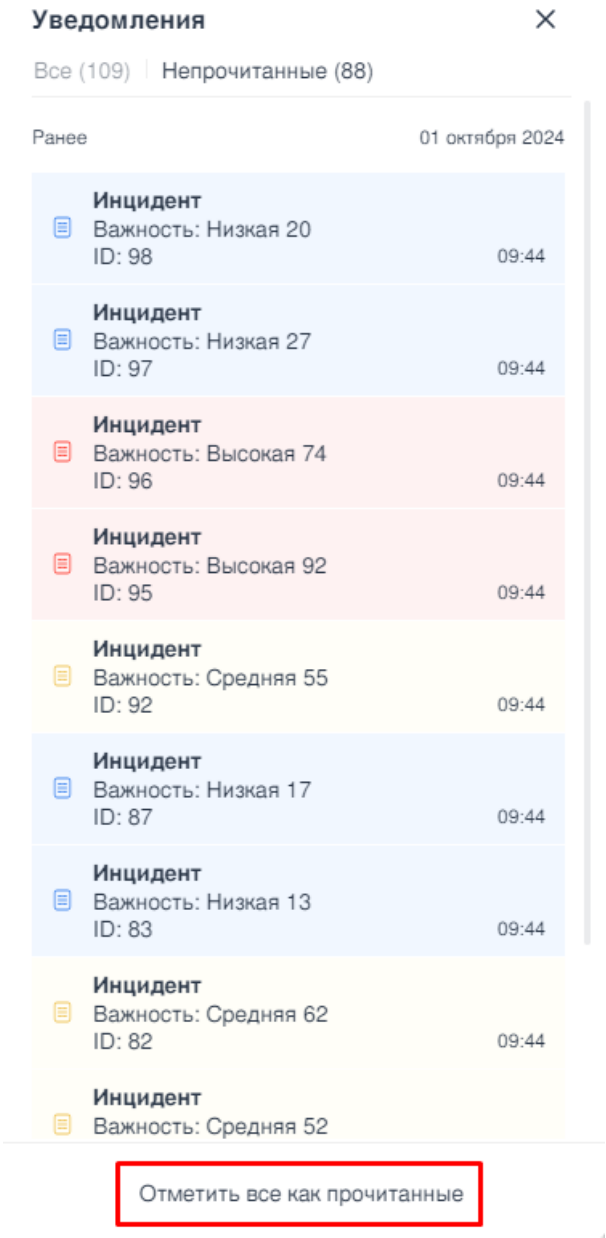


Рисунок – Кнопка «Отметить все как прочитанные»

3.1 Общие характеристики

Уведомления распределяются по двум вкладкам – **«Все»** и **«Непрочитанные»** (см. Рисунок – Вкладки). Вкладка **«Все»** содержит список всех уведомлений, вне зависимости от того, прочитаны они или нет. Вкладка **«Непрочитанные»** содержит список уведомлений в непрочитанном состоянии и является вкладкой по умолчанию. Справа от наименования вкладки расположено число хранящихся в ней уведомлений.

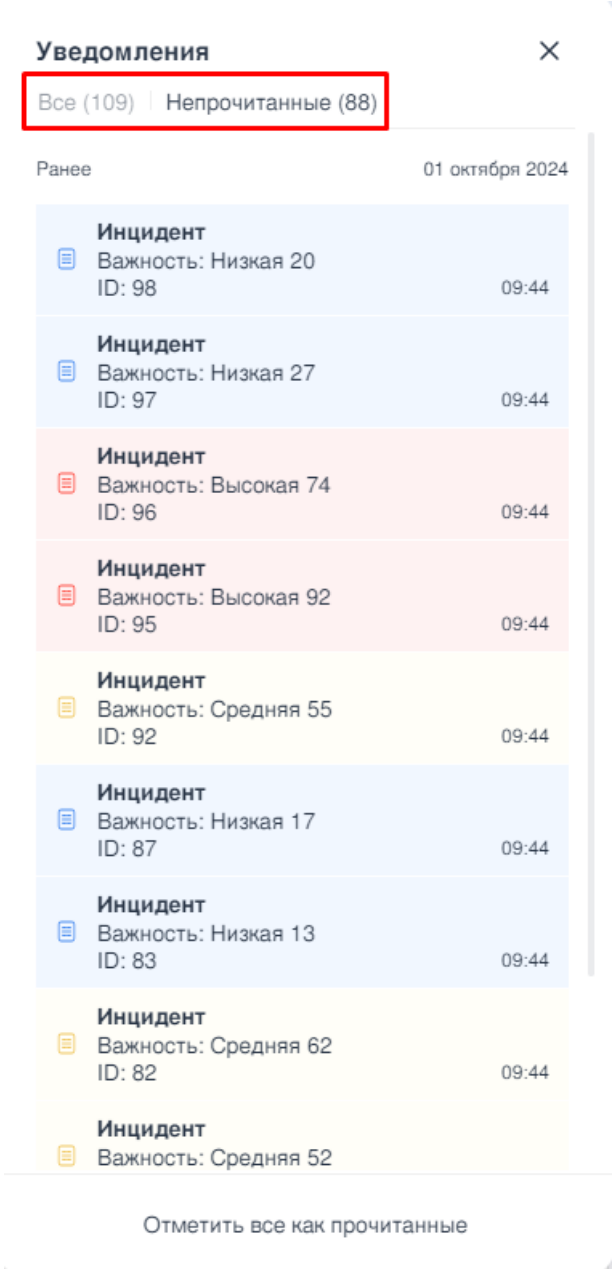


Рисунок – Вкладки

3.2 Типы уведомлений

В **«Уведомления»** попадают следующие типы сообщений:

- новые обнаруженные инциденты (см. раздел Инциденты настоящего руководства);
- статус раздела меню **«Хранилище»** (см. раздел Хранилище настоящего руководства).

3.2.1 Тип уведомления «Инцидент»

Тип уведомления **«Инцидент»** содержит в себе три основных атрибута:

- **«Важность»** – числовое значение, определяющее важность инцидента;
- **«ID»** – идентификатор инцидента;
- время – время, когда пришло уведомление (эквивалентно времени формирования инцидента).

Уведомления типа **«Инцидент»** имеют визуальное различие, в зависимости от важности события (см. Рисунок – Важность инцидента).

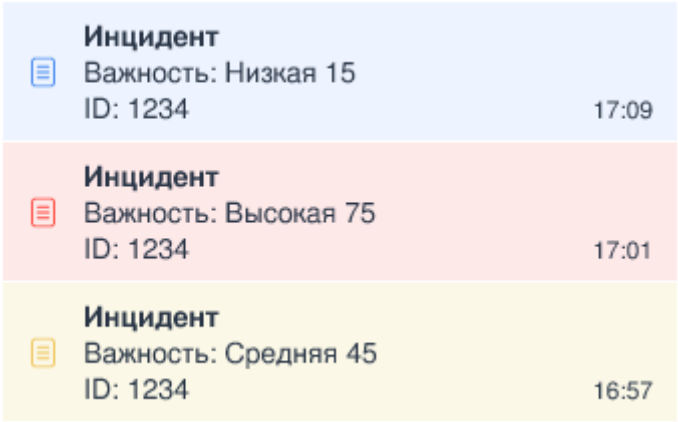


Рисунок – Важность инцидента

При нажатии на строку с уведомлением об инциденте происходит переход в подраздел меню **«Инциденты»** и открытие карточки выбранного инцидента (см. Рисунок – Переход в подраздел меню «Инциденты»).

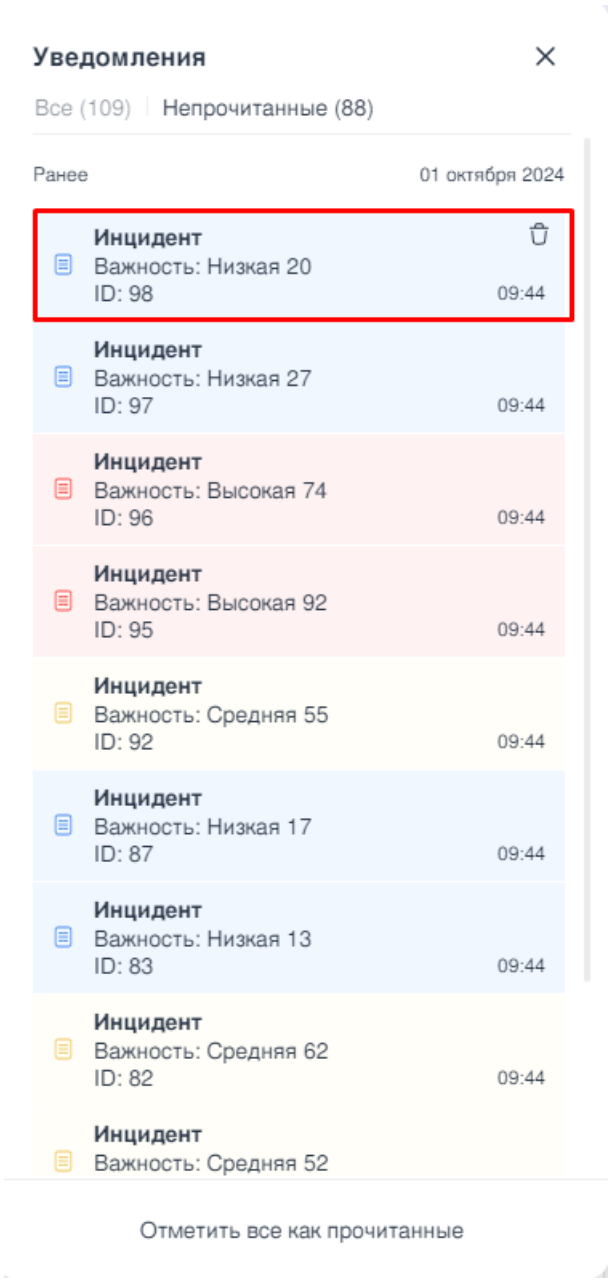


Рисунок – Переход в подраздел меню «Инциденты»

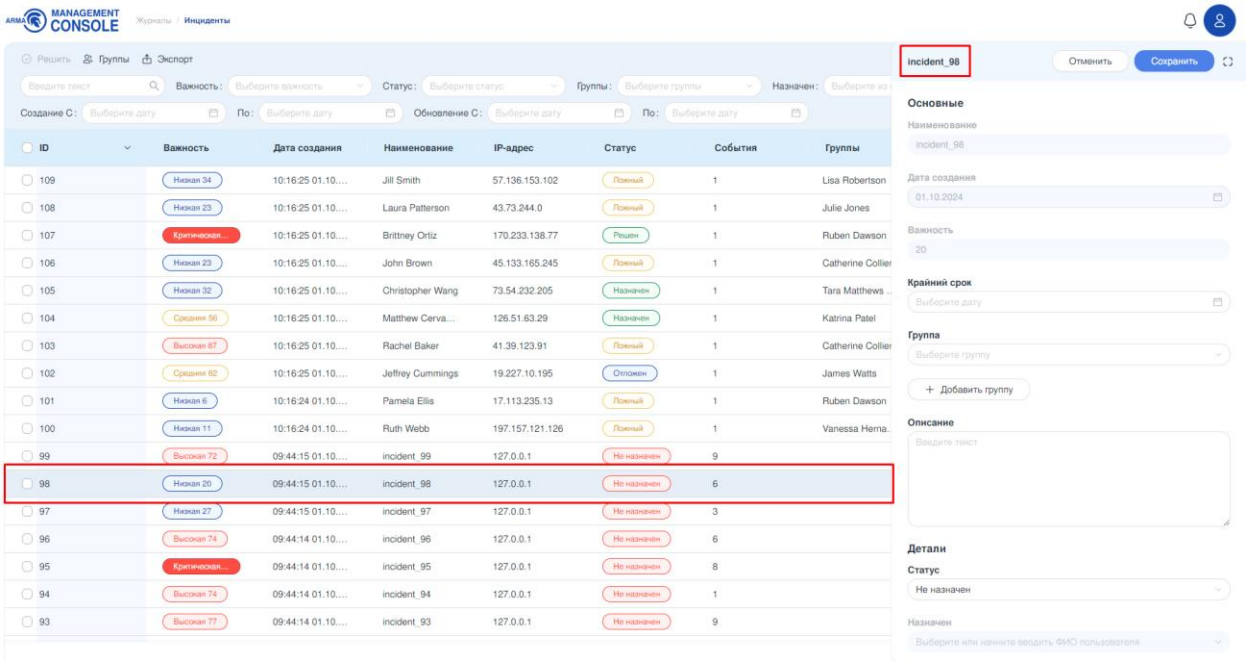


Рисунок – Выбранный инцидент

4 ОБЗОРНАЯ ПАНЕЛЬ

В настоящем разделе представлено описание раздела меню **«Обзорная панель»**.

Обзорная панель – инструмент для визуализации метрик в реальном времени, состоящий из виджетов, каждый из которых отображает определённый набор данных.

Для перехода на страницу **«Обзорная панель»** необходимо нажать на логотип **ARMA MC** или открыть раздел меню **«Обзорная панель»** (см. Рисунок – Обзорная панель).

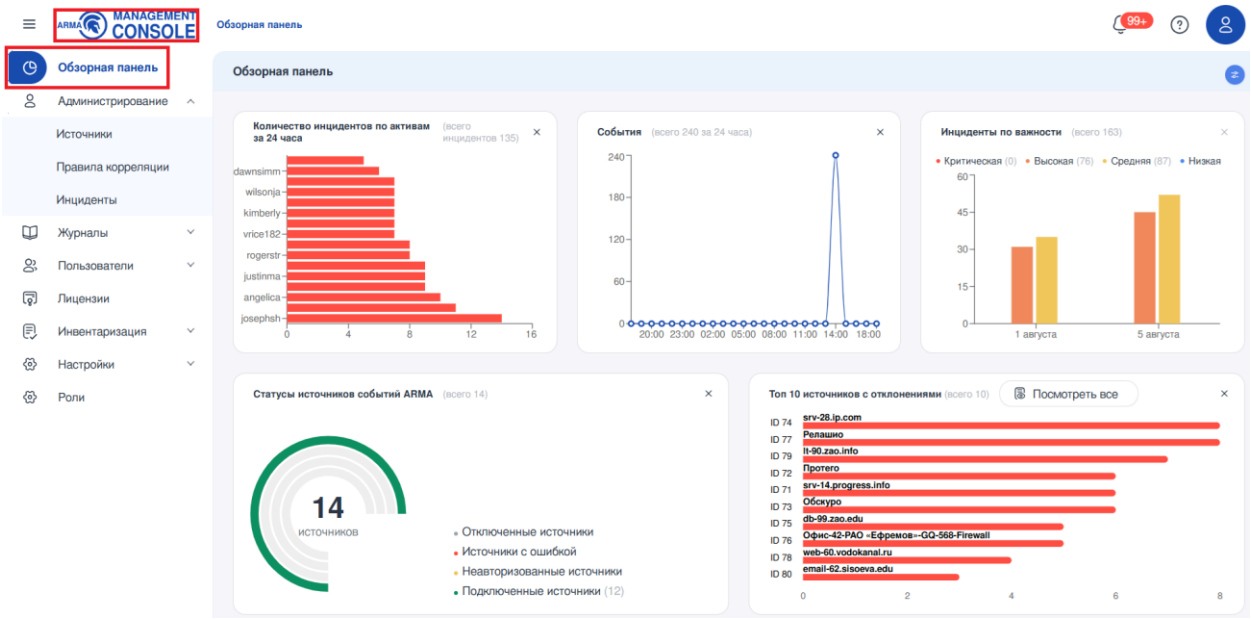


Рисунок – Обзорная панель

Существует возможность добавления следующих виджетов:

- **«Инциденты по важности»** (см. Виджет «Инциденты по важности»);
- **«События»** (см. Виджет «События»);
- **«Количество инцидентов по активам за 24 часа»** (см. Виджет «Количество инцидентов по активам за 24 часа»);
- **«Статусы источников событий ARMA»** (см. Виджет «Статусы источников событий ARMA»);
- **«Топ 10 источников с отклонениями»** (см. Виджет «Топ 10 источников с отклонениями»);
- **«Статусы кластеров»** (см. Виджет «Статусы кластеров»).

При добавлении виджета **«Статусы кластеров»** в случае отсутствия подключённых источников **«NGFW»** в составе кластера, будет выведено уведомление «Сервер не может найти данные согласно запросу».

ARMA MC позволяет каждому пользователю настраивать индивидуальное отображение виджетов. Пользователю доступны следующие действия:

- настройка набора отображаемых виджетов;
- настройка местоположения виджетов.

4.1 Настройка набора отображаемых виджетов

Для внесения изменений необходимо нажать кнопку **«Настройка столбцов»** в правом верхнем углу страницы и выбрать в выпадающем списке необходимые виджеты или скрыть их (см. Рисунок – Настройка отображения виджетов). Скрыть виджет **«Инциденты по важности»** невозможно.

Обзорная панель может содержать одновременно не более 5-и виджетов.

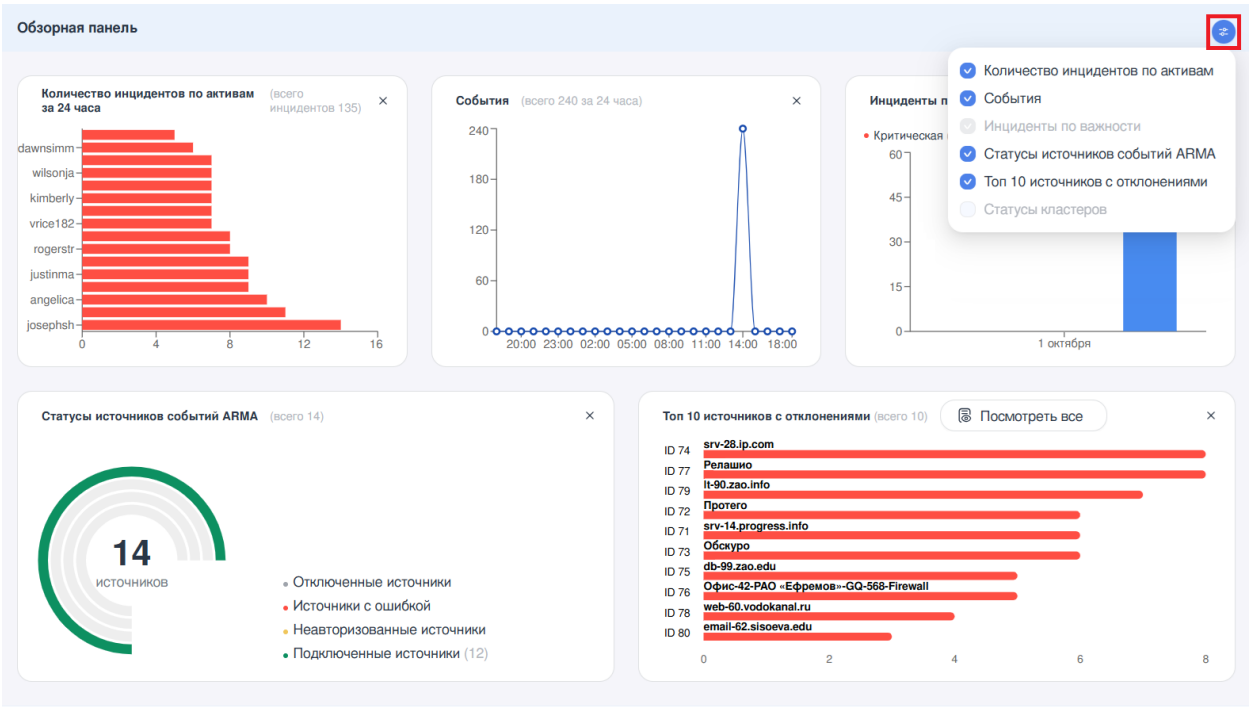


Рисунок – Настройка отображения виджетов

Кроме того, существует возможность скрыть виджет нажатием кнопки « × » в правом верхнем углу каждого отдельного виджета.

4.2 Настройка местоположения виджетов

Для перемещения виджета на обзорной панели необходимо нажать на необходимый виджет и, удерживая клавишу мыши зажатой, перетащить виджет в необходимое место на панели.

После внесения изменений, раздел меню **«Обзорная панель»** сохраняет уникальные настройки пользователя при работе в последующих активных сессиях.

4.3 Виджет «Инциденты по важности»

Виджет **«Инциденты по важности»** отображает информацию о количестве зарегистрированных инцидентов (см. Инциденты настоящего руководства) с градацией по важности. Информация представлена в виде диаграммы (см. Рисунок – Виджет «Инциденты по важности»).

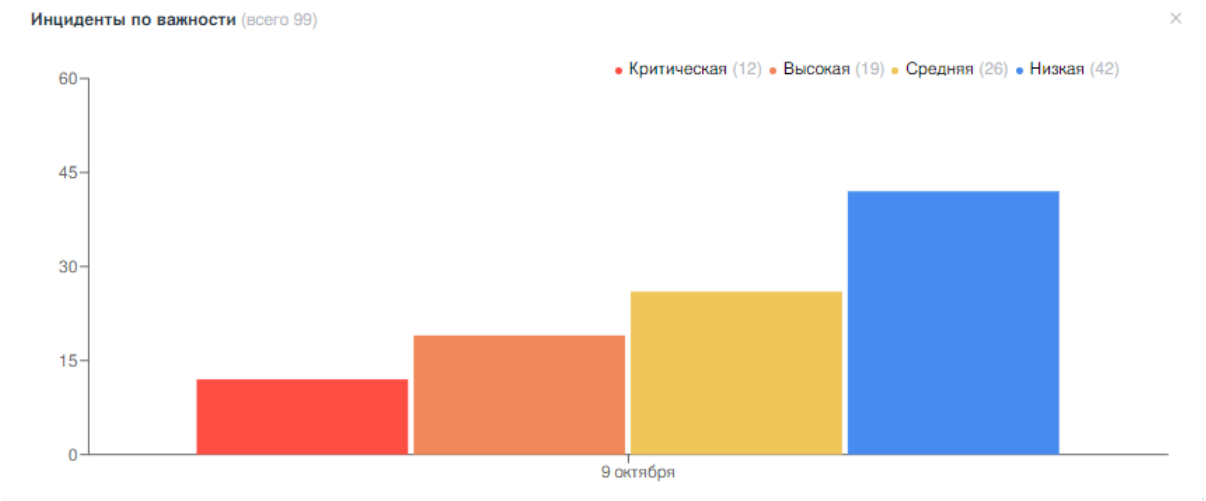


Рисунок – Виджет «Инциденты по важности»

Справа от наименования виджета в скобках указано общее количество инцидентов.

Вертикальная шкала отображает количество инцидентов с разбивкой на 5 средних значений от максимального числа инцидентов. Горизонтальная шкала отображает количество дней с разбивкой на неделю, от 1 до 7 дней.

Текстовое поле над виджетом содержит категории важности инцидента («Критическая», «Высокая», «Средняя», «Низкая»). Справа от каждой категории в скобках указано количество инцидентов данной категории. При нажатии на любую категорию будет выделена соответствующая зона диаграммы, остальные зоны потускнеют (см. Рисунок – Выбор категории важности).

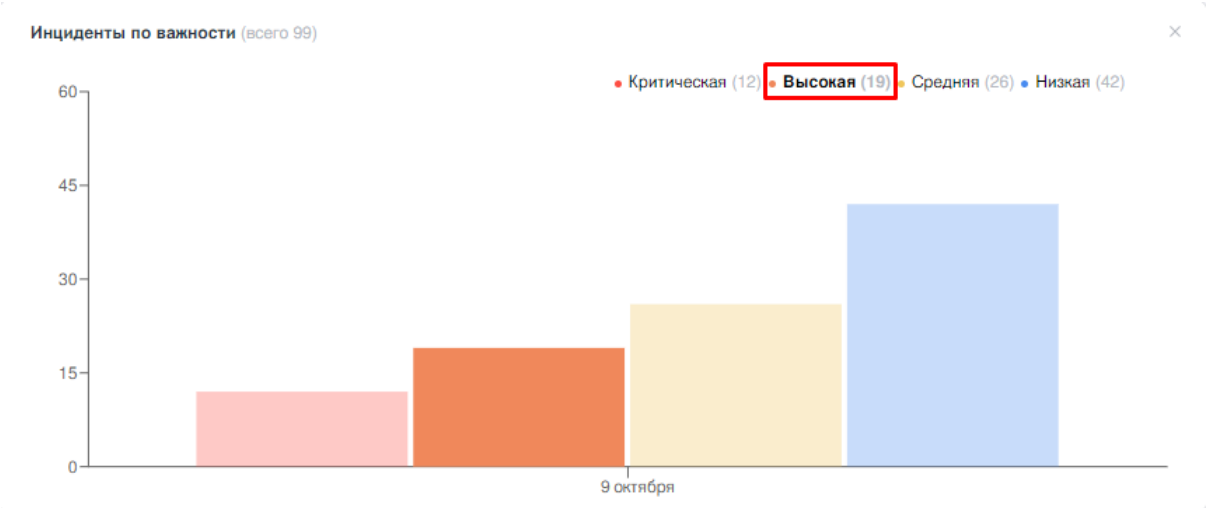


Рисунок – Выбор категории важности

При наведении на диаграмму появится окно, в котором дублируется значение текстового поля с градацией инцидентов по важности и указанием их количества (см. Рисунок – Количество инцидентов по важности).

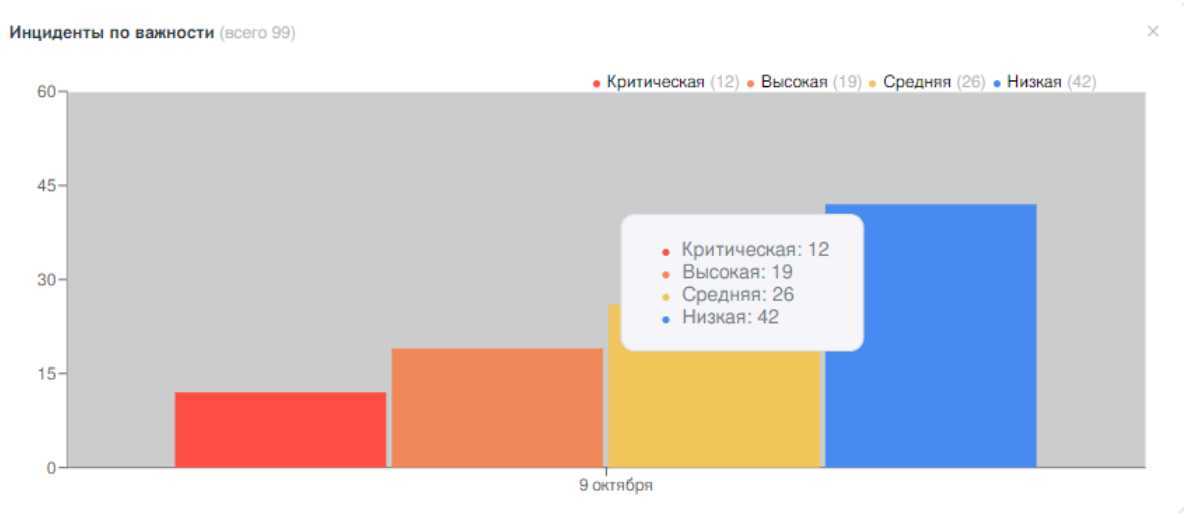


Рисунок – Количество инцидентов по важности

4.4 Виджет «События»

Виджет **«События»** отображает информацию о количестве зарегистрированных событий (см. События настоящего руководства). Информация представлена в виде графика (см. Рисунок – Виджет «События»).

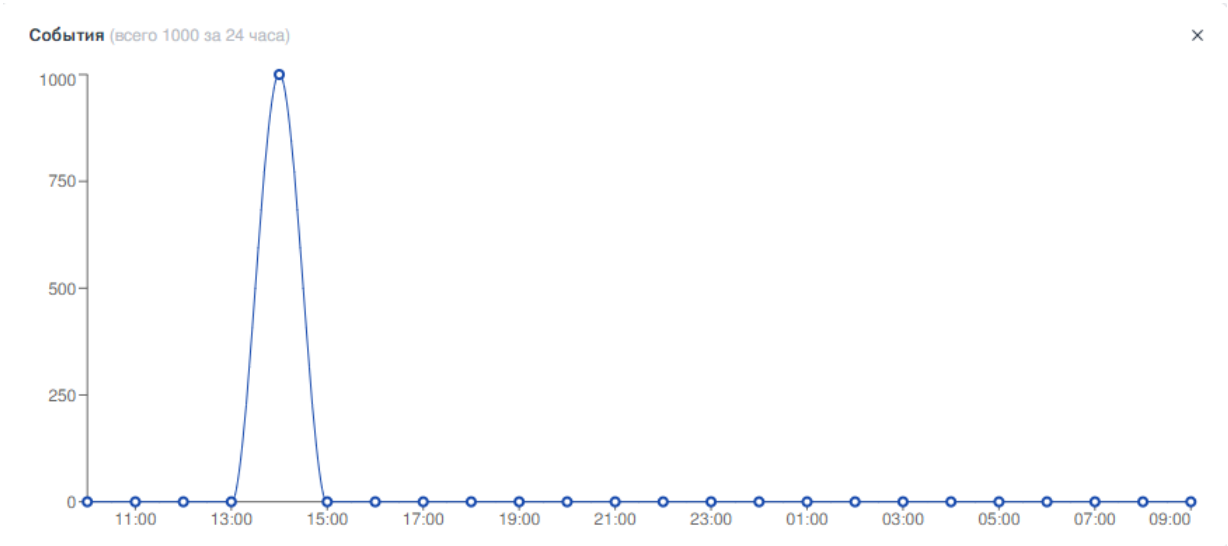


Рисунок – Виджет «События»

Справа от наименования виджета в скобках указано общее количество событий, произошедших за 24 часа.

Вертикальная шкала отображает количество событий за 24 часа с разбивкой на 5 средних значений от максимального числа событий. Горизонтальная шкала отображает количество часов с разбивкой на 24 часа, от 1 до 24.

При наведении на точки диаграммы отображается дата, отрезок времени и количество зарегистрированных в это время событий (см. Рисунок – Отображение количества событий).

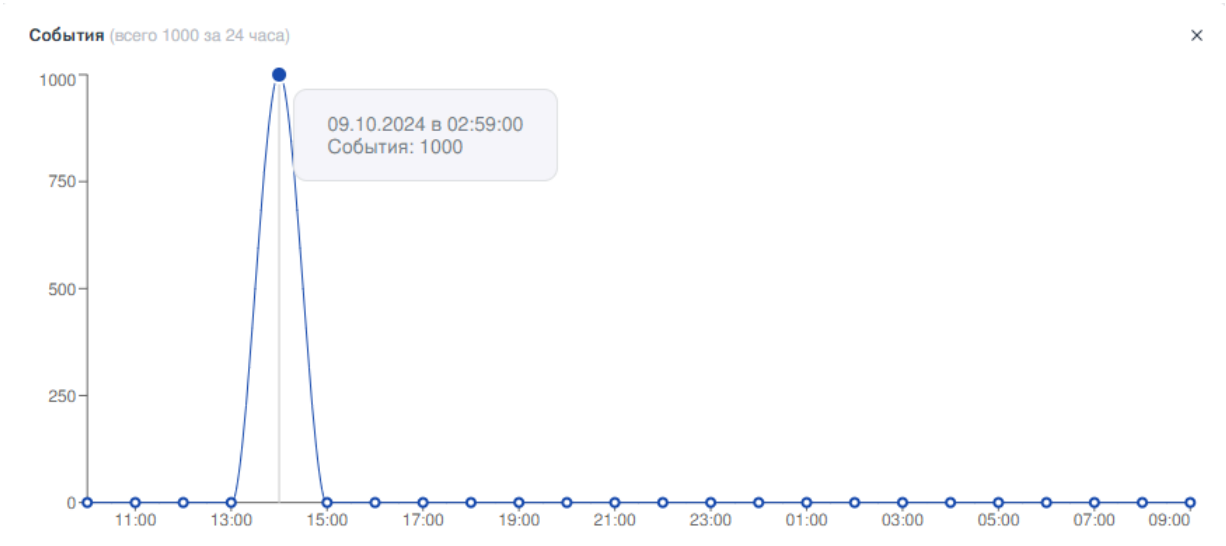


Рисунок – Отображение количества событий

4.5 Виджет «Количество инцидентов по активам за 24 часа»

Виджет **«Количество инцидентов по активам за 24 часа»** отображает информацию о количестве зарегистрированных инцидентов с привязкой к активам (см. Активы настоящего руководства). Информация представлена в виде диаграммы (см. Рисунок – Виджет «Количество инцидентов по активам за 24 часа»).

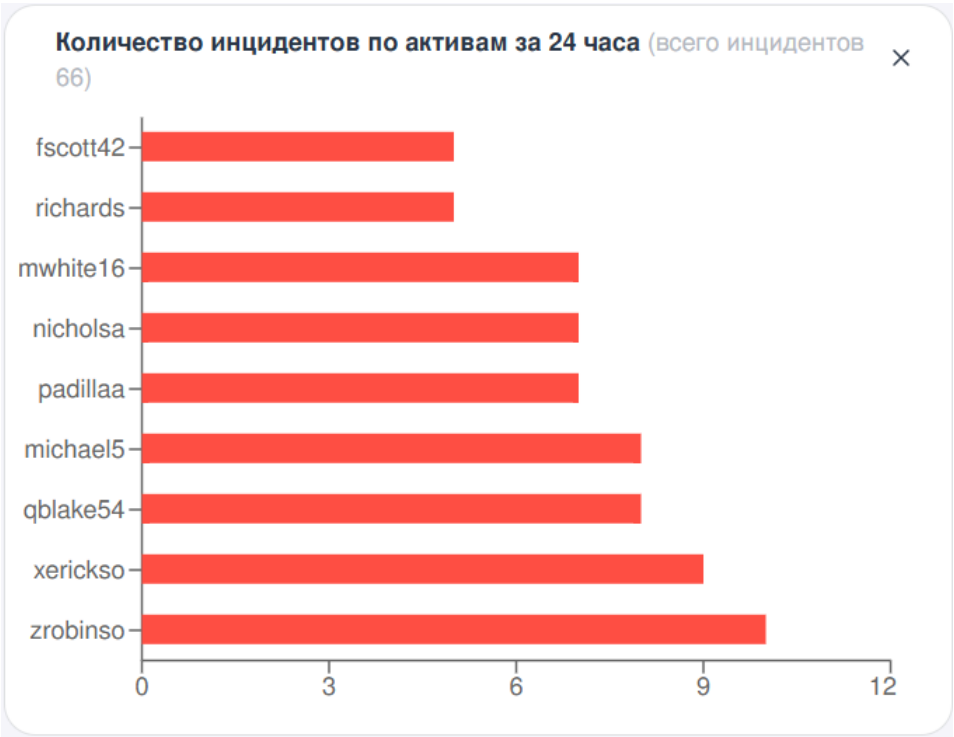


Рисунок – Виджет «Количество инцидентов по активам за 24 часа»

Справа от наименования виджета в скобках указано общее количество зарегистрированных инцидентов.

Вертикальная шкала отображает наименование актива. Горизонтальная шкала отображает количество инцидентов на активе за 24 часа, от 1 до 24.

При наведении на столбцы диаграммы отображается наименование актива и количество пришедших с него инцидентов (см. Рисунок – Отображение инцидентов на активе).

Рисунок – Отображение инцидентов на активе

4.6 Виджет «Статусы источников событий ARMA»

Виджет **«Статусы источников событий ARMA»** отображает информацию о количестве источников событий (см. События настоящего руководства), подключённых к **ARMA MC**, и их статусе. Информация представлена в виде диаграммы (см. Рисунок – Виджет «Статусы источников событий ARMA»).

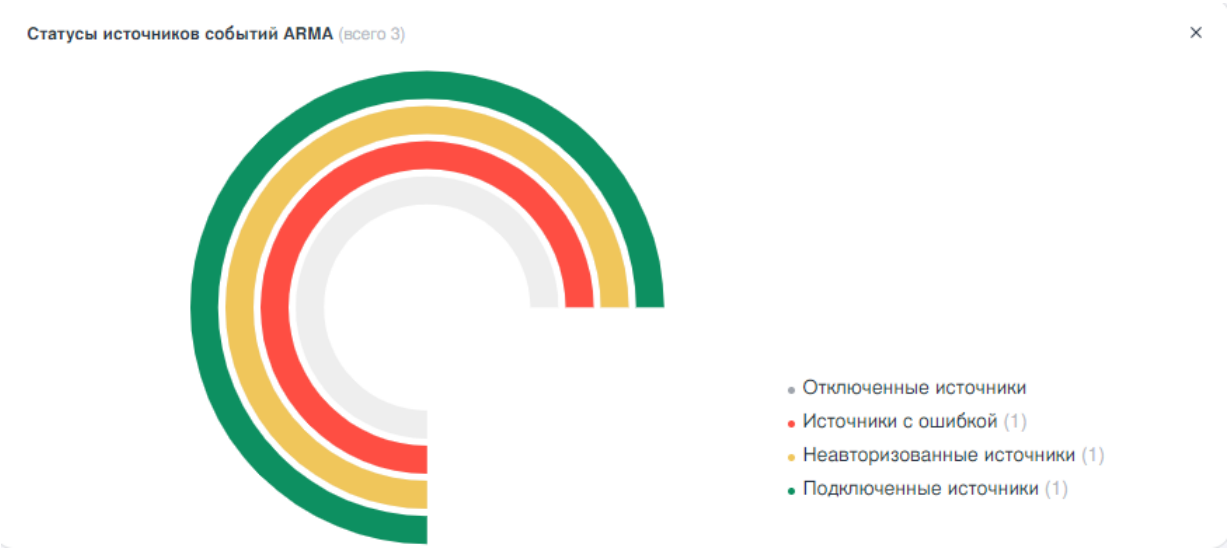


Рисунок – Виджет «Статусы источников событий ARMA»

Справа от наименования виджета в скобках указано общее количество источников, подключённых к **ARMA MC**.

Текстовое поле на диаграмме содержит следующие статусы источников (см. Рисунок – Статусы источников):

- **«Отключенные источники»**;
- **«Источники с ошибкой»**;
- **«Неавторизованные источники»**;
- **«Подключенные источники»**.

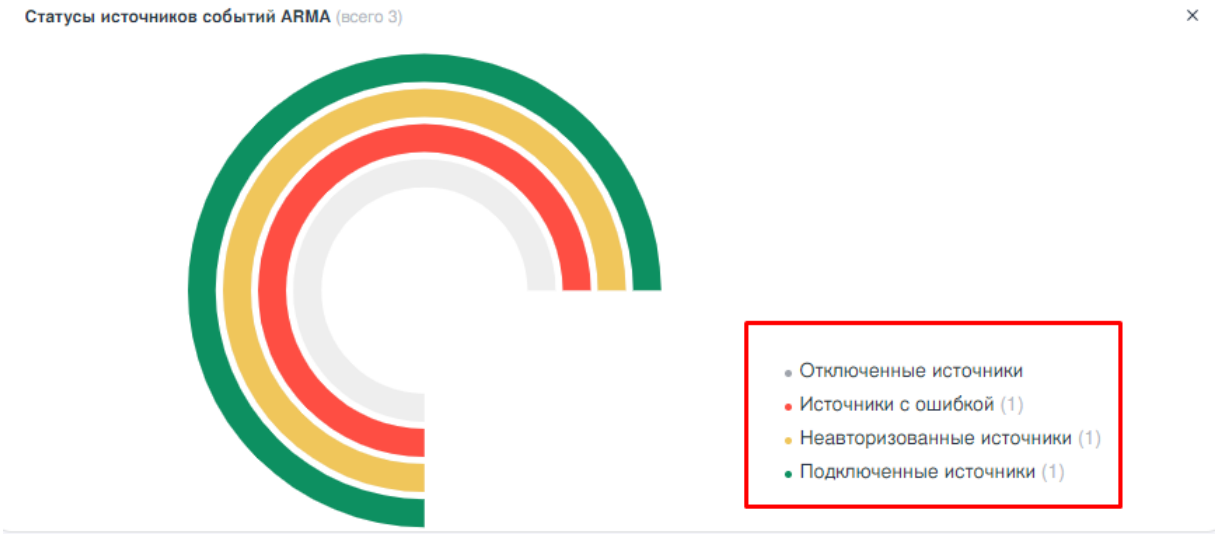


Рисунок – Статусы источников

Справа от статуса источника в скобках указано количество источников в каждом статусе.

При наведении на строку с каждым статусом подсвечивается соответствующая зона диаграммы (см. Рисунок – Отображение статуса источников):

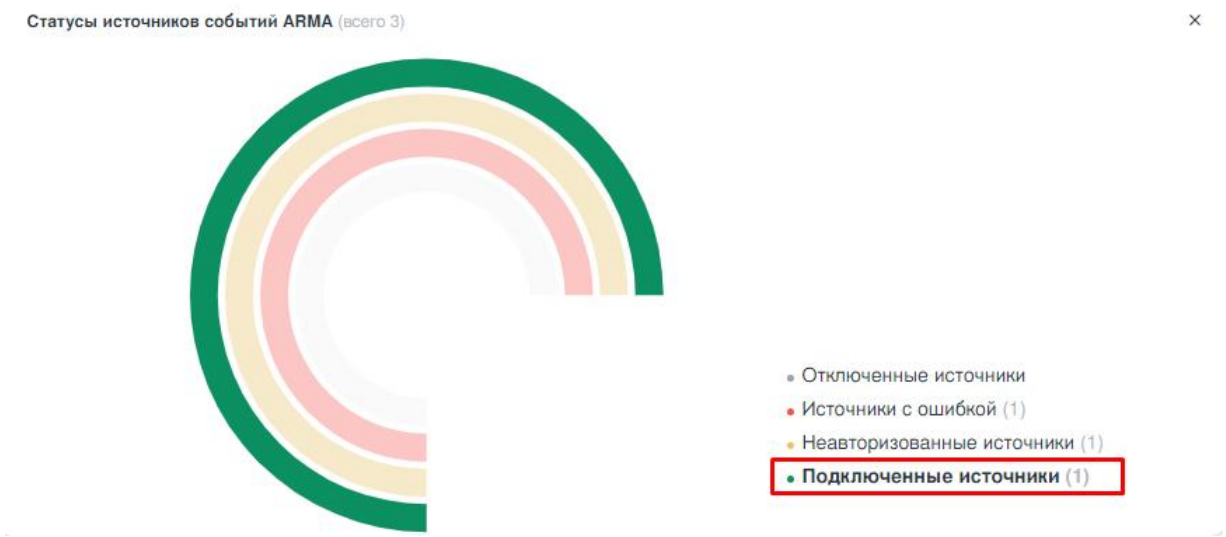


Рисунок – Отображение статуса источников

4.7 Виджет «Топ 10 источников с отклонениями»

Виджет **«Топ 10 источников с отклонениями»** отображает 10 источников **«NGFW»** (подробнее см. Руководство пользователя по эксплуатации ARMA Стена) с наибольшим количеством выявленных отклонений состояния аппаратной платформы.

Информация представлена в виде диаграммы (см. Рисунок – Виджет «Топ 10 источников с отклонениями»).

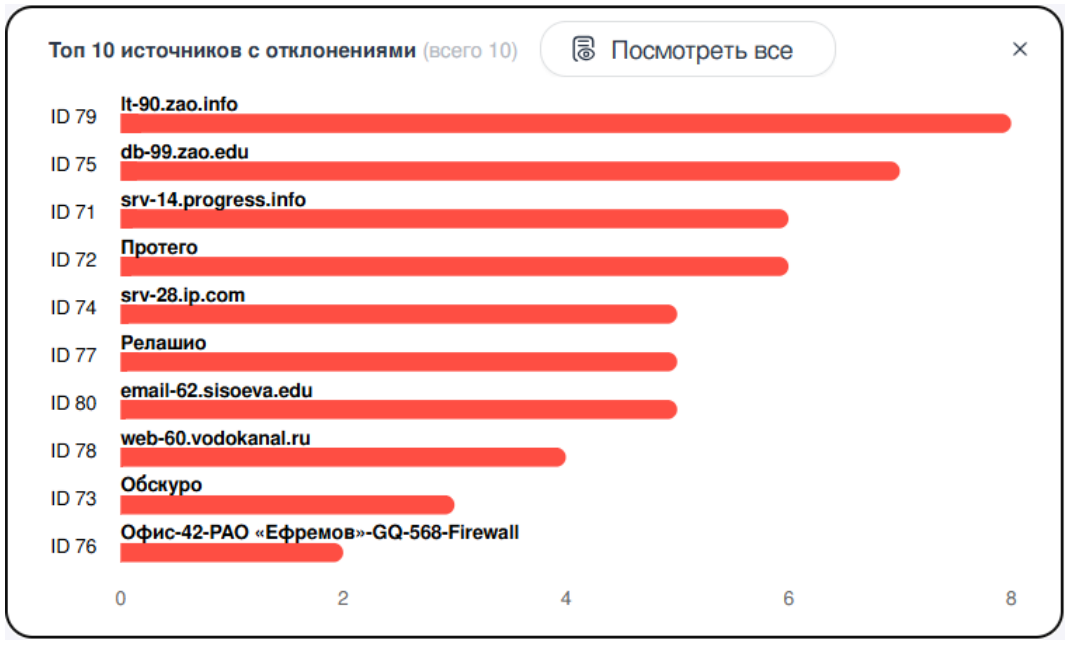


Рисунок – Виджет «Топ 10 источников с отклонениями»

Вертикальная шкала содержит идентификатор источника. Горизонтальная шкала отображает количество выявленных отклонений.

Над каждым столбцом выводится наименование источника. При наведении на столбец отображается число отклонений, выявленных для данного источника.

При нажатии на столбец выводится таблица **«Мониторинг параметров аппаратной платформы»**, содержащая список всех полученных параметров источника (см. Рисунок – Виджет «Топ 10 источников с отклонениями»).

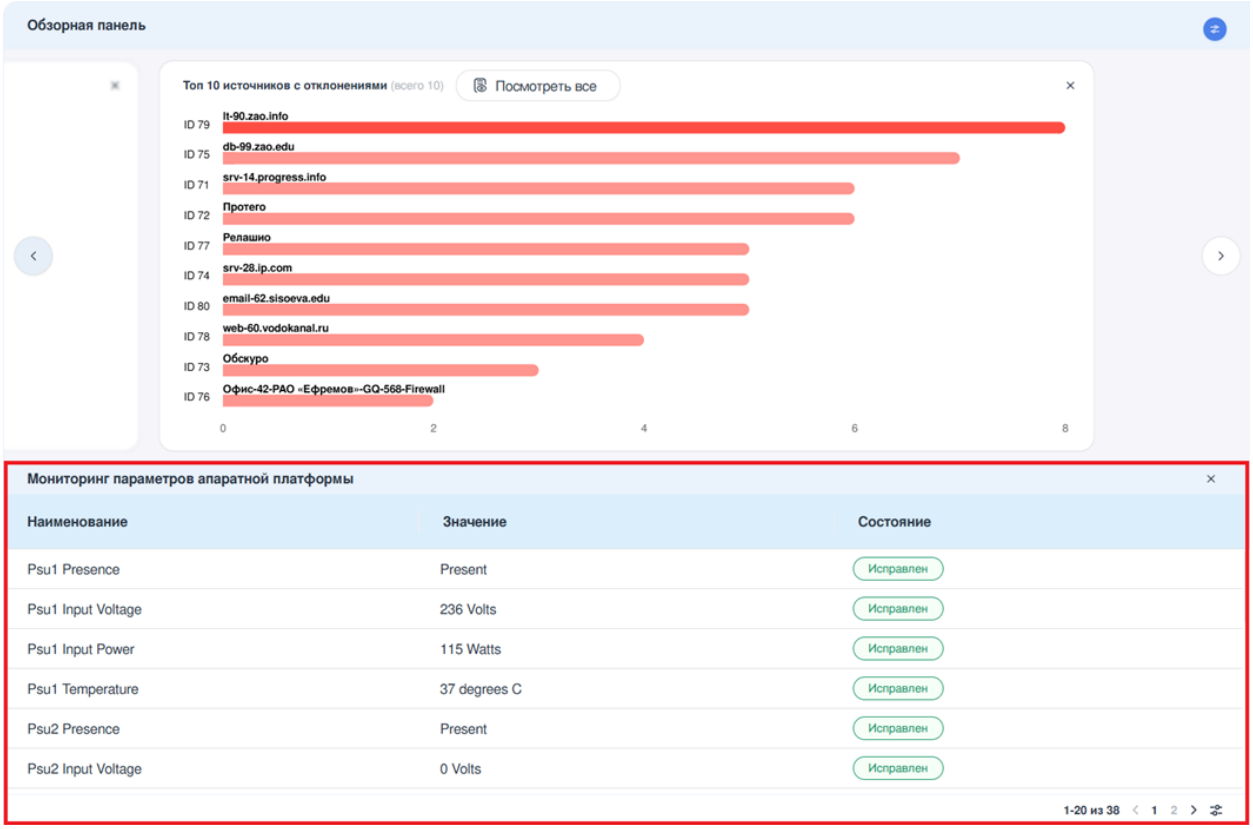


Рисунок – Таблица «Мониторинг параметров аппаратной платформы»

Нажатие на элемент **«Посмотреть все»** позволяет просмотреть данные по источникам в виде таблицы **«Список всех источников отклонений»** (см. Рисунок – Виджет «Топ 10 источников с отклонениями»).

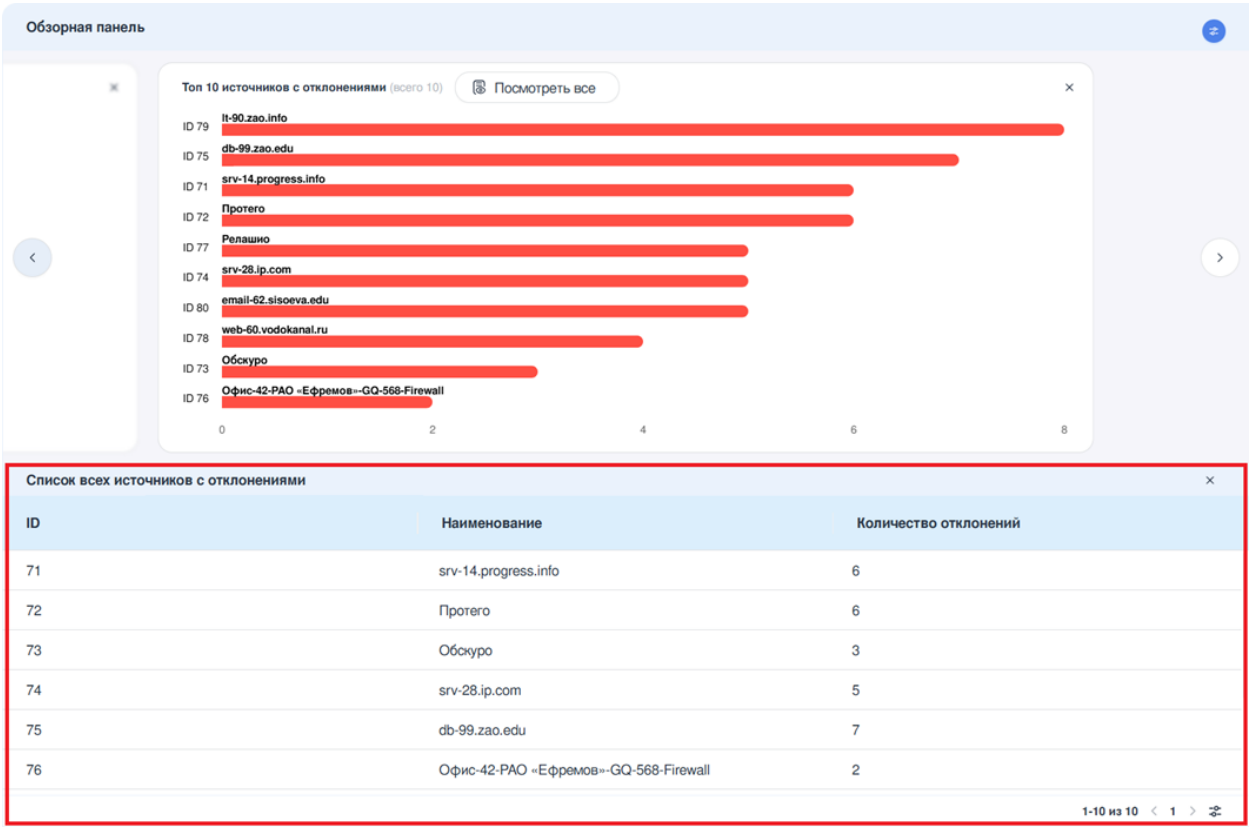


Рисунок – Таблица «Список всех источников отклонений»

4.8 Виджет «Статусы кластеров»

Виджет **«Статусы кластеров»** отображает информацию о количестве и статусе кластеров источников «NGFW», подключённых к **ARMA MC**. Информация представлена в виде диаграммы (см. Рисунок – Виджет «Статусы кластеров»).

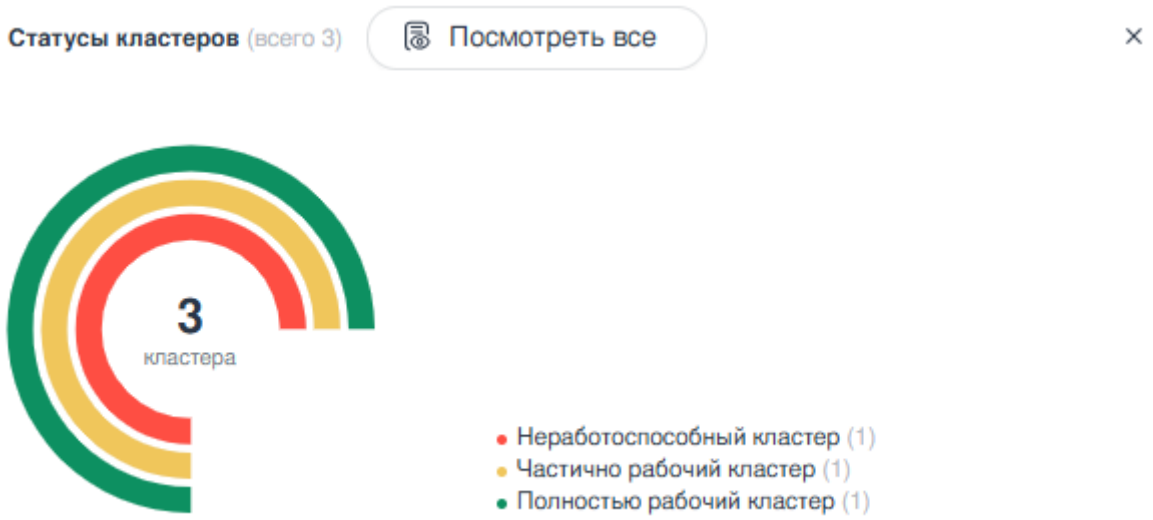


Рисунок – Виджет «Статусы кластеров»

Справа от наименования виджета в скобках указано общее количество кластеров, подключённых к **ARMA MC**.

Текстовое поле на диаграмме содержит следующие статусы кластеров (см. Рисунок – Статусы кластеров):

- **«Неработоспособный кластер»** – в составе кластера отсутствует источник «NGFW» в роли «MASTER» либо роли всех устройств кластера соответствуют значениям «FAULT» или «Не определена»;
- **«Частично рабочий кластер»** – роль какого-либо устройства в составе кластера соответствует значениям «FAULT» или «Не определена»;
- **«Полностью рабочий кластер»** – все устройства в составе кластера в рабочем состоянии.

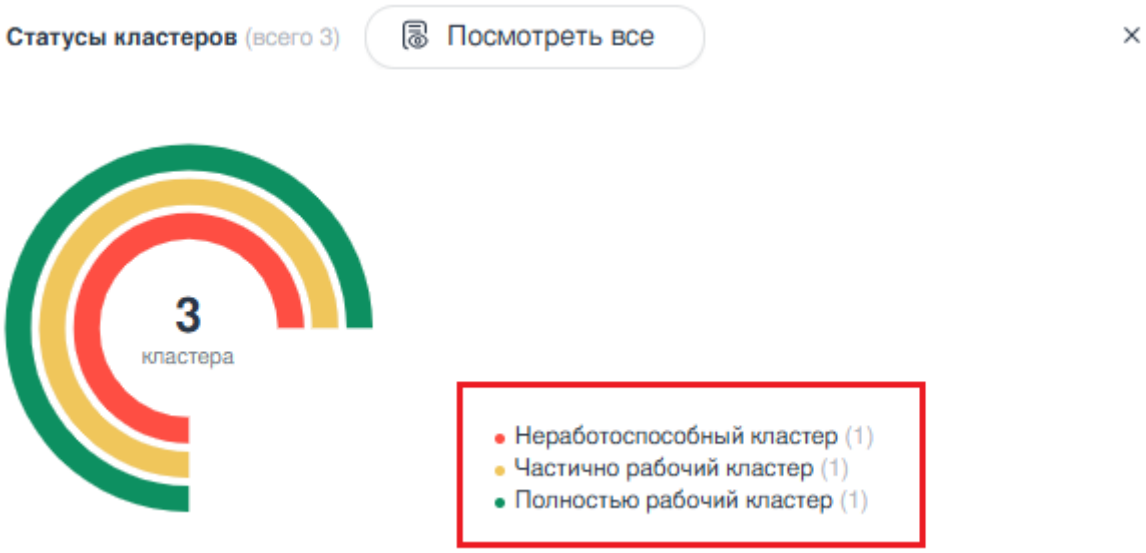


Рисунок – Статусы кластеров

Справа от статуса кластера в скобках указано количество кластеров в каждом статусе.

При наведении на строку с каждым статусом подсвечивается соответствующая зона диаграммы.

При нажатии кнопки **«Посмотреть все»** дополнительно будет выведена таблица, содержащая информацию только о состоящих в кластерах источниках «NGFW» (см. Кластер источника «NGFW» настоящего руководства).

В таблице можно отфильтровать кластеры с определённым состоянием, кликнув по значению в легенде или на диаграмме. Например, если выбрать Неработоспособный кластер, отобразятся только неработоспособные кластеры.

5 ИСТОЧНИКИ СОБЫТИЙ

В настоящем разделе представлено описание подраздела меню **«Источники»**, предусматривающего механизм управления следующими функциями:

- отображение подключаемых устройств;
- управление подключёнными устройствами.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Администрирование»**, затем – подраздел **«Источники»** (см. Рисунок – Источники).

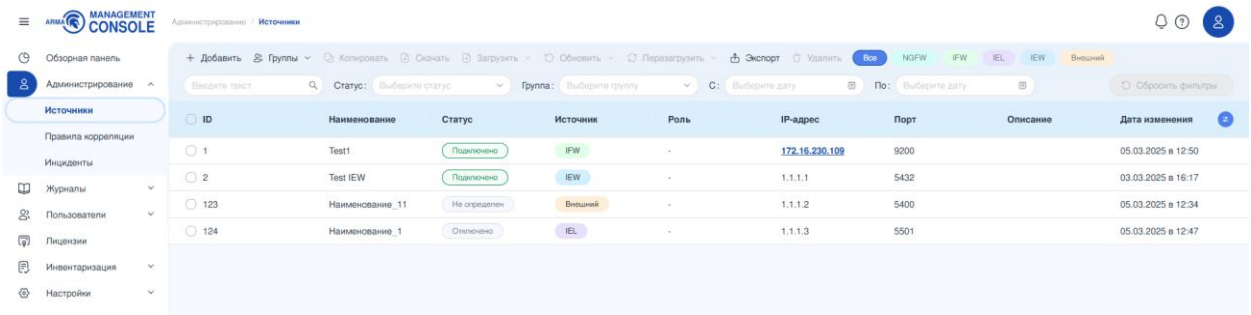


Рисунок – Источники

Подраздел меню позволяет просматривать источники событий в формате таблицы.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

5.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать источники по столбцам списка и по умолчанию состоит из следующих полей (см. Рисунок – Панель инструментов):

- **«Поиск»**;
- **«Статус»**;
- **«Группа»**;
- **«С»**;
- **«По»**;
- **кнопка «Сбросить фильтры»**.

Для фильтрации по типу источника на панели инструментов выделены отдельные кнопки соответствующего цвета. Можно фильтровать список как по одному, так и по нескольким типам. Кнопка **«Все»** показывает все источники.

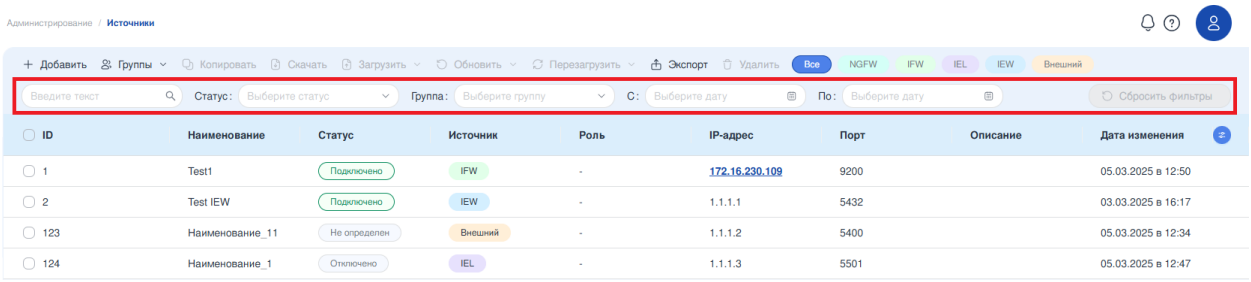


Рисунок – Панель инструментов

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам **«Наименование»**, **«Источник»**, **«IP-адрес»**, **«Описание»**.

Фильтрация по полю **«Статус»** позволяет отфильтровать данные по статусу источника. Поле **«Статус»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Подключено»** – статус отображается, если источник подключён к сети и отвечает на все запросы **ARMA MC**. Может быть присвоен любому источнику;
- **«Отключено»** – статус отображается в процессе подключения источника к **ARMA MC** или при отсутствии связи с устройством. Может быть присвоен любому источнику;
- **«Ошибка»** – статус отображается, если произошла ошибка, которая может быть связана с аппаратным или программным обеспечением источника **«NGFW»**;
- **«Перезагрузка»** – статус отображается в процессе перезагрузки источника **«IEL»**;
- **«Не авторизован»** – статус отображается, если пользователь не прошёл процесс авторизации или указал неверные учётные данные, поэтому не имеет доступа к системе или ресурсам. Может быть присвоен источникам **«NGFW»** и **«IFW»**;
- **«Не определен»** – статус источника **«Внешний источник»**.

Фильтрация по полю **«С»** позволяет отфильтровать источники по дате изменения и задаёт начальную дату диапазона. После ввода даты в таблице отобразятся лишь те источники, дата добавления которых совпадает или больше введённой в фильтр.

Фильтрация по полю **«По»** позволяет отфильтровать источники по дате изменения и задаёт конечную дату диапазона. После ввода даты в таблице отобразятся лишь те источники, дата добавления которых совпадает или меньше введённой в фильтр.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

5.2 Управление источниками событий

ARMA MC позволяет управлять следующими источниками событий:

- **«ARMA Стена (NGFW)»**, сокращённо **«NGFW»** (см. Источник «NGFW»);
- **«Industrial Firewall»**, сокращённо **«IFW»** (см. Источник «Industrial Firewall»);
- **«Industrial EndPoint Windows»**, сокращённо **«IEW»** (см. Источник «Industrial EndPoint Windows»);
- **«Industrial EndPoint Linux»**, сокращённо **«IEL»** (см. Источник «Industrial EndPoint Linux»);
- **«Внешнее устройство»** (см. Источник «Внешнее устройство»).

Количество доступных к добавлению устройств определяется параметрами лицензии (см. Лицензии). При превышении количества источников событий, доступного в соответствии с установленной лицензией, кнопка **«Добавить»** будет неактивна.

5.3 Источник «NGFW»

Примечание:

В случае задействования сертифицированной по 4 уровню доверия, классам Б, Д и СОВ **ARMA Стена (NGFW) 4.5** необходимо обеспечить использование **ARMA MC** исключительно внутри доверенного контура.

5.3.1 Добавление источника «NGFW»

Для подключения **«NGFW»** к **ARMA MC** необходимо выполнить следующие шаги:

1. В **«NGFW»** создать УЗ с правами администратора и с ключом API (см. раздел **«Установка и первоначальная настройка системы»** Руководства администратора **ARMA Стена**).
2. В **ARMA MC** на панели инструментов нажать кнопку **«Добавить»**.
3. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«NGFW»** и указать значения следующих параметров (см. Рисунок – Добавление нового источника событий «NGFW»):
   - **«Наименование»** – отображаемое в **ARMA MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
   - **«IP-адрес»** – IP-адрес подключаемого устройства;

- **«Логин пользователя»** – учётная запись пользователя, созданного на стороне **«NGFW»**;
- **«API-Ключ»** – API-ключ, созданный на стороне **«NGFW»** (см. раздел **«Веб-интерфейс»** Руководства администратора **ARMA Стена**);

Примечание:

Если добавить источник **«NGFW»** с неверными реквизитами для подключения, **«NGFW»** (**ARMA Стена**) со своей стороны заблокирует дальнейшие попытки подключения на 10 минут. При этом в **ARMA MC** этот источник сначала перейдёт в состояние **«Неавторизован»**, а затем в **«Отключен»**. Если это произошло, необходимо исправить данные и сохранить изменения. Подключение произойдёт через 10 минут.

- **«Порт»** – значение порта входящих логов. Указываются порты в диапазоне от 1500 до 65535. Значение должно быть уникальным, не заданным ранее.

Примечание:

Переключатель **«Передача шифрованных событий»** активирует режим приёма зашифрованных логов с данного источника (подробнее см. Просмотр шифрованных событий).

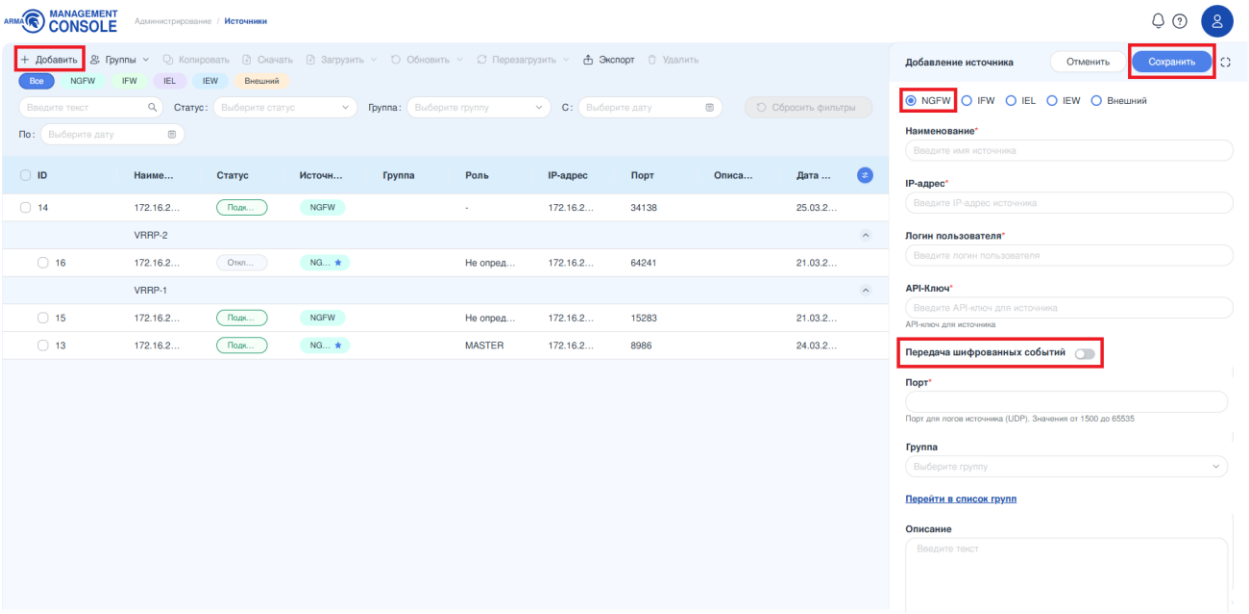


Рисунок – Добавление нового источника событий «NGFW»

4. Если источник нужно добавить в одну или несколько групп, следует выбрать требуемые группы из выпадающего списка в поле **«Группа»**.

Примечание:

Для удаления источника из группы, достаточно нажать на крестик рядом с наименованием группы или снять отметку с группы в выпадающем списке.

Если необходимо создать новую группу, это можно сделать в списке групп по ссылке **«Перейти в список групп»** (подробнее о группах см. Группы источников).

5. При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.
6. Нажать **«Сохранить»** для внесения изменений.

5.3.2 Просмотр шифрованных событий

В **ARMA MC** есть возможность принимать и просматривать шифрованные события **ARMA Стена (NGFW)**. Для активации режима приёма шифрованных событий используется переключатель **«Передача шифрованных событий»** в карточке источника **«NGFW»** (см. Добавление источника «NGFW»), передающего шифрованные данные.

Если переключатель активирован, события принимаются по протоколу **«TCP»** на порт **«6514»**, иначе события принимаются в незашифрованном виде по протоколу **«UDP»** на порт, указанный в поле **«Порт»** карточки источника.

5.3.3 Кластер источника «NGFW»

После интеграции нового источника **«NGFW»** в систему происходит его классификация по критериям принадлежности к определённому кластеру. Все источники **«NGFW»**, относящиеся к одному кластеру, объединяются в группу, которой присваивается наименование, соответствующее обозначению группы vrrp в конфигурационных настройках **«NGFW»** (см. Рисунок – Кластер источников «NGFW»).

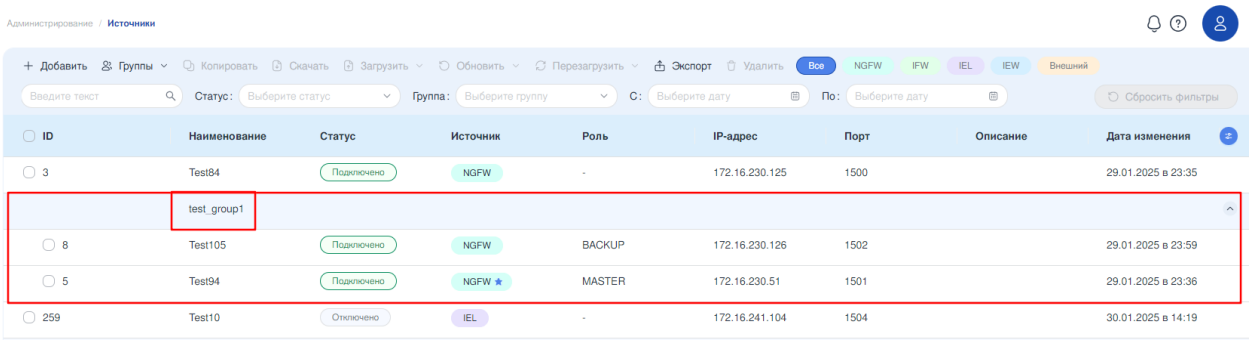


Рисунок – Кластер источников «NGFW»

Примечание:

Информация о принадлежности источников **«NGFW»** к определённому кластеру является статичной. Для актуализации этих данных необходимо обновить страницу браузера.

Информация о роли источника **«NGFW»** в кластере представлена в столбце **«Роль»** таблицы **«Источники»**, который может содержать следующие значения:

- **«MASTER»** – основное устройство, которое имеет наивысший приоритет в рамках одного кластера;
- **«BACKUP»** – резервное устройство, имеющее меньший приоритет по сравнению с «MASTER»;
- **«FAULT»** – состояние ошибки, в большинстве случаев возникает из-за сбоя или отключения интерфейса, связанного с кластером;
- **«Не определена»** – значение отображается, когда устройство отключено или возникает ошибка при запросе статуса VRRP. При этом приоритет источника остаётся неизменным.

Сведения о роли источника **«NGFW»** обновляются с периодичностью в 30 секунд.

Примечание:

Источник **«NGFW»** не может одновременно принадлежать двум и более кластерам.

В случае если источник **«NGFW»** имеет локальные настройки для более чем одного кластера, в **ARMA MC** будет отображаться первый по алфавиту кластер.

Например, в **«NGFW»** настроены два кластера: «vrrp_group1» и «vrrp_group2». В первом кластере **«NGFW»** назначен основным устройством, а во втором – резервным. При таких настройках в **ARMA MC** будет отображаться только кластер «vrrp_group1», а роль **«NGFW»** будет обозначена как «MASTER». Информация о наличии второго кластера на данном источнике **«NGFW»** отображаться не будет.

Источник **«NGFW»** с наивысшим приоритетом в кластере маркируется специальным символом «звезда» – « ★ » (см. Рисунок – Источник «NGFW» с наивысшим приоритетом в кластере).

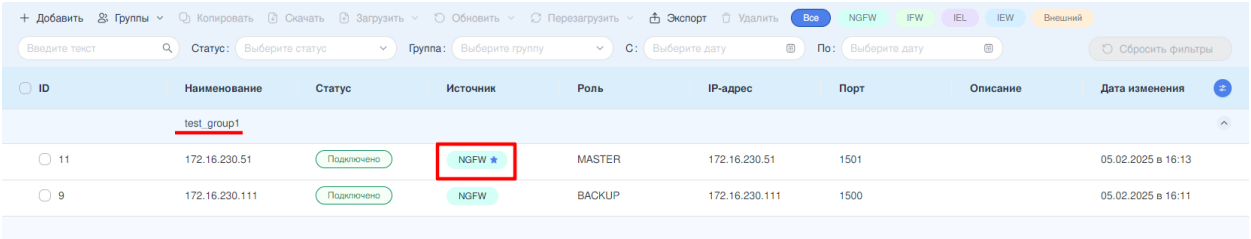


Рисунок – Источник «NGFW» с наивысшим приоритетом в кластере

В случае выхода из строя основного **«NGFW»** (Master) и перехода его функций к резервному **«NGFW»** (Backup), специальный символ «звезда» сохраняется на устройстве с более высоким приоритетом в кластере, то есть на основном **«NGFW»**,

который утратил работоспособность. Это позволяет определить, какое устройство вышло из строя – основное или резервное (см. Рисунок – Варианты отображения кластера источников «NGFW» в случае неисправности).

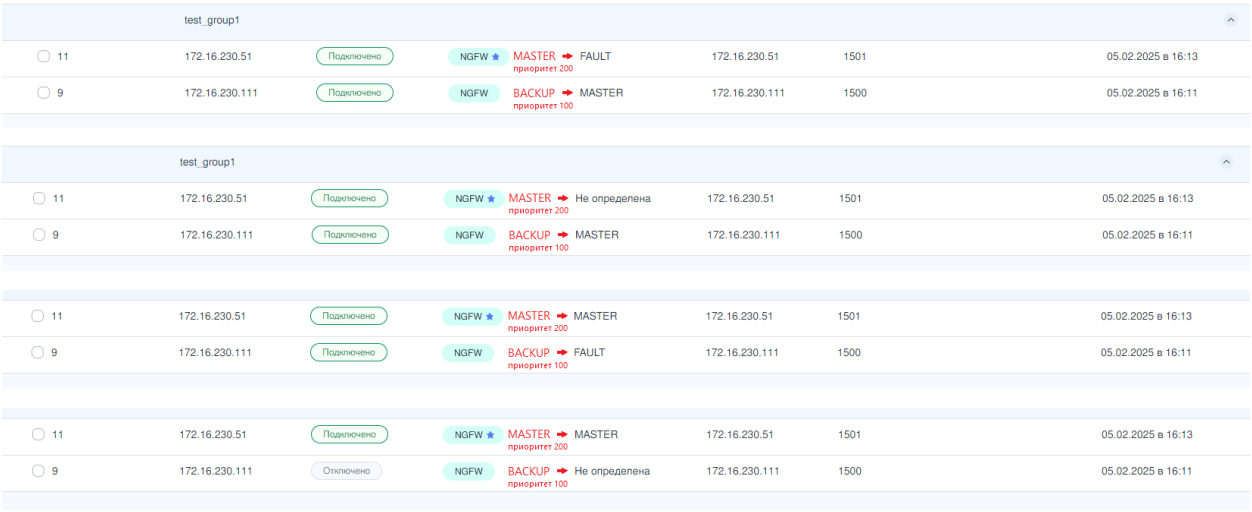


Рисунок – Варианты отображения кластера источников «NGFW» в случае неисправности

Примечание:

В случае, если в **ARMA MC** используется только один источник **«NGFW»** из кластера, ему присваивается специальный символ «звезда» независимо от его значения приоритета в кластере. Это связано с отсутствием информации о приоритетах других участников кластера.

В случае, если в настройках работы кластера **«NGFW»** параметр **«Вытеснение»** отключён, возможно возникновение ситуации, при которой все участники кластера находятся в рабочем состоянии, но роль основного **«NGFW»** выполняет устройство с более низким приоритетом по сравнению с резервным. В этом случае кластер будет отображаться в системе **ARMA MC** следующим образом (см. Рисунок – Режим работы кластера, при котором функция «Вытеснение» отключена).

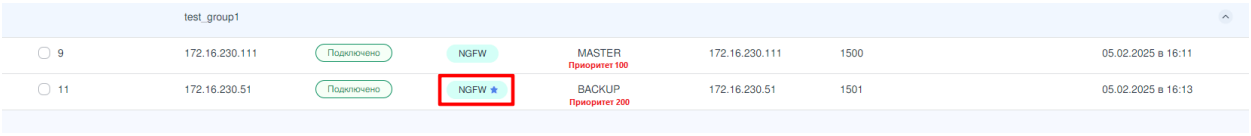


Рисунок – Режим работы кластера, при котором функция «Вытеснение» отключена

Информация о принадлежности источника к кластеру отображается в веб-интерфейсе **«NGFW»** в правом верхнем углу заголовка каждого раздела (см. Рисунок – Информация о принадлежности источника к кластеру). Отображаемые данные включают следующие поля:

- **«Пользователь»** — имя учётной записи, используемой для входа в веб-интерфейс, и имя хоста. Формат: *имя_УЗ@host*.
- **«Группа кластера»** — название группы VRRP или группы синхронизации с указанием роли устройства в этой группе. Для группы VRRP в скобках дополнительно отображается значение приоритета устройства.

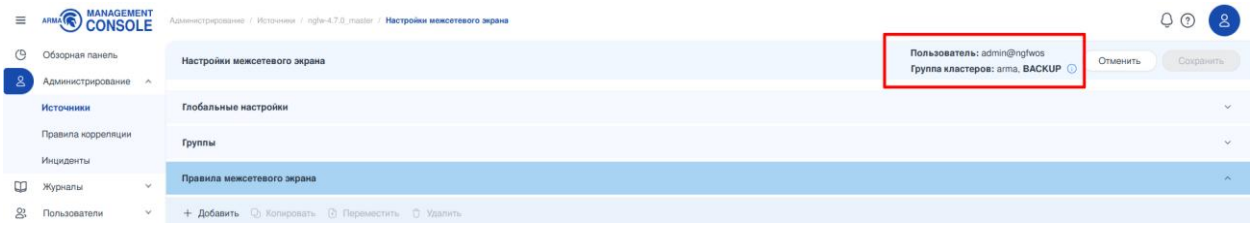


Рисунок – Информация о принадлежности источника к кластеру

Если конфигурация устройства содержит несколько групп VRRP и групп синхронизации, то в заголовке отображается группа, идущая первой по алфавитному порядку имени. Полный перечень всех групп VRRP и групп синхронизации, настроенных на устройстве, доступен по нажатию на значок «» (см. Рисунок – Полный перечень всех групп VRRP и групп синхронизации).

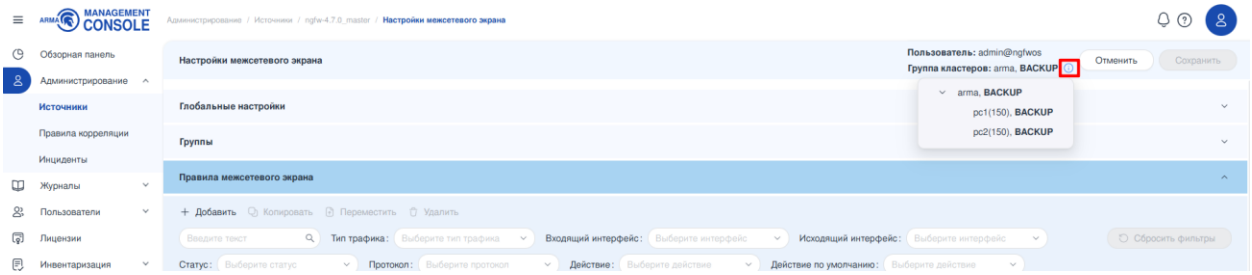


Рисунок – Полный перечень всех групп VRRP и групп синхронизации

5.3.4 Редактирование параметров источника «NGFW»

Для редактирования параметров источника **«NGFW»** необходимо выполнить следующие действия:

1. Выбрать подлежащий редактированию источник **«NGFW»**, кликнув на соответствующую запись в таблице источников.
2. В открывшейся карточке источника внести необходимые изменения в параметры (описание полей карточки источника см. Добавление источника «NGFW»).
3. По завершении редактирования нажать кнопку **«Сохранить»**.

После успешного редактирования источника появится соответствующее уведомление (см. Рисунок – Успешное редактирование источника).

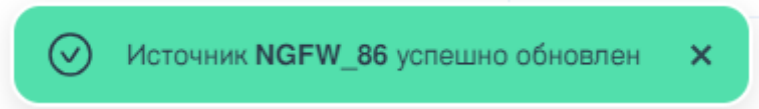


Рисунок – Успешное редактирование источника

5.3.5 Скачивание конфигурации источника «NGFW»

Для скачивания конфигурации одного или нескольких источников **«NGFW»** необходимо выполнить следующие действия (см. Рисунок – Скачивание конфигурации источника событий):

1. Выбрать один или несколько источников **«NGFW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Скачать»**.

Примечание:

У пользователя **«NGFW»**, заданного в параметрах источника, должны быть права на доступ к конфигурации.

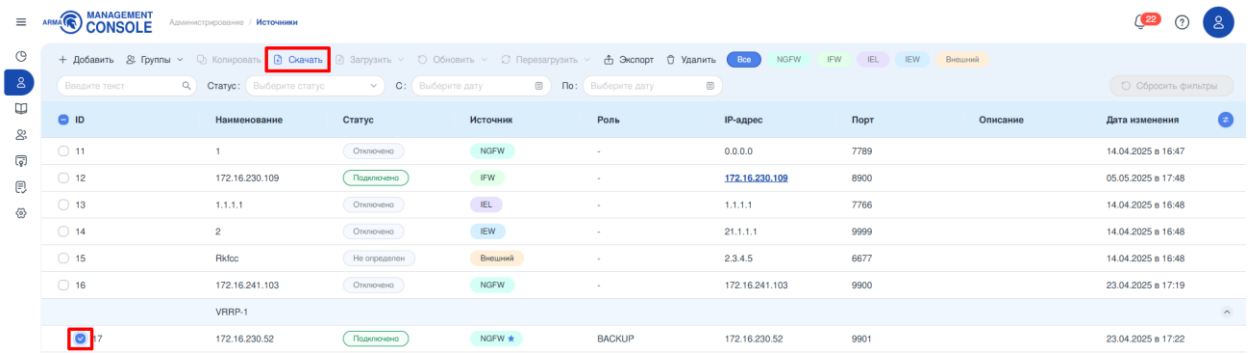


Рисунок – Скачивание конфигурации источника событий

В результате будет импортирован архив с расширением **«zip»**, содержащий следующие файлы:

- **«config.boot»** – основной файл конфигурации;
- **директория «files»** – полная копия содержимого директории «/config/files/», в которой могут быть сертификаты, правила и прочие файлы.

Примечание:

Внутренний формат архива **«7z»**. Для его открытия в ОС **«Windows»** следует использовать сторонние программы, такие как **«7-Zip»** или **«WinRAR»**.

Если конфигурация скачивается с источника **«NGFW»** версии ниже **«4.7»**, импортируется незаархивированный файл с расширением **«.config»**.

При успешном скачивании архива появится соответствующее уведомление (см. Рисунок – Успешное скачивание конфигурации).

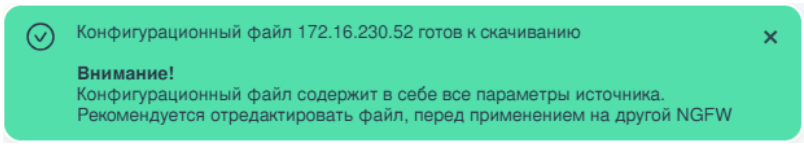


Рисунок – Успешное скачивание конфигурации

Данные конфигурационного файла соответствуют конфигурации, настроенной на конкретном **«NGFW»**.

5.3.6 Загрузка конфигурации источника «NGFW»

Примечание:

Загрузку конфигурации необходимо выполнять на источник **«NGFW»** версии, идентичной с версией того источника **«NGFW»**, с которого была импортирована эта конфигурация.

Для выполнения корректной загрузки конфигурации необходимо предварительно распаковать импортированный с источника **«NGFW»** архив (см. Скачивание конфигурации источника «NGFW»).

Для загрузки конфигурации на источник **«NGFW»** необходимо выполнить следующие действия (см. Рисунок – Загрузка конфигурации на источник событий):

1. Выбрать необходимый источник **«NGFW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Загрузить»**.
3. В выпадающем списке выбрать значение **«Загрузить конфигурацию NGFW»**.

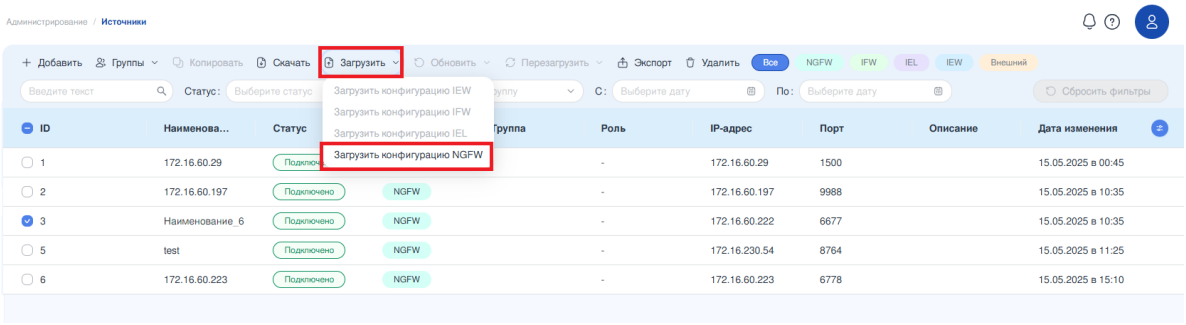


Рисунок – Загрузка конфигурации на источник событий

4. В проводнике установить **«Все файлы»**, выбрать **«config.boot»** и нажать кнопку **«Открыть»**. При успешной загрузке файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешная загрузка конфигурации).

Рисунок – Успешная загрузка конфигурации

Если имя или формат файла не соответствуют требованиям, будет показано сообщение об ошибке (см. Рисунок – Ошибка в наименовании файла и Рисунок – Неверный формат файла).

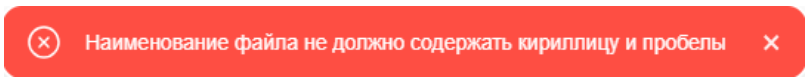


Рисунок – Ошибка в наименовании файла

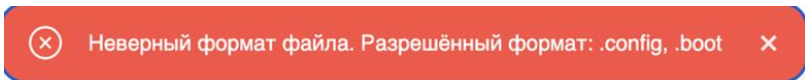


Рисунок – Неверный формат файла

5.3.7 Удаление источника «NGFW»

Для удаления одного или нескольких источников **«NGFW»** необходимо выполнить следующие действия (см. Рисунок – Удаление источника событий):

1. Выбрать необходимые источники **«NGFW»**, установив флажок слева от значений столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Удалить»**.
3. Подтвердить удаление, нажав кнопку **«Удалить»** в открывшемся окне.

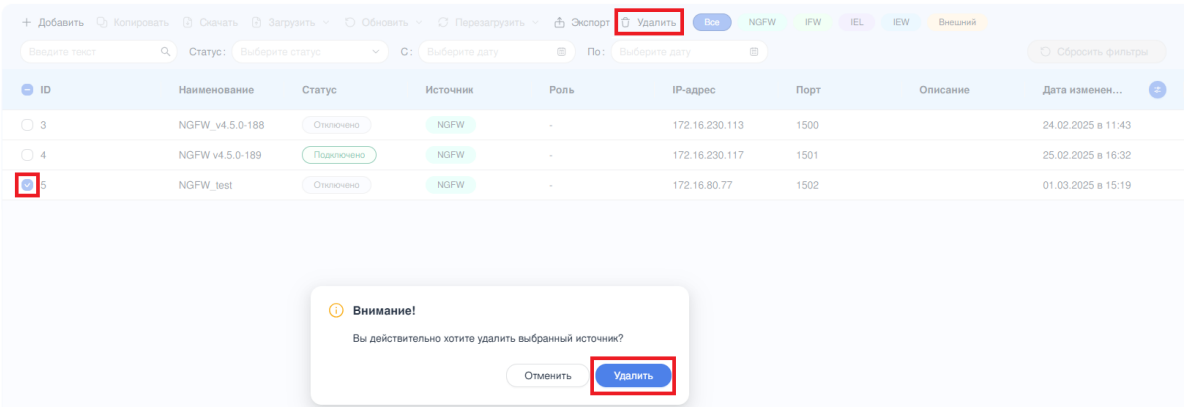


Рисунок – Удаление источника событий

После удаления источника появится соответствующее уведомление (см. Рисунок – Успешное удаление источника).

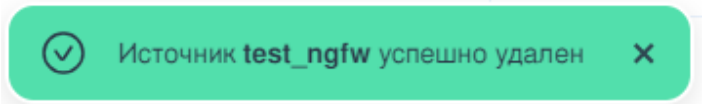


Рисунок – Успешное удаление источника

5.3.8 Группы источников

Объединение источников в группы может быть полезно, например, для объединения источников по структуре подразделений или физическому расположению. За взаимодействие с группами источников отвечает элемент **«Группы»** (см. Рисунок – Группы).

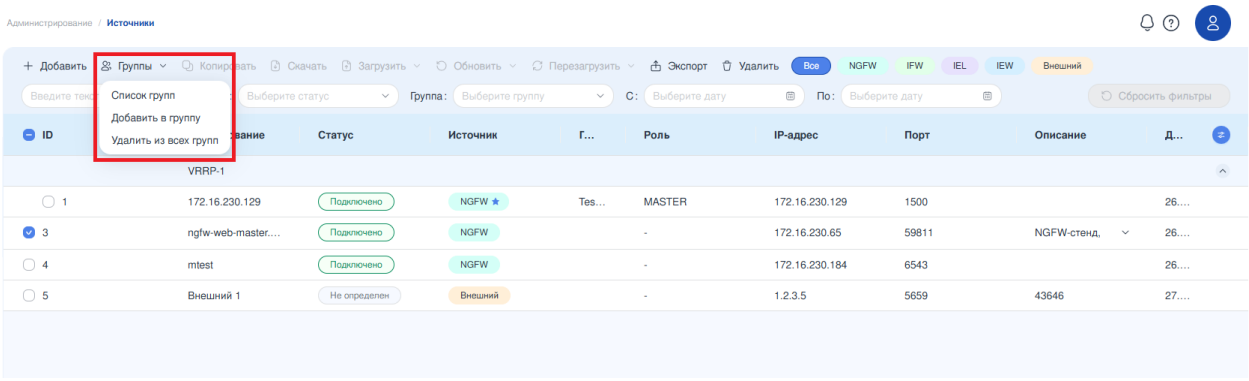


Рисунок – Группы

При нажатии на **«Группы»** отображаются следующие вложенные элементы:

- **«Список групп»** открывает окно, служащее для просмотра, изменения, создания и удаления групп (подробнее см. Работа со списком групп).
- **«Добавить в группу»**. Если при выбранных источниках нажать **«Добавить в группу»**, откроется окно (см. Рисунок – Окно выбора групп), где в выпадающем списке можно отметить одну или несколько групп. По нажатию **«Добавить»** выбранные источники будут добавлены в выбранные группы.

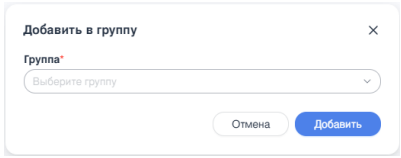


Рисунок – Окно выбора групп

- **«Удалить из всех групп»** позволяет удалить выбранные источники сразу из всех групп, в которых они состоят. Перед удалением будет запрошено подтверждение (см. Рисунок – Подтверждение удаления источников). Если нужно удалить источник **«NGFW»** из каких-то определённых групп, это можно сделать в карточке источника (см. Источник «NGFW»).

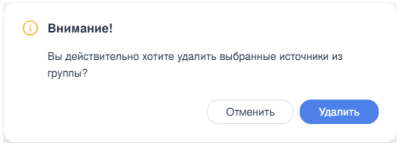


Рисунок – Подтверждение удаления источников

5.3.8.1 Работа со списком групп

В окне **«Список групп»** (см. Рисунок – Список групп) производится просмотр, изменение, добавление и удаление групп.

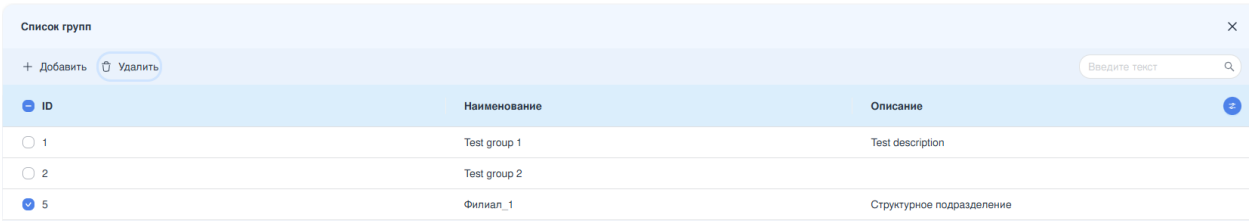


Рисунок – Список групп

Для просмотра или изменения группы достаточно нажать на строку группы, что приведёт к открытию карточки группы для просмотра и редактирования (см. Рисунок – Карточка группы). Карточка содержит поля **«Наименование»** и **«Описание»**. Если были внесены какие-либо изменения, для их применения необходимо нажать **«Сохранить»**.

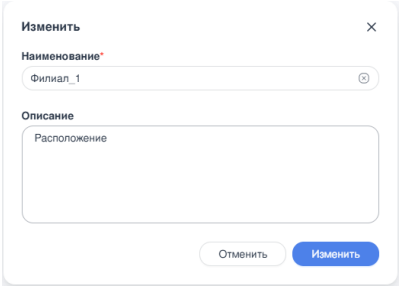


Рисунок – Карточка группы

Для добавления группы необходимо нажать кнопку **«Добавить»**. Откроется карточка группы, описанная ранее (см. Рисунок – Карточка группы). Ввести необходимую информацию и нажать **«Сохранить»**. **«ID»** для созданной группы присваивается автоматически.

Для удаления отмеченных групп используется кнопка **«Удалить»** на панели инструментов окна (см. Рисунок – Список групп). После нажатия **«Удалить»** в окне подтверждения (см. Рисунок – Предупреждение об удалении) группы будут удалены.

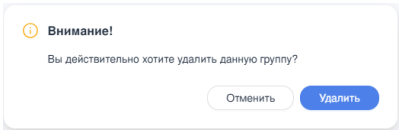


Рисунок – Предупреждение об удалении группы

Если в какой-либо из выбранных к удалению групп есть источники, это будет упомянуто в тексте предупреждения (см. Рисунок – Предупреждение об удалении групп с источниками).

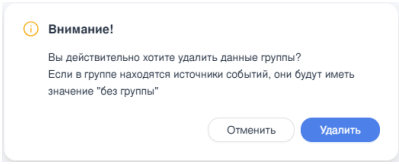


Рисунок – Предупреждение об удалении группы с источниками

5.4 Источник «Industrial Firewall»

5.4.1 Добавление источника «IFW»

Для подключения **«IFW»** к **ARMA MC** необходимо выполнить следующие шаги:

1. В **«IFW»** создать УЗ с правами администратора и ключом API (см. Руководство администратора **ARMA FW** Подключение к ARMA MC).
2. В **ARMA MC** на панели инструментов нажать кнопку **«Добавить»**.
3. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«IFW»** и указать значения следующих параметров (см. Рисунок – Добавление нового источника событий «IFW»):
   - **«Наименование»** – отображаемое в **ARMA MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
   - **«IP-адрес»** – IP-адрес или доменное имя подключаемого устройства. Не рекомендуется изменять IP-адрес добавляемого устройства после подключения к **ARMA MC** с целью исключения потери управления;
   - **«Ключ»** – ключ API. Параметр может содержать только латинские буквы, цифры, спецсимволы («+», «/») и должен состоять из 80 символов;
   - **«Секрет»** – значение «секрета» ключа API. Параметр может содержать только латинские буквы, цифры, спецсимволы («+», «/») и должен состоять из 80 символов;
   - **«Порт»** – значение порта входящих логов. Указываются порты UDP в диапазоне от 1500 до 65535. Значение должно быть уникальным, не заданным ранее.

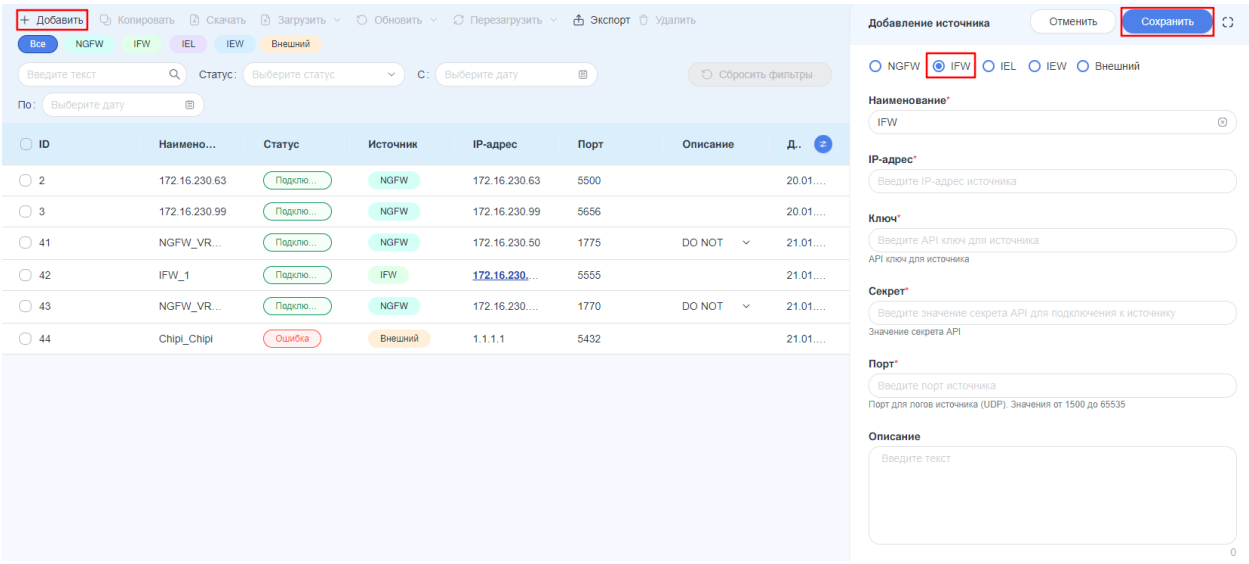


Рисунок – Добавление нового источника событий «IFW»

4. При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.
5. В **«IFW»** настроить экспорт событий по протоколу «Syslog» (см. Руководство пользователя **ARMA FW** Сервис Syslog).
6. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки источника.

   Примечание:

   Для успешной обработки событий от **«IFW»** в **ARMA MC** необходима точная синхронизация времени между устройствами.

Для удобства работы с источником, после его добавления в карточке источника появится ссылка для перехода в веб-интерфейс **«IFW»** (см. Рисунок – Ссылка на веб-интерфейс источника «IFW»). Ссылка откроется в новой вкладке браузера.

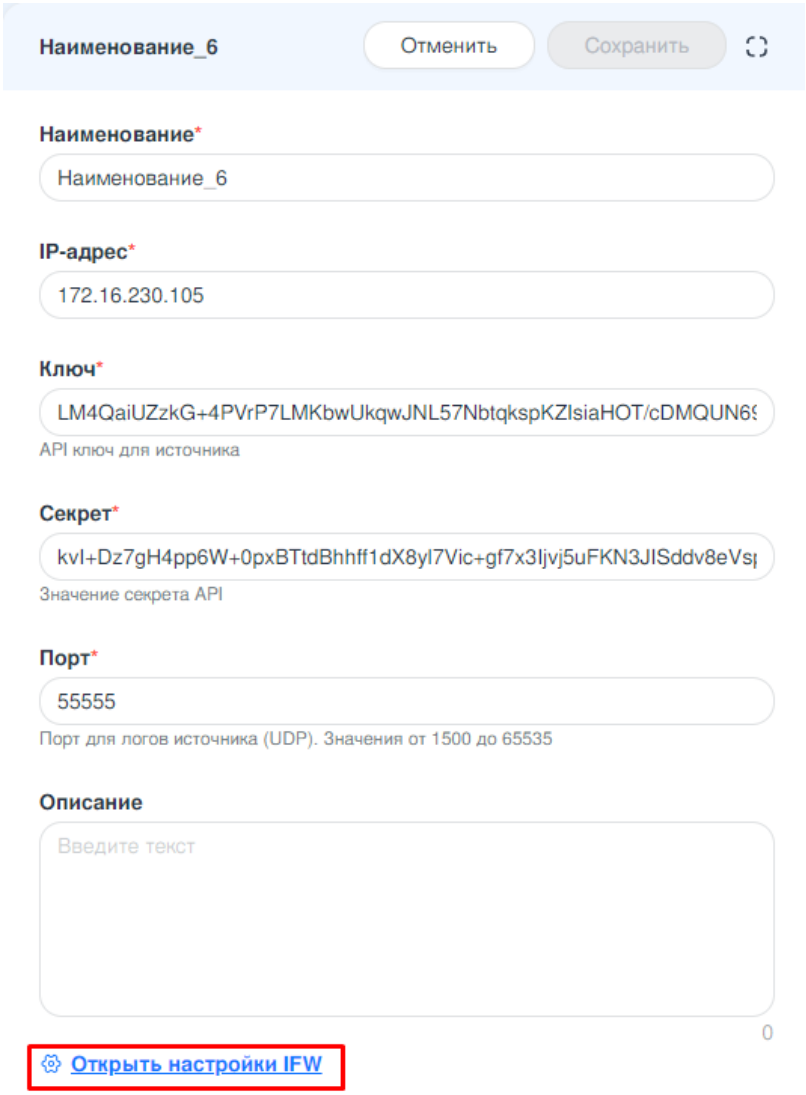


Рисунок – Ссылка на веб-интерфейс источника «IFW»

Переход в веб-интерфейс **«IFW»** также осуществляется нажатием на IP-адрес источника в таблице источников.

5.4.2 Редактирование параметров источника «IFW»

Для редактирования параметров источника **«IFW»** необходимо выполнить следующие действия:

1. Выбрать подлежащий редактированию **«IFW»**, нажав на запись с источником.
2. Указать требуемые значения параметров в открывшейся форме **«Изменить источник»** и нажать кнопку **«Сохранить»** для сохранения информации.

После успешного редактирования источника появится соответствующее уведомление (см. Рисунок – Успешное редактирование источника).

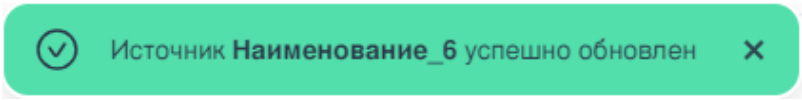


Рисунок – Успешное редактирование источника

5.4.3 Скачивание конфигурации источника «IFW»

Для скачивания конфигурации одного или нескольких источников **«IFW»** необходимо выполнить следующие действия (см. Рисунок – Скачивание конфигурации источника событий):

1. Выбрать необходимый источник **«IFW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Скачать»**.

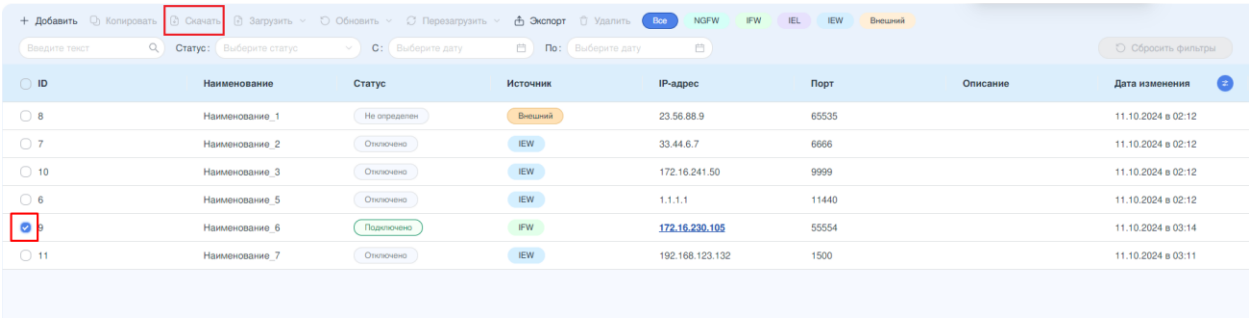


Рисунок – Скачивание конфигурации источника событий

Формат скачиваемого файла – **«xml»**. При успешном скачивании файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешное скачивание конфигурации).

Рисунок – Успешное скачивание конфигурации

Данные конфигурационного файла полностью соответствуют конфигурации, настроенной на конкретном **«IFW»**.

5.4.4 Загрузка конфигурации источника «IFW»

Для загрузки конфигурации на источник **«IFW»** необходимо выполнить следующие действия (см. Рисунок – Загрузка конфигурации на источник событий):

1. Выбрать необходимый источник **«IFW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Загрузить»**.
3. В выпадающем списке выбрать значение **«Загрузить конфигурацию IFW»**.

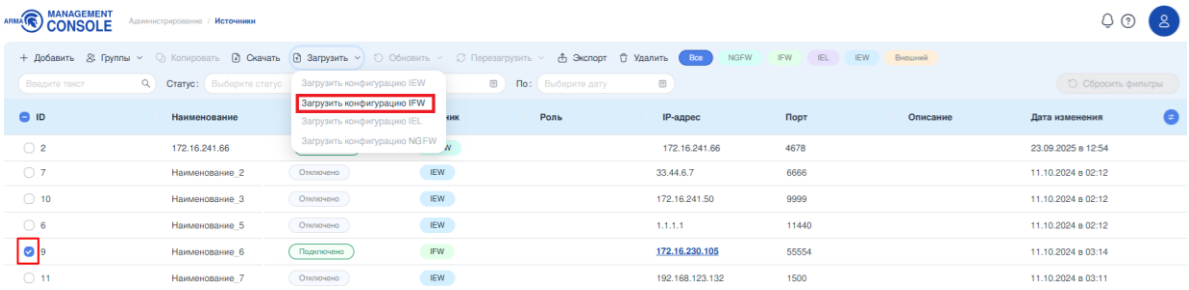


Рисунок – Загрузка конфигурации на источник событий

4. В проводнике выбрать конфигурационный файл и нажать кнопку **«Открыть»**. При успешной загрузке файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешная загрузка конфигурации).

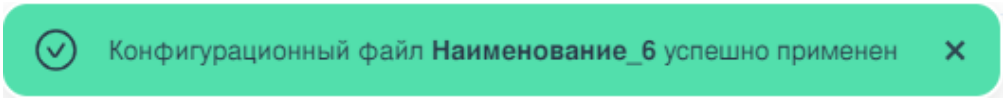


Рисунок – Успешная загрузка конфигурации

5. После загрузки файла произойдет автоматическая перезагрузка источника.

При возникновении проблем с загрузкой файла конфигурации появится уведомление (см. Рисунок – Загрузка некорректного файла конфигурации).

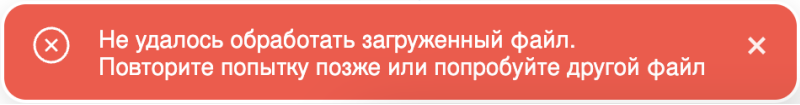


Рисунок – Загрузка некорректного файла конфигурации

Примечание:

Загрузка конфигурации **«IFW»** возможна только на том экземпляре **ARMA MC**, с которого был экспортирован конфигурационный файл.

При загрузке конфигурационного файла на **«IFW»** через **ARMA MC** данные, которые потенциально могут повлиять на потерю управления источником, не изменяются. К таким данным относятся конфигурации пользователей и сетевых интерфейсов, администрирования обнаружения вторжений и экспорта событий, настройки SNMP и Nginx.

Невозможно внести изменения в следующие секции конфигурационного файла для последующей загрузки на **«IFW»**:

```
./system/user
./system/dnsallowoverride
./interfaces
./OPNsense/netsnmp
./OPNsense/Nginx
./OPNsense/IDS
./OPNsense/Syslog/destinations
```

Внесение изменений в перечисленные настройки выполняется вручную на конфигурируемом **«IFW»** после загрузки файла конфигурации. Ниже представлены разделы веб-интерфейса **ARMA FW**, в которых производятся настройки:

- **./system/user**: «Система» - «Доступ» - «Пользователи»;
- **./system/dnsallowoverride**: «Система» - «Настройки» - «Общие настройки» - «Позволить переопределить список DNS-серверов DHCP/PPP на WAN»;
- **./interfaces**: «Интерфейсы»;
- **./OPNsense/netsnmp**: «Система» - «Настройки» - «SNMP»;
- **./OPNsense/Nginx**: «Службы» - «Nginx»;
- **./OPNsense/IDS**: «Обнаружение вторжений» - «Администрирование»;
- **./OPNsense/Syslog/destinations**: «Система» - «Настройки» - «Экспорт событий».

5.4.5 Обновление правил СОВ источника «IFW»

Для обновления правил СОВ источника **«IFW»** необходимо выполнить следующие действия (см. Рисунок – Обновление конфигурации источника событий):

1. Выбрать необходимый **«IFW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Обновить»**.
3. В выпадающем списке выбрать значение **«Обновить правила СОВ IFW»**.

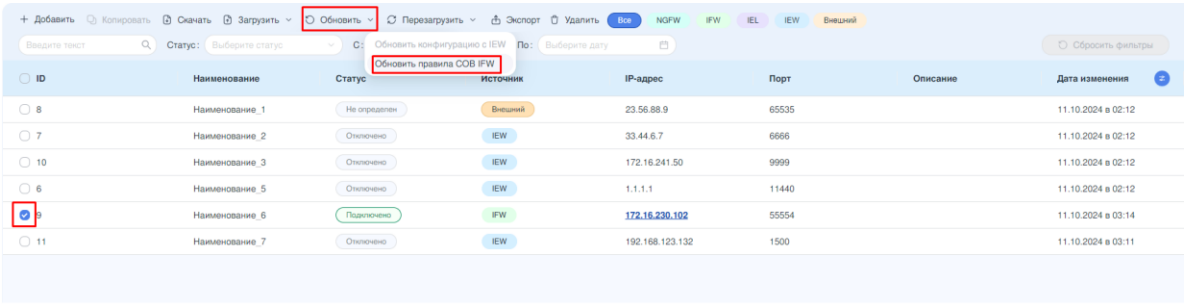


Рисунок – Обновление конфигурации источника событий

4. В проводнике выбрать необходимый файл и нажать кнопку **«Открыть»**. Форматы загружаемого файла: **«.tar.gz»**, **«.tgz»**, **«.rules»**.

При успешном обновлении правил СОВ появится соответствующее уведомление (см. Рисунок – Успешное обновление правил СОВ).

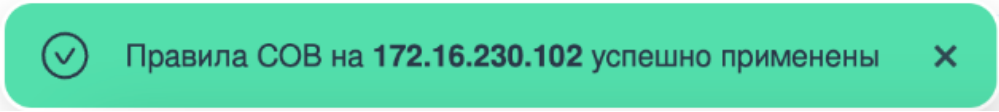


Рисунок – Успешное обновление правил СОВ

5.4.6 Перезагрузка источника «IFW»

Для перезагрузки одного или нескольких источников **«IFW»** необходимо выполнить следующие действия (см. Рисунок – Перезагрузка источника событий):

1. Выбрать необходимые источники **«IFW»**, установив флажок слева от значений столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Перезагрузить»**.
3. В выпадающем списке выбрать значение **«Перезагрузить IFW»**.

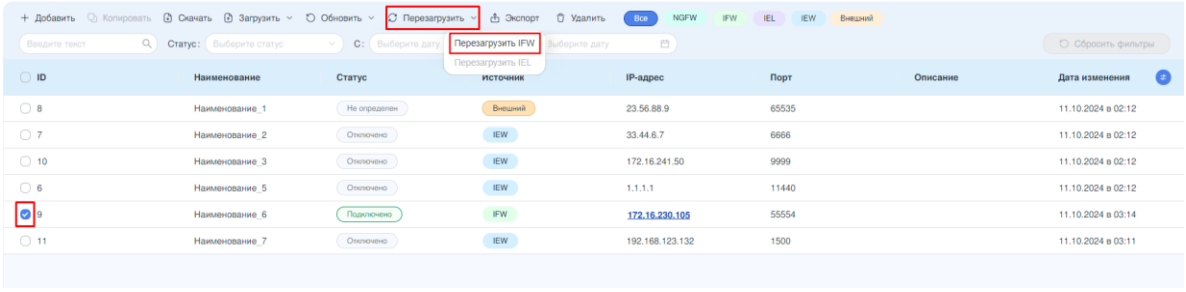


Рисунок – Перезагрузка источника событий

Появится уведомление, подтверждающее начало процесса перезагрузки.

5.4.7 Удаление источника «IFW»

Для удаления одного или нескольких источников **«IFW»** необходимо выполнить следующие действия (см. Рисунок – Удаление источника событий):

1. Выбрать необходимые источники **«IFW»**, установив флажок слева от значений столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Удалить»**.
3. Подтвердить удаление, нажав кнопку **«Удалить»** в открывшемся окне.

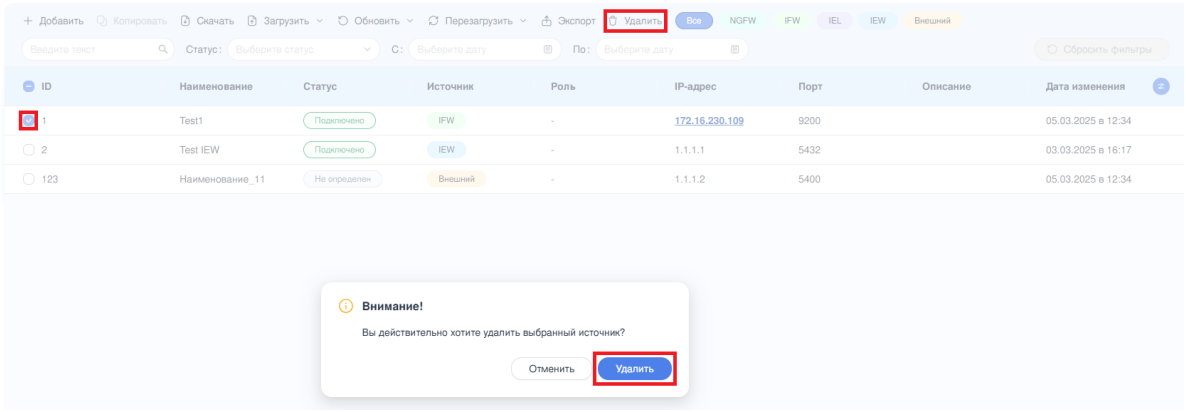


Рисунок – Удаление источника событий

После удаления источника появится соответствующее уведомление (см. Рисунок – Успешное удаление источника).

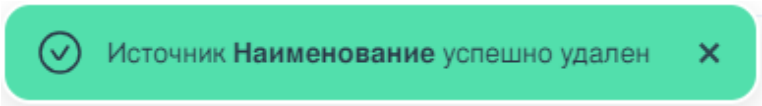


Рисунок – Успешное удаление источника

5.5 Источник «Industrial EndPoint Windows»

5.5.1 Добавление источника «IEW»

Для добавления источника необходимо выполнить следующие действия:

1. На панели инструментов нажать кнопку **«Добавить»**.
2. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«IEW»** и указать значения следующих параметров (см. Рисунок – Добавление нового источника событий):
   - **«Наименование»** – отображаемое в **ARMA MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
   - **«IP-адрес»** – IP-адрес или доменное имя подключаемого устройства. Не рекомендуется изменять IP-адрес добавляемого устройства после подключения к **ARMA MC** с целью исключения потери управления;

- **«Порт»** – значение порта входящих логов. Указываются порты UDP в диапазоне от 1500 до 65535. Значение должно быть уникальным, не заданным ранее.

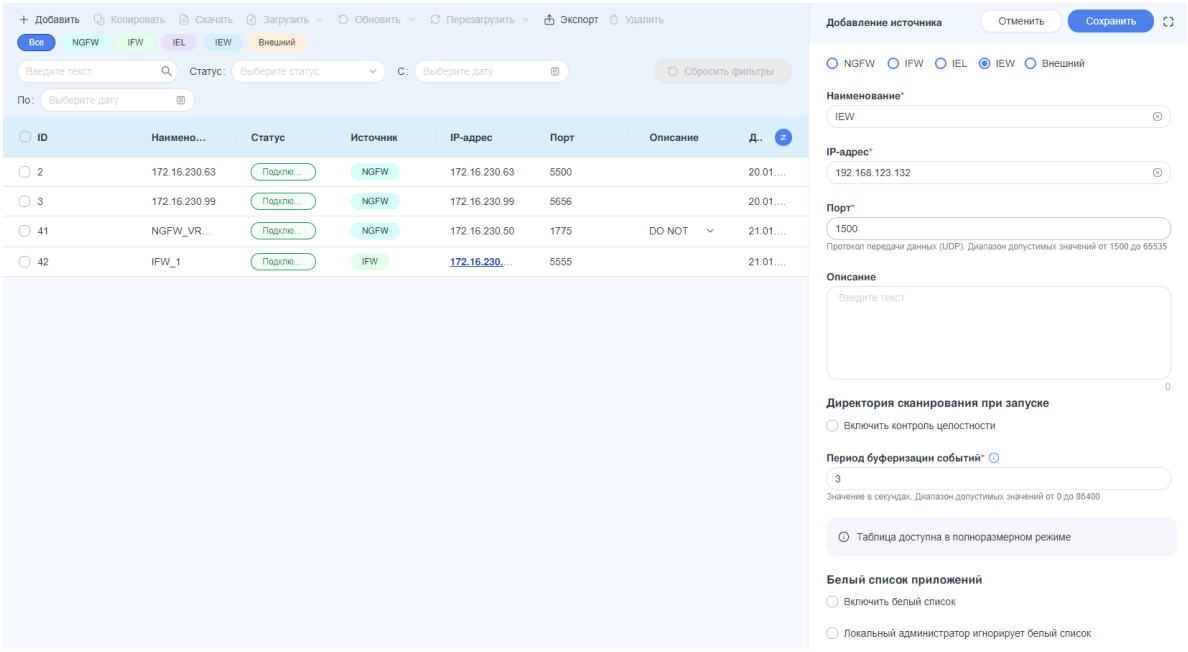


Рисунок – Добавление нового источника событий

3. При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.
4. При необходимости использования функции **«Контроль целостности»** в блоке **«Директория сканирования при запуске»** выполнить следующие действия:
   - включить функцию **«Контроль целостности»** установив флажок для параметра **«Включить контроль целостности»**;
   - в поле параметра **«Период буферизации событий»** указать частоту периодического сканирования добавленных файлов и директорий;
   - нажать кнопку **«Добавить»**;
   - в открывшемся поле указать полный путь к директории или файлу, подлежащему контролю целостности, и нажать кнопку **«Сохранить»**.
5. При необходимости использования функции **«Белый список приложений»** в блоке **«Белый список приложений»** выполнить следующие действия:
   - включить функцию **«Белый список приложений»**, установив флажок для параметра **«Включить белый список»**;
   - при необходимости установить флажок для параметра **«Локальный администратор игнорирует белый список»**;
   - нажать кнопку **«Добавить»**;

- в открывшемся поле указать полный путь к директории или файлу, подлежащему контролю целостности, и нажать кнопку **«Сохранить»**.

6. При необходимости использования функции **«Контроль устройств»** в блоке **«Настройки управления устройствами»** выполнить следующие действия:
   - включить функцию **«Контроль устройств»**, установив флажок для параметра **«Включить контроль устройств»**;
   - при необходимости запрета чтения и записи CD/DVD установить флажок для параметра **«Запретить доступ на чтение CD/DVD»**;
   - при необходимости установить флажок для параметра **«Включить контроль USB устройств»**.
7. В блоке **«Настройки ротации событий»** выбрать тип ротации журнала событий по **«Размеру»** или по **«Времени»**:
   - при выборе типа ротации **«Размер»** заполнить поле **«Размер таблицы»** значением в Кб, при котором будет происходить ротация;
   - при выборе типа ротации **«Время»** заполнить поле **«Период»**, в который следует запускать ротацию;
   - при выборе типа ротации **«Время»** заполнить поле **«Время»**, в которое будет запускаться ротация, в формате «чч:мм:сс».
8. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки для сохранения информации и добавления устройства.

После добавления источника **«IEW»** появится соответствующее уведомление (см. Рисунок – Успешное добавление источника).

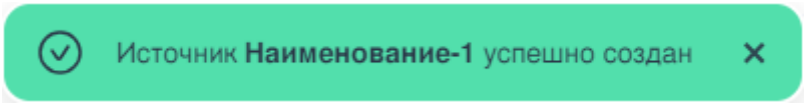


Рисунок – Успешное добавление источника

5.5.2 Настройка синхронизации с ARMA MC

После добавления источнику **«IEW»** будет автоматически присвоен порядковый номер в **ARMA MC**. Порядковый номер отображается в столбце **«ID»** и необходим для настройки синхронизации. Синхронизация **«IEW»** с **ARMA MC** описана в Руководстве пользователя **ARMA IE** (см. Настройка синхронизации с ARMA MC).

Настройки **«IEW»** при первой синхронизации не переносятся в **ARMA MC**. Для переноса настроек необходимо нажать кнопку **«Обновить»** в строке добавленного **«IEW»**.

5.5.3 Редактирование параметров источника «IEW»

Для редактирования параметров **«IEW»** необходимо выполнить следующие действия:

1. Выбрать подлежащий редактированию источник **«IEW»**, кликнув на соответствующую запись в таблице источников.
2. Указать требуемые значения параметров в открывшейся форме **«[Имя источника событий]»** и нажать кнопку **«Сохранить»**.

5.5.4 Копирование конфигурации источника «IEW»

Копирование конфигурации позволяет скопировать настройки добавленного источника событий, и на основе данных которого создаётся новый источник, без необходимости проводить однотипную настройку. Для копирования конфигурации **«IEW»** необходимо выполнить следующие действия (см. Рисунок – Копирование конфигурации источника событий):

1. Выбрать подлежащий копированию **«IEW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Копировать»**.
3. В открывшейся карточке **«Копирование источника»** заполнить обязательные поля:
   - **«Наименование»**;
   - **«IP»**;
   - **«Порт»**.
4. Нажать кнопку **«Сохранить»**.

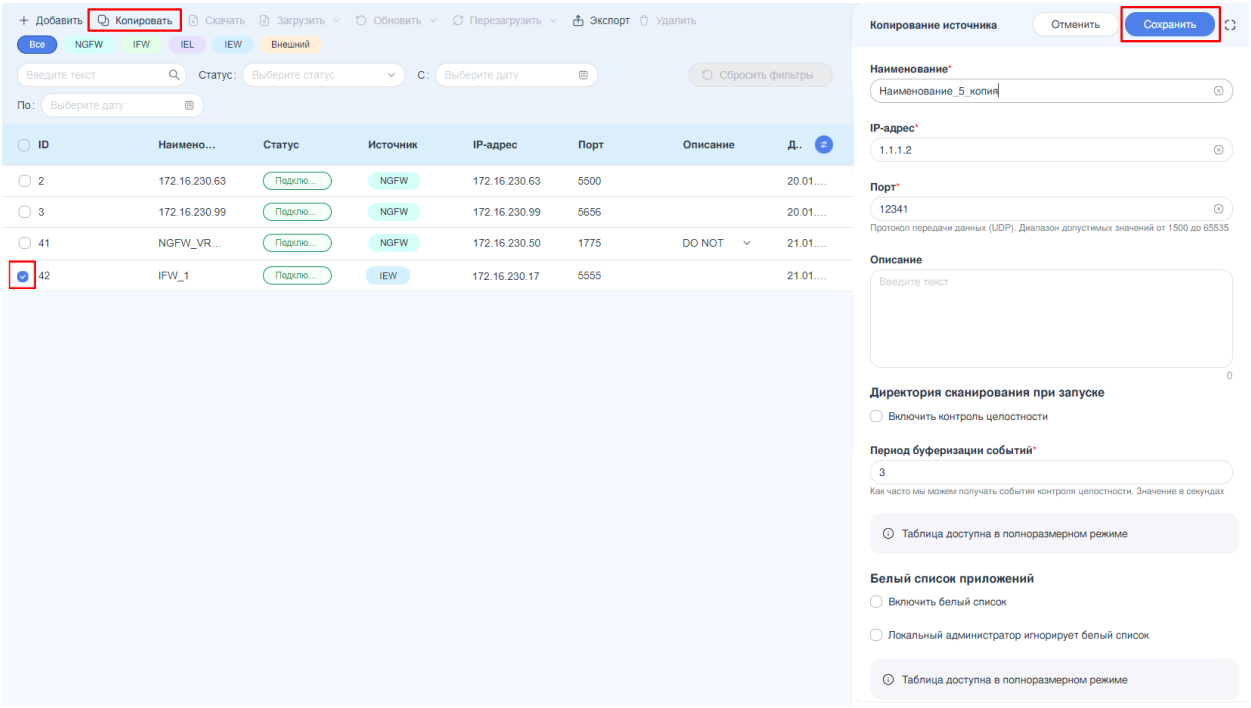


Рисунок – Копирование конфигурации источника событий

В результате копирования будет создан новый источник событий **«IEW»** с изменёнными обязательными полями из п. 3 (см. Рисунок – Успешное копирование конфигурации источника), остальные настройки будут скопированы.

Рисунок – Успешное копирование конфигурации источника

5.5.5 Скачивание конфигурации источника «IEW»

Для скачивания конфигурации одного или нескольких источников **«IEW»** необходимо выполнить следующие действия:

1. Выбрать один или несколько необходимых источников **«IEW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Скачать»**.

Формат скачиваемого файла – **«json»**. При успешном скачивании файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешное скачивание конфигурации).

Рисунок – Успешное скачивание конфигурации

5.5.6 Загрузка конфигурации источника «IEW»

Для загрузки конфигурации **«IEW»** необходимо выполнить следующие действия (см. Рисунок – Загрузка конфигурации на источник событий):

1. Выбрать необходимый **«IEW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Загрузить»**.
3. В выпадающем списке выбрать значение **«Загрузить конфигурацию IEW»**.
4. В проводнике выбрать конфигурационный файл и нажать кнопку **«Открыть»**.

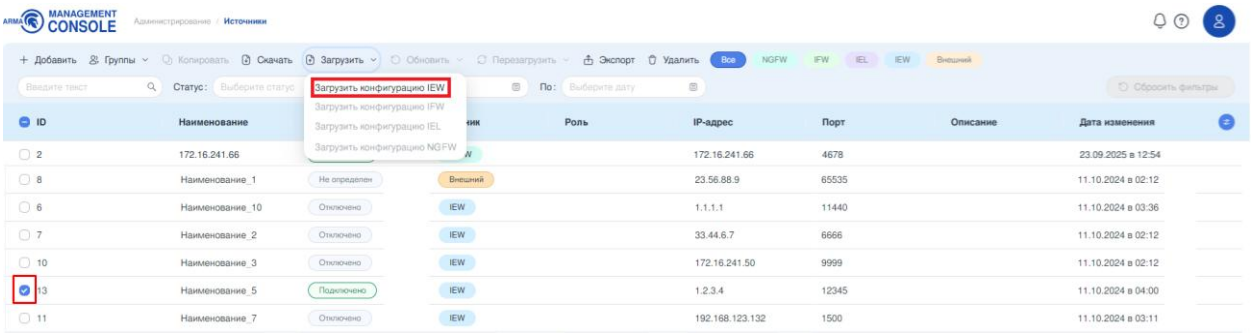


Рисунок – Загрузка конфигурации на источник событий

При успешной загрузке файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешная загрузка конфигурации).

Рисунок – Успешная загрузка конфигурации

5.5.7 Обновление конфигурации источника «IEW»

Для обновления конфигурации **«IEW»** необходимо выполнить следующие действия (см. Рисунок – Обновление конфигурации источника событий):

1. Выбрать необходимый **«IEW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Обновить»**.
3. В выпадающем списке выбрать значение **«Обновить конфигурацию с IEW»**.

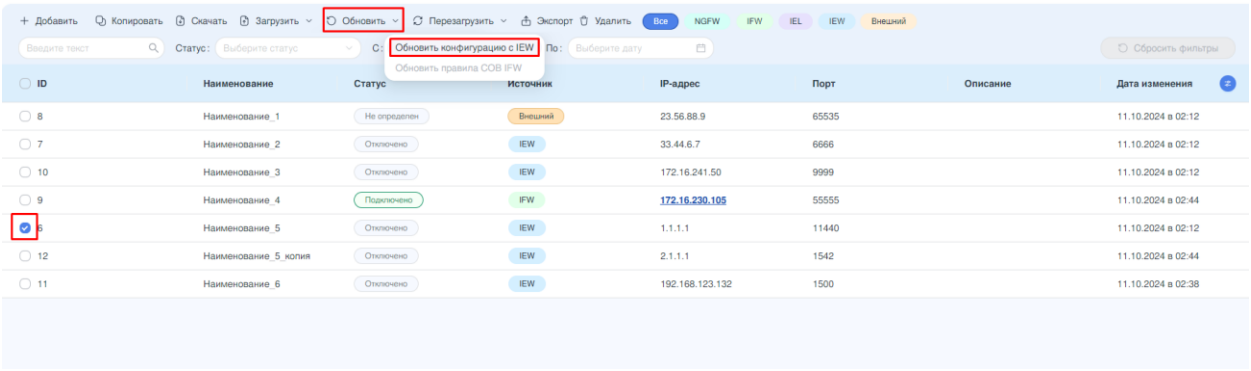


Рисунок – Обновление конфигурации источника событий

При успешном обновлении конфигурации появится соответствующее уведомление (см. Рисунок – Успешное обновление конфигурации).

Рисунок – Успешное обновление конфигурации

5.5.8 Удаление источника «IEW»

Для удаления одного или нескольких источников **«IEW»** необходимо выполнить следующие действия (см. Рисунок – Удаление источника событий):

1. Выбрать необходимые источники **«IEW»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Удалить»**.
3. Подтвердить удаление, нажав на кнопку **«Удалить»** в открывшемся окне.

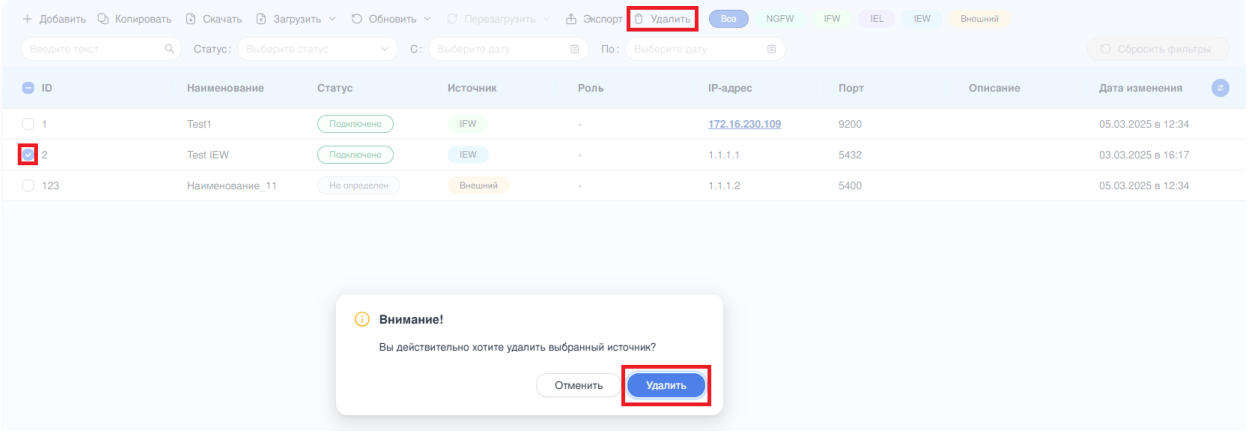


Рисунок – Удаление источника событий

При удалении источника появится соответствующее уведомление (см. Рисунок – Успешное удаление источника).

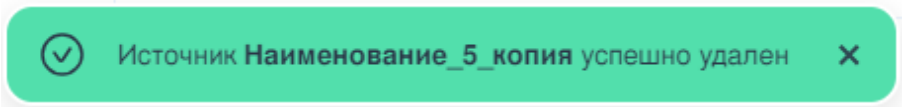


Рисунок – Успешное удаление источника

5.6 Источник «Industrial EndPoint Linux»

5.6.1 Добавление источника «IEL»

Для добавления источника **«IEL»** необходимо выполнить следующие действия:

1. На панели инструментов нажать кнопку **«Добавить»**.
2. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«IEL»** и указать значения следующих параметров (см. Рисунок – Добавление нового источника событий «IEL»):
   - **«Наименование»** – отображаемое в **ARMA MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
   - **«IP-адрес»** – IP-адрес или доменное имя подключаемого устройства. Не рекомендуется изменять IP-адрес добавляемого устройства после подключения к **ARMA MC** с целью исключения потери управления;
   - **«Порт»** – значение порта входящих логов. Указываются порты UDP в диапазоне от 1500 до 65535. Значение должно быть уникальным, не заданным ранее.

   Примечание:

   Не рекомендуется без крайней необходимости использовать для взаимодействия с **ARMA IEL** порт, отличный от «**5501**».

   Если изменить порт всё-таки необходимо, он должен быть разблокирован в nftables «**ENDPOINT_LINUX_GRPC_PORT**». Переменную нужно менять не глобально, а через изменение файла в месте установки консоли (/usr/local/armaconsole/app/amc-api/envs) - «**.devices.production.env**».

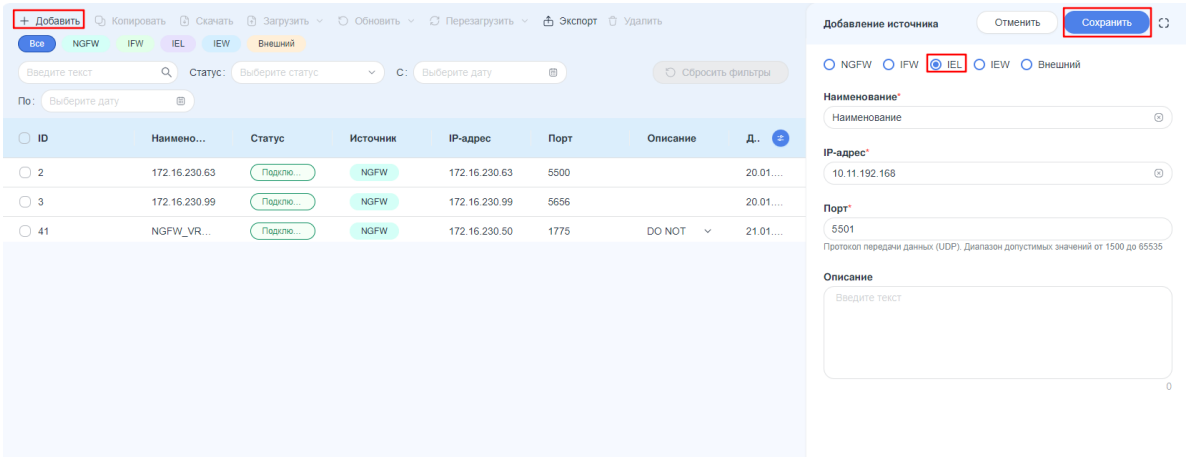


Рисунок – Добавление нового источника событий «IEL»

3. При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.
4. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки для сохранения информации и добавления устройства.

После добавления источника **«IEL»** появятся соответствующие уведомления (см. Рисунок – Скопируйте ключ) (см. Рисунок – Успешное добавление источника).

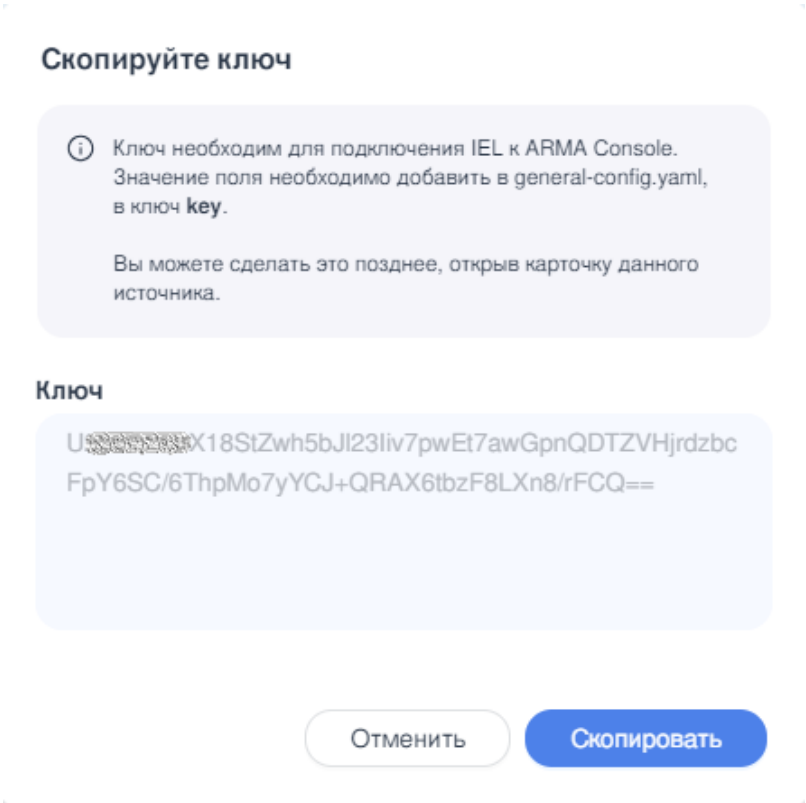


Рисунок – Скопируйте ключ

Предоставленный ключ необходим для настройки синхронизации с **«ARMA MC»**.

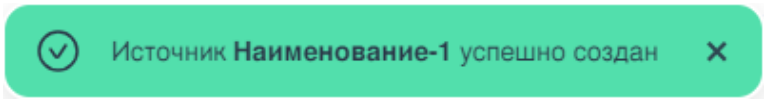


Рисунок – Успешное добавление источника

5.6.2 Настройка синхронизации с ARMA MC

Порядок настройки синхронизации **«IEL»** с **ARMA MC** описан в Руководстве администратора **ARMA IEL** (см. Синхронизация с Центром Управления).

5.6.3 Редактирование параметров источника «IEL»

Для редактирования параметров источника **«IEL»** необходимо выполнить следующие действия:

1. Выбрать подлежащий редактированию источник **«IEL»**, кликнув на соответствующую запись в таблице источников.
2. Указать требуемые значения параметров в открывшейся форме **«[Имя источника событий]»** и нажать кнопку **«Сохранить»**.

После успешного редактирования источника появится соответствующее уведомление (см. Рисунок – Успешное редактирование источника).

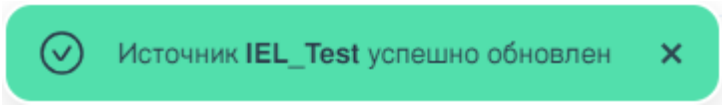


Рисунок – Успешное редактирование источника

Примечание:

При корректировке параметров источника **«IEL»** ключ, необходимый для подключения **IEL** к **ARMA MC**, остаётся неизменным и заблокирован для редактирования. Повторно прописывать ключ в файл **general-config.yaml** не требуется.

5.6.4 Скачивание конфигурации источника «IEL»

Для скачивания конфигурации одного или нескольких источников **«IEL»** необходимо выполнить следующие действия:

1. Выбрать один или несколько необходимых источников **«IEL»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Скачать»** (см. Рисунок – Скачивание конфигурации).

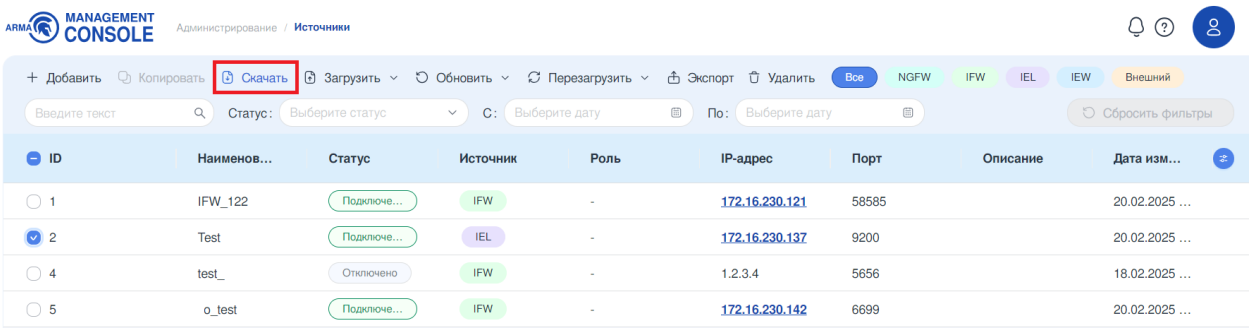


Рисунок – Скачивание конфигурации

Формат скачиваемого файла – **«yaml»**. При успешном скачивании файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешное скачивание конфигурации).

Рисунок – Успешное скачивание конфигурации

При потере интернет-соединения во время скачивания файла конфигурации появится соответствующее уведомление (см. Рисунок – Неуспешное скачивание конфигурации).

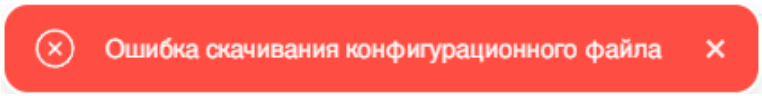


Рисунок – Неуспешное скачивание конфигурации

Данные конфигурационного файла полностью соответствуют конфигурации, настроенной на конкретном **«IEL»**.

5.6.5 Загрузка конфигурации источника «IEL»

Примечание:

Важно! Не следует загружать конфигурацию на неактивированный источник **«IEL»**. Сначала необходимо активировать лицензию на источнике **«IEL»** и только после этого загружать конфигурацию на него.

Для загрузки конфигурации **«IEL»** необходимо выполнить следующие действия:

1. Выбрать необходимый **«IEL»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Загрузить»**.
3. В выпадающем списке выбрать значение **«Загрузить конфигурацию IEL»**.
4. В проводнике выбрать конфигурационный файл и нажать кнопку **«Открыть»** (см. Рисунок – Загрузка конфигурации на источник событий «IEL»).

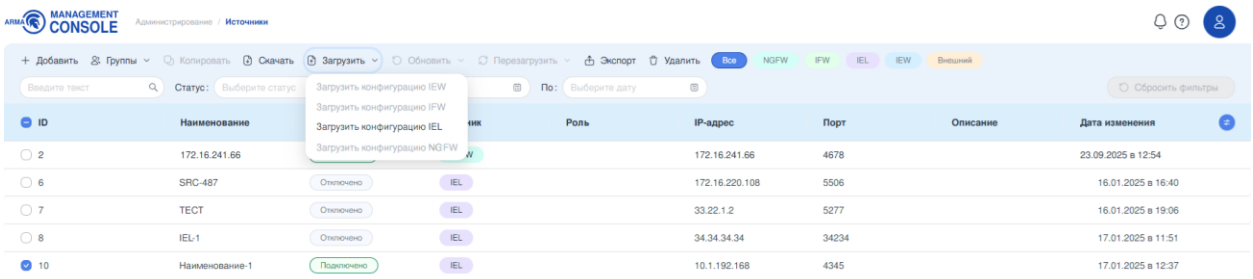


Рисунок – Загрузка конфигурации на источник событий «IEL»

При успешной загрузке файла конфигурации появится соответствующее уведомление (см. Рисунок – Успешная загрузка конфигурации).

Рисунок – Успешная загрузка конфигурации

При возникновении проблем с загрузкой файла конфигурации появится уведомление (см. Рисунок – Загрузка некорректного файла конфигурации).

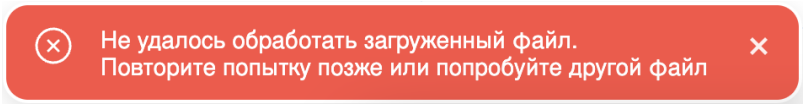


Рисунок – Загрузка некорректного файла конфигурации

Примечание:

Существует ограничение на размер загружаемого конфигурационного файла. При попытке загрузить файл, размер которого превышает 10 Мб, выводится сообщение **«Файл конфигурации не может превышать 10 Мб»**.

5.6.6 Перезагрузка источника «IEL»

Для перезагрузки одного или нескольких источников **«IEL»** необходимо выполнить следующие действия:

1. Выбрать необходимые источники **«IEL»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Перезагрузить»**.
3. В выпадающем списке выбрать значение **«Перезагрузить IEL»** (см. Рисунок – Перезагрузка источника событий «IEL»).

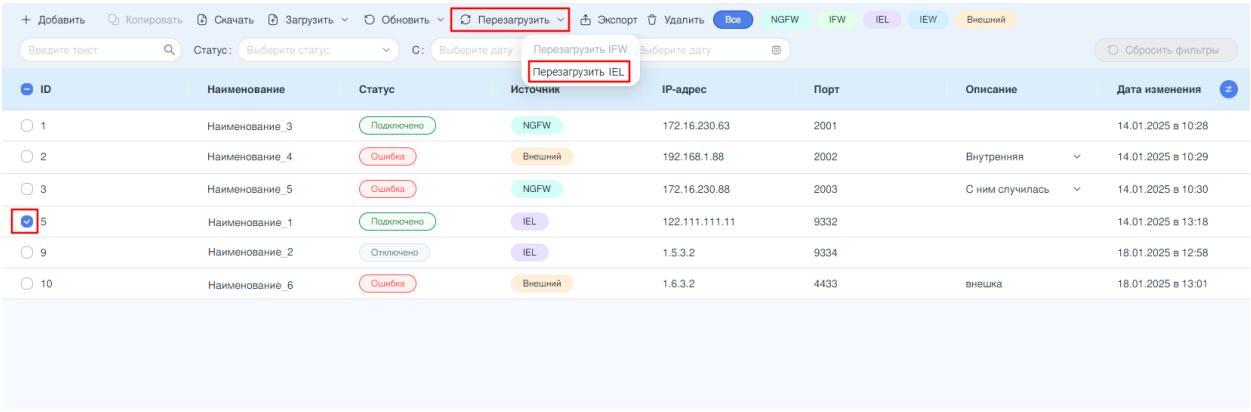


Рисунок – Перезагрузка источника событий «IEL»

После перезагрузки источника появится соответствующее уведомление (см. Рисунок – Успешная перезагрузка источника).

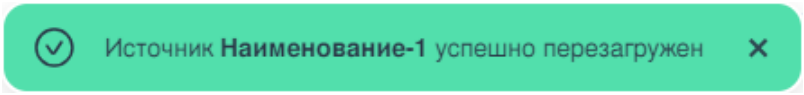


Рисунок – Успешная перезагрузка источника

5.6.7 Удаление источника «IEL»

Для удаления одного или нескольких источников **«IEL»** необходимо выполнить следующие действия:

1. Выбрать необходимые источники **«IEL»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Удалить»**.
3. Подтвердить удаление, нажав на кнопку **«Удалить»** в открывшемся окне (см. Рисунок – Удаление источника событий «IEL»).

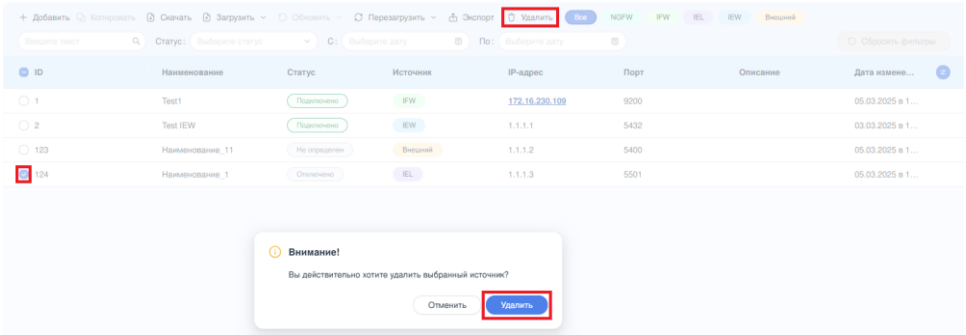


Рисунок – Удаление источника событий «IEL»

При удалении источника появится соответствующее уведомление (см. Рисунок – Успешное удаление источника).

Рисунок – Успешное удаление источника

5.7 Источник «Внешнее устройство»

5.7.1 Добавление источника «Внешнее устройство»

Для подключения источника **«Внешнее устройство»** к **ARMA MC** необходимо выполнить следующие шаги:

1. На панели инструментов нажать кнопку **«Добавить»**.
2. В открывшейся карточке **«Добавление источника»** выбрать тип источника **«Внешнее устройство»** и указать значения следующих параметров (см. Рисунок – Добавление нового источника событий):
   - **«Наименование»** – отображаемое в **ARMA MC** имя устройства. Параметр может содержать только латинские и кириллические буквы, пробел, спецсимволы («.», «_», «-») и не может превышать 128 символов;
   - **«IP»** – IP-адрес подключаемого устройства. Не рекомендуется изменять IP-адрес добавляемого устройства после подключения к **ARMA MC** с целью исключения потери управления;
   - **«Порт»** – значение порта входящих логов. Указываются порты UDP в диапазоне от 1500 до 65535. Значение должно быть уникальным, не заданным ранее.

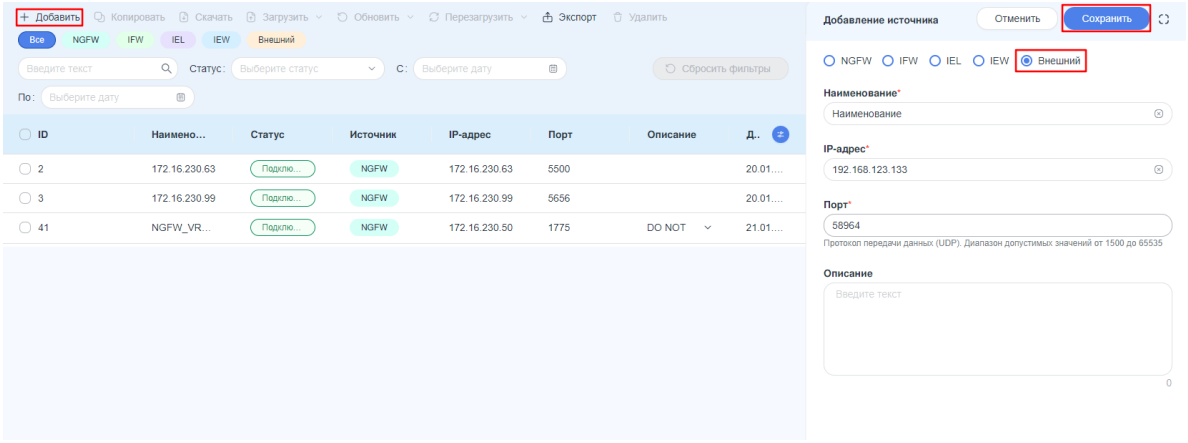


Рисунок – Добавление нового источника событий

3. При необходимости заполнить поле **«Описание»** дополнительной информацией об устройстве. Поле может содержать не более 250 символов.
4. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки для сохранения информации и добавления устройства.

После успешного добавления источника появится соответствующее уведомление (см. Рисунок – Успешное добавление источника).

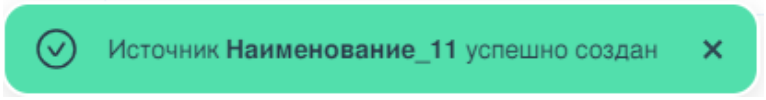


Рисунок – Успешное добавление источника

5.7.2 Редактирование параметров источника «Внешнее устройство»

Для редактирования параметров источника **«Внешнее устройство»** необходимо выполнить следующие действия:

1. Выбрать подлежащий редактированию источник **«Внешнее устройство»**, кликнув на соответствующую запись в таблице источников.
2. Указать требуемые значения параметров в открывшейся форме **«[Имя источника событий]»** и нажать кнопку **«Сохранить»** для сохранения информации.

После успешного редактирования источника появится соответствующее уведомление (см. Рисунок – Успешное редактирование источника).

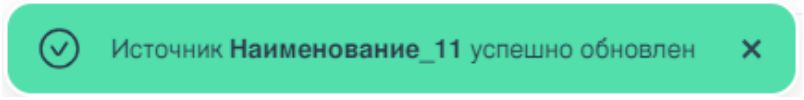


Рисунок – Успешное редактирование источника

5.7.3 Удаление источника «Внешнее устройство»

Для удаления одного или нескольких источников **«Внешнее устройство»** необходимо выполнить следующие действия:

1. Выбрать необходимые источники **«Внешнее устройство»**, установив флажок слева от значения столбца **«ID»**.
2. На панели инструментов нажать кнопку **«Удалить»**.
3. Подтвердить удаление, нажав на кнопку **«Удалить»** в открывшемся окне (см. Рисунок – Удаление источника событий «Внешнее устройство»).

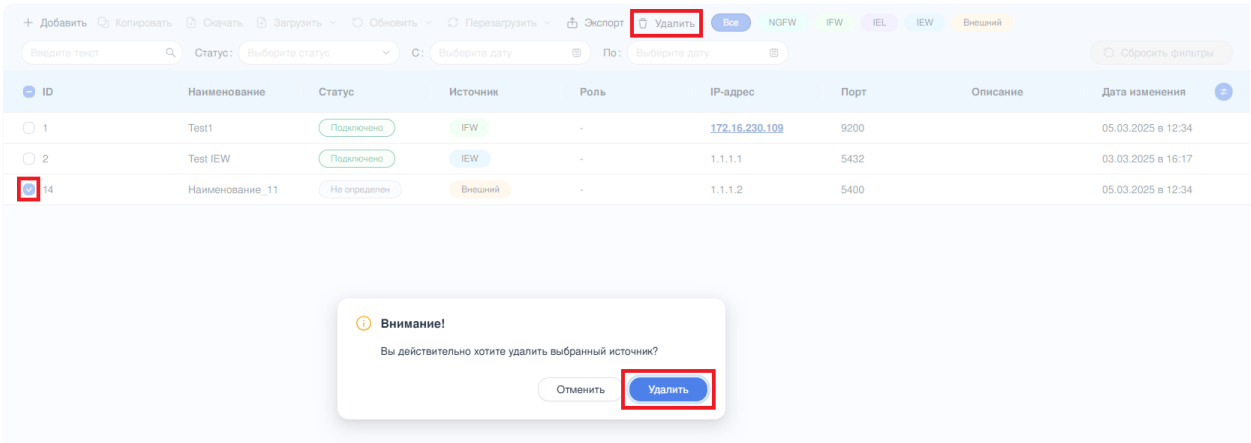


Рисунок – Удаление источника событий

После удаления источника появится соответствующее уведомление (см. Рисунок – Успешное удаление источника).

Рисунок – Успешное удаление источника

5.8 Экспорт таблицы источники

Существует возможность локально сохранить таблицу источников. Для этого необходимо перейти в раздел **«Источники»** меню **«Администрирование»** и нажать кнопку **«Экспорт»** на панели инструментов (см. Рисунок – Экспорт информации об источниках). Формат экспортируемого файла – **«csv»**.

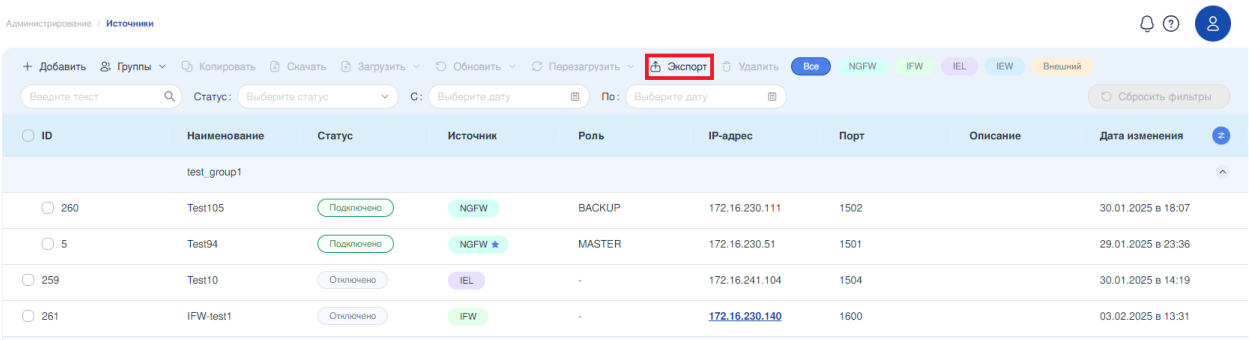


Рисунок – Экспорт информации об источниках

После успешного экспорта информации об источниках появится соответствующее уведомление (см. Рисунок – Успешный экспорт информации об источниках).

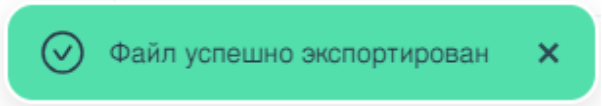


Рисунок – Успешный экспорт информации об источниках

Ниже представлен пример того, как может выглядеть экспортированный файл таблицы источников событий в соответствии с параметрами, указанными на рисунке «Экспорт информации об источниках»:

```
id,type,name,description,ip,port,group,updated
5,ngfw,Test94,,172.16.230.51,1501,,Wed, 29 Jan 2025 20:36:27 GMT
259,endpoint-linux,Test10,,172.16.241.104,1504,,Thu, 30 Jan 2025 11:19:43 GMT
260,ngfw,Test105,,172.16.230.111,1502,,Thu, 30 Jan 2025 15:07:28 GMT
261,firewall,IFW-test1,,172.16.230.140,1600,,Mon, 03 Feb 2025 10:31:40 GMT
```

В первой строке файла перечислены названия заголовков таблицы источников, разделённые запятыми (см. Таблица «Соответствие заголовкам таблицы источников»). Информация о статусе источников, а также сведения о кластере и роли источников **«NGFW»** не экспортируются.

Таблица «Соответствие заголовкам таблицы источников»

Значение	Заголовок таблицы источников	Описание
id	ID	Идентификационный номер источника
type	Источник	Тип подключённого источника
name	Наименование	Имя источника указанное пользователем.
description	Описание	Краткое описание источника
ip	IP-адрес	IP-адрес источника
port	Порт	Порт для приёма входящих логов от источника
group		В данной таблице не используется
updated	Дата изменения	Дата последнего внесения изменений

6 ПРАВИЛА КОРРЕЛЯЦИИ

В настоящем разделе представлено описание подраздела меню **«Правила корреляции»**, предусматривающего механизм управления правилами корреляции.

В **ARMA MC** предусмотрен механизм сбора и агрегации логов – **коррелятор**. Корреляция событий осуществляется на базе правил, обеспечивающей автоматизированный анализ поступающих событий и выдачу реакции на определённое событие.

Для перехода в подраздел на панели навигации необходимо выбрать раздел меню **«Администрирование»**, затем подраздел **«Правила корреляции»** (см. Рисунок – Правила корреляции).

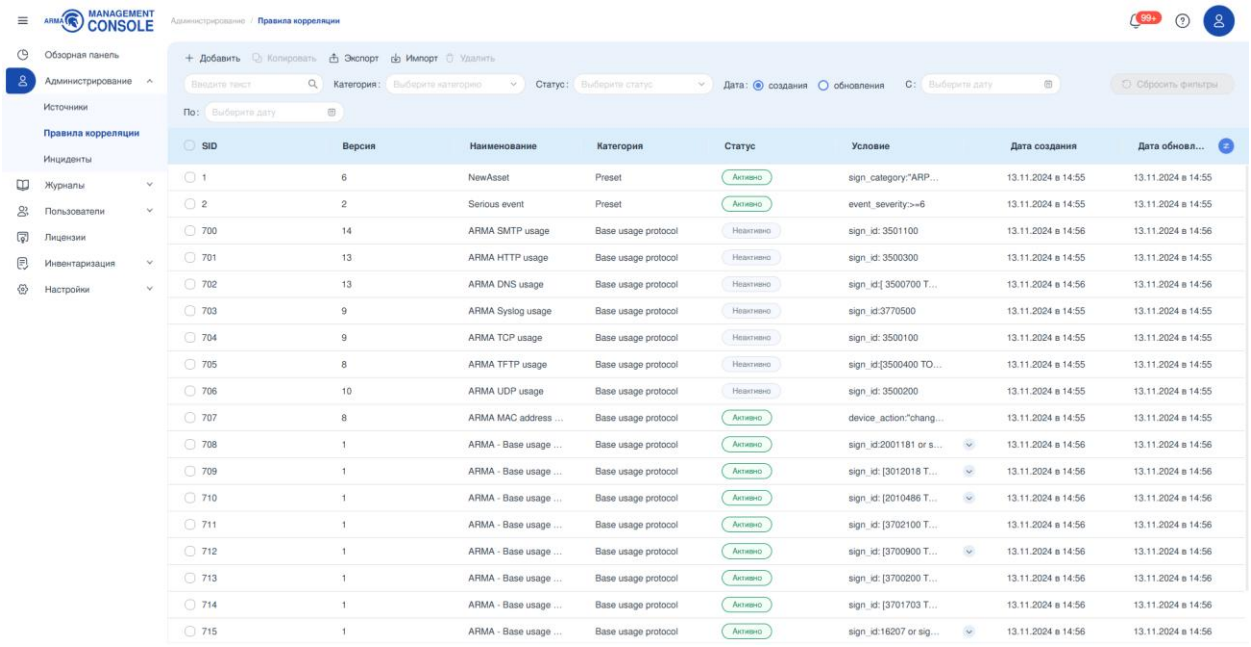


Рисунок – Правила корреляции

Информация о правилах корреляции представлена в формате таблицы, состоящей из следующих столбцов:

- **«SID»** – идентификатор безопасности. Генерируется системой автоматически;
- **«Версия»** – версия правила. Порядковый номер версии увеличивается при обновлении правила корреляции. Генерируется системой автоматически;
- **«Наименование»** – наименование правила корреляции;
- **«Категория»** – отображает категорию угрозы ИБ, в которую входит правило корреляции;
- **«Статус»** – состояние правила корреляции («Активно»/«Неактивно»);
- **«Условие»** – условие срабатывания правила корреляции;

- **«Дата создания»** – дата создания правила корреляции;
- **«Дата обновления»** – дата редактирования правила корреляции. При обновлении правила корреляции является датой создания следующей версии правила.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

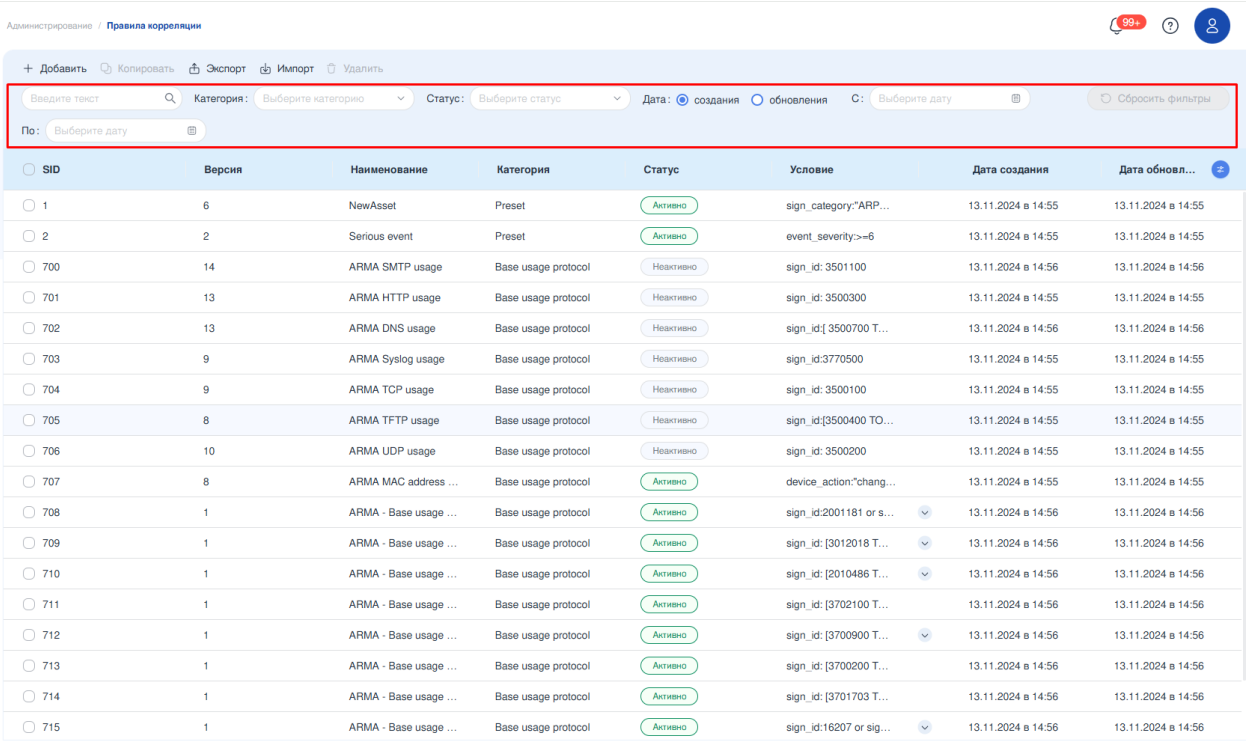
Доступно две категории правил корреляции:

- **Предустановленные правила** (SID от 1 до 500 000) – правила, созданные разработчиком и загруженные в систему. Правила данной категории невозможно редактировать, пользователю доступен только просмотр настроек правила. Подобное правило возможно скопировать для дальнейшего использования в качестве основы для создания пользовательского правила.
- **Пользовательские правила** (SID от 500 000 до 1 000 000) – правила, которые создаёт пользователь. Правила данной категории возможно редактировать через карточку правил корреляции.

6.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать правила корреляции по всем столбцам списка и по умолчанию состоит из следующих полей (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **«Категория»**;
- **«Статус»**;
- **«Дата»**;
- **«С»**;
- **«По»**;
- **кнопка «Сбросить фильтры»**.



SID	Версия	Наименование	Категория	Статус	Условие	Дата создания	Дата обновл...
1	6	NewAsset	Preset	Активно	sign_category:"ARP...	13.11.2024 в 14:55	13.11.2024 в 14:55
2	2	Serious event	Preset	Активно	event_severity:>=6	13.11.2024 в 14:55	13.11.2024 в 14:55
700	14	ARMA SMTP usage	Base usage protocol	Неактивно	sign_id: 3501100	13.11.2024 в 14:56	13.11.2024 в 14:56
701	13	ARMA HTTP usage	Base usage protocol	Неактивно	sign_id: 3500300	13.11.2024 в 14:55	13.11.2024 в 14:55
702	13	ARMA DNS usage	Base usage protocol	Неактивно	sign_id:[3500700 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
703	9	ARMA Syslog usage	Base usage protocol	Неактивно	sign_id:3770500	13.11.2024 в 14:55	13.11.2024 в 14:55
704	9	ARMA TCP usage	Base usage protocol	Неактивно	sign_id: 3500100	13.11.2024 в 14:55	13.11.2024 в 14:55
705	8	ARMA TFTP usage	Base usage protocol	Неактивно	sign_id:[3500400 TO...	13.11.2024 в 14:55	13.11.2024 в 14:55
706	10	ARMA UDP usage	Base usage protocol	Неактивно	sign_id: 3500200	13.11.2024 в 14:55	13.11.2024 в 14:55
707	8	ARMA MAC address ...	Base usage protocol	Активно	device_action:"chang...	13.11.2024 в 14:55	13.11.2024 в 14:55
708	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id:2001181 or s...	13.11.2024 в 14:56	13.11.2024 в 14:56
709	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id: [3012018 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
710	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id: [2010486 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
711	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id: [3702100 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
712	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id: [3700900 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
713	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id: [3700200 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
714	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id: [3701703 T...	13.11.2024 в 14:56	13.11.2024 в 14:56
715	1	ARMA - Base usage ...	Base usage protocol	Активно	sign_id:16207 or sig...	13.11.2024 в 14:56	13.11.2024 в 14:56

Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем столбцам.

Фильтрация по полю **«Категория»** позволяет отфильтровать данные по категории угрозы ИБ, в которую входит правило корреляции. Поле **«Категория»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Attack»** – эксплуатация уязвимостей, действие по проникновению или нарушению безопасности информационной системы;
- **«Base usage protocol»** – обнаружение использования прикладного L7 протокола;
- **«Usage for connect»** – обнаружение установленной сессии управления в прикладном протоколе;
- **«SCAN»** – сканирование портов и служб с целью перечисления и определения уязвимых к эксплойтам сервисов;
- **«Modbus»** – обнаружение использования промышленного протокола Modbus;
- **«S7Comm»** – обнаружение использования промышленного протокола S7Comm;
- **«OPCUA»** – обнаружение использования промышленного протокола OPCUA;

- **«OPCDA»** – обнаружение использования промышленного протокола OPCDA;
- **«IEC104»** – обнаружение использования промышленного протокола IEC104;
- **«Preset»** – служебная категория, используемая в процессе корреляции;
- **«BACnet»** – обнаружение использования промышленного протокола BACnet;
- **«OMRON»** – обнаружение использования промышленного протокола OMRON;
- **«KRUG»** – обнаружение использования промышленного протокола KRUG.

Фильтрация по полю **«Статус»** позволяет отфильтровать данные по статусу правила корреляции. Поле **«Статус»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Активно»**;
- **«Неактивно»**.

Фильтр **«Дата»** представляет собой переключатель и предоставляет выбор из следующих вариантов значений:

- **«создания»** – для фильтрации данных по дате создания правила корреляции;
- **«обновления»** – для фильтрации данных по дате обновления правила корреляции.

Фильтрация по полю **«С»** позволяет отфильтровать данные по дате создания/обновления правила корреляции и задаёт начальную дату диапазона. После ввода даты в таблице отобразятся лишь те действия, где **«Дата»** совпадает или больше введённой в фильтр.

Фильтрация по полю **«По»** позволяет отфильтровать данные по дате создания/обновления правила корреляции и задаёт конечную дату диапазона. После ввода даты в таблице отобразятся лишь те действия, где **«Дата»** совпадает или меньше введённой в фильтр.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

6.2 Карточка правила корреляции

Карточка правила корреляции содержит подробную информацию о правиле. Для того чтобы открыть карточку, необходимо нажать на необходимое правило (см.

Рисунок – Карточка правила корреляции). В предустановленных правилах пользователю доступен только просмотр настроек правила.

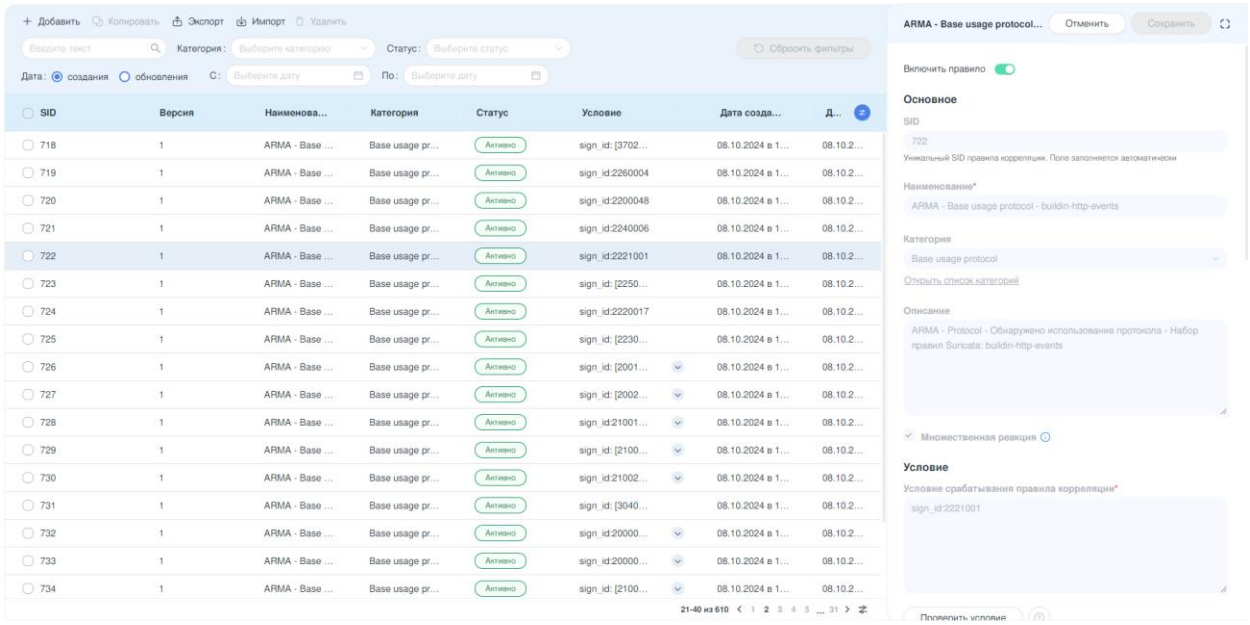


Рисунок – Карточка правила корреляции

Карточка правила содержит следующие блоки:

- **переключатель статуса правила («Активно»/«Неактивно»)**;
- **«Основное»**;
- **«Условие»**;
- **«Действия»**.

Блок **«Основное»** содержит следующую информацию о правиле (см. Рисунок – Карточка. Блок «Основное»):

- **«SID»**;
- **«Наименование»**;
- **«Категория»**;
- **«Описание»**;
- **чек-бокс «Множественная реакция»**.

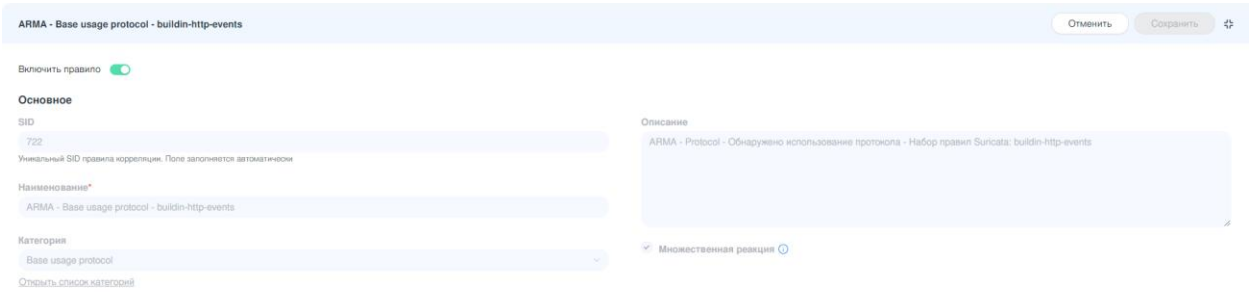


Рисунок – Карточка. Блок «Основное»

Блок **«Условие»** содержит **«Условие срабатывания правила корреляции»** (см. Рисунок – Карточка. Блок «Условие»).

Рисунок – Карточка. Блок «Условие»

Примечание:

С версии **ARMA MC «1.8»** коррелятор обрабатывает поле **«sign_id»** исключительно как числовое значение. Если ранее созданные правила корреляции опирались на использование **«sign_id: строка»**, рекомендуется заменить их на правила корреляции, соответствующие новым требованиям.
Например, правило корреляции, использующее проверку **«sign_id:webauth»**, больше не будет обрабатывать события корректно. Такое правило следует заменить на **«sign_name:'Web authentication'»**.
Аналогично, **«sign_id:idspower»** заменяется на **«sign_name:'IDS power'»**; **«sign_id:idsalert»** заменяется на **«sign_name:'IDS rule alert'»**; **«sign_id:arpwatchalert»** заменяется на **«sign_name:'Arpwatch alert'»** и так далее.

Рекомендуется учитывать эти изменения в синтаксисе правил корреляции для обеспечения корректной обработки приходящих событий.

Блок **«Действие»** содержит список действий при срабатывании конкретного правила корреляции, а также подробные настройки каждого типа действия (см. Рисунок – Карточка. Блок «Действие»).

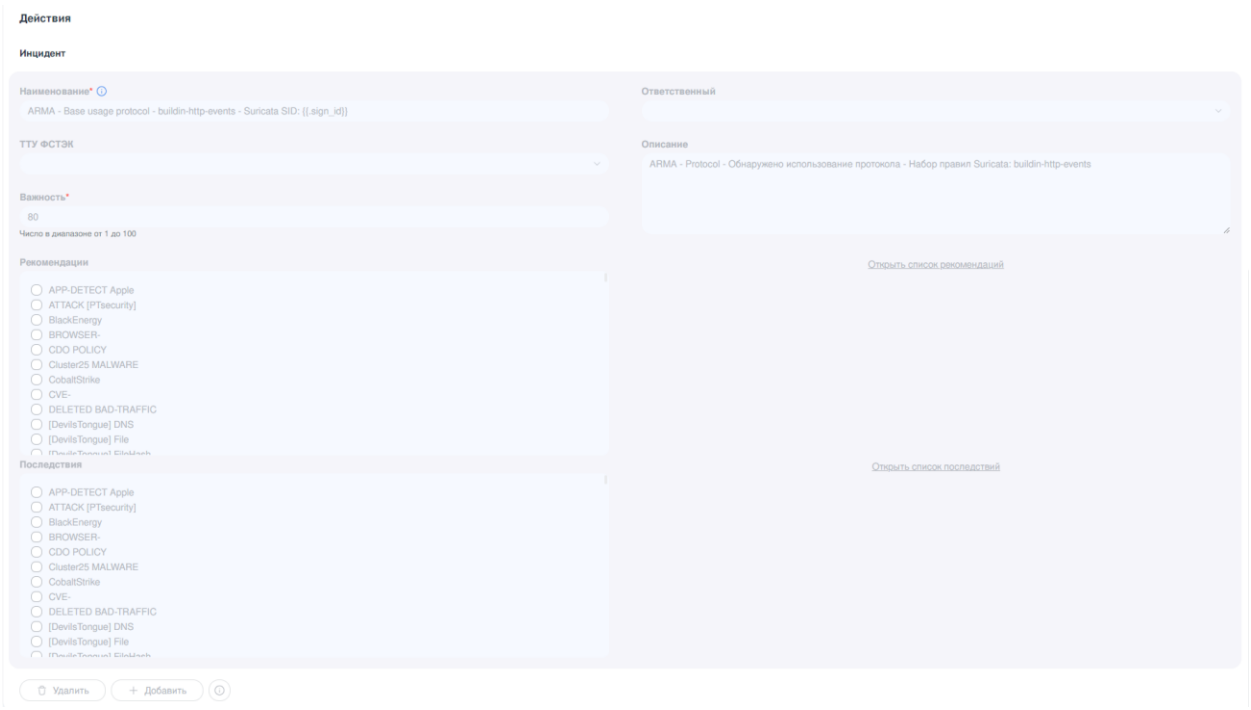


Рисунок – Карточка. Блок «Действие»

6.3 Добавление правила корреляции

Существует два способа добавления пользовательского правила корреляции:

- копирование предустановленного правила с внесением необходимых изменений;
- создание нового правила.

6.3.1 Копирование правила корреляции

Для копирования правила корреляции необходимо выполнить следующие действия:

1. Выбрать правило корреляции, установив флажок рядом с его SID.
2. На панели инструментов нажать кнопку **«Копировать»**.
3. В открывшейся карточке правила внести необходимые изменения и нажать кнопку **«Сохранить»** в правом верхнем углу карточки (см. Рисунок – Копирование правила корреляции).

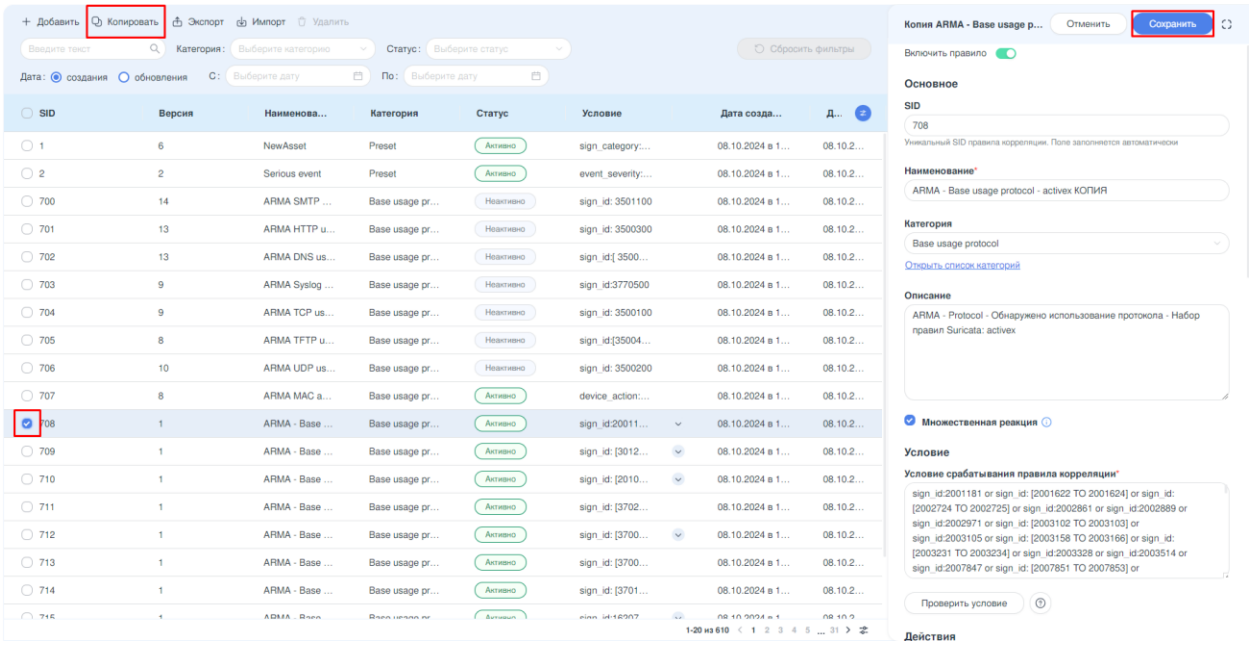


Рисунок – Копирование правила корреляции

При успешном копировании правила корреляции появится соответствующее уведомление (см. Рисунок – Успешное копирование правила).

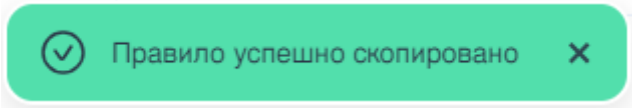


Рисунок – Успешное копирование правила

6.3.2 Создание правила корреляции

Для создания правила корреляции необходимо выполнить следующие действия:

1. На панели инструментов нажать кнопку **«Добавить»**.
2. В открывшейся карточке **«Добавление правила»** указать значения необходимых параметров в блоке **«Основное»**:
   - поле **«SID»** автоматически заполнится уникальным идентификатором правила в диапазоне от 500 000 до 1 000 000;
   - в поле **«Наименование»** ввести уникальное наименование правила. Поле может содержать кириллические и латинские буквы, цифры, спецсимволы и ограничено 128 символами;
   - в выпадающем списке поля **«Категория»** выбрать одну из предустановленных категорий;
   - в случае, если ни одна из предустановленных категорий не подходит, существует возможность добавить пользовательскую категорию. Для этого необходимо открыть список категорий, нажать кнопку **«Добавить»**, в

открывшемся окне ввести **«Наименование»** и **«Описание категории»**, затем нажать кнопку **«Сохранить»** (см. Рисунок – Добавление категории);

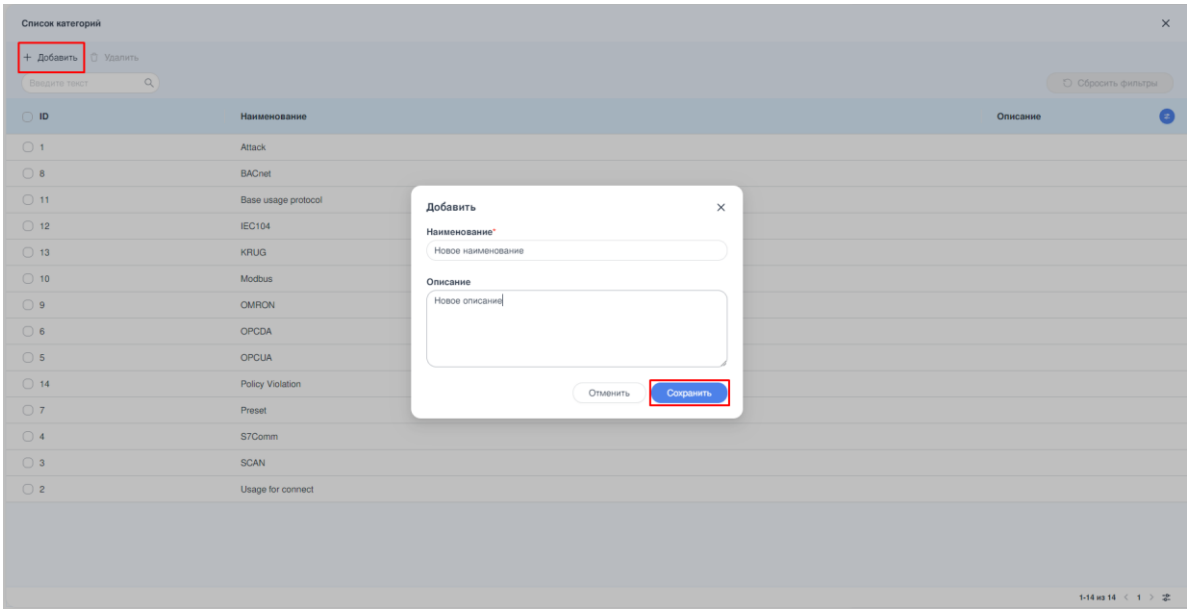


Рисунок – Добавление категории

- при необходимости заполнить поле **«Описание»**. Поле ограничено 250 символами;
- при необходимости снять флажок с чек-бокса **«Множественная реакция»**. Функция **«Множественная реакция»** применяет действия к каждому событию, которое соответствует правилу, и по умолчанию включена.

3. Указать значения необходимых параметров в блоке **«Условие»**:
   - в поле **«Условие срабатывания правила корреляции»** ввести условия срабатывания правила с помощью специального синтаксиса. Условия правила корреляции задаются на основании деталей события, для которого предназначено правило;
   - при необходимости нажать кнопку **«Помощь по коррелятору»** (см. Рисунок – Кнопка «Помощь по коррелятору»).

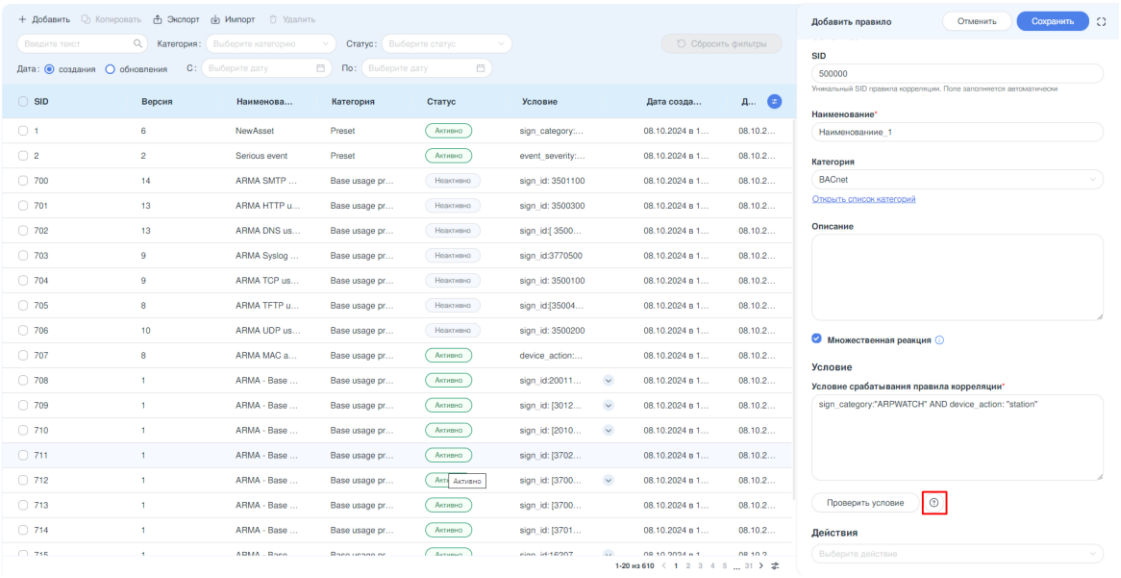


Рисунок – Кнопка «Помощь по коррелятору»

Кнопка открывает карточку с двумя вкладками – **«Синтаксис»** и **«Поля»**. Вкладка **«Синтаксис»** содержит пояснения по именам полей и терминам, особым символам, диапазонам и логическим операторам. Вкладка **«Поля»** содержит описание полей и типа данных каждого поля (см. Рисунок – Помощь по коррелятору);

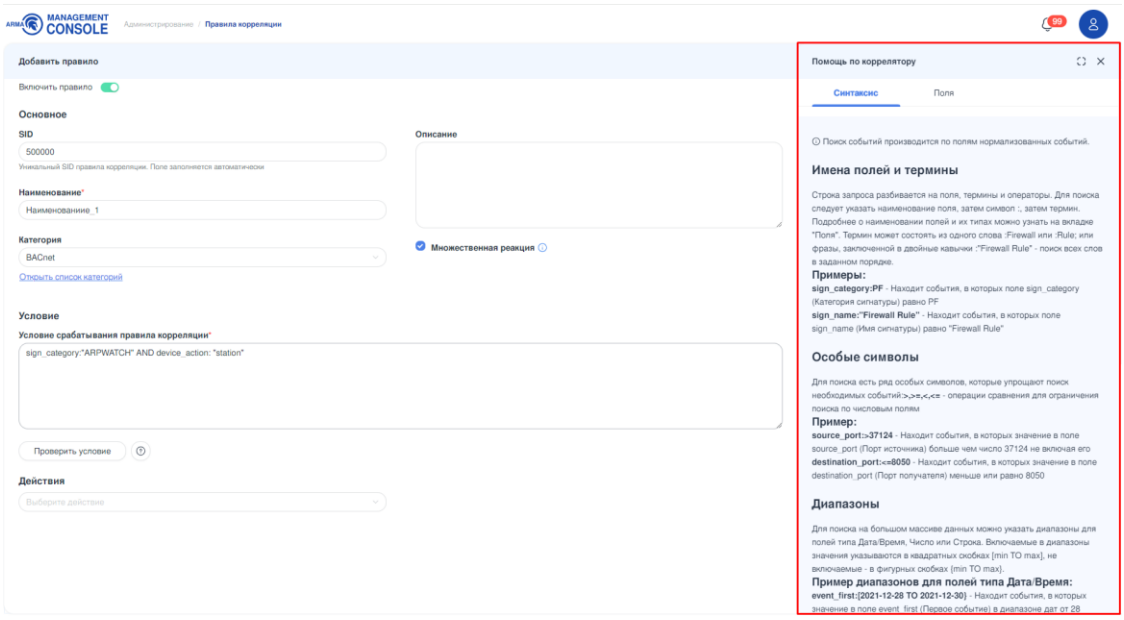


Рисунок – Помощь по коррелятору

- нажать кнопку **«Проверить условие»**. В случае если условие совпадает с имеющимися событиями, отобразится список найденных условий с количеством совпадений. Отсутствие записей в таблице **«Найденные условия»** не означает, что условие задано некорректно.

4. В блоке **«Действие»** из выпадающего списка (см. Типы действий настоящего руководства) выбрать необходимые значения из предустановленных типов:

- **«Добавить инцидент»** (см. Тип действия «Добавить инцидент»);
- **«Добавить актив»** (см. Тип действия «Добавить актив»);
- **«Выполнить сценарий Bash»** (см. Тип действия «Выполнить сценарий Bash»);
- **«Отправить Syslog сообщение»** (см. Тип действия «Отправить Syslog сообщение»);
- **«HTTP POST запрос»** (см. Тип действия «HTTP POST запрос»);
- **«Запустить исполняемый файл»** (см. Тип действия «Запустить исполняемый файл»);
- **«Правило межсетевого экрана»** (см. Тип действия «Правило межсетевого экрана»).

В зависимости от выбранного типа действия в блоке **«Действия»** будут отображены различные параметры.

5. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки **«Добавить правило»**.

6.4 Типы действий

Для описания типов действий используется подключённый источник событий **ARMA FW** (см. Раздел Источники событий настоящего руководства). На **ARMA FW** включено обнаружение устройств (см. раздел **«Обнаружение устройств»** руководства пользователя **ARMA FW**). Подключено новое устройство в сеть прослушиваемого сетевого интерфейса **ARMA FW**.

6.4.1 Тип действия «Добавить инцидент»

Тип действия **«Добавить инцидент»** при срабатывании определённого события позволяет создавать инцидент и отправлять его в журнал инцидентов **ARMA MC** (см. Инциденты настоящего руководства).

Для создания инцидента необходимо выполнить следующие действия (см. Рисунок – Действие «Инцидент»):

1. В блоке **«Действие»** выбрать **«Добавить инцидент»**.
2. Заполнить поле **«Наименование»**. Поле может содержать кириллические и латинские буквы, цифры, символы «.», «_», «-», «пробел» и не может содержать спецсимволы. Поле ограничено 128 символами. Существует возможность использования шаблонов коррелятора для создания наименования инцидента. Для ознакомления с шаблонами необходимо открыть подсказку справа от поля **«Наименование»**. Пример использования шаблона для заполнения поля **«Наименование»**:

Обнаружено сканирование Web интерфейсов, источник: {{.source_ip}}

3. При необходимости из выпадающего списка поля **«ТТУ ФСТЭК»** выбрать необходимое значение. Доступные значения:
   - **«INFO»**;
   - **«T1070 Скрытие идентификаторов компрометации»**;
   - **«T1202 Непрямое выполнение команды»**;
   - **«T2.10 Несанкционированный доступ путем подбора учетных данных»**;
   - **«T2.5 Эксплуатация уязвимостей компонентов систем и сетей при удаленной и локальной атаке»**;
   - **«T1 Сбор информации о системах и сетях»**.
4. Заполнить поле **«Важность»**, допустимые значения важности от 1 до 100.
5. При необходимости заполнить поле **«Ответственный»**, выбрав из выпадающего списка поля необходимого пользователя, зарегистрированного в **ARMA MC**.
6. При необходимости заполнить поле **«Описание»**.
7. В поле **«Рекомендации»** выбрать рекомендации по решению инцидента. В случае, если ни одна из предустановленных рекомендаций не подходит, существует возможность добавить пользовательскую рекомендацию. Для этого необходимо открыть список рекомендаций, нажать кнопку **«Добавить»**, в открывшемся окне ввести **«Наименование»** и **«Описание»**, затем нажать кнопку **«Сохранить»**.
8. В поле **«Последствия»** выбрать последствия инцидента. В случае, если ни одно из предустановленных последствий не подходит, существует возможность добавить пользовательское последствие. Для этого необходимо открыть список последствий, нажать кнопку **«Добавить»**, в открывшемся окне ввести **«Наименование»** и **«Описание»**, затем нажать кнопку **«Сохранить»**.
9. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки.

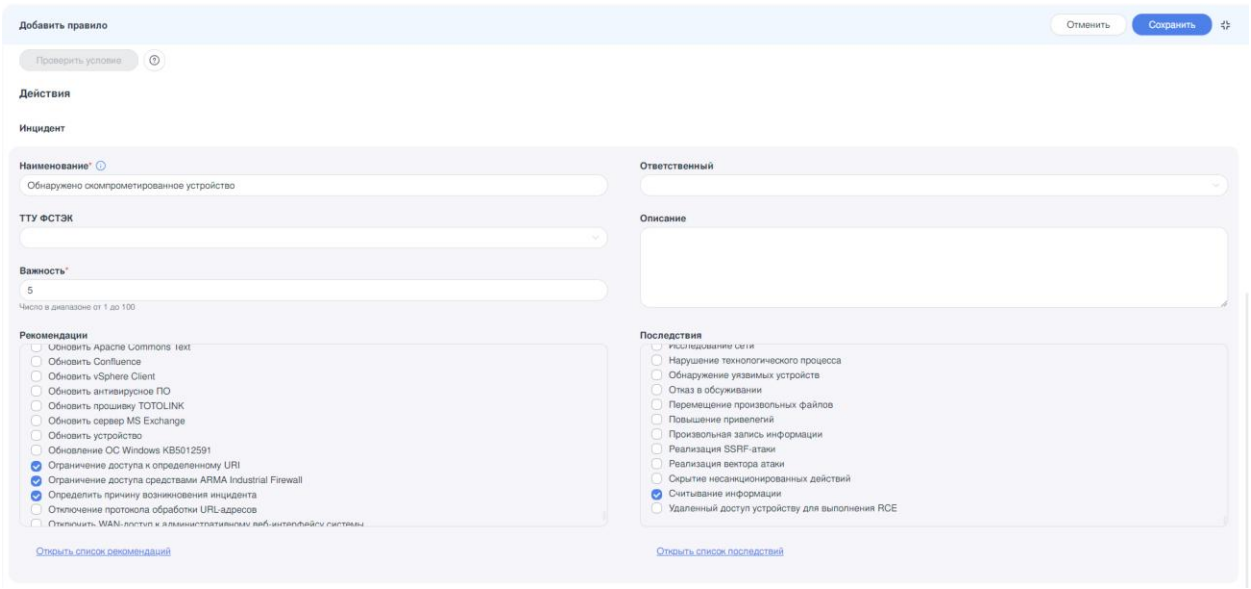


Рисунок – Действие «Инцидент»

Результатом срабатывания правила корреляции с типом действия **«Инцидент»** будет появление инцидента об обнаружении скомпрометированного устройства в подразделе **«Инциденты»** (см. Инциденты настоящего руководства) раздела меню **«Журналы»**.

6.4.2 Тип действия «Добавить актив»

При появлении новых устройств в сети тип действия **«Добавить актив»** позволяет добавлять записи в журнал активов **ARMA MC** (см. Активы настоящего руководства).

Для добавления правила, позволяющего добавлять активы, необходимо выполнить следующие шаги (см. Рисунок – Действие «Добавить актив»):

1. В блоке **«Действие»** выбрать **«Добавить актив»**.
2. Заполнить поле **«Наименование актива»**. Поле может содержать кириллические и латинские буквы, цифры, символы «.», «_», «-», «пробел» и не может содержать спецсимволы. Поле ограничено 128 символами.
3. При необходимости заполнить следующие необязательные поля:
   - **«Тип актива»**. Поле содержит выпадающий список с предустановленными типами активов (см. Активы);
   - **«Группа»**. Поле содержит выпадающий список с группами, созданными пользователем (см. Активы);
   - **«Описание»**. Поле может содержать кириллические и латинские буквы, спецсимволы и ограничено 250 символами;
   - **«Производитель»**. Поле содержит выпадающий список. Список по умолчанию пуст. Для первичного создания элемента списка необходимо открыть список производителей, нажать кнопку **«Добавить»**, в

открывшемся окне ввести **«Наименование»** и **«Описание»**, затем нажать кнопку **«Сохранить»**. Поле может содержать кириллические и латинские буквы, не может содержать спецсимволы и ограничено 128 символами;

- **«Модель»**. Поле может содержать кириллические и латинские буквы, не может содержать спецсимволы и ограничено 128 символами;
- **«Операционная система»**. Поле содержит выпадающий список. Список по умолчанию пуст. Для первичного создания элемента списка необходимо открыть список операционных систем, нажать кнопку **«Добавить»**, в открывшемся окне ввести **«Наименование»** и **«Описание»**, затем нажать кнопку **«Сохранить»**. Поле может содержать кириллические и латинские буквы, цифры, символы «.», «_», «-», «пробел» и не может содержать спецсимволы. Поле ограничено 128 символами.

4. Заполнить поле **«IP-адрес»**. Кроме фиксированного IP-адреса можно указать **«{{.source_ip}}»**.
5. При необходимости заполнить поле **«Порты»**.
6. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки правила корреляции.

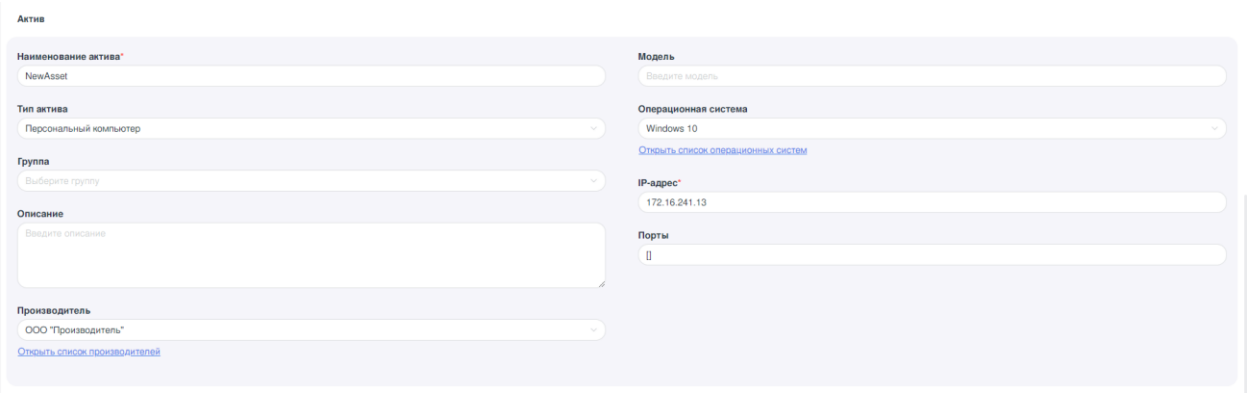


Рисунок – Действие «Добавить актив»

Результатом срабатывания правила корреляции с типом действия **«Добавить актив»** будет появление актива в подразделе **«Активы»** (см. Активы настоящего руководства) раздела меню **«Инвентаризация»**.

6.4.3 Тип действия «Выполнить сценарий Bash»

Тип действия **«Выполнить сценарий Bash»** позволяет при срабатывании определённых событий запускать сценарий написанного Bash-скрипта.

Примечание:

Для обеспечения стабильной и предсказуемой работы системы при использовании bash-скриптов следует:

- избегать использования потенциально опасных команд, таких как **«rm -rf /, dd, mkfs, chmod/chown»** на системные пути, а также любых операций, затрагивающих критическую файловую структуру ОС;
- не эскалировать привилегии, так как попытки обхода этого ограничения могут привести к непредсказуемому поведению системы;
- использовать только пути, предназначенные для взаимодействия с коррелятором (например, рабочие каталоги, логи, конфигурации приложения);
- не обращаться к системным конфигурационным файлам (**«/etc/*»**, кроме явно разрешённых);
- скрипты должны быть максимально легковесными и завершаться в разумное время. Бесконечные циклы, ожидание ввода, запуск сервисов – недопустимы.

Для запуска Bash-скрипта необходимо выполнить следующие действия (см. Рисунок – Действие «Выполнить сценарий Bash»):

1. В блоке **«Действия»** выбрать **«Выполнить сценарий Bash»**.
2. Заполнить поле **«Тело Bash скрипта»**. Не более 2000 символов. Первой строкой скрипта указать #!/bin/bash.
3. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки правила корреляции.

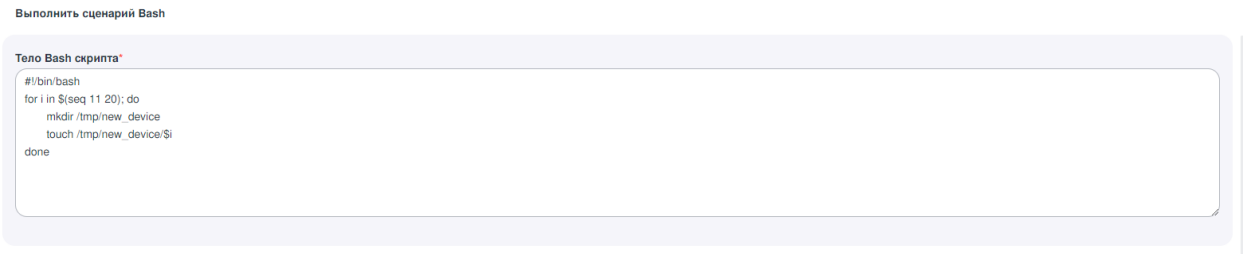


Рисунок – Действие «Выполнить сценарий Bash»

Результатом срабатывания правила корреляции с типом действия **«Выполнить сценарий Bash»** из приведённого выше примера будет добавление каталога «new_device» в каталог «tmp».

6.4.4 Тип действия «Отправить Syslog сообщение»

Тип действия **«Отправить Syslog сообщение»** позволяет отправлять запись по протоколу «Syslog» при возникновении определённого события.

Для отправки записи необходимо выполнить следующие действия (см. Рисунок – Действие «Отправить Syslog сообщение»):

1. В блоке **«Действие»** выбрать **«Отправить Syslog сообщение»**.
2. Заполнить поле **«Хост»** – IP-адрес хоста для отправки Syslog-события.
3. Заполнить поле **«Порт»**, поле может содержать значения от 1 до 65535.
4. Из выпадающего списка поля **«Протокол»** выбрать необходимое значение («TCP»/«UDP»).
5. Заполнить поле **«Получатель»** – имя Syslog сервера.
6. Заполнить поле **«Сообщение»**, поле может содержать кириллические и латинские буквы, спецсимволы и ограничено 256 символами.
7. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки правила корреляции.

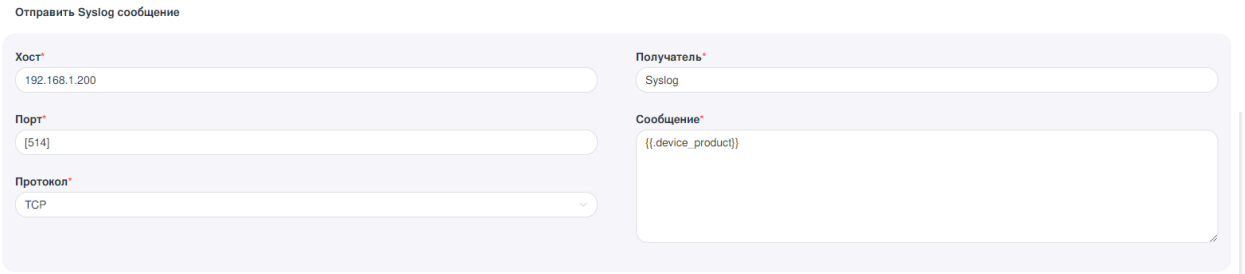


Рисунок – Действие «Отправить Syslog сообщение»

Результатом срабатывания правила корреляции с типом действия **«Отправить Syslog сообщение»** будет отправление записи на Syslog-сервер.

6.4.5 Тип действия «HTTP POST запрос»

Тип действия **«HTTP POST запрос»** позволяет отправлять информацию на внешний сервер при срабатывании определённого события. Предварительно необходимо убедиться в наличии доступа к используемому внешнему серверу.

Для отправки информации на внешний сервер необходимо выполнить следующие действия (см. Рисунок – Действие «HTTP POST запрос»):

1. В блоке **«Действие»** выбрать **«HTTP POST запрос»**.
2. Заполнить поле **«URL»** – URL назначения для отправки события.
3. Из выпадающего списка поля **«Протокол»** выбрать необходимое значение («text/plain»/«application/json»).
4. Заполнить поле **«Шаблон»** – шаблон для тела HTTP запроса, поле ограничено 256 символами.

5. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки правила корреляции.

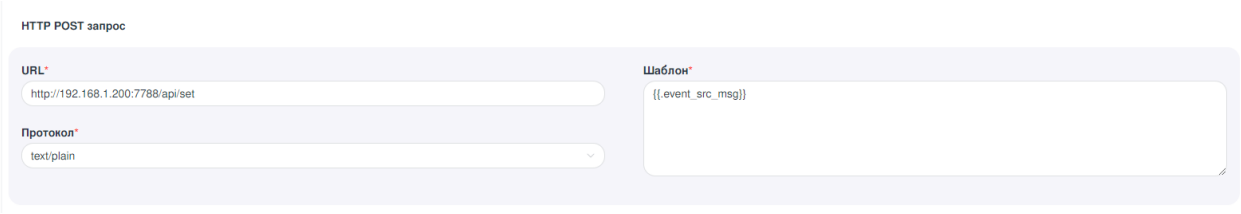


Рисунок – Действие «HTTP POST запрос»

Результатом срабатывания правила корреляции с типом действия **«HTTP POST запрос»** будет появление события на внешнем сервере.

6.4.6 Тип действия «Запустить исполняемый файл»

Действие **«Запустить исполняемый файл»** позволяет при срабатывании определённых событий запускать исполняемый файл, например, для реагирования на инцидент.

Для запуска исполняемого файла необходимо выполнить следующие действия (см. Рисунок – Действие «Запустить исполняемый файл»):

1. В блоке **«Действие»** выбрать **«Запустить исполняемый файл»**.
2. Заполнить поле **«Путь к исполняемому файлу»** – абсолютный путь к исполняемому файлу.
3. При необходимости заполнить поле **«Аргументы»**.
4. При необходимости заполнить поле **«Окружение»** переменными окружения.
5. При необходимости заполнить поле **«Рабочая папка»**.
6. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки правила корреляции.

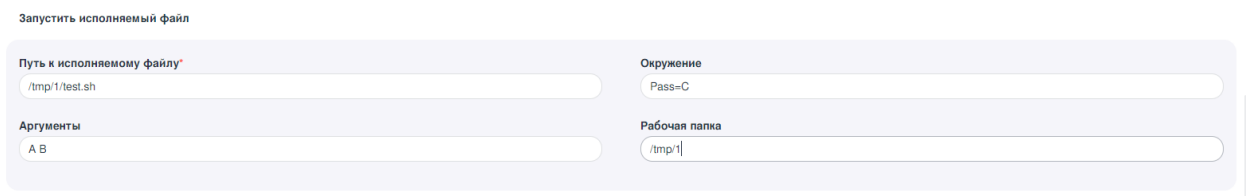


Рисунок – Действие «Запустить исполняемый файл»

Результатом срабатывания правила корреляции с типом действия **«Запустить исполняемый файл»** будет запуск исполняемого файла из указанной директории.

6.4.7 Тип действия «Правило межсетевого экрана»

Тип действия **«Правило межсетевого экрана»** позволяет создавать правило МЭ на определённое событие (см. Рисунок – Действие «Правило межсетевого экрана»).

Для создания правила МЭ необходимо выполнить следующие действия:

1. В блоке **«Действие»** выбрать **«Правило межсетевого экрана»**.
2. В поле **«Межсетевой экран ARMA»** выбрать необходимый межсетевой экран из списка подключённых к **ARMA MC**.
3. Выбрать статус правила на переключателе **«Статус правила»** – «Активно»/«Неактивно».
4. Заполнить поле **«Последовательность»** порядковым номером. Последовательность определяет порядок исполнения правила.
5. Выбрать из выпадающего списка поля **«Действие»** необходимое действие над пакетом трафика. Доступные значения:
   - **«Pass»** – разрешить движение пакета;
   - **«Drop»** – отбросить пакет;
   - **«Reject»** – отбросить пакет и отправить уведомление отправителю.
6. Выбрать принцип совпадения на переключателе **«Быстрая проверка»**. Включённое состояние переключателя **«Быстрая проверка»** соответствует принципу первого совпадения, выключенное - принципу последнего совпадения (Подробная информация о **«Быстрой проверке»** описана в Руководстве пользователя **ARMA FW**, раздел **«Межсетевой экран»** -> **«Настройка правил МЭ»**).
7. Выбрать из выпадающего списка поля **«Интерфейс»** один или несколько необходимых интерфейсов. Доступные значения:
   - **«LAN»**;
   - **«OPT1»**;
   - **«OPT2»**;
   - **«WAN»**.
8. Выбрать из выпадающего списка поля **«Направление»** необходимое направление. Доступные значения:
   - **«In»** – входящий трафик;
   - **«Out»** – исходящий трафик.
9. Выбрать из выпадающего списка поля **«Версия TCP/IP»** необходимую версию. Доступные значения:
   - **«IPv4»**;
   - **«IPv6»**.
10. Выбрать из выпадающего списка поля **«Протокол»** необходимый протокол.

11. Заполнить поле **«Отправитель»** IP-адресом отправителя.
12. При необходимости заполнить поле **«Порт отправителя»**.
13. Выбрать необходимый параметр на переключателе **«Инвертировать отправителя»**. При включённом состоянии переключателя **«Инвертировать отправителя»** правило будет применено для всех отправителей, кроме указанного в поле **«Отправитель»**.
14. Заполнить поле **«Получатель»** IP-адресом получателя.
15. При необходимости заполнить поле **«Порты получателя»**.
16. Выбрать необходимый параметр на переключателе **«Инвертировать получателя»**. При включённом состоянии переключателя **«Инвертировать получателя»** правило будет применено для всех получателей, кроме указанного в поле **«Получатель»**.
17. Выбрать необходимый параметр на переключателе **«Журналирование»**.
18. При необходимости заполнить поле **«Описание»**.
19. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки правила корреляции.

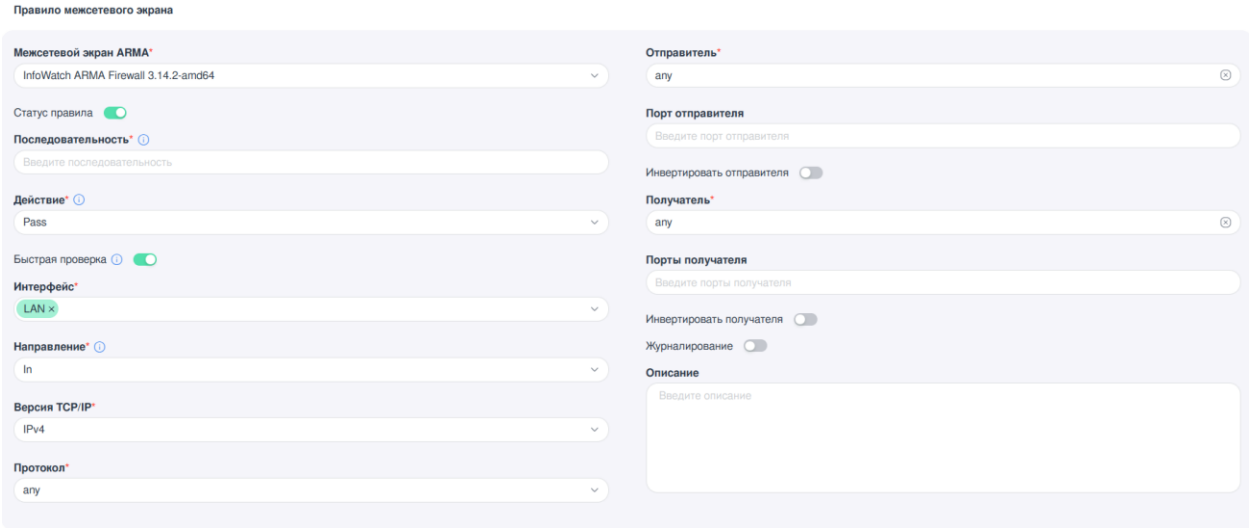


Рисунок – Действие «Правило межсетевого экрана»

Результатом срабатывания правила корреляции с типом действия **«Правило межсетевого экрана»** будет добавление правила МЭ в **ARMA FW** в раздел меню **Межсетевой экран: API правила**.

> **Примечание**:
>
> При редактировании созданного правила корреляции с типом действия **«Правило межсетевого экрана»** при выборе другого МЭ в параметре **«ARMA FW»** текущие настройки будут сброшены.

6.5 Импорт и экспорт правил корреляции

Существует возможность импорта и экспорта правил корреляции в формате **«json»**.

Для **импорта** правил корреляции необходимо на панели инструментов нажать кнопку **«Импорт»**, в открывшейся форме проводника выбрать необходимый файл с правилами корреляции и нажать кнопку **«Открыть»** (см. Рисунок – Импорт правил корреляции).

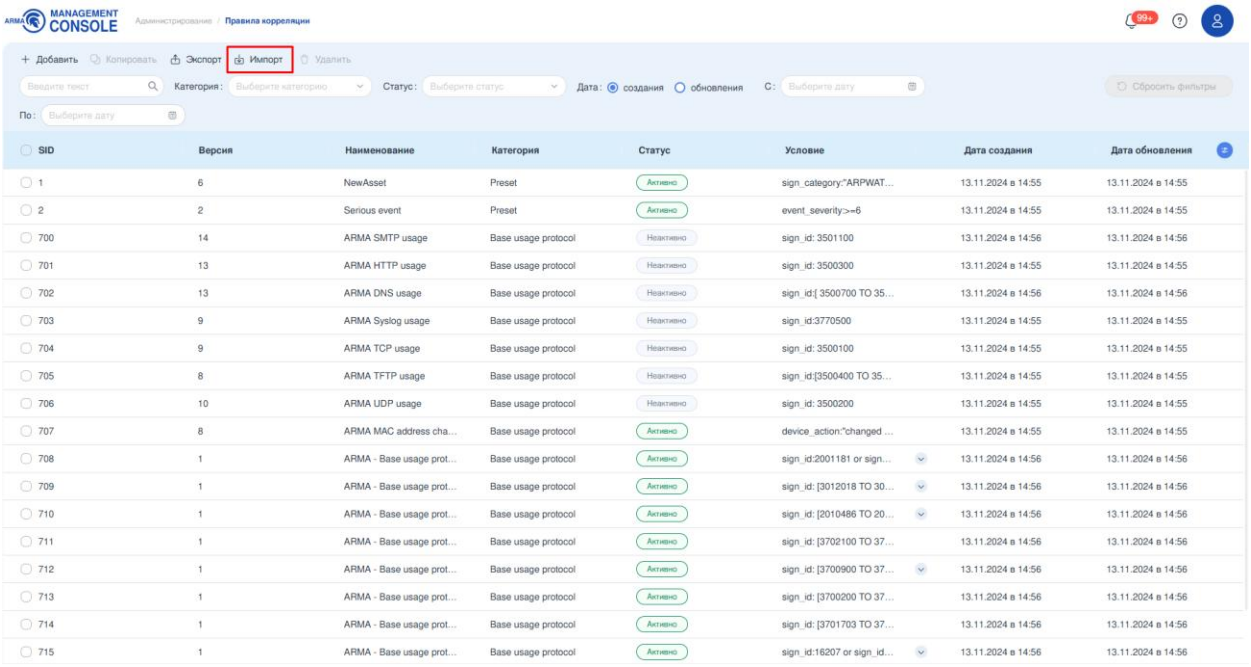


Рисунок – Импорт правил корреляции

При успешном окончании импорта правил корреляции появится соответствующее уведомление (см. Рисунок – Успешный импорт правил корреляции).

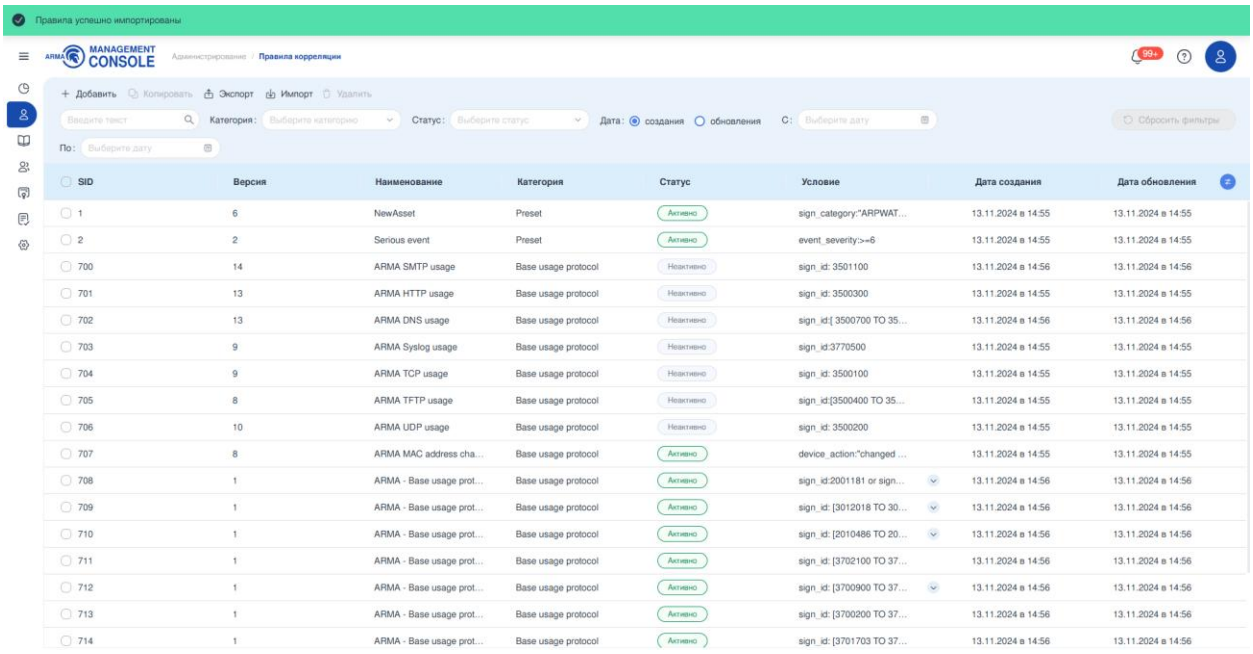


Рисунок – Успешный импорт правил корреляции

Для **экспорта** правил корреляции необходимо на панели инструментов нажать кнопку **«Экспорт»** (см. Рисунок – Экспорт правил корреляции).

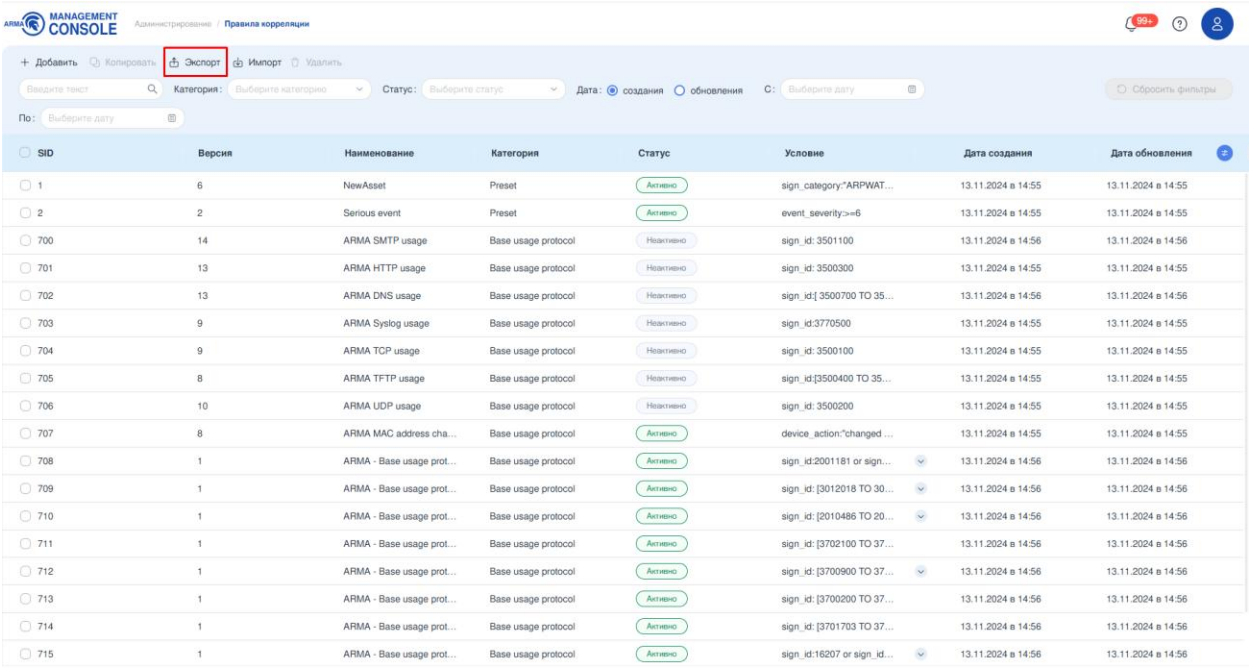


Рисунок – Экспорт правил корреляции

В случае успешного экспорта данные сохранятся на локальный диск, и появится соответствующее уведомление (см. Рисунок – Успешный экспорт правил корреляции).

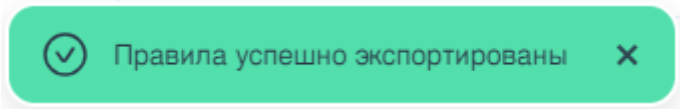


Рисунок – Успешный экспорт правил корреляции

6.6 Удаление правила корреляции

Существует возможность удаления пользовательского правила корреляции.

Для удаления правила корреляции необходимо выполнить следующие действия (см. Рисунок – Удаление правила корреляции):

1. Выбрать правило корреляции, установив флажок рядом с его SID.
2. На панели инструментов нажать кнопку **«Удалить»**.

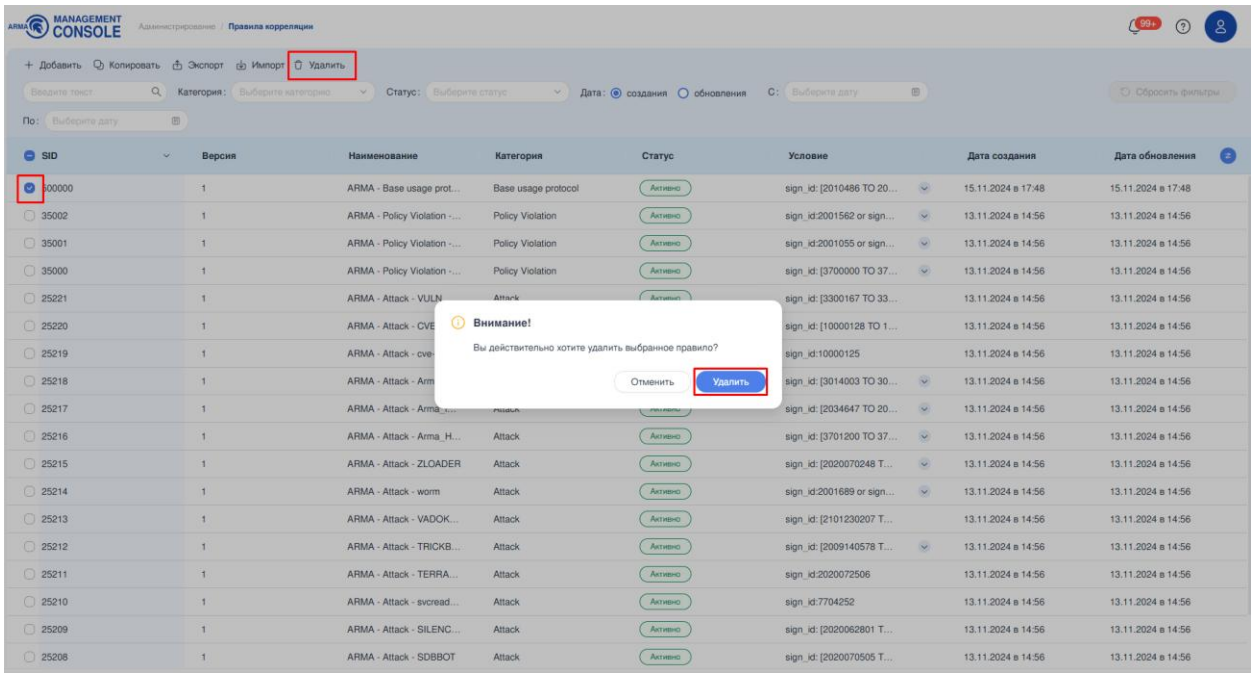


Рисунок – Удаление правила корреляции

При успешном удалении правила корреляции появится соответствующее уведомление (см. Рисунок – Успешное удаление правила корреляции).

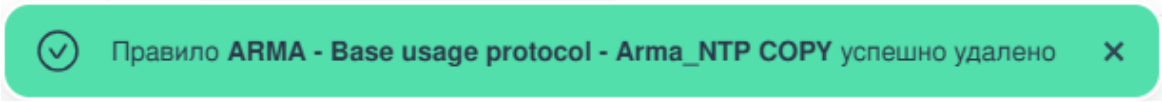


Рисунок – Успешное удаление правила корреляции

7 ИНЦИДЕНТЫ

В настоящем разделе представлено описание подраздела меню **«Инциденты»**, предусматривающего механизм управления следующими функциями:

- управление инцидентами;
- экспорт инцидентов;
- управление группами инцидентов.

В подразделе **«Инциденты»** отображаются инциденты, обнаруженные подключёнными к **ARMA MC** устройствами.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Администрирование»**, затем – подраздел **«Инциденты»** (см. Рисунок – Список инцидентов).

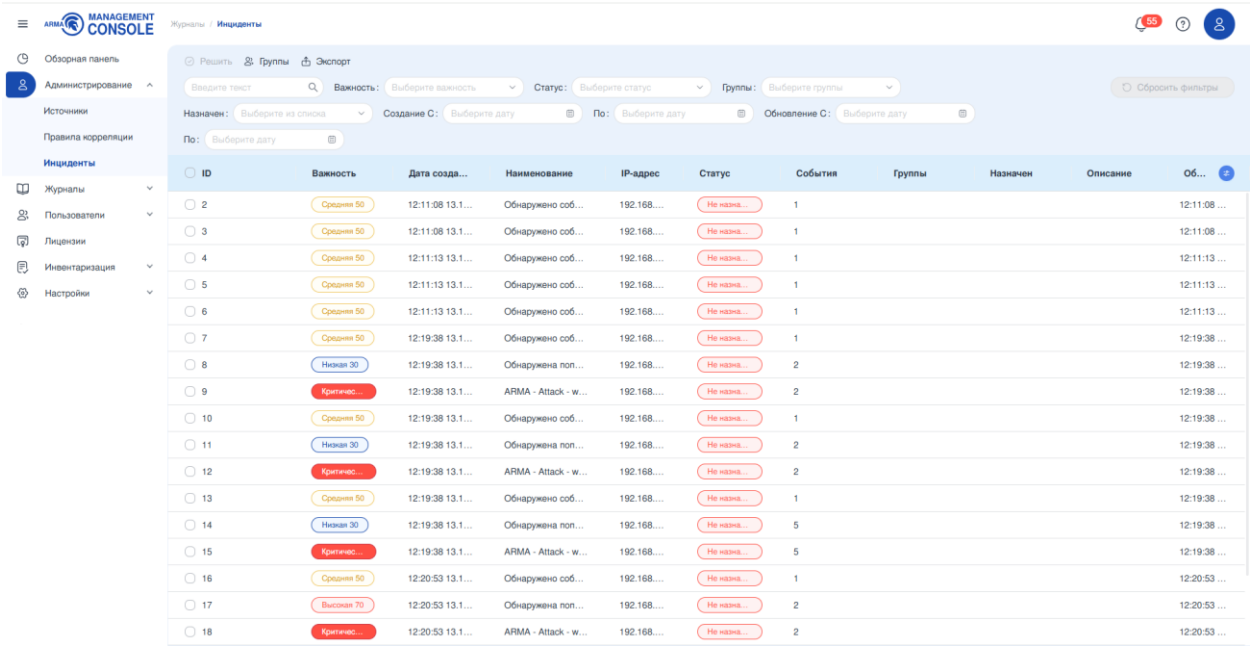


Рисунок – Список инцидентов

Подраздел меню позволяет просматривать инциденты в формате таблицы, состоящей из следующих столбцов:

- **«ID»** – порядковый номер инцидента;
- **«Важность»** – важность инцидента, определяется системой на основании сработавшего правила корреляции;
- **«Дата создания»** – время и дата создания инцидента;
- **«Наименование»** – наименование инцидента, определяется системой на основании сработавшего правила корреляции;
- **«IP адрес»** – IP адрес получателя;

- **«Статус»** – статус инцидента для расследования офицером ИБ;
- **«События»** – количество событий, на основании которых был создан инцидент;
- **«Группы»** – группа, в которую определён инцидент. Группы назначаются пользователем и используются для удобства фильтрации;
- **«Назначен»** – имя пользователя, на которого назначен инцидент для расследования;
- **«Описание»** – описание инцидента, определяется системой на основании сработавшего правила корреляции;
- **«Обновление»** – время и дата обновления инцидента в карточке инцидента.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

7.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать инциденты по всем столбцам списка и по умолчанию состоит из следующих полей (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **«Важность»**;
- **«Статус»**;
- **«Группы»**;
- **«Назначен»**;
- **«Создание»**;
- **«Обновление»**;
- **кнопка «Сбросить фильтры»**.

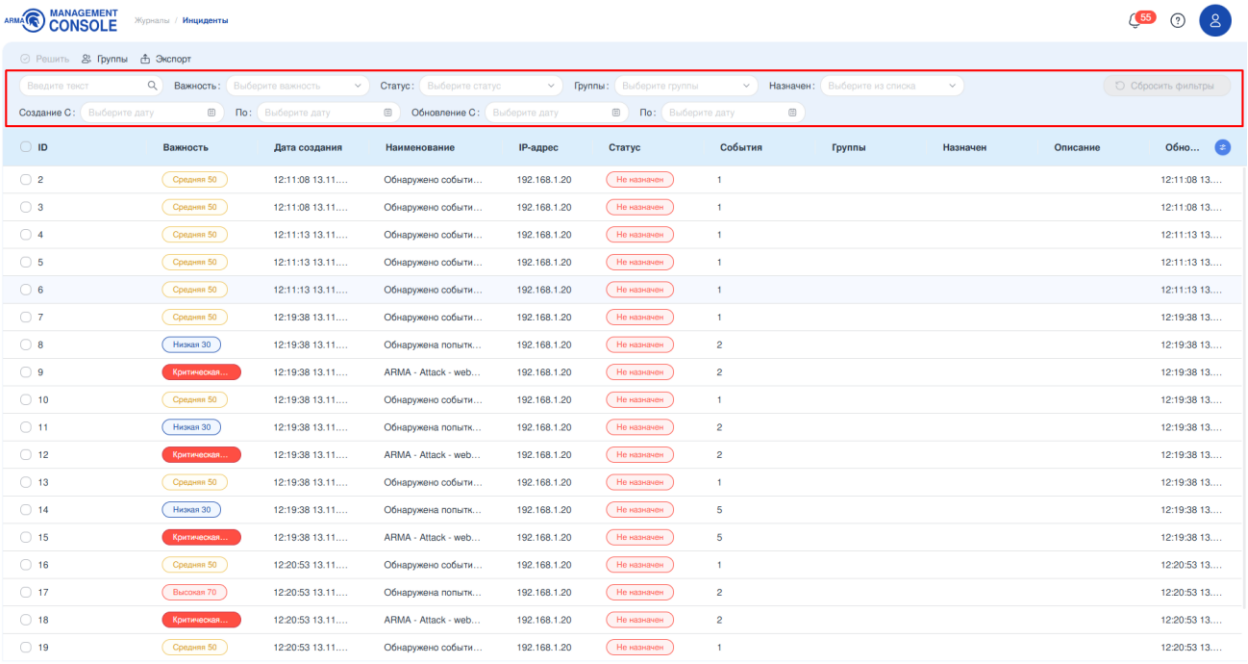


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам **«ID»**, **«Наименование»**, **«Группы»** и **«Назначен»**.

Фильтрация по полю **«Важность»** позволяет отфильтровать данные по важности инцидента. Поле **«Важность»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Критическая»** (90-100);
- **«Высокая»** (70-89);
- **«Средняя»** (40-69);
- **«Низкая»** (1-39).

Фильтрация по полю **«Статус»** позволяет отфильтровать данные по статусу инцидента. Поле **«Статус»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Назначен»** – расследование инцидента назначено на конкретного пользователя;
- **«Отложен»** – расследование инцидента отложено;
- **«Ложный»** – расследование инцидента проведено, инцидент определён как ложный;
- **«Не назначен»** – статус инцидента по умолчанию;
- **«Решен»** – расследование инцидента проведено, инцидент решён.

Фильтрация по полю **«Группы»** позволяет отфильтровать данные по группам, в которые включены инциденты.

Фильтрация по полю **«Назначен»** позволяет отфильтровать данные по исполнителям, на которых назначены инциденты.

Фильтрация по полям **«Создание»** и **«Обновление»** позволяет отфильтровать данные по дате создания и обновления и включает в себя следующие поля:

- **«С»** позволяет отфильтровать инциденты по дате создания/добавления и задаёт начальную дату диапазона. После ввода даты в таблице отобразятся лишь те инциденты, где **«Дата»** совпадает или больше введённой в фильтр.
- **«По»** позволяет отфильтровать инциденты по дате создания/добавления и задаёт конечную дату диапазона. После ввода даты в таблице отобразятся лишь те инциденты, где **«Дата»** совпадает или меньше введённой в фильтр.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

7.2 Просмотр подробной информации об инциденте

Для просмотра подробной информации об инциденте необходимо нажать на запись с необходимым инцидентом, в результате будет отображена карточка **«[Имя инцидента]»** (см. Рисунок – Карточка инцидента). Данные в карточке невозможно отредактировать.

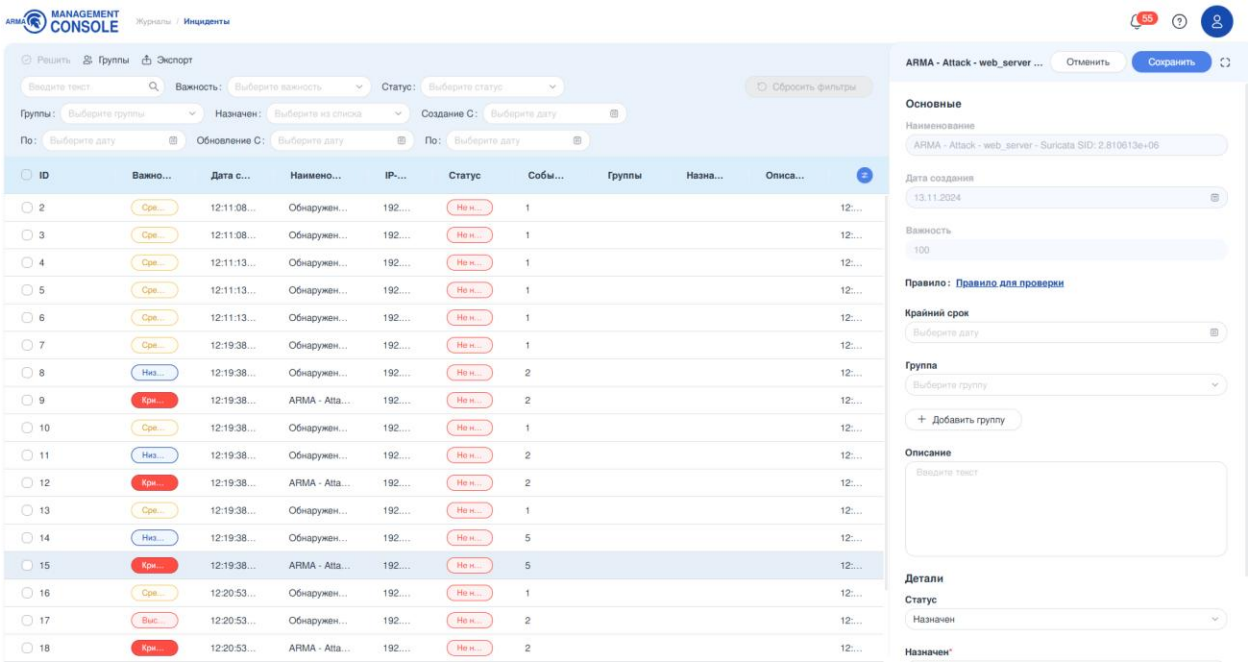


Рисунок – Карточка инцидента

При нажатии кнопки «  » карточка инцидента откроется в полноразмерном режиме. Карточка содержит подробную информацию об инциденте и включает следующие блоки (см. Рисунок – Полноразмерная карточка инцидента):

- **«Основные»**;
- **«Детали»**;
- **«Рекомендации»**;
- **«Последствия»**;
- **«События»**.

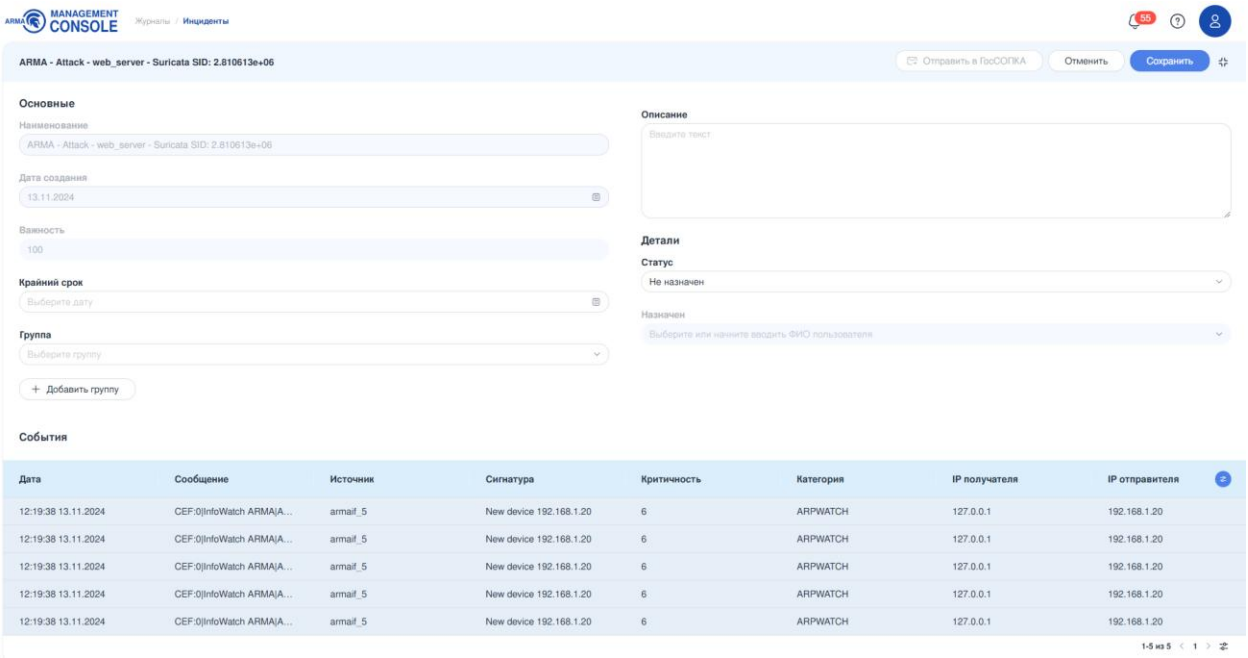


Рисунок – Полноразмерная карточка инцидента

Блок **«Основные»** позволяет выполнить следующие действия:

- ознакомиться с информацией о наименовании, дате создания и важности инцидента;
- перейти по ссылке на правило корреляции, по которому был создан инцидент;
- назначить крайний срок расследования инцидента;
- добавить инцидент в существующую группу или создать новую группу для инцидента;
- изменить/добавить описание инцидента.

Блок **«Детали»** позволяет выполнить следующие действия:

- назначить инциденту статус;

- назначить пользователя для работы с инцидентом.

Блок **«Рекомендации»** позволяет ознакомиться с информацией о рекомендациях по работе с инцидентом.

Блок **«Последствия»** позволяет ознакомиться с информацией о последствиях инцидента.

Блок **«События»** отображает связанные с инцидентом события в табличной форме со следующими столбцами:

- **«Дата»**;
- **«Сообщение»**;
- **«Источник»**;
- **«Сигнатура»**;
- **«Критичность»**;
- **«Категория»**;
- **«IP получателя»**;
- **«IP отправителя»**.

7.3 Управление инцидентами

В **ARMA MC** предусмотрены следующие шаги для работы с инцидентами:

- назначение пользователя для решения инцидента, даты до которой данный инцидент необходимо решить, изменение статуса инцидента;
- пользователь, назначенный для решения инцидента, исходя из результата проведённого расследования, должен изменить статус инцидента, в случае положительного решения инцидента – отметить инцидент как решённый.

7.3.1 Назначение пользователя для решения инцидента

Для назначения пользователей для решения инцидента необходимо выполнить следующие действия:

1. Открыть карточку инцидента **«[Имя инцидента]»**.
2. В поле параметра **«Статус»** выбрать значение **«Назначен»**.
3. В поле параметра **«Назначен»** выбрать пользователя, на которого будет назначен инцидент.
4. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки для сохранения изменений.

7.3.2 Внесение результата проведенного расследования

Для внесения результата проведённого расследования назначенному пользователю необходимо выполнить следующие действия:

1. Открыть карточку инцидента **«[Имя инцидента]»**.
2. Изменить значение поля параметра **«Статус»**.
3. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки для сохранения изменений.

   Примечание:

   В случае положительного решения инцидента нажать кнопку **«Решить»** на панели инструментов для того, чтобы отметить инцидент как решённый.

7.4 Экспорт инцидентов

Существует возможность локально сохранить таблицу инцидентов. Для этого необходимо нажать кнопку **«Экспорт»** на панели инструментов (см. Рисунок – Список инцидентов).

7.5 Управление группами инцидентов

Существует возможность объединять инциденты в группы. Группы назначаются пользователем и используются для удобства фильтрации.

7.5.1 Добавление группы

Для добавления группы необходимо выполнить следующие действия (см. Рисунок – Добавление группы):

1. На панели инструментов нажать кнопку **«Группы»**.
2. В открывшейся форме **«Список групп»** нажать кнопку **«Добавить»**.
3. В открывшемся окне указать значения в полях параметров **«Наименование»** и **«Описание»**.
4. Нажать кнопку **«Сохранить»**.

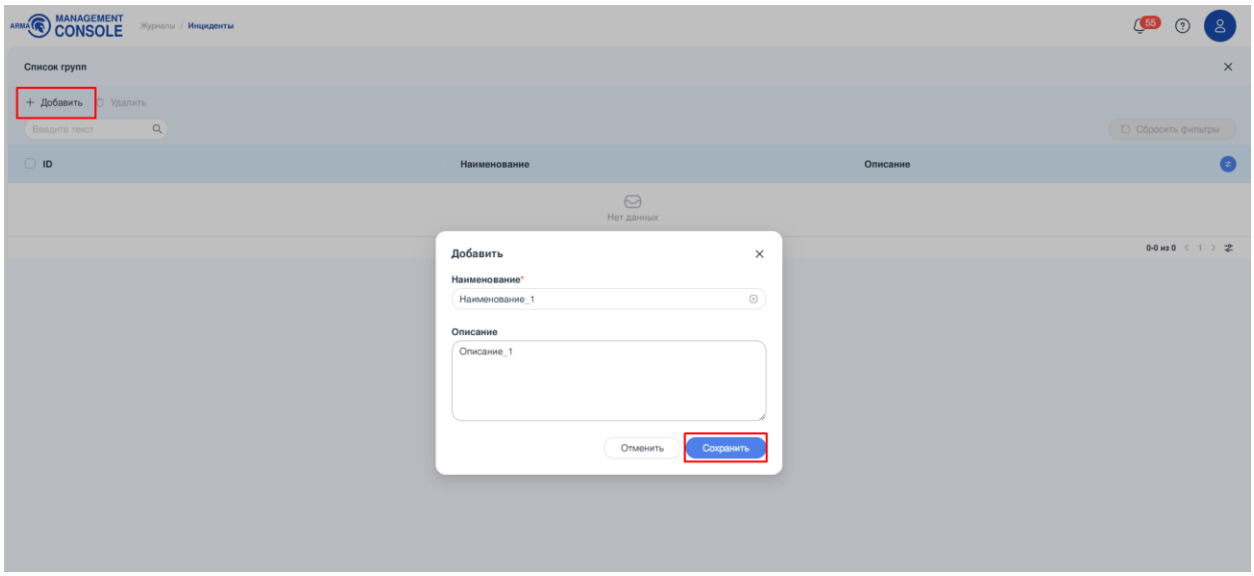


Рисунок – Добавление группы

В случае успешного создания группы появится соответствующее уведомление (см. Рисунок – Успешное добавление группы).

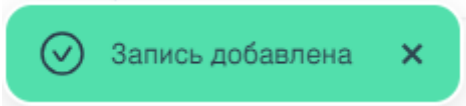


Рисунок – Успешное добавление группы

7.5.2 Редактирование группы

Для редактирования группы необходимо выполнить следующие действия (см. Рисунок – Изменение группы):

1. На панели инструментов нажать кнопку **«Группы»**.
2. В форме **«Список групп»** нажать на необходимую группу.
3. В открывшемся окне отредактировать значения в полях параметров **«Наименование»** и/или **«Описание»**.
4. Нажать кнопку **«Изменить»**.

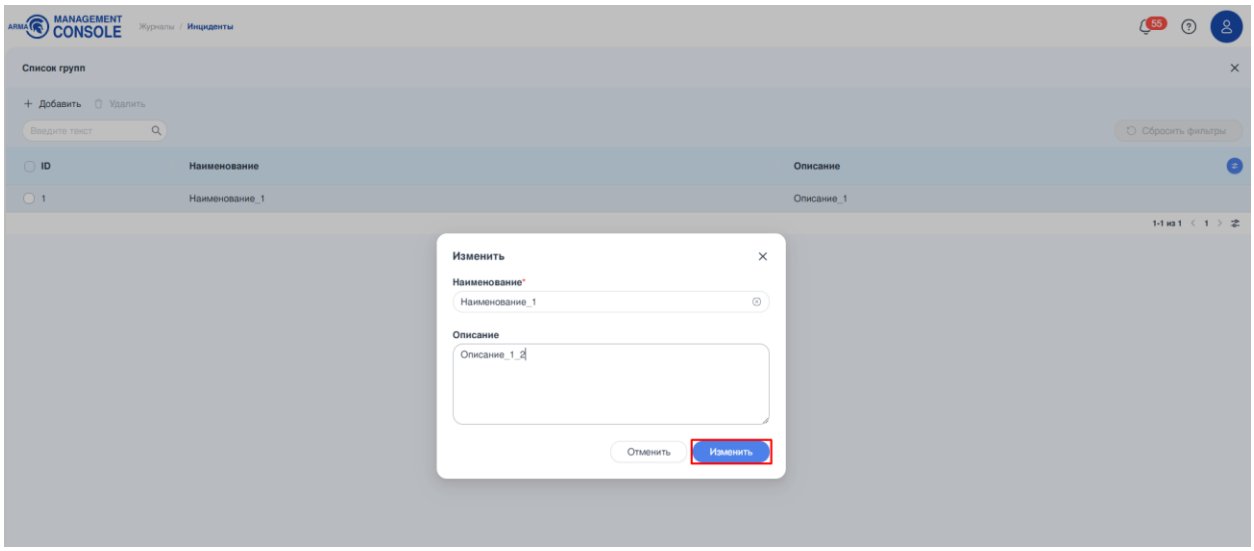


Рисунок – Изменение группы

В случае успешного редактирования группы появится соответствующее уведомление (см. Рисунок – Успешное изменение группы).

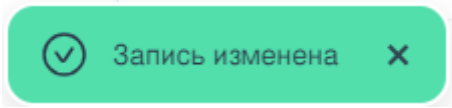


Рисунок – Успешное изменение группы

7.5.3 Удаление группы

Для удаления группы необходимо выполнить следующие действия (см. Рисунок – Удаление группы):

1. В форме **«Список групп»** установить флажок в чек-боксе слева от значения **«ID»** необходимой группы или групп.
2. Нажать кнопку **«Удалить»** на панели инструментов.
3. В появившемся окне подтвердить удаление группы, нажав кнопку **«Удалить»**.

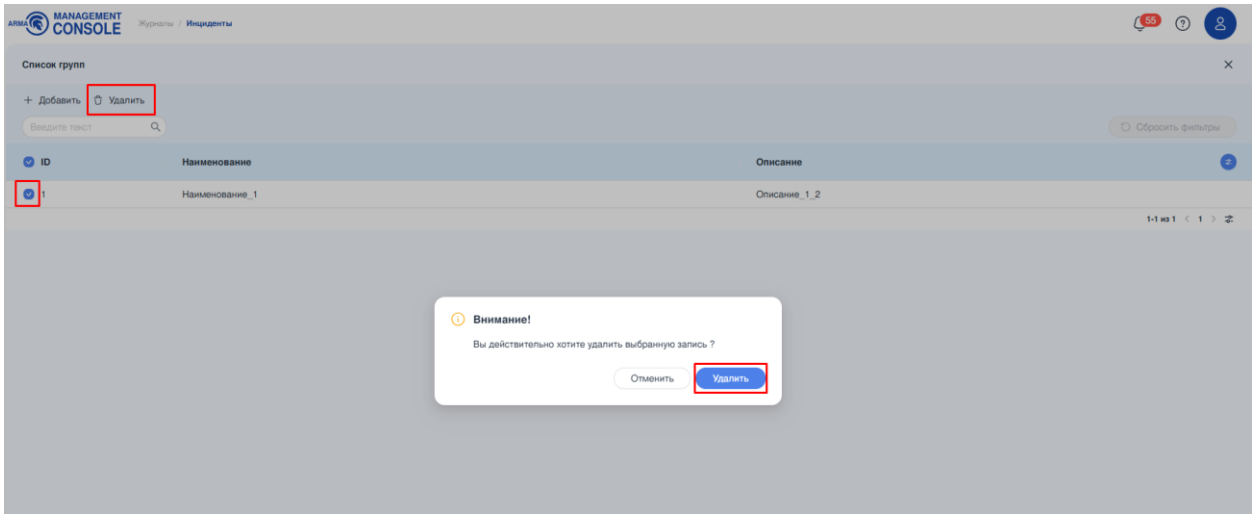


Рисунок – Удаление группы

В случае успешного удаления группы появится соответствующее уведомление (см. Рисунок – Успешное удаление группы).

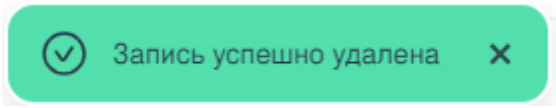


Рисунок – Успешное удаление группы

7.6 Формат сообщения об инциденте

Формат основного сообщения имеет следующий вид:

```
«<DateTime> <Host/IP> AMC: <MessageBody>»
```

где:

- **«<DateTime>»** – дата и время получения сообщения;
- **«<Host/IP>»** – хост или IP адрес отправителя;
- **«<MessageBody>»** – тело сообщения.

Пример основного сообщения:

```
Dec 17 17:26:32 172.18.0.10 AMC: CEF:0|InfoWatch ARMA|ARMAMC|1.0.1|Incident|test|5|cnt=1 rt=1608216295000
cs1=1c5f4516-27cb4714-af79-9643f8c18022 cs1Label=IncidentID start=1608216259000 end=1608216259000
msg=<14>CEF:0|armaif|Suricata|2.0|429496728|suricataalert|8|unixdate\=1608216259 .676164 log_from\=suricata
cid\=28775 gid\=1 signature\=429496728 rev\=1 msg\=test classification\=null priority\=3 proto\=TCP
ip_src\=192.168.56.100 port_src\=80 ip_dst\=10.20.30.1 port_dst\=34568 mechanic\=IDS
```

7.6.1 Формат вложенного сообщения «cef»

Формат вложенного сообщения **«cef»** имеет следующий вид:

```
«CEF:<Version>|<Device Vendor>|<Device Product>|<Device Version>
|<Device Event Class ID>|<Name>|<Severity>|<Extension>»
```

где:

- **«<Version>»** – версия **«cef»**;
- **«<Device Vendor>»** – производитель источника логов, всегда **InfoWatch ARMA**;
- **«<Device Product>»** – название продукта источника логов, **ARMA MC**;

- **«<Device Version>»** – версия продукта источника логов;
- **«<Device Event Class ID>»** – тип сообщения, всегда равен «Incident»;
- **«<Name>»** – название инцидента;
- **«<Severity>»** – серьёзность инцидента от «0» до «10»;
- **«<Extension>»** – дополнительные поля, представляющие собой пары ключ=значение, в значении допускаются пробелы:
  - **«cnt»** – количество событий, сформировавших инцидент;
  - **«rt»** – время создания инцидента в формате «unixtime» в миллисекундах, например, «1608216295000»;
  - **«cs1»** – уникальный идентификатор инцидента, например, «1c5f451627cb–4714–af79–9643f8c18022»;
  - **«cs1Label»** – описание того, что записывается в **«cs1»**, всегда «IncidentID»;
  - **«start»** – время появления первого события для текущего инцидента в формате «unixtime» в миллисекундах, например, «1608216295000»;
  - **«end»** – время появления последнего события для текущего инцидента в формате «unixtime» в миллисекундах, например, «1608216295000»;
  - **«msg»** – описание инцидента, зависит от сформировавшего инцидент правила корреляции.

Применяется экранирование символов \ и = с помощью постановки символа \ перед ними.

Пример вложенного сообщения:

```
CEF:0|InfoWatch ARMA|ARMAMC|1.0.1|Incident|test|5|cnt=1rt=1608216295000
cs1=1c5f4516-27cb-4714-af79-9643f8c18022cs1Label=IncidentID
start=1608216259000 end=1608216259000
msg=<14>CEF:0|armaif|Suricata|2.0|429496728|suricataalert|8|unixdate\=16082162
59 .676164
log_from\=suricata cid\=28775 gid\=1 signature\=429496728 rev\=1 msg\=test
classification\=null
priority\=3 proto\=TCP ip_src\=192.168.56.100 port_src\=80 ip_dst\=10.20.30.1
port_dst\=34568
mechanic\=IDS
```

В данном случае значение ключа **«msg»** в поле **«Extension»** представляет собой другое сообщение формата **«cef»**:

```
<14>CEF:0|armaif|Suricata|2.0|429496728|suricataalert|8|unixdate=1608
216259.676164
log_from=suricata cid=28775 gid=1 signature=429496728 rev=1 msg=test
classification=null
priority=3 proto=TCP ip_src=192.168.56.100 port_src=80 ip_dst=10.20.30.1
port_dst=34568 mechanic=IDS
```

8 СОБЫТИЯ

В настоящем разделе представлено описание раздела меню **«События»**, предусматривающего механизм просмотра событий от подключённых к **ARMA MC** источников.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Журналы»**, затем – подраздел **«События»** (см. Рисунок – Список событий).

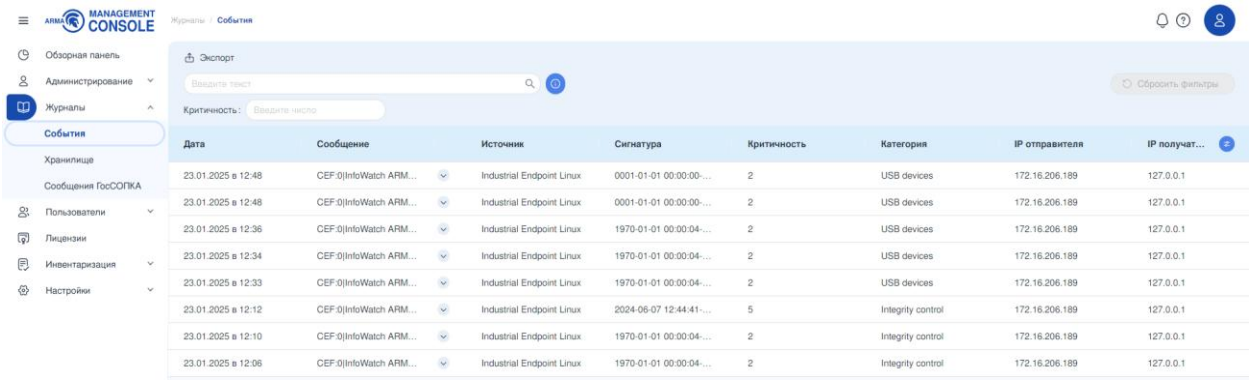


Рисунок – Список событий

Подраздел меню позволяет просматривать события в формате таблицы, состоящей из следующих столбцов:

- **«Дата»** – дата формирования события в **ARMA MC**;
- **«Сообщение»** – текст сообщения от источника в формате **«cef»**;
- **«Источник»** – источник, зафиксировавший событие;
- **«Сигнатура»** – образец, используемый для идентификации атаки в сети;
- **«Критичность»** – критичность события, определяется источником, возможные значения от 0 до 10;
- **«Категория»** – категория сигнатуры, модуль источника событий, отреагировавшего на пакет;
- **«IP отправителя»**;
- **«IP получателя»**.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

Порядок работы с информацией, представленной в формате таблицы описан в разделе «Форма раздела меню. Таблица» настоящего руководства.

Примечание:

Просмотр информации о каждом событии доступен через поле **«Поиск»** на панели инструментов.

8.1 Поиск и фильтрация

Блок фильтрации позволяет отфильтровать необходимые события и по умолчанию состоит из следующих полей (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **кнопка «Помощь по коррелятору»**;
- **«Критичность»**;
- **кнопка «Сбросить фильтры»**.

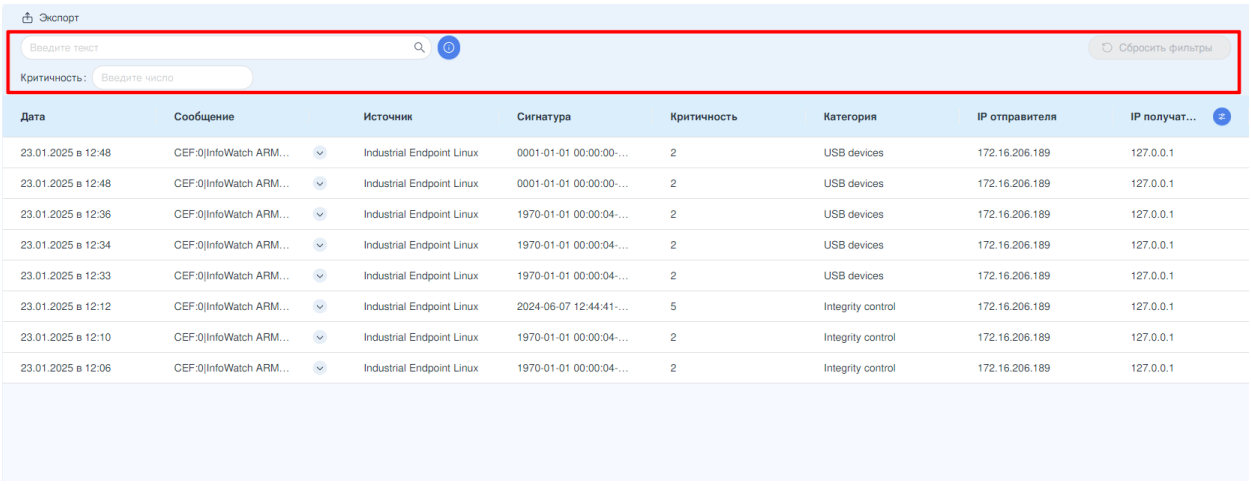


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по исходному cef-сообщению с использованием синтаксиса коррелятора. В качестве примера приведён поиск событий по категории сигнатуры, содержащей значение «control» (см. Рисунок – Помощь по коррелятору).

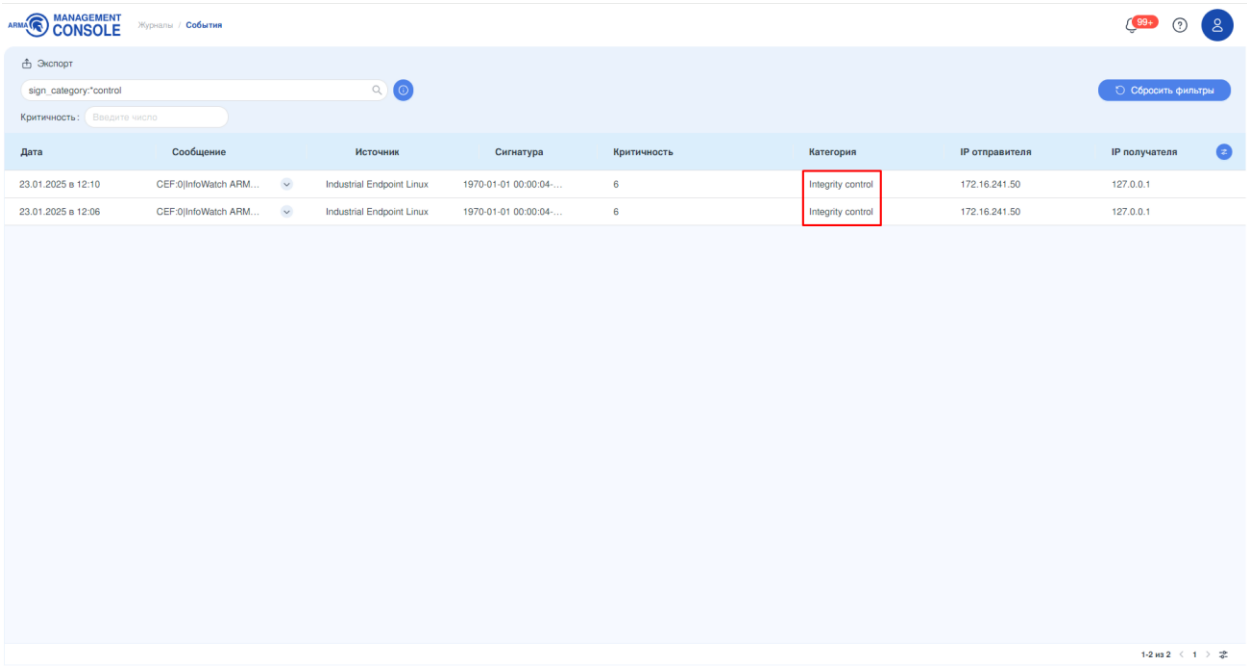


Рисунок – Блок фильтрации

Кнопка « » содержит рекомендации, упрощающие поиск необходимых событий, и открывает карточку **«Помощь по коррелятору»** с двумя вкладками – **«Синтаксис»** и **«Поля»** (см. Рисунок – Помощь по коррелятору). Вкладка **«Синтаксис»** содержит пояснения по именам полей и терминам, особым символам, диапазонам и логическим операторам. Вкладка **«Поля»** содержит описание полей и типа данных каждого поля.

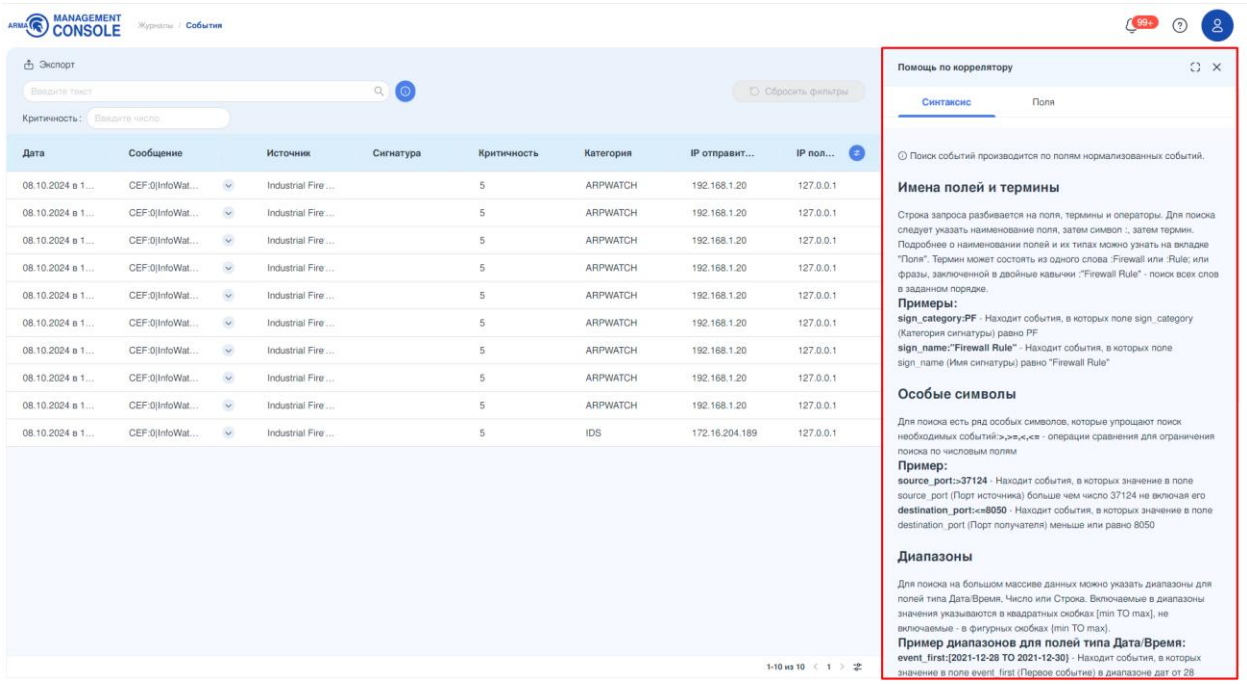


Рисунок – Помощь по коррелятору

Фильтрация по полю **«Критичность»** позволяет отфильтровать данные по критичности события.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

8.2 Просмотр подробной информации о событии

Для просмотра подробной информации о событии необходимо нажать на запись с событием, в результате будет отображена карточка **«Информация о событии [дата] в [время]»** (см. Рисунок – Информация о событии).

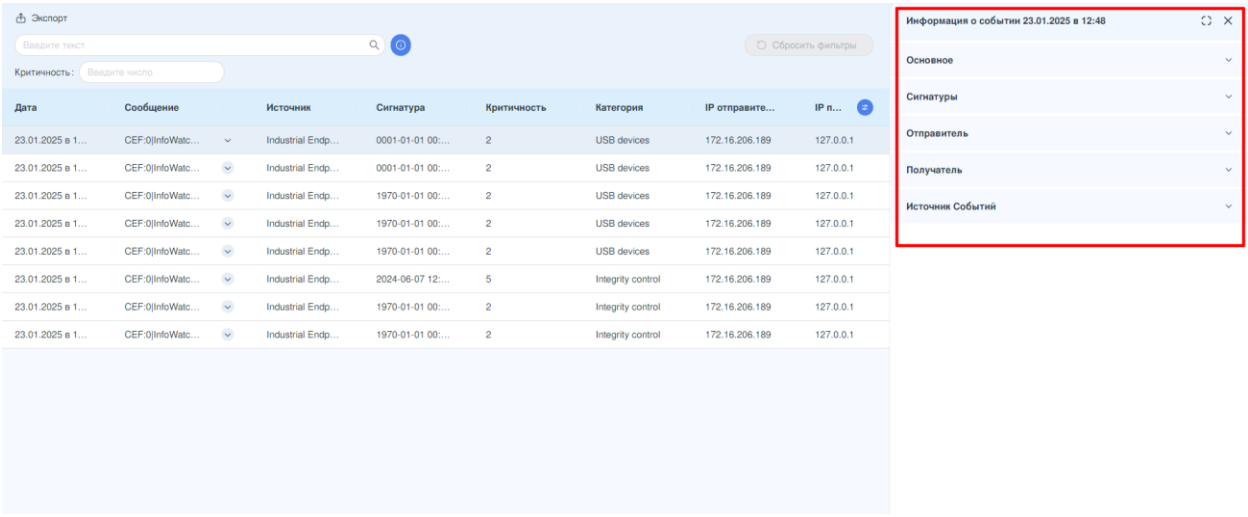


Рисунок – Информация о событии

Информация в карточке событий разбита на следующие блоки:

- **«Основное»**;
- **«Сигнатуры»**;
- **«Отправитель»**;
- **«Получатель»**;
- **«Источник события»**.

Блок **«Основное»** содержит информацию об ID события, дате и времени создания записи о событии, исходное сообщение в формате **«cef»**, критичность события, данные о первом и последнем срабатывании, суммарном количестве срабатываний, тип и протокол события, информацию о действии, которое предпринял источник события по отношению к сетевому пакету, а также тэги правил корреляции, которые сработали на сетевой пакет.

Блок **«Сигнатуры»** содержит информацию об ID, имени и категории сигнатуры.

Блок **«Отправитель»** содержит информацию об IP, порте, исходном хосте отправителя, а также об исходном пользователе.

Блок **«Получатель»** содержит информацию об IP, порте и целевом хосте получателя.

Блок **«Источник события»** содержит информацию о версии, модуле и производителе источника событий, отреагировавших на сетевой пакет.

> **Примечание**:
>
> Информация о событии может отличаться в зависимости от категории события.

8.3 Экспорт событий

Существует возможность локально сохранить таблицу событий. Для этого необходимо нажать кнопку **«Экспорт»** на панели инструментов. Формат экспортируемого файла – **«csv»**.

После успешного экспорта списка событий появится соответствующее уведомление (см. Рисунок – Успешный экспорт событий).

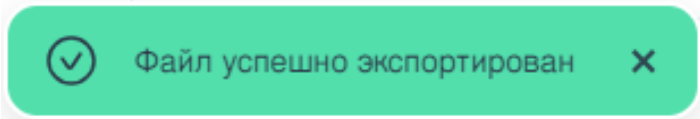


Рисунок – Успешный экспорт событий

9 ХРАНИЛИЩЕ

В настоящем разделе представлено описание подраздела меню **«Хранилище»**, предусматривающего механизм управления следующими архивами данных:

- архив ротированных событий в формате **«tar.gz»**;
- архив ротированных инцидентов в формате **«tar.gz»**;
- архив ротированных действий пользователей в формате **«tar.gz»**.

Для перехода в раздел меню на панели навигации необходимо выбрать раздел меню **«Журналы»**, затем – подраздел **«Хранилище»** (см. Рисунок – Хранилище).

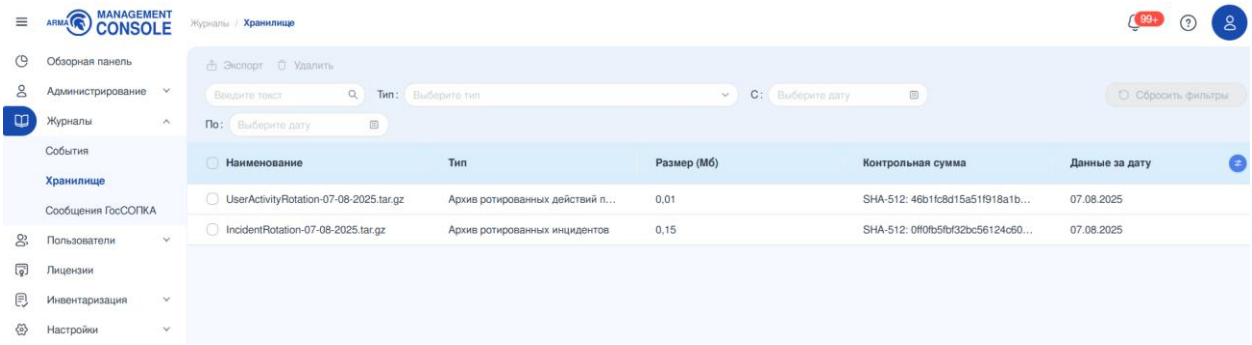


Рисунок – Хранилище

Раздел меню позволяет в табличном представлении просматривать, удалять и экспортировать архивы данных.

Порядок работы с информацией, представленной в формате таблицы, описан в разделе Форма раздела меню. Таблица настоящего руководства.

По умолчанию таблица содержит следующие столбцы:

- **«Наименование»** – имя файла архива;
- **«Тип»** – тип данных **«Архив ротированных событий»**, **«Архив ротированных инцидентов»** или **«Архив ротированных действий пользователей»**;
- **«Размер (Мб)»** – размер файла архива в мегабайтах;
- **«Контрольная сумма»** – контрольная сумма, рассчитанная при создании архива;
- **«Данные за дату»** – дата создания записей, добавленных в архив при ротации.

Примечание:

«Данные за дату» – имеется в виду дата добавления в систему исходных записей об инцидентах, событиях или действиях пользователей, и эта дата будет отличаться от даты создания файла архива в момент ротации, так

как записи добавляются по факту в течение дня, а архив создаётся в 00:00 дня, удовлетворяющего условиям ротации (подробнее о ротации см. Настройки ротации настоящего руководства).

9.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать архивы по всем столбцам списка и по умолчанию состоит из следующих полей (см. Рисунок – Поиск и фильтрация):

- поле **«Поиск»** позволяет отфильтровать записи путем сквозного поиска по столбцам **«Наименование»** и **«Тип»**;
- **«Тип»** осуществляет фильтрацию по типу архивированных данных путем выбора из выпадающего списка элементов: **«Архив ротированных событий»**, **«Архив ротированных инцидентов»** и/или **«Архив ротированных действий пользователей»**;
- **«С»** позволяет отфильтровать архивы по дате и задаёт начальную дату диапазона;
- **«По»** позволяет отфильтровать архивы по дате и задаёт конечную дату диапазона;
- кнопка **«Сбросить фильтры»** сбрасывает все установленные фильтры.

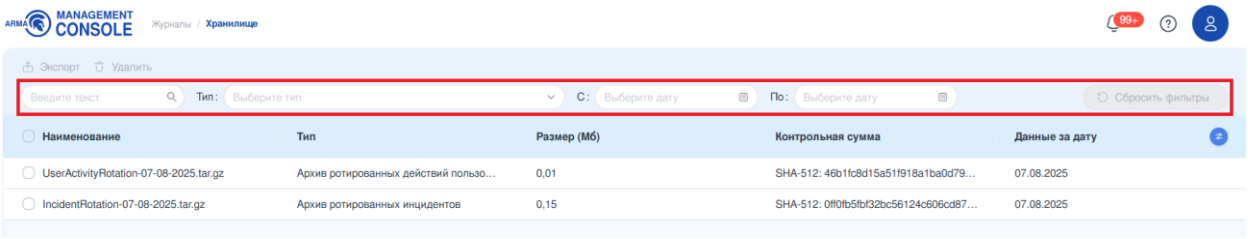


Рисунок – Поиск и фильтрация

9.2 Экспорт и удаление архива

Для экспорта архива необходимо выполнить следующие действия:

1. Выбрать архив или архивы, установив флажок рядом с названием архива.
2. Нажать кнопку **«Экспорт»**.

При успешном экспорте архива появится соответствующее уведомление (см. Рисунок – Успешный экспорт архива).

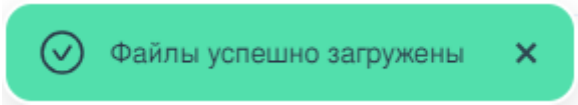


Рисунок – Успешный экспорт архива

Для удаления архива необходимо выполнить следующие действия:

1. Выбрать архив или архивы, установив флажок рядом с названием архива.
2. Нажать кнопку **«Удалить»**.
3. Подтвердить удаление, нажав на кнопку **«Удалить»** в открывшейся форме.

При успешном удалении архива появится соответствующее уведомление (см. Рисунок – Успешное удаление архива).

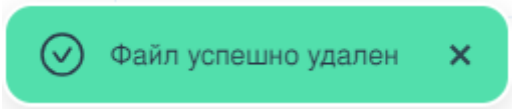


Рисунок – Успешное удаление архива

Примечание:

В целях предотвращения потери данных, рекомендуется использовать стороннее ПО для перемещения архивов на внешние устройства хранения.

9.3 Нехватка места на диске и автоматическая очистка

В **ARMA MC** реализован механизм определения свободного места на основном диске. Если свободно менее **«5%»** от общего объема диска, запускается процесс автоматического удаления данных.

В первую очередь удаляются системные журналы, не оказывающие влияния на работу системы. Если этого недостаточно, очищается директория с файлами обновлений. Если и этого недостаточно, то будут удаляться архивы ротированных событий, инцидентов и действий пользователей, начиная с самых старых.

По достижении допустимого объема свободного места (**«7,5%»** и более) процесс удаления завершается, а в раздел уведомлений (см. Уведомления настоящего руководства) добавляется сообщение с заголовком **«Экстренная очистка дискового пространства произошла успешно»**.

Если после удаления всех вышеперечисленных данных объем свободного места составляет менее **«5%»**, выводится баннер (см. Рисунок – Автоматическая очистка невозможна), а в раздел уведомлений добавляется сообщение с заголовком: **«Экстренная очистка дискового пространства не выполнена»**.

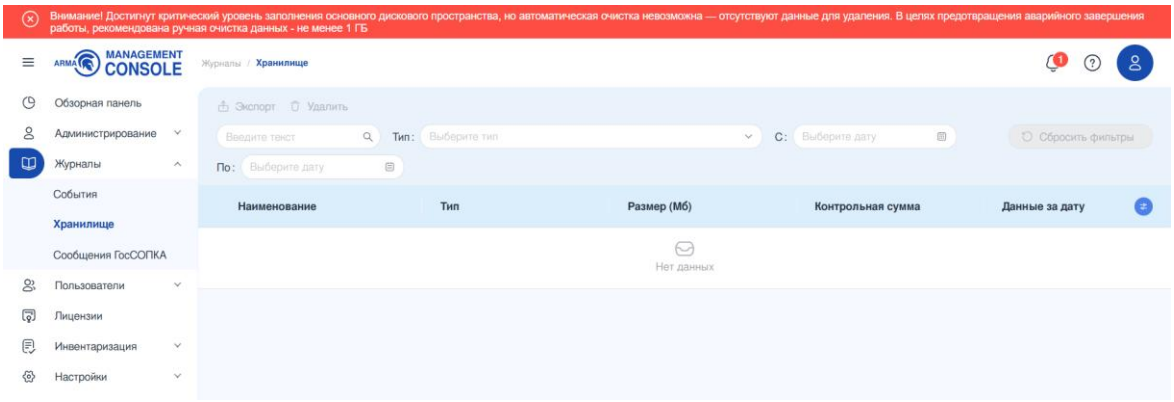


Рисунок – Автоматическая очистка невозможна

Примечание:

Если место на диске занято данными, не имеющими отношение к работе **ARMA MC**, рекомендуется как можно скорее удалить эти данные средствами ОС.

10 ГОССОПКА

В настоящем разделе меню представлено описание подраздела меню **«Организация»**, предусматривающего механизм управления следующими функциями:

- управление карточкой организации в НКЦКИ;
- переход в личный кабинет НКЦИКИ;
- обмен сообщениями с системой ГосСОПКА.

Корпоративный центр ГосСОПКА автоматизирует выявление инцидентов, реагирование на них и взаимодействие с НКЦКИ. Подраздел меню **«Организация»** позволяет информировать НКЦКИ о произошедших инцидентах.

Подраздел меню реализован в рамках исполнения следующих приказов:

- ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 года;
- ФСБ РФ № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» от 19.06.2019 года.

10.1 Карточка организации

Карточка организации отображает информацию об организации, необходимую для отправки уведомлений в НКЦКИ.

Для перехода к карточке организации на панели навигации необходимо выбрать раздел **«Настройки»**, затем подраздел **«Организация»** (см. Рисунок – Карточка организации).

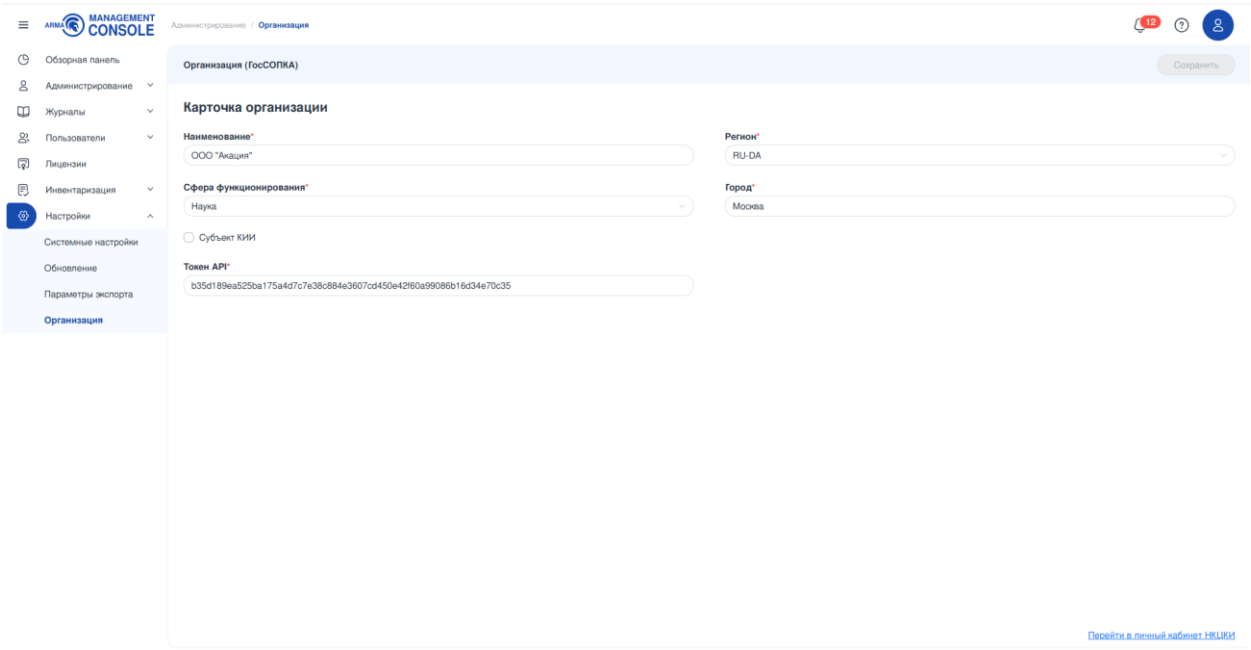


Рисунок – Карточка организации

Для заполнения карточки организации необходимо выполнить следующие действия:

1. Ввести название организации в поле **«Наименование»**.
2. Выбрать необходимое значение из выпадающего списка параметра **«Сфера функционирования»**:
   - «Атомная энергетика»;
   - «Банковская сфера и иные сферы финансового рынка»;
   - «Горнодобывающая промышленность»;
   - «Государственная/муниципальная власть»;
   - «Здравоохранение»;
   - «Металлургическая промышленность»;
   - «Наука»;
   - «Оборонная промышленность»;
   - «Образование»;
   - «Ракетно-космическая промышленность»;
   - «Связь»;
   - «СМИ»;
   - «Топливно-энергетический комплекс»;
   - «Транспорт»;

- «Химическая промышленность»;
- «Иная».

3. Если компания является субъектом КИИ, установить флажок в чек-бокс **«Субъект КИИ»**.
4. Выбрать необходимое значение из выпадающего списка параметра **«Регион»** (см. Справочник по регионам настоящего руководства).
5. Ввести название города в поле **«Город»**.
6. Нажать кнопку **«Перейти в личный кабинет НКЦКИ»** в правом нижнем углу экрана.
7. В открывшемся окне авторизации ввести логин и пароль организации для входа в личный кабинет НКЦКИ.
8. После авторизации в личном кабинете НКЦКИ перейти в пункт **«Настройки»**, скопировать значение поля **«Токен API»**.
9. Вернуться в **ARMA MC**, скопировать значение из предыдущего пункта в поле **«Токен API»**.
10. Нажать кнопку **«Сохранить»**.

В случае изменения данных об организации и последующем их редактировании необходимо в пункте **«Карточка организации»** выполнить следующие действия:

1. Отредактировать необходимую информацию об организации.
2. Нажать кнопку **«Сохранить»**.

10.2 Работа с уведомлениями

10.2.1 Отправка уведомления об инциденте в НКЦКИ

Для отправки уведомления об инциденте в НКЦКИ необходимо выполнить следующие действия:

1. Перейти в подраздел меню **«Инциденты»** (см. Инциденты настоящего руководства).
2. Выбрать необходимый инцидент и открыть его карточку в полноэкранном режиме (см. Работа с карточками настоящего руководства).
3. Нажать кнопку **«Отправить в ГосСОПКА»** в правом верхнем углу экрана (см. Рисунок – Отправить в ГосСОПКА).

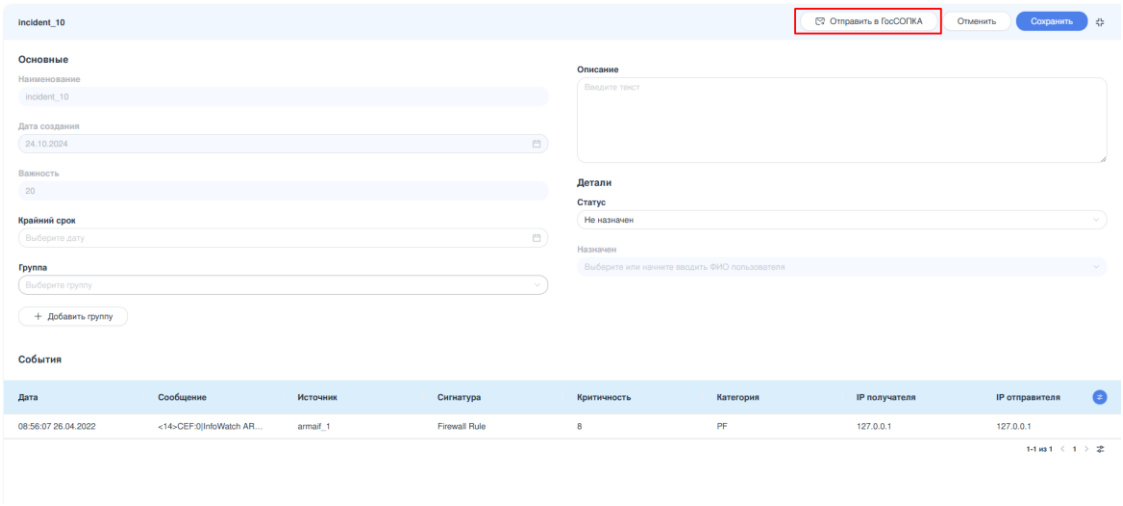


Рисунок – Отправить в ГосСОПКА

В случае уже отправленного инцидента в ГосСОПКА, кнопка будет иметь название **«Показать уведомление»**. При нажатии на кнопку откроется карточка уведомления в ГосСОПКА.

4. В открывшейся карточке **«Уведомление в ГосСОПКА»** выбрать категорию инцидента из выпадающего списка **«Категория»** (см. Рисунок – Выбор категории):

   - «Уведомление о компьютерном инциденте»;
   - «Уведомление о компьютерной атаке».

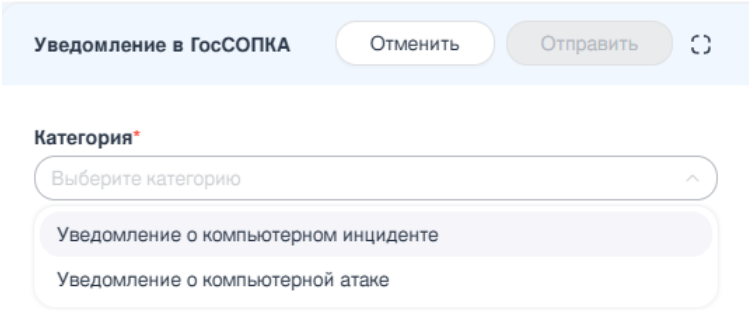


Рисунок – Выбор категории

5. Заполнить все необходимые поля карточки, при необходимости установить флажки в чек-боксы и нажать кнопку **«Отправить»** (см. Рисунок – Заполнение карточки).

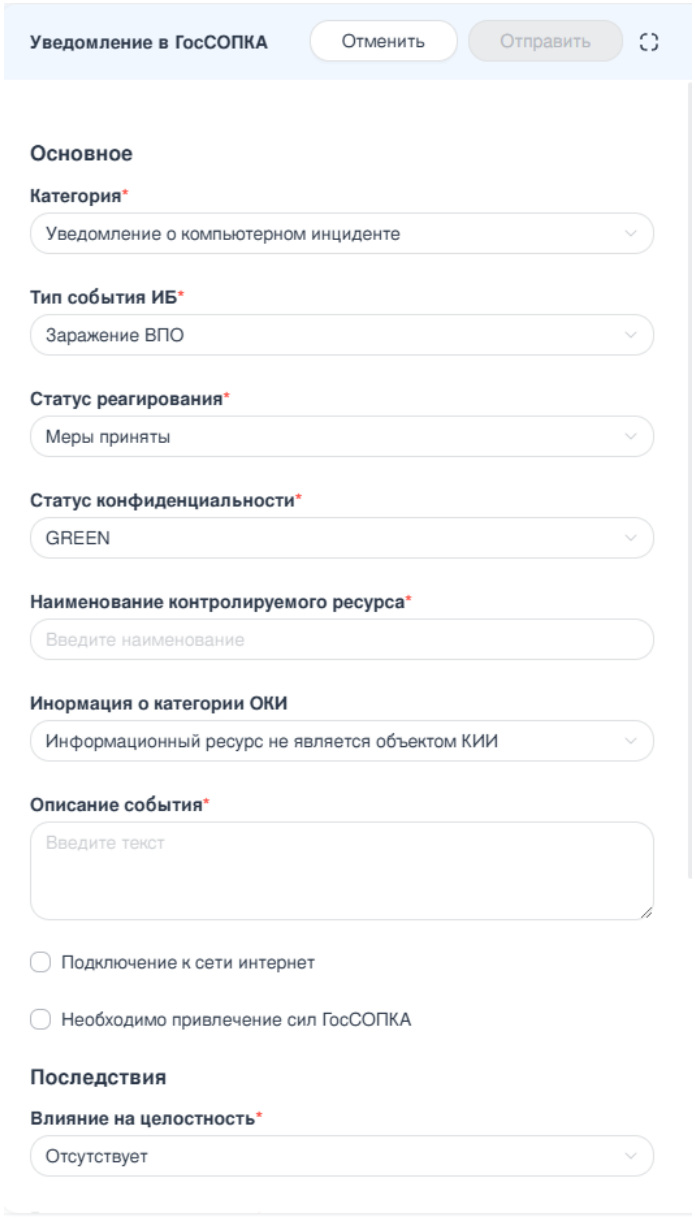


Рисунок – Заполнение карточки

10.2.2 Сообщения от НКЦКИ

Для просмотра уведомлений от НКЦКИ необходимо на панели навигации выбрать раздел **«Журналы»**, затем подраздел **«Сообщения ГосСОПКА»** (см. Рисунок – Сообщения).

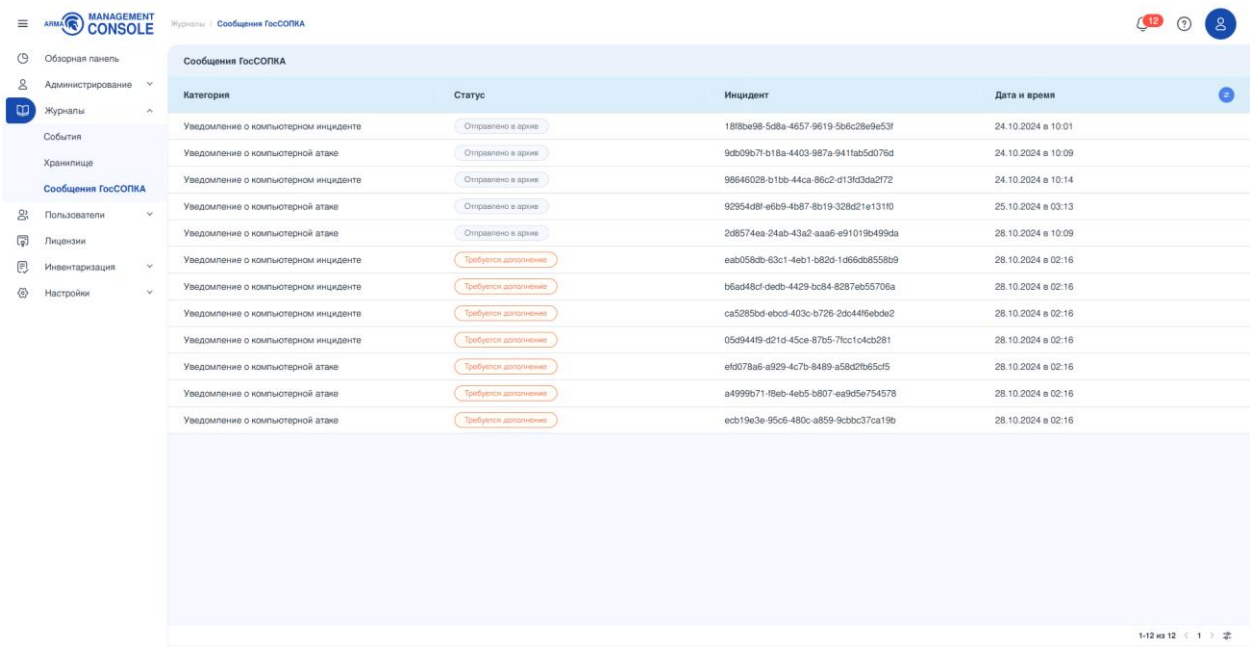


Рисунок – Сообщения

Сообщения отображаются в формате таблицы с указанием категории, текущего статуса, даты и времени отправки сообщения, а также идентификатора инцидента.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

При нажатии на строку с уведомлением откроется карточка **«Уведомление о компьютерном инциденте»**, в которой существует возможность вести переписку с сотрудниками НКЦКИ. Для этого необходимо ввести текст сообщения в поле ввода **«Введите текст»** и нажать кнопку **«Отправить»** (см. Рисунок – Уведомления).

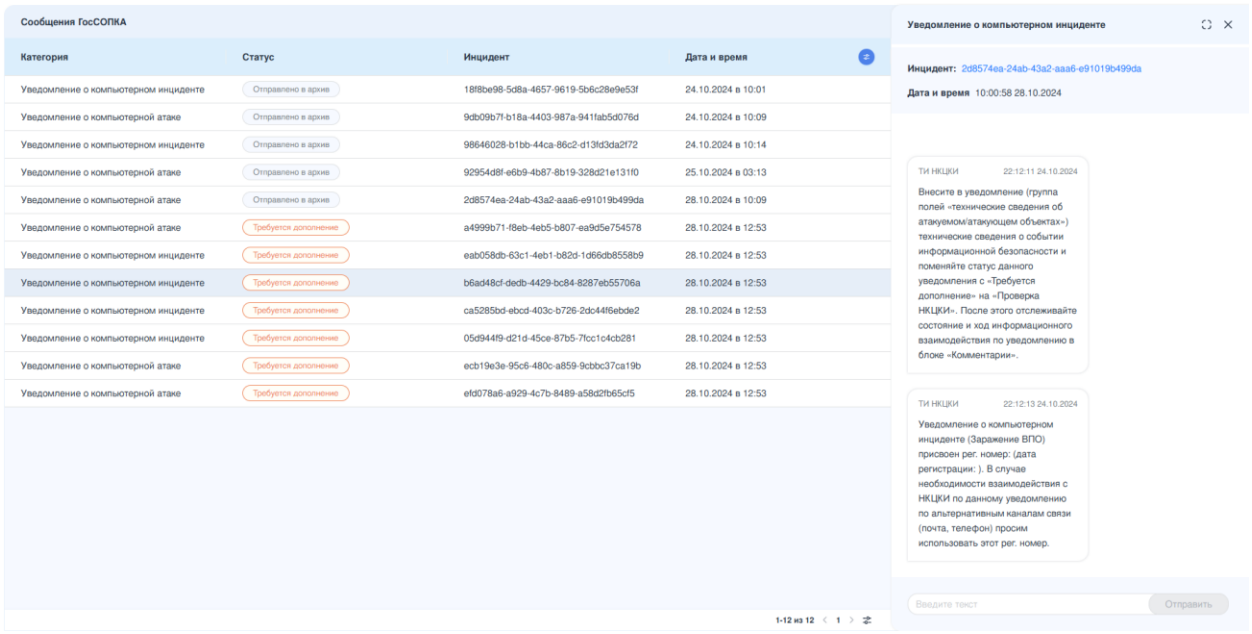


Рисунок – Уведомления

При нажатии на ссылку идентификационного номера инцидента (см. Рисунок – Ссылка на инцидент) произойдёт открытие его карточки в подразделе меню **«Инциденты»**.

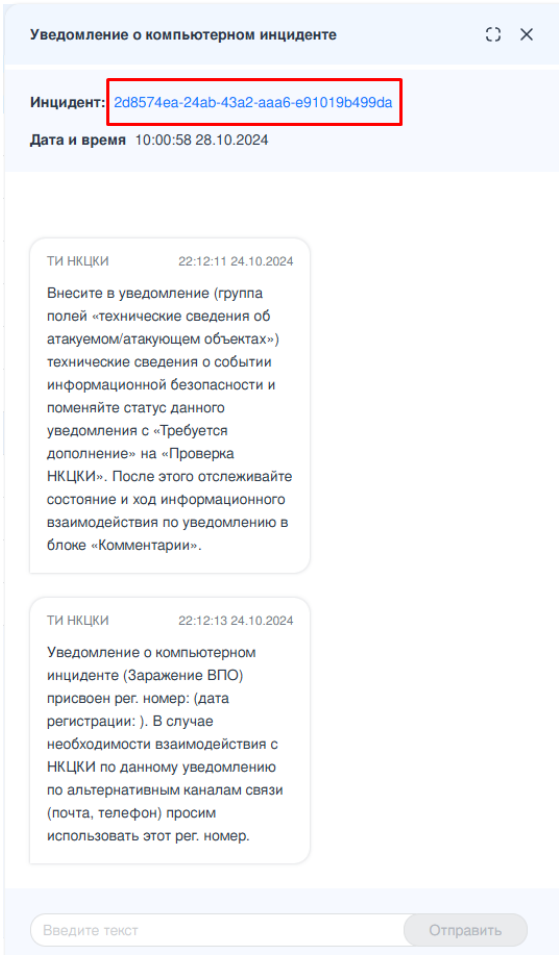


Рисунок – Ссылка на инцидент

10.3 Справочник по регионам

Таблица «Справочник по регионам»

Сокращение	Значение
RU-KK	Республика Хакасия
RU-KO	Республика Коми
RU-ME	Республика Марий Эл
RU-MO	Республика Мордовия
RU-SA	Республика Саха (Якутия)
RU-SE	Республика Северная Осетия – Алания
RU-TA	Республика Татарстан (Татарстан)
RU-TY	Республика Тыва

RU-UD	Удмуртская Республика
RU-ALT	Алтайский край
RU-KAM	Камчатский край
RU-KHA	Хабаровский край
RU-KDA	Краснодарский край
RU-KYA	Красноярский край
RU-PER	Пермский край
RU-PRI	Приморский край
RU-STA	Ставропольский край
RU-ZAB	Забайкальский край
RU-AMU	Амурская область
RU-ARK	Архангельская область
RU-AST	Астраханская область
RU-BEL	Белгородская область
RU-BRY	Брянская область
RU-CHE	Челябинская область
RU-IRK	Иркутская область
RU-IVA	Ивановская область
RU-KGD	Калининградская область
RU-KLU	Калужская область
RU-KEM	Кемеровская область – Кузбасс
RU-KIR	Кировская область
RU-KOS	Костромская область
RU-KGN	Курганская область
RU-KRS	Курская область
RU-LEN	Ленинградская область
RU-LIP	Липецкая область
RU-MAG	Магаданская область
RU-MOS	Московская область
RU-MUR	Мурманская область

RU-NIZ	Нижегородская область
RU-NGR	Новгородская область
RU-NVS	Новосибирская область
RU-OMS	Омская область
RU-ORE	Оренбургская область
RU-ORL	Орловская область
RU-PNZ	Пензенская область
RU-PSK	Псковская область
RU-ROS	Ростовская область
RU-RYA	Рязанская область
RU-SAK	Сахалинская область
RU-SAM	Самарская область
RU-SAR	Саратовская область
RU-SMO	Смоленская область
RU-SVE	Свердловская область
RU-TAM	Тамбовская область
RU-TOM	Томская область
RU-TUL	Тульская область
RU-TVE	Тверская область
RU-TYU	Тюменская область
RU-ULY	Ульяновская область
RU-VLA	Владимирская область
RU-VGG	Волгоградская область
RU-VLG	Вологодская область
RU-VOR	Воронежская область
RU-YAR	Ярославская область
RU-MOW	Москва
RU-SPE	Санкт-Петербург
RU-YEV	Еврейская автономная область
RU-CHU	Чукотский автономный округ

RU-KHM	Ханты-Мансийский автономный округ – Югра
RU-NEN	Ненецкий автономный округ
RU-YAN	Ямало-Ненецкий автономный округ

11 ПОЛЬЗОВАТЕЛИ

В настоящем разделе представлено описание раздела меню **«Пользователи»**, предусматривающее механизм управления следующими функциями:

- профиль пользователя;
- список пользователей;
- действия пользователей.

Для выхода из активной пользовательской сессии необходимо нажать кнопку « », затем нажать кнопку **«Выход»**.

Примечание:

Через 15 минут бездействия осуществляется прекращение сеанса работы в **ARMA MC** текущей УЗ. При этом если под одной учетной записью работает несколько пользователей, то через 15 минут бездействия первого пользователя, залогинившегося под данной УЗ, произойдёт прекращение сеанса для всех пользователей, использующих эту УЗ.

Рекомендуется создавать отдельную учётную запись для каждого пользователя в системе.

11.1 Профиль текущего пользователя

Раздел меню **«Управление профилем»** позволяет просматривать подробную информацию об УЗ текущего пользователя (см. Рисунок – Профиль пользователя).

Для перехода в раздел меню необходимо нажать кнопку « » и пройти по ссылке **«Управление профилем»**.

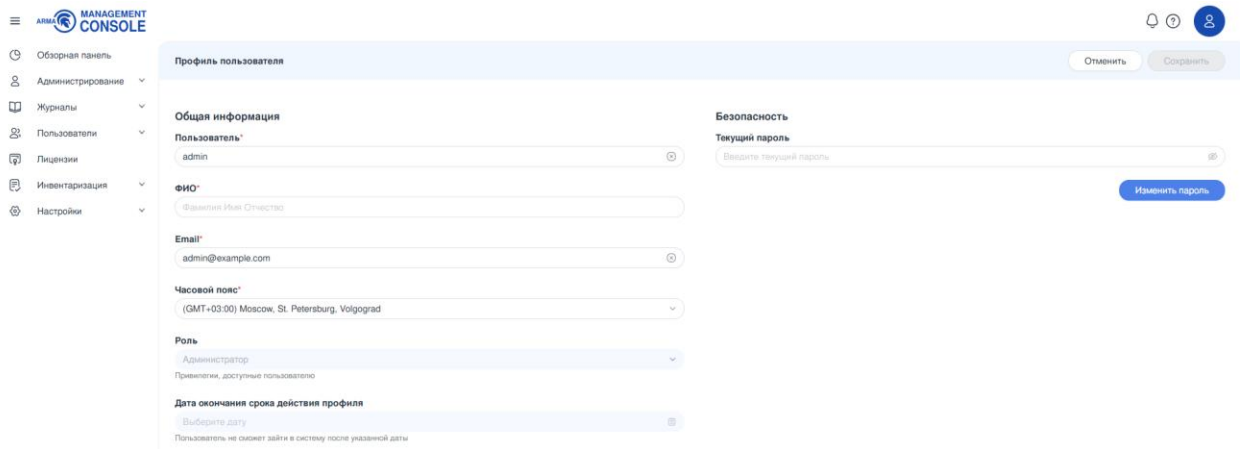


Рисунок – Профиль пользователя

11.1.1 Изменение общей информации УЗ

Для изменения информации профиля пользователя необходимо выполнить следующие действия:

1. Отредактировать информацию профиля. Для редактирования доступны поля **«Пользователь», «ФИО», «Email», «Часовой пояс», «Текущий пароль»**.
2. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки **«Профиль пользователя»**.

В случае успеха в левом нижнем углу экрана появится соответствующее уведомление (см. Рисунок – Пользователь обновлён).

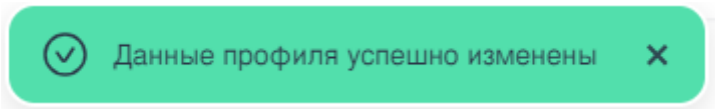


Рисунок – Пользователь обновлён

Примечание:

Для первоначальной УЗ с ролью администратор необходимо отредактировать информацию профиля, заполнив поле **«ФИО»**, для корректного отображения действий пользователя в разделе меню **«Действия»**.

11.1.2 Смена пароля УЗ

Для смены пароля текущего пользователя необходимо выполнить следующие действия:

1. Нажать кнопку **«Изменить пароль»**.
2. В поле **«Текущий пароль»** ввести действующий пароль.
3. В поле **«Новый пароль»** ввести новый пароль.

Примечание:

Предъявляются следующие требования к сложности пароля:

- разрешено использование только латиницы;
- должен содержать как минимум одну цифру;
- должен содержать как минимум одну букву в верхнем регистре;
- должен содержать как минимум одну букву в нижнем регистре;
- должен содержать как минимум один спецсимвол;
- пароль может содержать от 8-ми до 32-х символов;

- новый пароль не может совпадать с текущим паролем.

4. В поле **«Повторить пароль»** ввести пароль, идентичный введённому в поле **«Новый пароль»**.
5. Нажать кнопку **«Изменить пароль»**.
6. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки **«Профиль пользователя»**.

11.2 Список

Подраздел меню **«Список»** отображает все УЗ, зарегистрированные в **ARMA MC**. Для перехода в подраздел на панели навигации необходимо выбрать в разделе меню **«Пользователи»** подраздел **«Список»** (см. Рисунок – Список пользователей).

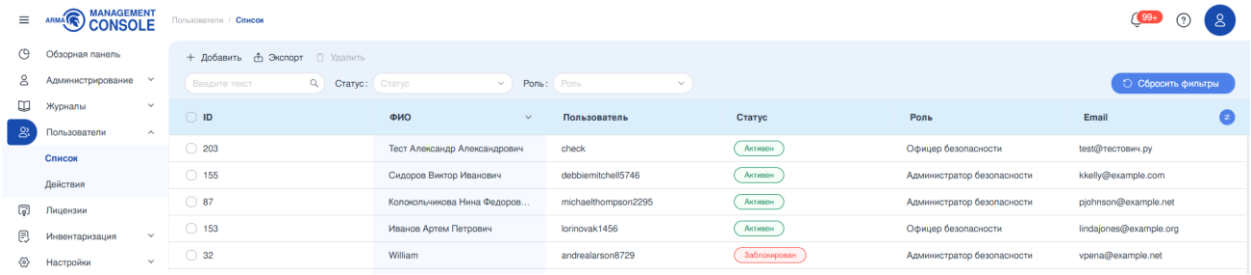


Рисунок – Список пользователей

Информация о зарегистрированных в **ARMA MC** пользователях представлена в формате таблицы, состоящей из следующих столбцов:

- **«ID»** – идентификатор пользователя. Генерируется в момент создания пользователя автоматически;
- **«ФИО»** – фамилия, имя и отчество пользователя;
- **«Пользователь»** – логин пользователя;
- **«Статус»** – статус пользователя («Активен»/«Заблокирован»);
- **«Роль»** – роль пользователя в **ARMA MC**;
- **«Email»** – email пользователя;
- **«Дата окончания»** – дата блокировки УЗ.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются столбцы **«ID»**, **«ФИО»**, **«Пользователь»**, **«Статус»**, **«Роль»**, **«Email»**. Столбец **«Дата окончания»** скрыт.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

11.2.1 Управление УЗ

Параметры УЗ доступны для просмотра и изменения в форме карточки пользователя, которая открывается при выборе УЗ в списке (см. Рисунок – Просмотр УЗ).

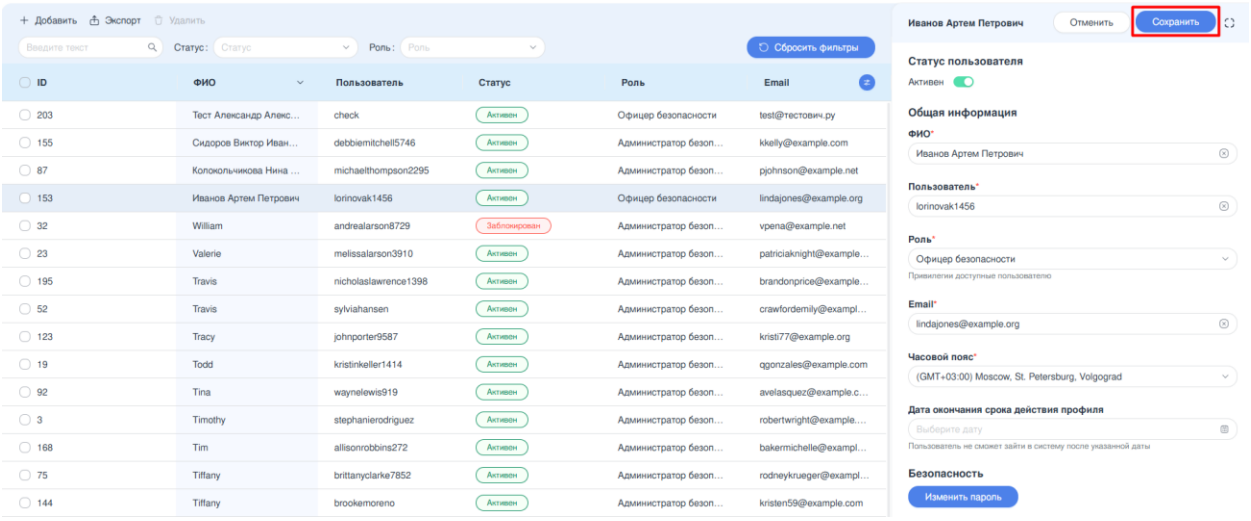


Рисунок – Карточка пользователя

Чтобы изменить один или несколько параметров УЗ, достаточно внести изменения в карточку пользователя и нажать кнопку **«Сохранить»** в правом верхнем углу.

> **Примечание**:
>
> В карточке пользователя можно разблокировать пользователя, заблокированного по любой причине, нажав на переключатель **«Активен»** (см. Рисунок – Просмотр УЗ). Изменения применятся после нажатия на кнопку **«Сохранить»**.

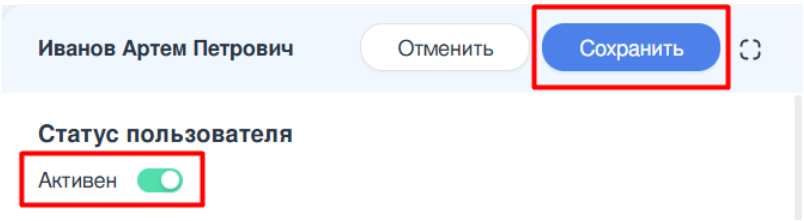


Рисунок – Снятие блокировки пользователя

11.2.2 Поиск и фильтрация

Блок фильтрации на панели инструментов позволяет фильтровать записи по всем столбцам списка и состоит из следующих элементов (см. Рисунок – Блок фильтрации):

- поле **«Поиск»**;
- поле **«Статус»**;
- поле **«Роль»**;

- кнопка **«Сбросить фильтры»**.

Если кнопка **«Сбросить фильтры»** неактивна, она становится активной при применении фильтрации в поле **«Поиск»**, **«Статус»** или **«Роль»**.

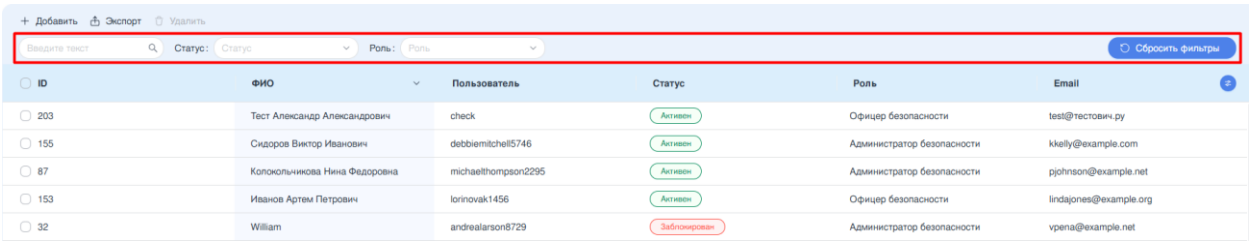


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем доступным столбцам таблицы.

Фильтрация по полю **«Роль»** позволяет отфильтровать данные по роли сотрудника в **ARMA MC**. Поле **«Роль»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Администратор безопасности»**;
- **«Офицер безопасности»**.

11.2.3 Добавление пользователя

Для создания новой УЗ необходимо выполнить следующие действия:

1. Нажать кнопку **«Добавить»** на панели инструментов.
2. В открывшейся карточке **«Добавление пользователя»** заполнить поля (см. Рисунок – Пример заполнения карточки пользователя):
   - **«Статус пользователя»**. Выбрать одно из двух значений статуса пользователя. Значение по умолчанию **«Активен»** позволяет пользователю использовать **ARMA MC**, значение **«Заблокирован»** блокирует УЗ, пользователь не может войти в **ARMA MC**.
   - **«ФИО»**. Ввести фамилию, имя и отчество пользователя.

     Примечание:

     Предъявляются следующие требования к полю **«ФИО»**:

     - разрешено использование кириллицы или латиницы;
     - разрешено использование пробелов;
     - поле не может содержать более 64-х символов.

   - **«Пользователь»**. Ввести уникальный логин пользователя. В **ARMA MC** не допускается создание двух и более УЗ с одним логином.

Примечание:

Предъявляются следующие требования к полю **«Пользователь»**:

- разрешено использование только латиницы;
- разрешено использование букв, цифр;
- запрещено использование пробела;
- поле не может содержать более 32-х символов.

- **«Роль»**. Выбрать одно из значений в выпадающем списке **«Роль»**. В **ARMA MC** доступны две роли – **«Администратор безопасности»** и **«Офицер безопасности»**. Доступные пользователю привилегии описаны в Руководстве администратора **ARMA MC** (Пользовательские роли).
- **«Email»**. Ввести уникальный email пользователя. В **ARMA MC** не допускается создание двух и более УЗ с одним email.
- **«Часовой пояс»**. Выбрать одно из значений в выпадающем списке **«Часовой пояс»**. Часовой пояс по умолчанию **GMT+3**.
- **«Дата окончания»**. Данное поле позволяет установить срок действия УЗ и не является обязательным к заполнению. После указанной в поле даты пользователь не сможет зайти в **ARMA MC**, его УЗ будет заблокирована.
- **«Пароль»**. Ввести пароль, по которому новый пользователь будет осуществлять вход в **ARMA MC**. Требования к сложности пароля описаны в разделе Смена пароля УЗ настоящего руководства.
- **«Повторить пароль»**. Повторить введённый пароль.

3. Нажать кнопку **«Сохранить»** в верхней части карточки **«Добавление пользователя»**.

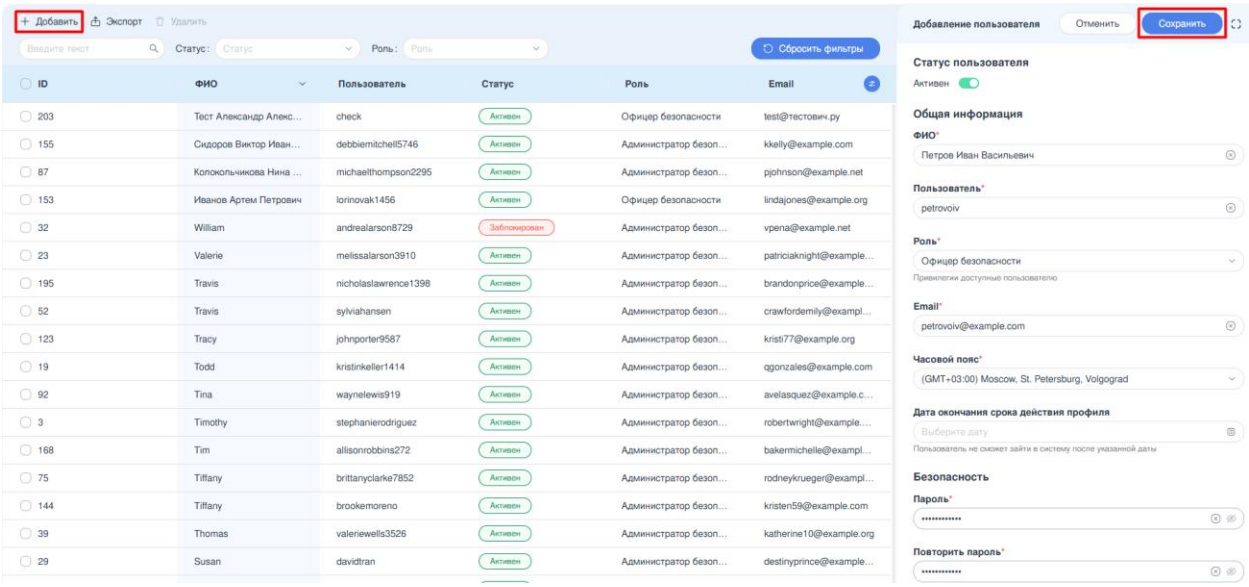


Рисунок – Пример заполнения карточки пользователя

В случае успеха в левой нижней части экрана появится соответствующее уведомление (см. Рисунок – Уведомление о добавлении пользователя).

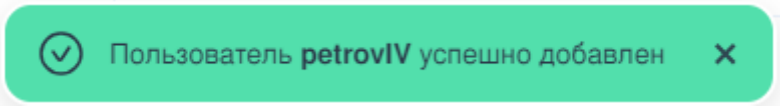


Рисунок – Уведомление о добавлении пользователя

11.2.4 Изменение информации в карточке пользователя

Для изменения информации в УЗ необходимо выполнить следующие действия:

1. Выбрать из списка пользователей необходимую УЗ.
2. В карточке пользователя отредактировать необходимую информацию профиля.
3. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки **«Профиль пользователя»**.

В случае успеха в левой нижней части экрана появится соответствующее уведомление (см. Рисунок – Уведомление об обновлении информации).

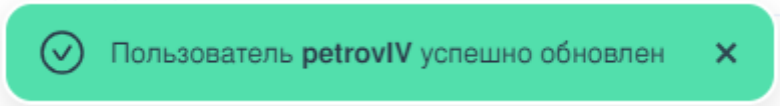


Рисунок – Уведомление об обновлении информации

11.2.5 Блокировка пользователя

Для блокировки УЗ необходимо выполнить следующие действия:

1. Выбрать из списка пользователей необходимую УЗ.

2. В карточке пользователя перевести переключатель **«Статус пользователя»** в положение **«Заблокирован»** (см. Рисунок – Статус пользователя: заблокирован).
3. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки пользователя.

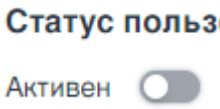


Рисунок – Статус пользователя: заблокирован

В случае успеха в левой нижней части экрана появится соответствующее уведомление (см. Рисунок – Уведомление о блокировке пользователя).

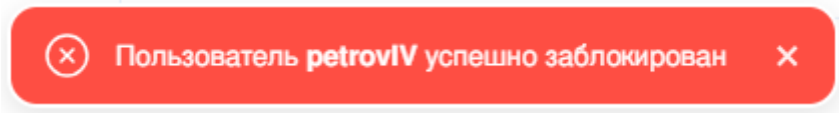


Рисунок – Уведомление о блокировке пользователя

11.2.6 Удаление пользователя

Для удаления одной или нескольких существующих УЗ необходимо выполнить следующие действия:

1. Установить флажок в чек-бокс, расположенный слева от ID пользователя или пользователей, которых необходимо удалить.
2. Нажать кнопку **«Удалить»** на панели инструментов.
3. В появившемся окне необходимо подтвердить удаление, нажав кнопку **«Удалить»** (см. Рисунок – Удаление пользователей). Текст подтверждения может незначительно отличаться в зависимости от количества удаляемых пользователей и наличия назначенных на них нерешённых инцидентов.

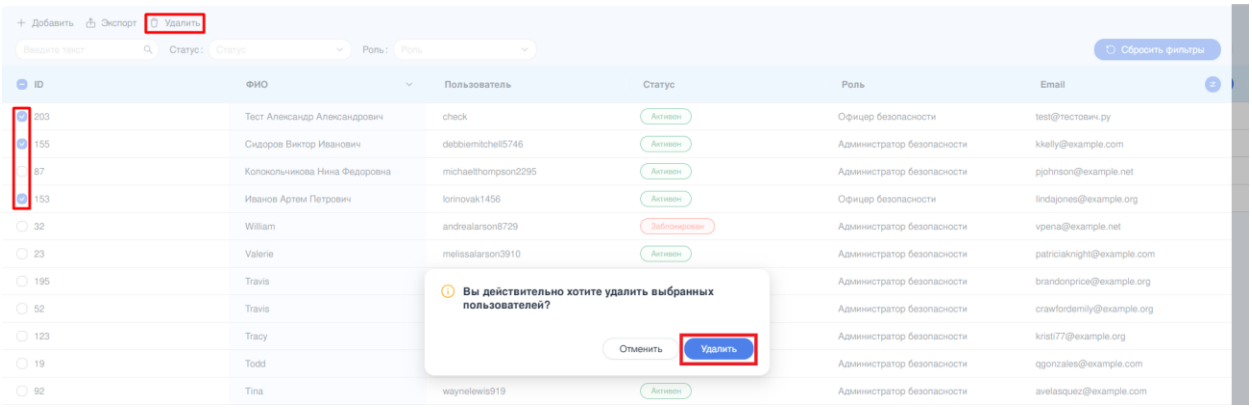


Рисунок – Удаление пользователей

В случае успеха в левой нижней части экрана появится соответствующее уведомление (см. Рисунок – Уведомление об удалении пользователей).

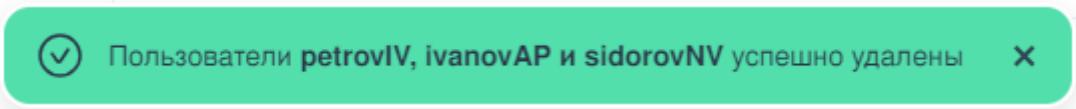


Рисунок – Уведомление об удалении пользователей

11.2.7 Экспорт

Подраздел меню **«Действия»** позволяет экспортировать список действий пользователей в формате таблицы. Для экспорта списка действий необходимо нажать кнопку **«Экспорт»** на панели инструментов.

Экспортированный файл формата **«CSV»** будет содержать следующий список значений:

- **«ID»**;
- **«ФИО»**;
- **«Пользователь»**;
- **«Статус»**;
- **«Роль»**;
- **«Email»**.

11.3 Действия

Подраздел меню **«Действия»** отображает произведённые пользователями действия в **ARMA MC**. Для перехода в подраздел на панели навигации необходимо выбрать в разделе меню **«Пользователи»** подраздел **«Действия»** (см. Рисунок – Действия).

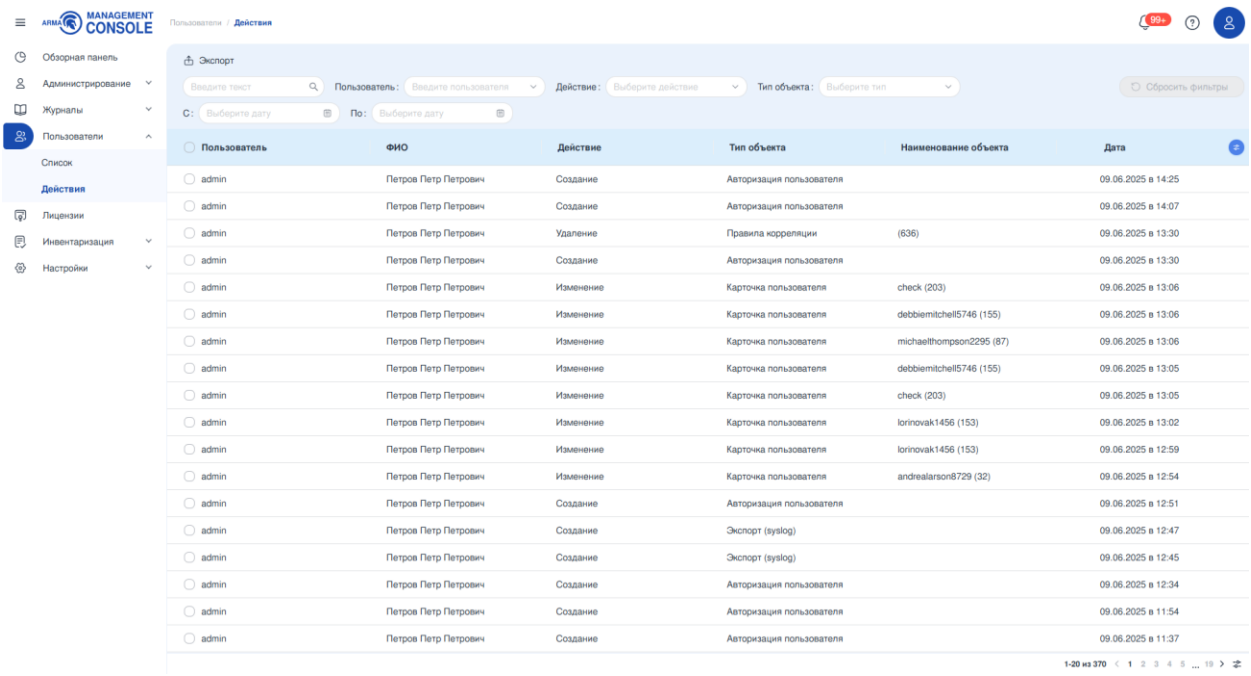


Рисунок – Действия

Подраздел меню **«Действия»** позволяет просматривать список действий пользователей в формате таблицы. Информация о каждом действии представлена в следующих столбцах таблицы:

- **«Пользователь»** – логин пользователя, совершившего действие;
- **«ФИО»** – фамилия, имя и отчество пользователя, совершившего действие;
- **«Действие»** – конкретное действие, совершённое пользователем («Создание»/«Изменение»/«Удаление»);
- **«Тип объекта»** – тип объекта, в котором произошло изменение (например, **«NGFW»**);
- **«Наименование объекта»** – наименование объекта, в котором произошло изменение;
- **«Дата»** – дата и время произведённого действия.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

11.3.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать записи по всем столбцам списка и по умолчанию состоит из следующих полей (см. Рисунок – Блок фильтрации).

- **«Поиск»**;
- **«Пользователь»**;
- **«Действие»**;
- **«Тип объекта»**;
- **«С»**;
- **«По»**.

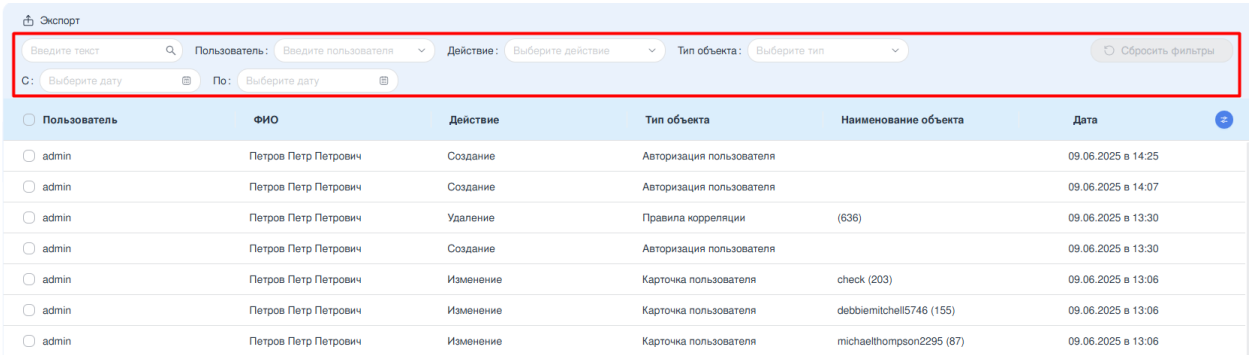


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам **«Пользователь»**, **«ФИО»** и **«Наименование объекта»**.

Фильтрация по полю **«Пользователь»** позволяет отфильтровать данные по логину или ФИО пользователя. Для корректного формирования запроса при заполнении поисковой строки предоставляются подсказки быстрого заполнения с вариантом выбора.

Фильтрация по полю **«Действие»** позволяет отфильтровать данные по типу действия, совершённого пользователем. Поле **«Действие»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений: «Создание», «Изменение», «Удаление».

Фильтрация по полю **«Тип объекта»** позволяет отфильтровать данные по типу объекта, над которым было совершено действие. Поле **«Тип объекта»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Активы»**;
- **«Группы активов»**;
- **«Источник «IFW»**;
- **«Источник «IEW»**;
- **«Источник «IEL»**;
- **«Источник «NGFW»**;
- **«Источник «Внешний источник»**;
- **«Группы источников событий»**;
- **«Источник событий»**;
- **«Карточка организации»**;
- **«Правила корреляции»**;
- **«Категория правил корреляции»**;
- **«Инциденты»**;
- **«Группы инцидентов»**;
- **«Экспорт (syslog)»**;
- **«Карта сети»**;
- **«TLS сертификат»**;
- **«Параметры аутентификации»**;
- **«Карточка пользователя»**;

- **«Авторизация пользователя»**.

Фильтрация по полю **«С»** позволяет отфильтровать данные по дате произведённого действия и задаёт начальную дату диапазона. После ввода даты в таблице отобразятся лишь те действия, где **«Дата»** совпадает или больше введённой в фильтр.

Фильтрация по полю **«По»** позволяет отфильтровать данные по дате произведённого действия и задаёт конечную дату диапазона. После ввода даты в таблице отобразятся лишь те действия, где **«Дата»** совпадает или меньше введённой в фильтр.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

11.3.2 Экспорт

Подраздел меню **«Действия»** позволяет экспортировать список действий пользователей в формате таблицы. Для экспорта списка действий необходимо нажать кнопку **«Экспорт»** на панели инструментов.

Экспортированный файл с именем **«<Users Activity {date}>»** в формате **«.CSV»** будет содержать следующий список значений:

- **«Пользователь»**;
- **«ФИО»**;
- **«Действие»**;
- **«Тип объекта»**;
- **«Наименование объекта»**;
- **«Дата»**.

12 ЛИЦЕНЗИИ

В настоящем разделе представлено описание раздела меню **«Лицензии»**, предусматривающего механизм управления лицензиями, который позволяет:

- активировать новую лицензию:
  - автоматическим способом;
  - ручным способом;
- просматривать информацию о текущей лицензии.

Активация и изменение лицензии описаны в руководстве администратора **ARMA MC** (см. Управление лицензиями).

12.1 Информация о текущей лицензии

Для перехода на страницу с информацией о текущей лицензии на панели навигации необходимо выбрать раздел меню **«Лицензии»** (см. Рисунок – Текущая лицензия).

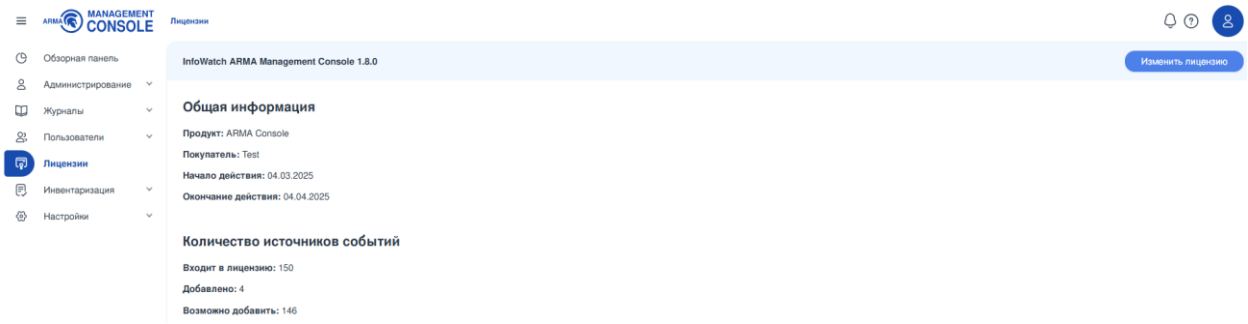


Рисунок – Текущая лицензия

На странице текущей лицензии представлена общая информация о лицензии и информация о количестве источников событий.

Секция **«Общая информация»** содержит следующие данные:

- **«Продукт»** – название продукта;
- **«Покупатель»** – название компании;
- **«Начало действия»** – дата начала действия текущей лицензии;
- **«Окончание действия»** – дата окончания действия текущей лицензии.

Секция **«Количество источников событий»** содержит следующие данные:

- **«Входит в лицензию»** – общее количество источников, доступных к добавлению в список **«Источники»** (см. раздел Источники событий настоящего руководства);
- **«Добавлено»** – количество источников, добавленных в список **«Источники»** в настоящий момент;

- **«Возможно добавить»** – количество источников, доступных к добавлению в список **«Источники»** в настоящий момент.

13 КАРТА СЕТИ

В настоящем параграфе представлено описание подраздела меню **«Карта сети»**, представляющего собой визуализацию инфраструктуры сети и предусматривающего механизм управления следующими функциями:

- отображение устройств сети (активов);
- просмотр информации об активе;
- отображение связей между активами и их индикация;
- добавление новой карты сети;
- добавление группы активов на карту сети;
- фильтрация активов.

«Карта сети» отображает все обнаруженные в сети активы (см. раздел Активы настоящего руководства).

Для перехода к подразделу необходимо на панели навигации в разделе **«Инвентаризация»** выбрать **«Карта сети»** (см. Рисунок – Карта сети).

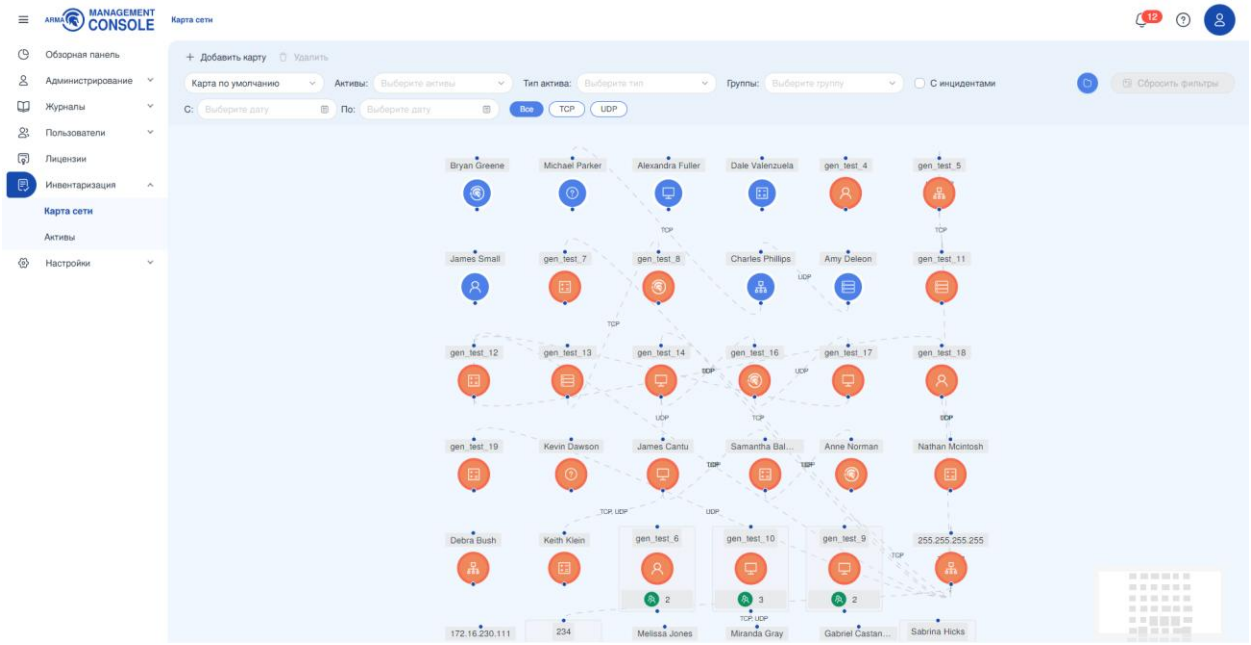


Рисунок – Карта сети

Существует два типа карт сети – карта по умолчанию и пользовательская карта.

Карта **по умолчанию** создаётся автоматически. Все активы на карте расположены в центре, без возможности перемещения активов по карте или удаления. Все активы, удалённые в подразделе меню **«Активы»** (см. Удаление актива настоящего руководства), автоматически пропадают с карты.

Пользовательская карта по умолчанию не содержит активов. Активы добавляются через кнопку « », существует возможность создания связей между активами, добавления фонового изображения и перемещения активов по карте.

13.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать активы и по умолчанию состоит из следующих полей (см. Рисунок – Блок фильтрации):

- **«Карта сети»**;
- **«Активы»**;
- **«Тип актива»**;
- **«Группы»**;
- **чек-бокс «С инцидентами»**;
- **«С»**;
- **«По»**;
- **переключатель «Все/TCP/UDP»**;
- **кнопка «Выбор активов»**;
- **кнопка «Сбросить фильтры»**.

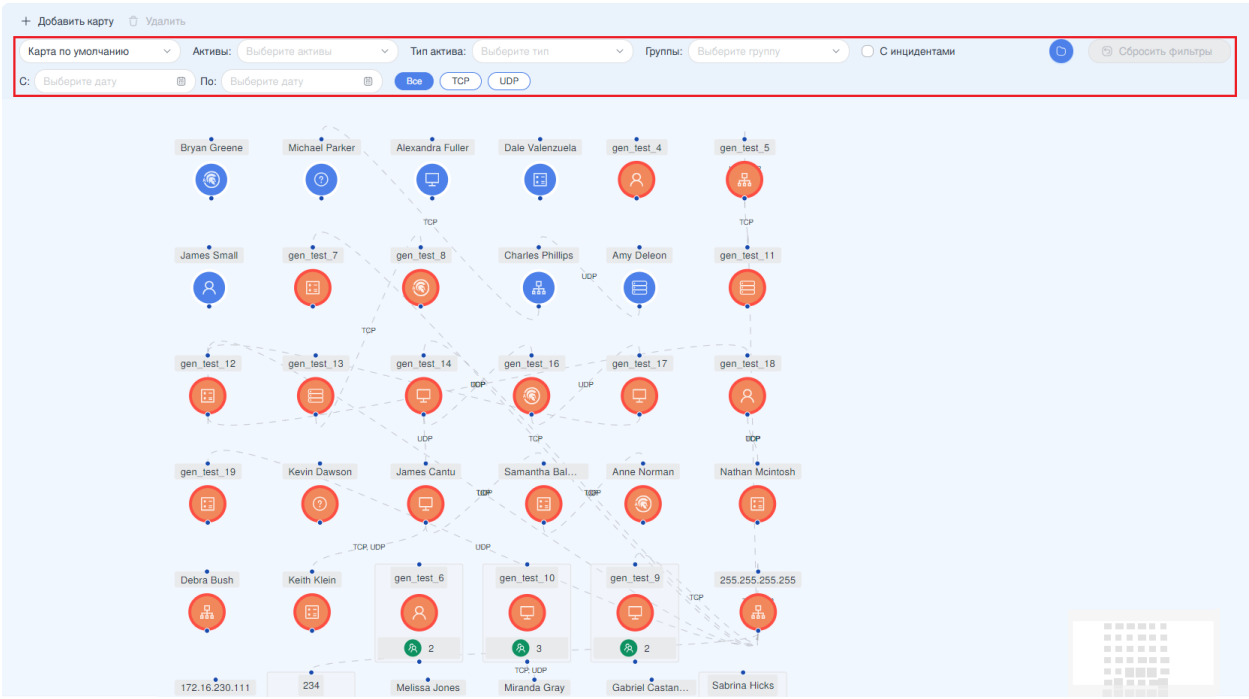


Рисунок – Блок фильтрации

Поле **«Карта сети»** содержит выпадающий список с перечнем пользовательских карт. Существует возможность удалить пользовательскую карту, нажав на кнопку удаления справа от названия карты.

Поле **«Актив»** содержит выпадающий список с перечнем всех добавленных на карту активов. При выборе одного или нескольких активов оставшиеся на карте активы будут отображены серым цветом.

Поле **«Тип актива»** представляет собой выпадающий список и содержит следующие значения:

- **«Без типа»**;
- **«Пользователь»**;
- **«IFW»**;
- **«ПЛК»**;
- **«АРМ»**;
- **«Сервер»**;
- **«Сетевое устройство»**.

Поле **«Группы»** содержит выпадающий список со списком всех созданных пользователем групп активов в подразделе меню **«Активы»** (см. Активы настоящего руководства).

При установке флажка в чек-бокс **«С инцидентами»** на карте отобразятся те активы, на которых зафиксированы инциденты (см. Инциденты настоящего руководства). Остальные будут отображены серым цветом.

Фильтрация по полю **«С»** позволяет отфильтровать активы по дате добавления и задаёт начальную дату диапазона. После ввода даты на карте отобразятся лишь те активы, где **«Дата»** совпадает или больше введённой в фильтр, остальные будут отображены серым цветом.

Фильтрация по полю **«По»** позволяет отфильтровать активы по дате добавления и задаёт конечную дату диапазона. После ввода даты на карте отобразятся лишь те активы, где **«Дата»** совпадает или меньше введённой в фильтр, остальные будут отображены серым цветом.

Переключатель **«Все/TCP/UDP»** позволяет отфильтровать активы с созданными связями. Значение **«TCP»** отображает активы, между которыми существует связь по TCP, значение **«UDP»** отображает активы, между которыми существует связь по UDP. По умолчанию выбрано значение **«Все»**.

При нажатии кнопки «  » открывается боковая панель с древовидным списком всех групп и активов. Активы, которым присвоена группа, будут находиться в папке группы.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

13.2 Связи между активами

Связи между активами отображаются в виде пунктирной линии.

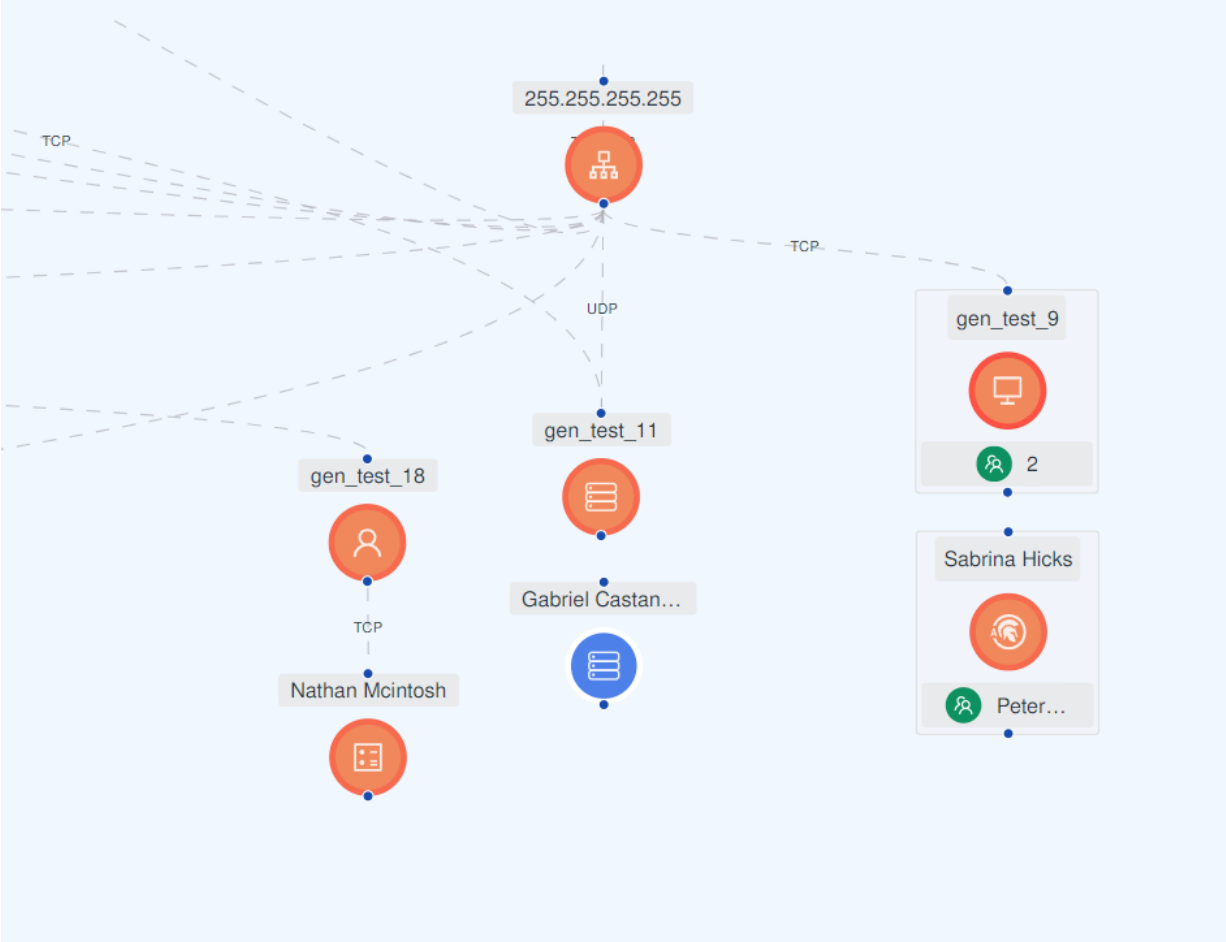


Рисунок – Связи между активами

Для удаления связи необходимо нажать на пунктирную линию между активами, затем нажать кнопку **«Удалить»**.

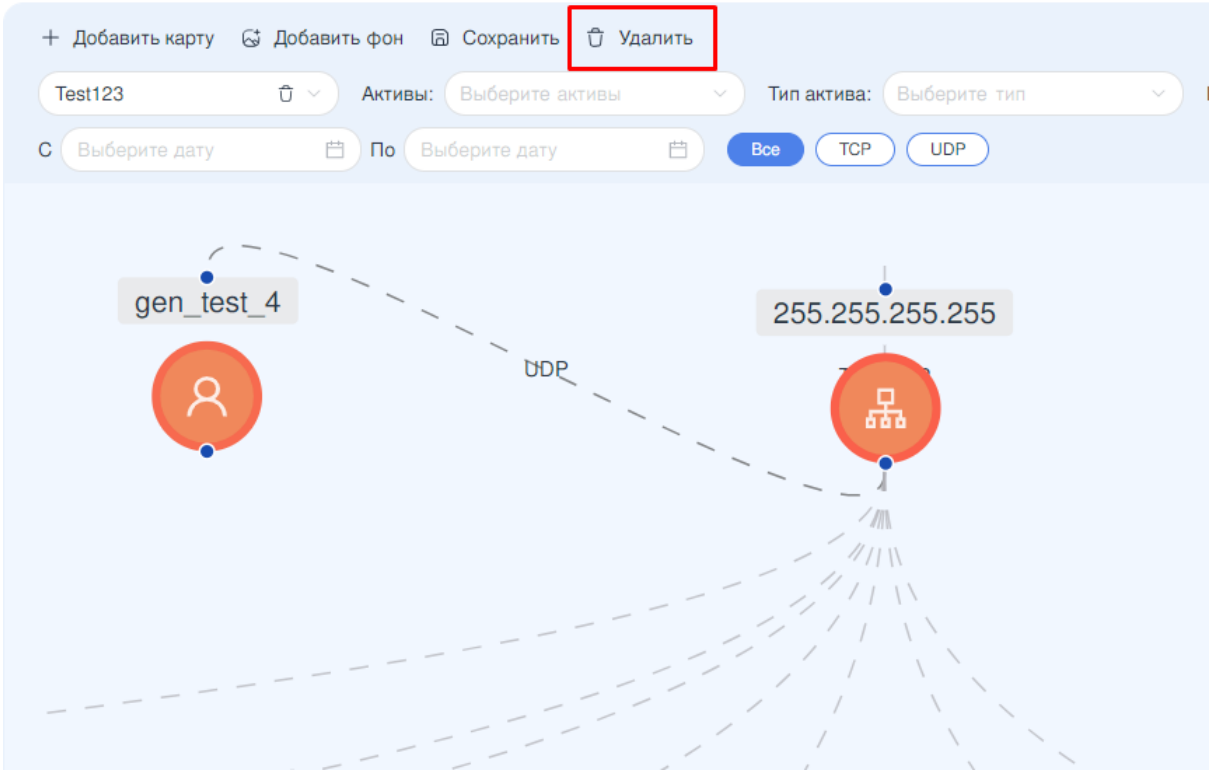


Рисунок – Удаление связи

13.3 Индикация на активе

Активы без обнаруженных инцидентов отображаются синей иконкой с белой рамкой вокруг актива.

Все активы, на которых были обнаружены инциденты, отображаются оранжевой иконкой с красной рамкой.

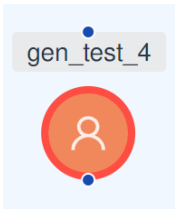


Рисунок – Индикация устройства сети

13.4 Информация об активе

При нажатии на актив отобразится карточка, содержащая следующую информацию об этом узле сети (см. Рисунок – Информация об узле):

- **«Имя узла»**;
- **«IP адрес»**;
- **«Порты»**;
- **«Обновлено»**;

- **«ОС»**;
- **«Описание»**.

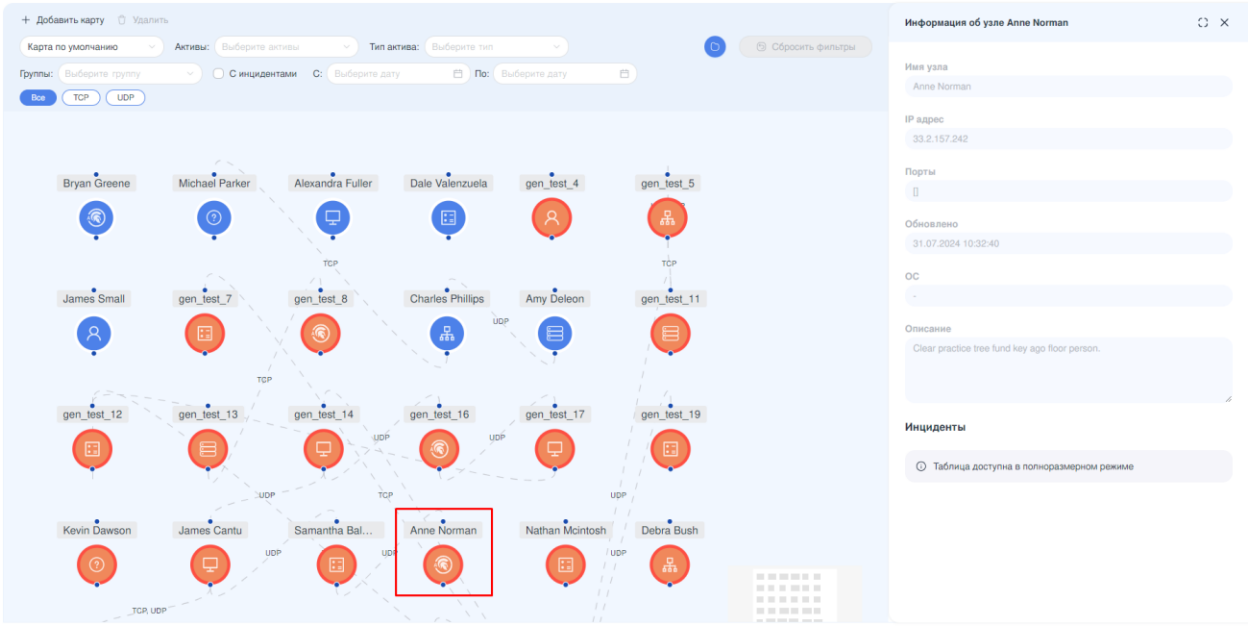


Рисунок – Информация об узле

Информацию об активе невозможно отредактировать в текущем разделе меню. Внесение изменений в параметры актива описано в разделе Карточка актива настоящего руководства.

13.4.1 Инциденты на активе

Просмотр списка зафиксированных на активе инцидентов доступен в полноразмерной карточке актива. Для открытия полноразмерной карточки необходимо нажать кнопку « ». Информация об инцидентах на активе представлена в формате таблицы и состоит из следующих столбцов (см. Рисунок – Полноразмерная карточка актива):

- **«ID»** – порядковый номер инцидента;
- **«Важность»** – важность инцидента, определяется системой на основании сработавшего правила корреляции;
- **«Дата создания»** – время и дата создания инцидента;
- **«Наименование»** – наименование инцидента, определяется системой на основании сработавшего правила корреляции;
- **«IP адрес»** – IP адрес получателя;
- **«Статус»** – статус инцидента для расследования офицером ИБ;
- **«Назначен»** – имя пользователя, на которого назначен инцидент для расследования;

- **«Обновление»** – время и дата обновления инцидента в карточке инцидента.

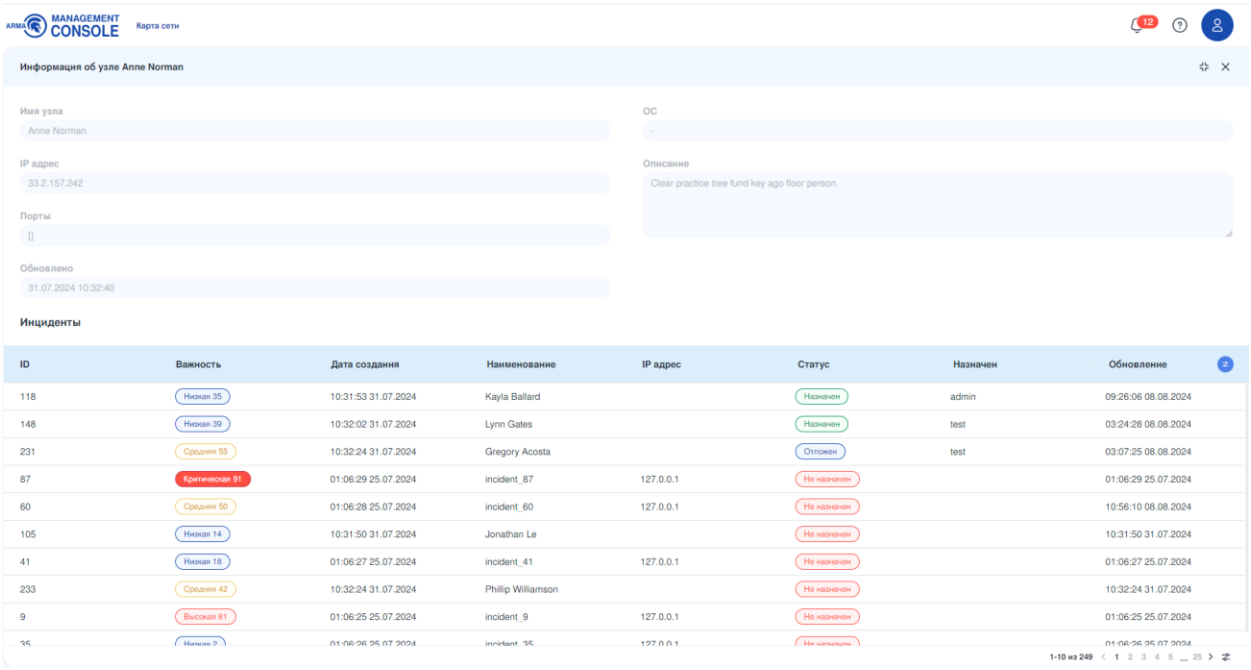


Рисунок – Полноразмерная карточка актива

При нажатии на инцидент отобразится содержащая подробную информацию карточка инцидента (см. Рисунок – Информация об инциденте в карточке актива).

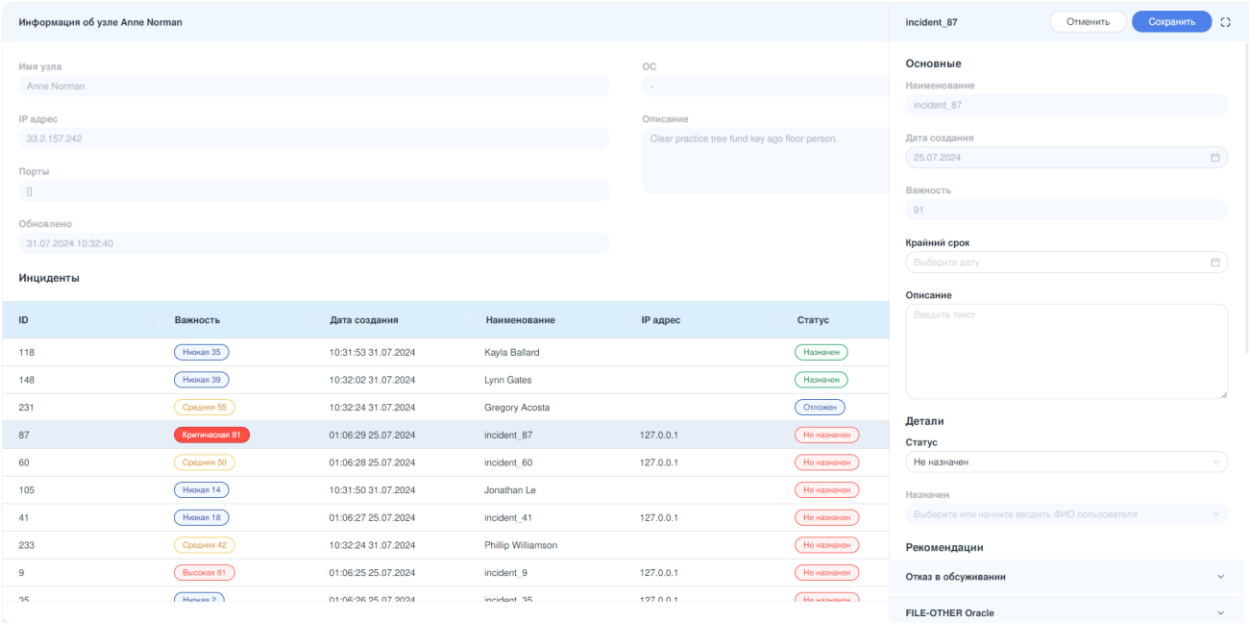


Рисунок – Информация об инциденте в карточке актива

В открывшейся карточке инцидента пользователь имеет возможность внести изменения в следующие поля:

- **«Крайний срок»**;
- **«Описание»**;

- **«Статус»**;
- **«Назначен»**.

Подробная информация о назначении полей и управлении инцидентами описана в разделе Инциденты настоящего руководства.

13.5 Добавление пользовательской карты

Для добавления пользовательской карты сети необходимо выполнить следующие действия:

1. На панели инструментов нажать кнопку **«Добавить карту»**.
2. В появившемся окне **«Создать новую карту»** заполнить поле **«Название карты»** и, при необходимости, поле **«Описание карты»**.
3. Нажать кнопку **«ОК»** (см. Рисунок – Добавление карты).

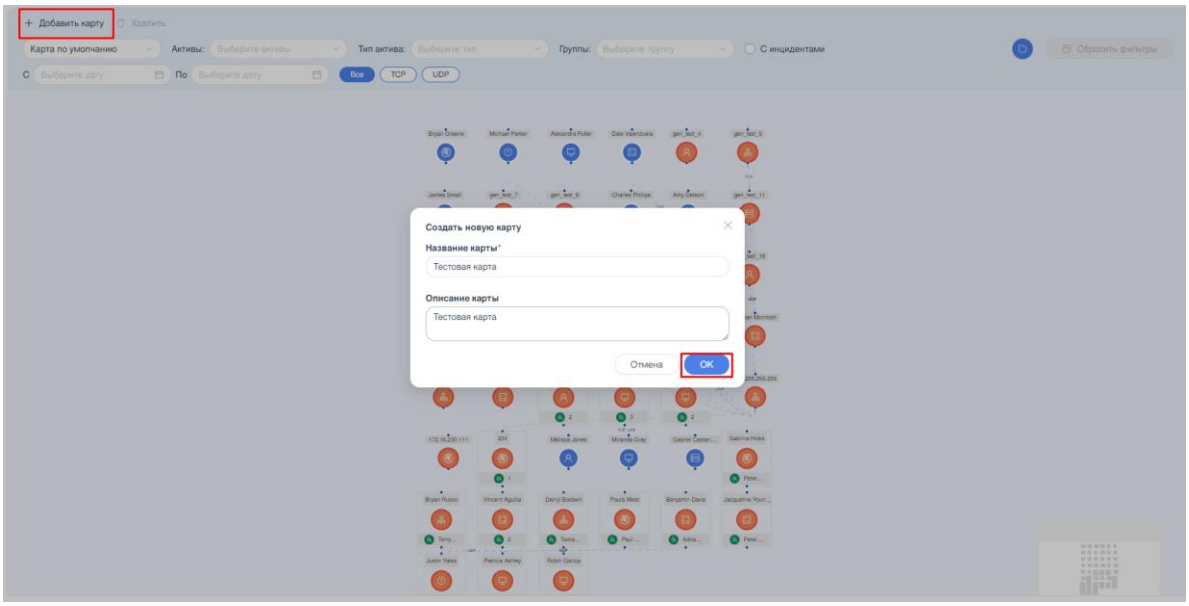


Рисунок – Добавление карты

После успешного создания новой карты появится соответствующее уведомление (см. Рисунок – Успешное добавление карты).

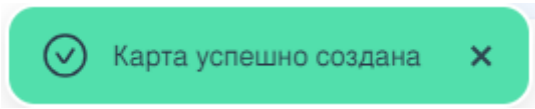


Рисунок – Успешное добавление карты

4. На панели инструментов нажать кнопку **«Сохранить»** или продолжить работу с картой.

После создания карты пользователю доступны следующие действия:

- управление активами через карточку **«Выбор активов»**;
- управление расположением активов;

- управление связями между активами;
- добавление фонового изображения на карту сети.

13.5.1 Управление активами через карточку «Выбор активов»

Для добавления или удаления активов и групп активов с карты сети необходимо нажать кнопку « », в открывшейся карточке установить флажки в чек-боксы напротив необходимых активов и нажать кнопку **«Сохранить»** в правом верхнем углу карточки (см. Рисунок – Добавление/удаление активов).

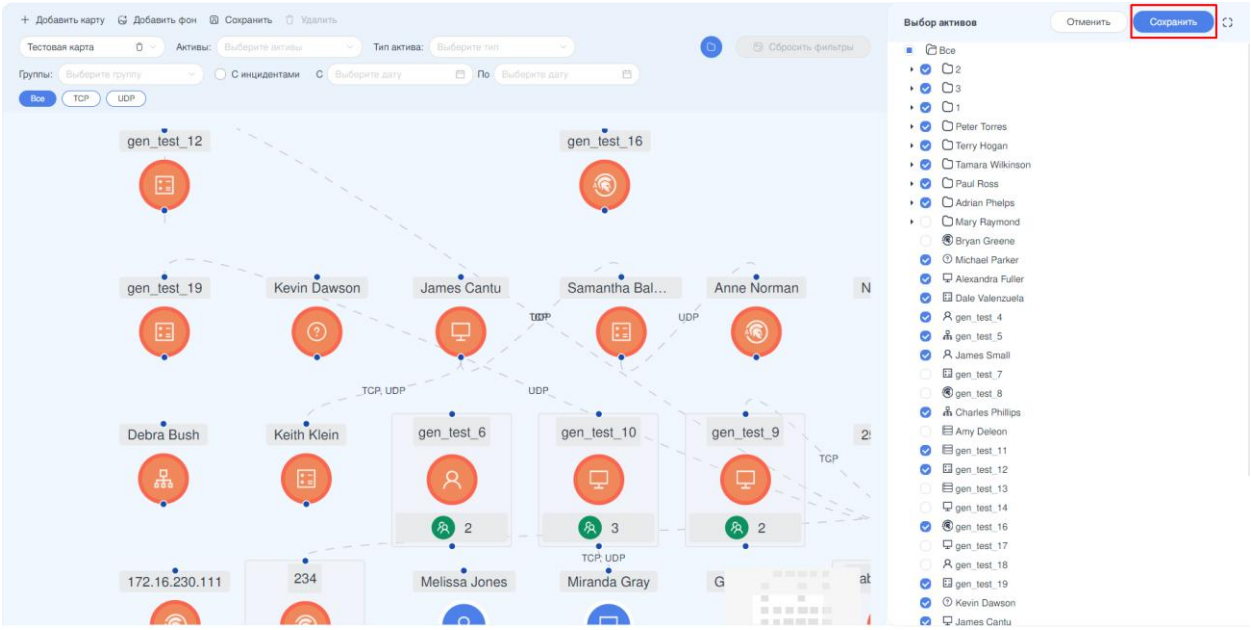


Рисунок – Добавление/удаление активов

13.5.2 Управление расположением активов

Для перемещения актива на карте сети необходимо нажать на необходимый актив и, удерживая клавишу мыши зажатой, перетащить актив в необходимое место на карте.

Для перемещения нескольких активов необходимо зажать на клавиатуре клавишу **«command», «shift»** или **«ctrl»** в зависимости от используемой ОС, выделить необходимые активы, удерживая клавишу мыши зажатой, перетащить активы в необходимое место на карте.

13.5.3 Управление связями между активами

Для добавления связи между активами необходимо нажать на синюю точку связи вверху/внизу актива и, удерживая клавишу мыши зажатой, протянуть линию связи до точки связи другого актива (см. Рисунок – Связь между активами).

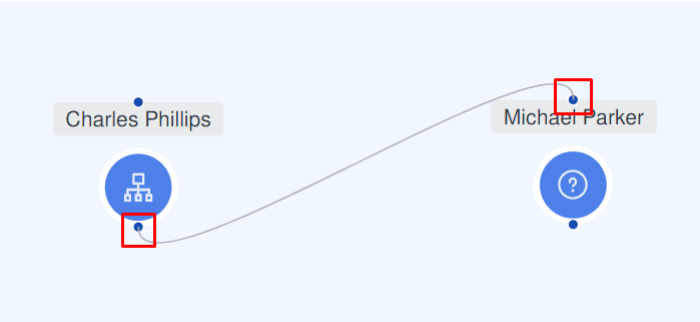


Рисунок – Связь между активами

Для удаления связи необходимо нажать на пунктирную линию между устройствами сети, затем нажать кнопку **«Удалить»** (см. Рисунок – Удаление связи между активами).

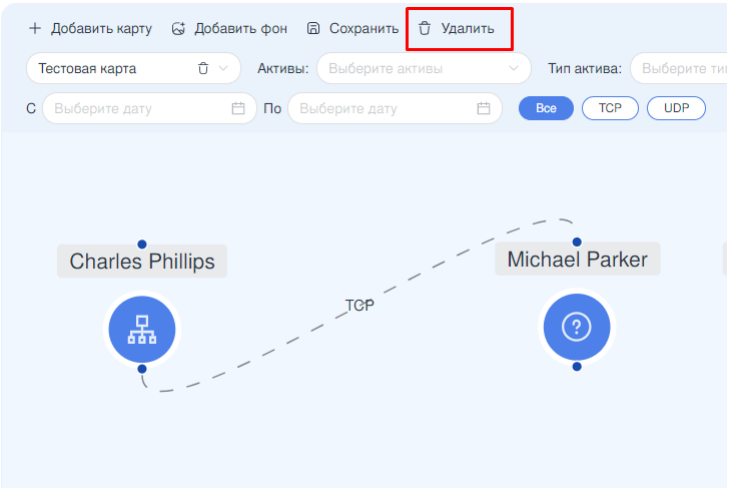


Рисунок – Удаление связи между активами

13.5.4 Фоновое изображение

Для добавления **фонового изображения** на карту сети, например, схемы помещения, необходимо на панели инструментов нажать кнопку **«Добавить фон»**, в открывшемся окне проводника выбрать необходимый файл фонового изображения и нажать кнопку **«Открыть»** (см. Рисунок – Добавление фона). Доступные форматы фонового изображения – **«jpeg»**, **«jpg»**, **«png»**, **«webp»**. После добавления фонового изображения существует возможность увеличить изображение до необходимых масштабов, нажав на край изображения и растянув его.

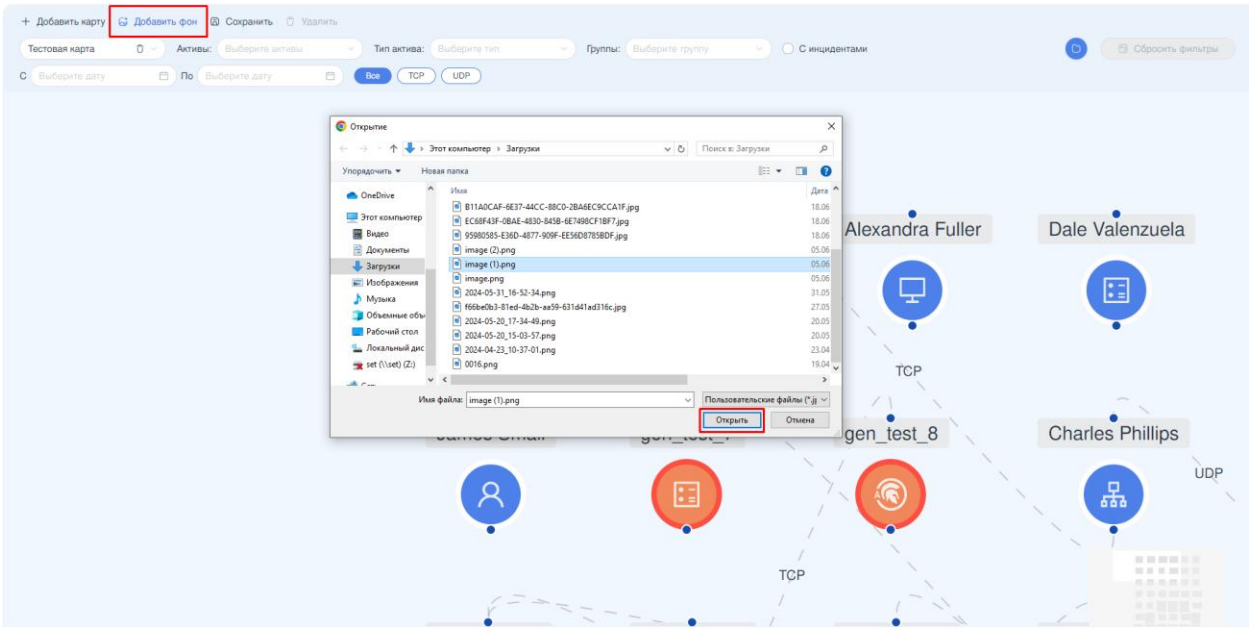


Рисунок – Добавление фона

Для удаления фонового изображения необходимо нажать на изображение, затем кнопку « » в правом верхнем углу изображения и подтвердить удаление в открывшемся окне уведомления.

После внесения всех необходимых изменений на карте сети необходимо нажать кнопку **«Сохранить»** на панели инструментов.

> **Примечание**:
>
> **ARMA MC** отслеживает несохранённые изменения. При попытке перехода в другой раздел меню и наличии несохранённых изменений на карте сети, появится всплывающее окно с уведомлением: **«У вас есть несохраненные изменения на карте сети. Вы действительно хотите перейти без сохранения?»**.

14 АКТИВЫ

В настоящем разделе представлено описание подраздела меню **«Активы»**, предназначенного для удобства проведения инвентаризации инфраструктуры сети и предусматривающего механизм управления следующими функциями:

- просмотр обнаруженных устройств сети;
- регистрация обнаруженных устройств сети.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Инвентаризация»**, затем – подраздел **«Активы»** (см. Рисунок – Активы).

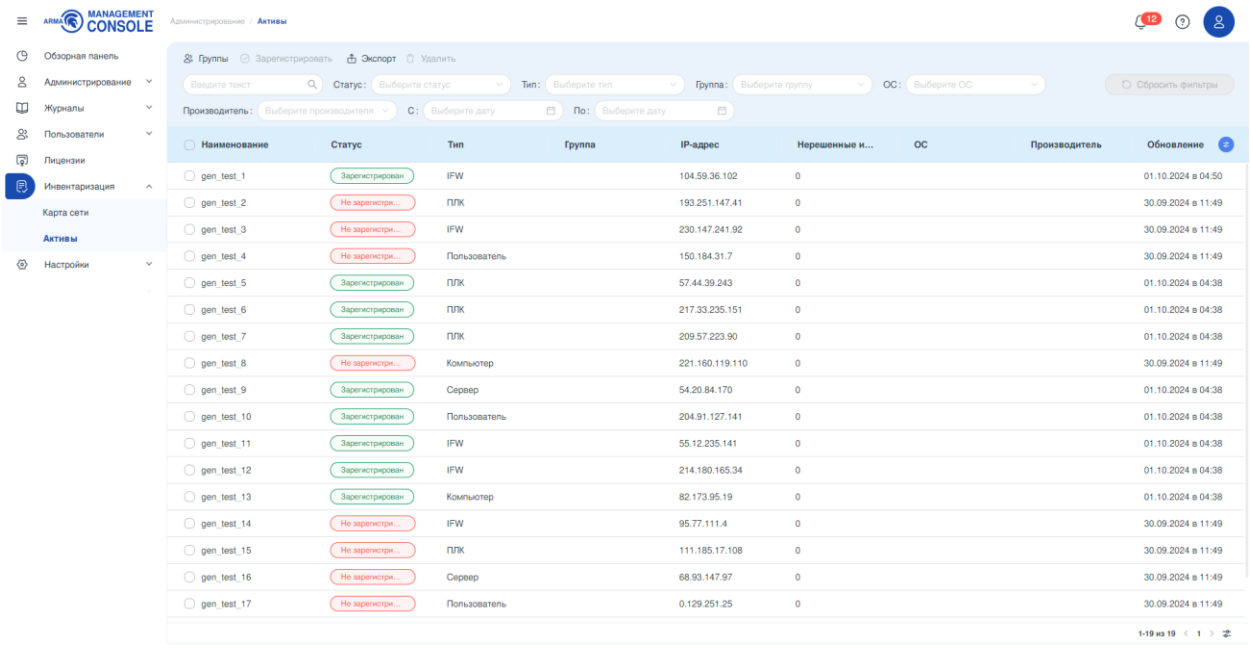


Рисунок – Активы

Подраздел меню позволяет просматривать активы в формате таблицы, состоящей из следующих столбцов:

- **«Наименование»** – наименование актива;
- **«Статус»** – статус регистрации актива («Зарегистрирован»/«Не зарегистрирован»), по умолчанию «Не зарегистрирован»;
- **«Тип»** – тип актива («IFW»/«Сетевое устройство»/«Компьютер»/«ПЛК»/«Сервер»/«Пользователь»);
- **«Группа»** – группа, в которую определён актив. Группы назначаются пользователем и используются для удобства фильтрации;
- **«IP адрес»** – IP адрес актива, определяется системой на основании сработавшего правила корреляции;
- **«Нерешенные инциденты»** – количество нерешённых инцидентов, привязанных к конкретному активу;

- **«ОС»** – операционная система актива;
- **«Производитель»** – производитель актива;
- **«Обновление»** – время и дата обновления актива в карточке актива.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

14.1 Поиск и фильтрация

Блок фильтрации позволяет фильтровать инциденты по всем столбцам списка и по умолчанию состоит из следующих полей (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **«Статус»**;
- **«Тип»**;
- **«Группа»**;
- **«ОС»**;
- **«Производитель»**;
- **«С»**;
- **«По»**;
- **кнопка «Сбросить фильтры»**.

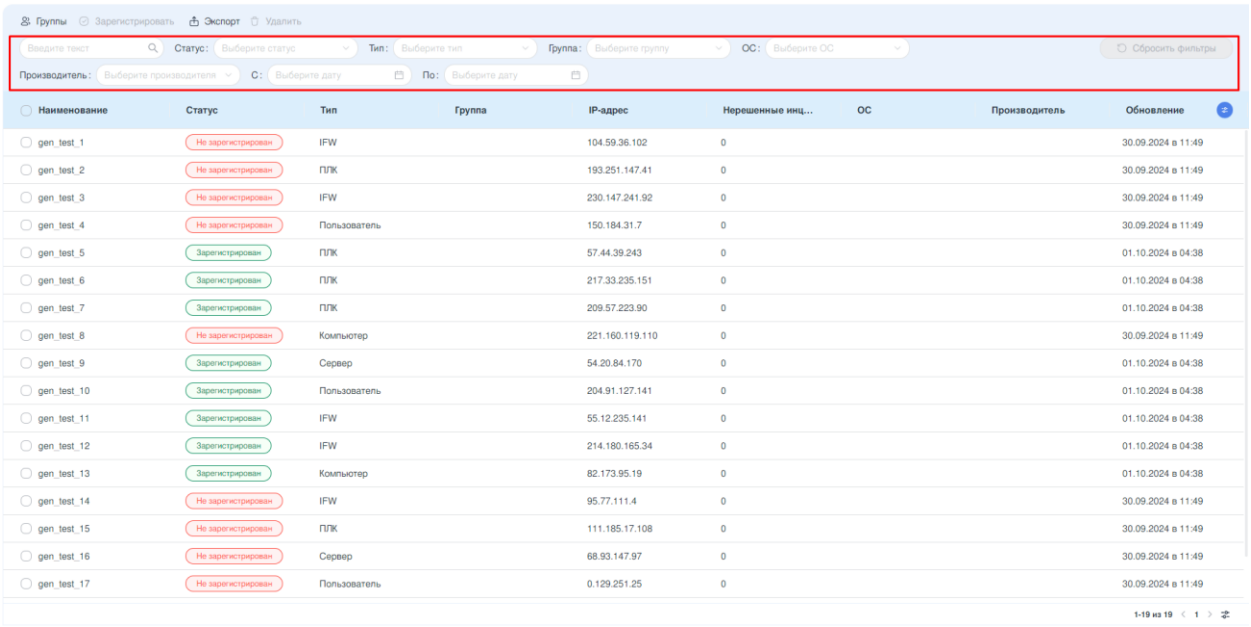


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам **«Наименование»** и **«IP адрес»**.

Фильтрация по полю **«Статус»** позволяет отфильтровать данные по статусу регистрации актива. Поле **«Статус»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«Зарегистрирован»**;
- **«Не зарегистрирован»**.

Фильтрация по полю **«Тип»** позволяет отфильтровать данные по типу актива. Поле **«Тип»** содержит выпадающий список и предоставляет выбор из следующих вариантов значений:

- **«IFW»**;
- **«Сетевое устройство»**;
- **«Компьютер»**;
- **«ПЛК»** – программируемый логический контроллер;
- **«Сервер»**;
- **«Пользователь»**.

Фильтрация по полю **«Группа»** позволяет отфильтровать данные по группам, в которые включены активы.

Фильтрация по полю **«ОС»** позволяет отфильтровать данные по операционным системам активов.

Фильтрация по полю **«Производитель»** позволяет отфильтровать данные по производителю активов.

Фильтрация по полю **«С»** позволяет отфильтровать активы по дате обновления и задаёт начальную дату диапазона. После ввода даты в таблице отобразятся лишь активы, обновлённые не ранее указанной даты.

Фильтрация по полю **«По»** позволяет отфильтровать активы по дате обновления и задаёт конечную дату диапазона. После ввода даты в таблице отобразятся лишь активы, обновлённые не позднее указанной даты.

Сброс всех установленных фильтров осуществляется нажатием кнопки **«Сбросить фильтры»**.

14.2 Управление активами

В **ARMA MC** предусмотрены следующие шаги для работы с активами:

- добавление актива;
- регистрация актива;
- просмотр информации об активах.

14.2.1 Добавление актива

Формирование актива и его отображение в списке активов происходит после срабатывания правила корреляции. Добавление актива вручную невозможно. Логика работы правила заключается в проверке приходящих от источника логов и, в случае получения события о появлении в сети нового сетевого устройства, создании нового актива. Следовательно, для добавления актива в список активов необходимо, чтобы к **ARMA MC** был подключён источник, например, **«IFW»**. Предварительные настройки источника на примере **«IFW»** описаны в Руководстве пользователя **ARMA FW** (см. Обнаружение устройств).

> **Примечание**:
>
> Предустановленное правило корреляции «(SID 1, «NewAsset»)», отвечавшее за создание активов от источника **«IFW»**, в данной версии **ARMA MC** не используется. Поэтому для источника **«IFW»** также необходимо создавать пользовательское правило.
>
> Порядок создания правила:
>
> 1. Открыть раздел **«Правила корреляции»** (подробнее см. Правила корреляции настоящего руководства).
> 2. Нажать кнопку **«Добавить»** – откроется карточка правила.
> 3. Заполнить поле **«Наименование»**.

4. Заполнить поле **«Условие срабатывания правила корреляции»** (например, **«sign_category:"ARPWATCH"»**).
5. Выбрать действие **«Добавить актив»** (подробнее см. Тип действия «Добавить актив» настоящего руководства).
6. В открывшейся ниже области заполнить поле **«Наименование актива»**.
7. Там же заполнить поле **«IP-адрес»** значением **«{{.source_ip}}»**, чтобы обрабатывать все возможные адреса.
8. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки.

Теперь получение соответствующих правилу событий, будет приводить к добавлению активов в список.

14.2.2 Регистрация актива

После обнаружения актив появляется в списке активов в статусе **«Не зарегистрирован»**.

Для регистрации актива необходимо сверить IP-адрес обнаруженного системой актива со списком устройств организации. В случае, если IP-адрес совпал, необходимо выполнить следующие действия (см. Рисунок – Регистрация актива):

1. Выбрать актив или активы, установив флажок в чек-боксе слева от **«Наименования»** актива.
2. Нажать кнопку **«Зарегистрировать»** на панели инструментов.

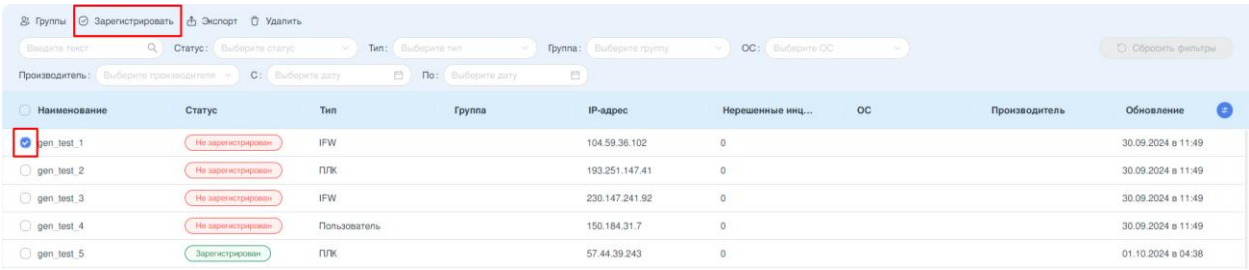


Рисунок – Регистрация актива

После успешной регистрации актива появится соответствующее уведомление (см. Рисунок – Успешная регистрация актива).

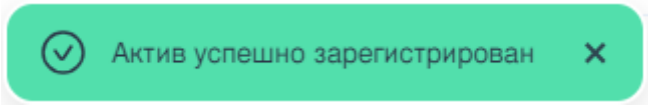


Рисунок – Успешная регистрация актива

Внесение дополнительной информации об активе и изменения текущей информации производится в карточке актива.

14.3 Карточка актива

Карточка актива содержит следующую информацию об активе (см. Рисунок – Карточка актива):

- **«Наименование»**;
- **«Статус»**;
- **«Группа»**;
- **«Тип»**;
- **«IP-адрес»**;
- **«ОС»**;
- **«Производитель»**;
- **«Модель»**;
- **«Порты»**;
- **«Описание»**.

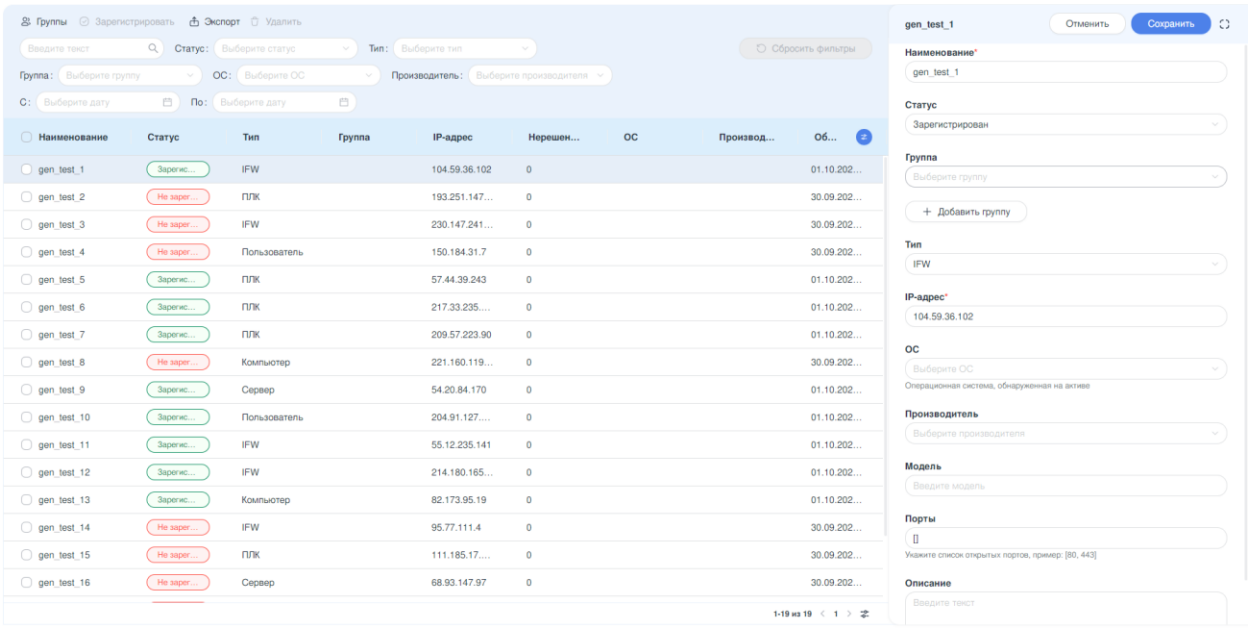


Рисунок – Карточка актива

Для просмотра или изменения информации об активе необходимо выполнить следующие действия:

1. Выбрать необходимый актив, нажав на записи с активом.
2. В открывшейся карточке заполнить или внести изменения в необходимые поля.
3. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки.

После успешного изменения информации об активе появится соответствующее уведомление (см. Рисунок – Успешное изменение информации об активе).

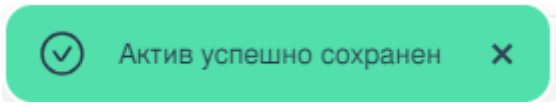


Рисунок – Успешное изменение информации об активе

14.4 Удаление актива

Для удаления актива необходимо выполнить следующие действия (см. Рисунок – Удаление актива):

1. Выбрать актив или активы, установив флажок в чек-боксе слева от **«Наименования»** актива.
2. Нажать кнопку **«Удалить»** на панели инструментов.
3. Подтвердить удаление актива.

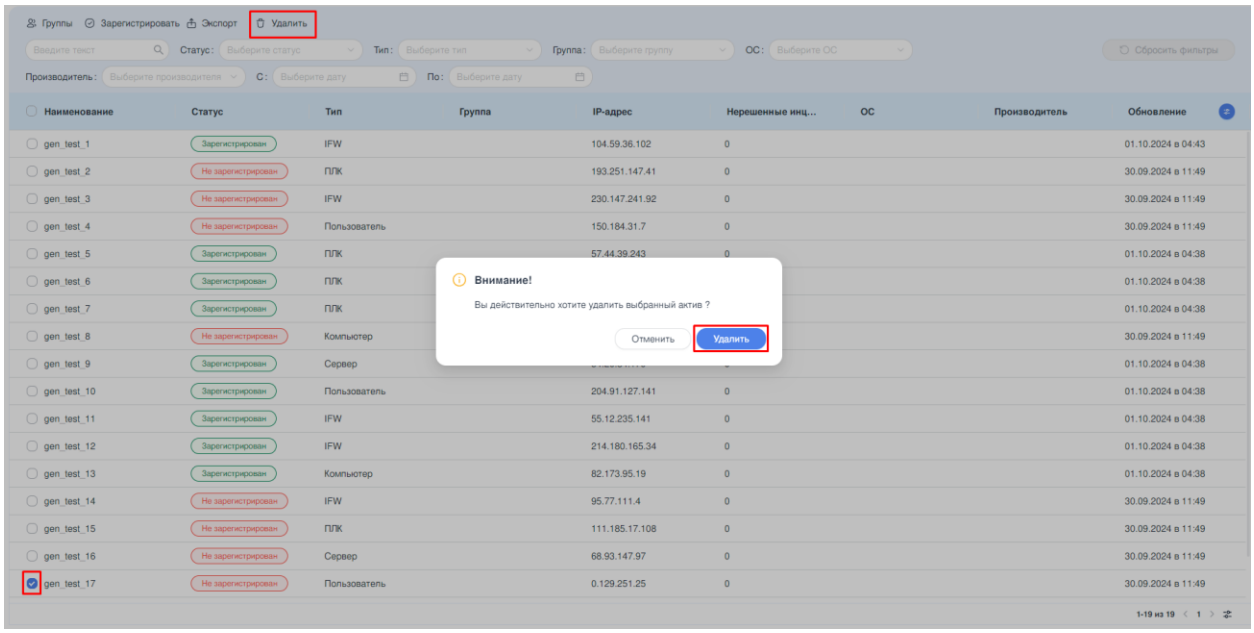


Рисунок – Удаление актива

После успешного удаления актива появится соответствующее уведомление (см. Рисунок – Успешное удаление актива).

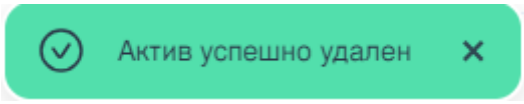


Рисунок – Успешное удаление актива

14.5 Экспорт активов

Существует возможность локально сохранить таблицу активов. Для этого необходимо на панели инструментов нажать кнопку **«Экспорт»** (см. Рисунок – Активы). Формат экспортированного файла – **«csv»**.

После успешного экспорта списка активов появится соответствующее уведомление (см. Рисунок – Успешный экспорт актива).

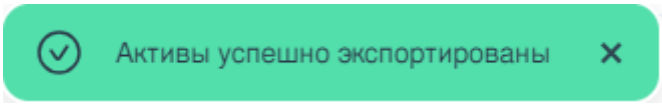


Рисунок – Успешный экспорт актива

14.6 Управление группами активов

Существует возможность объединять активы в группы. Группы назначаются пользователем и используются для удобства фильтрации.

14.6.1 Добавление группы

Для добавления группы необходимо выполнить следующие действия (см. Рисунок – Добавление группы):

1. На панели инструментов нажать кнопку **«Группы»**.
2. В открывшейся форме **«Список групп»** нажать кнопку **«Добавить»**.
3. В открывшемся окне указать значения в полях параметров **«Наименование»** и **«Описание»**.
4. Нажать кнопку **«Сохранить»**.

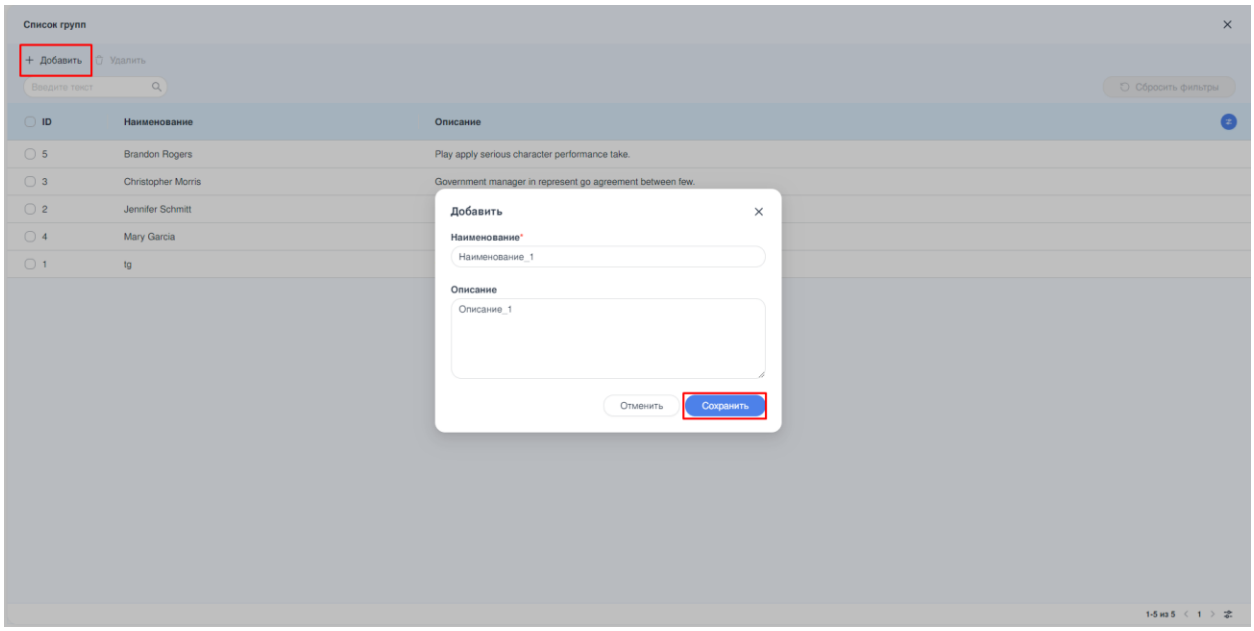


Рисунок – Добавление группы

В случае успешного создания группы появится соответствующее уведомление (см. Рисунок – Успешное добавление группы).

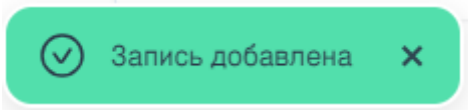


Рисунок – Успешное добавление группы

14.6.2 Редактирование группы

Для редактирования группы необходимо выполнить следующие действия (см. Рисунок – Изменение группы):

1. На панели инструментов нажать кнопку **«Группы»**.
2. В форме **«Список групп»** нажать на необходимую группу.
3. В открывшемся окне отредактировать значения в полях параметров **«Наименование»** и/или **«Описание»**.
4. Нажать кнопку **«Изменить»**.

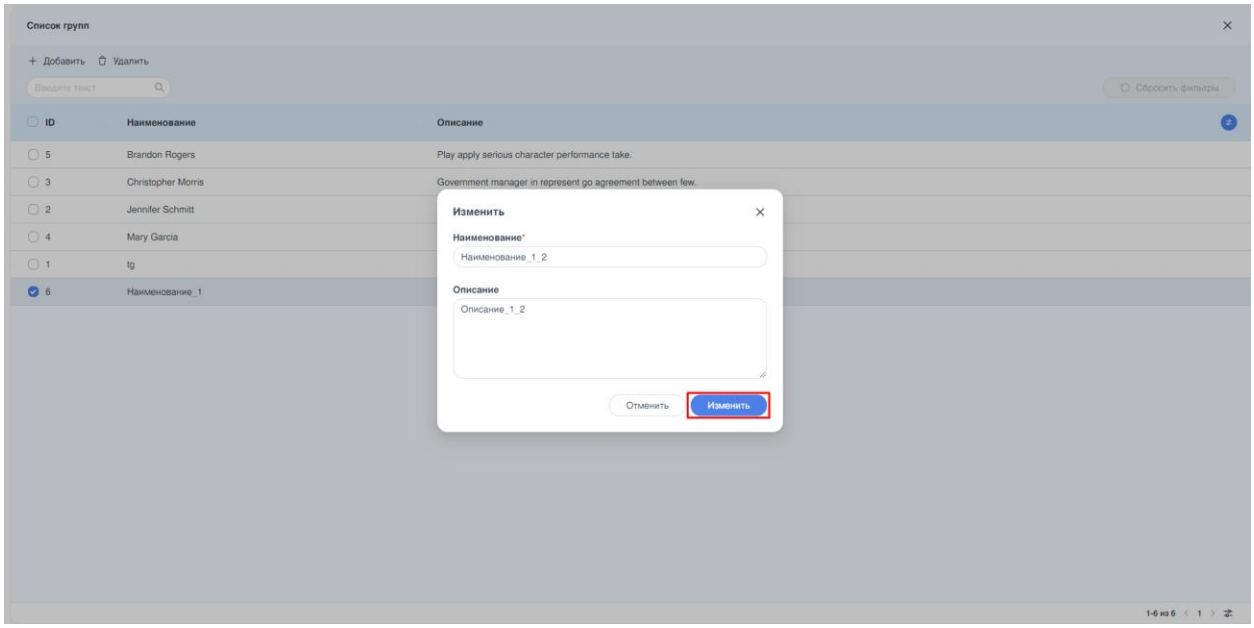


Рисунок – Изменение группы

В случае успешного редактирования группы появится соответствующее уведомление (см. Рисунок – Успешное изменение группы).

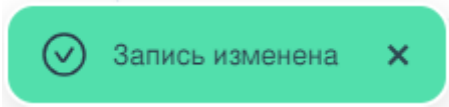


Рисунок – Успешное изменение группы

14.6.3 Удаление группы

Для удаления группы необходимо выполнить следующие действия (см. Рисунок – Удаление группы):

1. В форме **«Список групп»** установить флажок в чек-боксе слева от значения **«ID»** необходимой группы или групп.
2. Нажать кнопку **«Удалить»** на панели инструментов.
3. В появившемся окне подтвердить удаление группы, нажав кнопку **«Удалить»**.

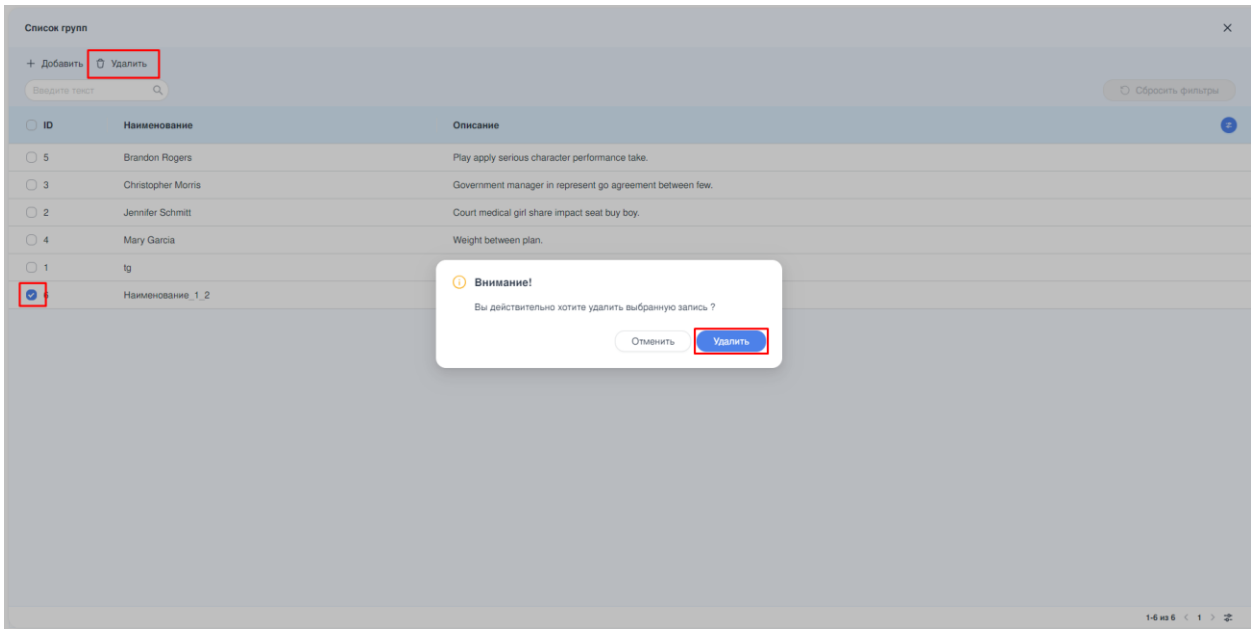


Рисунок – Удаление группы

В случае успешного удаления группы появится соответствующее уведомление (см. Рисунок – Успешное удаление группы).

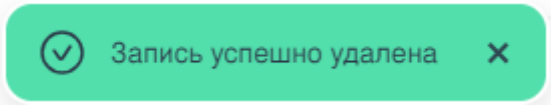


Рисунок – Успешное удаление группы

15 НАСТРОЙКИ

В настоящем разделе представлено описание раздела меню **«Настройки»**, предусматривающего механизм управления следующими функциями:

- настройка TLS сертификата;
- настройка аутентификации;
- просмотр настроек ротации инцидентов и событий;
- обновление **ARMA MC**;
- редактирование карточки организации (см. Карточка организации настоящего руководства).

15.1 Системные настройки

15.1.1 TLS сертификат

В **ARMA MC** предусмотрен механизм настройки протокола TLS для криптографического шифрования канала связи.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Настройки»**, затем подраздел **«Системные настройки»**.

Включение TLS позволяет передавать данные по протоколу защиты транспортного уровня TLS, обеспечивающему зашифрованную передачу данных при подключении к веб-интерфейсу **ARMA MC**.

В блоке **«TLS сертификат»** существует возможность (см. Рисунок – TLS сертификат):

- удалить сертификат и ключ;
- сгенерировать новые сертификат и ключ;
- добавить пользовательские сертификат и ключ;
- экспортировать сертификат и ключ.

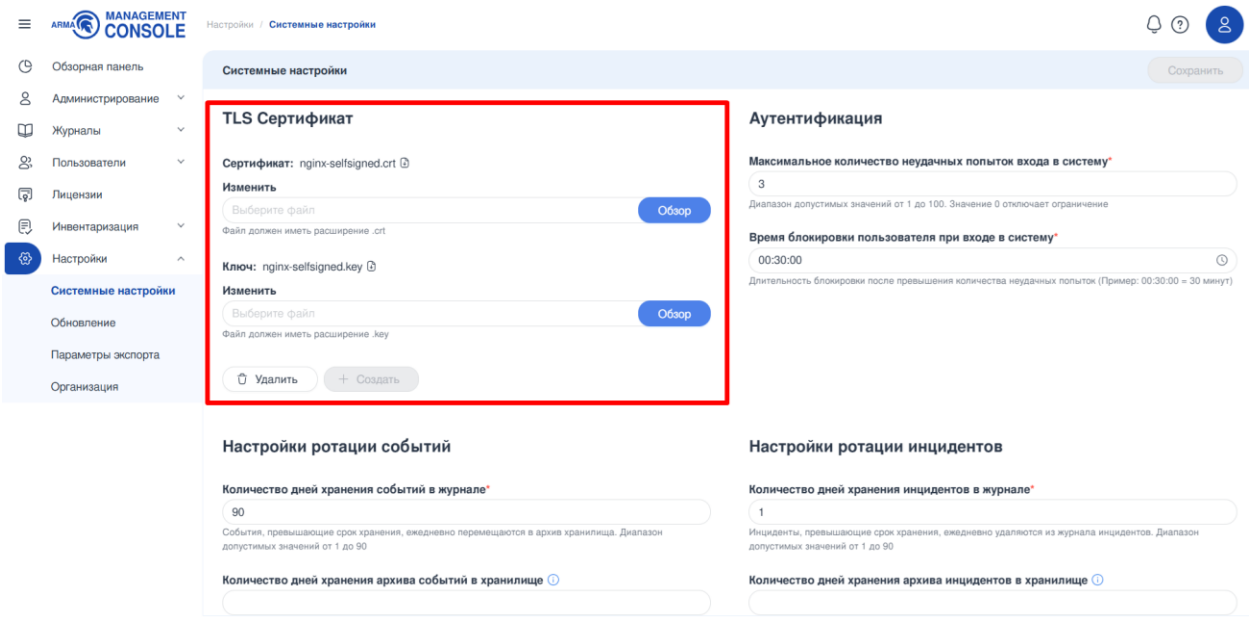


Рисунок – TLS сертификат

Примечание:

Сертификат и ключ генерируются со сроком действия 1 год. После окончания срока действия текущего сертификата и ключа необходимо сгенерировать их повторно.

15.1.1.1 Создание TLS сертификата

Примечание:

С версии **ARMA MC «1.7»** и выше сертификат создаётся автоматически после установки. Но при необходимости его можно заменить.

Для генерации сертификата и ключа безопасности необходимо нажать кнопку **«Создать»** в блоке **«TLS сертификат»** (см. Рисунок – Кнопка «Создать новый»).

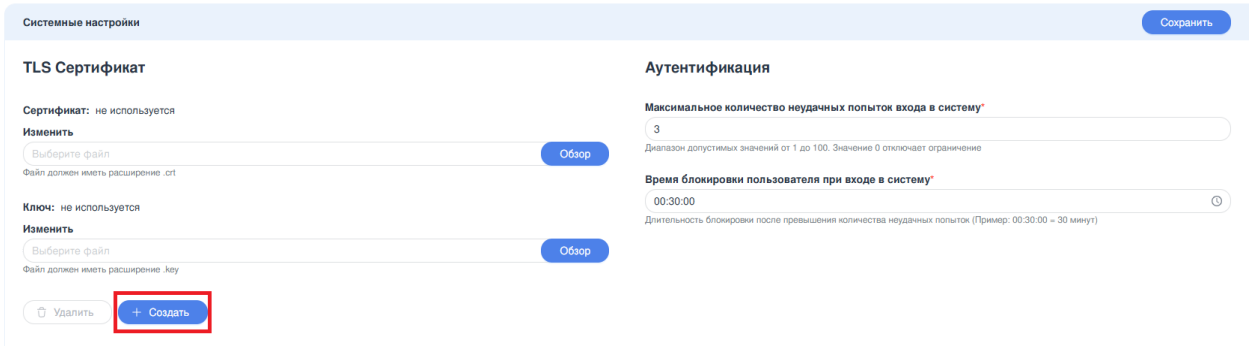


Рисунок – Кнопка «Создать новый»

Появится уведомление о создании нового сертификата (см. Рисунок – Генерация сертификата и ключа).

Примечание:

Созданный сертификат и ключ безопасности будут отображаться в полях **«Сертификат»** и **«Ключ»** соответственно. Кнопки для скачивания сертификата и ключа появятся правее имён файлов.

При отсутствии сертификата **ARMA MC** использует **«http»**. После добавления сертификата **ARMA MC** перейдёт на **«https»** (страница перезагрузится автоматически).

Рисунок – Генерация сертификата и ключа

15.1.1.2 Добавление пользовательского TLS сертификата

Для добавления пользовательских сертификата и ключа в блоке **«TLS сертификат»** необходимо выполнить следующие действия:

1. Нажать кнопку **«Обзор»** в поле **«Изменить»** для добавления сертификата безопасности, в открывшемся проводнике выбрать файл необходимого сертификата. Файл должен иметь расширение **«.crt»** (см. Рисунок – Кнопка «Обзор»).
2. Нажать кнопку **«Обзор»** в поле **«Изменить»** для добавления ключа безопасности, в открывшемся проводнике выбрать файл необходимого ключа. Файл должен иметь расширение **«.key»** (см. Рисунок – Кнопка «Обзор»).

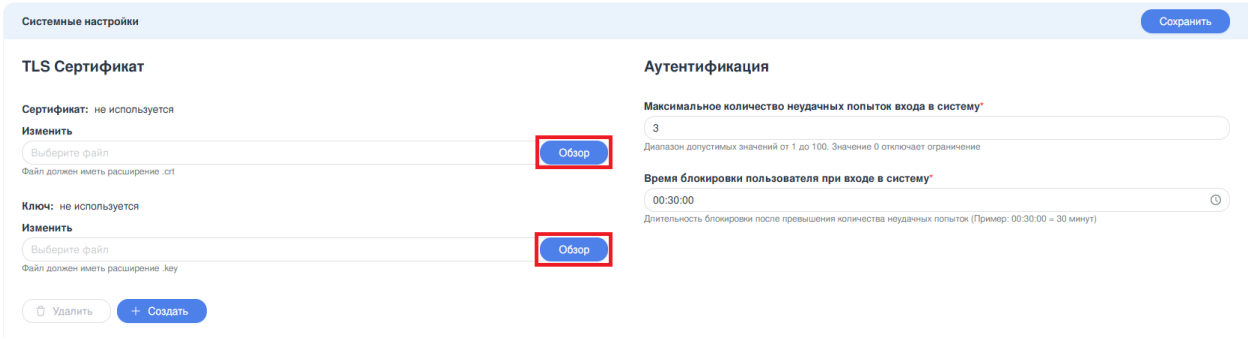


Рисунок – Кнопка «Обзор»

3. Нажать кнопку **«Сохранить»** в правом верхнем углу экрана.

Примечание:

В текущей версии **ARMA MC** не поддерживаются TLS-сертификаты с поддержкой алгоритмов ГОСТ (ГОСТ TLS) – ГОСТ Р 34.13-2018.

Загрузка некорректного TLS-сертификата блокирует возможность обновления **ARMA MC** на следующую версию, а также может привести к потере данных.

При загрузке некорректного сертификата и/или ключа появится соответствующее уведомление (см. Рисунок – Некорректный ключ/сертификат):

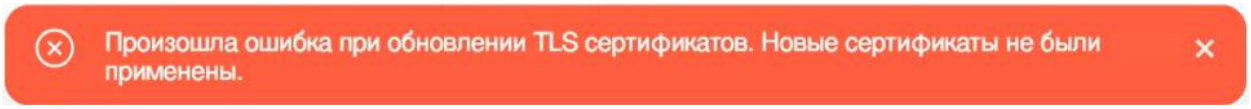


Рисунок – Некорректный ключ/сертификат

15.1.1.3 Экспорт TLS сертификата

Для экспорта сертификата и ключа в блоке **«TLS сертификат»** необходимо нажать иконку экспорта справа от сгенерированного сертификата или ключа безопасности (см. Рисунок – Экспорт сертификата и ключа).

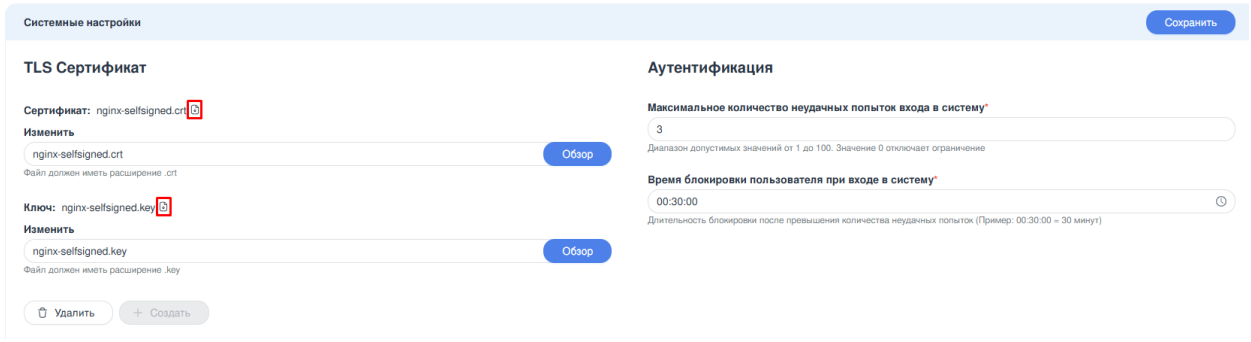


Рисунок – Экспорт сертификата и ключа

15.1.1.4 Удаление TLS сертификата

> **Примечание**:
>
> Внимание! Стабильная работа **ARMA MC** не гарантируется, если сертификат отсутствует.
> Не удаляйте сертификат без необходимости, а если это произошло, следует немедленно добавить или сгенерировать новый.

Для удаления сертификата и ключа безопасности достаточно нажать кнопку **«Удалить»** в блоке **«TLS сертификат»** (см. Рисунок – Кнопка «Удалить»).

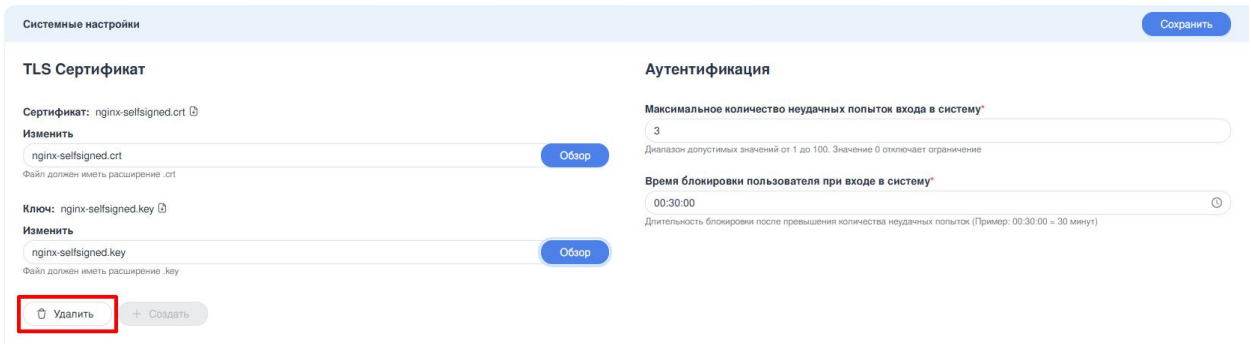


Рисунок – Кнопка «Удалить»

Появится уведомление об удалении текущего сертификата и ключа безопасности (см. Рисунок – Удаление сертификата и ключа).

Рисунок – Удаление сертификата и ключа

15.1.2 Аутентификация

Подраздел меню **«Аутентификация»** позволяет настраивать параметры аутентификации.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Настройки»**, затем подраздел **«Системные настройки»**.

В подразделе **«Аутентификация»** существует возможность задавать количество допустимых попыток входа в веб-интерфейс и время ожидания, в течение которого пользователю будет отказано в аутентификации после превышения попыток входа (см. Рисунок – Аутентификация).

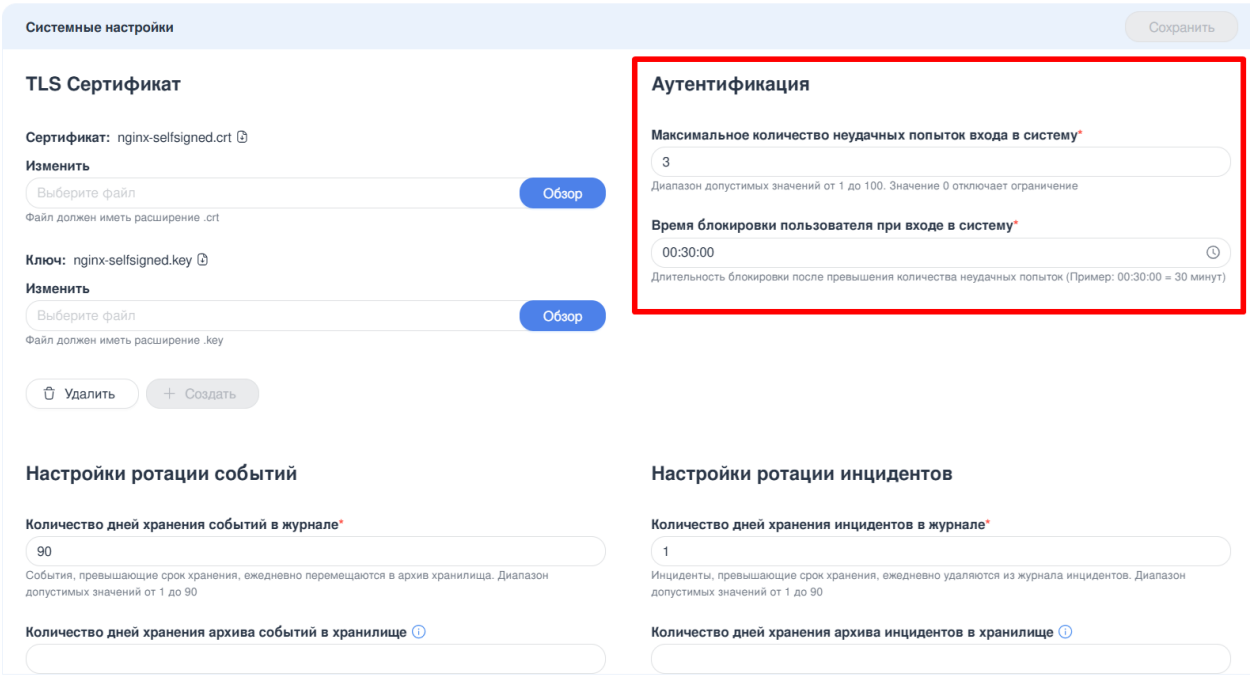


Рисунок – Аутентификация

Для установки параметров аутентификации необходимо выполнить следующие действия:

1. Выставить значение в диапазоне от 1 до 100 в поле **«Максимальное количество неудачных попыток входа в систему»**. Значение «0» отключает ограничение на попытки входа в систему.
2. Выставить значение времени, на которое будет заблокирован пользователь при достижении ограничения на неудачные попытки входа, в поле **«Время блокировки пользователя при входе в систему»**.
3. Нажать кнопку **«Сохранить»**.

Примечание:

По прошествии времени, указанного в поле параметра **«Время блокировки пользователя при входе в систему»**, пользователю снова будет доступна аутентификация в веб-интерфейсе.

Администратор может досрочно разблокировать пользователя, изменив его статус в карточке пользователя, как это описано в параграфе Управление УЗ настоящего руководства.

15.1.3 Настройки ротации

Подраздел меню **«Настройки ротации»** позволяет настраивать ротацию журналов инцидентов, событий и действий пользователя.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Настройки»**, затем подраздел **«Системные настройки»** (см. Рисунок – Настройки ротации).

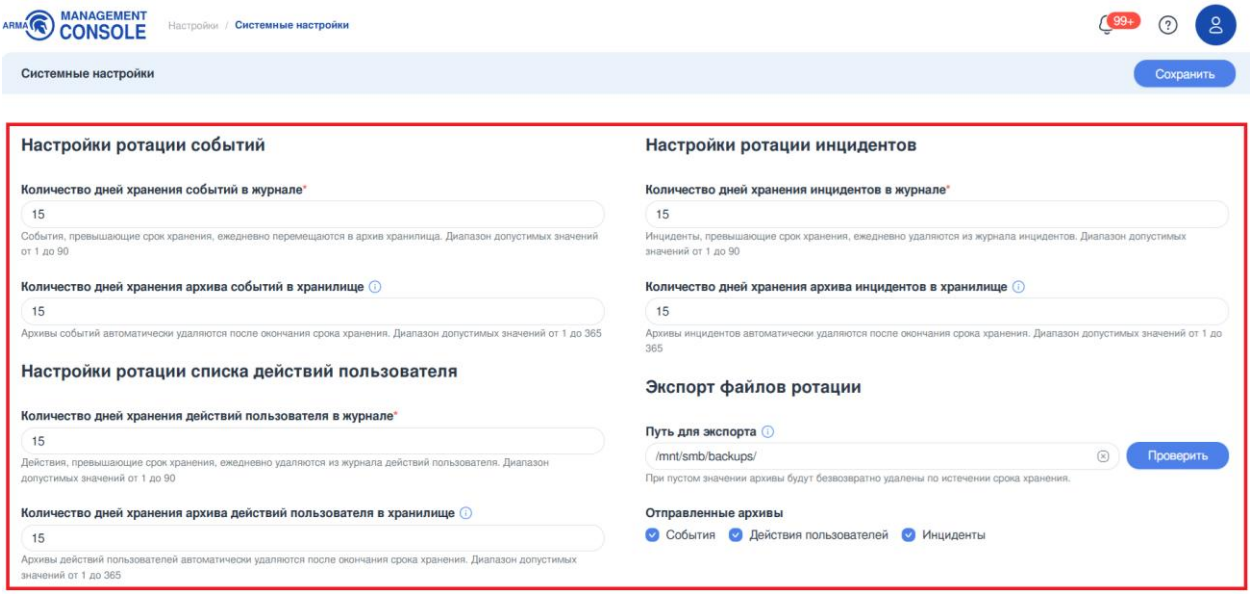


Рисунок – Настройки ротации

В области **Настройки ротации инцидентов** можно задать следующие параметры:

- **«Количество дней хранения инцидентов в журнале»** – как долго запись должна храниться в журнале;
- **«Количество дней хранения архива инцидентов в хранилище»** – как долго архив записей должен находиться в хранилище. Если поле не заполнено, хранилище не используется (инциденты безвозвратно удаляются при ротации).

Область **Настройки ротации событий** позволяет задать:

- **«Количество дней хранения событий в журнале»** – как долго запись должна храниться в журнале;
- **«Количество дней хранения архива событий в хранилище»** – как долго архив записей должен находиться в хранилище. Если поле не заполнено, хранилище не используется (события безвозвратно удаляются при ротации).

Область **Настройки ротации списка действий пользователя** позволяет задать:

- **«Количество дней хранения действий пользователя в журнале»** – как долго запись должна храниться в журнале;
- **«Количество дней хранения архива действий пользователя в хранилище»** – как долго архив записей должен находиться в хранилище. Если поле не заполнено, хранилище не используется (записи о действиях пользователя безвозвратно удаляются при ротации).

Примечание:

При указании значений, которые могут привести к ротации уже имеющихся данных, под полем выводится сообщение **«Уменьшение значения может привести к частичной потере данных в журнале»**.

Область **Экспорт файлов ротации** позволяет настроить выгрузку файлов ротации на внешний ресурс (подробнее см. Экспорт файлов ротации настоящего руководства).

Подробнее с логикой хранения можно ознакомиться далее.

15.1.3.1 Хранение в журнале

Для определения продолжительности хранения записи используется только дата её создания. Часы, минуты и секунды отбрасываются. Данные за день архивируются и уже в виде архива помещаются в хранилище. В случае если **«Количество дней хранения архива событий в хранилище»** не задано, архивация не производится и записи безвозвратно удаляются в момент ротации.

Например, в течение дня 5 мая в журнал было добавлено 99 событий, а значение **«Количество дней хранения событий в журнале»** равно **«5»**, следовательно 10 мая в 00:00 все 99 событий будут заархивированы и перемещены в хранилище.

Ротация записей инцидентов и действий пользователя выполняется аналогично.

Примечание:

Ротация производится в 00:00.

Если настройки хранения были изменены в сторону уменьшения так, что ротация каких-либо записей уже должна была произойти, записи будут обработаны при ротации в 00:00 следующего дня.

15.1.3.2 Хранение в хранилище

Продолжая пример из предыдущего параграфа, если **«Количество дней хранения архива событий в хранилище»** = **«10»**, то архив событий будет безвозвратно удалён 20 мая в 00:00. Общее время хранения информации о событии составит 15 дней (5 в журнале и 10 в архиве).

Если **«Количество дней хранения архива событий в хранилище»** не задано, записи удаляются в момент ротации (согласно примеру выше – 10 мая в 00:00).

> **Примечание**:
>
> Если поле **«Количество дней хранения архива событий в хранилище»** было очищено и оставлено пустым, или время хранения было уменьшено так, что имеющиеся архивы должны быть удалены, они удалятся в 00:00 следующего дня.

Ротация архивов инцидентов и действий пользователя выполняется аналогично.

15.1.3.3 Экспорт файлов ротации

Файлы архивов, предназначенные для удаления из хранилища в процессе ротации, можно вместо удаления сохранять на внешний ресурс, например, на внешний накопитель данных. Для этого достаточно выполнить следующие действия:

1. Смонтировать ресурс средствами операционной системы с учётом рекомендаций из раздела Монтирование внешнего ресурса Руководства администратора **ARMA MC**.
2. Заполнить поле **«Путь для экспорта»** в области настроек ротации (см. Рисунок – Настройки ротации).
3. Нажать кнопку **«Проверить»**, чтобы убедиться в наличии доступа. При успешной проверке появится всплывающее сообщение **«Путь доступен»**.
4. В разделе **«Отправленные архивы»** выбрать типы данных, которые следует сохранять.
5. Нажать кнопку **«Сохранить»** в правом верхнем углу окна системных настроек.

> **Примечание**:
>
> Данные об инцидентах бесполезны без данных о событиях, поэтому если требуется сохранять архивы инцидентов, следует сохранять и архивы событий.

15.2 Параметры экспорта

В настоящем разделе представлено описание подраздела меню **«Параметры экспорта»**, предусматривающего механизм управления параметрами экспорта инцидентов в сторонние системы.

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Настройки»**, затем подраздел **«Параметры экспорта»**.

Подраздел **«Параметры экспорта»** позволяет просматривать информацию о получателях автоматической отправки сообщений об инцидентах в формате таблицы, состоящей из следующих столбцов (см. Рисунок – Экспорт инцидентов):

- **«Наименование»** – наименование хоста;
- **«Статус»** – статус пользователя («Активно»/«Неактивно»);
- **«Хост»** – IP-адрес или DNS-имя;
- **«Порт»** – порт хоста;
- **«Протокол»** – протокол передачи («UDP»/«TCP»).

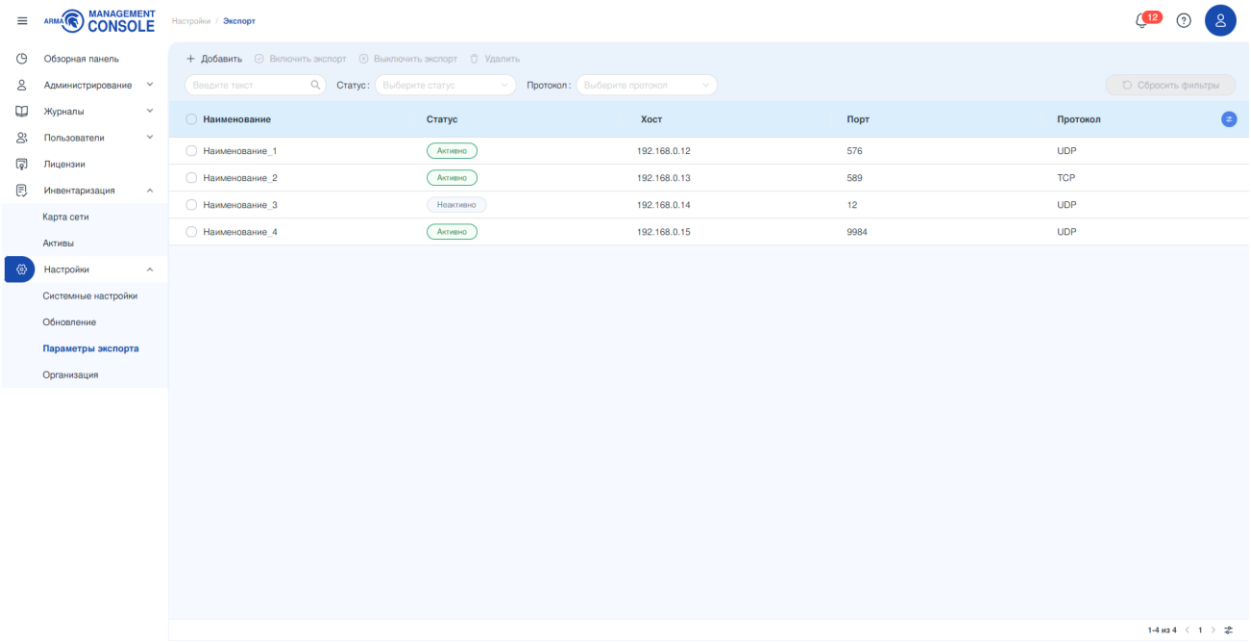


Рисунок – Экспорт инцидентов

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать кнопку **«Настройка столбцов»** и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

Порядок работы с информацией, представленной в формате таблицы описан в разделе Форма раздела меню. Таблица настоящего руководства.

15.2.1 Поиск и фильтрация получателей

Блок фильтрации на панели инструментов позволяет фильтровать записи по всем столбцам списка и состоит из следующих элементов (см. Рисунок – Блок фильтрации).

- поле **«Поиск»**;
- поле **«Статус»**;
- поле **«Протокол»**;
- кнопка **«Сбросить фильтры»**.

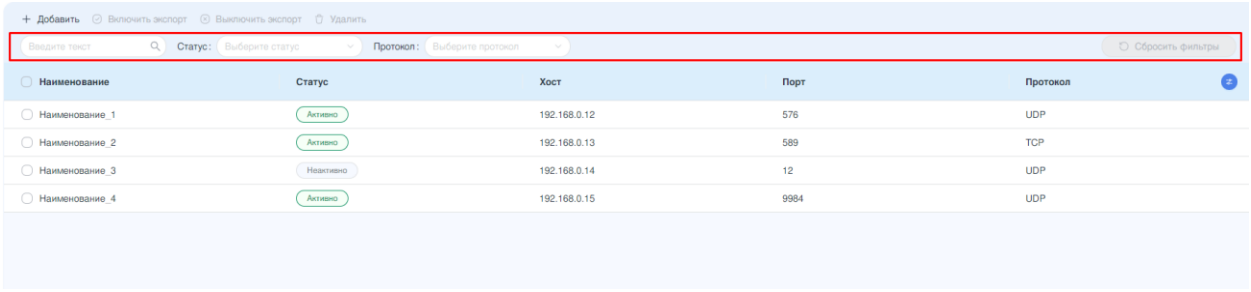


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем доступным столбцам таблицы.

Фильтрация по полю **«Статус»** позволяет отфильтровать получателей списка инцидентов по статусу получателя. Поле **«Статус»** содержит выпадающий список и предоставляет выбор из двух вариантов значений – **«Активно»** и **«Неактивно»**.

Фильтрация по полю **«Протокол»** позволяет отфильтровать получателей списка инцидентов по протоколу получателя. Поле **«Протокол»** содержит выпадающий список и предоставляет выбор из двух вариантов значений – **«TCP»** и **«UDP»**.

15.2.2 Добавить нового получателя

Для настройки экспорта инцидентов необходимо выполнить следующие действия (см. Рисунок – Добавление получателя списка инцидентов):

1. На панели инструментов нажать кнопку **«Добавить»** для создания нового получателя.
2. В открывшейся карточке **«Добавление получателя»** заполнить поля:
   - **«Наименование»** – может содержать латиницу, кириллицу, числа, спецсимволы, пробел и ограничено 100 символами;
   - **«Хост»** – ввести IP-адрес или DNS-имя;
   - **«Протокол»** – выбрать из двух значений – **«UDP»**/**«TCP»**;
   - **«Порт»** – указать значение из диапазона от 1 до 65535.

3. Нажать кнопку **«Сохранить»** в правом верхнем углу карточки.

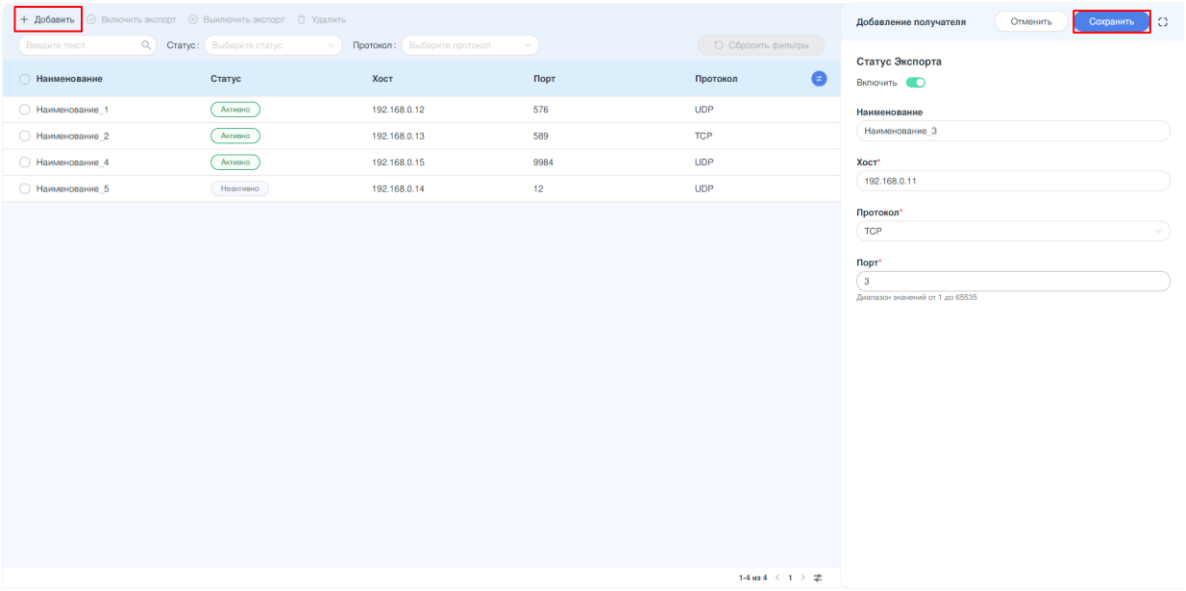


Рисунок – Добавление получателя списка инцидентов

В случае успешного добавления получателя списка инцидентов появится соответствующее уведомление (см. Рисунок – Успешное добавление получателя).

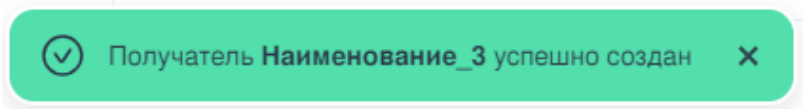


Рисунок – Успешное добавление получателя

15.2.3 Удалить получателя

Для удаления получателя необходимо установить флажок в чек-бокс рядом с наименованием получателя, нажать кнопку **«Удалить»** на панели инструментов и подтвердить удаление в появившемся окне (см. Рисунок – Удаление получателя списка инцидентов).

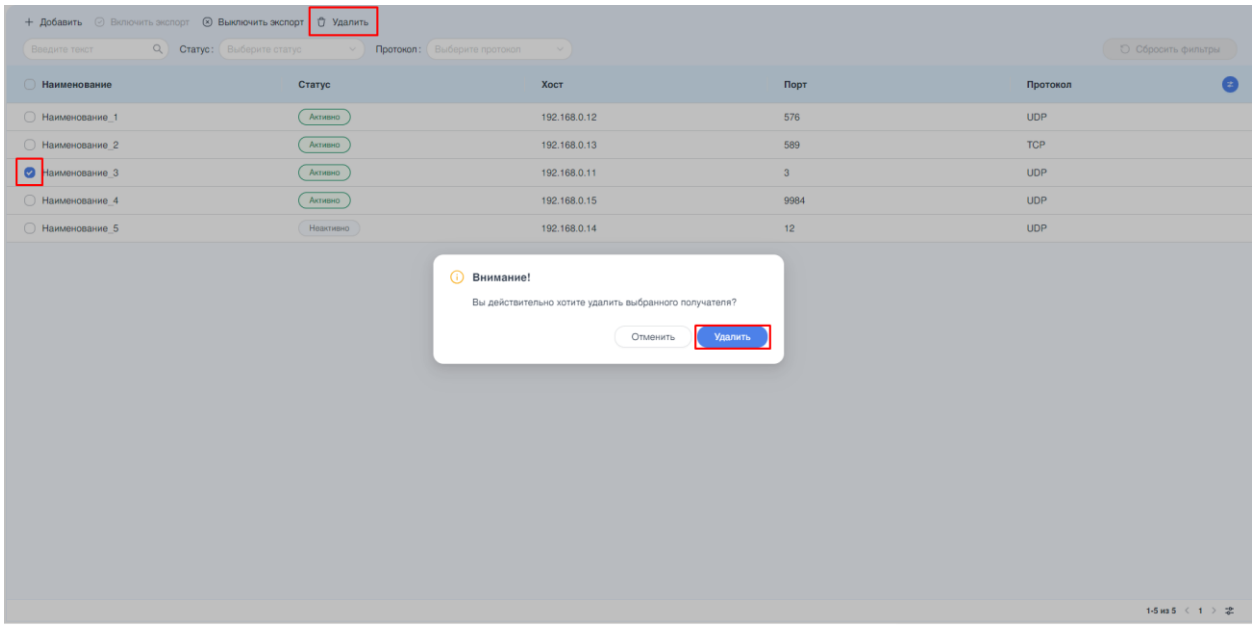


Рисунок – Удаление получателя списка инцидентов

В случае успешного удаления получателя списка инцидентов появится соответствующее уведомление (см. Рисунок – Успешное удаление получателя).

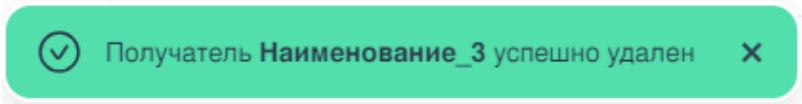


Рисунок – Успешное удаление получателя

15.2.4 Включение и выключение экспорта

Существует возможность одновременного включения/выключения экспорта для одного или нескольких получателей без необходимости открытия карточки каждого. Для этого необходимо установить флажок в чек-боксы рядом с наименованиями необходимых получателей и нажать кнопку **«Включить экспорт»**/кнопку **«Выключить экспорт»** на панели инструментов (см. Рисунок – Выключение экспорта для нескольких получателей).

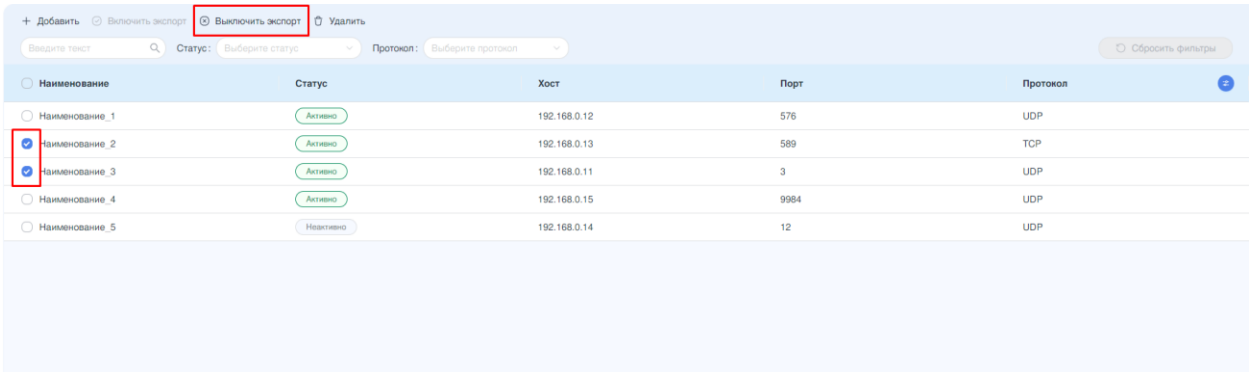


Рисунок – Выключение экспорта для нескольких получателей

15.3 Обновление версии

Обновление необходимо для замены **ARMA MC** на новую версию.

В случае прерывания обновления произойдёт откат к предыдущей версии **ARMA MC** с сохранением всех данных и установленных настроек.

15.3.1 Подготовка к обновлению

Данный параграф относится к случаю, когда **ARMA MC** обновляется с версии **«1.8»** (в т.ч. **«1.8.2»**) на версию **«2.1»**.

До начала обновления необходимо выполнить следующее:

1. Сохранить архивы ротации через интерфейс хранилища (см. Хранилище настоящего руководства).

   Примечание:

   В связи с обновлением системы ротации старые форматы архивов перестанут быть доступны в версии **«2.1»**. Хотя эти данные не будут доступны через веб-интерфейс, они могут занимать место на диске. Порядок удаления описан в разделе Удаление устаревших данных после обновления Руководства администратора **ARMA MC**.

2. Проверить версию ОС.

   Примечание:

   Минимальная поддерживаемая версия ОС – **«Debian 11.9»**, тестирование обновления проводилось на версии **«Debian 11.11»**. Проверить версию можно с помощью команды cat /etc/debian_version. Если версия ниже **«Debian 11.9»**, необходимо обновить систему как минимум до **«Debian 11.9»**.

3. Установить пакет **«UFW»** для ОС (если он ещё не установлен).

   Примечание:

   Наличие **«UFW»** критично для проведения обновления. Установка пакета должна производиться администратором системы, например, с помощью команды sudo apt install ufw. Проверить наличие и активный статус службы **«UFW»** можно командой: systemctl status ufw (в выдаче должно присутствовать **Active: active**).

4. Проверить наличие и версию **«elasticsearch»**.

   Примечание:

   Пакет **«elasticsearch»** уже должен быть в системе, но если версия была обновлена в процессе обслуживания системы, при обновлении **ARMA MC** могут возникнуть ошибки. Для проверки версии можно использовать

команду usr/share/elasticsearch/bin/elasticsearch –version. Версия должна быть строго **«7.12.0»**. Если версия отличается, нужно установить **«7.12.0»** (см. п.3 параграфа Установка Руководства администратора **ARMA MC**).

Пункты 2, 3 и 4 должны выполняться администратором ОС.

К обновлению можно приступать только после выполнения всех перечисленных пунктов.

15.3.2 Обновление ARMA MC

Для перехода в подраздел меню на панели навигации необходимо выбрать раздел меню **«Настройки»**, затем – подраздел **«Обновления»** (см. Рисунок – Обновление).

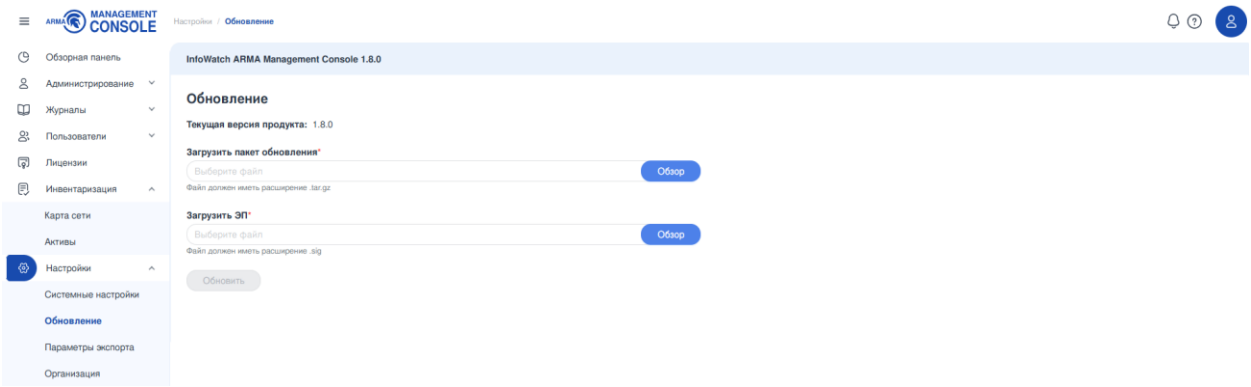


Рисунок – Обновление

Для обновления **ARMA MC** на версию выше необходимо выполнить следующие действия:

1. В поле **«Загрузить пакет обновления»** нажать кнопку **«Обзор»**, в открывшемся окне Проводника выбрать необходимый пакет обновления. Формат файла **«tar.gz»** (см. Рисунок – Загрузка пакета обновления).

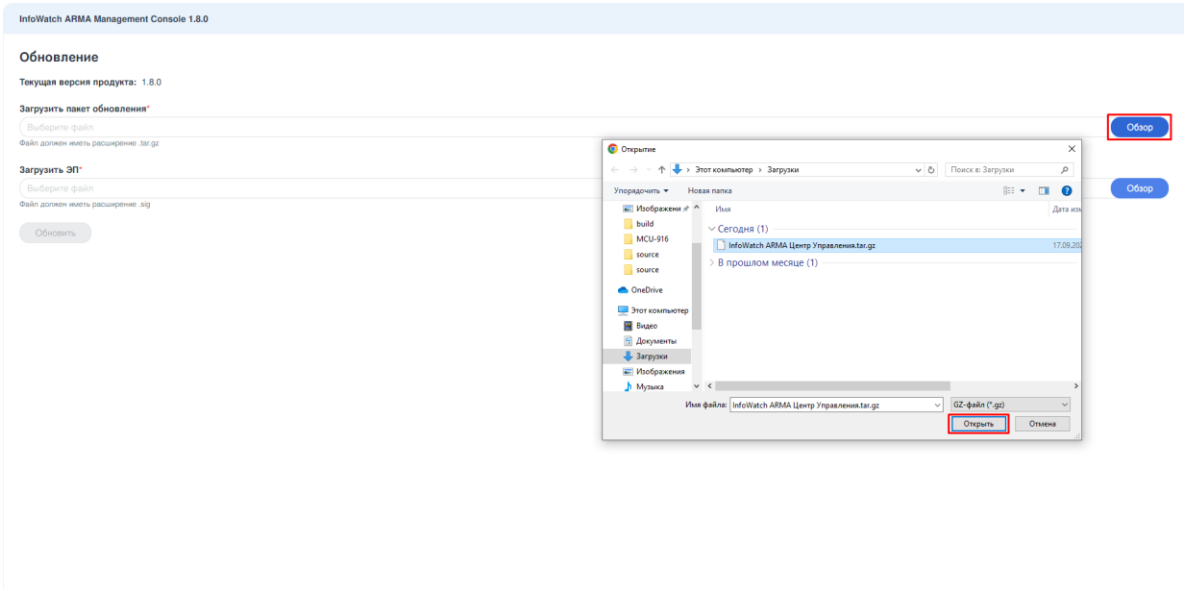


Рисунок – Загрузка пакета обновления

2. В поле **«Загрузить ЭП»** нажать кнопку **«Обзор»**, в открывшемся окне Проводника выбрать необходимый файл подписи. Формат файла **«sig»** (см. Рисунок – Загрузка ЭП).

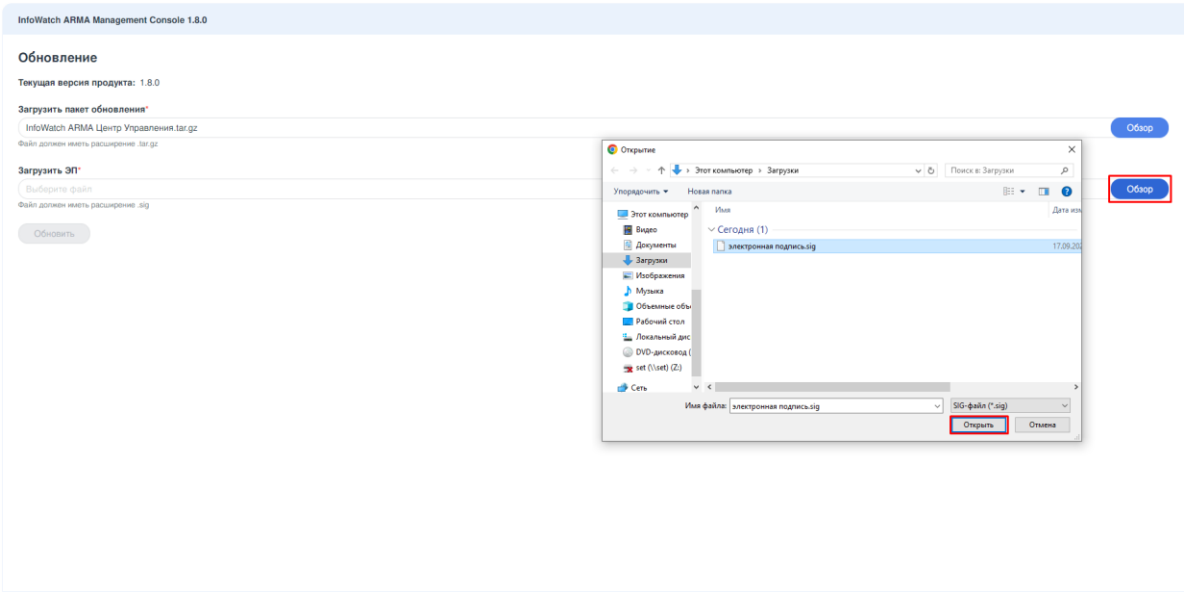


Рисунок – Загрузка ЭП

3. Нажать кнопку **«Обновить»**.

После запуска процесса обновления появится индикатор выполнения обновления и уведомление **«Внимание! При обновлении страницы в процессе загрузки пакета скачивание будет прервано. Запустите его заново»** (см. Рисунок – Индикатор выполнения обновления).

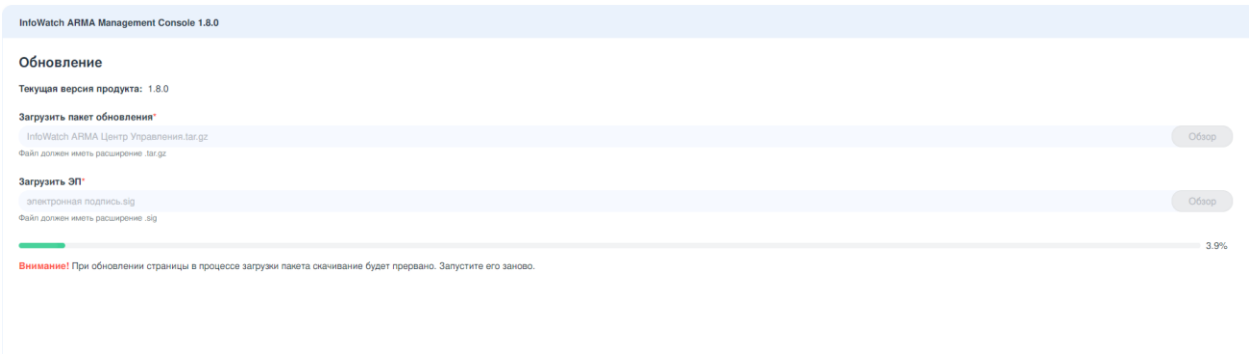


Рисунок – Индикатор выполнения обновления

Во время обновления **ARMA MC** появится информационный баннер **«Внимание! Выполняется процесс обновления. Все сервисы остановлены, система будет недоступна для использования. Пожалуйста, подождите»** (см. Рисунок – Процесс обновления):

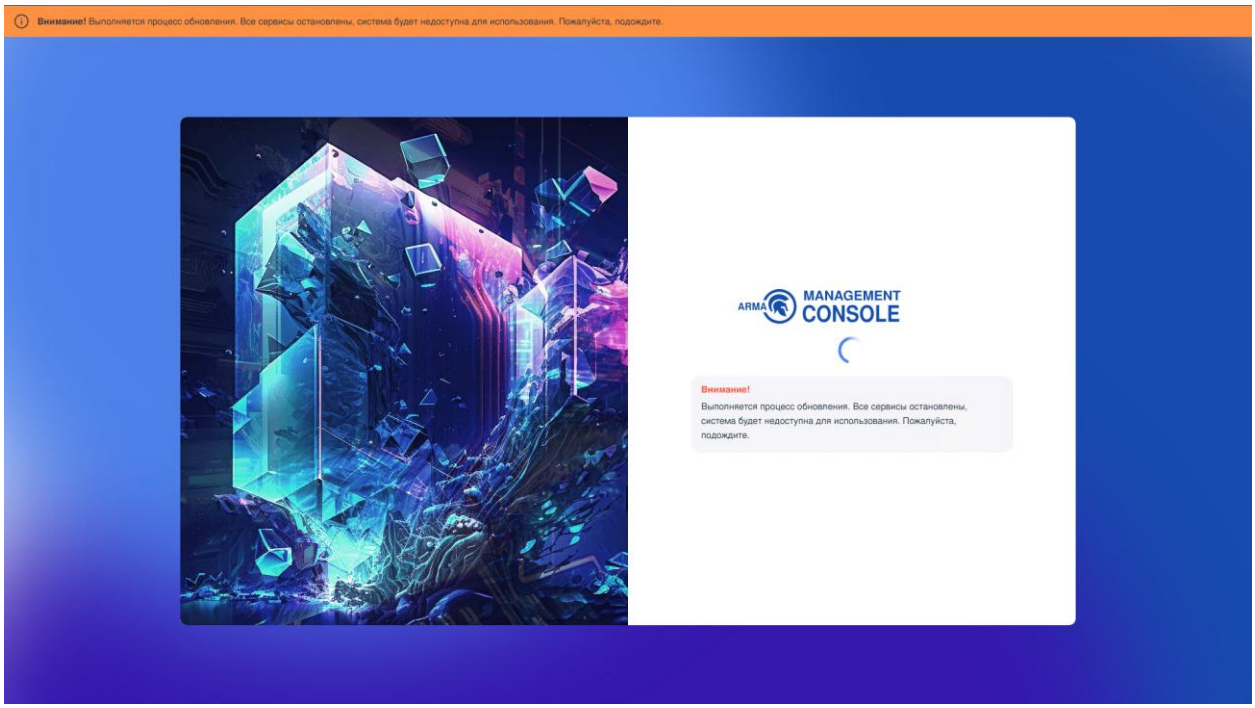


Рисунок – Процесс обновления

Примечание:

Не рекомендуется перезагружать сервер во время обновления. Процесс обновления может занять длительное время.

После завершения процесса обновления произойдёт перезапуск сервисов и перезагрузка **ARMA MC** (см. Рисунок – Перезагрузка сервисов), затем будет отображена страница авторизации (см. Рисунок – Страница авторизации в веб-интерфейсе).

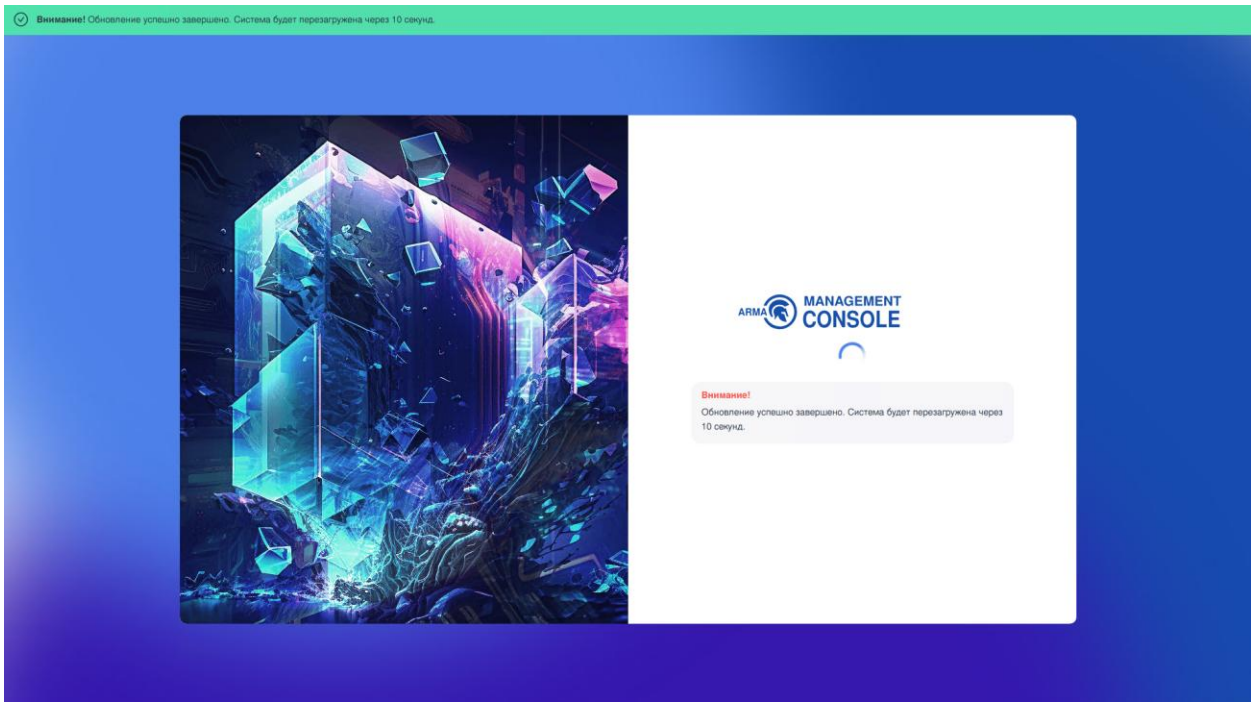


Рисунок – Перезагрузка сервисов

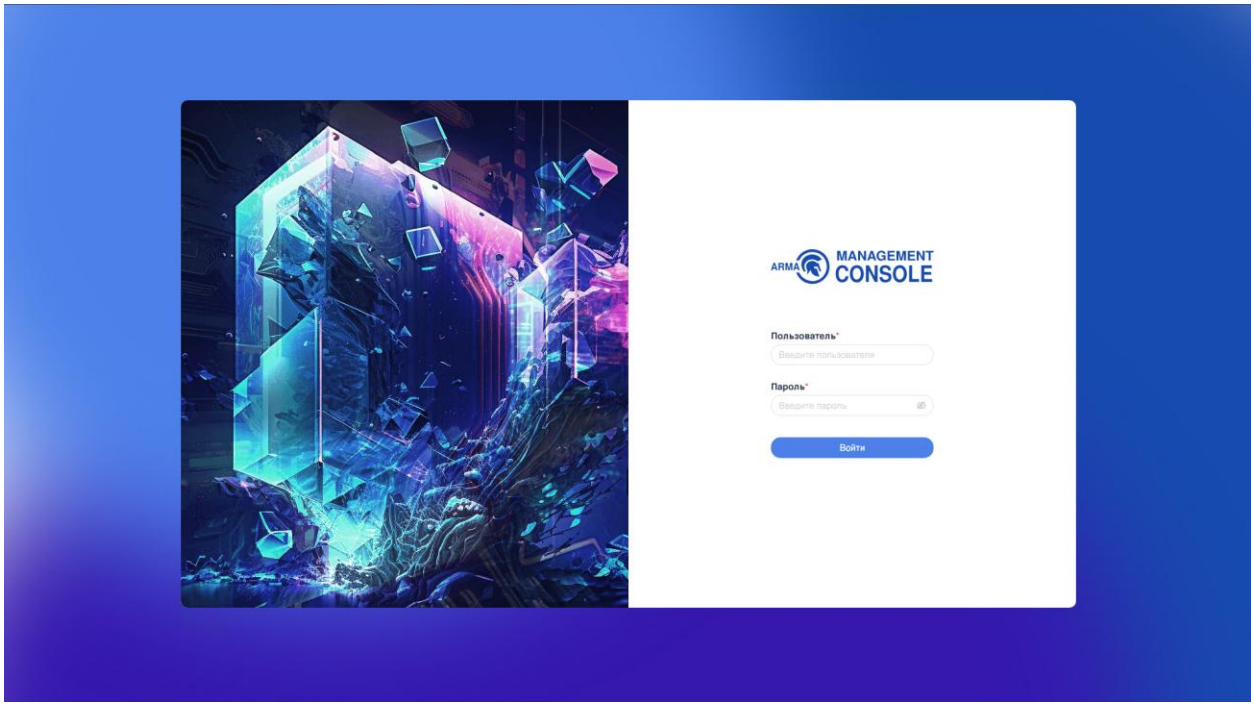


Рисунок – Страница авторизации в веб-интерфейсе