Руководство пользователя по эксплуатации

версия 36 ред. от 14.12.2022

Листов 81

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем документе использованы определения, представленные в таблице (см. Таблица 1).

Таблица 1
Термины и сокращения

Термины и сокращения	Значение
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак
КИИ	Критическая информационная инфраструктура
МЭ	Межсетевой экран
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
УЗ	Учётная запись
ЦП	Центральный процессор
API	Application Programming Interface – программный интерфейс приложения
ARMA IE	InfoWatch ARMA Industrial Firewall
ARMA IF	InfoWatch ARMA Industrial Endpoint
ARMA MC	InfoWatch ARMA Management Console
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
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
ID	Идентификатор

Термины и сокращения	Значение
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
MAC-адрес	Уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях
SID	Security IDentifier, идентификатор безопасности
TLS	Transport Layer Security, протокол защиты транспортного уровня

В настоящем документе использованы ссылки на документы, представленные в таблице (см. Таблица 2).

Таблица 2

Смежные документы

Сокращенное наименование	Полное наименование
Руководство администратора ARMA MC	Руководство администратора InfoWatch ARMA Management Console
Руководство пользователя ARMA IF	Руководство пользователя по эксплуатации InfoWatch ARMA Industrial Firewall
Руководство пользователя ARMA IE	Руководство пользователя по эксплуатации InfoWatch ARMA Industrial Endpoint

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Management Console v.1.4.3**.

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.

1 ОПИСАНИЕ ВЕБ-ИНТЕРФЕЙСА

Общий вид веб-интерфейса **ARMA MC** представлен на рисунке (см. Рисунок 1).

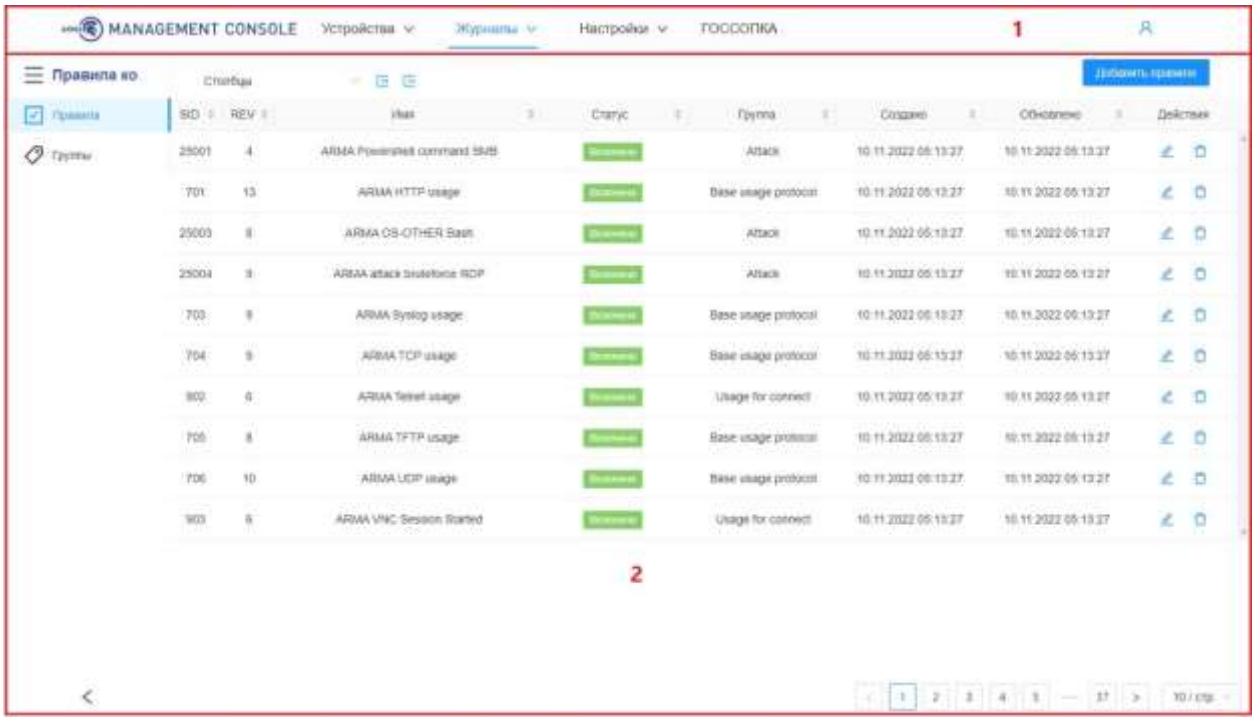

Рисунок 1 – Веб-интерфейс ARMA MC

Основные разделы веб-интерфейса:

- область навигации (**1**);
- форма раздела меню (**2**).

Информация о порядке работы в **ARMA MC** изложена в следующих разделах настоящего руководства:

- **«Просмотр журнала событий»** (см. Раздел 2);
- **«Расследование инцидентов»** (см. Раздел 3);
- **«Просмотр архивов»** (см. Раздел 4);
- **«Настройка правил корреляции»** (см. Раздел 5);
- **«Настройка ротации журналов»** (см. Раздел 6);
- **«Системные настройки»** (см. Раздел 7);
- **«Управление лицензиями»** (см. Раздел 8);
- **«Управление источниками событий»** (см. Раздел 9);
- **«Управление списком устройств сети»** (см. Раздел 10);
- **«Управление учетными записями»** (см. Раздел 11);
- **«Управление ГОССОПКой»** (см. Раздел 12);

- **«Сообщения пользователю»** (см. Раздел 13).

1.1 Область навигации

Область быстрой навигации **ARMA MC** представлена на рисунке (см. Рисунок 2).

Рисунок 2– Область навигации

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

- логотип **ARMA MC** (**1**);
- область меню (**2**);
- меню пользователя (**3**);

1.1.1 Область меню

Область меню предназначена для осуществления доступа к различным функциям **ARMA MC**, переход к которым осуществляется нажатием **левой кнопки мыши**.

В меню существует следующие уровни вложенности:

- **«вкладка»**;
- **«группа разделов»** – присутствует не во всех вкладках;
- **«пункт перехода в раздел»**.

Пример уровней вложенности представлен на рисунке (см. Рисунок 3):

- **«Настройки»** – вкладка;
- **«Журналы»** – группа разделов;
- **«Ротация»**/**«Хранилище»** – пункт перехода в раздел.

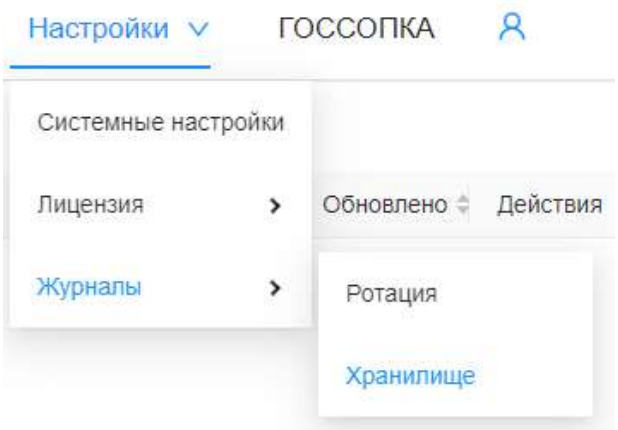

Рисунок 3 – Пример уровней вложенности

1.1.2 Меню пользователя

Меню пользователя выполняет следующие функции:

- отображение имени профиля текущего пользователя;
- переход в разделы управления пользователями;
- выход из веб-интерфейса.

Для выхода из веб-интерфейса необходимо нажать **кнопку «** **»**, а затем нажать **кнопку «Выход»**.

1.2 Форма раздела меню

В качестве примера представлена форма раздела **«Настройки ротации»** (см. Рисунок 4).

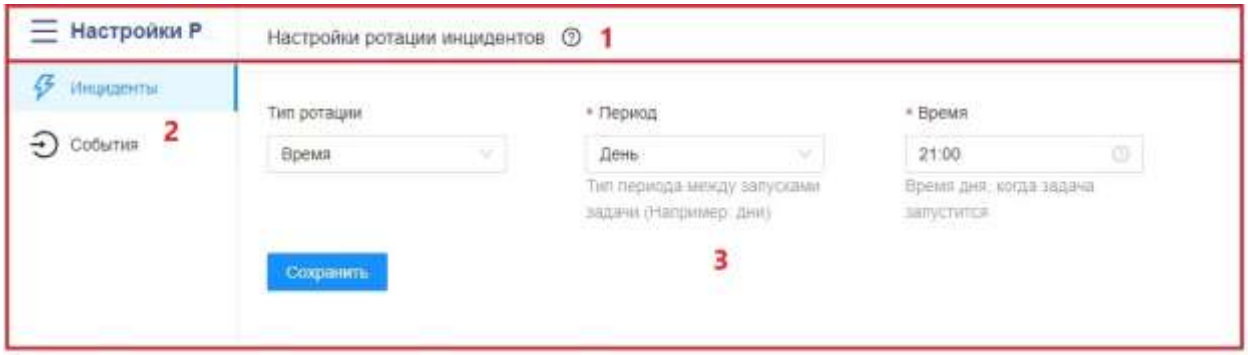

Рисунок 4 – Форма раздела меню

Форма раздела меню содержит:

- название раздела (**1**);
- область навигации (**2**);
- содержание раздела (**3**) – может содержать несколько блоков.

Символ красной звёздочки **«*»** в названии параметра означает необходимость указать значение данного параметра.

1.3 Работа с карточками

Работа с карточками доступна в двух вариантах:

- в сайт-баре;
- в полноэкранном режиме.

При нажатии на строку в журнале производится открытие свернутой карточки (сайт-бар) в правом углу экрана (см. Рисунок 5).

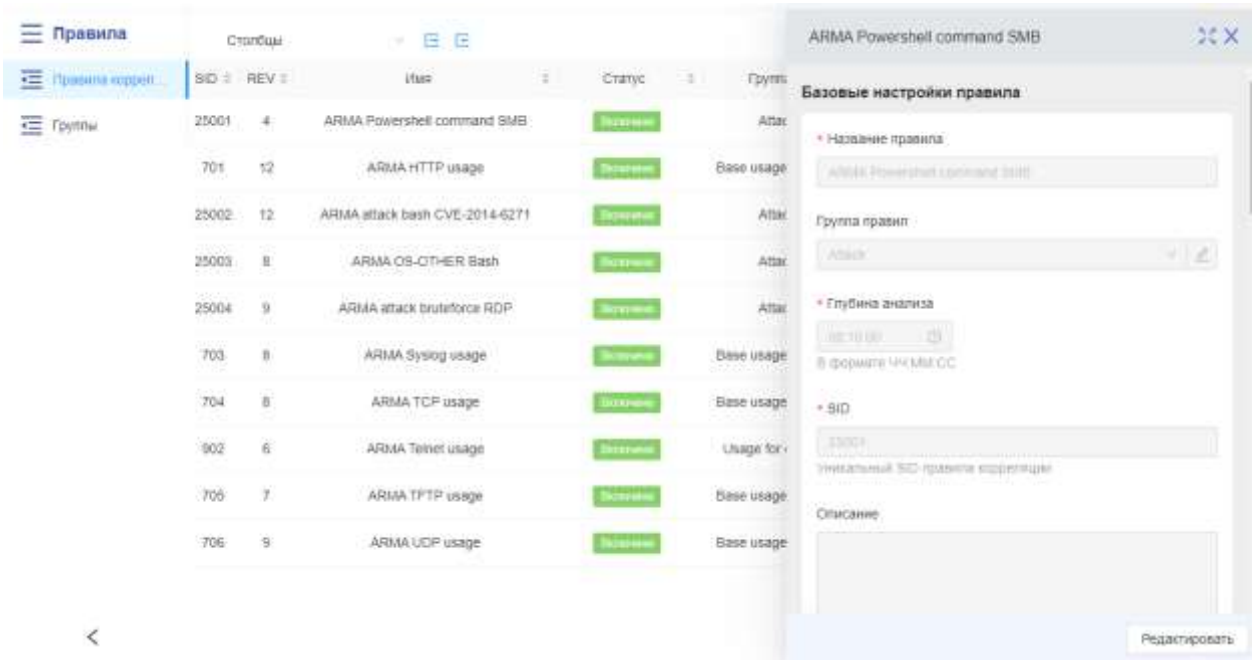

Рисунок 5 – Карточка (сайт-бар)

При нажатии **кнопки «** **»** в правом верхнем углу формы производится открытие карточки в полноэкранном режиме (см. Рисунок 6).

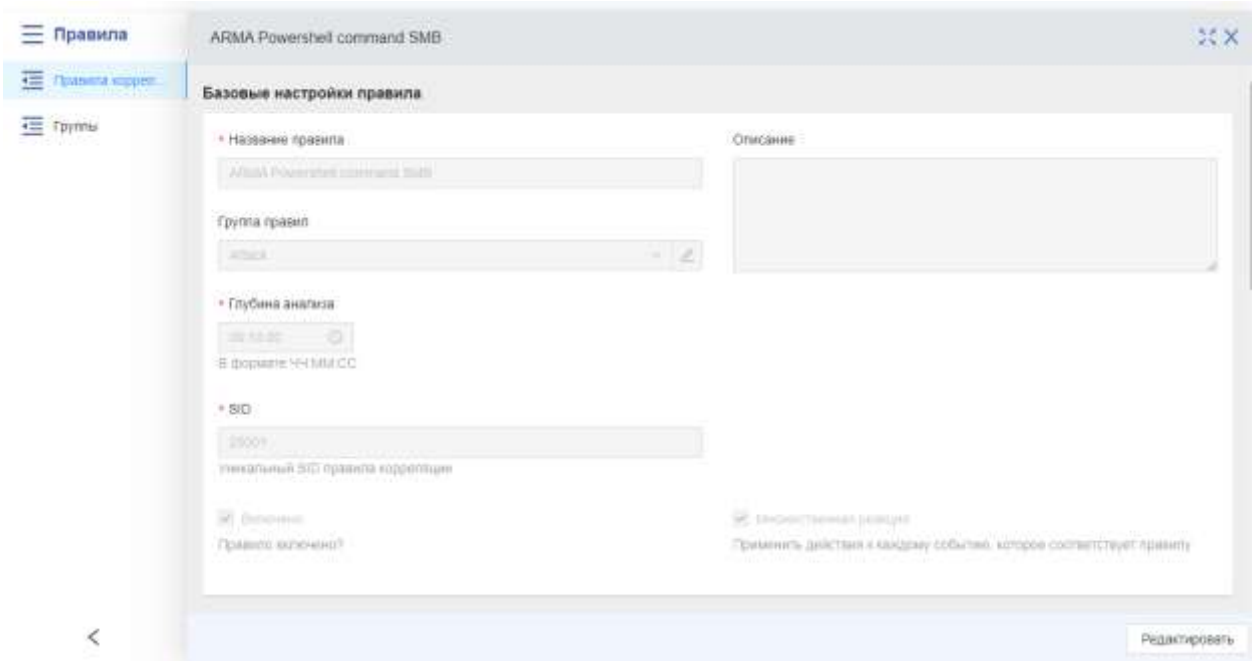

Рисунок 6 – Карточка (полноэкранный режим)

Для возврата к свернутой карточки (сайт-бар) необходимо нажать **кнопку «** **»**.

1.4 Работа с информацией, представленной в виде таблицы

В значительной части разделов и форм **ARMA MC** информация представлена в виде таблицы, например, в разделе **«Правила корреляции** (см. Рисунок 7).

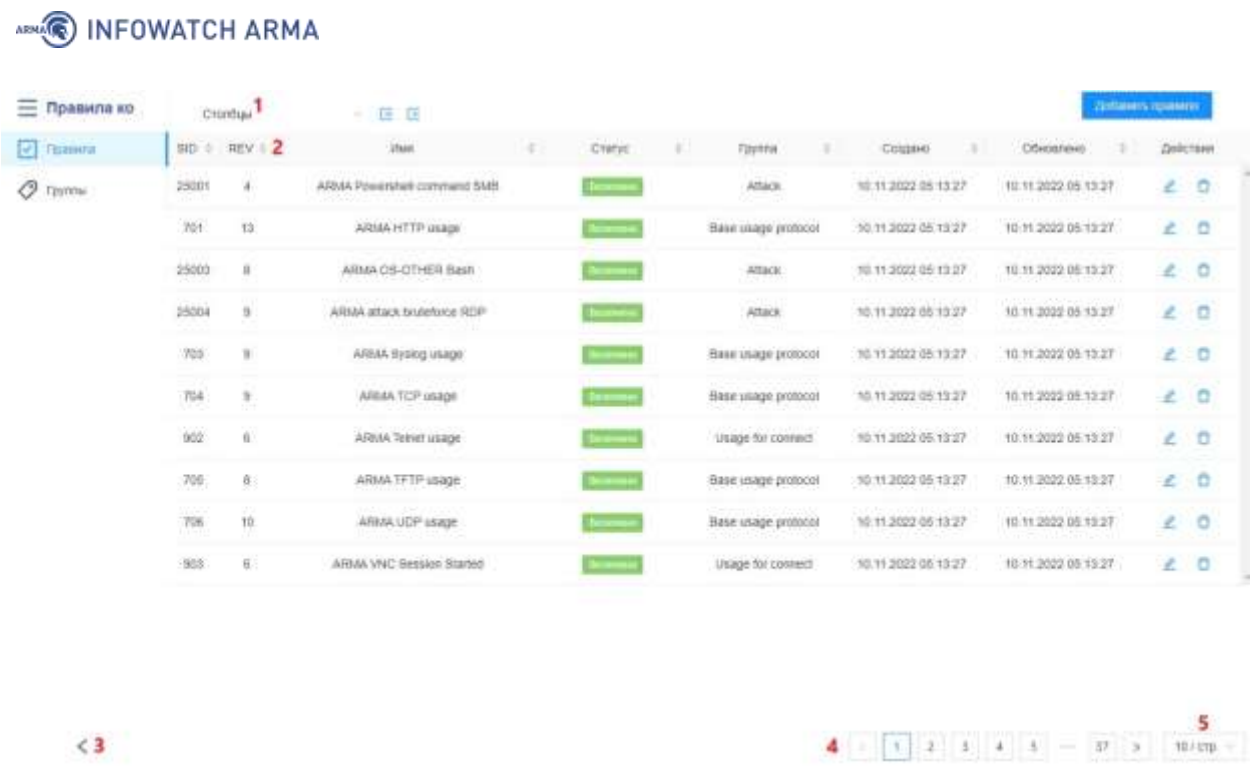

Рисунок 7 – Раздел «Правила корреляции» в виде таблицы

В подобных разделах существуют следующие возможности:

- выбирать отображаемые столбцы (**1**);
- сортировать данные в столбцах (**2**);
- сворачивать/разворачивать меню (**3**);
- переходить к предыдущей или следующей странице с записями (**4**);
- выбирать количество отображаемых записей (**5**).

1.4.1 Выбор отображаемых столбцов

Настройка отображаемых столбцов осуществляется с помощью **кнопки «Столбцы»** и последующим выбором в выпадающем списке отображаемых столбцов (см. Рисунок 8).

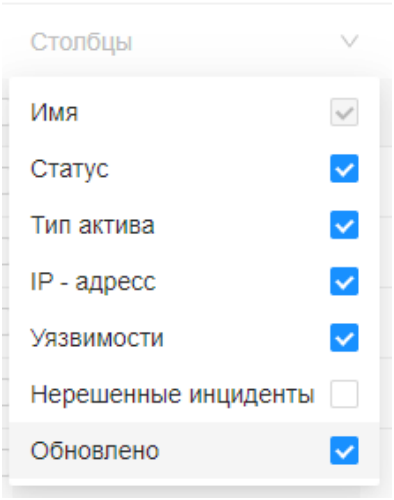

Рисунок 8 – Выбор отображаемых столбцов

1.4.2 Выбор количества отображаемых записей

Для выбора количества отображаемых записей в таблице необходимо указать количество записей в выпадающем списке снизу таблицы (см. Рисунок 9).

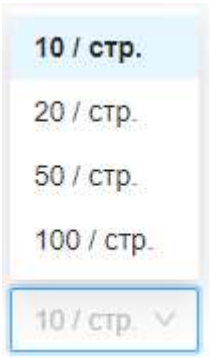

Рисунок 9 – Выбор количества отображаемых записей

1.4.3 Сортировка данных в столбцах

Сортировка данных по столбцу осуществляется нажатием **кнопки «**  **»** рядом с названием столбца.

1.4.4 Переход к предыдущим и следующим страницам с записями

Для перехода к предыдущей и следующей странице с записями необходимо нажать **кнопки «**  **»** и **«**  **»** соответственно. Порядковый номер текущей страницы отображен между данных кнопок (см. Рисунок 10).

Рисунок 10 – Порядковый номер текущей страницы

2 ПРОСМОТР ЖУРНАЛА СОБЫТИЙ

В разделе **«Журнал событий»** (см. Рисунок 11) отображаются события устройств, подключенных к **ARMA MC**.

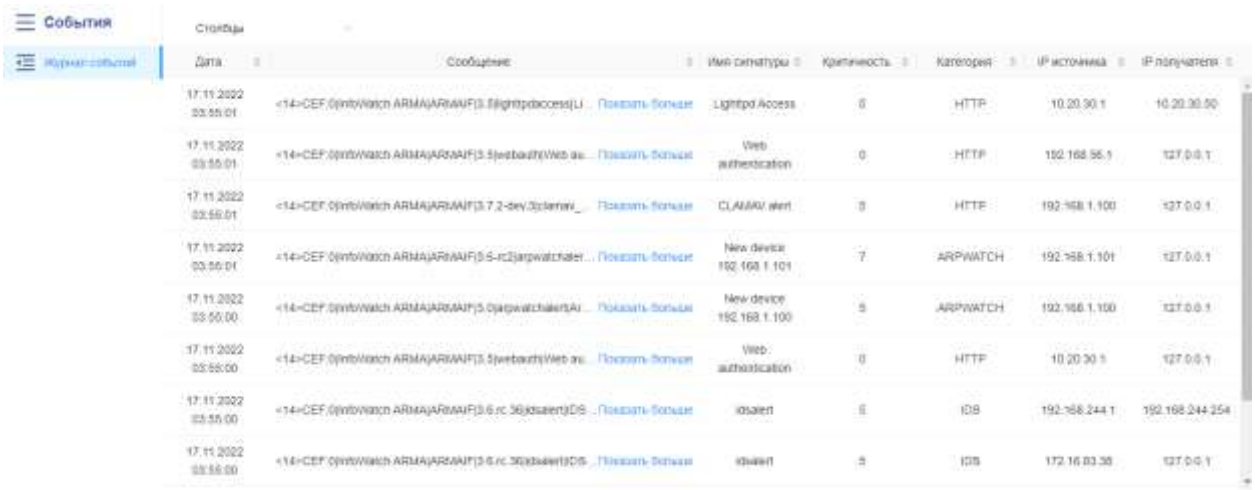

Рисунок 11 – Журнал событий

Для перехода в раздел необходимо развернуть вкладку **«Журналы»** и выбрать пункт **«События»**.

2.1 Описание журнала событий

Раздел позволяет просматривать журнал событий в формате таблицы, содержащей столбцы со следующими данными:

- **«Дата»**;
- **«Сообщение»**;
- **«Имя сигнатуры»**;
- **«Критичность»**;
- **«Категория»**;
- **«IP источника»**;
- **«IP получателя»**.

!Важно Если количество записей в журнале событий превышает 10000 записей, то последующие страницы таблицы журнала будут неактивны и появится соответствующее уведомление (см. Рисунок 106).

2.2 Поиск событий

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

Для корректного формирования запроса при заполнении поисковой строки предоставляются подсказки быстрого заполнения с вариантом выбора (см. Рисунок 12).

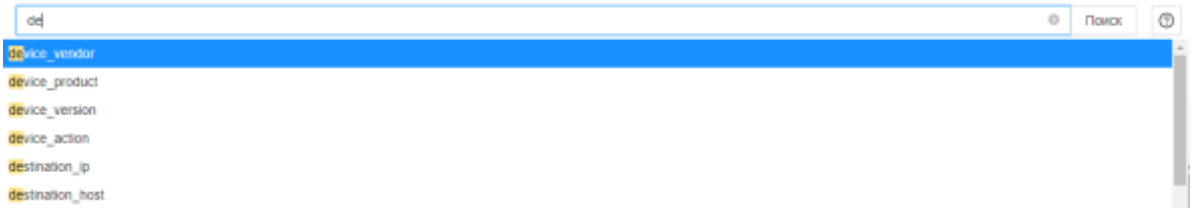

Рисунок 12 – Подсказки при заполнении поисковой строки

В строке возможно создать запрос с помощью специального синтаксиса. Описание синтаксиса запроса, примеры используемых операторов и наименования используемых полей доступны при нажатии **кнопки «** **»**.

2.3 Просмотр подробной информации о событии

Для просмотра подробной информации о событии необходимо нажать **левой кнопкой мыши** на запись с нужным событием. В результате будет отображена форма **«Событие [ID]»**, состоящая из таблицы, содержащей следующие блоки:

1. **«Основное»** (см. Раздел 2.3.1).
2. **«Источник»** (см. Раздел 2.3.2).
3. **«Получатель»** (см. Раздел 2.3.3).
4. **«Устройство»** (см. Раздел 2.3.4).
5. **«Дополнительно»** (см. Раздел 2.3.5).

2.3.1 Блок «Основное»

Блок содержит основную информацию о событии (см. Рисунок 13).

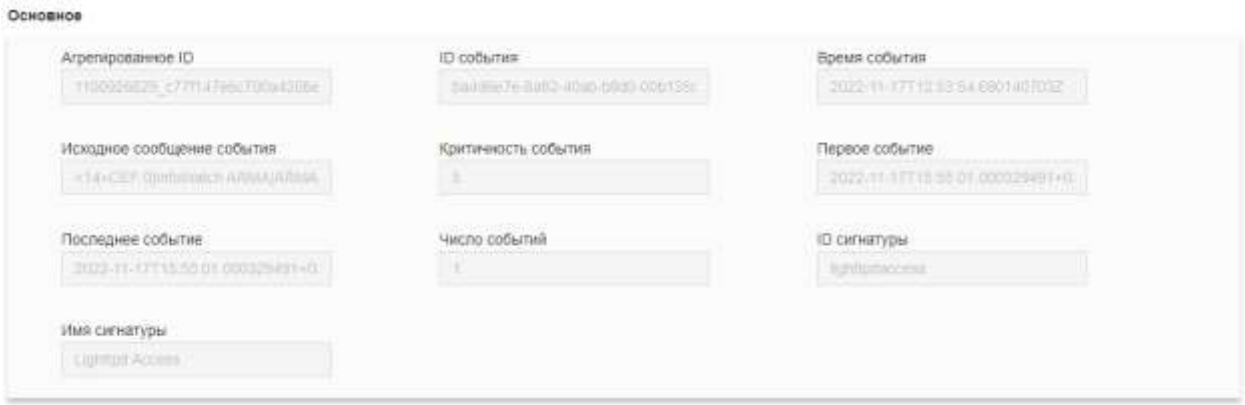

Рисунок 13 – Детали события. Основное

2.3.2 Блок «Источник»

Блок содержит информацию об источнике, которое регистрирует событие (см. Рисунок 14).

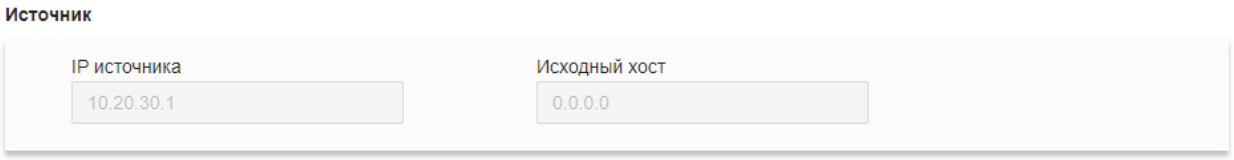

Рисунок 14 – Детали события. Источник

2.3.3 Блок «Получатель»

Блок содержит информацию о получателе события (см. Рисунок 15).

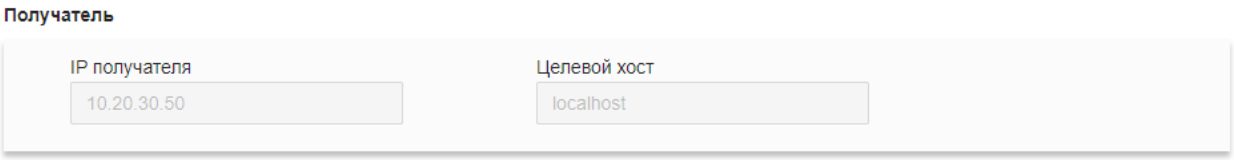

Рисунок 15 – Детали события. Получатель

2.3.4 Блок «Устройство»

Блок содержит информацию об устройстве, с которого получено событие, включающее в себя следующие данные (см. Рисунок 16):

- **«Версия устройства»**;
- **«Действие устройства»**;
- **«Модуль устройства»**;
- **«Производитель устройства»**.

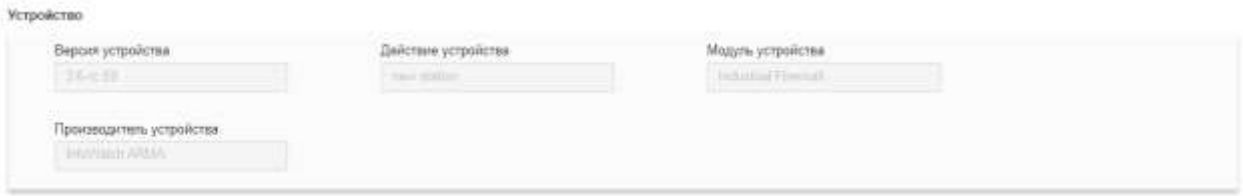

Рисунок 16 – Детали события. Устройство

2.3.5 Блок «Дополнительно»

Блок содержит дополнительную информацию о событии (см. Рисунок 17):

- **«Хэш события»**;
- **«Тип события»**;
- **«Категория сигнатуры»**;
- **«Подкатегория сигнатуры»**.

Рисунок 17 – Детали события. Дополнительно

3 РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

В разделе **«Инциденты»** (см. Рисунок 18) отображаются инциденты устройств, подключенных к **ARMA MC**.

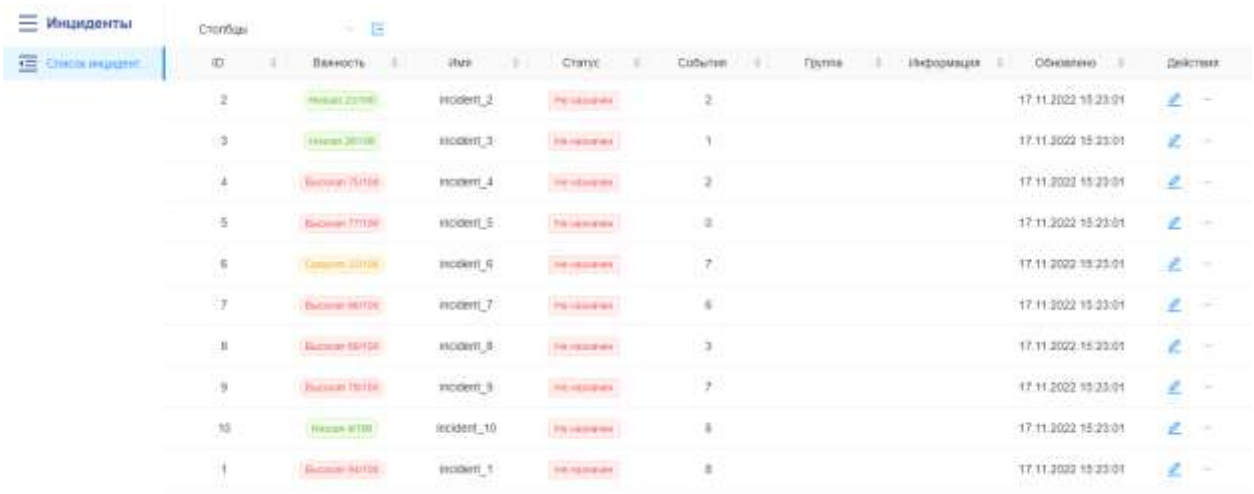

Рисунок 18 – Журнал инцидентов

Для перехода в раздел необходимо развернуть вкладку **«Журналы»** и выбрать пункт **«Инциденты»**.

3.1 Описание журнала инцидентов

Раздел позволяет просматривать журнал инцидентов в формате таблицы, содержащей столбцы со следующими данными:

- **«ID»**;
- **«Важность»**;
- **«Имя»**;
- **«Группа»**;
- **«Статус»**;
- **«События»**;
- **«Информация»**;
- **«Обновлено»**;
- **«Действия»**.

В журнале отображаются следующие инциденты:

- решенные;
- решенные назначенные на пользователя;
- решенные назначенные на других пользователей;

- решенные не назначенные ни на кого;
- нерешенные назначенные на пользователя;
- нерешенные назначенные на других пользователей;
- нерешенные не назначенные ни на кого;
- ложного срабатывания.

3.2 Просмотр подробной информации об инциденте

Для просмотра подробной информации об инциденте необходимо нажать **левой кнопкой мыши** на запись с нужным инцидентом. В результате будет отображена форма **«[Имя инцидента]»**, содержащая подробную информацию об инциденте и включающая следующие блоки:

1. **«Основные»** (см. Раздел 3.2.1).
2. **«Детали»** (см. Раздел 3.2.2).
3. **«Рекомендации»** (см. Раздел 3.2.3).
4. **«Последствия»** (см. Раздел 3.2.4).
5. **«События»** (см. Раздел 3.2.5).

В случае решения инцидента необходимо нажать **кнопку «Решен»** или выбрать значение «Решен» из выпадающего списка параметра **«Статус»** блока **«Детали»** (см. Раздел 3.2.2).

Для отправки уведомления об инциденте в НКЦКИ необходимо нажать **кнопку «Отправить в ГосСОПКА»** (см. Раздел 12.2.2).

3.2.1 Блок «Основные»

Блок содержит основную информацию об инциденте (см. Рисунок 19).

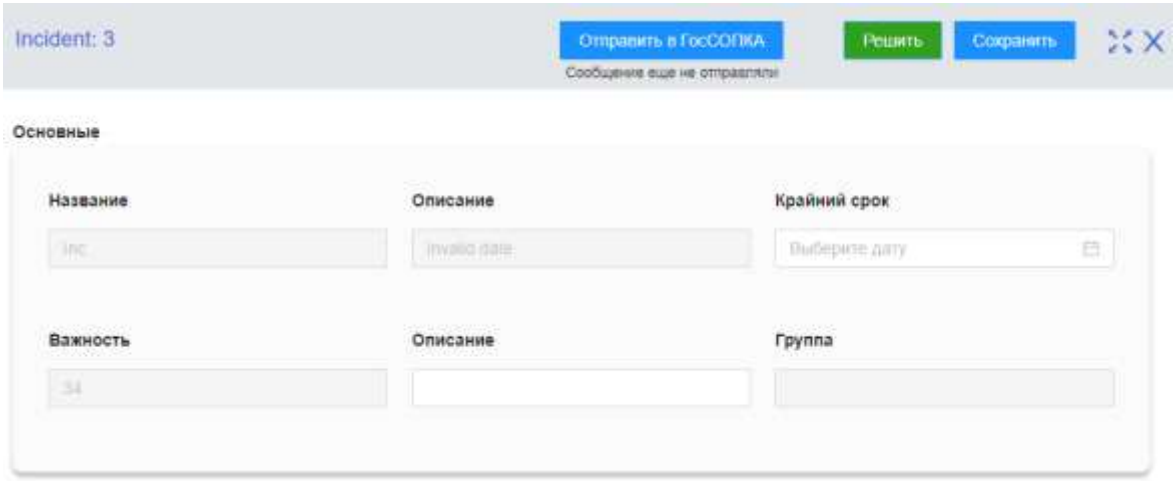

Рисунок 19 – Информация об инциденте. Основные

Поля параметров **«Название»**, **«Важность»**, **«Описание»** и **«Группа»** не подлежат редактированию.

3.2.2 Блок «Детали»

Блок содержит детали инцидента (см. Рисунок 20).

Рисунок 20 – Информация об инциденте. Детали

В выпадающем списке параметра **«Статус»** выбирается один из возможных статусов инцидента:

- **«Не назначен»**;
- **«Назначен»**;
- **«Отложен»**;
- **«Решен»**;
- **«Ложное срабатывание»**.

Для сохранения изменений в случае редактирования полей параметров необходимо нажать **кнопку «Сохранить»**.

3.2.3 Блок «Рекомендации»

Блок содержит рекомендации для закрытия инцидента (см. Рисунок 21).

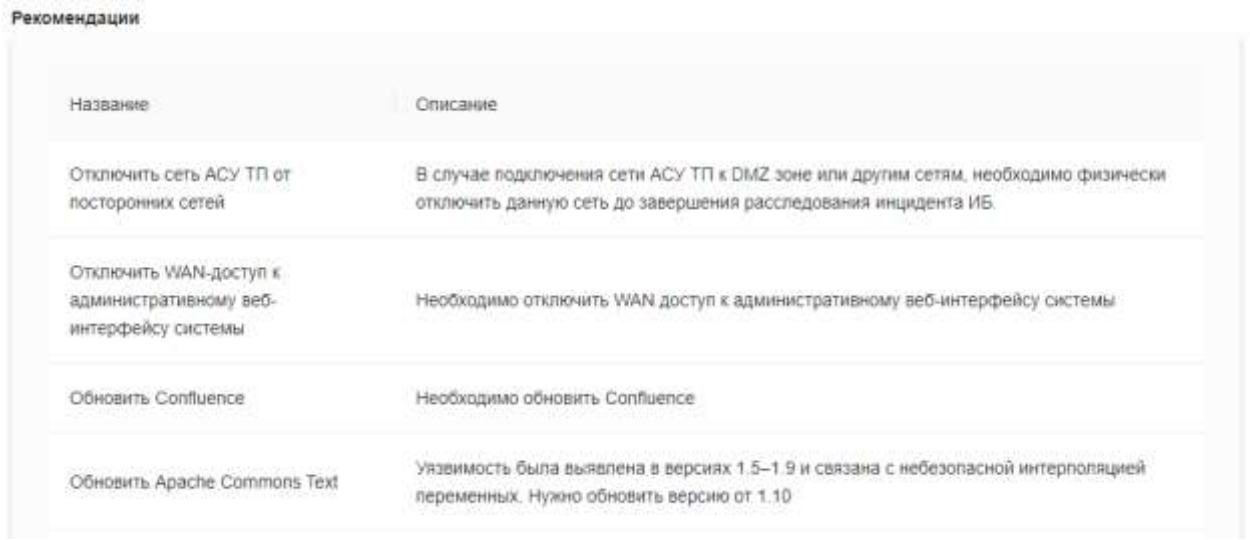

Рисунок 21 – Информация об инциденте. Рекомендации

3.2.4 Блок «Последствия»

Блок содержит информацию о возможных последствиях инцидента (см. Рисунок 22).

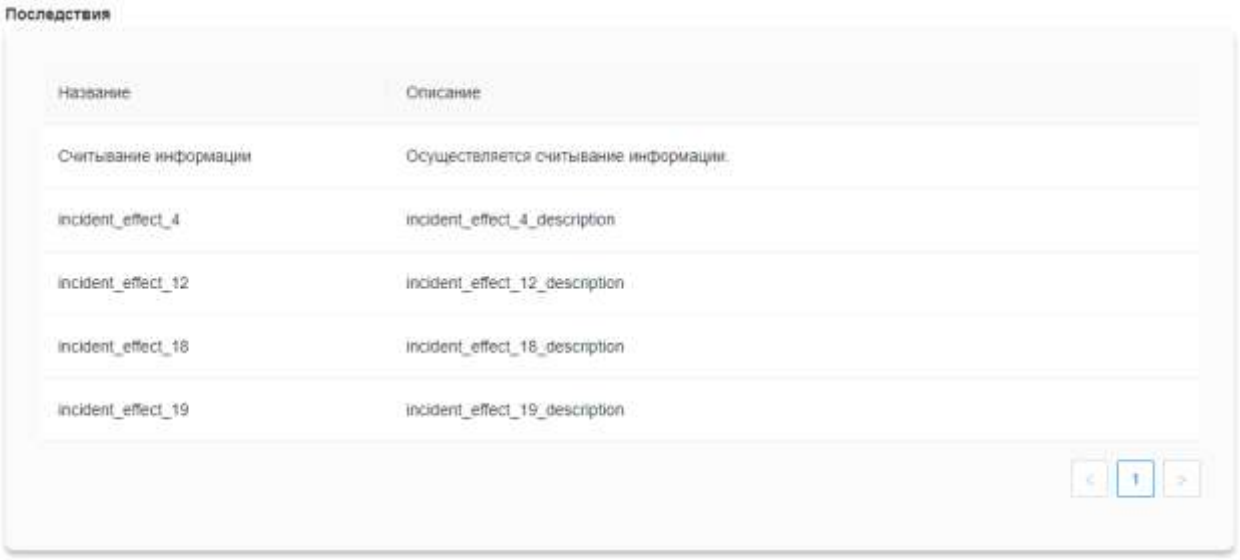

Рисунок 22 – Информация об инциденте. Последствия

3.2.5 Блок «События»

Блок отображает список событий, из которых сформирован инцидент, и представлен в виде таблицы со следующей информацией (см. Рисунок 23):

- **«Дата создания»**;
- **«Сообщение»**;
- **«Продукт»**;
- **«IP источника»**;
- **«IP получателя»**.

Рисунок 23 – Информация об инциденте. События

3.3 Экспорт инцидентов

Существует возможность локально сохранить таблицу инцидентов. Для этого необходимо нажать **кнопку «** **»** в левой части формы раздела (см. Рисунок 18).

3.4 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, создание комментария для отображения мнения о данном инциденте;
- пользователь, назначенный для решения инцидента, исходя из результата проведенного расследования, должен изменить статус инцидента, в случае положительного решения инцидента – отметить инцидент как решенный.

3.4.1 Назначение пользователя для решения инцидента

Для назначения пользователей для решения инцидента необходимо выполнить следующие действия:

1. Открыть форму **«[Имя инцидента]»** (см. Раздел 3.2).
2. В поле параметра **«Статус»** выбрать значение **«Назначен»**.
3. В поле параметра **«Назначен на»** выбрать пользователя, на которого будет назначен инцидент.
4. Нажать **кнопку «Сохранить»** для сохранения изменений.

3.4.2 Внесение результата проведенного расследования

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

1. Открыть форму **«[Имя инцидента]»** (см. Раздел 3.2).
2. Изменить значение поля параметра **«Статус»**.
3. Нажать **кнопку «Сохранить»** для сохранения изменений.
4. В случае положительного решения инцидента нажать **кнопку «Решить»** для того, чтобы отметить инцидент как решенный.

4 ПРОСМОТР АРХИВОВ

Раздел **«Хранилище»** позволяет просматривать архивы собранных инцидентов и событий.

Для перехода в раздел **«Хранилище»** необходимо развернуть вкладку **«Настройки»**, выбрать группу раздела **«Журналы»** и выбрать пункт **«Хранилище»** (см. Рисунок 24).

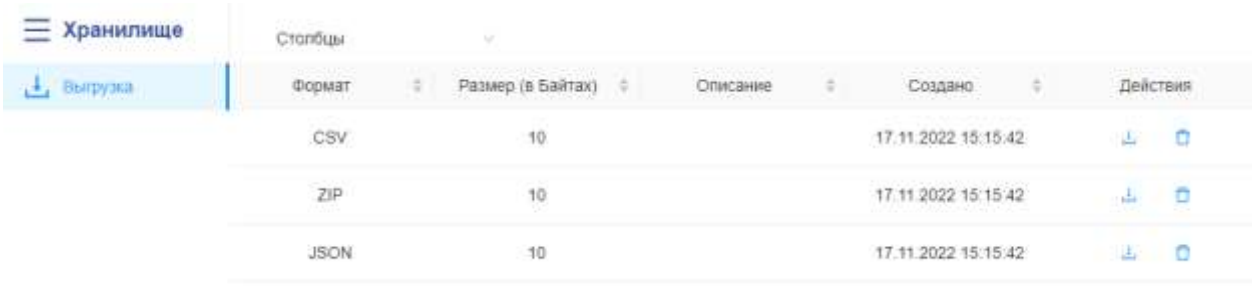

Рисунок 24 – Хранилище

Архивы собранных инцидентов поддерживают следующие форматы:

- **«.CSV»**;
- **«.ZIP»**;
- **«.JSON»** - архив собранных инцидентов, настроенных по ротации (см. Раздел 6).

4.1 Просмотр подробной информации о хранилище

Для просмотра подробной информации о хранилище необходимо нажать **левой кнопкой мыши** на запись с нужным хранилищем. В результате будет отображена форма **«Детали»** (см. Рисунок 25).

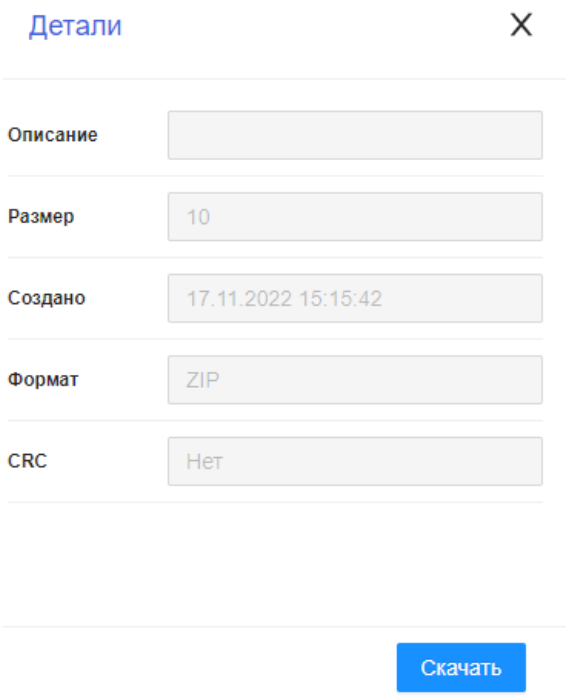

Рисунок 25 – Детали хранилища

4.2 Удаление хранилища

Для удаления выбранного хранилища необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»** в столбце **«Действия»** строки записи информации о хранилище.

4.3 Скачивание архива

Для скачивания архива необходимо нажать одну из **кнопок**:

- **«** **»** – в форме раздела **«Хранилище»** (см. Рисунок 24).
- **«Скачать»** – в форме **«Детали»** (см. Рисунок 25).

5 НАСТРОЙКА ПРАВИЛ 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 определенное событие.

Раздел **«Правила корреляции»** (см. Рисунок 26) позволяет управлять правилами корреляции.

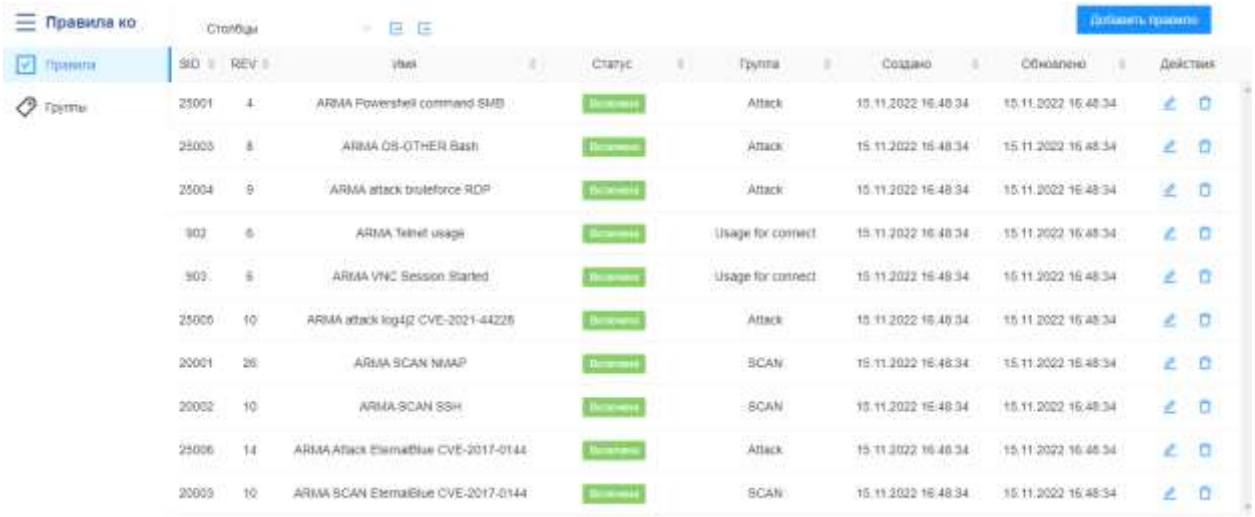

Рисунок 26 – Правила корреляции

Для перехода в раздел необходимо развернуть вкладку **«Журналы»** и выбрать пункт **«Правила корреляции»**.

По умолчанию в **ARMA MC** предустановлены следующие правила корреляции:

- системные:
  - **«NewAsset»**;
  - **«Serious event»**.
- информационные по обнаружению протоколов.

5.1 Описание коррелятора

Раздел позволяет просматривать правила коррелятора в формате таблицы, содержащей столбцы со следующими данными:

- **«SID»**;
- **«REV»**;
- **«Имя»**;
- **«Статус»**;
- **«Группа»**;

- **«Создано»**;
- **«Обновлено»**;
- **«Действия»**.

!Важно Комбинация столбцов **«SID»** и **«REV»** позволяет идентифицировать правило среди нескольких **ARMA MC**.

5.2 Добавление правила корреляции

Для добавления правила корреляции необходимо выполнить следующие действия:

1. Нажать **кнопку «Добавить правило»** в правой части формы раздела.
2. В блоке **«Базовые настройки правила»** (см. Рисунок 27) открывшейся формы **«Новое правило корреляции»** указать значения обязательных параметров:
    - **«Название правила»** – отображаемое имя правила;
    - **«Глубина анализа»** – глубина анализа, показывающая насколько далеко во времени от текущего момента коррелятор будет искать события для конкретного правила корреляции, например, глубина 30 секунд означает, что события, пришедшие минуту назад, не будут учитываться при поиске;
    - **«SID правила»** – идентификатор правила;

рекомендуется выбрать группу правила в выпадающем списке параметра **«Группа правил»** (см. Раздел 5.3) или добавить новую, нажав **кнопку «** **»**.

!Важно При создании пользовательских правил корреляции значение параметра SID указывается в диапазоне от 3 до 699.

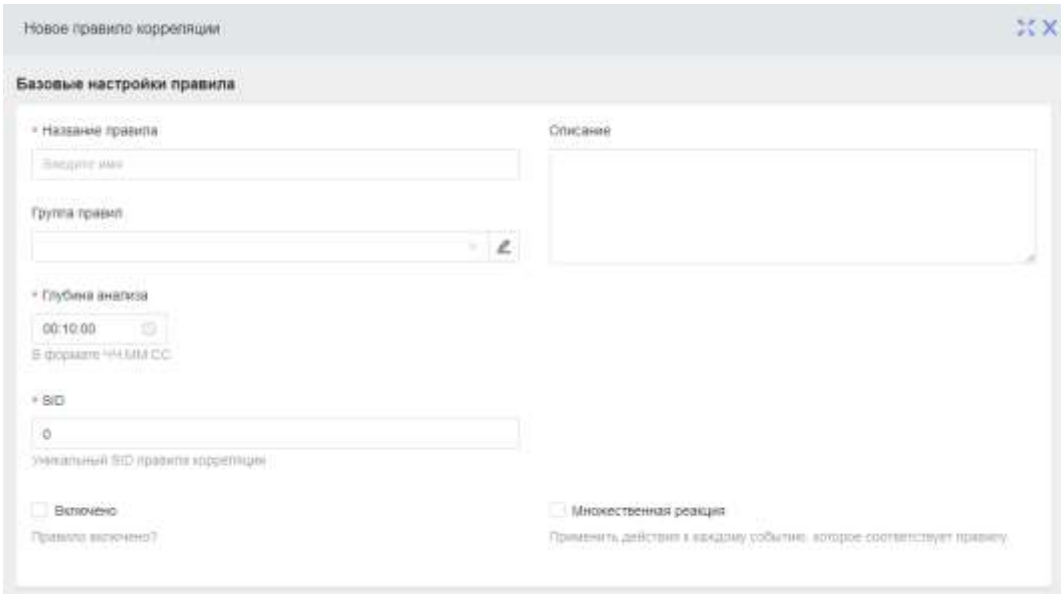

Рисунок 27 – Правило корреляции. Базовые настройки правила

3. В блоке **«Условия срабатывания правила»** (см. Рисунок 28) задать условия срабатывания правила с помощью специального синтаксиса. Описание синтаксиса запроса, примеры используемых операторов и наименования используемых полей доступны при нажатии **кнопки «** **»**.

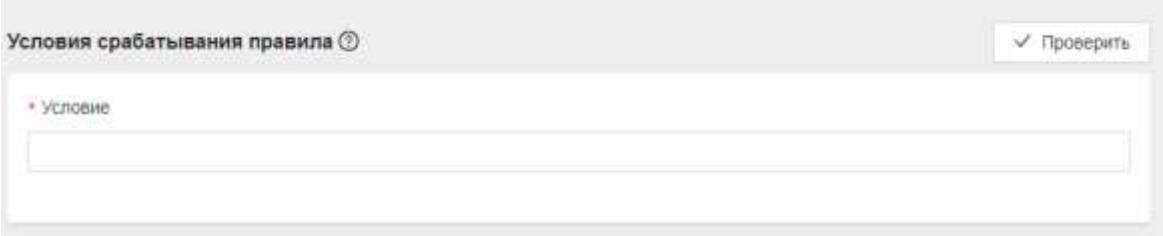

Рисунок 28 – Правило корреляции. Условия срабатывания правила

!Важно Условия правила корреляции задаются на основании деталей события, для которого предназначено правило.

4. В блоке **«Условия срабатывания правила»** (см. Рисунок 28) нажать **кнопку «Проверить»** для проверки условия срабатывания правила. Результатом проверки будет отображенная таблица **«Найденные условия»**. В случае, когда в списке существующих событий будут события, подходящие под условие срабатывания правила, данные события будут отображены (см. Рисунок 29).

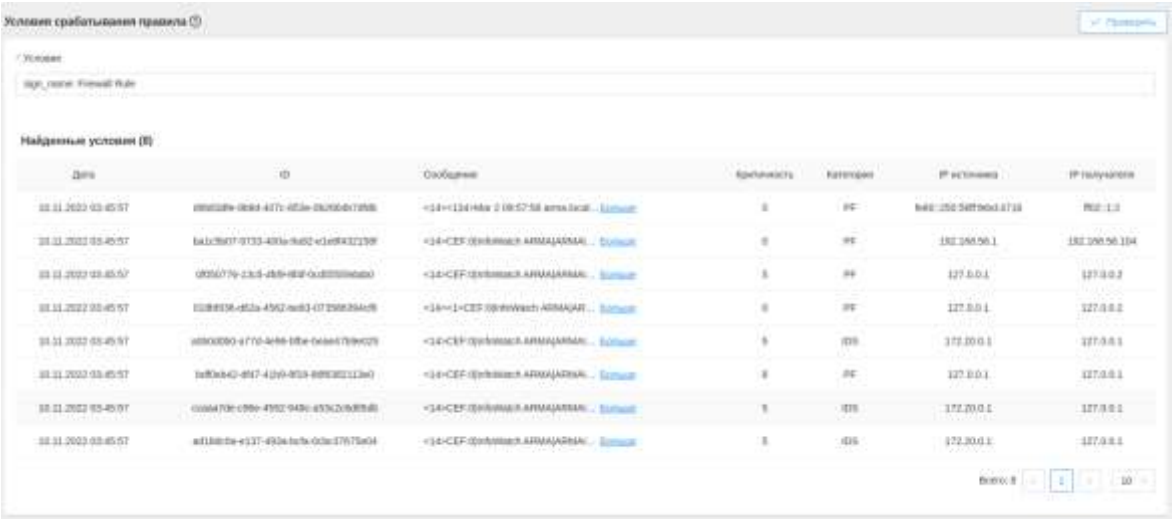

Рисунок 29 – Результаты проверки срабатывания условий правила корреляции

В случае, когда в списке существующих событий не будет событий, подходящих под условие срабатывания правила, в таблице записей не будет (см. Рисунок 30).

Рисунок 30 – Уведомление об отсутствии записей, отвечающих условию срабатывания правила

!Важно Отсутствие записей в таблице **«Найденные условия»** не означает, что условие задано некорректно.

5. В блоке **«Действия»** (см. Рисунок 31) нажать **кнопку «+ Добавить»**.

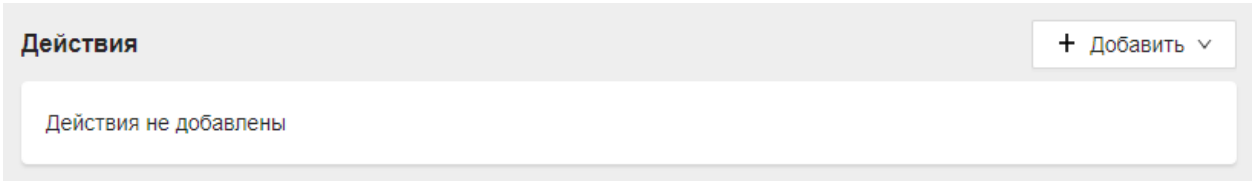

Рисунок 31 – Правило корреляции. Действия

6. В выпадающем списке (см. Рисунок 32) выбрать один из предложенных типов действий.

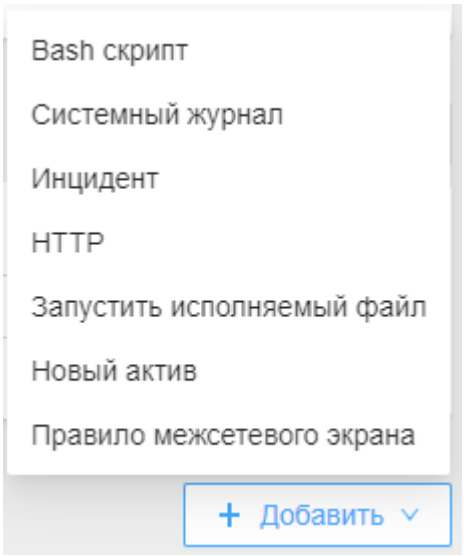

Рисунок 32 – Типы действий

В зависимости от выбранного типа действия в блоке **«Действия»** будут отображены различные параметры. Примеры правил с различными типами действий приведены в Разделе 5.5 настоящего руководства.

7. Для сохранения правила нажать **кнопку «Сохранить»**.

5.3 Управление группами правил корреляции

Для управления группами правил корреляции необходимо перейти во вкладку **«Группы»**.

В открывшейся вкладке **«Группы»** (см. Рисунок 33) возможно выполнить различные действия с помощью следующих кнопок:

- **«Добавить»** – добавить группу;
- **«Редактировать»** – редактировать выбранную группу;
- **«** **»** – удалить выбранную группу.

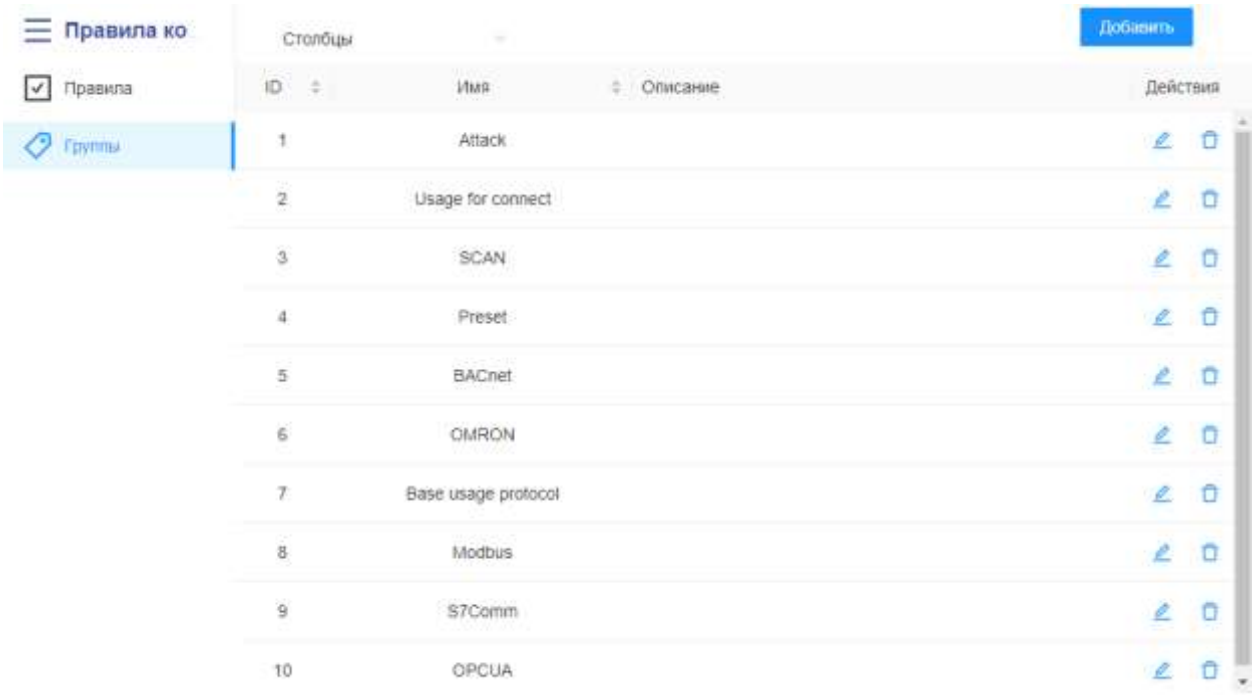

Рисунок 33 – Группы правил

При создании или редактировании группы откроется форма **«Новая группа»** или **«[Имя группы правил]»** соответственно. В данной форме необходимо указать значения в полях параметров **«Имя»** и **«Описание»**, а затем нажать **кнопку «Сохранить»** для принятия изменений.

5.4 Импорт и экспорт правил корреляции

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

Для импорта правил корреляции необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»**, а затем в открывшемся стандартном окне выбора файла выбрать файл и нажать **кнопку «Открыть»** (см. Рисунок 34).

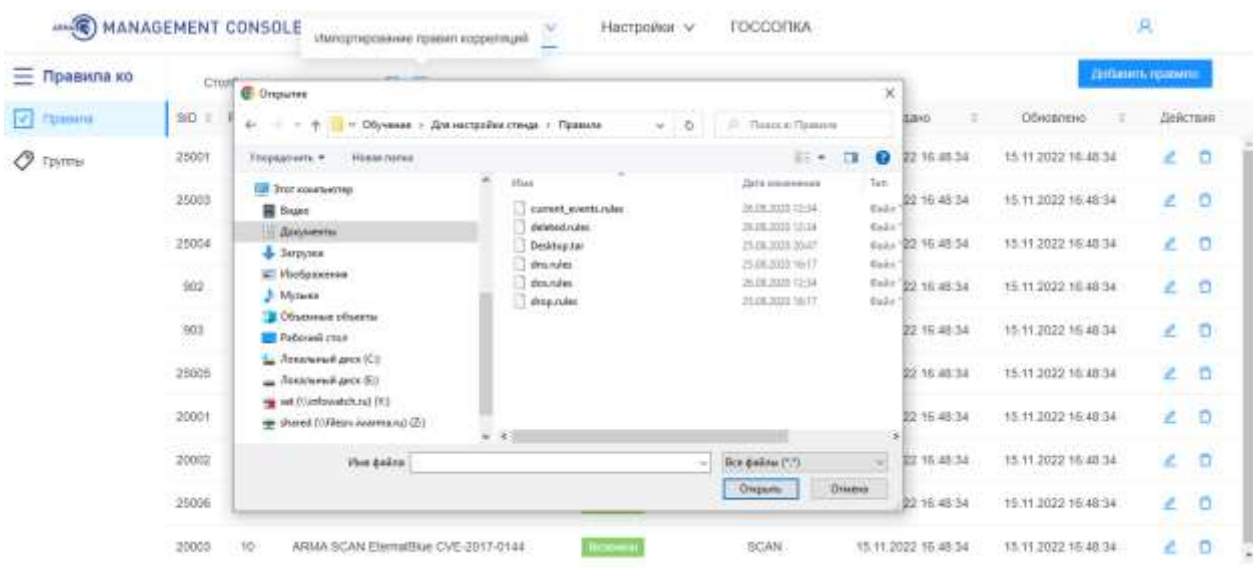

Рисунок 34 – Импорт правил корреляции

По окончании импорта появится соответствующее уведомление:

- импорт завершился успешно (см. Рисунок 101);
- импорт завершился неуспешно (см. Рисунок 102).

Если длительность ответа при запуске импорта превышает 1 секунду появляется всплывающее окно (см. Рисунок 103).

Для экспорта правил корреляции необходимо нажать **кнопку «** **»** и следовать указаниям веб-браузера.

5.5 Примеры правил корреляции с различными типами действий

В качестве примера используется правило корреляции со следующими параметрами:

- **«Название правила»** – «Test»;
- **«Глубина анализа»** – «00:05:00»;
- **«SID»** – «1»;
- **«Условие»** – «device_product: arpwatch and device_action: "new station"» – появление новых устройств в сети.

создание правила описано в Разделе 5.2 настоящего руководства.

Для проверки работоспособности правил корреляции используется подключенный **ARMA IF** (см. Раздел 9.6.1).

Генерация события осуществляется с помощью **ARMA IF**, для этого необходимо выполнить следующие действия:

1. Включить обнаружение устройств в **ARMA IF**. Описание функции «Обнаружение устройств» приведено в разделе **«Обнаружение устройств»** Руководства пользователя **ARMA IF**.
2. Подключить новое устройство в сеть прослушиваемого сетевого интерфейса **ARMA IF**.

5.5.1 Тип действия «Системный журнал»

Действие **«Системный журнал»** позволяет отправлять запись по syslog при возникновении определенного события.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать правило корреляции с типом действия **«Системный журнал»** и в блоке **«Действие»** (см. Рисунок 35) указать следующие значения параметров:
   - **«Хост»** – «192.168.1.200»;
   - **«Порт»** – «514»;
   - **«Протокол»** – «TCP»;
   - **«Имя источника»** – «Syslog»;
   - **«Сообщение»** – «{{.device_product}}».

   Параметры syslog-сервера приведены справочно и могут отличаться в зависимости от используемого ПО.

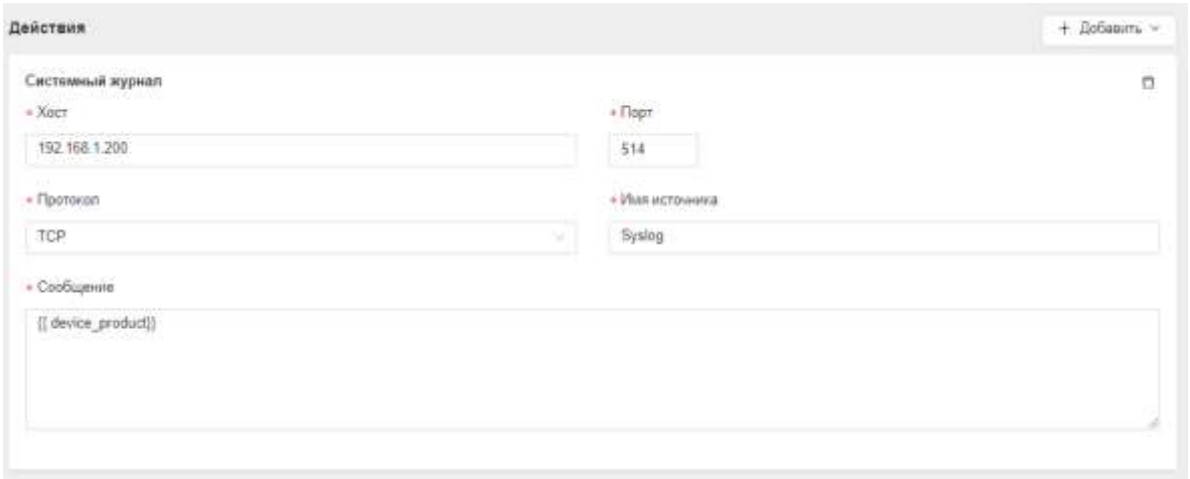

Рисунок 35 – Действие «Системный журнал»

2. Сгенерировать событие.
3. Убедиться, что правило корреляции сработало и запись отправилась в syslog-сервер (см. Рисунок 36).

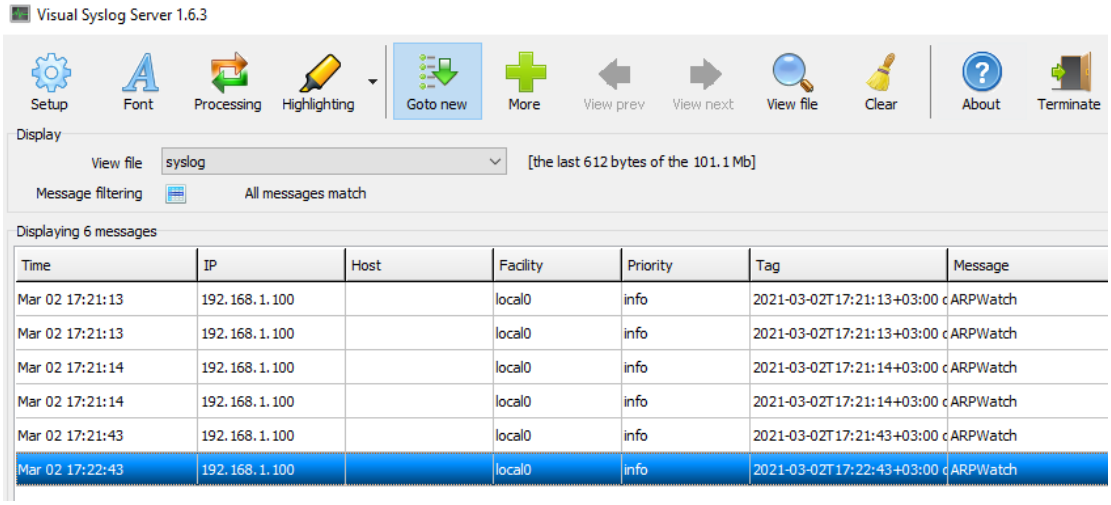

Рисунок 36 – Результат срабатывания правила корреляции с действием «Syslog»

5.5.2 Тип действия «HTTP»

Действие **«HTTP»** позволяет при срабатывании определенного события отправлять информацию на внешний сервер. Предварительно необходимо убедиться в наличии доступа к используемому внешнему серверу.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать правило корреляции с типом действия **«HTTP»** и в блоке **«Действие»** (см. Рисунок 37) указать следующие значения параметров:
   - **«URL»** – «http://192.168.1.200:7788/api/set»;
   - **«Тип содержимого»** – «text/plain»;
   - **«Шаблон»** – «{{.event_src_msg}}».

   Параметры внешнего сервера приведены справочно и могут отличаться в зависимости от используемого ПО.

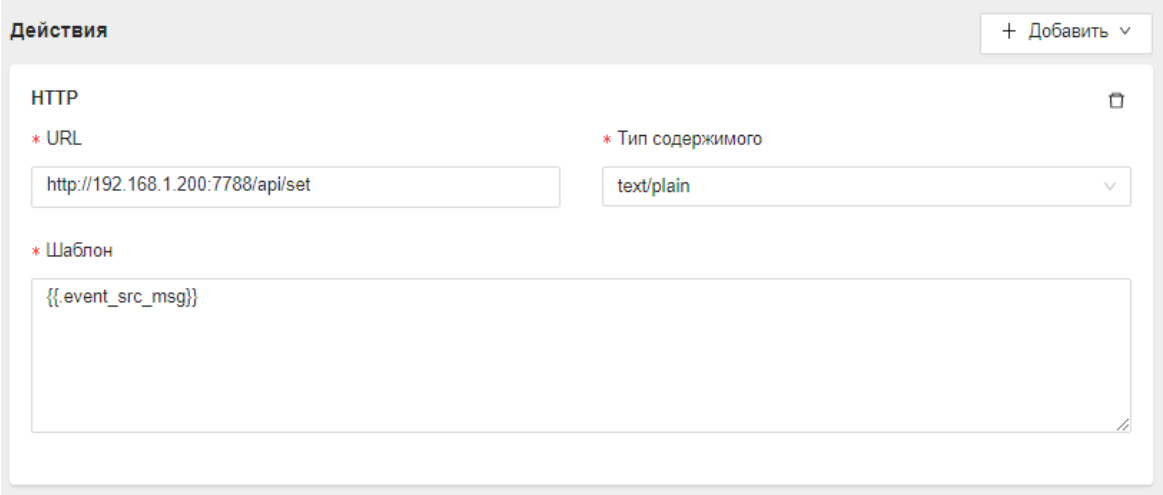

Рисунок 37 – Действие «HTTP»

2. Сгенерировать событие.
3. Убедиться, что правило корреляции сработало и событие появилось на внешнем сервере (см. Рисунок 38).

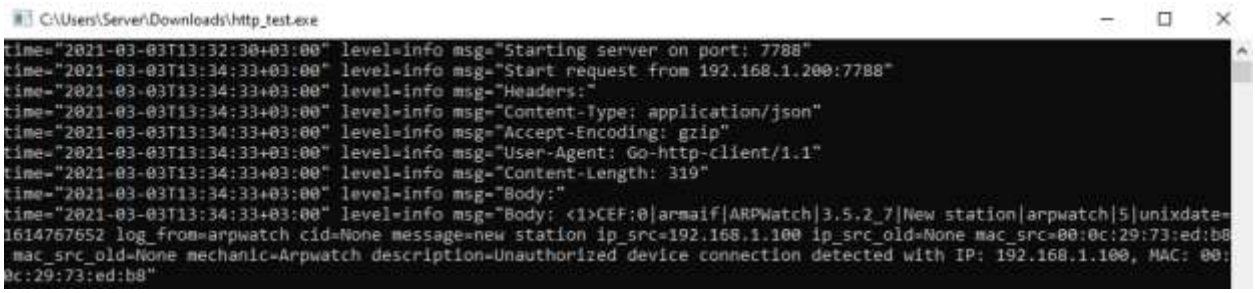

Рисунок 38 – Результат срабатывания правила корреляции с действием «HTTP»

5.5.3 Тип действия «Инцидент»

Действие **«Инцидент»** позволяет при срабатывании определенного события создавать инцидент и отправлять его в журнал инцидентов **ARMA MC**.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать правило корреляции с типом действия **«Инцидент»** и в блоке **«Действие»** (см. Рисунок 39) указать следующие значения параметров:
   - **«Название»** – «{{.sign_name}}»;
   - **«Важность»** – «5»;
   - **«Описание»** – «{{.event_src_msg}}».

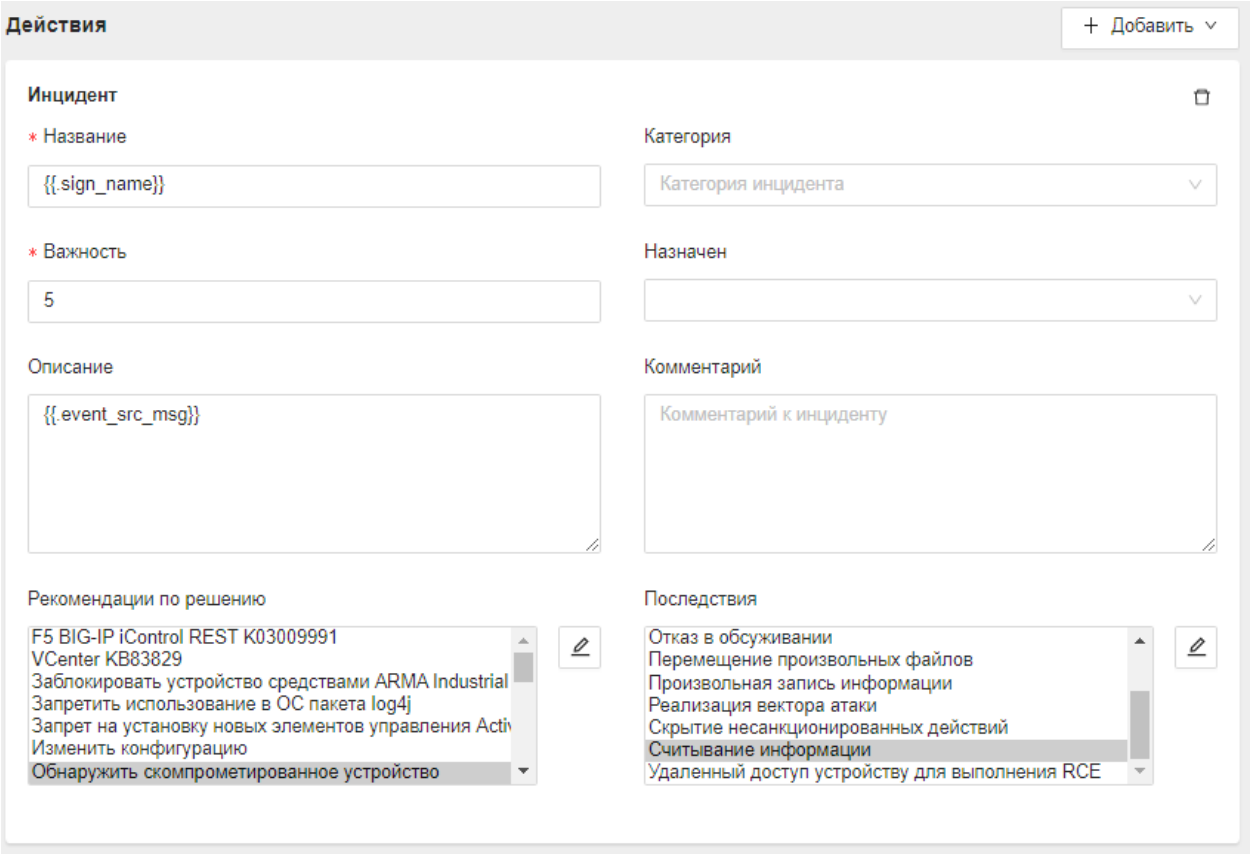

Рисунок 39 – Действие «Инцидент»

Значение параметров **«Рекомендации по решению»** и **«Последствия»** можно выбрать из выпадающего списка или добавить новый, нажав **кнопку «** ✎ **»**.

2. Сгенерировать событие.
3. Убедиться, что правило корреляции сработало и в разделе **«Инциденты»** (см. Раздел 3) появился инцидент с названием исходного сообщения самого события (см. Рисунок 40).

Рисунок 40 – Результат срабатывания правила корреляции с действием «Инцидент»

5.5.4 Тип действия «Bash скрипт»

Действие **«Bash скрипт»** позволяет при срабатывании определенных событий запускать сценарий скрипта.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать правило корреляции с типом действия **«Bash скрипт»** и в блоке **«Действие»** (см. Рисунок 41) указать следующую строку в значении параметра **«Тело Bash скрипта»**:
   - «Echo "{.sign_name}}">/tmp/{.sign_name}}_.txt».

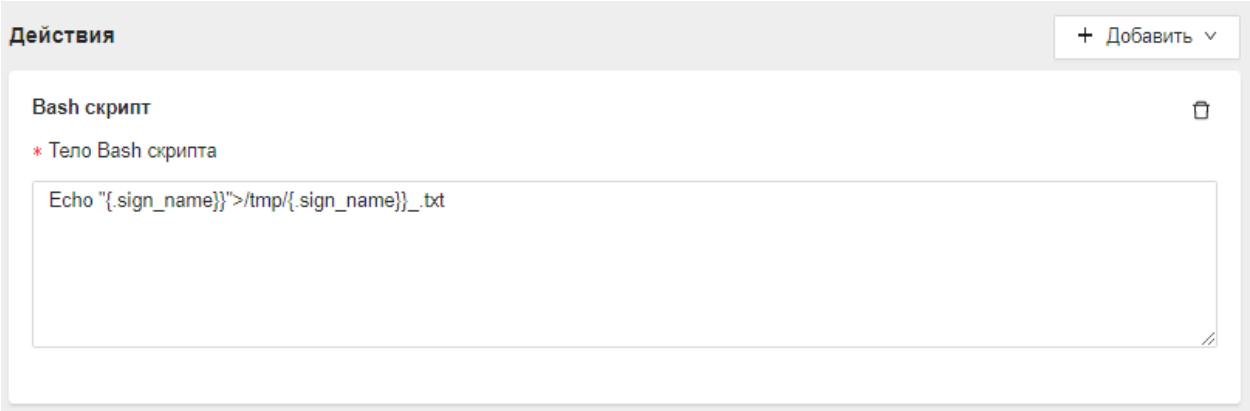

Рисунок 41 – Действие «Bash скрипт»

2. Сгенерировать событие.
3. Через локальный консольный интерфейс убедиться, что в каталог «tmp» добавляются файлы с именем, совпадающем по имени сигнатуры самого события (см. Рисунок 42), согласно функционалу указанного скрипта.

Рисунок 42 – Результат срабатывания правила корреляции с действием «Bash скрипт»

5.5.5 Тип действия «Запустить исполняемый файл»

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

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Через локальный консольный интерфейс в каталоге «/tmp/1» создать исполняемый файл **«script.sh»**, создающий файл в каталоге.

2. Создать правило корреляции с типом действия **«Запустить исполняемый файл»** и в блоке **«Действие»** (см. Рисунок 43) указать следующие значения параметров:
    - **«Путь к исполняемому файлу»** – «/tmp/1/script.sh»;
    - **«Аргументы»** – «AAA BBB»;
    - **«Окружение»** – «T_1=RRR»;
    - **«Рабочая папка»** – «/tmp/1».

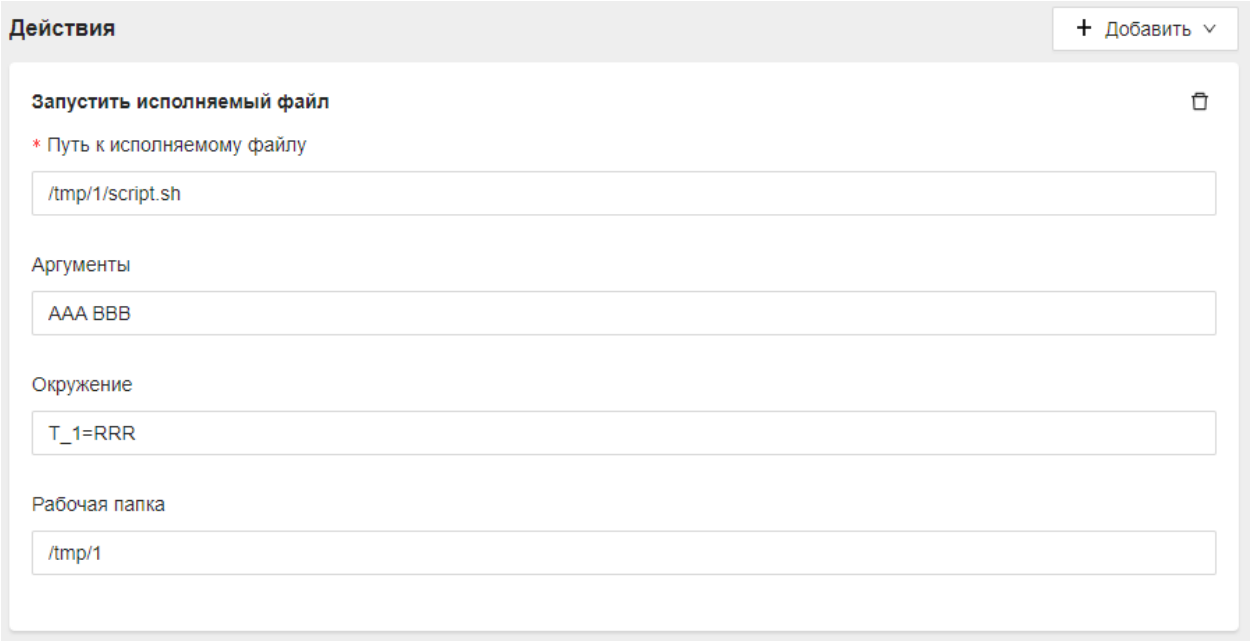

Рисунок 43 – Действие «Запустить исполняемый файл»

3. Сгенерировать событие.
4. Убедиться, что правило корреляции сработало и в каталоге «/tmp/1» создан текстовый документ **«1.txt»** с заданными параметрами из правила корреляции (см. Рисунок 44).

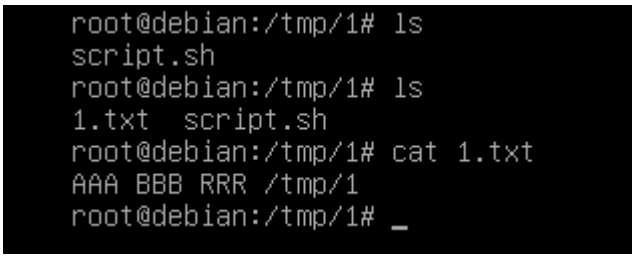

Рисунок 44 – Результат срабатывания правила корреляции с действием «Запустить исполняемый файл»

5.5.6 Тип действия «Новый актив»

Действие **«Новый актив»** позволяет при появлении новых устройств в сети **ARMA IF** отправлять об этом события в журнал событий **ARMA MC**.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать правило корреляции с типом действия **«Новый актив»** и в блоке **«Действие»** (см. Рисунок 45) указать следующие значения параметров:
    - **«Имя»** – «{{.source_ip}»;
    - **«Тип актива»** – «APM»;
    - **«IP»** – «192.168.1.1».

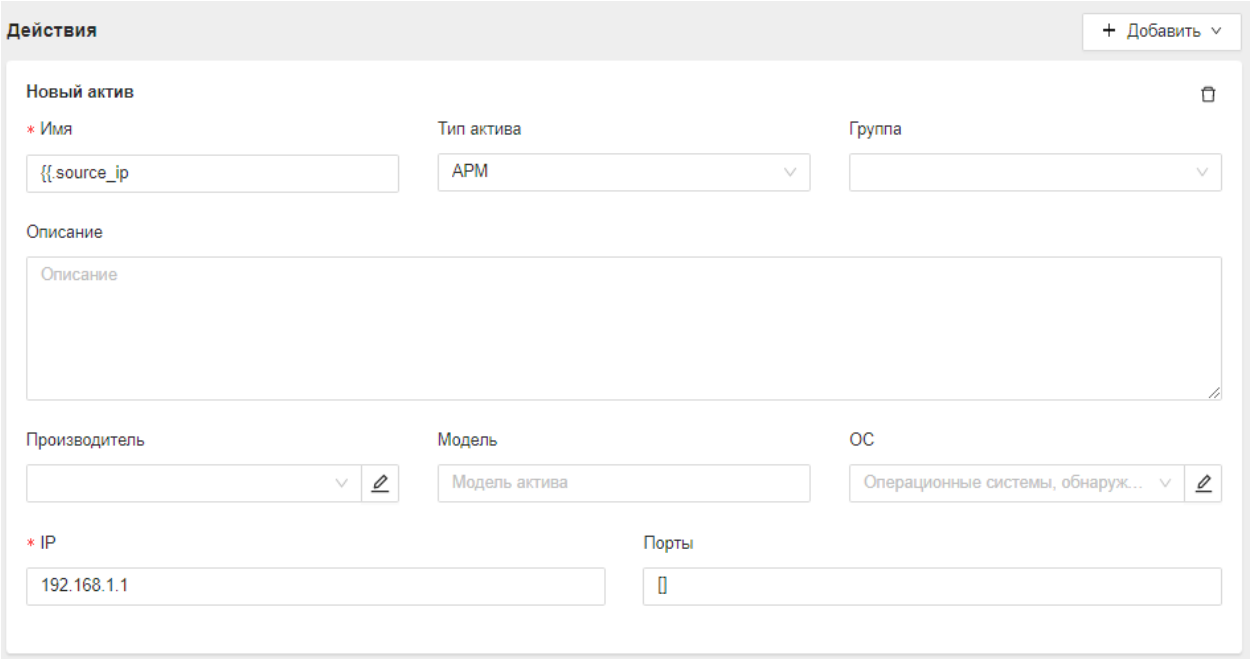

Рисунок 45 – Действие «Новый актив»

2. Сгенерировать событие.
3. Убедиться, что правило корреляции сработало и в разделе **«Журнал событий»** (см. Раздел 2) появились события со словами «New Device» (см. Рисунок 46).

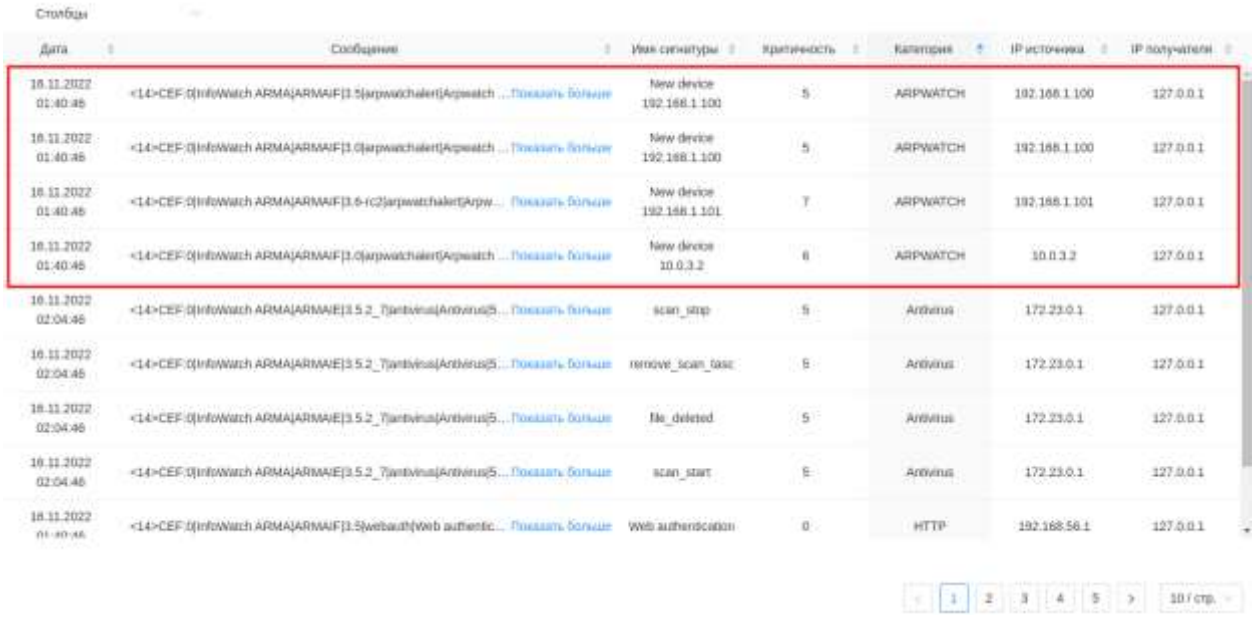

Рисунок 46 – Результат срабатывания правила корреляции с действием «Новый актив»

Значение параметров **«Производитель»** и **«ОС»** можно выбрать из выпадающего списка или добавить новый, нажав **кнопку «** **»** и в форме **«Создать новый элемент»** указать значения параметров **«Имя»** и **«Описание»** (см. Рисунок 47).

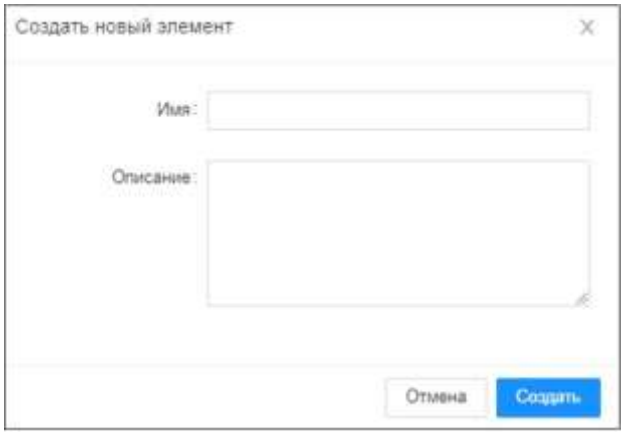

Рисунок 47 – Создание нового элемента

5.5.7 Тип действия «Правило межсетевого экрана»

Действие **«Правило межсетевого экрана»** позволяет на определенное событие создавать правило МЭ:

- разрешающее;
- блокирующее;
- запрещающее.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать правило корреляции с типом действия **«Правило межсетевого экрана»** и в блоке **«Действие»** (см. Рисунок 48) указать следующие значения параметров:
    - **«ARMA IF»** – выбрать подключенный **ARMA IF**;
    - **«Интерфейсы»** – «LAN»;
    - **«Направление»** – «In»;
    - **«Приоритет»** – «1»;
    - **«Действие»** – «Pass»;
    - **«IP протокол»** – «IPv4»;
    - **«Включено»** – «any»;
    - **«Сеть источника»** – «any»;
    - **«Сеть назначения»** – «any»;
    - **«Описание»** – «rule firewall test».

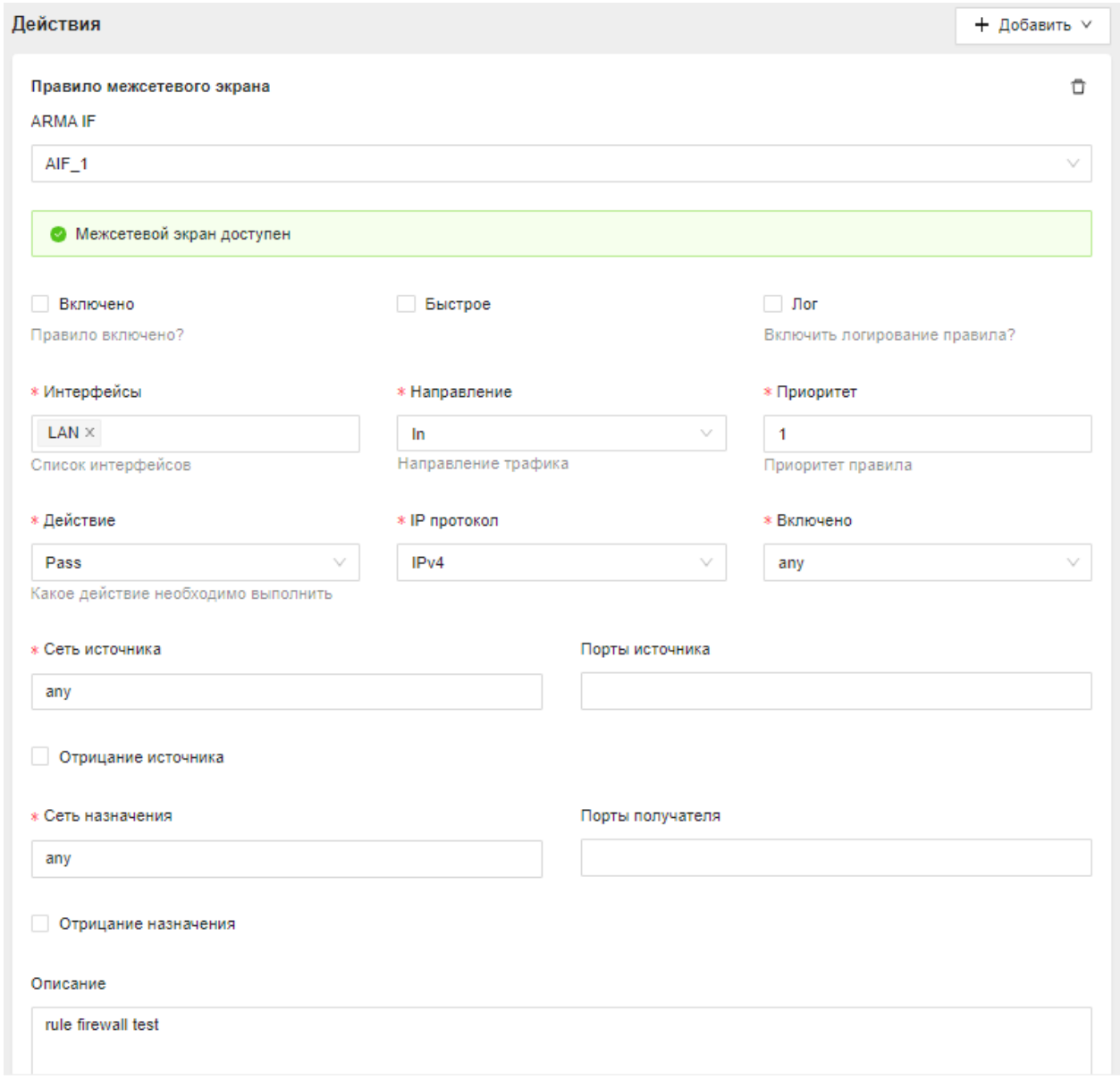

Рисунок 48 – Действие «Правило межсетевого экрана»

2. Сгенерировать событие.
3. Убедиться, что правило корреляции сработало и в разделе API правил **ARMA IF** (**«Межсетевой экран» - «API правила»**) появилось правило с заданными параметрами (см. Рисунок 49).

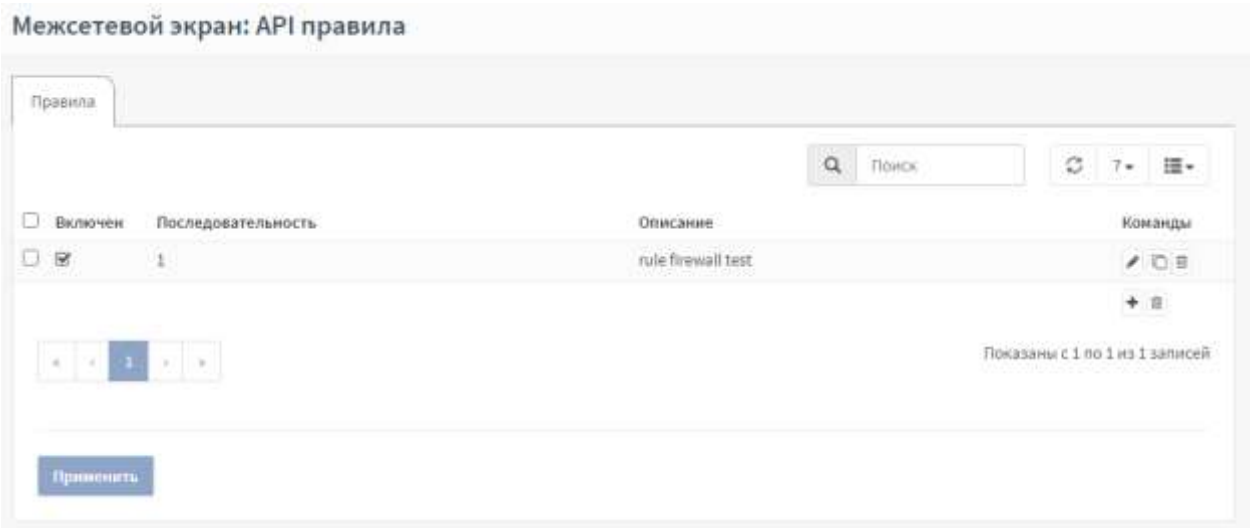

Рисунок 49 – Результат срабатывания правила корреляции с действием «Правило межсетевого экрана»

!Важно При редактировании созданного правила корреляции с типом действия **«Правило межсетевого экрана»** при выборе другого МЭ в параметре «**ARMA IF**» текущие настройки будут сброшены.

6 НАСТРОЙКА РОТАЦИИ ЖУРНАЛОВ

В **ARMA MC** предусмотрен механизм ротации журналов инцидентов и событий по двум типам:

- **«по времени»** – с указанием периодичности: день, неделя или месяц;
- **«по размеру»** – с указанием размера таблицы.

Раздел **«Настройки ротации»** (см. Рисунок 50) позволяет управлять параметрами ротации.

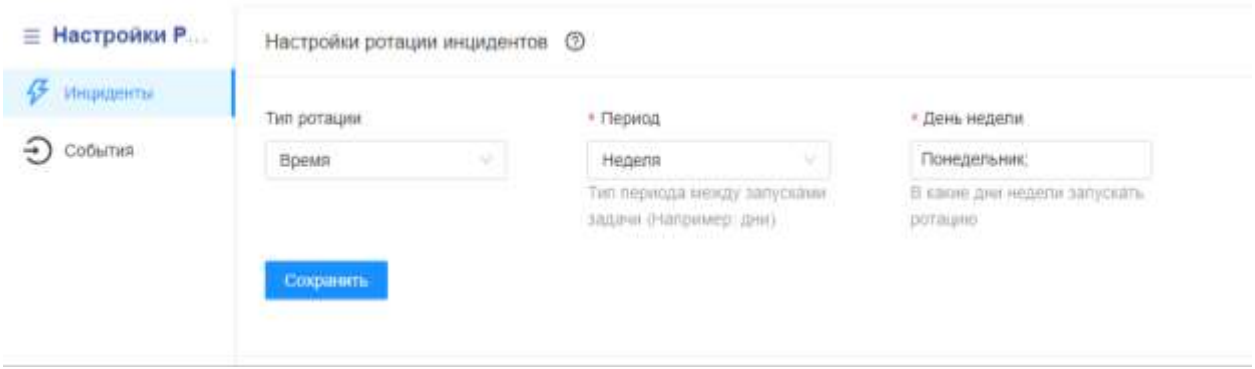

Рисунок 50 – Настройки ротации

Для перехода в раздел необходимо развернуть вкладку **«Настройки»**, выбрать группу **«Журналы»** и выбрать пункт **«Ротация»**.

Для настройки ротации журнала инцидентов перейти во вкладку **«Инциденты»**, для настройки ротации событий перейти во вкладку **«События»**.

Для изменения типа ротации необходимо выполнить следующие действия:

1. Выбрать в выпадающем списке параметра **«Тип ротации»** одно из следующих значений:
   - **«Размер»** – для включения ротации по размеру;
   - **«Время»** – для включения ротации по времени;
   - **«Отключено»** – для отключения ротации.
2. Указать параметры ротации в полях следующих параметров:
   - **«Размер таблицы, когда происходит ротация»** для ротации по размеру – указать размер в Кб;
   - **«Период»** для ротации по времени – выбрать из выпадающего списка одно из значений:
     - **«День»** – указать в поле проявившего параметра **«Время»** время, в которое следует запускать ротацию;

- **«Неделя»** – указать в поле проявившего параметра **«День недели»** дни недели, в которые следует запускать ротацию;
- **«Месяц»** – указать в поле проявившего параметра **«Месяц»** месяцы, в которые следует запускать ротацию.

3. Нажать **кнопку «Сохранить»**.

!Важно При срабатывании ротации инцидентов ротируются инциденты только со статусом **«Решен»** и **«Ложное срабатывание»**, а при запуске ротации событий текущий индекс не будет удален.

7 СИСТЕМНЫЕ НАСТРОЙКИ

В **ARMA MC** предусмотрен механизм настройки режима работы **ARMA MC** по протоколу **HTTPS**.

Для перехода в раздел необходимо развернуть вкладку **«Настройки»** и выбрать пункт **«Системные настройки»**.

Раздел **«Системные настройки»** позволяет выполнять следующие действия:

- настраивать TLS сертификат;
- настраивать аутентификацию.

7.1 TLS сертификат

Во вкладке «**TLS сертификат**» есть возможность включать TLS, генерировать сертификат безопасности и ключ к нему (см. Рисунок 51).

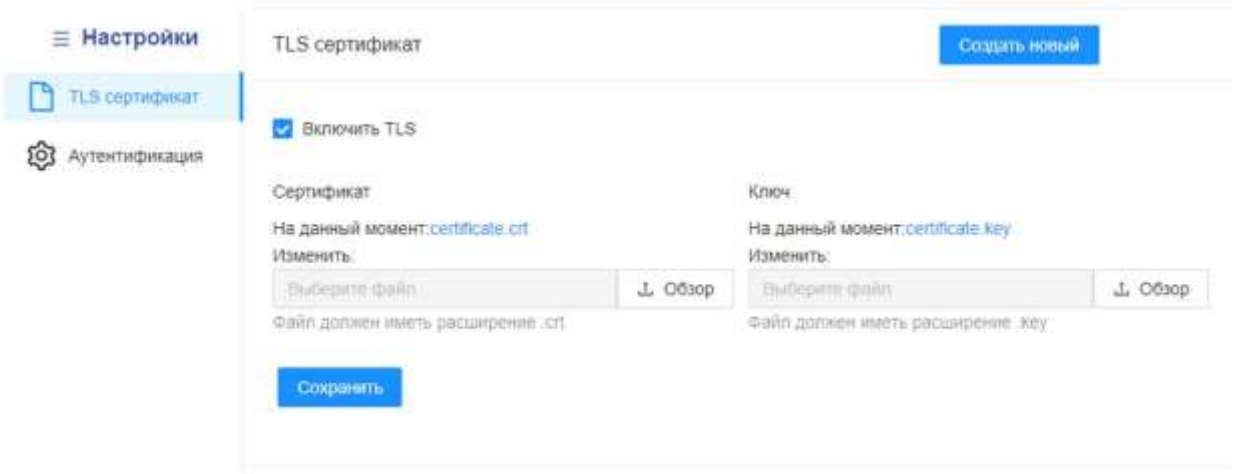

Рисунок 51 – Системные настройки. TLS сертификат

Действующий сертификат и ключ сгенерированы со сроком действия 1 год. После окончания срока действия текущего сертификата и ключа необходимо сгенерировать новый, нажав **кнопку «Создать новый»**.

Действующие сертификат и ключ возможно скачать, нажав **левой кнопкой мыши** их название, а далее следуя инструкциями веб-браузера.

7.2 Аутентификация

Во вкладке **«Аутентификация»** есть возможность задавать количество допустимых попыток входа в систему и время, в течение которого пользователю будет отказано в аутентификации после превышения попыток входа (см. Рисунок 52).

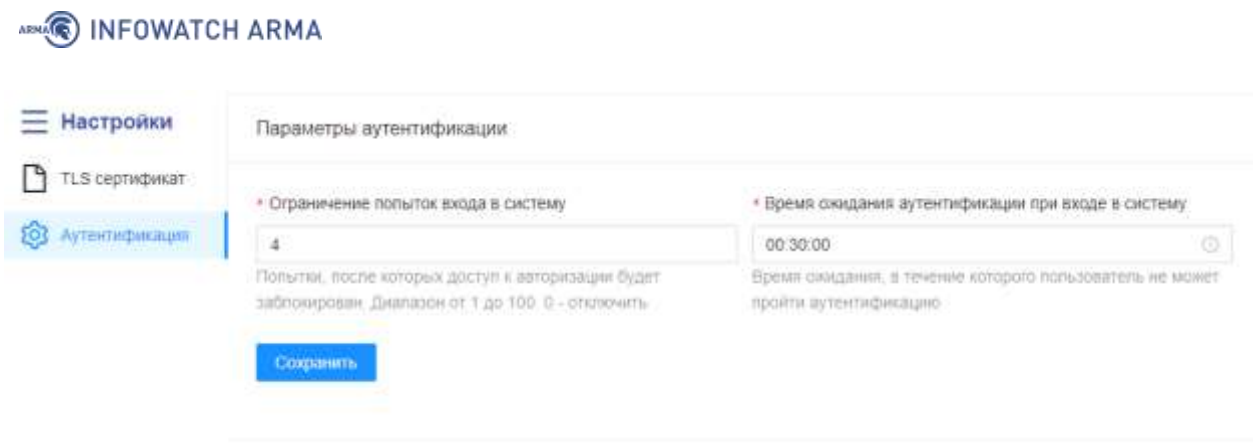

Рисунок 52 – Системные настройки. Аутентификация

!Важно После выключения TLS и первого перенаправления на нужный протокол появится сообщение **«Невозможно загрузить список виджетов»**. В таком случае необходимо очистить кэш веб-браузера и перезагрузить страницу.

!Важно По прошествии времени, указанного в поле параметра **«Тайм-аут попыток аутентификации»**, пользователю снова будет доступна аутентификация в веб-интерфейсе.

8 УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

В **ARMA MC** предусмотрен механизм управления лицензиями.

Раздел **«Лицензия»** позволяет:

- просматривать информацию о действующей лицензии;
- активировать новую лицензию.

8.1 Информация о лицензии

В подразделе **«Текущая лицензия»** можно просматривать информацию о действующей лицензии.

Для перехода в подраздел необходимо развернуть вкладку **«Настройки»**, выбрать группу **«Лицензия»** и выбрать пункт **«Текущая лицензия»**.

Информация о лицензии включает в себя (см. Рисунок 53):

- основную информацию;
- функциональные параметры лицензии;
- опции лицензии.

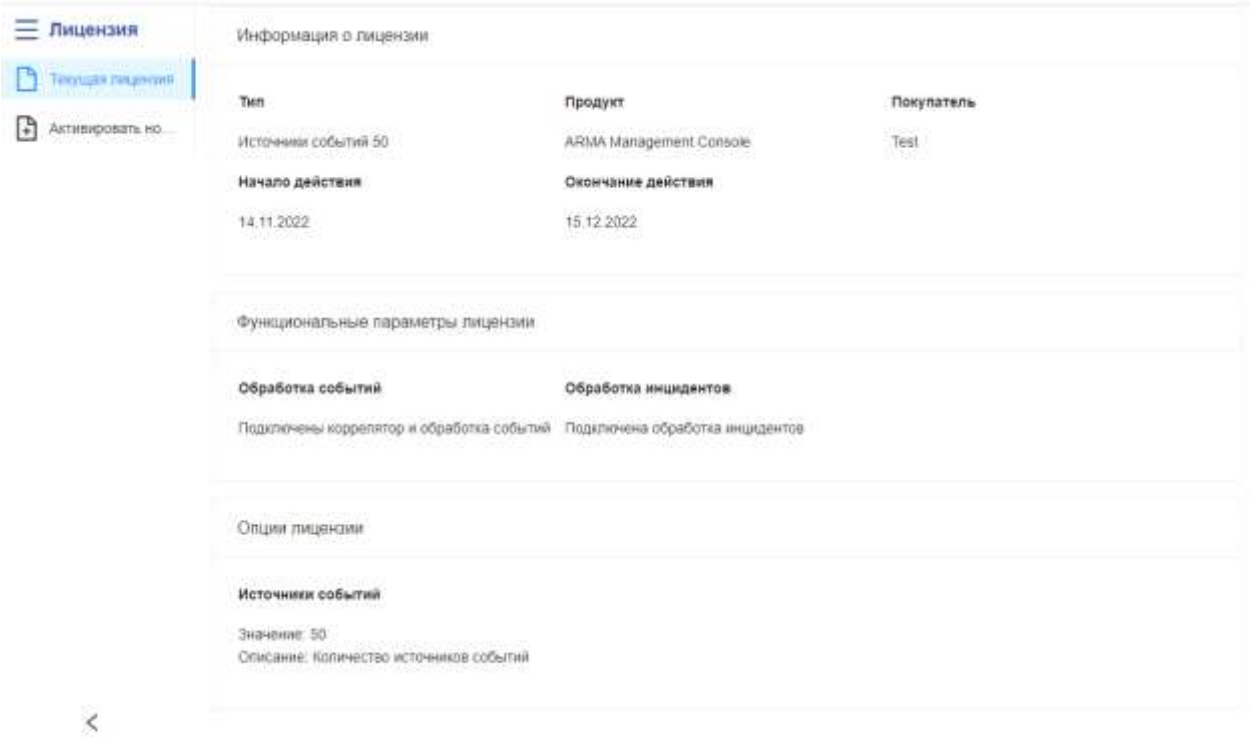

Рисунок 53 – Информация о текущей лицензии

8.2 Активация новой лицензии

В подразделе **«Активировать новую»** можно произвести активацию новой лицензии.

Для перехода в подраздел необходимо развернуть вкладку **«Настройки»**, выбрать группу **«Лицензия»** и выбрать пункт **«Активировать новую»** (см. Рисунок 54).

Рисунок 54 – Активация новой лицензии

Активация лицензии производится аналогично активации при первом подключении к **ARMA MC** (см. раздел **«Активация лицензии»** Руководства администратора **ARMA MC**).

9 УПРАВЛЕНИЕ ИСТОЧНИКАМИ СОБЫТИЙ

В разделе **«Источники событий»** (см. Рисунок 55) отображаются подключенные к **ARMA MC** устройства.

Рисунок 55 – Источники событий

Для перехода в раздел необходимо развернуть вкладку **«Устройства»** и выбрать пункт **«Источники событий»**.

9.1 Описание таблицы источников событий

Раздел позволяет просматривать устройства в формате таблицы, содержащей столбцы со следующими данными:

- **«ID»**;
- **«Статус»**;
- **«Имя»**;
- **«Тип»**;
- **«IP»**;
- **«Группа»**;
- **«Порт»**;
- **«Доп. информация»**;
- **«Дата обновления»**;
- **«Действия»**.

В столбце **«Действия»** доступны следующие кнопки управления источником события:

- **«**  **»** – редактировать информацию об источнике события;
- **«**  **»** – удалить источник события из списка.

Доступны дополнительные действия:

- применимые к источникам событий IF:
  - **«**  **»** – загрузить конфигурацию Firewall;

- «  » – скачать конфигурацию Firewall;
- «  » – обновить базу правил СОВ;
- «  » – перезагрузить.

- применимые к источникам событий IE:
  - «  » загрузить конфигурацию с IE;
  - «  » скачать конфигурацию IE;
  - «  » копировать конфигурацию IE.

Выбор нескольких источников событий с целью применения к ним действий осуществляется установкой флажков слева от значения столбца **«ID»** выбранных устройств.

9.2 Добавление источника событий

Для добавления устройства необходимо выполнить следующие действия:

1. Нажать **кнопку «Добавить устройство»**.

!Важно При превышении количества источников событий, которое предоставлено в соответствии с установленной лицензией, **кнопка «Добавить устройство»** будет неактивна, а при наведении на нее будет отображаться подсказка (см. Рисунок 107).

2. В открывшейся форме **«Новый источник событий»** (см. Рисунок 56) и указать значения следующих параметров:
   - **«Тип»** – тип источника событий:
     - ARMA Industrial Firewall;
     - ARMA Industrial Endpoint.
   - **«Имя»** – отображаемое в **ARMA MC** имя устройства;
   - **«IP»** – IP-адрес или доменное имя подключаемого устройства;
   - параметры для типа источника событий **ARMA Industrial Firewall:**
     - **«Ключ»** – ключ API;
     - **«Секрет»** – значение «секрета» ключа API;
   - **«Порт»** – значение порта входящих логов. Указываются порты TCP – 80, 443, 5672 и порты UDP в диапазоне от 1500 до 65535, остальные порты будут закрыты.
   - **«Группа»** – значение группы, в которую входит источник события.

!Важно В поле параметра **«Порт»** указанный порт не должен быть занятым ранее.

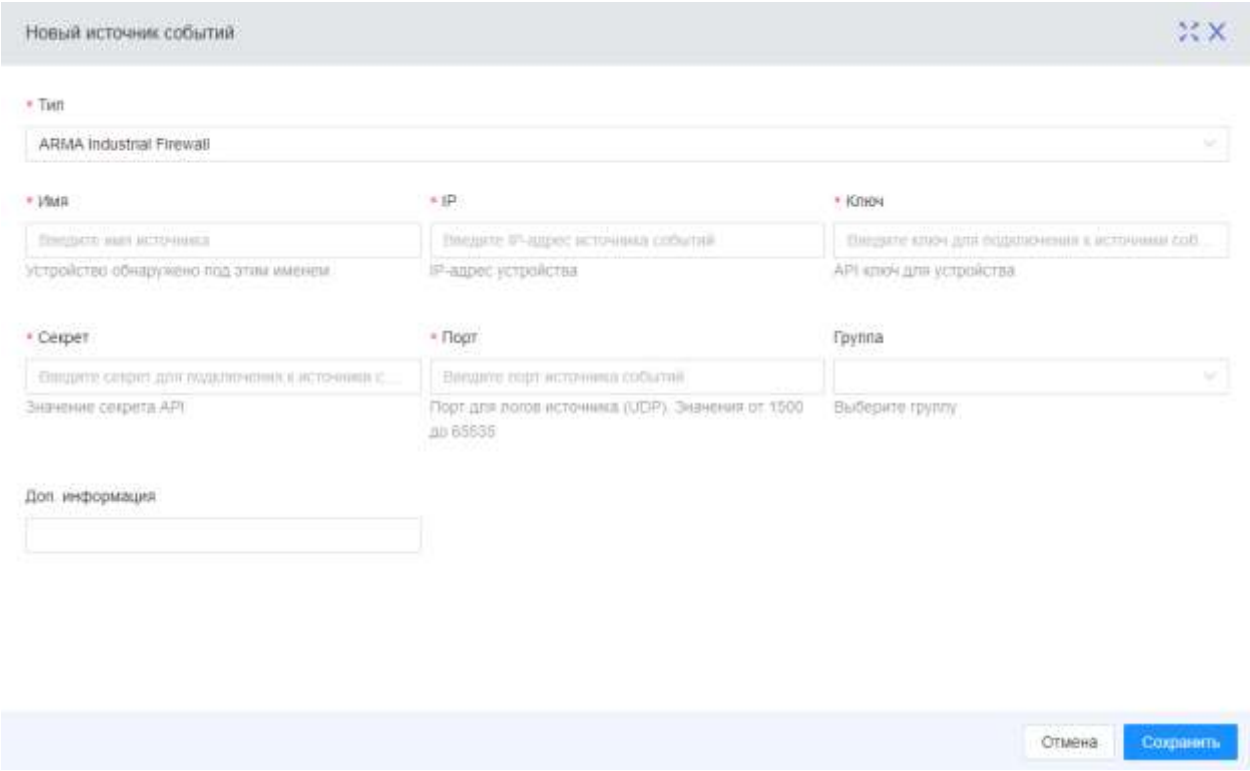

Рисунок 56 – Добавление нового источника событий

3. При необходимости указать дополнительную информацию об устройстве заполнить поле **«Доп. информация»**.
4. Нажать **кнопку «Сохранить»** для сохранения информации и добавления устройства.

!Важно При добавлении источника событий типа **«ARMA Industrial Firewall»** устройство с **ARMA IF** должно быть не ниже версии 3.6.

В случае некорректного ввода данных отобразится соответствующее уведомление (см. Рисунок 100).

!Важно После подключения устройства не рекомендуется изменять IP-адреса подключаемого устройства и **ARMA MC** с целью исключения потери управления.

9.3 Удаление источника событий

Для удаления источника событий необходимо выполнить следующие действия:

1. Нажать **кнопку «🗑»** в строке подлежащего удалению источника события.
2. Подтвердить удаление, нажав **кнопку «ОК»** в открывшемся уведомлении (см. Рисунок 84).

9.3.1 Удаление нескольких источников событий

Выбор нескольких источников событий с целью удаления осуществляется установкой флажков слева от значения столбца **«ID»** выбранных источников событий.

Для удаления выбранных источников событий необходимо выполнить следующие действия:

3. Нажать **кнопку «** **»**, находящуюся в верхней части формы раздела.
4. Подтвердить удаление, нажав **кнопку «ОК»** в открывшемся уведомлении (см. Рисунок 85).

9.4 Редактирование основной информации источника событий

Для редактирования источника событий необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»** в строке подлежащего редактированию источника события или **кнопку «Редактировать»** в карточке источника событий.
2. В открывшейся форме **«[Имя устройства]»** (см. Рисунок 57) внести требуемые изменения и нажать **кнопку «Сохранить»**.

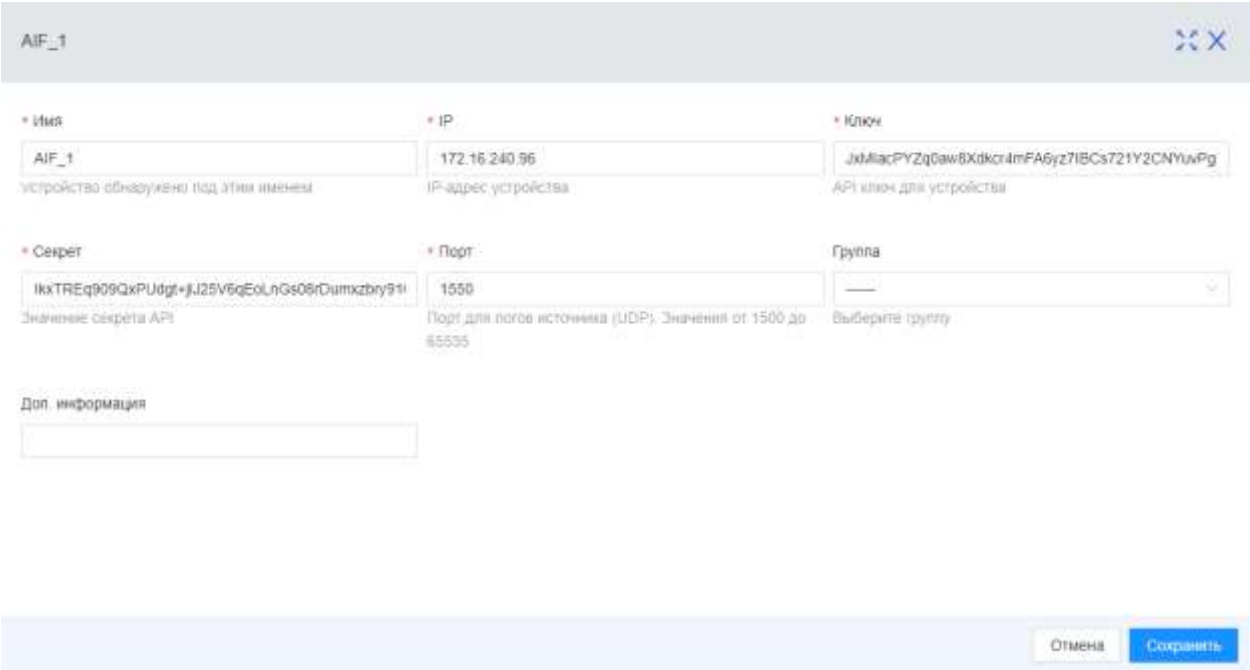

Рисунок 57 – Редактирование источника событий

9.5 Управление группами устройств сети

Управление группами устройств сети осуществляется во вкладке **«Группы»** раздела **«Источники событий»** (см. Рисунок 58).

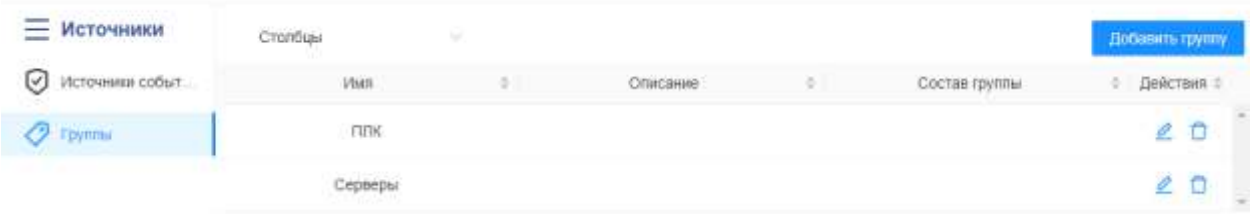

Рисунок 58 – Список групп устройств сети

9.5.1 Добавление группы устройств сети

Для добавления группы устройств сети необходимо выполнить следующие действия:

1. Во вкладке **«Группы»** (см. Рисунок 58) нажать **кнопку «Добавить группу»**.
1. В открывшейся форме **«Создать новую группу»** (см. Рисунок 59) указать значения в полях параметров **«Название»** и **«Описание»**, а затем нажать **кнопку «Сохранить»**.

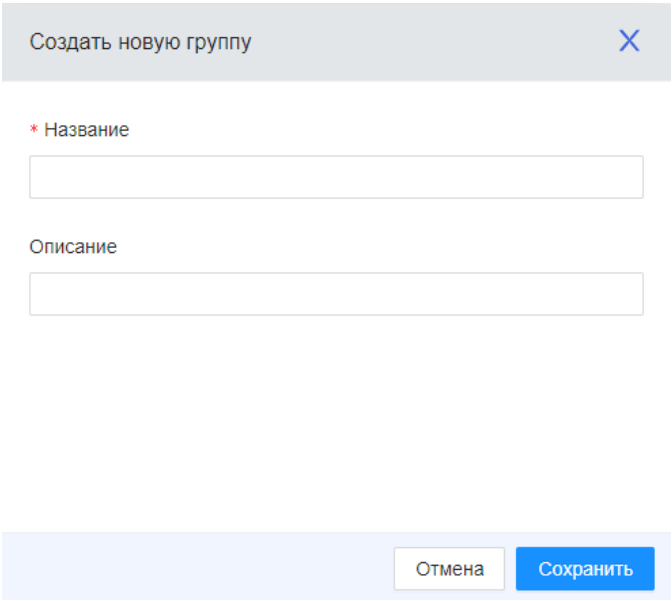

Рисунок 59 – Добавление группы устройств сети

2. В случае успешного создания группы появится соответствующее уведомление (см. Рисунок 91).

9.5.2 Удаление группы устройств сети

Для удаления группы устройств сети необходимо выполнить следующие действия:

1. Во вкладке **«Группы»** нажать **кнопку «**  **»** в строке подлежащей удалению группы устройств сети.
2. Подтвердить удаление, нажав **кнопку «ОК»** в открывшемся уведомлении (см. Рисунок 87).

3. В случае успешного удаления группы появится соответствующее уведомление (см. Рисунок 98).

9.5.3 Редактирование групп

Для редактирования группы активов необходимо выполнить следующие действия:

1. Во вкладке **«Группы»** нажать **кнопку «** **»** в строке подлежащей редактированию группы устройств сети или **кнопку «Редактировать»** в карточке группы.
2. В открывшейся форме **«[Имя группы]»** (см. Рисунок 60) изменить значения в полях параметров, а затем нажать **кнопку «Сохранить»**.

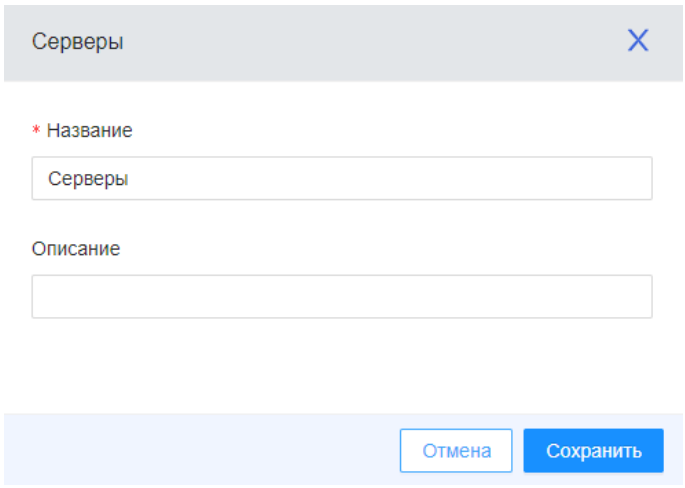

Рисунок 60 – Редактирование группы устройств сети

3. В случае успешного редактирования группы появится соответствующее уведомление (см. Рисунок 99).

9.6 Управление источниками событий ARMA IF

9.6.1 Добавление источника событий ARMA IF

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

Для подключения **ARMA IF** к **ARMA MC** необходимо выполнить следующие шаги:

1. В **ARMA IF** создать УЗ с правами администратора и с ключом API.
2. В **ARMA MC** добавить устройство защиты.
3. В **ARMA IF** настроить экспорт событий по Syslog.

!Важно Взаимодействие **ARMA MC** и **ARMA IF** осуществляется по протоколу HTTPS.

9.6.1.1 Шаг 1. Создание УЗ

В **ARMA IF** необходимо создать УЗ, входящую в группу администраторов **ARMA IF**, по умолчанию **«admins»**. Процесс создания УЗ в **ARMA IF** описан в разделе **«Учетные записи и права доступа»** Руководства пользователя **ARMA IF**.

После создания УЗ необходимо скачать файл, содержащий ключ API данной УЗ. Процесс получения ключа API описан в разделе **«Дополнительные параметры УЗ»** Руководства пользователя **ARMA IF**.

9.6.1.2 Шаг 2. Добавление устройства защиты

Для добавления **ARMA IF** в **ARMA MC** необходимо выполнить процедуру добавления источника событий типа **«ARMA Industrial Firewall»** (см. Раздел 9.2).

Значения параметров **«Ключ»** и **«Секрет»** берутся из файла, скачанного на первом шаге (см. Раздел 9.6.1.1).

Добавленный **ARMA IF** будет отображен в списке источников событий (см. Рисунок 55).

9.6.1.3 Шаг 3. Настройка экспорта событий по Syslog

В **ARMA IF** необходимо настроить экспорт событий со следующими параметрами:

- **«Транспортный протокол»** – «UDP(4)»;
- **«Формат»** – «CEF»;
- **«Имя хоста»** – IP-адрес или доменное имя **ARMA MC**;
- **«Порт»** – порт, указанный при добавлении источника событий (см. Раздел 9.6.1.2).

9.6.2 Загрузка конфигурации на источник/источники событий

Для загрузки файла конфигурации на источник/источники событий необходимо выполнить следующие действия:

1. Выбрать один или несколько источников событий установкой флажка слева от значения столбца **«ID»** выбранных источников событий.
2. Нажать **кнопку «** **»**, находящуюся в верхней части формы раздела.
3. В открывшемся окне проводника выбрать файл конфигурации и нажать **кнопку «Открыть»**.
4. При успешной загрузке конфигурации появится соответствующее уведомление (см. Рисунок 94).
5. Для восстановления подключения к источнику событий, на который был загружен файл конфигурации, необходимо в настройках заменить значения

параметров **«Ключ»** и **«Сервер»** на значения этих же параметров того источника событий, с которого был скачан файл конфигурации.

!Важно После загрузки файла конфигурации необходимо перезагрузить источник событий.

9.6.3 Скачивание конфигурации источника событий

Для скачивания конфигурации источника событий необходимо нажать **кнопку «**  **»** в строке выбранного источника событий. В случае успешной попытки скачивания файла конфигурации появится соответствующее уведомление (см. Рисунок 96).

9.6.4 Обновление базы правил СОВ на источник/источники событий

Для обновления базы правил СОВ на источник/источники событий необходимо выполнить следующие действия:

1. Выбрать один или несколько источников событий установкой флажка слева от значения столбца **«ID»** выбранных источников событий.
2. Нажать **кнопку «**  **»**, находящуюся в верхней части формы раздела.
3. В открывшемся окне проводника выбрать файл наборов правил СОВ и нажать **кнопку «Открыть»**.
4. При успешной загрузке конфигурации появится соответствующее уведомление (см. Рисунок 95).

9.6.5 Перезагрузка источника событий

Для перезагрузки источника событий необходимо нажать **кнопку «**  **»** в строке выбранного источника событий. В случае успешной перезагрузки источника событий появится соответствующее уведомление (см. Рисунок 104).

9.7 Управление источниками событий ARMA IE

9.7.1 Добавление источника событий ARMA IE

Для подключения **ARMA IE** к **ARMA MC** необходимо выполнить следующие шаги:

1. В **ARMA MC** создать техническую УЗ.
2. В **ARMA MC** добавить **ARMA IE**.
3. В **ARMA IE** выполнить настройку синхронизации с **ARMA MC**.

!Важно После подключения **ARMA IE** не рекомендуется изменять IP-адрес **ARMA MC** с целью исключения потери управления.

9.7.1.1 Шаг 1. Создание УЗ

Создание УЗ приведено в разделе 11 настоящего руководства.

9.7.1.2 Шаг 2. Добавление ARMA IE

Для добавления **ARMA IE** в **ARMA MC** необходимо выполнить процедуру добавления источника событий (см. Раздел 9.2).

ARMA IE будет автоматически присвоен порядковый номер после добавления в **ARMA MC**. Порядковый номер отображается в столбце **«ID»** и необходим для настройки синхронизации на третьем шаге (см. Раздел 9.7.1.3).

При добавлении **ARMA IE** возможно указать настройки конфигурации **ARMA IE**. Для этого необходимо перед нажатием **кнопки «Сохранить»** задать соответствующие значения параметров (см. Раздел 9.7.2).

9.7.1.3 Шаг 3. Настройка синхронизации с ARMA MC

В **ARMA IE** необходимо настроить синхронизацию, указав параметры УЗ, созданной на первом шаге (см. Раздел 9.7.1.1) и идентификатор **«ID»**, полученный на втором шаге (см. Раздел 9.7.1.2).

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

9.7.2 Редактирование параметров ARMA IE

Для редактирования параметров **ARMA IE** необходимо выполнить следующие действия:

1. Нажать **кнопку «**  **»** в строке подлежащему редактированию **ARMA IE**.
2. Указать требуемые значения параметров в открывшейся форме **«[Имя источника событий]»** и нажать **кнопку «Сохранить»** для сохранения информации.

Помимо настроек подключения в форме **«[Имя источника событий]»** доступны настройки для редактирования в следующих блоках:

- **«Директории сканирования при запуске»** (см. Раздел 9.7.2.1);
- **«Белый список приложений»** (см. Раздел 9.7.2.2);
- **«Настройки управления устройствами»** (см. Раздел 9.7.2.3);
- **«Настройки ротации событий»** (см. Раздел 9.7.2.4);
- **«Настройки антивируса»** (см. Раздел 9.7.2.5);
- **«Результаты антивирусного сканирования»** (см. Раздел 9.7.2.6).

9.7.2.1 Блок «Директории сканирования при запуске»

Блок **«Директории сканирования при запуске»** (см. Рисунок 61) предназначен для управления функцией **«Контроль целостности» ARMA IE**.

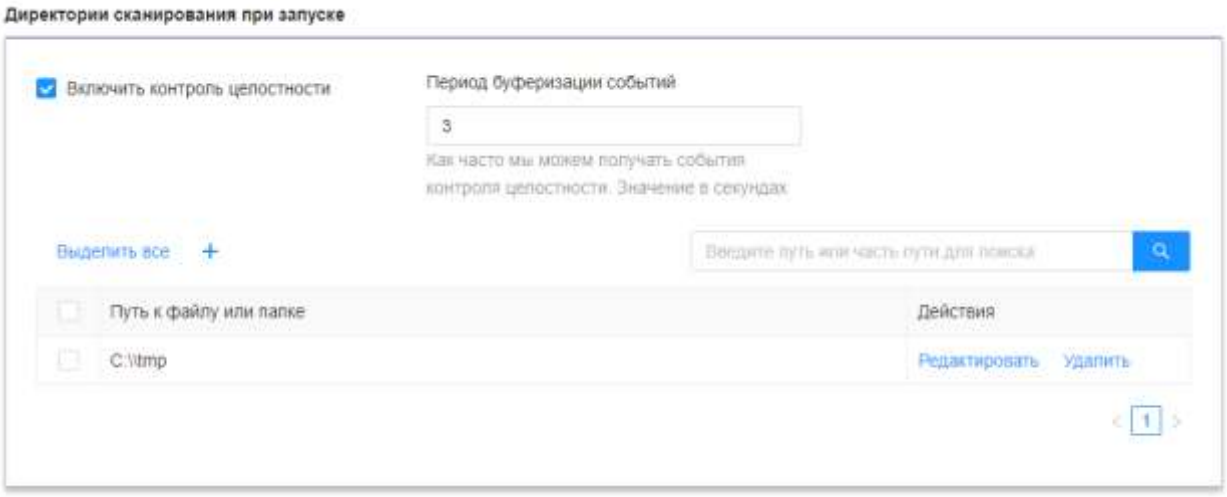

Рисунок 61 – Блок «Директории сканирования при запуске»

Подробная работа функции описана в разделе **«Управление контролем целостности»** Руководства пользователя **ARMA IE**.

Для включения/отключения функции **«Контроль целостности»** необходимо установить/снять флажок для параметра **«Включить контроль целостности»**.

Для добавления директории или файла, подлежащим контролю целостности, в перечень контролируемых директорий необходимо выполнить следующие действия:

1. Нажать **кнопку «+»**.
2. В открывшемся поле (см. Рисунок 62) указать полный путь к директории или файлу, подлежащим контролю целостности, и нажать **кнопку «Сохранить»**.

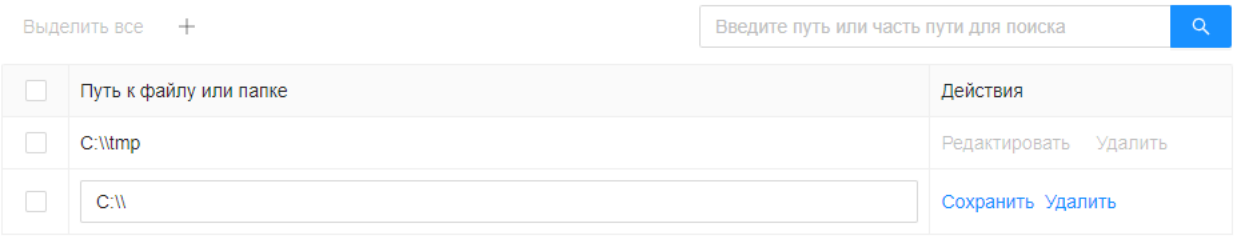

Рисунок 62 – Добавление директории или файла

В поле параметра **«Период буферизации событий»** указывается частота периодического сканирования добавленных файлов и директорий.

9.7.2.2 Блок «Белый список приложений»

Блок **«Белый список приложений»** (см. Рисунок 63) предназначен для управления функцией **«Белый список программ» ARMA IE**.

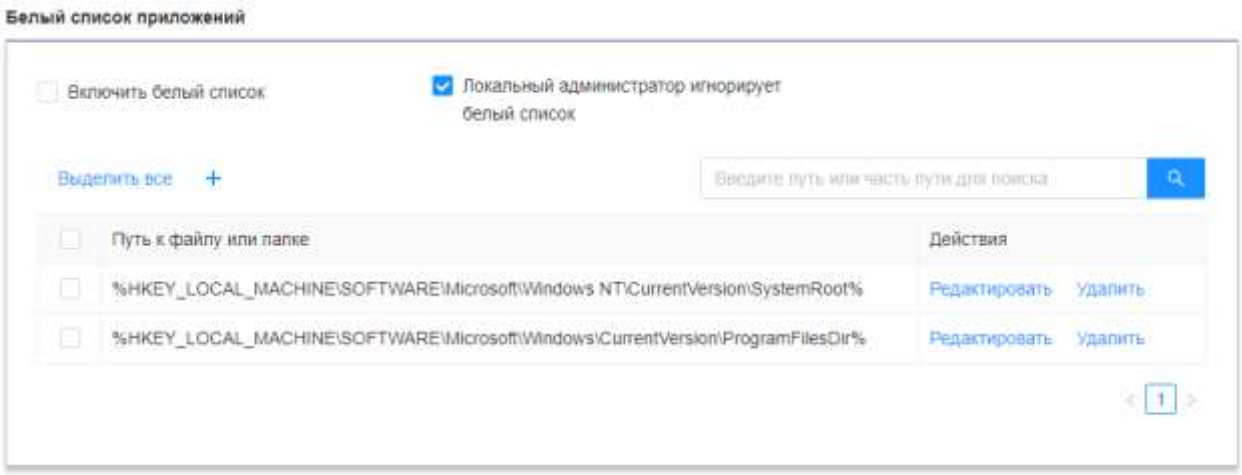

Рисунок 63 – Блок «Белый список приложений»

Подробная работа функции описана в разделе **«Управление белым списком программ»** Руководства пользователя **ARMA IE**.

Для включения/отключения функции **«Белый список программ»** необходимо установить/снять флажок для параметра **«Включить белый список»**.

Для добавления директории, содержащей исполняемые файлы, разрешённые к запуску, в белый список необходимо выполнить следующие действия:

1. Нажать **кнопку «+»**.
2. В открывшемся поле (см. Рисунок 64) указать полный путь к разрешенному к запуску исполняемому файлу или к директории, содержащей разрешенные к запуску исполняемые файлы, и нажать **кнопку «Сохранить»**.

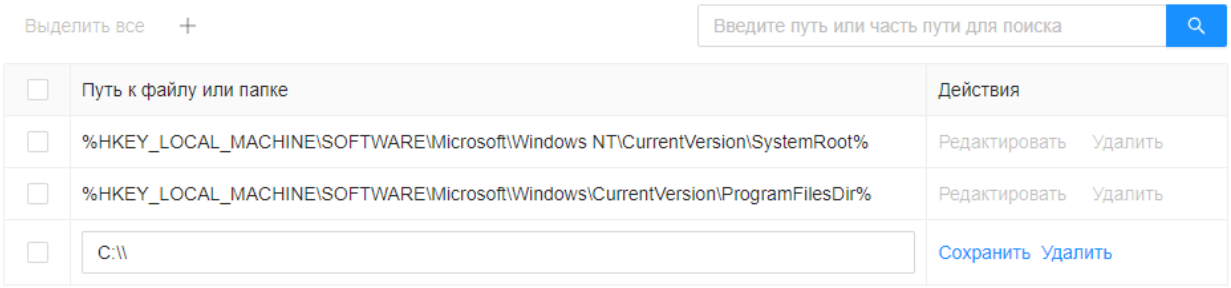

Рисунок 64 – Добавление директории или файла

9.7.2.3 Блок «Настройки управления устройствами»

Блок **«Настройки управления устройствами»** (см. Рисунок 65) предназначен для управления функцией **«Контроль устройств» ARMA IE**.

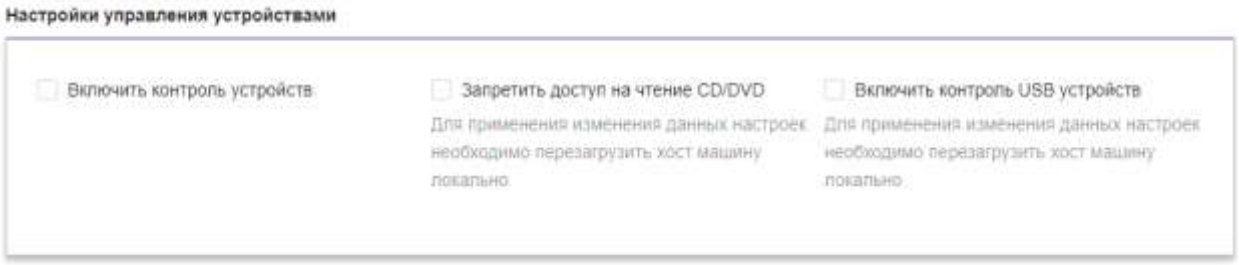

Рисунок 65 – Блок «Настройки управления устройствами»

Подробная работа функции описана в разделе **«Управление контролем устройств»** Руководства пользователя **ARMA IE**.

Для включения/отключения функции **«Контроль устройств»** необходимо установить/снять флажок для параметра **«Включить контроль устройств»**.

Для запрета чтения и записи CD/DVD необходимо установить флажок для соответствующего параметра **«Запретить доступ на чтение CD/DVD»**.

Для включения/отключения функции контроля USB устройств необходимо установить/снять флажок для параметра **«Включить контроль USB устройств»**.

9.7.2.4 Блок «Настройки ротации событий»

Блок **«Настройки ротации событий»** (см. Рисунок 66) предназначен для настройки ротации журнала событий **ARMA IE**.

Рисунок 66 – Блок «Настройки ротации событий»

Подробная работа функции описана в разделе **«Настройка журналирования»** Руководства пользователя **ARMA IE**.

Ротация журнала событий задается в выпадающем списке параметра **«Тип ротации»** и доступна по следующим типам:

- **«Размер»** – размер ротации указывается в поле параметра **«Настройки ротации событий»**;

- **«Время»** – период ротации задаётся с помощью выпадающего списка **«Период ротации событий»** и указания значения в поле параметра **«Время ротации событий»**.

9.7.2.5 Блок «Настройки антивируса»

Блок **«Настройки антивируса»** (см. Рисунок 67) предназначен для управления функцией **«Антивирус» ARMA IE**.

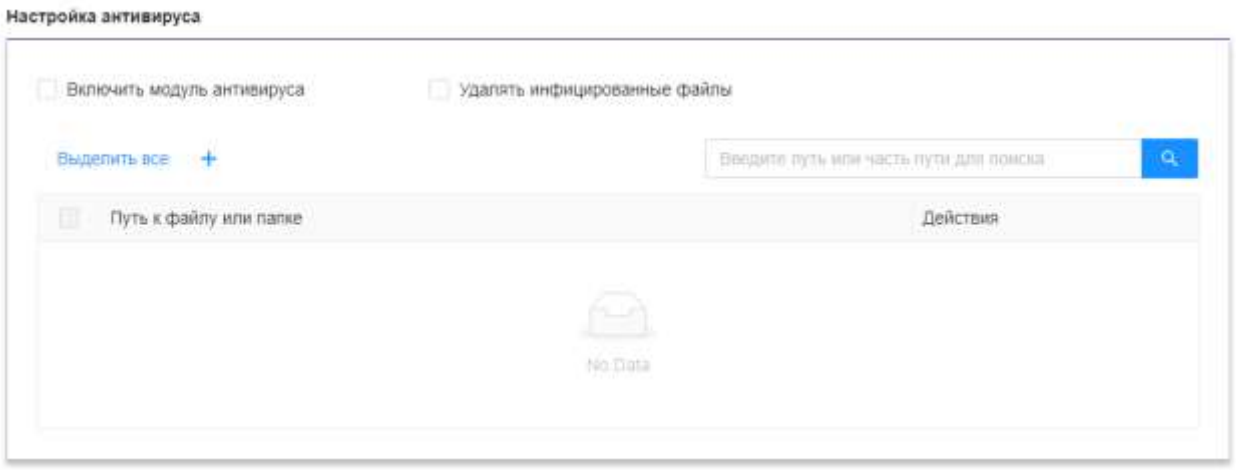

Рисунок 67 – Блок «Настройки антивируса»

Подробная работа функции описана в разделе **«Управление антивирусом»** Руководства пользователя **ARMA IE**.

Для включения/отключения функции **«Антивирус»** необходимо установить/снять флажок для параметра **«Включить модуль антивируса»**.

Для добавления директорий или файлов, подлежащих сканированию на наличие вирусов и вредоносного ПО, необходимо выполнить следующие действия:

1. Нажать кнопку «+».
2. В открывшемся поле (см. Рисунок 68) указать полный путь к директории или файлу, подлежащим сканированию на наличие вирусов и вредоносного ПО, и нажать **кнопку «Сохранить»**.

Рисунок 68 – Добавление директории или файла

Для обновления антивирусной базы всех источников событий Endpoint необходимо нажать **кнопку «»**, расположенную сверху таблицы источников событий, в появившемся окне проводника выбрать файл и нажать **кнопку «Открыть»**.

Все события от функции **«Антивирус»** (см. Рисунок 69) фиксируются в журнале событий (см. Раздел 2).

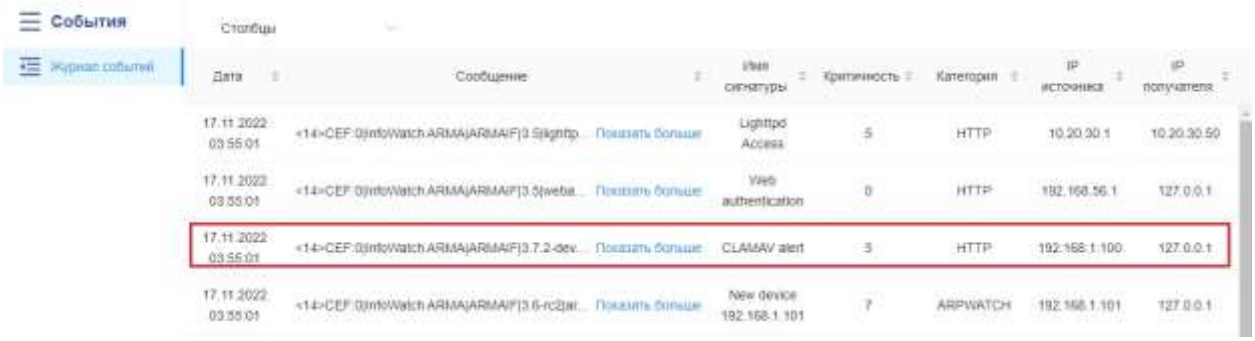

Рисунок 69 – Пример события от функции «Антивирус»

9.7.2.6 Результаты антивирусного сканирования

Блок **«Результаты антивирусного сканирования»** (см. Рисунок 70) предназначен для запуска сканирования на вирусы и просмотра результатов сканирования.

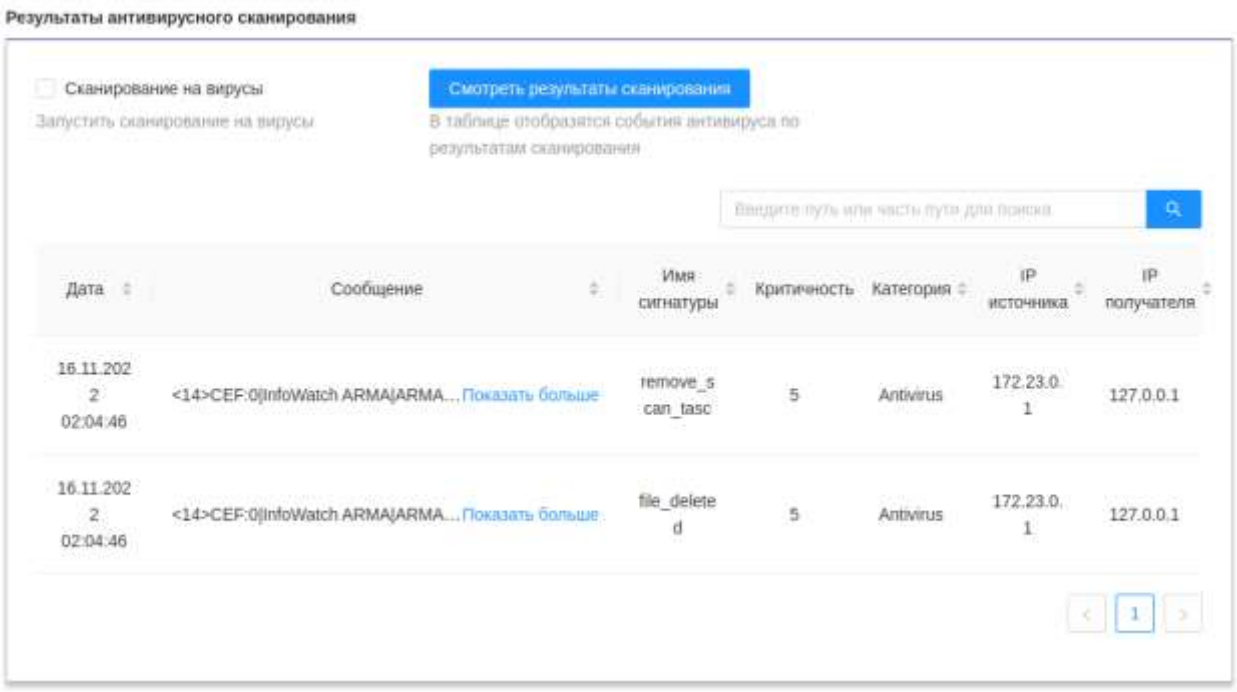

Рисунок 70 – Блок «Результаты антивирусного сканирования»

Для запуска/остановки сканирования на вирусы необходимо установить/снять флажок для параметра **«Сканирование на вирусы»**.

При нажатии **кнопки «Смотреть результаты сканирования»** в таблице произойдет обновление событий антивируса в режиме реального времени.

9.7.3 Обновление конфигурации ARMA IE

Для обновления конфигурации с **ARMA IE** нажать **кнопку «↻»** в строке выбранного **ARMA IE**.

При успешном обновлении конфигурации появится соответствующее уведомление (см. Рисунок 97).

9.7.4 Скачивание конфигурации ARMA IE

Для скачивания конфигурации **ARMA IE** необходимо нажать **кнопку «** **»** в строке выбранного **ARMA IE**.

При успешном скачивании файла конфигурации появится соответствующее уведомление (см. Рисунок 96).

9.7.5 Копирование конфигурации ARMA IE

Для копирования конфигурации **ARMA IE** необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»** в строке выбранного **ARMA IE**.
2. В карточке **«Копирование Endpoint: [Имя Endpoint]»** заполнить обязательные поля:
   - **«Имя»;**
   - **«IP»;**
   - **«Порт»**

   и нажать **кнопку «Сохранить»**.
3. После этого будет создан новый источник событий **ARMA IE** с измененными обязательными полями из п. 2, а остальные настройки будут скопированы.

10 УПРАВЛЕНИЕ СПИСКОМ УСТРОЙСТВ СЕТИ

Раздел **«Таблица активов»** (см. Рисунок 71) позволяет просматривать устройства сети, являющиеся источниками событий или фигурирующие в них.

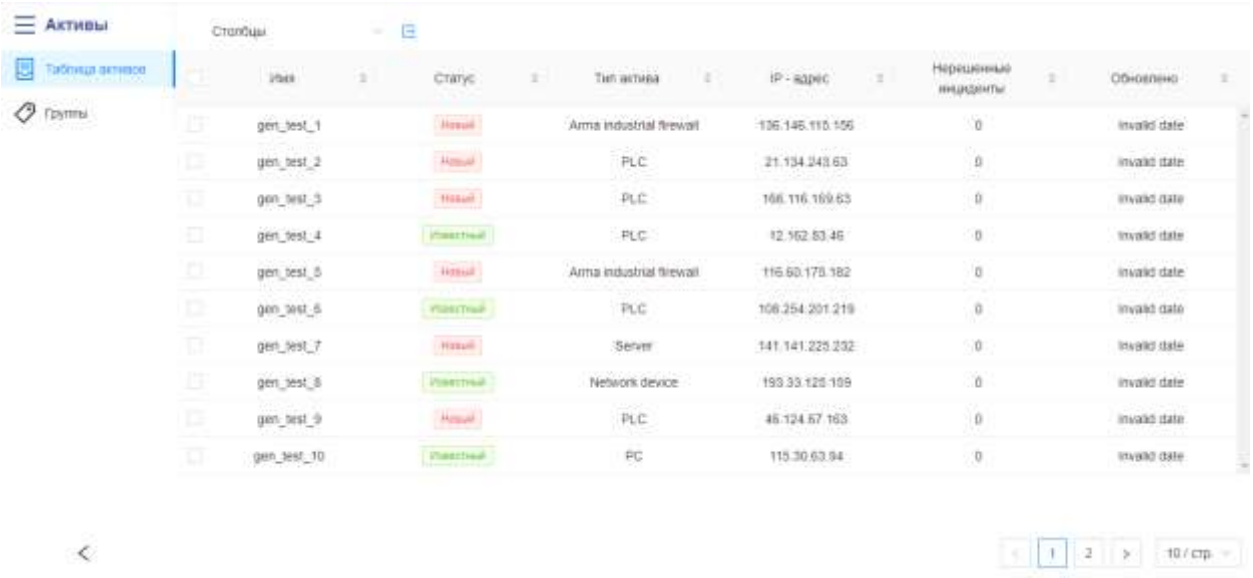

Рисунок 71 – Таблица активов

Для перехода в раздел необходимо развернуть вкладку **«Устройства»** и выбрать пункт **«Активы»**.

10.1 Описание таблицы устройств сети

Раздел позволяет просматривать активы в формате таблицы, содержащей столбцы со следующими данными:

- **«Имя»**;
- **«Статус»**;
- **«Тип актива»**;
- **«IP-адрес»**;
- **«Нерешенные инциденты»**;
- **«Обновлено»**.

10.2 Редактирование основной информации об устройстве сети

Для редактирования основной информации об устройстве сети необходимо выполнить следующие действия:

1. Нажать **левой кнопкой мыши** на запись с нужным активом.
2. В открывшейся форме нажать **кнопку «Редактировать»**, внести изменения в значения параметров и нажать **кнопку «Сохранить»** (см. Рисунок 72).

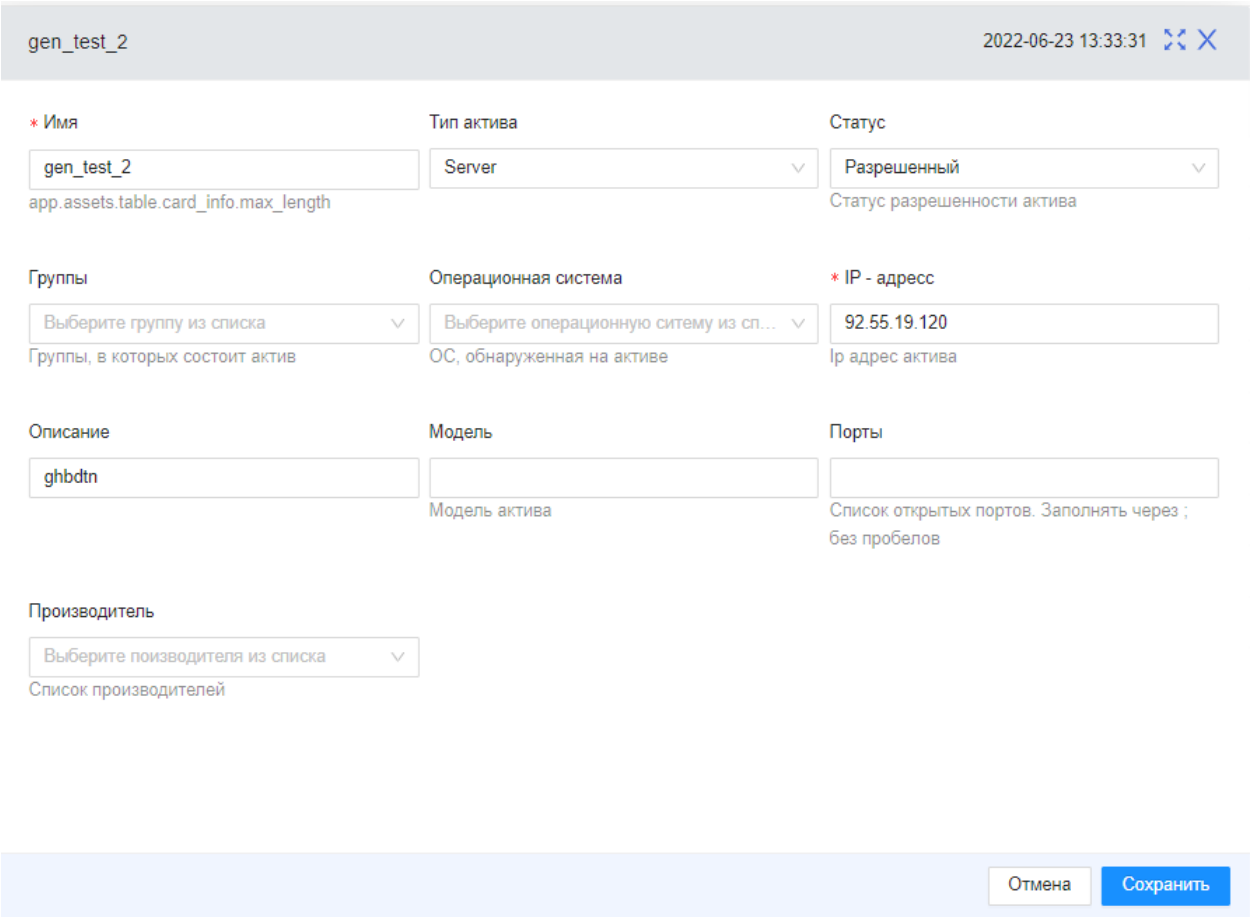

Рисунок 72 – Детали актива

10.3 Управление группами устройств сети

Управление группами устройств сети осуществляется во вкладке **«Группы»**, доступной в левой части формы раздела.

10.3.1 Добавление группы устройств сети

Для добавления группы активов необходимо выполнить следующие действия:

1. Во вкладке **«Группы»** (см. Рисунок 73) нажать **кнопку «Добавить группу»**.

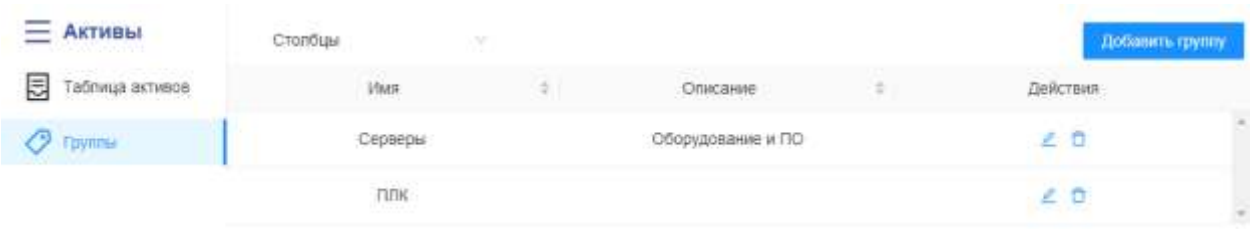

Рисунок 73 – Список групп активов

2. В открывшейся форме **«Создание новой группы»** (см. Рисунок 74) указать значения в полях параметров **«Название»** и **«Описание»**, а затем нажать **кнопку «Сохранить»**.

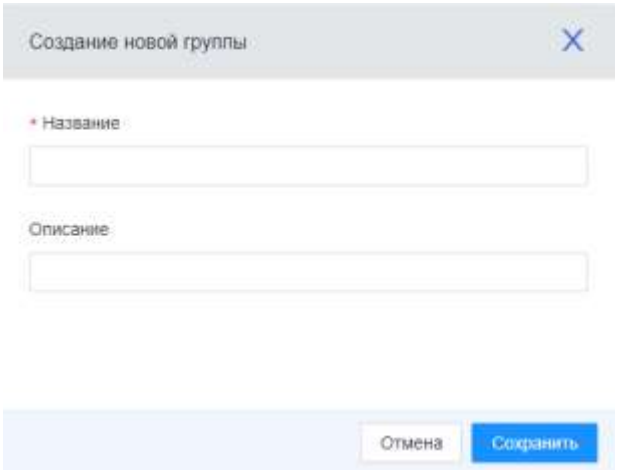

Рисунок 74 – Добавление группы активов

10.3.2 Удаление группы устройств сети

Для удаления группы активов необходимо выполнить следующие действия:

1. Во вкладке **«Группы»** нажать **кнопку «** **»** в строке подлежащей удалению группы активов.
1. Подтвердить удаление, нажав **кнопку «ОК»** в открывшемся уведомлении (см. Рисунок 87).
2. В случае успешного удаления группы появится соответствующее уведомление (см. Рисунок 98).

10.3.3 Редактирование групп

Для редактирования группы активов необходимо выполнить следующие действия:

1. Во вкладке **«Группы»** нажать **кнопку «** **»** в строке подлежащей редактированию группы активов.
2. Нажать **кнопку «Редактировать»**.
3. В открывшейся форме (см. Рисунок 75) изменить значения в полях параметров, а затем нажать **кнопку «Сохранить»**.

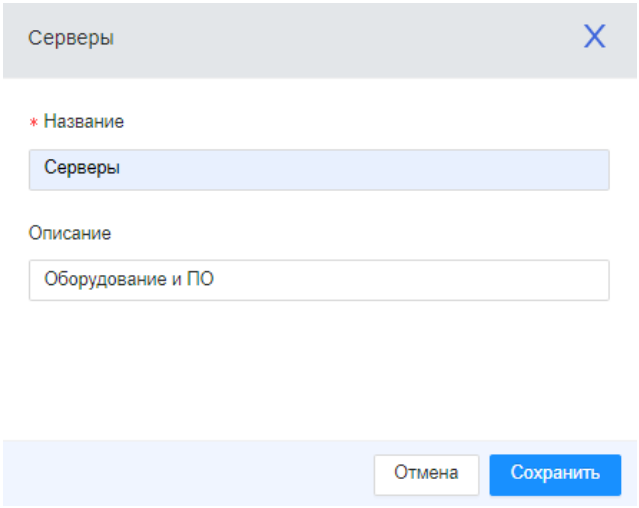

Рисунок 75 – Редактирование группы активов

4. В случае успешного редактирования группы появится соответствующее уведомление (см. Рисунок 99)

11 УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ

11.1 Профиль текущего пользователя

Раздел **«Профиль пользователя»** (см. Рисунок 76) позволяет просматривать подробную информацию об УЗ пользователя.

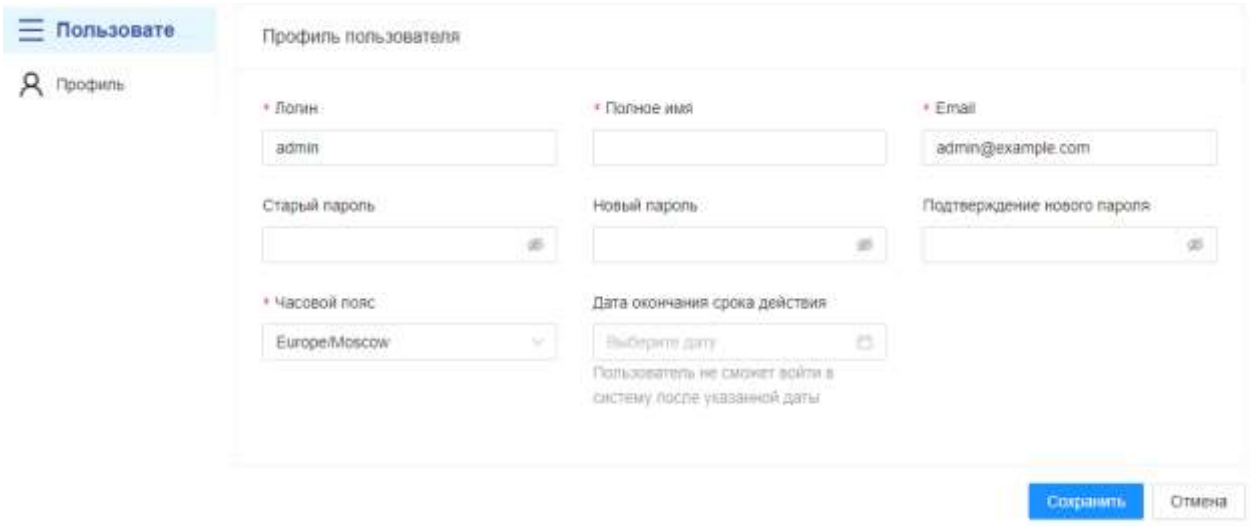

Рисунок 76 – Просмотр профиля выбранного пользователя

Для перехода в раздел текущего пользователя необходимо нажать **кнопку «** **»**, а затем нажать **кнопку «Профиль пользователя»**.

11.1.1 Смена пароля УЗ текущего пользователя

Для смены пароля текущего пользователя необходимо выполнить следующие действия:

1. В разделе **«Профиль пользователя»** (см. Рисунок 76) указать:
   - текущий пароль в поле параметра **«Старый пароль»**;
   - новый пароль в полях параметров **«Новый пароль»** и **«Подтверждение нового пароля»**.
2. Нажать **кнопку «Сохранить»**.

Предъявляются следующие требования к сложности пароля:

- должен содержать как минимум 8 символов;
- должен содержать хотя бы одну цифру, 0-9;
- должен содержать хотя бы одну букву в верхнем регистре, A-Z;
- должен содержать хотя бы одну букву в нижнем регистре, a-z.

11.2 Список пользователей

Раздел **«Список пользователей»** (см. Рисунок 77) отображает все УЗ, зарегистрированные в **ARMA MC**.

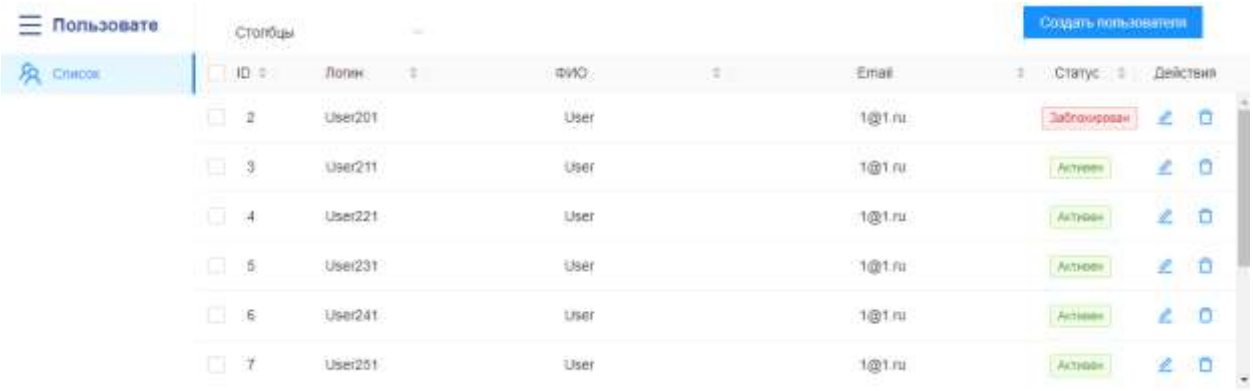

Рисунок 77 – Список пользователей

Для перехода в раздел необходимо нажать **кнопку «»**, а затем нажать **кнопку «Список пользователей»**.

Раздел позволяет просматривать список УЗ в формате таблицы, содержащей столбцы со следующими данными:

- **«ID»**;
- **«Логин»**;
- **«ФИО»**;
- **«Email»**;
- **«Статус»**;
- **«Группы»**;
- **«Действия»**.

В столбце **«Действия»** доступны следующие кнопки управления УЗ:

- **«»** – редактировать УЗ, доступна для УЗ;
- **«»** – удалить УЗ.

11.2.1 Просмотр учетной записи пользователя

Раздел **«Список пользователей»** (см. Рисунок 77) позволяет просматривать подробную информации об УЗ пользователя.

Для просмотра подробной информации об УЗ необходимо нажать **левой кнопкой мыши** в строке УЗ, подлежащей к просмотру.

Для редактирования УЗ необходимо нажать **кнопку «Редактировать»**. Подробная информация о редактировании УЗ представлена в разделе 11.2.3 настоящего руководства.

11.2.2 Добавление учетной записи пользователя

Раздел **«Новый пользователь»** (см. Рисунок 78) позволяет добавить УЗ пользователя.

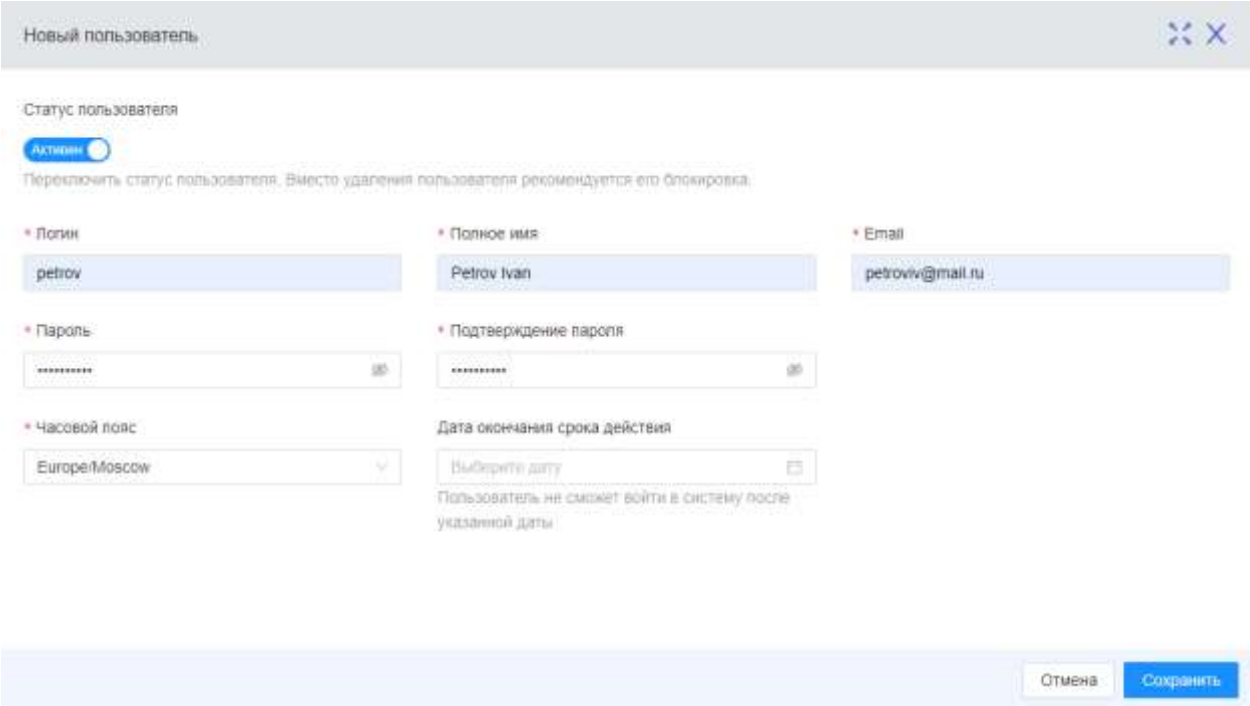

Рисунок 78 – Добавление УЗ пользователя

Для перехода в раздел необходимо нажать **кнопку «Создать пользователя»** во вкладке **«Список»** раздела **«Список пользователей»**.

Для добавления УЗ необходимо выполнить следующие действия:

1. Указать значения в полях обязательных параметров:
   - **«Логин»**;
   - **«Полное имя»**;
   - **«Email»**;
   - **«Пароль»**;
   - **«Повторный ввод пароля»**;
   - **«Часовой пояс»**.
2. При необходимости указать значения для параметров:
   - **«Дата окончания срока действия»**.
3. Нажать **кнопку «Сохранить»**.

Пароль должен соответствовать требованиям, указанным в разделе 11.1.1 настоящего руководства.

!Важно Имя УЗ должно быть уникальным в **ARMA MC**, так как является идентификатором пользователя в **ARMA MC**.

Установленный флажок параметра **«Активный»** предоставляет УЗ доступ в **ARMA MC**, снятый флажок – доступ блокирует.

11.2.3 Редактирование учетной записи пользователя

Раздел **«Редактирование пользователя»** (см. Рисунок 79) позволяет редактировать УЗ пользователя.

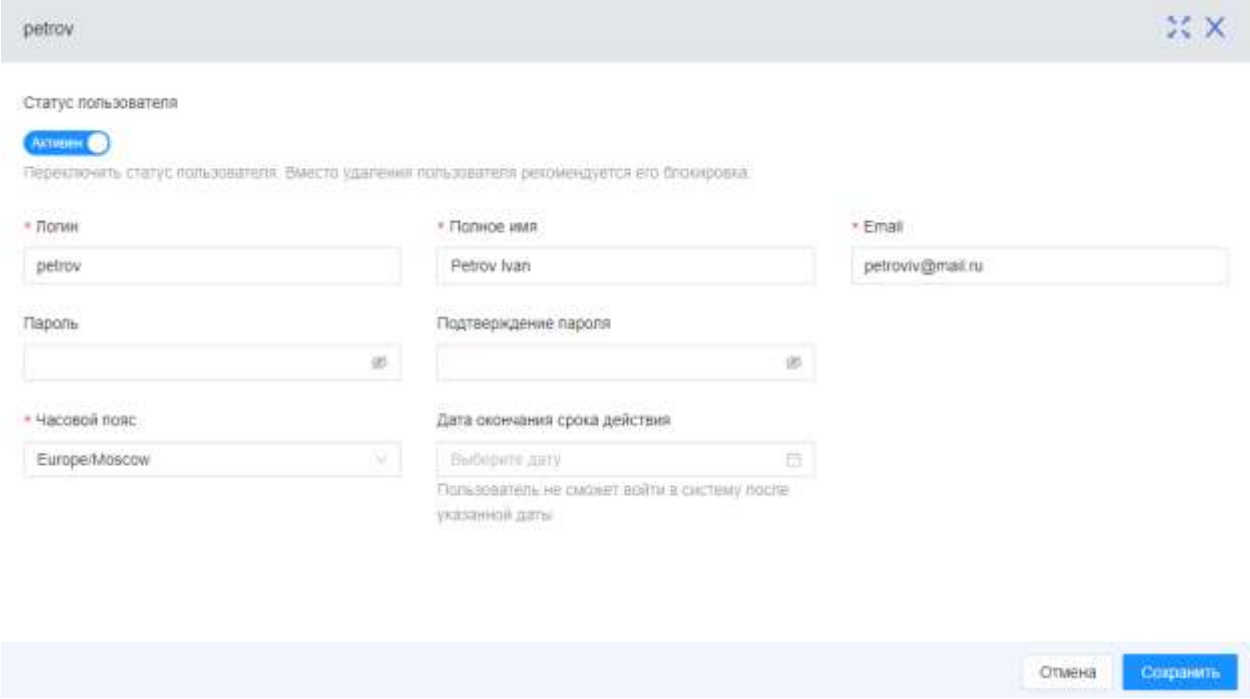

Рисунок 79 – Редактирование учетной записи пользователя

Для перехода в раздел необходимо нажать **кнопку «** **»** в строке подлежащей редактированию УЗ вкладки **«Пользователи»** раздела **«Список пользователей»** или **кнопку «Редактировать»** в карточке пользователя.

Для редактирования УЗ необходимо изменить значения параметров и нажать **кнопку «Сохранить»**.

11.2.4 Удаление учетной записи

Для удаления УЗ из вкладки **«Список»** раздела **«Список пользователей»** необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»** в строке УЗ, подлежащей удалению.

2. Подтвердить удаление, нажав **кнопу «ОК»** в открывшемся уведомлении (см. Рисунок 86).
3. В случае успешного удаления УЗ появится соответствующее уведомление (см. Рисунок 93).

Выбор нескольких УЗ с целью удаления осуществляется установкой флажков слева от значения столбца **«ID»** выбранных УЗ.

Для удаления выбранных УЗ необходимо выполнить следующие действия:

1. Нажать **кнопку «** **»**, находящуюся в верхней части формы вкладки.
2. Подтвердить удаление, нажав **кнопку «ОК»** в открывшемся уведомлении (см. Рисунок 85).

12 УПРАВЛЕНИЕ ГОССОПКОЙ

Раздел **«ГОССОПКА»** (см. Рисунок 80) позволяет информировать НКЦКИ о произошедших инцидентах.

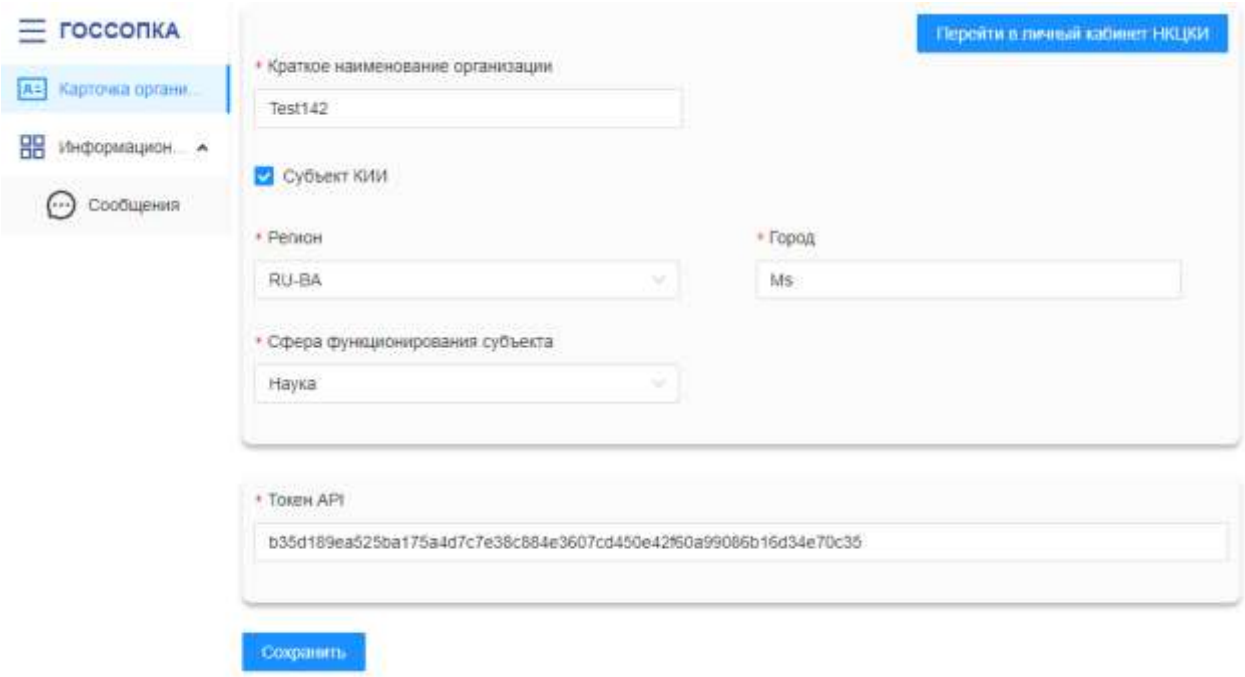

Рисунок 80 – ГОССОПКА

Раздел 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.

Для перехода в раздел необходимо выбрать вкладку **«ГОССОПКА»**.

12.1 Карточка организации

Вкладка **«Карточка организации»** (см. Рисунок 80) отображает информацию об организации, необходимую для отправки уведомлений в НКЦКИ.

Информация о компании содержит следующие параметры:

- **«Краткое наименование организации»**;
- **«Принадлежность к субъектам КИИ»**;
- **«Регион»**;

- **«Город»**;
- **«Сфера функционирования субъекта»;**
- **«Токен API»** – токен для доступа к аппарату ГОССОПКА.

Для перехода в личный кабинет ГОССОПКА необходимо нажать **кнопку «Перейти в личный кабинет НКЦКИ»**.

В случае необходимости сохранения изменений значений полей параметров необходимо нажать **кнопку «Сохранить»**.

12.2 Описание работы с уведомлениями

12.2.1 Сообщения от НКЦКИ

Уведомления отображаются в виде списка со статусом обработки во вкладке **«Сообщения»** (см. Рисунок 81).

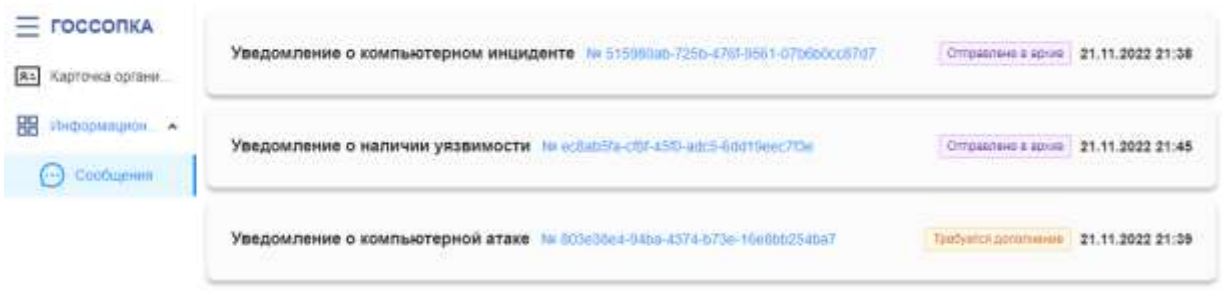

Рисунок 81 – Сообщения от НКЦКИ

При нажатии на строку с уведомлением откроется форма в формате переписки, в которой есть возможность отвечать сотрудникам НКЦКИ. Для этого необходимо ввести информацию в поле ввода **«Введите текст»** и нажать **кнопку «Отправить»** (см. Рисунок 82).

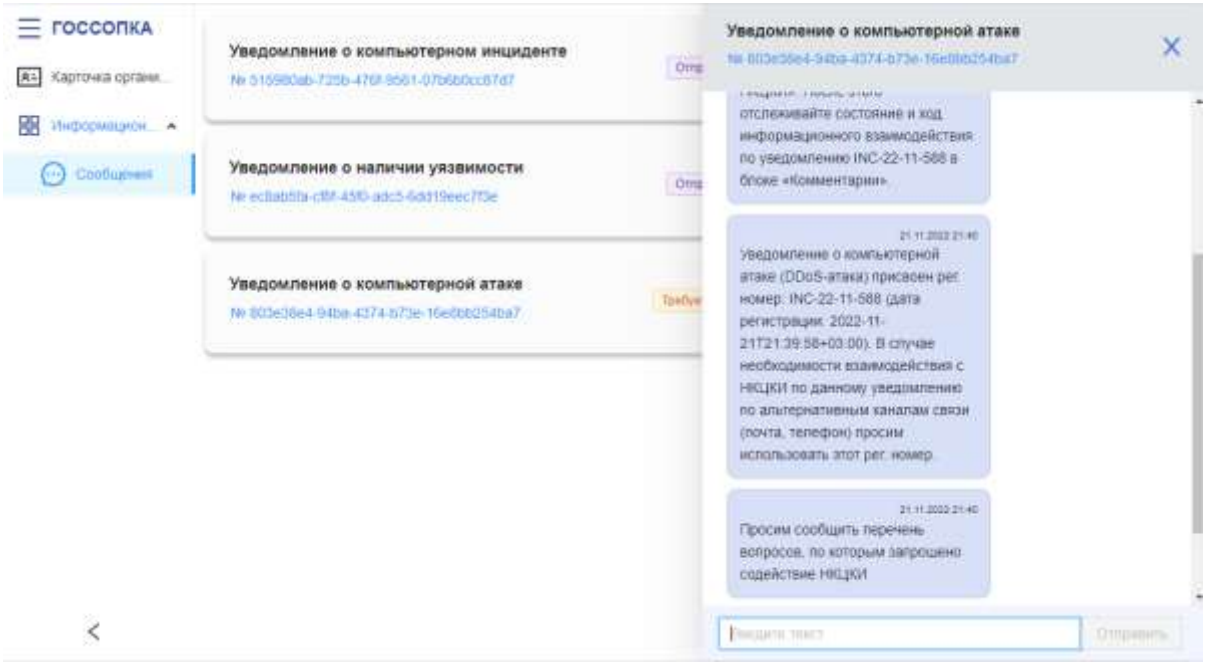

Рисунок 82 – Работа с уведомлениями

Для просмотра информации об инциденте, породившего уведомление, необходимо нажать **левой кнопкой мыши** ссылку идентификационного номера инцидента, расположенную рядом с названием уведомления.

12.2.2 Отправка уведомления об инциденте в НКЦКИ

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

1. Открыть подробную информацию об инциденте (см. Раздел 3.2) и нажать **кнопку «Отправить в ГосСОПКА»**.
2. В открывшейся форме **«Уведомления в ГосСОПКА»** (см. Рисунок 83) выбрать категорию уведомления из выпадающего списка:
   - **«Уведомление о компьютерном инциденте»**;
   - **«Уведомление о компьютерной атаке»**;
   - **«Уведомление о наличии уязвимости»**.
3. Указать значения обязательных параметров:
   - для всех уведомлений:
     - **«Тип события ИБ»**;
     - **«Статус реагирования»**;
     - **«Статус конфиденциальности»**;
     - **«Наименование контролируемого ресурса»**;
     - **«Описание события»**.

- для уведомлений категорий **«Уведомление о компьютерном инциденте»** и **«Уведомление о компьютерной атаке»** в блоке **«Последствия»:**
  - **«Влияние на целостность»**;
  - **«Влияние на доступность»**;
  - **«Влияние на конфиденциальность»**.

остальные поля заполняются вручную при необходимости. Нажать **кнопку «Отправить»**.

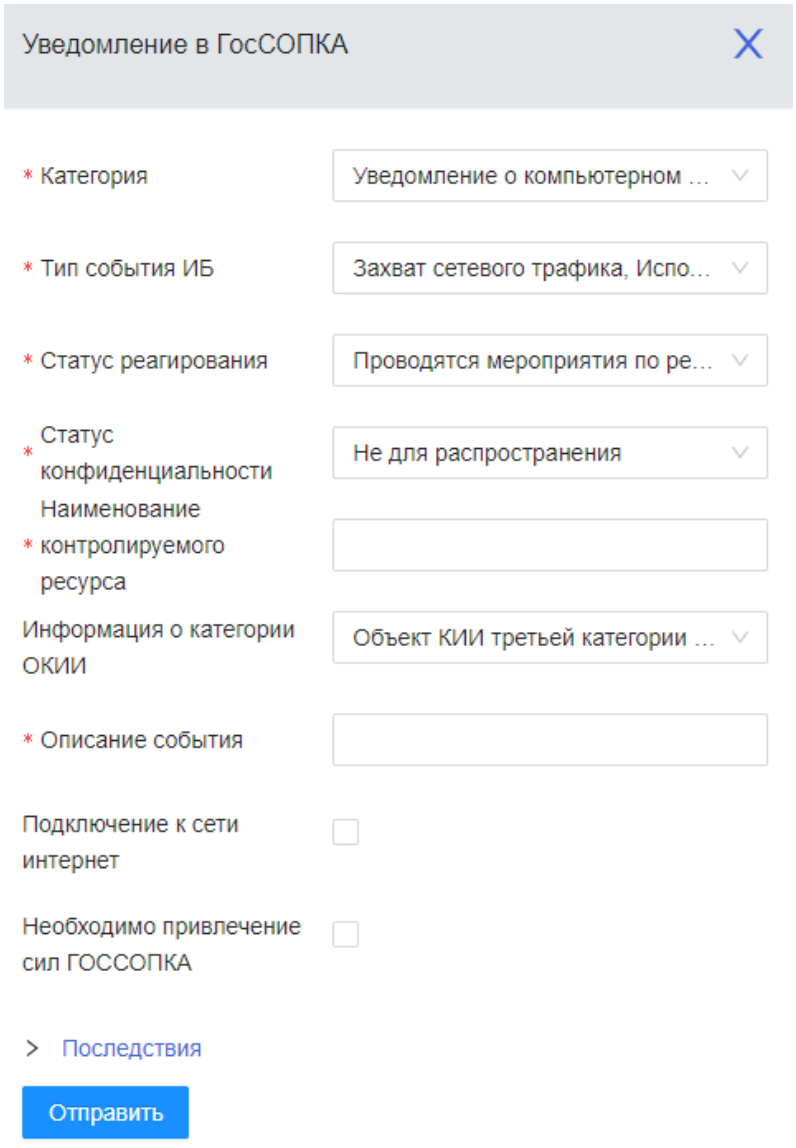

Рисунок 83 – Форма заполнения уведомления в ГосСОПКА

13 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

13.1 Предупреждения при необходимости подтверждения действий

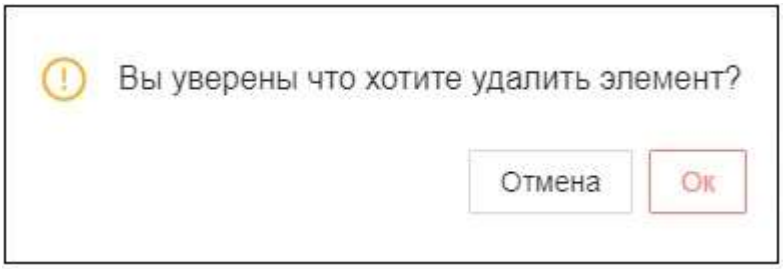

Рисунок 84 – Подтверждение удаления элемента

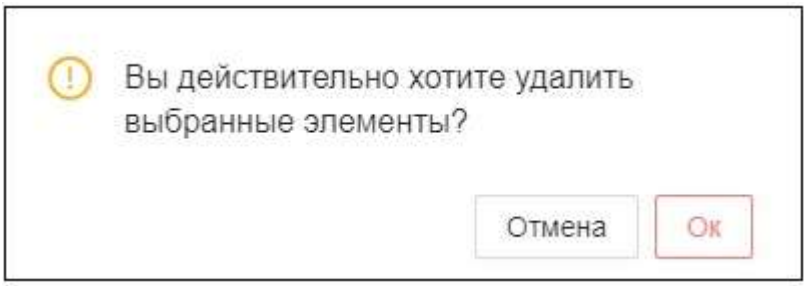

Рисунок 85 – Подтверждение удаления выбранных элементов

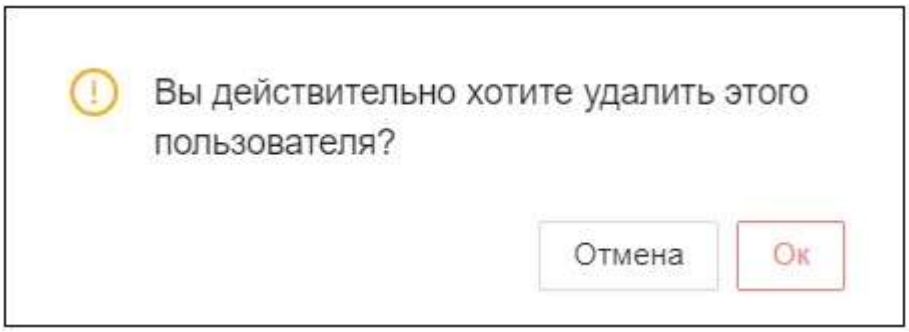

Рисунок 86 – Подтверждение удаления пользователя

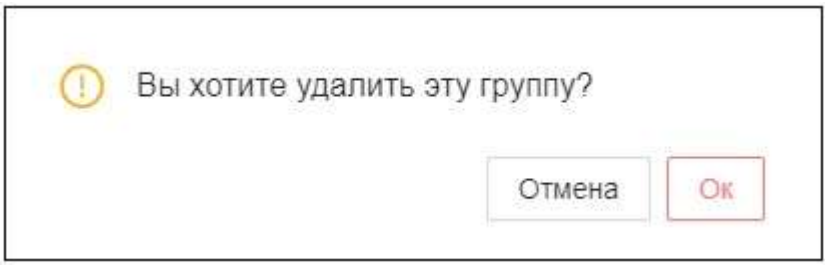

Рисунок 87 – Подтверждение удаления группы

13.2 Предупреждения при любом неправильном вводе данных в поле

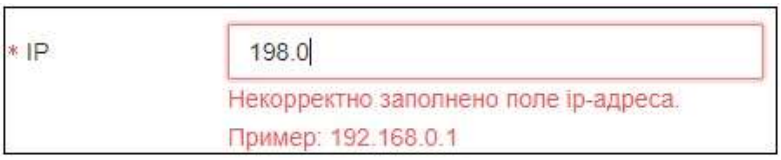

Рисунок 88 – Предупреждение о неправильном вводе в поле №1

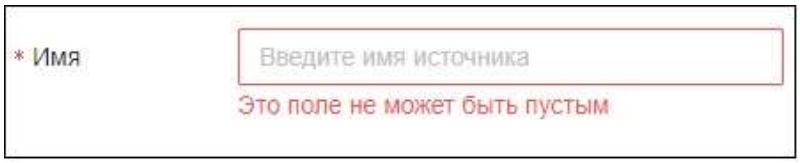

Рисунок 89 – Предупреждение о неправильном вводе в поле №2

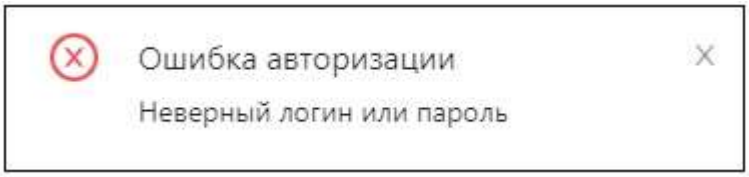

Рисунок 90 – Предупреждение о неправильном вводе в поле №3

13.3 Предупреждения при применении настроек

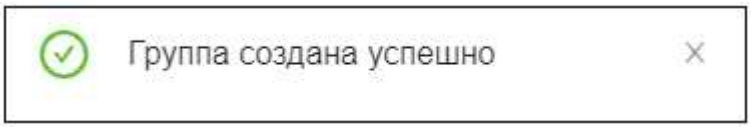

Рисунок 91 – Добавление группы

Рисунок 92 – Создание пользователя

Рисунок 93 – Удаление пользователя

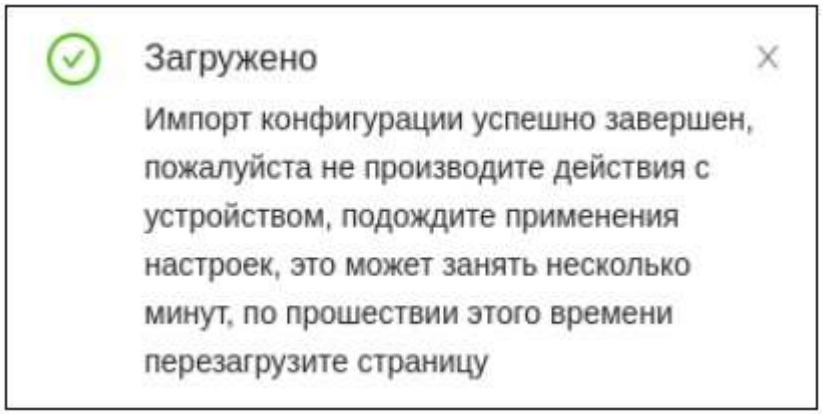

Рисунок 94 – Загрузка конфигурации

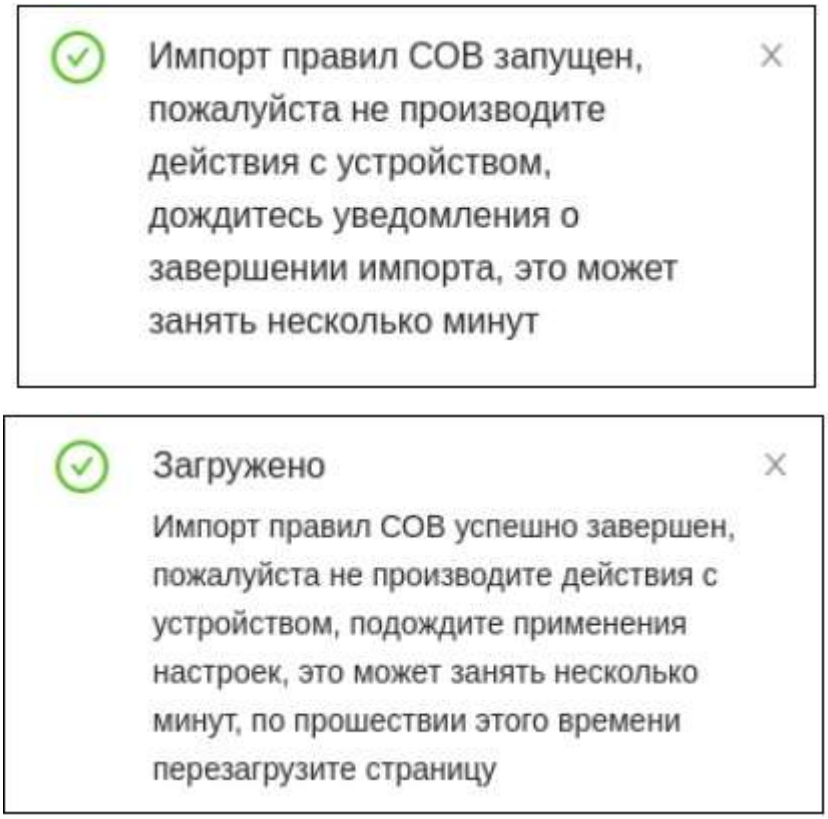

Рисунок 95 – Загрузка/импорт правил СОВ

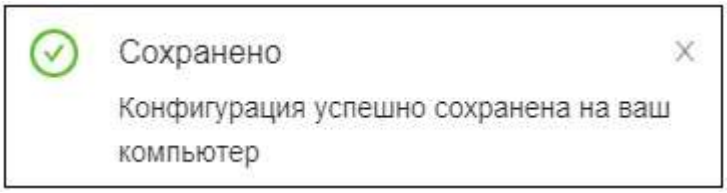

Рисунок 96 – Скачивание конфигурации

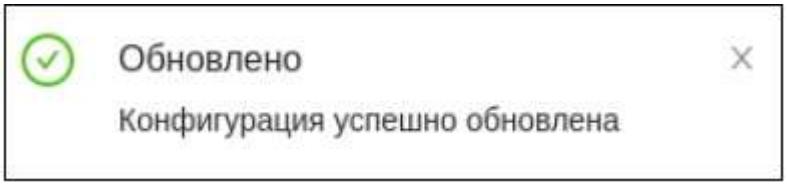

Рисунок 97 – Обновление конфигурации Endpoint

Рисунок 98 – Удаление группы

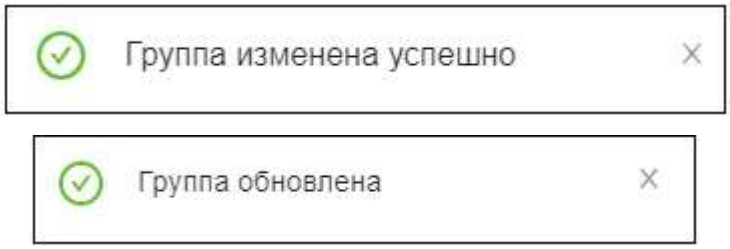

Рисунок 99 – Редактирование группы

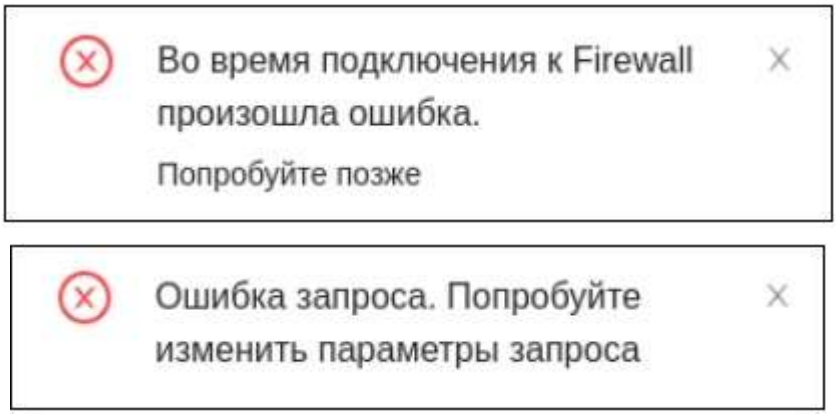

Рисунок 100 – Уведомления об ошибке подключения к источнику событий ARMA Industrial Firewall

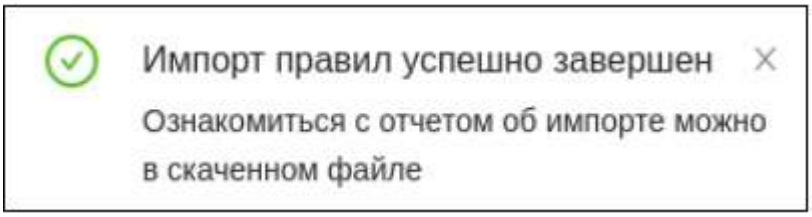

Рисунок 101 – Успешный импорт правил корреляции

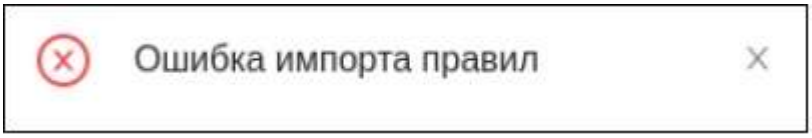

Рисунок 102 – Неуспешный импорт правил корреляции

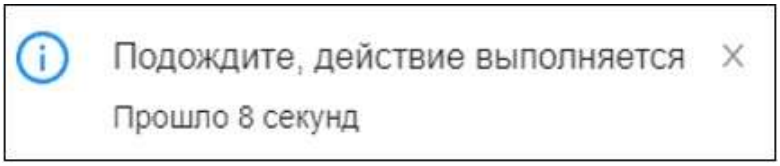

Рисунок 103 – Ожидание окончания импорта правил

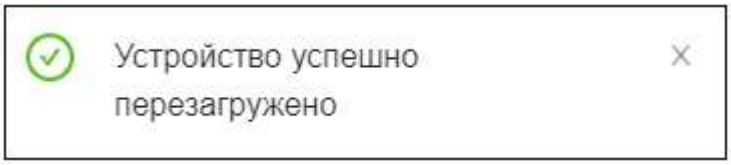

Рисунок 104 – Успешная перезагрузка устройства

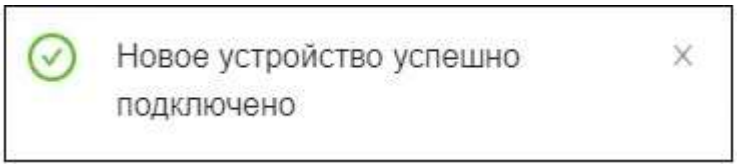

Рисунок 105 – Успешное добавление источника событий

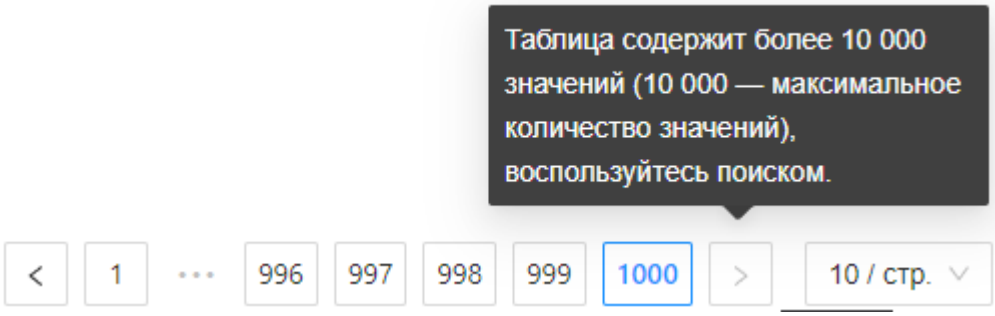

Рисунок 106 – Уведомление при превышении количества записей в журнале событий

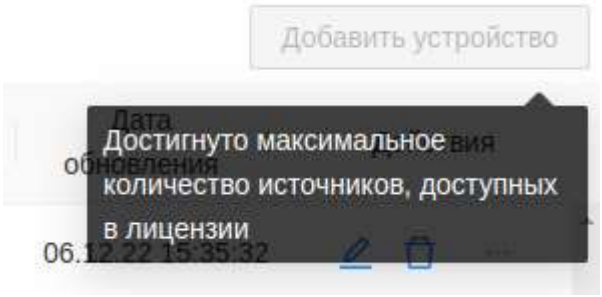

Рисунок 107 – Уведомление о превышении количества источников событий