Руководство пользователя по эксплуатации

версия 32 ред. от 24.12.2021

Листов 111

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОС	–	операционная система
ПК	–	программный комплекс
СОВ	–	система обнаружения вторжений
DHCP	–	(англ. Dynamic Host Configuration Protocol) – протокол динамической настройки узла
HTTP	–	(англ. HyperText Transfer Protocol) – протокол передачи гипертекста
HTTPS	–	(англ. HyperText Transfer Protocol Secure) – расширенный протокол HTTP
ID		идентификатор
IP	–	(англ. Internet Protocol) – межсетевой протокол
MAC	–	(англ. Media Access Control) – управление доступом к среде
SID	–	(англ. Security IDentifier) – идентификатор безопасности
TLS	–	(англ. Transport Layer Security) – протокол защиты транспортного уровня

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, которые выполняют конфигурирование и мониторинг работы ARMA Management Console версии 1.1.0.

Руководство пользователя по эксплуатации содержит описание графического и консольного интерфейса, доступных функций с подробным описанием их настройки и использования, а также принципов работы с ARMA Management Console.

Перед эксплуатацией ARMA Management Console пользователю необходимо изучить настоящее руководство.

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Общие сведения

ARMA Management Console представляет собой единый центр управления решениями InfoWatch ARMA и реагирования на инциденты и решает следующие задачи:

- расследование инцидентов ARMA Industrial Firewall;
- централизованное управление ARMA Industrial Firewall;
- доступ к веб-интерфейсу управляемых устройств ARMA Industrial Firewall;
- управление правилами СОВ на ARMA Industrial Firewall;
- управление конфигурацией ARMA Industrial Firewall;
- управление списком устройств сети;
- построение карты сети:
  - по анализу трафика (по производителю, по типу ОС, по назначению устройства);
  - отображение групп устройств;
  - отображение несанкционированных сетевых узлов (хостов);
  - отображение несанкционированных информационных потоков;
  - отображение информации об устройстве (IP-адрес, MAC-адрес, наименование и производитель сетевой карты);
- управление учетными записями и правами доступа ARMA Management Console.

1.2 Требования к среде функционирования

Установка ARMA Management Console производится на следующие типы платформ:

- аппаратная;
- виртуальная (гипервизор).

Установка на аппаратную платформу выполняется с использованием USB-накопителя, на который должен быть записан образ ARMA Management Console в формате «*.ISO».

Установка на виртуальную платформу (гипервизор) производится с помощью образа в формате «*.ISO».

1.2.1 Требования к аппаратной платформе

При установке ARMA Management Console на аппаратную платформу необходимо использовать микропроцессорную архитектуру x64 или Байкал-М (ARMv8).

Для аппаратной платформы, на которую устанавливается ARMA Management Console достаточно руководствоваться минимальными требованиями к аппаратному обеспечению (Таблица 1).

Таблица 1 – Минимальные требования к аппаратному обеспечению

Название оборудования	**Требования**
Процессор	2,0 ГГц, четырехъядерный, x64 или Байкал-М (ARMv8)
ОЗУ	16 ГБ
Интерфейсы, необходимые для установки программного обеспечения	Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры
Жесткий диск	512 ГБ, SSD
Сетевые интерфейсы	Не менее 1 x Ethernet 100/1000 Мбит/сек

1.2.2 Требования к виртуальной платформе

Виртуализация ARMA Management Console поддерживается для следующих виртуальных платформ (гипервизоров):

- HyperV Generation 1;
- VirtualBox версии 6.0.4 и выше;
- VMware ESXi версии 5.5 обновления 2 и выше.

Для запуска ARMA Management Console предъявляются следующие минимальные требования к виртуальной среде:

Таблица 2 – Минимальные требования к виртуальной среде

Название оборудования	**Требования**
Процессор	4 ядра
Объем оперативной памяти	16 ГБ
Размер виртуального диска	512 ГБ
Сетевые интерфейсы	Не менее 1

Для корректного отображения веб-интерфейса к веб-браузерам предъявляются следующие требования:

- для ОС семейства Windows:
  - Chrome, Firefox;
- для ОС семейства Linux:
  - Chrome для Linux, Firefox для Linux.

2 НАЧАЛО РАБОТЫ

2.1 Установка

Установка ARMA Management Console производится с установочного носителя (образа диска в формате «*.ISO», flash-накопителя, DVD-диска). При загрузке будет запущен обратный отсчёт до начала установки равный 10 секундам. Чтобы пропустить обратный отсчёт необходимо выбрать тип установки системы «Quick install» и нажать «Enter» (Рисунок 1).

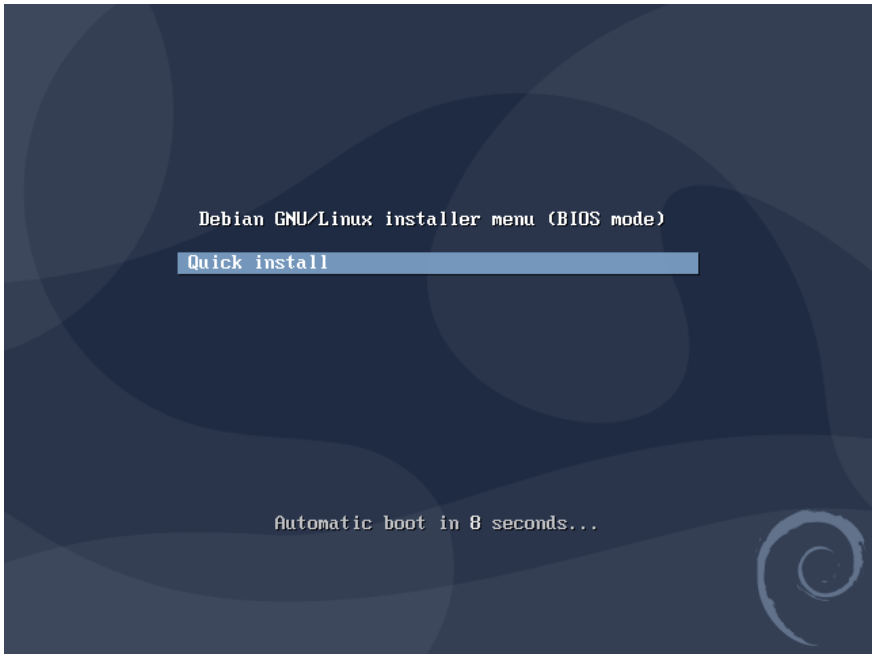


Рисунок 1 – Выбор типа установки

Затем запустится загрузка списка пакетов для установки системы (Рисунок 2).

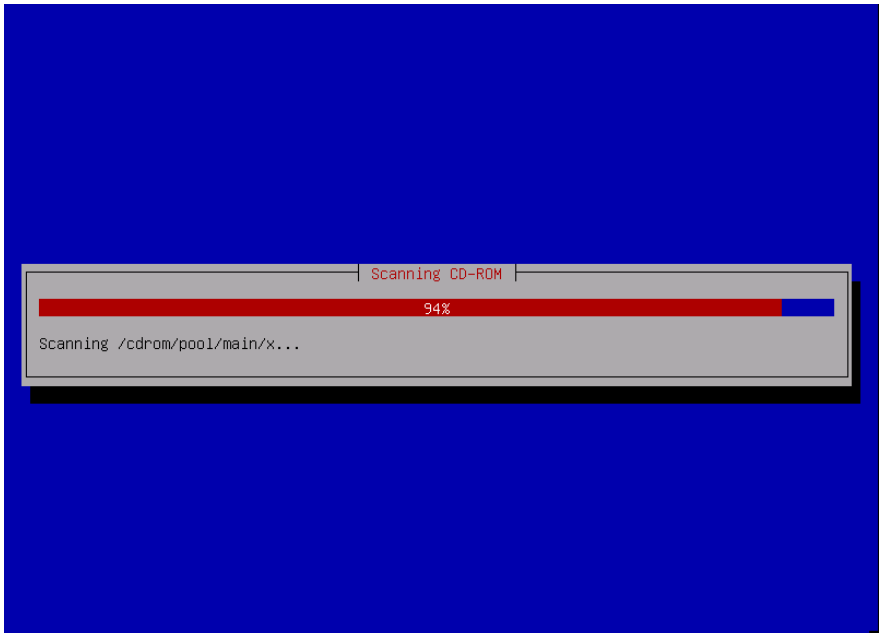


Рисунок 2 – Загрузка списка пакетов

Далее необходимо ввести имя хоста для системы или оставить его по умолчанию и нажать «Enter» (Рисунок 3)

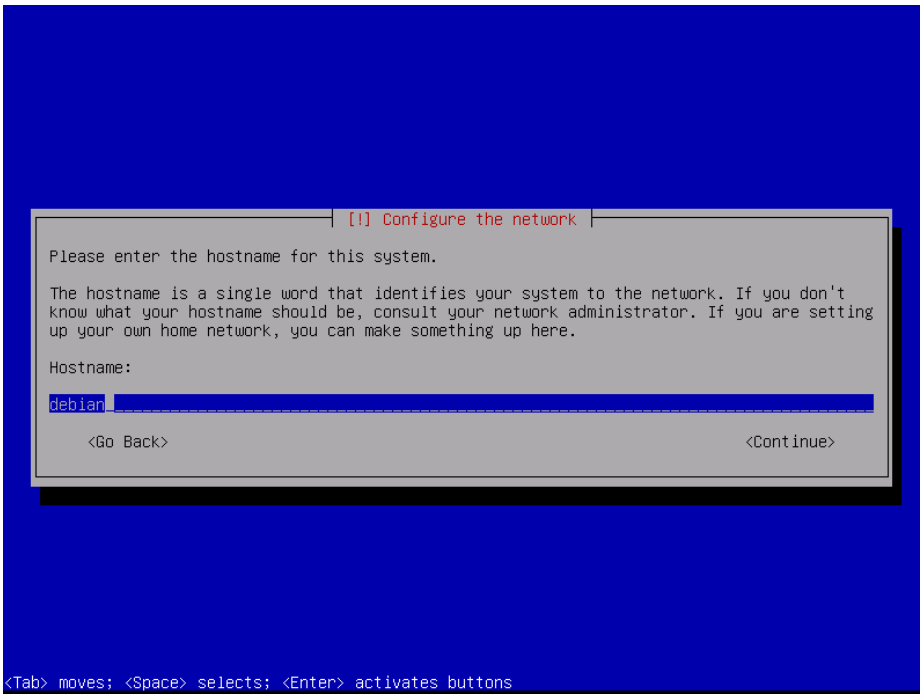


Рисунок 3 – Настройка сети. Выбор имени хоста

После выбора имени хоста необходимо задать доменное имя или оставить его по умолчанию и нажать на «Enter» (Рисунок 4).

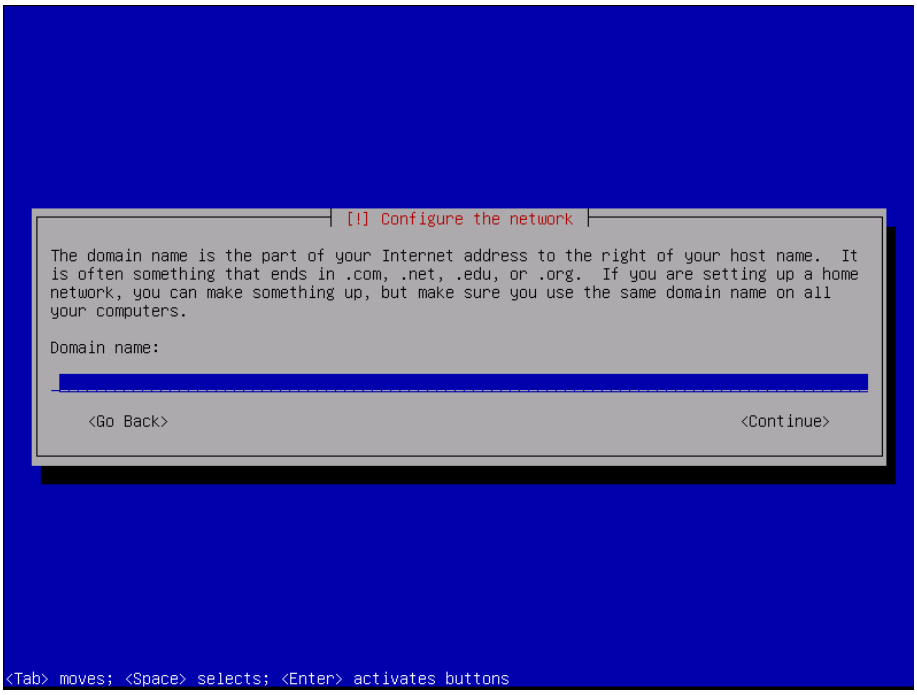


Рисунок 4 – Настройка сети. Выбор доменного имени

Затем необходимо установить пароль для учетной записи «root» и подтвердить его (Рисунок 5, Рисунок 6).

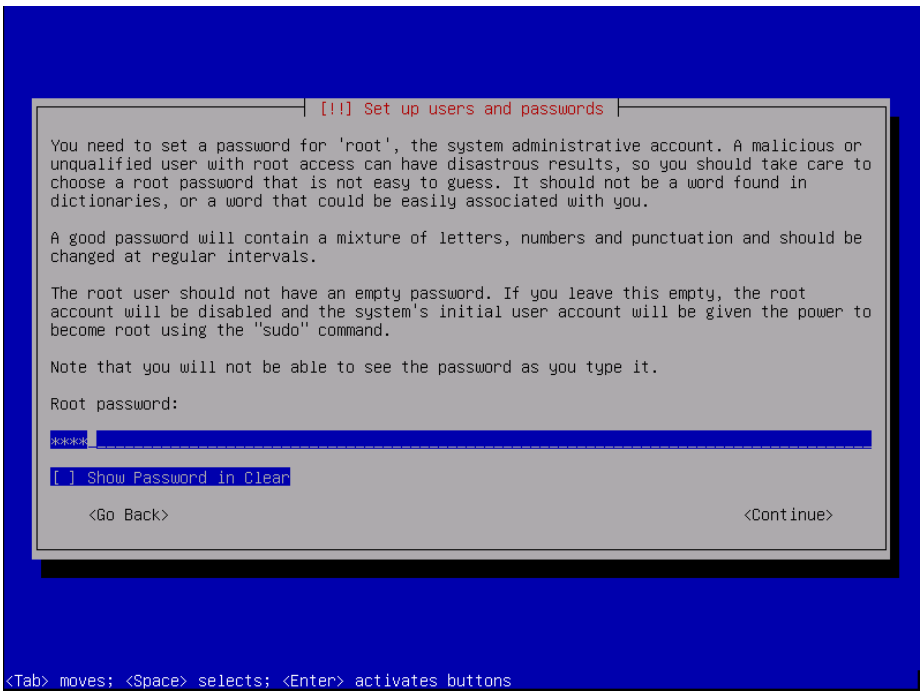


Рисунок 5 – Настройка пользователей и паролей. Ввод пароля

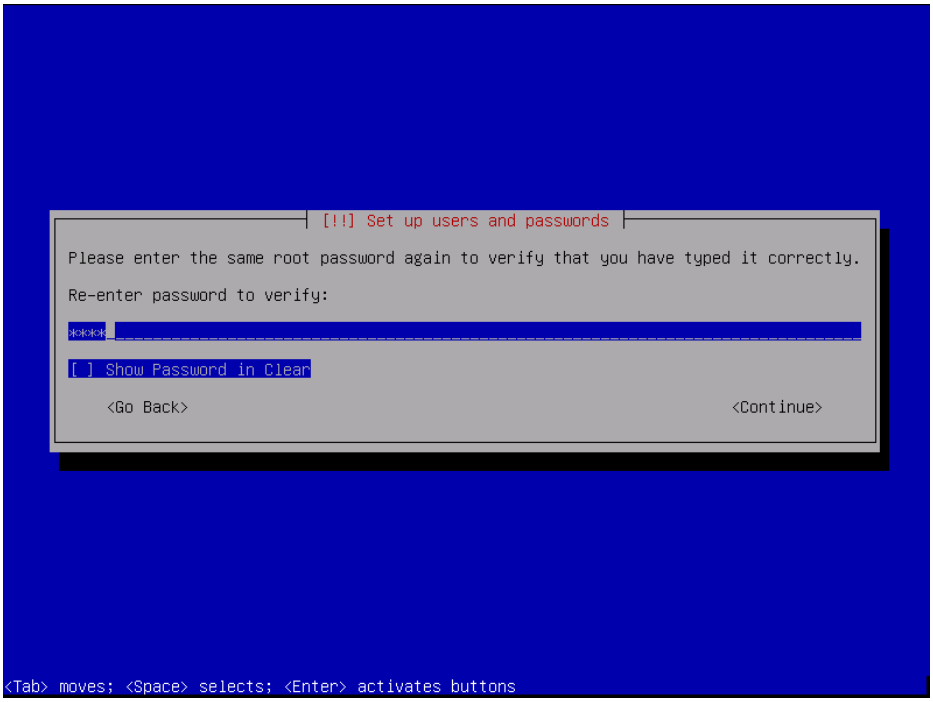


Рисунок 6 – Настройка пользователей и паролей. Повтор пароля

Далее перед настройкой диспетчера логических томов необходимо подтвердить запись текущей схемы секционирования на диск. Для этого необходимо выбрать «Yes» и нажать на «Enter» (Рисунок 7).

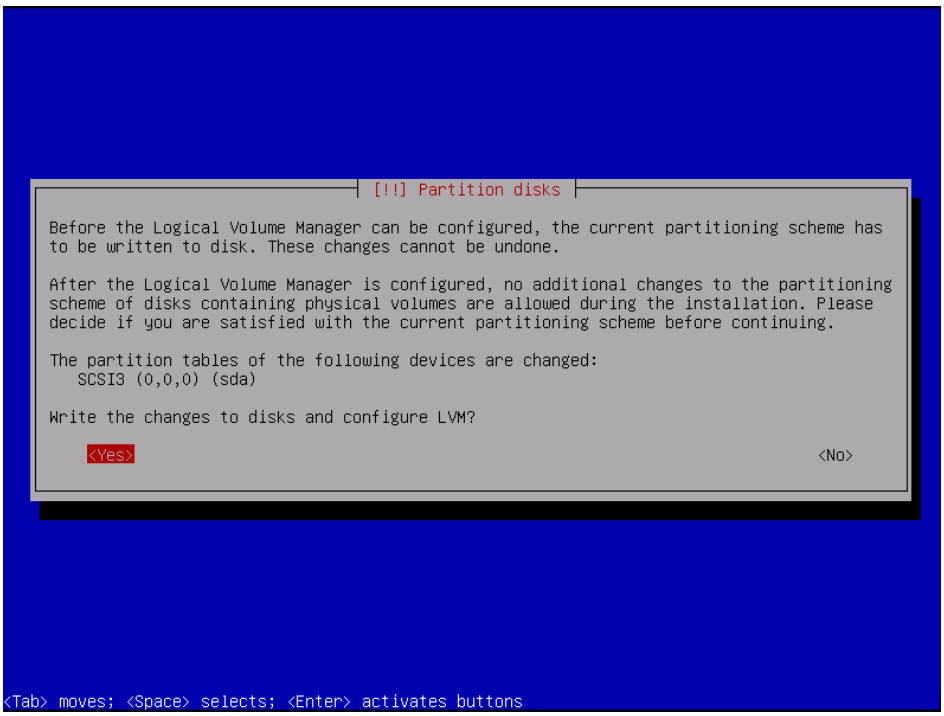


Рисунок 7 – Диски разделов

Рисунок 8 – Установка базовой системы

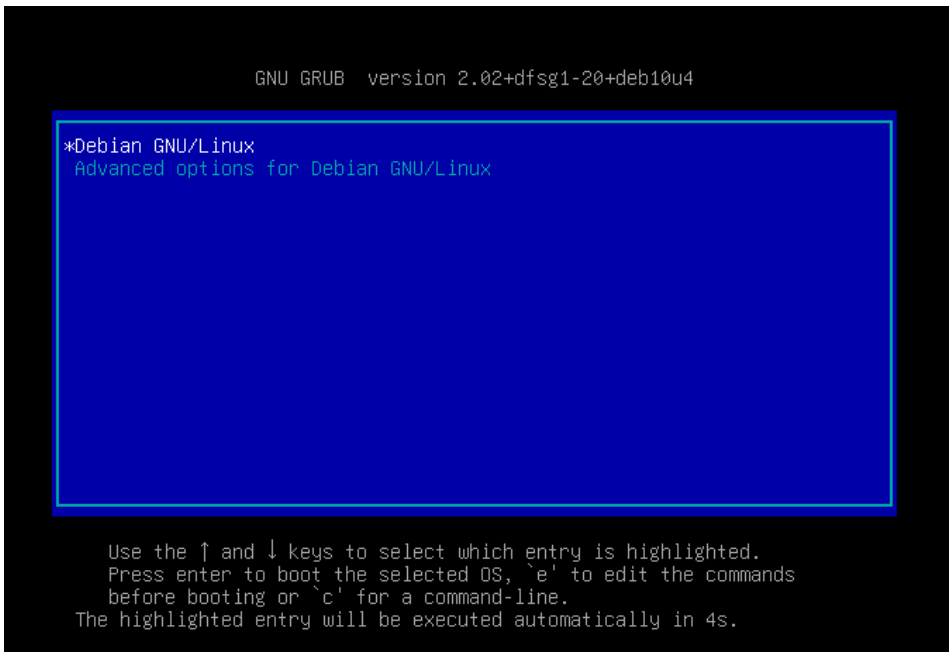


Рисунок 9 – Загрузка системы

Рисунок 10 – Аутентификация в локальном (консольном) интерфейсе

2.2 Базовая настройка сетевых интерфейсов

Адрес по умолчанию выдается по DHCP для каждого интерфейса у ARMA Management Console.

Для того чтобы задать IP-адрес для сетевого интерфейса необходимо:

1. Зайти в локальный (консольный) интерфейс, используя учетные данные пользователя по умолчанию (логин – root, пароль – root).

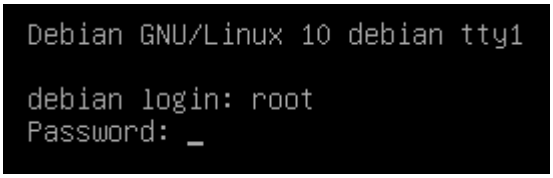


Рисунок 11 – Вход в локальный (консольный) интерфейс

2. Выполнить команду *nano /etc/network/interfaces*
3. Задать параметры в секции #The primary network interface согласно рисунку ниже (Рисунок 12) и сохранить изменения, нажав комбинации клавиш «Ctrl+O», а затем «Ctrl+X».

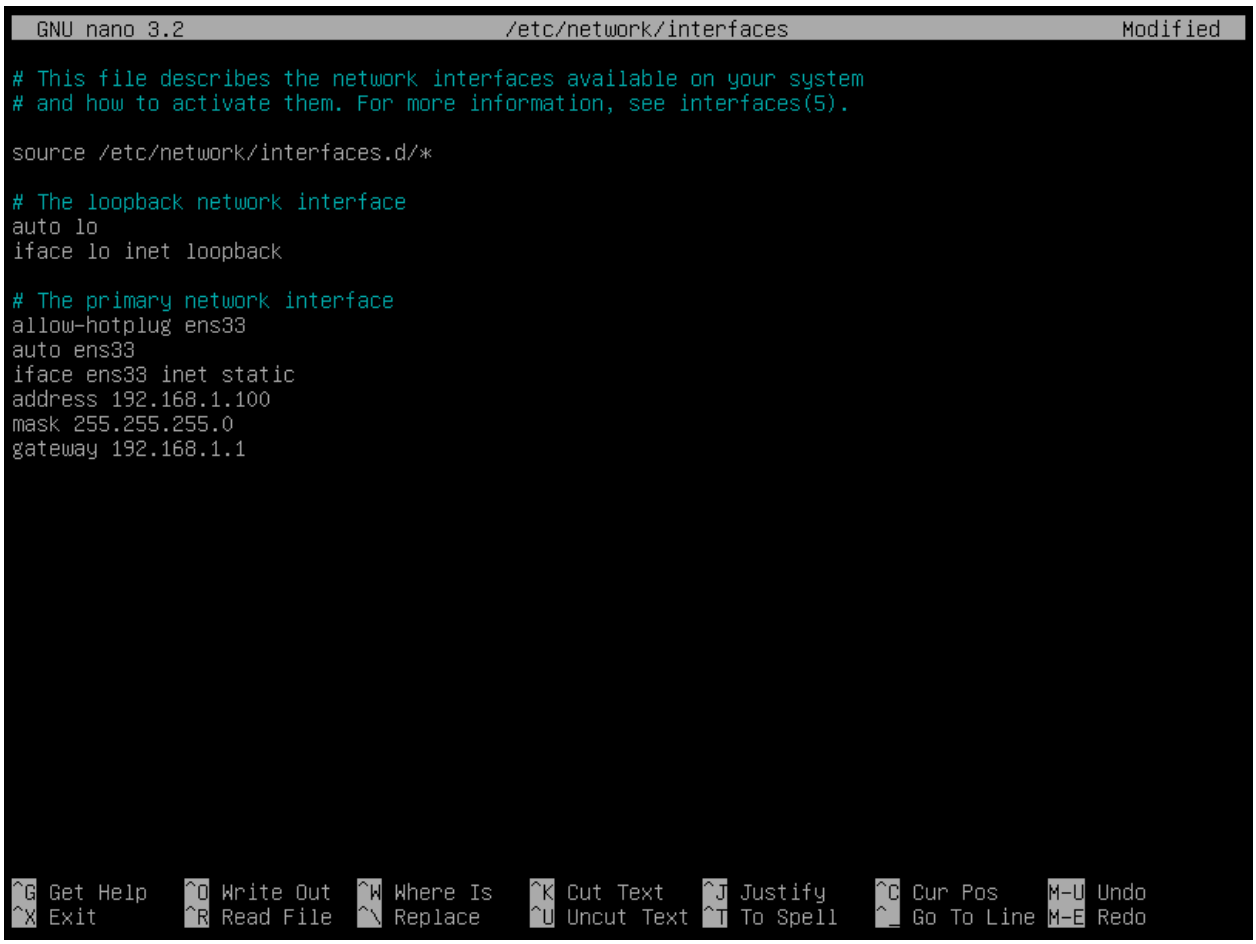
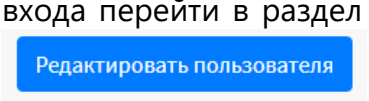


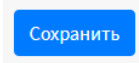
Рисунок 12 – Настройка сетевого интерфейса

4. Выполнить команду *service networking restart*.
5. Затем с помощью команды *ip a* убедиться в том, что настройки применились.

2.3 Изменение пароля по умолчанию

Для изменения пароля по умолчанию пользователя консольного интерфейса необходимо зайти в консольный интерфейс ARMA Management Console, используя пользователя по умолчанию (логин – root, пароль – root). После успешного входа необходимо выполнить команду *passwd*, указать новый пароль, нажать «Enter», повторить пароль, нажать «Enter».

Для изменения пароля по умолчанию пользователя веб-интерфейса необходимо зайти в веб-интерфейс ARMA Management Console, используя пользователя по умолчанию (логин – admin, пароль – nimda). После успешного входа перейти в раздел «Профиль пользователя», нажав на кнопку , нажать на 

и в полях «Пароль» и «Подтверждение пароля» задать новый пароль и нажать на 

.

2.4 Подключение к ARMA Management Console

Для доступа к веб-интерфейсу управления ARMA Management Console

необходимо:

– открыть веб-браузер (для ОС Windows: Chrome, Firefox; для ОС Linux: Chrome для Linux, Firefox для Linux);

– ввести IP-адрес, установленный при первоначальной настройке ARMA Management Console (по умолчанию используется получение по DHCP).

До того, как появится окно входа в систему (Рисунок 18), система произведет загрузку необходимых сервисов (Рисунок 13).

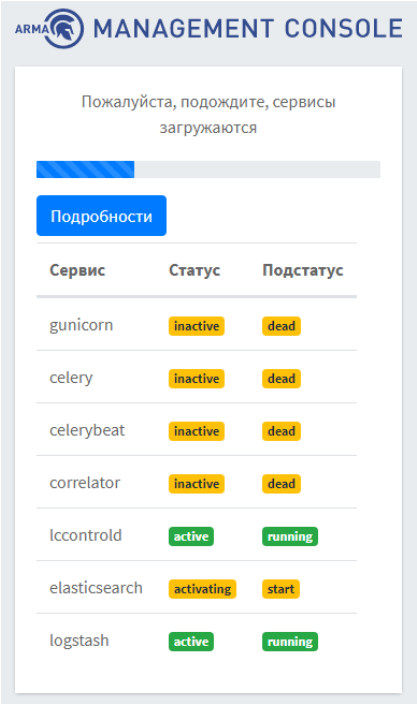


Рисунок 13 – Загрузка сервисов

После загрузки сервисов пользователю будет предложено активировать лицензию одним из предложенных способов (Рисунок 14):

1) активация лицензии с доступом в Интернет;

2) активация лицензии без доступа в Интернет.

Примечание – лицензионный ключ предоставляется согласно условиям в договоре поставки.

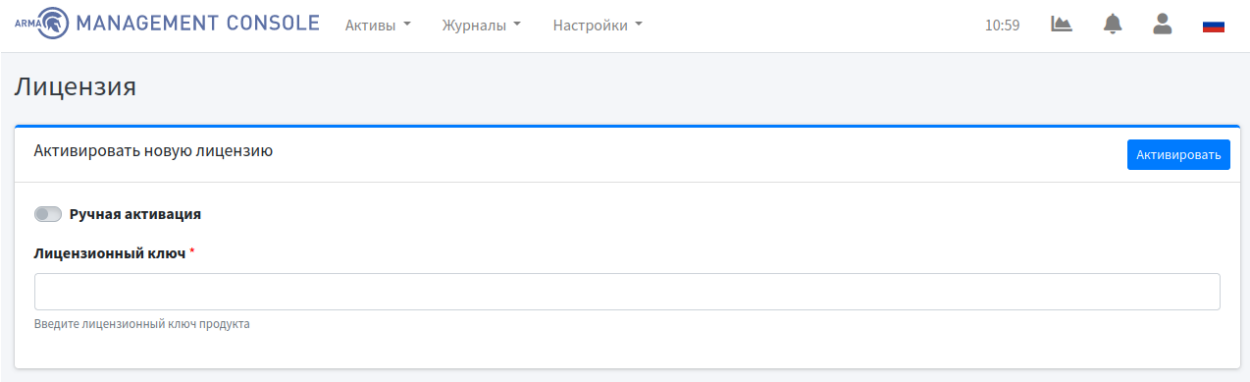


Рисунок 14 – Активация лицензии

2.4.1 Активация лицензии с доступом в Интернет

Для активации лицензии с доступом в Интернет необходимо в поле «Лицензионный ключ» вставить ключ и нажать на кнопку Активировать (Рисунок 15).

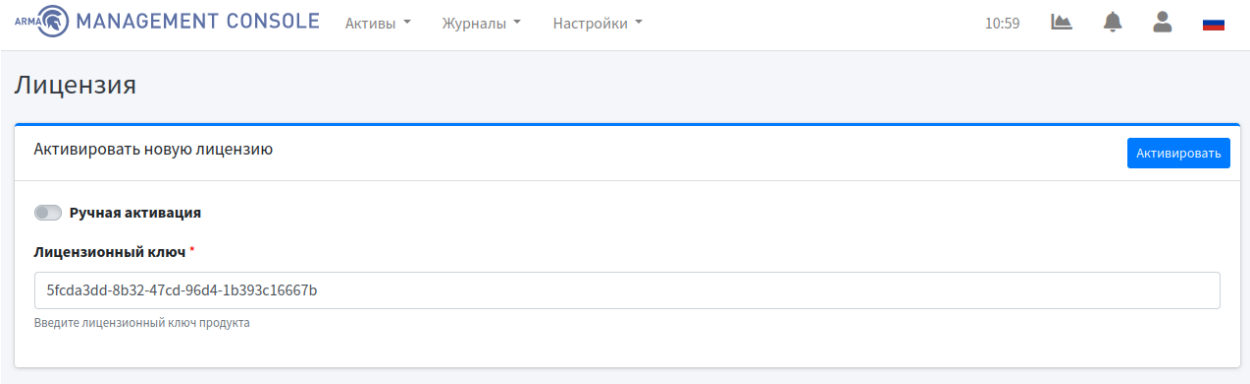


Рисунок 15 – Активация лицензии с доступом в Интернет

2.4.2 Активация лицензии без доступа в Интернет

Для активации лицензии без доступа в Интернет необходимо установить ползунок в сторону «Ручная активация», в поле «Лицензионный ключ» вставить ключ и нажать на кнопку Получить токен (Рисунок 16).

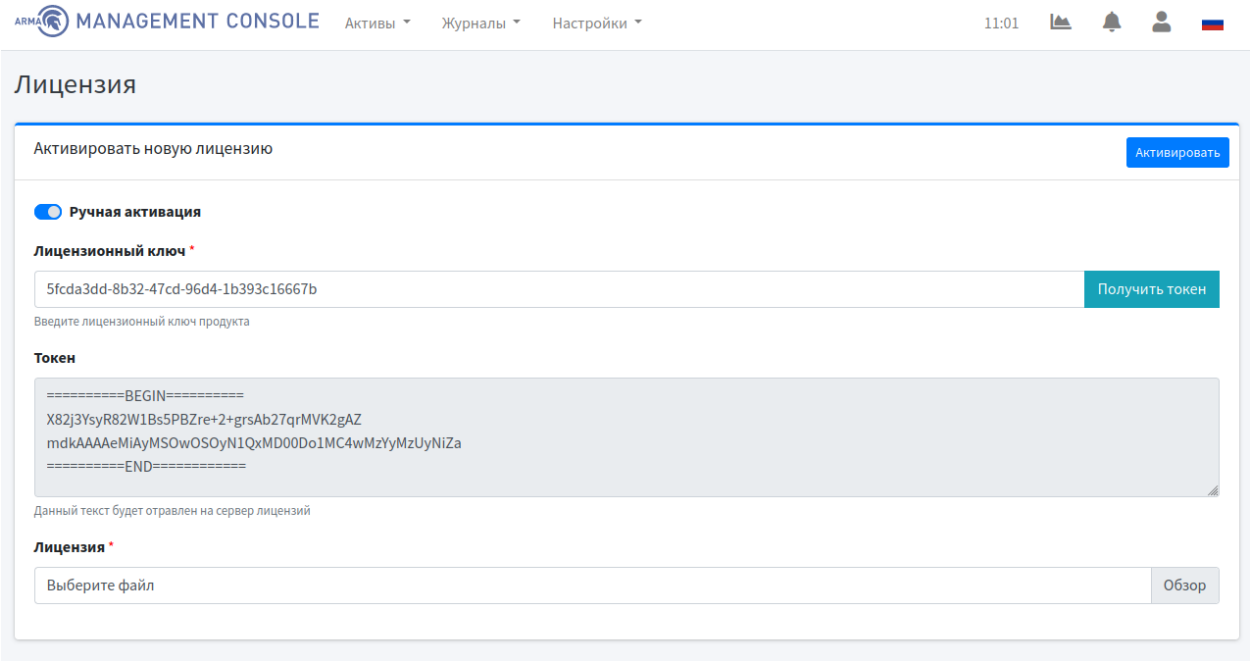


Рисунок 16 – Активация лицензии без доступа в Интернет (1)

Сгенерированный токен необходимо скопировать и направить в техподдержку ООО «Инфовотч АРМА», после чего в ответ будет получен файл лицензии с названием «license.bin», который необходимо загрузить, нажав на кнопку Обзор в поле «Лицензия», а затем на кнопку Активировать (Рисунок 17).

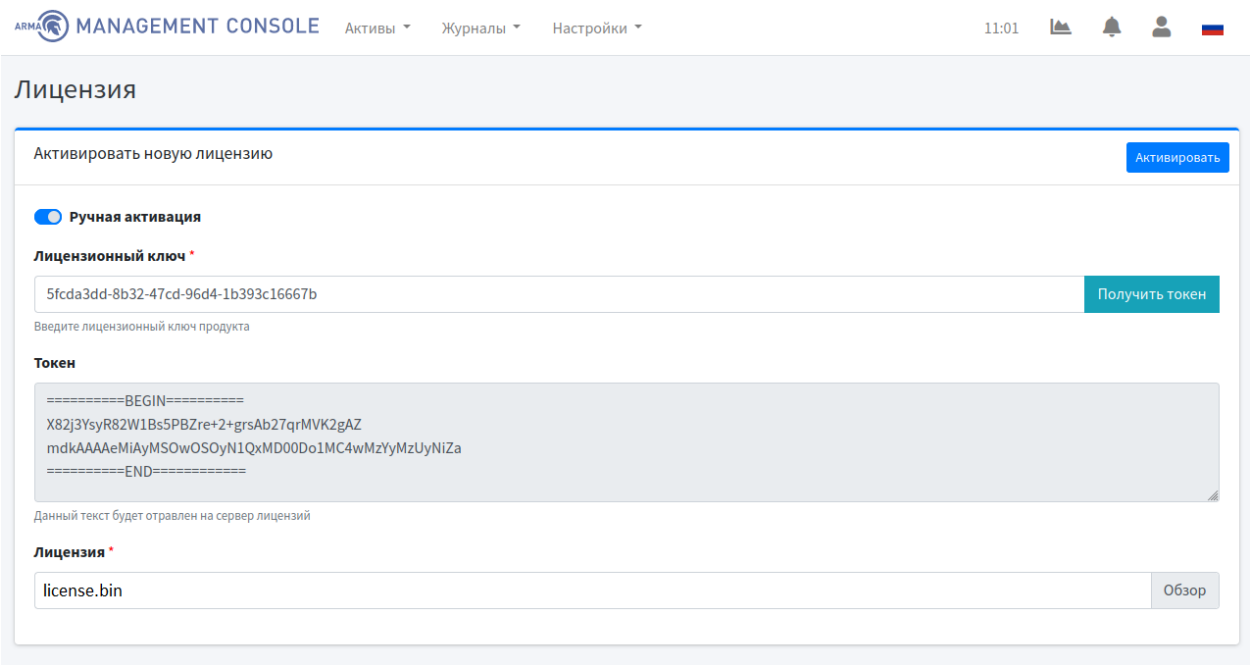


Рисунок 17 – Активация лицензии без доступа в Интернет (2)

После активации лицензии для начала работы с системой необходимо ввести аутентификационные данные (по умолчанию логин – admin, пароль – nimda) и нажать на кнопку Войти (Рисунок 18).

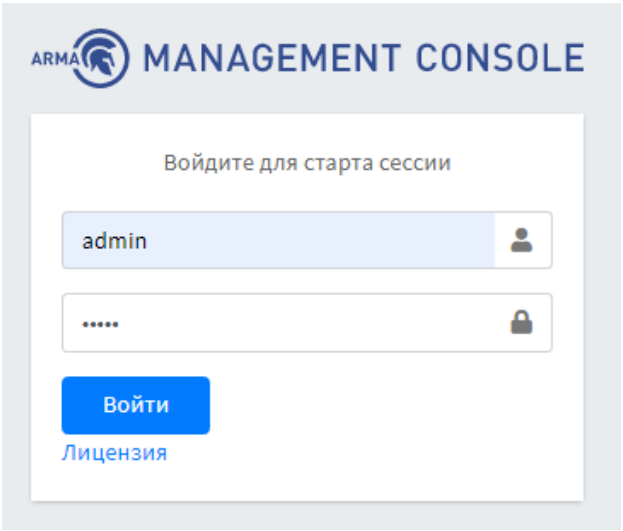


Рисунок 18 – Вход в систему

После входа в систему открывается стартовая панель («Обзорная панель») (Рисунок 19).

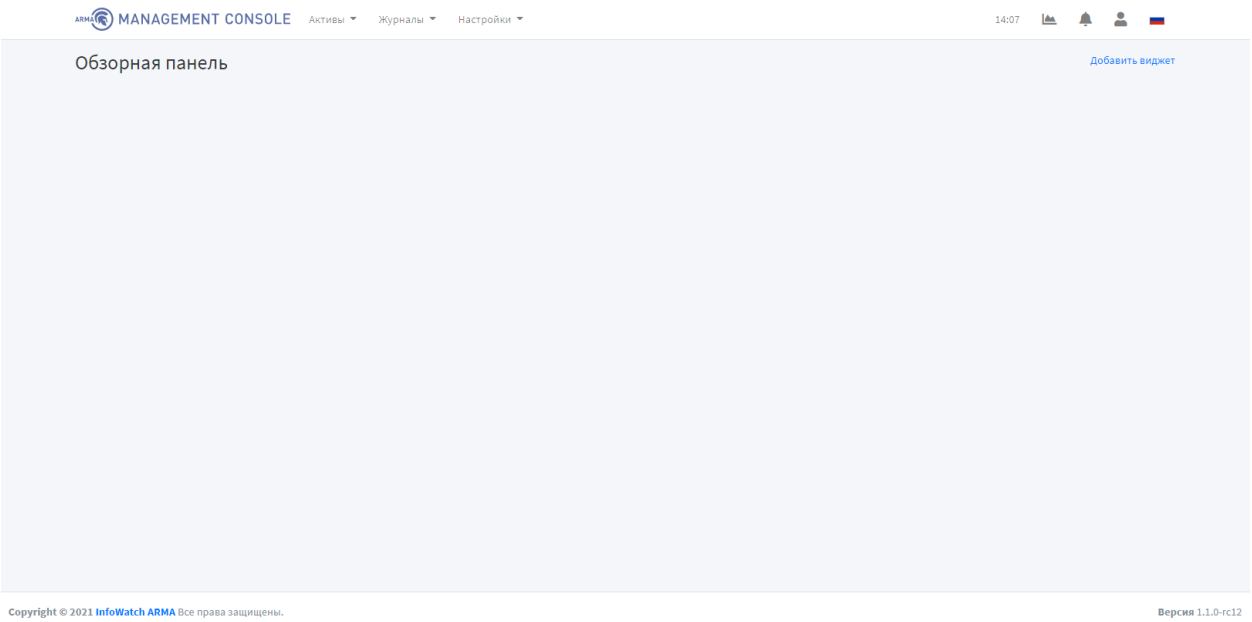


Рисунок 19 – Обзорная панель

Информация о порядке работы в ARMA Management Console изложена в следующих разделах:

- Просмотр журналов событий (раздел 3);
- Расследование инцидентов (раздел 4);
- Настройки (раздел 5);
- Управление системами защиты (раздел 6);
- Управление Endpoint (раздел 7);
- Управление источниками события (раздел 8);
- Управление списком устройств сети (раздел 9);
- Настройка карты сети и сетевых взаимодействий (раздел 10);
- Управление учетными записями и правами доступа системы (раздел 11);
- Управление стартовой панелью (раздел 12);
- Сообщения пользователю (раздел 13).

3 ПРОСМОТР ЖУРНАЛОВ СОБЫТИЙ

Текущий раздел доступен пользователям с правом доступа «Может просматривать список событий». Описание добавления пользователя и назначение прав доступа приведены в разделе 10 настоящего руководства.

Для просмотра журнала событий необходимо перейти на страницу «Журналы» - «События» (Рисунок 20).

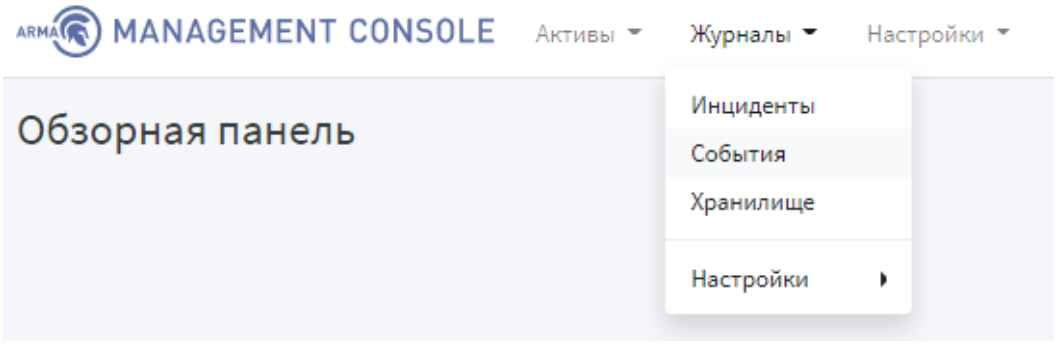


Рисунок 20 – Переход на страницу событий

3.1 Описание журнала событий

В журнале событий отображаются события систем защиты, подключенных к ARMA Management Console.

Страница «Журнал событий» позволяет просматривать журнал событий в формате таблицы, которая содержит следующие данные (Рисунок 21):

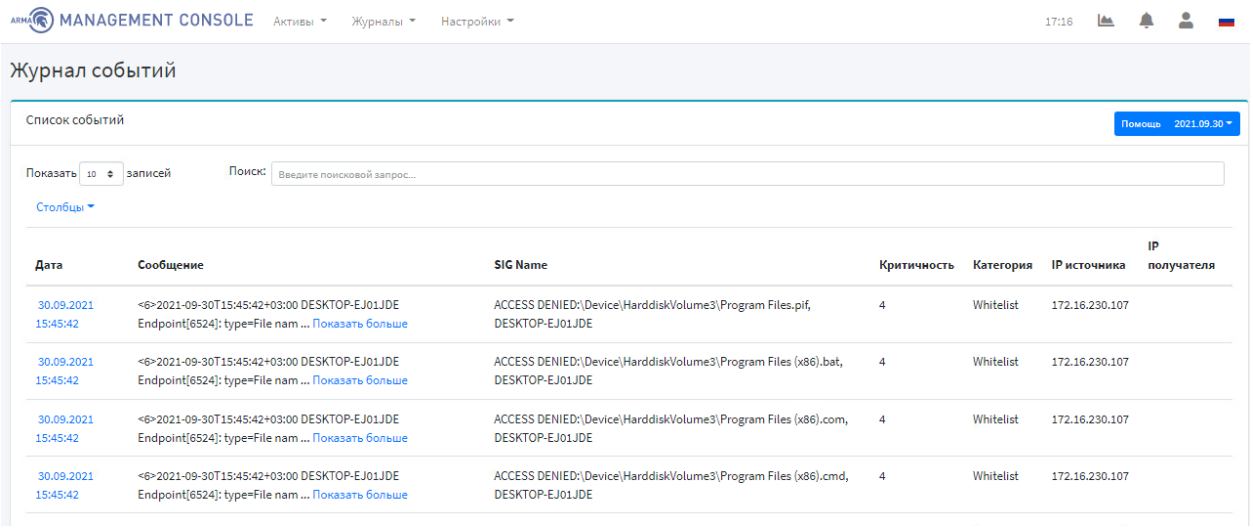


Рисунок 21 – Журнал событий

Данные о событиях можно настраивать вручную. Для этого необходимо нажать на «Столбцы» и в выпадающем списке выбрать/убрать данные, которые будут отображаться в таблице (Рисунок 22).

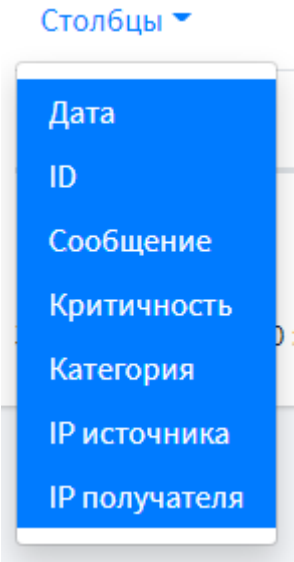
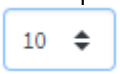


Рисунок 22 – Выбор данных о событиях

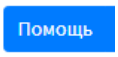
Для выбора конкретной даты отображения данных таблицы событий необходимо нажать на кнопку 

в правом верхнем углу страницы.

Для выбора количества записей, отображаемых в таблице событий на странице «Журнал событий» необходимо нажать на кнопку 

в левом в верхнем углу страницы.

3.2 Поиск событий

Поле «Поиск» вверху таблицы событий позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести одно из доступных полей, которые можно посмотреть, нажав на кнопку 

(Рисунок 23), и строку совпадения в поле «Поиск».

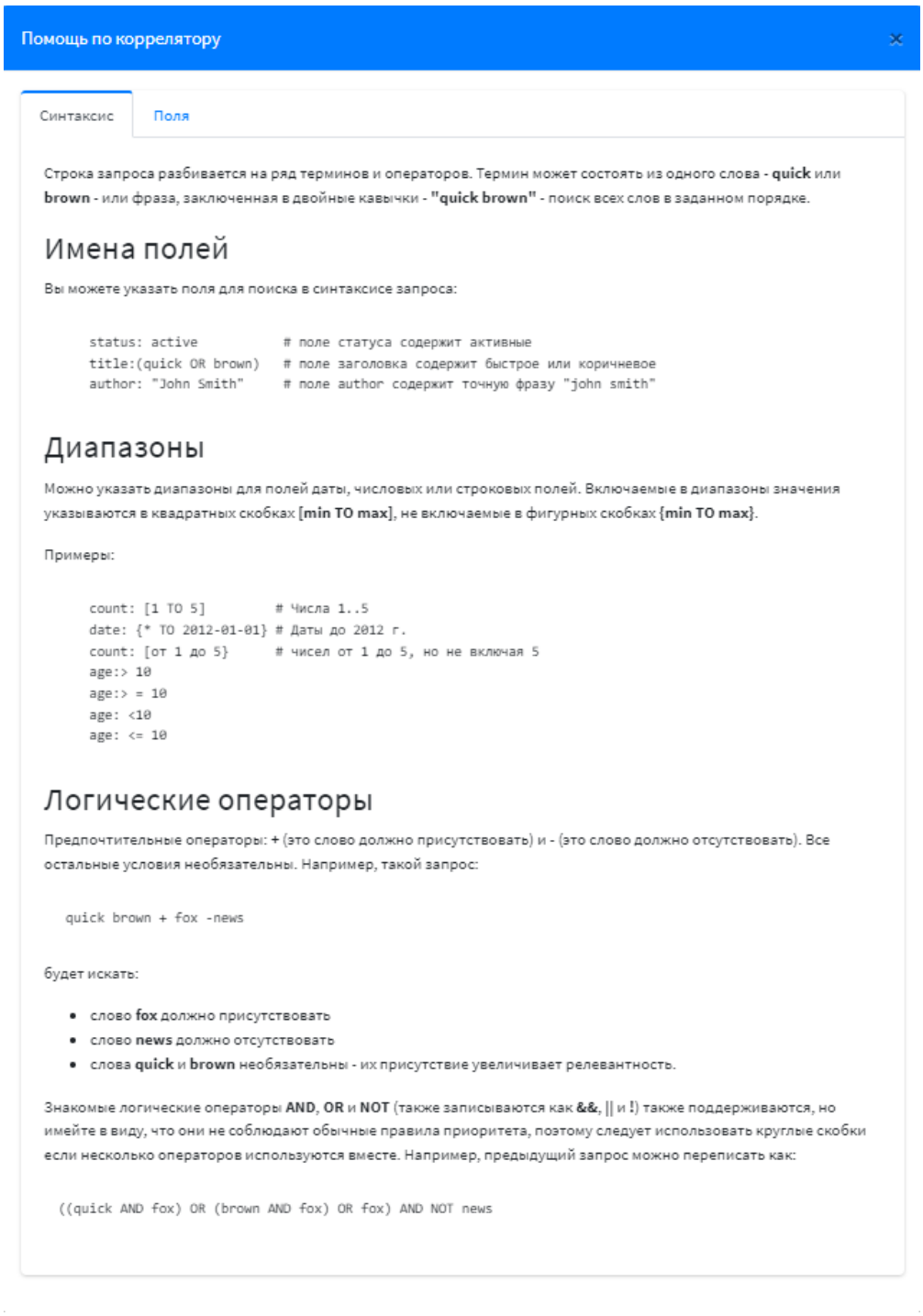


Рисунок 23 – Синтаксис коррелятора

Во вкладке «Поля» представлены возможные поля для поиска запроса в синтаксисе (Таблица 3).

Таблица 3 – Поля для поиска запроса в синтаксисе

Имя	**Описание**
event_first	Дата и время первого события в правиле
event_last	Дата и время последнего события в правиле
event_count	Количество событий в правиле
event_timestamp	Дата и время, когда правило вызвало срабатывание действия

Имя	Описание
event_severity	Критичность события в промежутке от 0 до 100
event_src_msg	Исходное сообщение события
event_protocol	Протокол события
device_vendor	Производитель устройства
device_product	Модуль устройства
device_version	Версия устройства
device_action	Действие устройства
sign_id	ID сигнатуры
sign_category	Категория сигнатуры
sign_subcategory	Подкатегория сигнатуры
sign_name	Имя сигнатуры
source_ip	IP источника
source_mac	Source MAC
source_host	Исходный хост
source_port	Порт источника
source_user	Исходный пользователь
destination_ip	IP получателя
destination_host	Целевой хост
destination_port	Порт получателя
destination_user	Целевой пользователь

3.3 Просмотр подробной информации о событии

Для просмотра подробной информации о событии необходимо перейти на страницу «Журнал» - «События». В таблице событий необходимо нажать на ссылку идентификационного номера этого события (столбец «ID»), например, 6e6a9821-7cf3-43c4-9c4b-f7df567ab734 . При нажатии на идентификационный номер события ARMA Management Console отобразит страницу подробной информации о событии со следующими разделами (Рисунок 24, Рисунок 25, Рисунок 26):

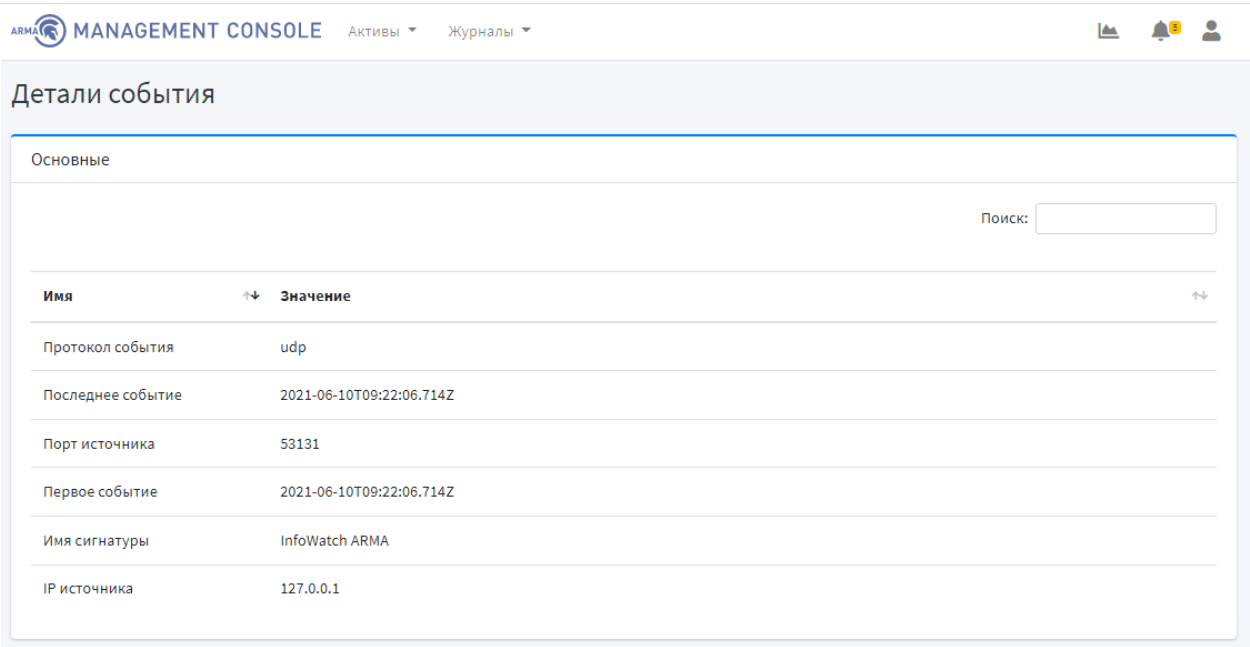


Рисунок 24 – Детали события. Основные

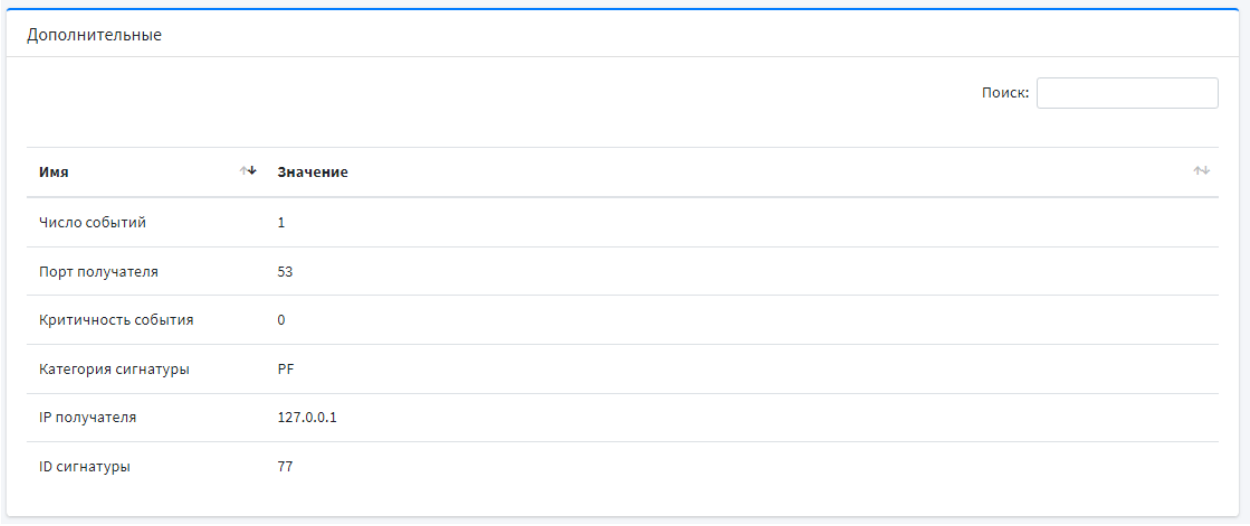


Рисунок 25 – Детали события. Дополнительные

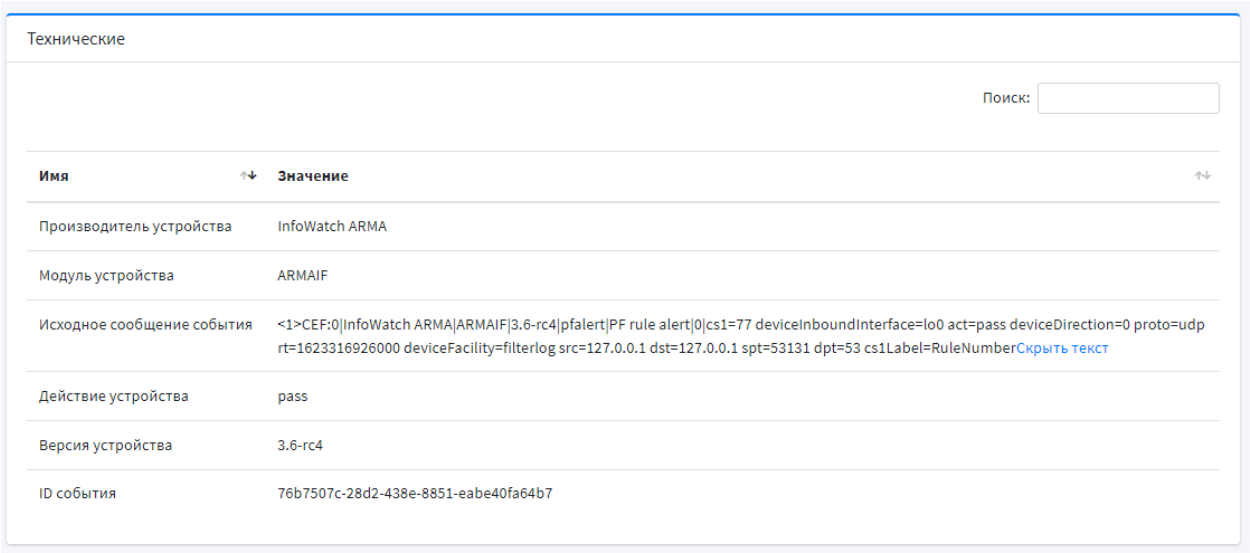


Рисунок 26 – Детали события. Технические

Поле «Поиск» вверху страницы позволяет осуществлять сквозной поиск по всей информации о событии. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица данных события позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

4 РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Текущий раздел доступен пользователям с правом доступа «Может просматривать инциденты». Описание добавления пользователя и назначение прав доступа приведены в разделе 10 настоящего руководства.

Пользователю с правом доступа «Может просматривать сетевые атаки» также отображаются инциденты, связанные с сетевыми атаками.

Для просмотра журнала инцидентов необходимо перейти на страницу «Журналы» - «Инциденты» (Рисунок 27).

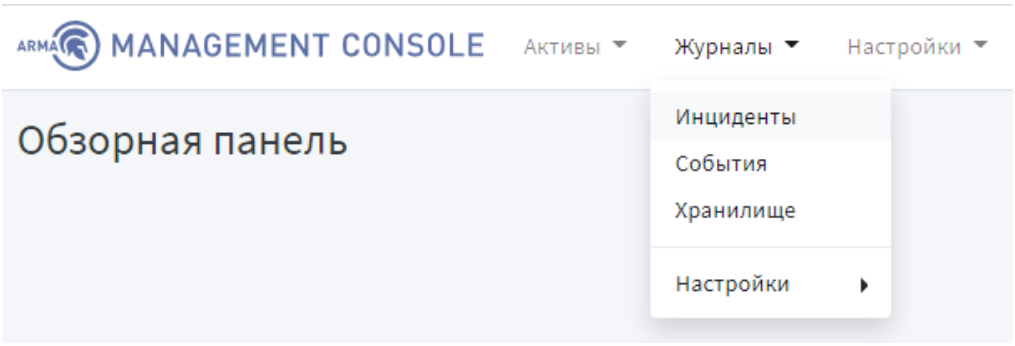


Рисунок 27 – Переход на страницу инцидентов

4.1 Уведомление о нерешенных инцидентах

Кнопка  в верхнем меню позволяет просматривать все уведомления ARMA Management Console.

При наличии/появлении нерешенных инцидентов появится уведомление об этом. Для просмотра нерешенных инцидентов, необходимо нажать на  , а затем выбрать уведомление об инцидентах (Рисунок 28). При нажатии на уведомление о нерешенных инцидентах ARMA Management Console отобразит страницу «Журналы» - «Инциденты» (Рисунок 29).

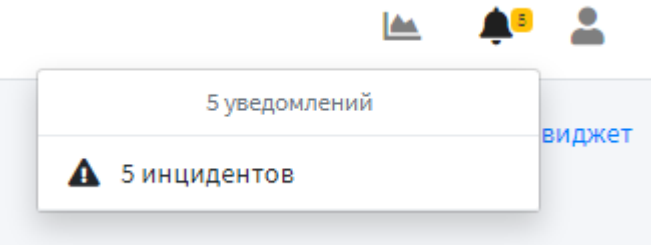


Рисунок 28 – Уведомление об инцидентах

4.2 Описание журнала инцидентов

В журнале инцидентов отображаются инциденты систем защиты, подключенных к ARMA Management Console.

Страница «Инциденты» позволяет просматривать журнал инцидентов в формате таблицы, которая содержит следующие данные (Рисунок 29).

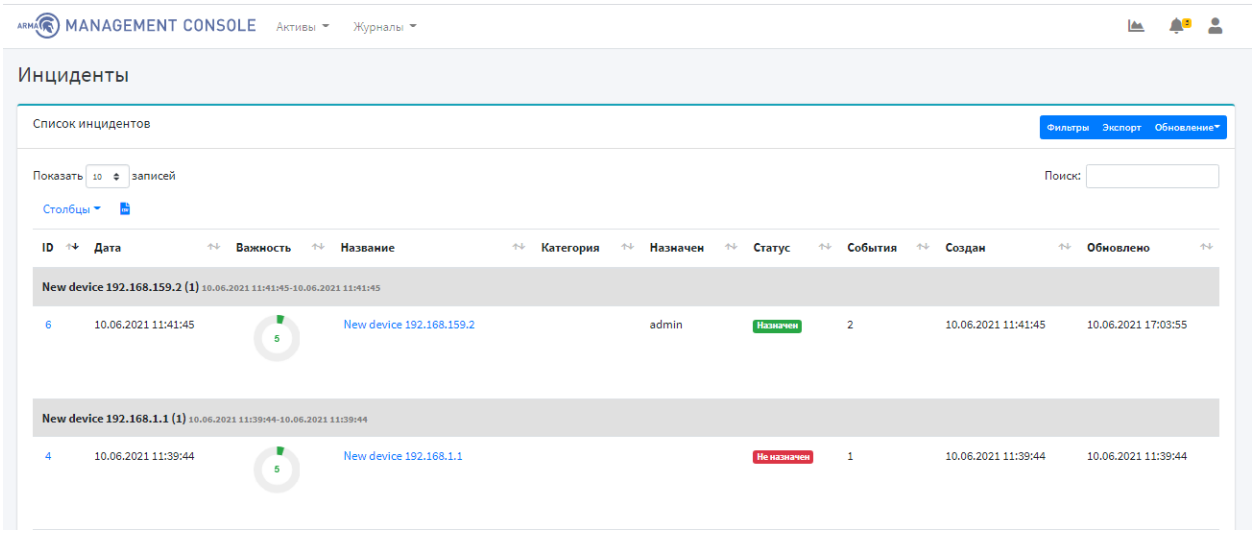


Рисунок 29 – Журнал инцидентов

Console поддерживает автоматическую группировку инцидентов.

Для выбора промежутка обновления данных таблицы инцидентов необходимо нажать на кнопку Обновление в правом верхнем углу страницы и выбрать частоту обновления данных. При выборе частоты обновления данных к

н

Для выбора количества записей, отображаемых в таблице инцидентов на о

странице «Инциденты» необходимо нажать на кнопку 10 в левом в верхнем углу страницы.

п

4.3 Поиск, сортировка и фильтрация инцидентов

к

Поле «Поиск» вверху таблицы событий позволяет осуществлять сквозной а

поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Для фильтрации по определенным столбцам таблицы событий необходимо с

нажать на кнопку Фильтры. Всплывающее окно позволяет задать фильтры м

отображения таблицы инцидентов (Рисунок 30).

е

н

и

т

в

и

д

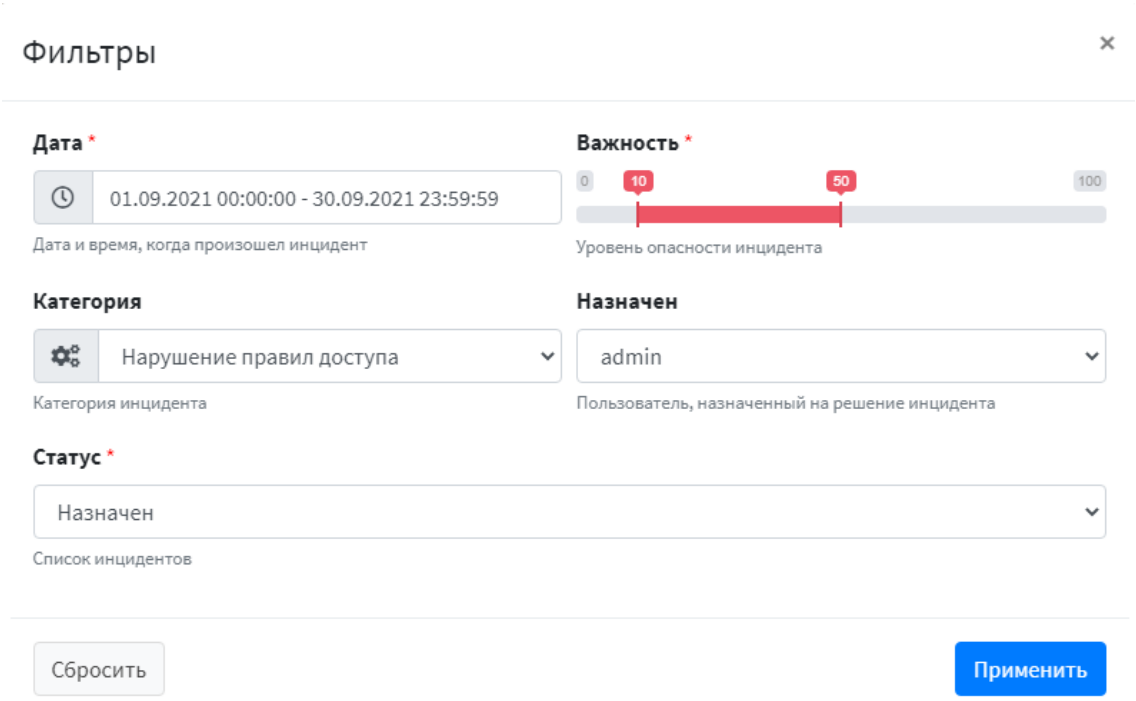


Рисунок 30 – Фильтры журнала инцидентов

В поле «Дата» необходимо выбрать промежуток времени отображения инцидентов. В поле «Важность» необходимо задать значение важности инцидентов. В поле «Категория» необходимо выбрать категорию инцидента или создать новую, нажав на кнопку , а затем на кнопку + (Рисунок 31, Рисунок 32).

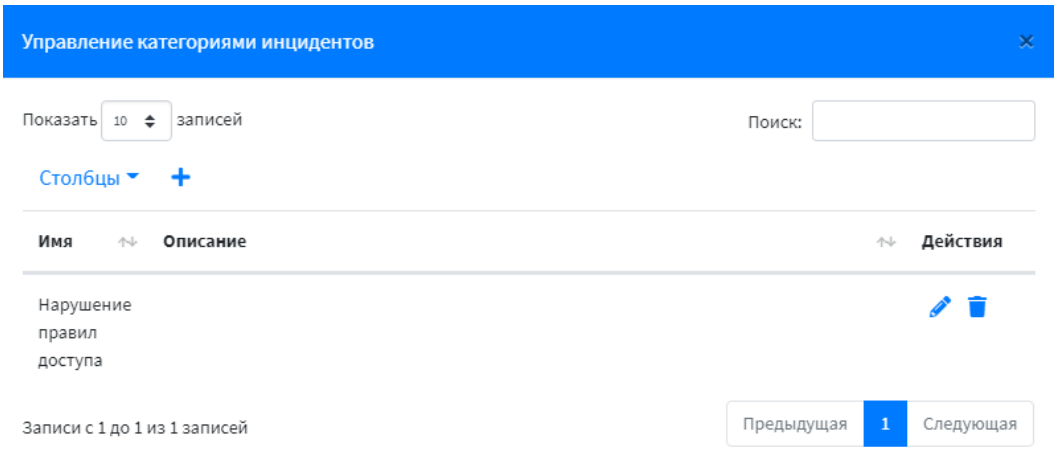


Рисунок 31 – Управление категориями инцидентов

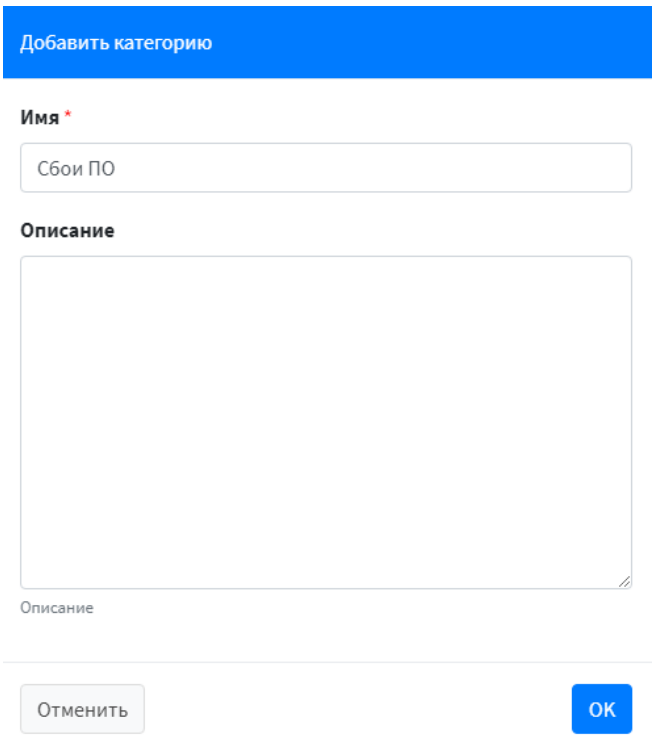


Рисунок 32 – Добавление категории

В поле «Назначен» необходимо выбрать пользователя, который назначается для решения инцидента. В поле «Статус» необходимо выбрать статус, отображаемых инцидентов. Для сброса фильтров необходимо нажать на кнопку Сбросить. Для сохранения и применения фильтров необходимо нажать на кнопку Применить.

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

4.4 Просмотр подробной информации об инциденте

Для просмотра подробной информации об инциденте необходимо перейти на страницу «Журналы» - «Инциденты». В таблице инцидентов необходимо нажать на ссылку идентификационного номера этого инцидента (столбец «ID»), например, 15332. При нажатии на идентификационный номер инцидента ARMA Management Console отобразит страницу подробной информации об инциденте (Рисунок 33, Рисунок 34). Поля «Название», «Число событий», «Важность», «Описание» не редактируемые.

Для пользователя с правом доступа «Может назначать инциденты» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для пользователя с правом доступа «Может работать с инцидентами» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен», «Категория», «Комментарий».

Для пользователя с правом доступа «Может изменять решенные инциденты» доступны для редактирования поля «Статус», «Крайний срок», «Назначен», «Категория», «Комментарий».

В поле «Статус» необходимо выбрать статус инцидента из следующих возможных:

- не назначен;
- назначен;
- отложен;
- решен;
- ложное срабатывание.

В поле «Категория» необходимо выбрать категорию инцидента. В поле «Крайний срок» необходимо выбрать крайний срок решения инцидента. В поле «Назначен» необходимо выбрать пользователя, назначенного для решения инцидента. В поле «Комментарий» необходимо ввести комментарий к инциденту. Далее отображается список событий, из которых сформирован инцидент, представленный в виде таблице со следующей информацией:

- дата события;
- сообщение;
- имя узла;
- продукт;
- IP источника;
- IP получателя.

Затем отображаются рекомендации по закрытию инцидента и последствия инцидента (Рисунок 35). Для сохранения изменений на странице «Детали инцидента» необходимо нажать на кнопку Сохранить. При решении инцидента необходимо нажать на кнопку Решить. Для просмотра подробной информации о системе защиты, с которой был обнаружен инцидент, необходимо нажать на кнопку Посмотреть систему защиты.

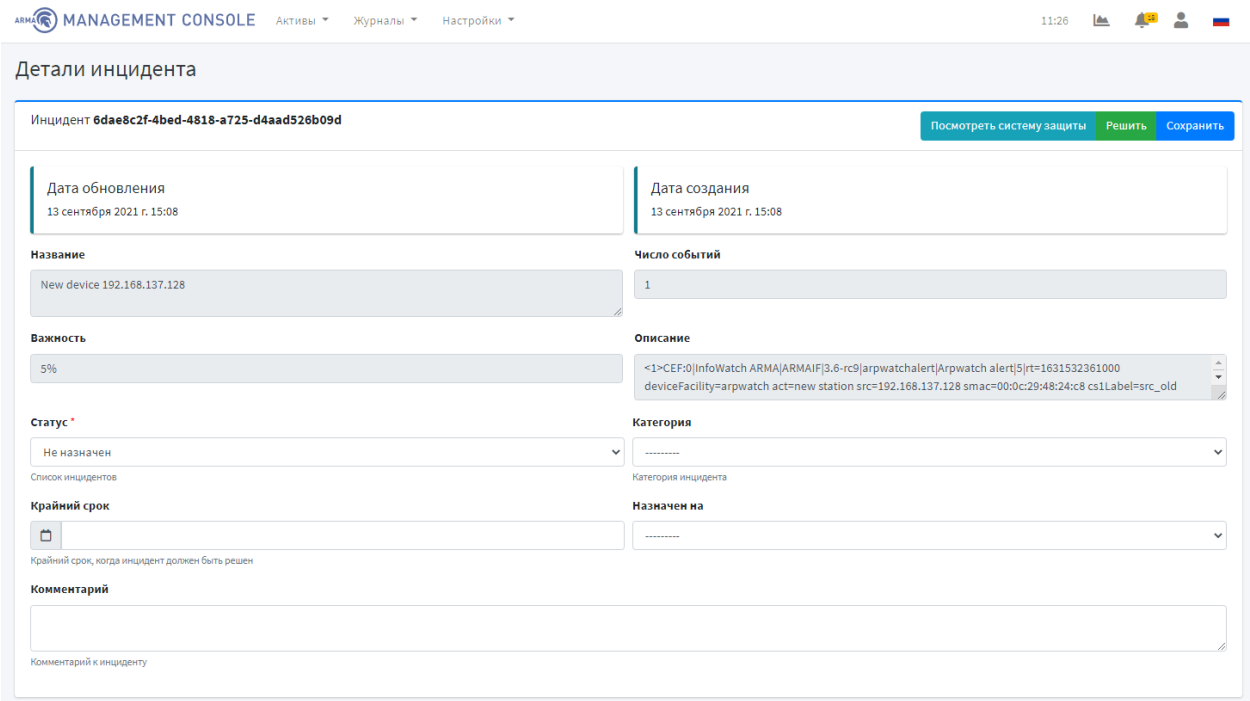


Рисунок 33 – Детали инцидента (1)

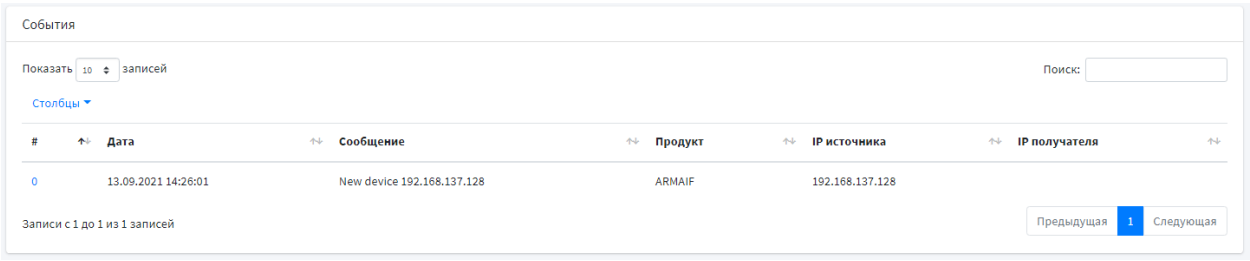


Рисунок 34 – Детали инцидента (2)

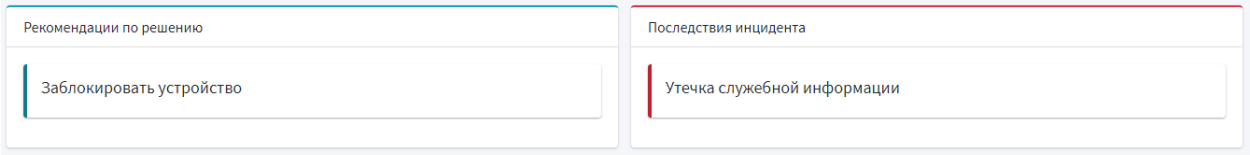
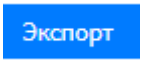


Рисунок 35 – Детали инцидента (3)

4.5 Экспорт инцидентов

4.5.1 Экспорт всей таблицы

Для того чтобы экспортировать всю таблицу инцидентов необходимо нажать на кнопку 

справа сверху таблицы.

4.5.2 Экспорт отфильтрованной таблицы в формате CSV

Для того чтобы скачать отфильтрованную таблицу инцидентов необходимо сначала задать фильтр (Рисунок 30), а затем нажать на кнопку 

слева сверху таблицы.

4.6 Управление инцидентами

Для работы с инцидентами с помощью ARMA Management Console предусмотрены следующие шаги:

– 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.

4.6.1 Назначение пользователя для решения инцидента

Для назначения пользователей для решения инцидента необходимо перейти на страницу «Журналы» - «Инциденты». В таблице инцидентов необходимо нажать на ссылку идентификационного номера этого инцидента (столбец «ID»), например, 15332 . При нажатии на идентификационный номер инцидента ARMA Management Console отобразит страницу подробной информации об инциденте (Рисунок 33).

Для пользователя с правом доступа «Может назначать инциденты» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для пользователя с правом доступа «Может работать с инцидентами» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для пользователя с правом доступа «Может изменять решенные инциденты» доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для назначения пользователя на инцидент необходимо в поле «Статус» выбрать «Назначен». В поле «Назначен» необходимо выбрать пользователя, на которого будет назначен инцидент. В поле «Крайний срок» необходимо выбрать дату, до которой необходимо решить инцидент. Для сохранения настроек необходимо нажать на кнопку Сохранить.

4.6.2 Внесение результата проведенного расследования

По результатам проведенного расследования пользователю необходимо перейти на страницу «Журналы» - «Инциденты». В таблице инцидентов необходимо нажать на ссылку идентификационного номера этого инцидента (столбец «ID»), например, 15332 . При нажатии на идентификационный номер инцидента ARMA Management Console отобразит страницу подробной информации об инциденте (Рисунок 33).

Для пользователя с правом доступа «Может работать с инцидентами» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Комментарий».

Для пользователя с правом доступа «Может изменять решенные инциденты» доступны для редактирования поля «Статус», «Комментарий».

Для внесения результата проведенного расследования пользователю необходимо изменить статус в поле «Статус». В поле «Комментарий» необходимо ввести комментарий к инциденту. Для сохранения изменений необходимо нажать на кнопку Сохранить.

В случае положительного решения инцидента, отметить инцидент как решенный. Для этого необходимо нажать на кнопку Решить.

4.7 Просмотр архивов

Страница «Хранилище» позволяет просматривать архивы собранных инцидентов (Рисунок 36).

Для просмотра хранилища необходимо перейти на страницу «Журналы» - «Хранилище».

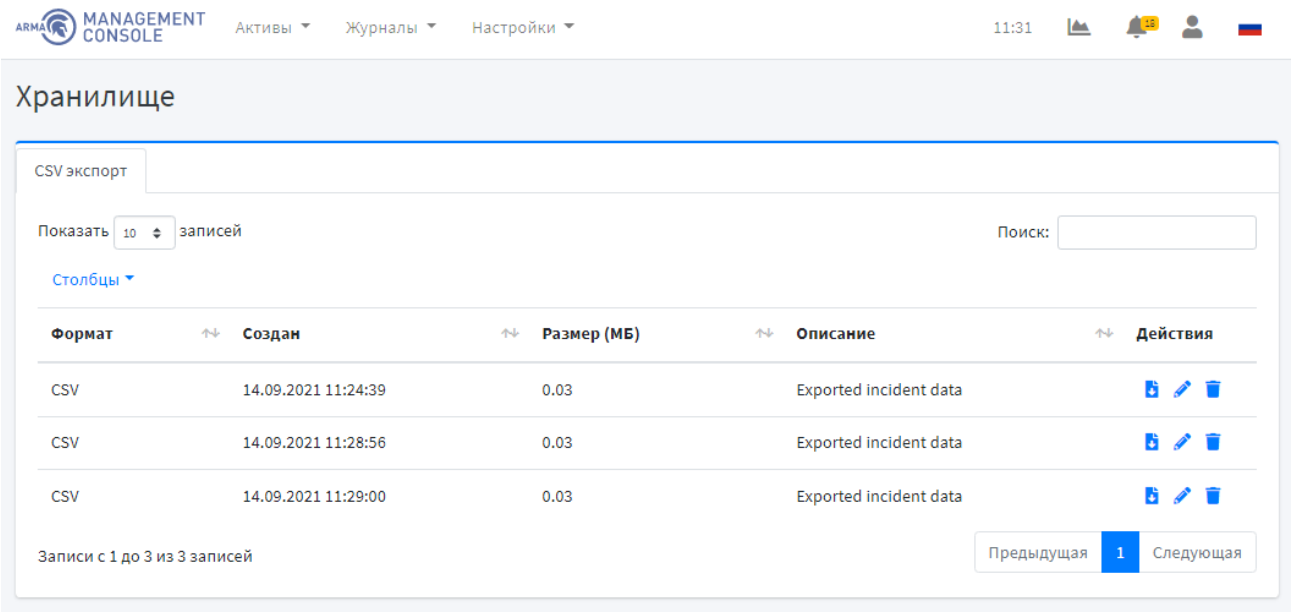


Рисунок 36 – Хранилище. CSV экспорт

Во вкладке «CSV экспорт» хранятся архивы собранных инцидентов в формате CSV. Во вкладке «Дамп БД» хранятся архивы собранных инцидентов, настроенных по ротации (Рисунок 37).

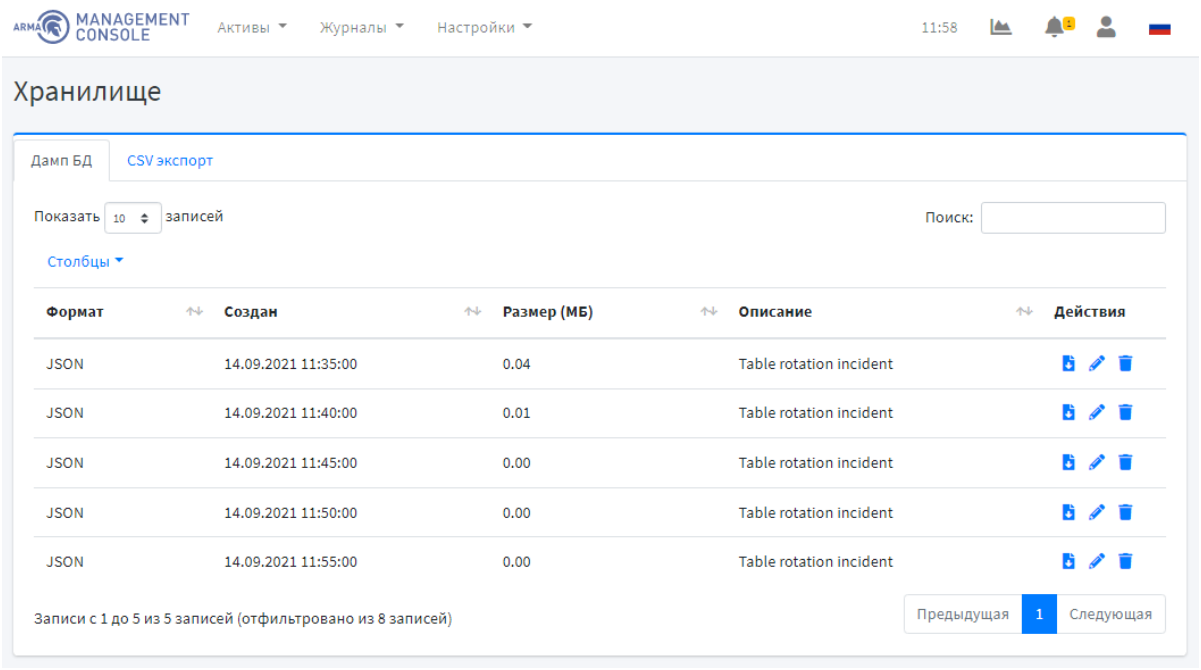


Рисунок 37 – Хранилище. Дамп БД

Для редактирования описания хранилища необходимо нажать на кнопку напротив соответствующего хранилища и в разделе «Редактировать» изменить описание, а затем нажать на кнопку Сохранить (Рисунок 38). Для скачивания архива необходимо нажать на кнопку (Рисунок 36) либо на кнопку Скачать (Рисунок 38).

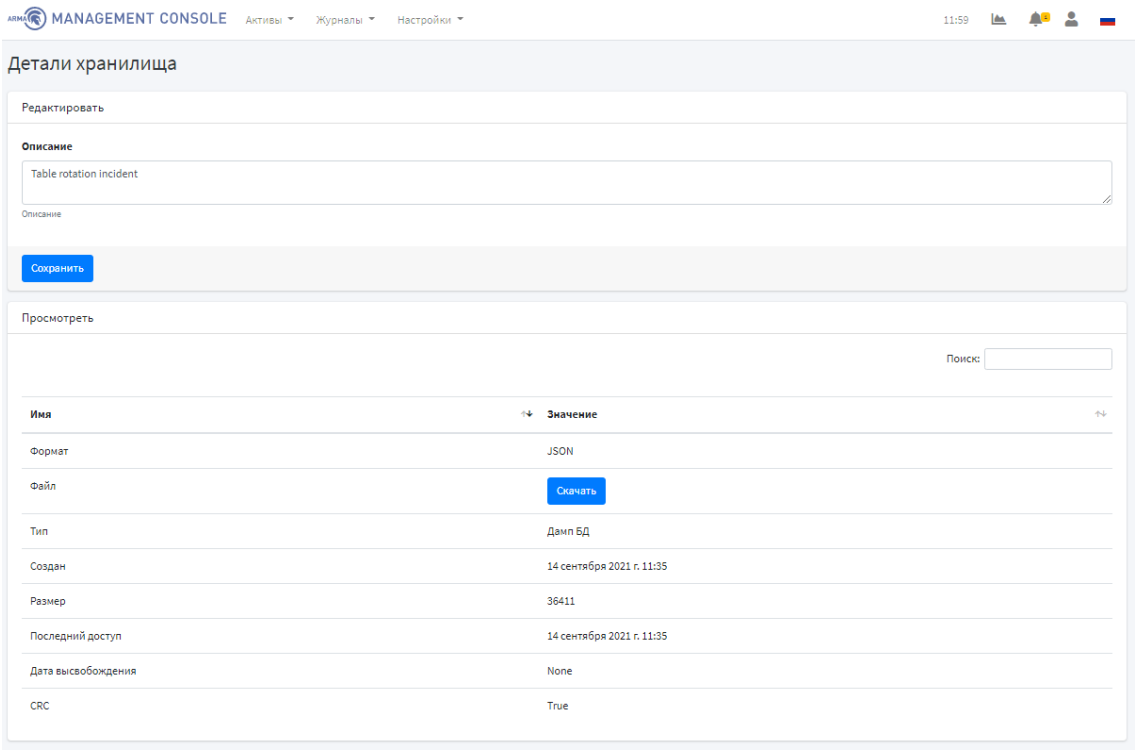


Рисунок 38 – Детали хранилища

5 НАСТРОЙКИ

5.1 Настройка правил корреляции

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

Текущий раздел позволяет создавать и настраивать правила корреляции. По умолчанию создано два правила корреляции (Рисунок 39).

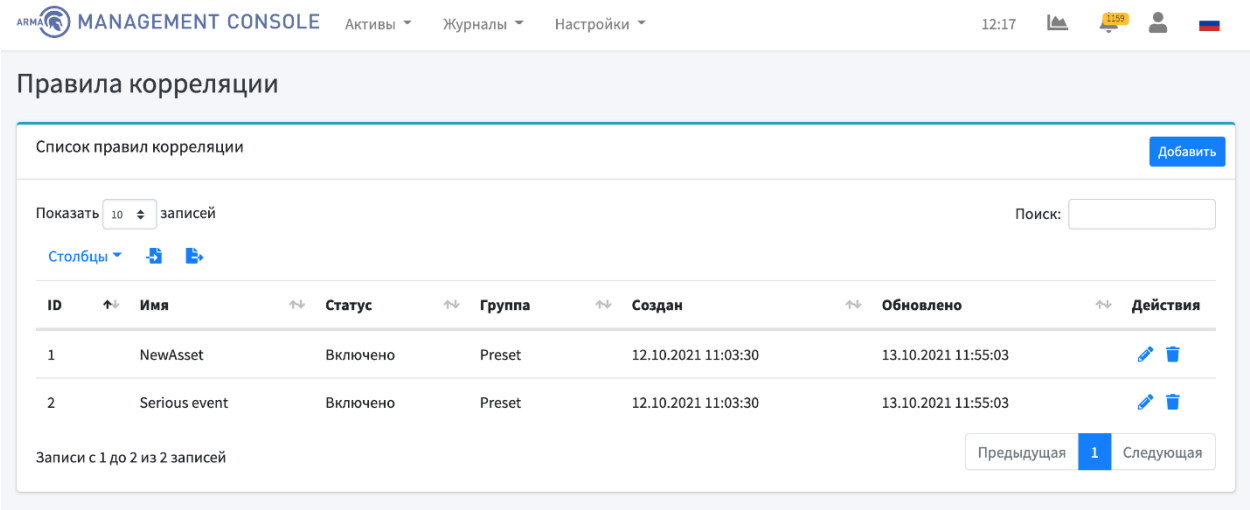


Рисунок 39 – Правила корреляции

Также есть возможность импорта и экспорта правил корреляции. Для импорта правил корреляции необходимо нажать на кнопку , выбрать файл в формате JSON и нажать на кнопку Импорт (Рисунок 40).

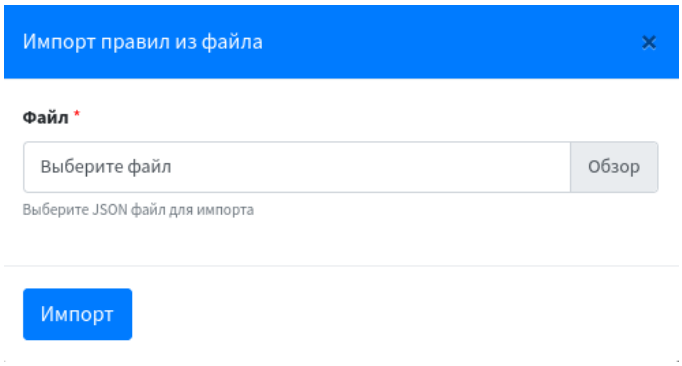


Рисунок 40 – Импорт правил корреляции

В случае успешного или неуспешного импорта правил корреляции появится окно отчета по импорту (Рисунок 41, Рисунок 42).

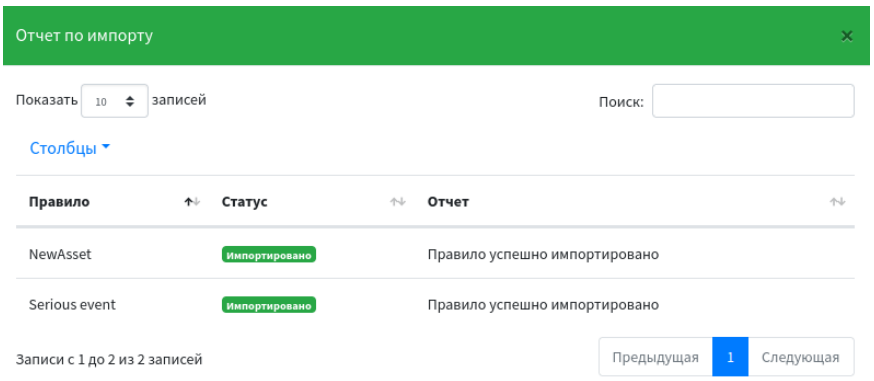


Рисунок 41 – Успешный импорт правил корреляции

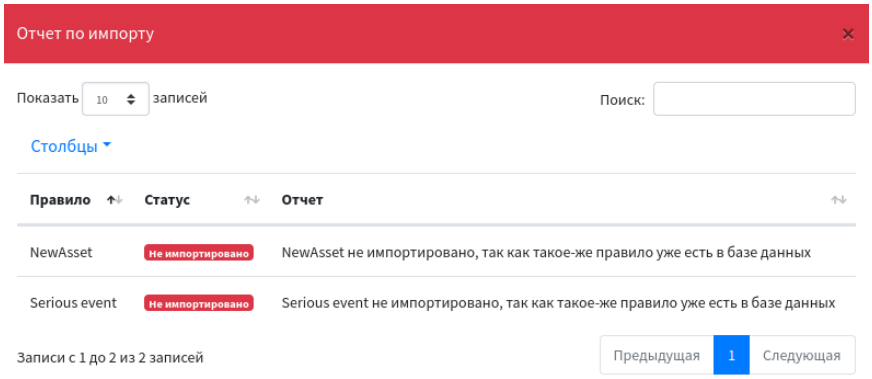


Рисунок 42 – Неуспешный импорт правил корреляции

Для экспорта правил корреляции необходимо нажать на кнопку .

Для добавления правила корреляции необходимо нажать на кнопку Добавить. В разделе «Базовые настройки» задаются общие настройки правила – имя, группа, глубина анализа и описание правила (Рисунок 46). Группу правила можно выбирать из существующих, а также добавлять новые, нажав на кнопку и затем на кнопку + (Рисунок 43, Рисунок 44). Глубина анализа показывает, насколько далеко во времени от текущего момента коррелятор будет искать события для конкретного правила корреляции (допустим, глубина 30 секунд означает, что события пришедшие минуту назад не будут учитываться при поиске).

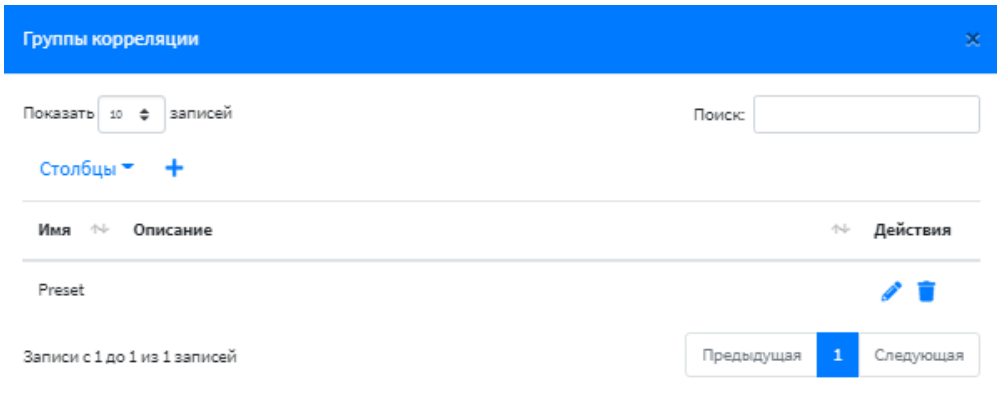


Рисунок 43 – Группы корреляции

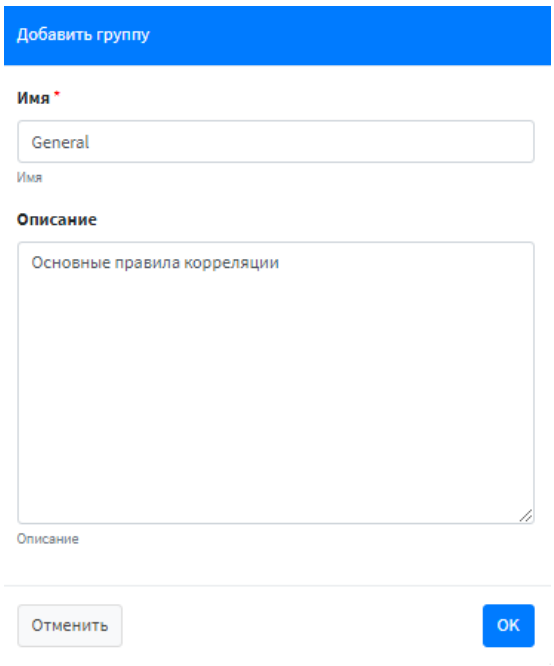


Рисунок 44 – Добавление группы корреляции

В разделе «Условия срабатывания правила» задаются условия, по которым будут формироваться инциденты на основе правила корреляции (Рисунок 46). Условия срабатывания правила задаются с помощью специального синтаксиса, пояснение к которому можно посмотреть, нажав на кнопку Помощь. Синтаксис коррелятора и поля для поиска запроса в нем рассмотрены в п. 3.2 настоящего руководства.

Примечание – условия задаются на основании деталей события, на которое создается то или иное правило корреляции.

Для проверки срабатывания условия правила корреляции необходимо нажать на кнопку Проверить. Если в списке событий есть подходящие события под заданное условие, то они отобразятся в виде таблицы (Рисунок 45).

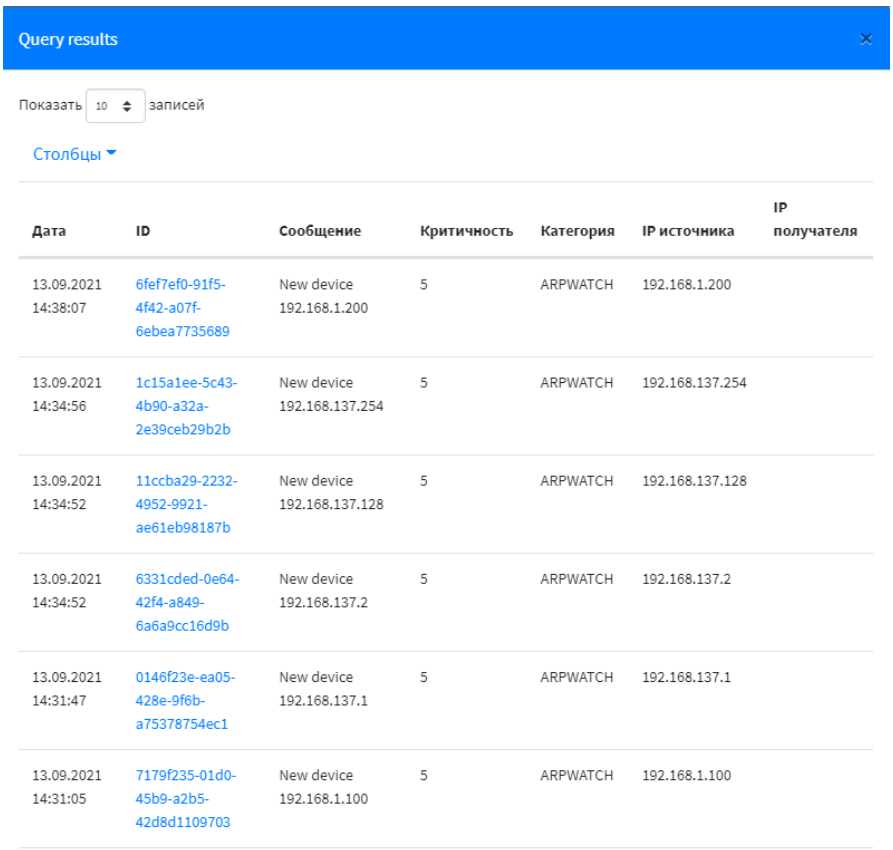
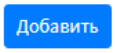


Рисунок 45 – Результаты проверки срабатывания условий правила корреляции

Примечание – отсутствие записей в таблице не означает, что условие задано некорректно.

После задания общих настроек и условий срабатывания правила корреляции необходимо добавить действие, которое будет выполняться при заданных условиях, нажав на кнопку 

, выбрать одно из предложенных действий (Рисунок 47) и нажать на кнопку 

.

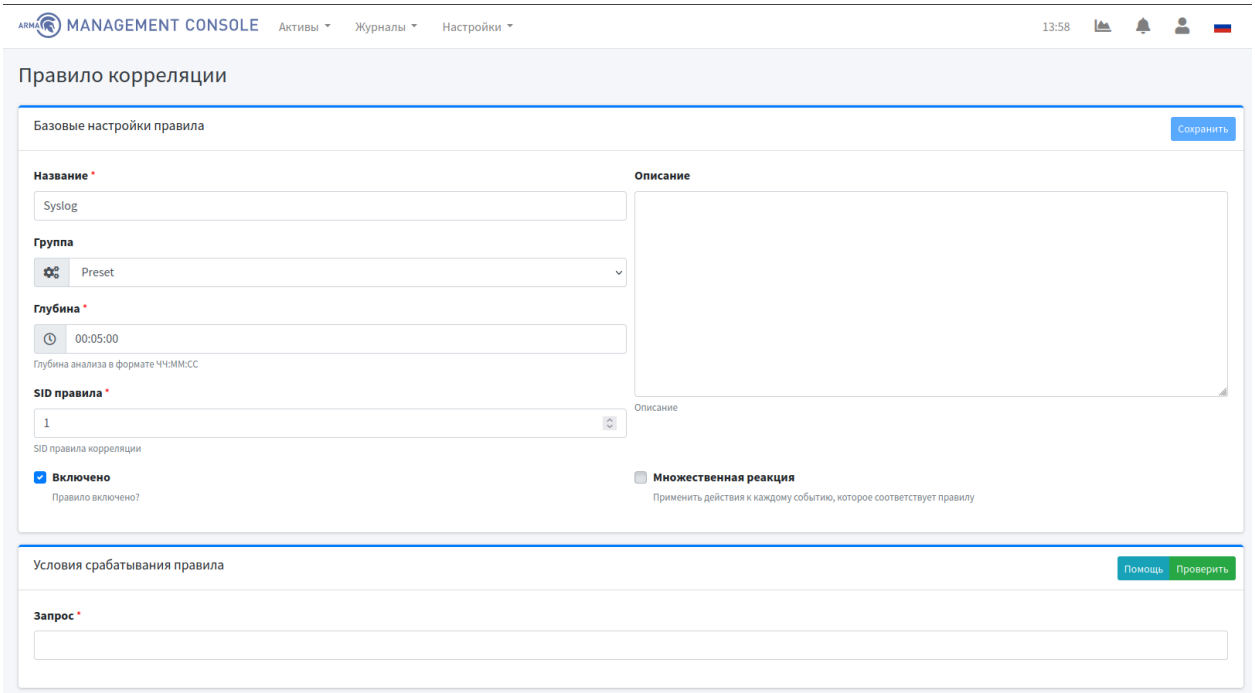


Рисунок 46 – Добавление правила корреляции

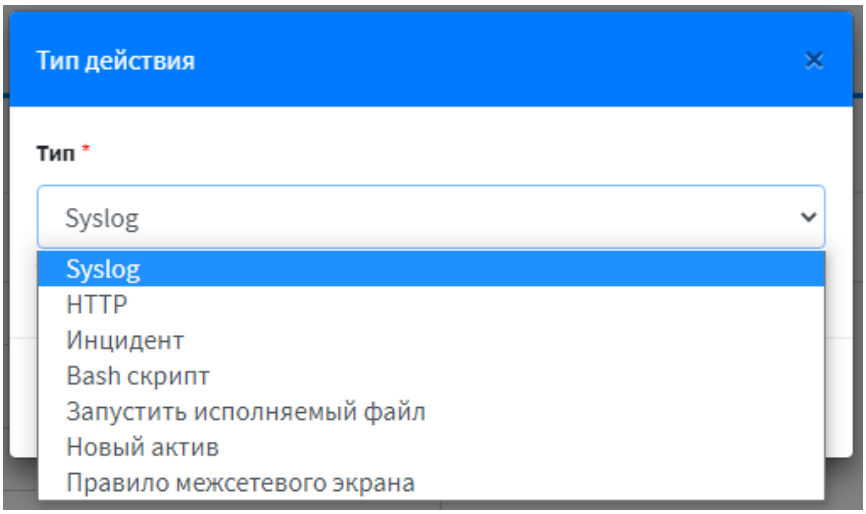


Рисунок 47 – Типы действий

Примечание – для проверки работоспособности правил корреляции необходимо подключиться к ARMA Industrial Firewall (см. п. 6.7 настоящего руководства).

5.1.1 Правило корреляции с типом действия «Syslog»

Действие «Syslog» позволяет отправлять запись по syslog при возникновении определенного события.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «Syslog» как показано на рисунках (Рисунок 48, Рисунок 49).

2. Сгенерировать событие (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.

3. Убедиться, что правило корреляции сработало и появилась запись в syslog (Рисунок 50).

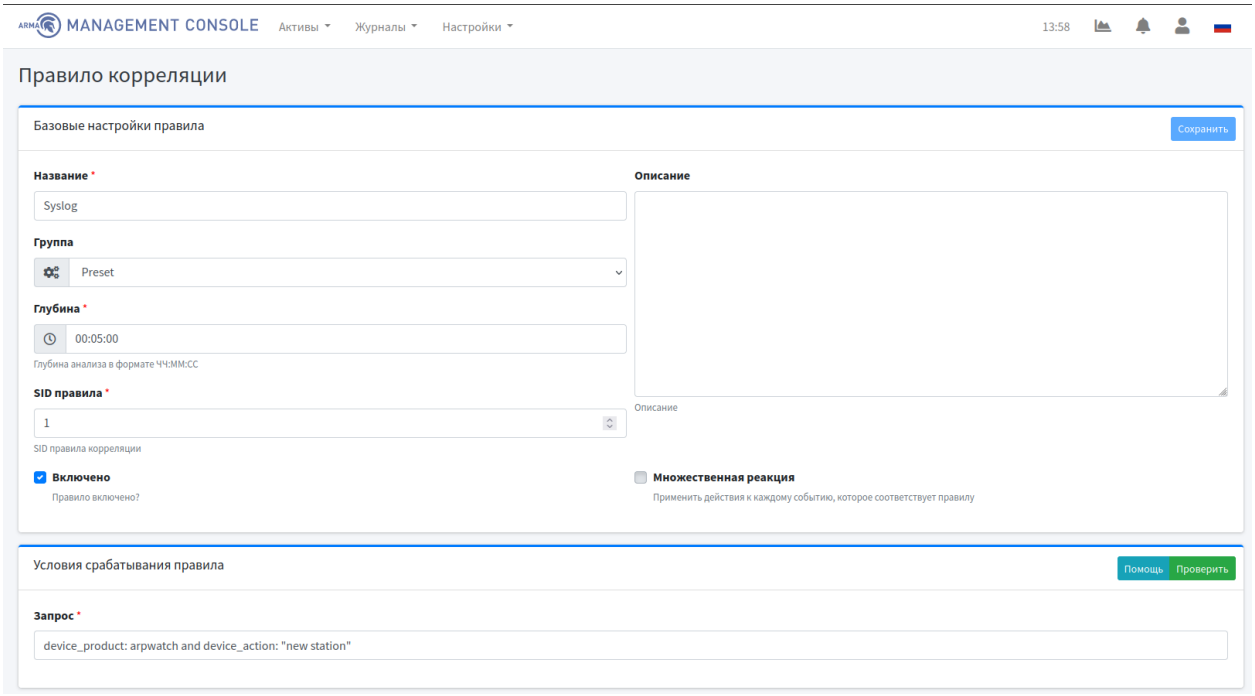


Рисунок 48 – Базовые настройки и условия срабатывания правила корреляции с действием «Syslog»

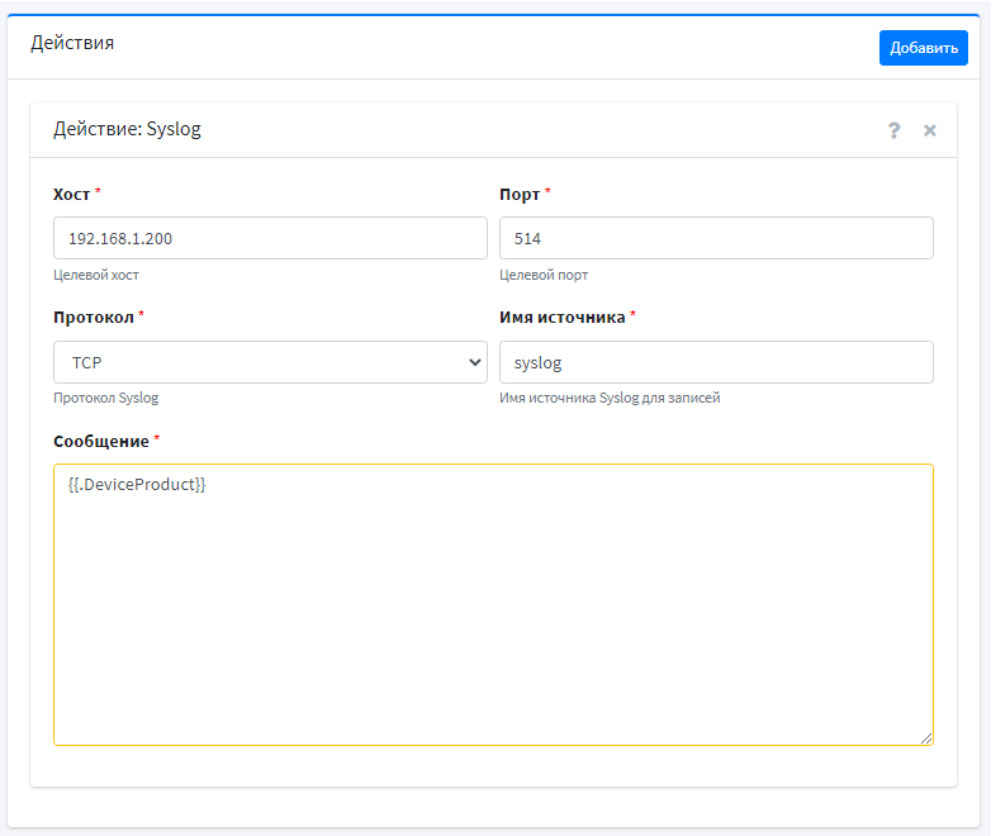


Рисунок 49 – Действие «Syslog»

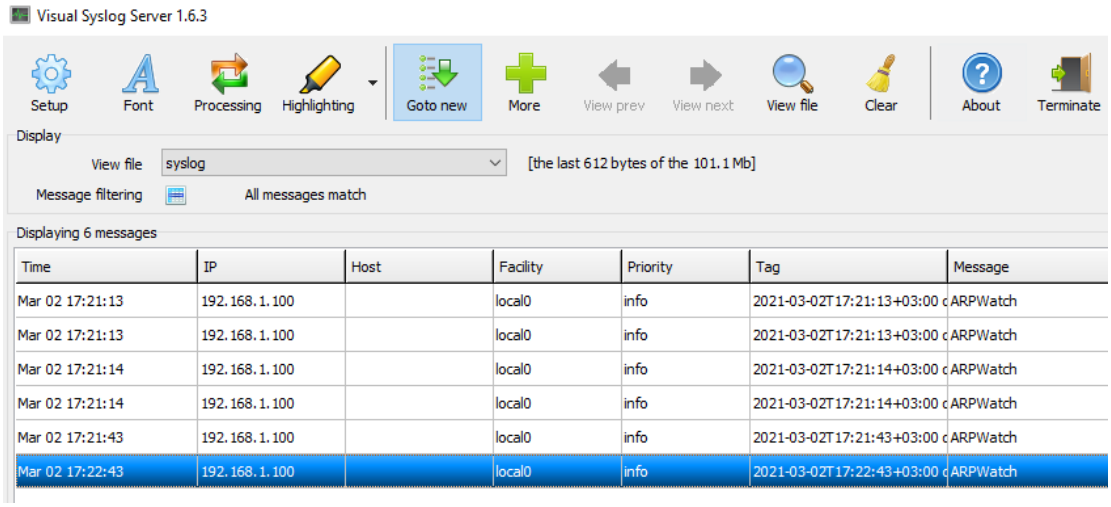


Рисунок 50 – Результат срабатывания правила корреляции с действием «Syslog»

5.1.2 Правило корреляции с типом действия «HTTP»

Действие «HTTP» позволяет при срабатывании определенного события отправлять информацию на внешний сервер, к которому должен быть доступ.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило с действием «HTTP» как показано на рисунках (Рисунок 51, Рисунок 52).

2. Сгенерировать событие (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.

3. Убедиться, что правило корреляции сработало и событие появилось на внешнем сервере (Рисунок 53).

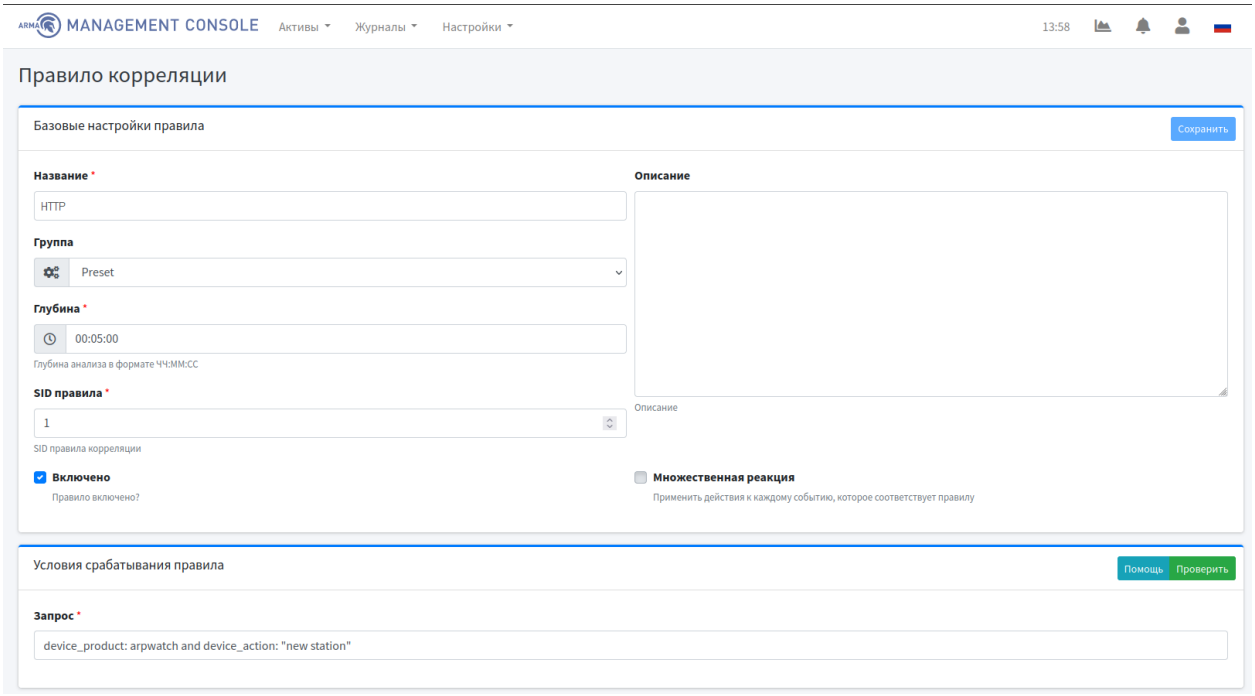


Рисунок 51 – Базовые настройки и условия срабатывания правила корреляции с действием «HTTP»

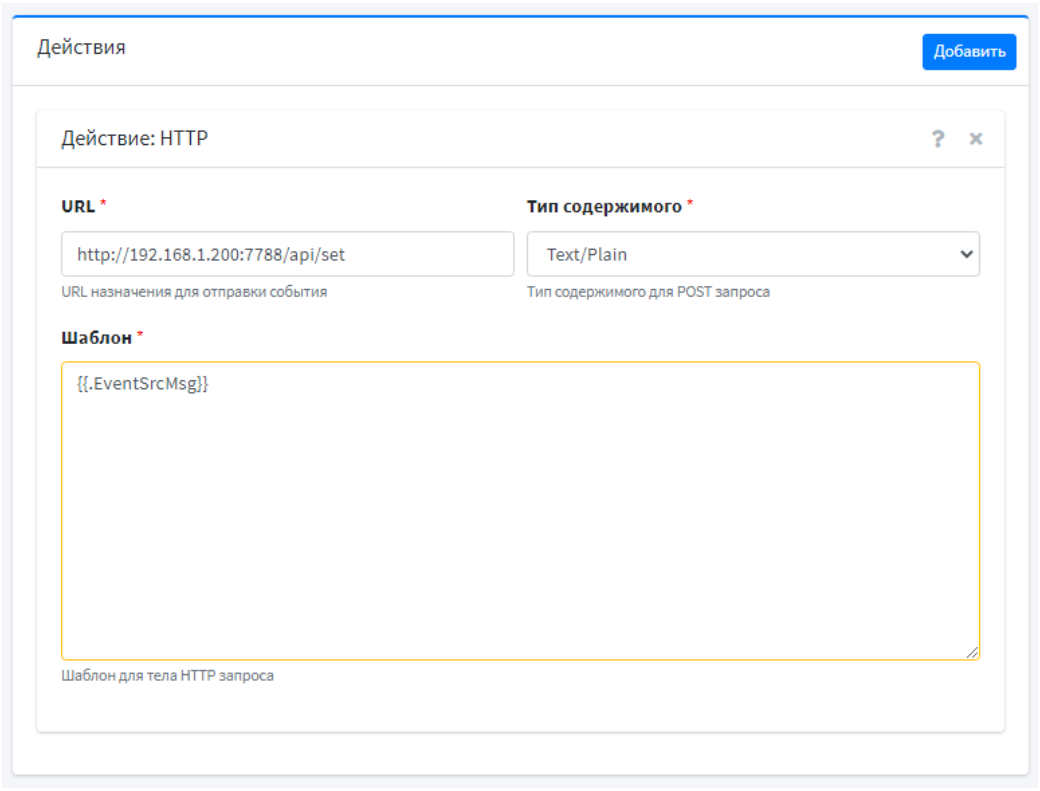


Рисунок 52 – Действие «HTTP»

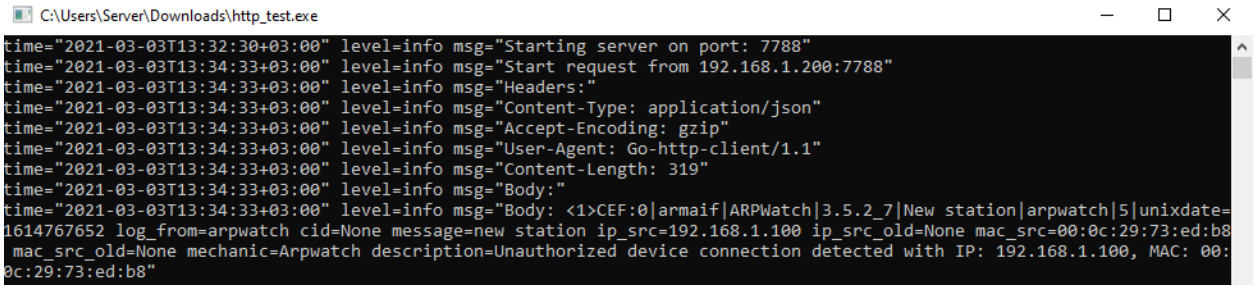


Рисунок 53 – Результат срабатывания правила корреляции с действием «HTTP»

5.1.3 Правило корреляции с типом действия «Инцидент»

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

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «Инцидент» как показано на рисунках (Рисунок 54, Рисунок 55).

2. Сгенерировать событие (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.

3. Убедиться, что правило корреляции сработало и в журнале инцидентов (**«Журналы» - «Инцидент»**) появился инцидент с названием исходного сообщения самого события (Рисунок 56).

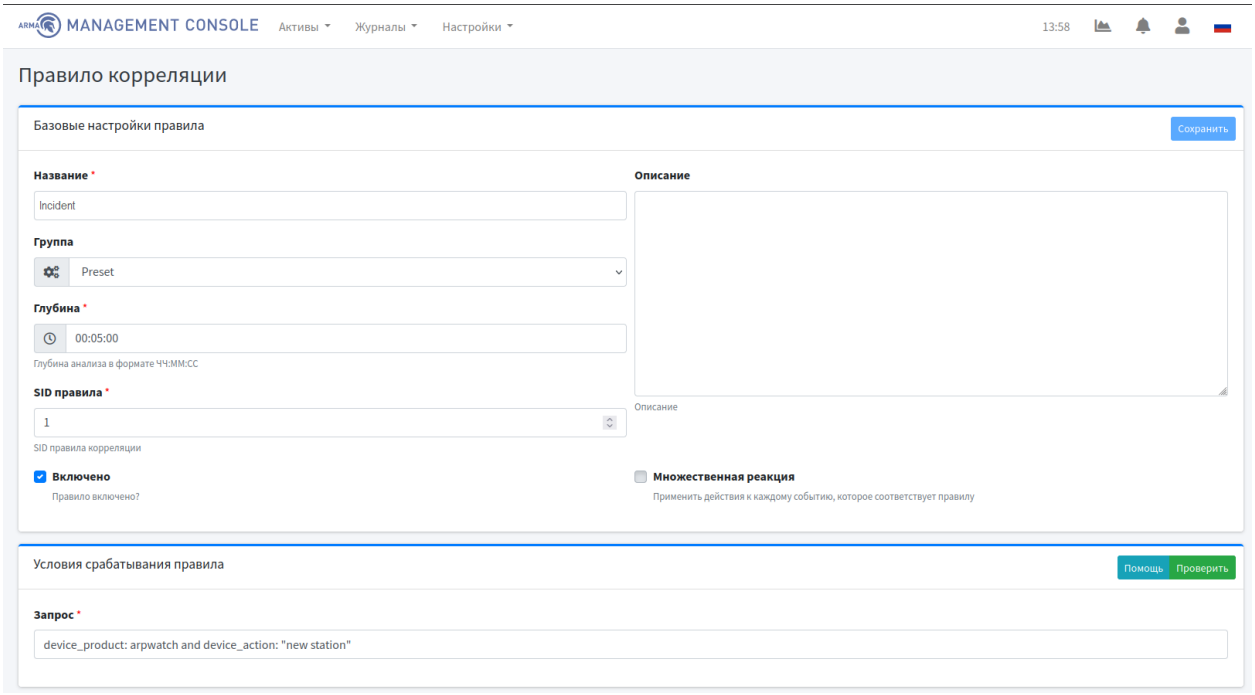


Рисунок 54 – Базовая настройка и условия срабатывания правила корреляции с действием «Инцидент»

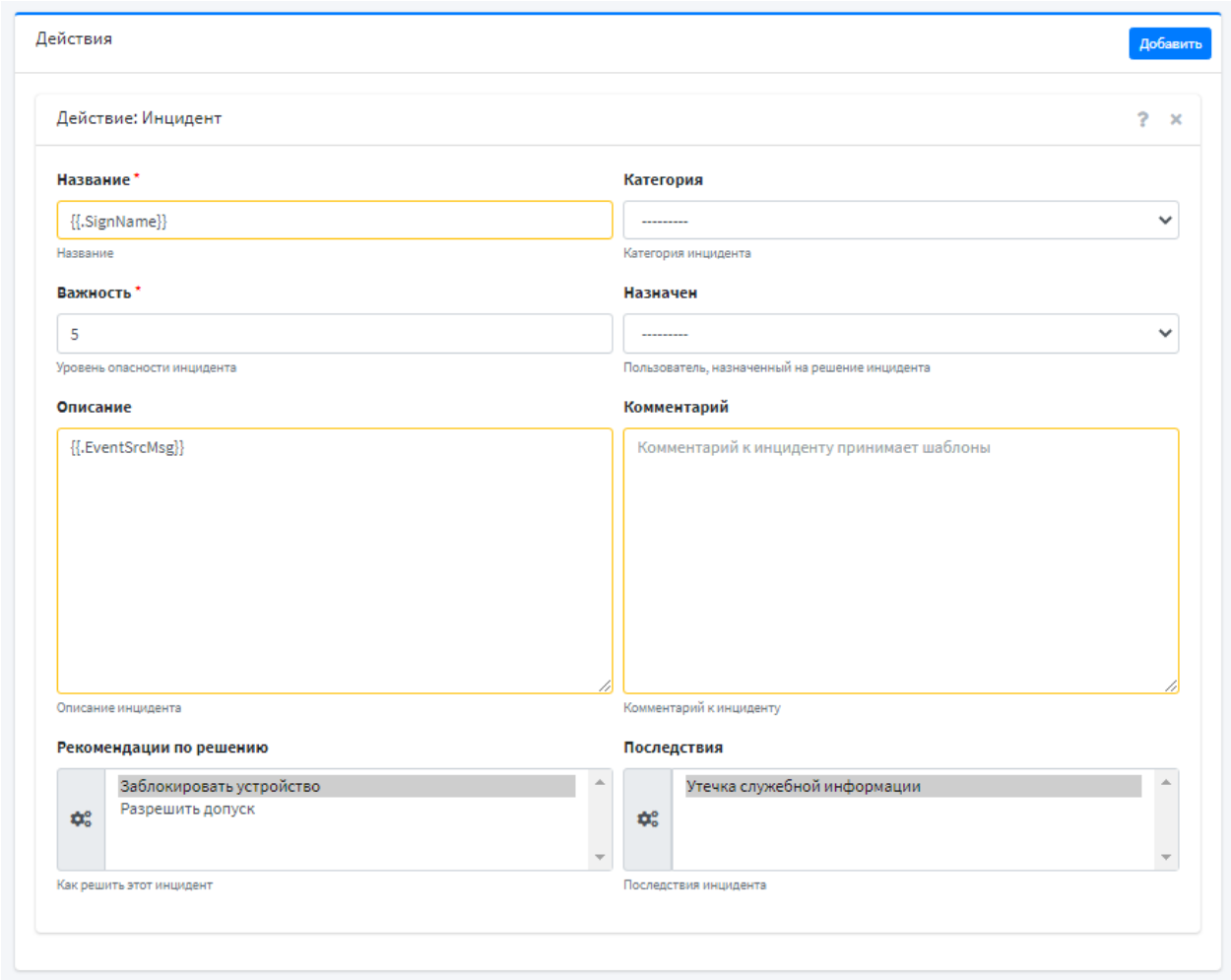


Рисунок 55 – Действие «Инцидент»

При добавлении действия «Инцидент» в поле «Важность» необходимо указать уровень важности инцидента согласно следующей классификации (Таблица 4):

Таблица 4 – Классификация уровней важности инцидентов

Уровень важности инцидента	**Значение параметра**	**Цветовой индикатор на виджете «Инциденты по важности»**
Нет	0	
Информационный	от 0 до 10	
Низкий	от 10 до 40	
Средний	от 40 до 70	
Высокий	от 70 до 90	
Критичный	от 90 до 100	

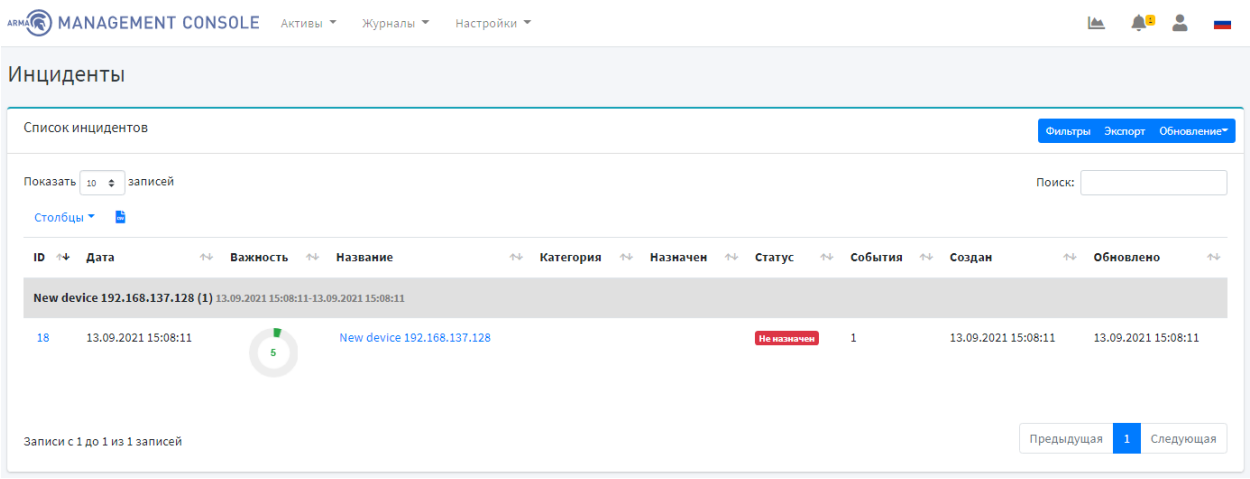


Рисунок 56 – Результат срабатывания правила корреляции с действием «Инцидент»

5.1.4 Правило корреляции с типом действия «Bash скрипт»

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

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «Bash скрипт» как показано на рисунках (Рисунок 57, Рисунок 58).

2. Сгенерировать события (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.

3. Через локальный (консольный) интерфейс убедиться, что в папку tmp добавляются файлы с именем совпадающем по имени сигнатуры самого события, как прописано в сценарии скрипта bash (Рисунок 59).

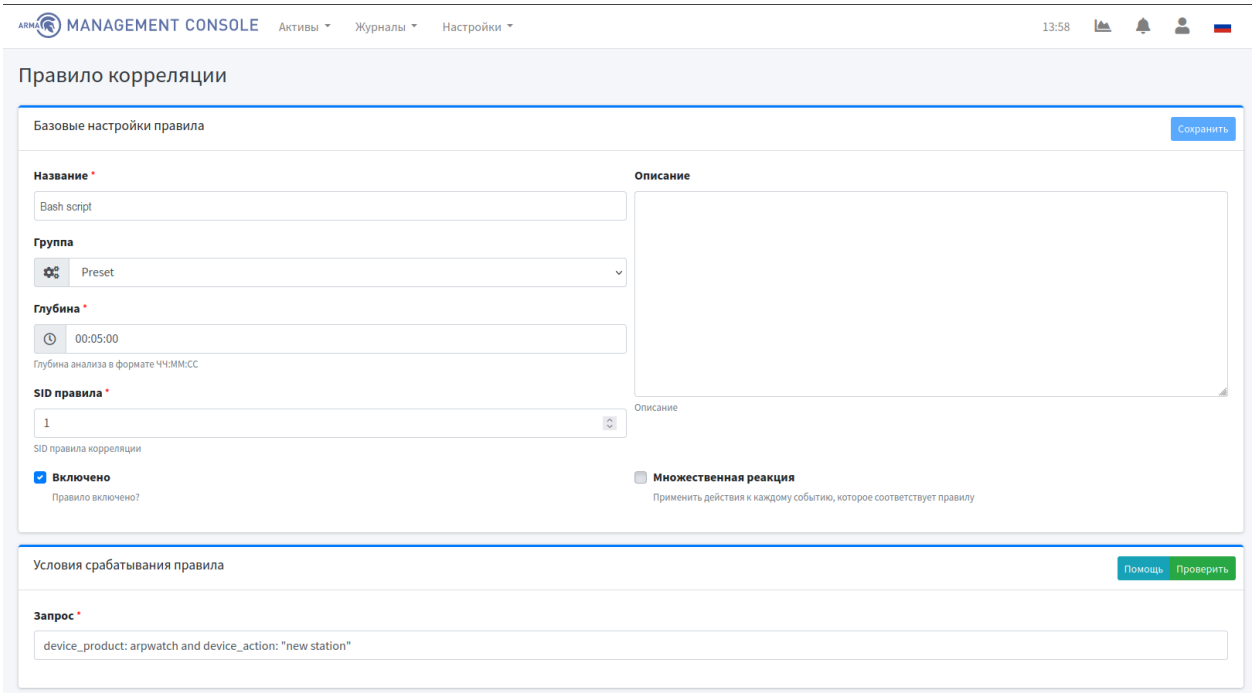


Рисунок 57 – Базовые настройки и условия срабатывания правила корреляции с действием «Bash скрипт»

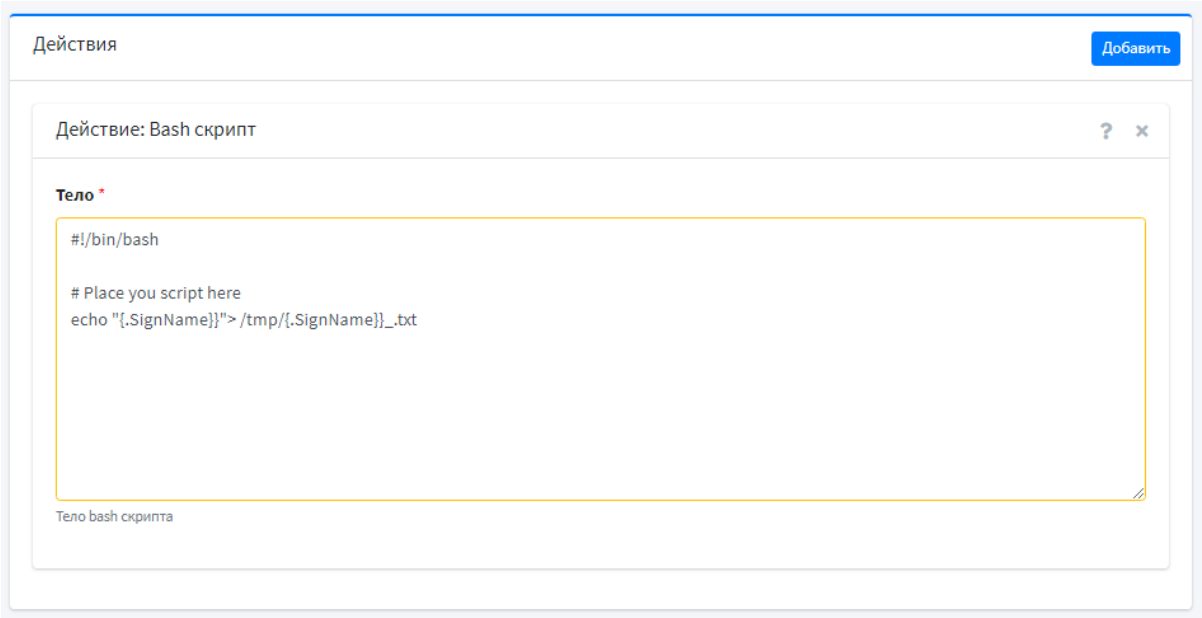


Рисунок 58 – Сценарий Bash скрипта

Рисунок 59 – Результат срабатывания правила корреляции с действием «Bash скрипт»

5.1.5 Правило корреляции с типом действия «Запустить исполняемый файл»

Действие «Запустить исполняемый файл» это некий инструмент физического реагирования на инцидент.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Создать в локальном (консольном) интерфейсе исполняемый файл «script.sh» в папке /tmp/1.
2. Настроить правило корреляции с действием «Запустить исполняемый файл» как показано на рисунках (Рисунок 60, Рисунок 61).
3. Сгенерировать событие (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.
4. Убедиться, что правило корреляции сработало: при возникновении события в папке /tmp/1 создался текстовый документ «1.txt» с заданными параметрами из правила корреляции (Рисунок 62).

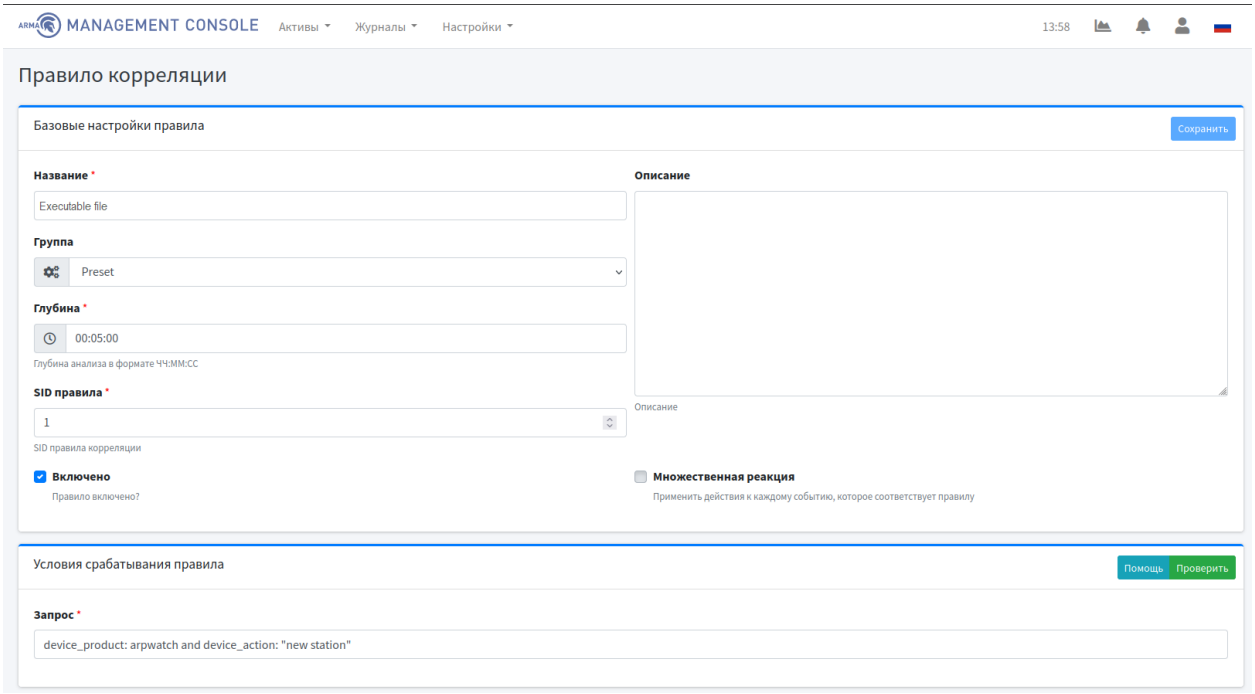


Рисунок 60 – Базовая настройка и условия срабатывания правила корреляции с действием «Запустить исполняемый файл»

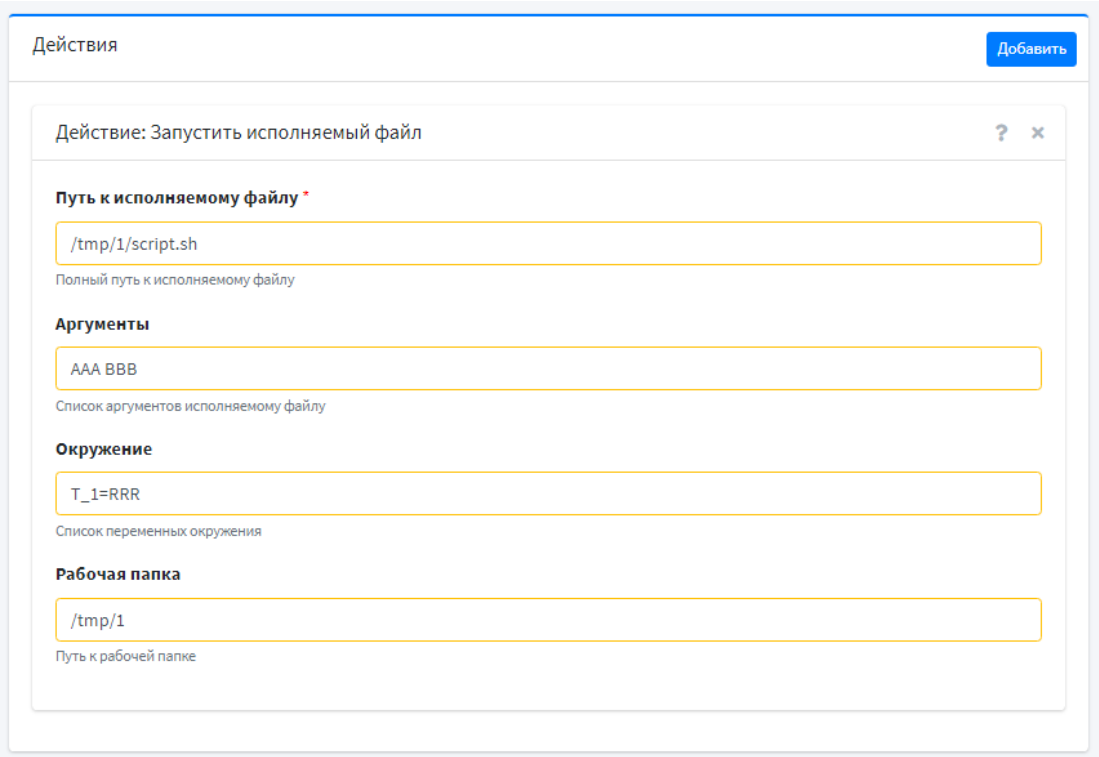


Рисунок 61 – Действие «Запустить исполняемый файл»

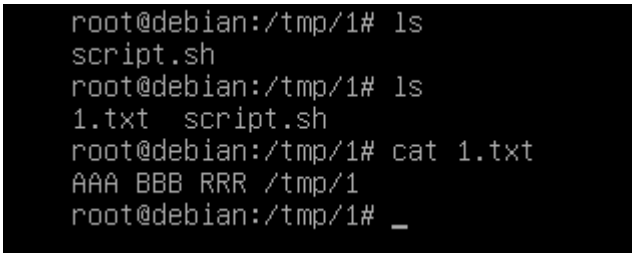


Рисунок 62 – Результат срабатывания правила корреляции с действием «Запустить исполняемый файл»

5.1.6 Правило корреляции с типом действия «Новый актив»

Действие «Новый актив» позволяет при появлении новых устройств в сети ARMA Industrial Firewall отправлять об этом события в журнал событий ARMA Management Console.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «Новый актив» как показано на рисунках (Рисунок 63, Рисунок 64).
2. Сгенерировать событие (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.
3. Убедиться, что в журнале событий (**«Журналы» - «Журнал событий»**) появились нужные события (Рисунок 65).

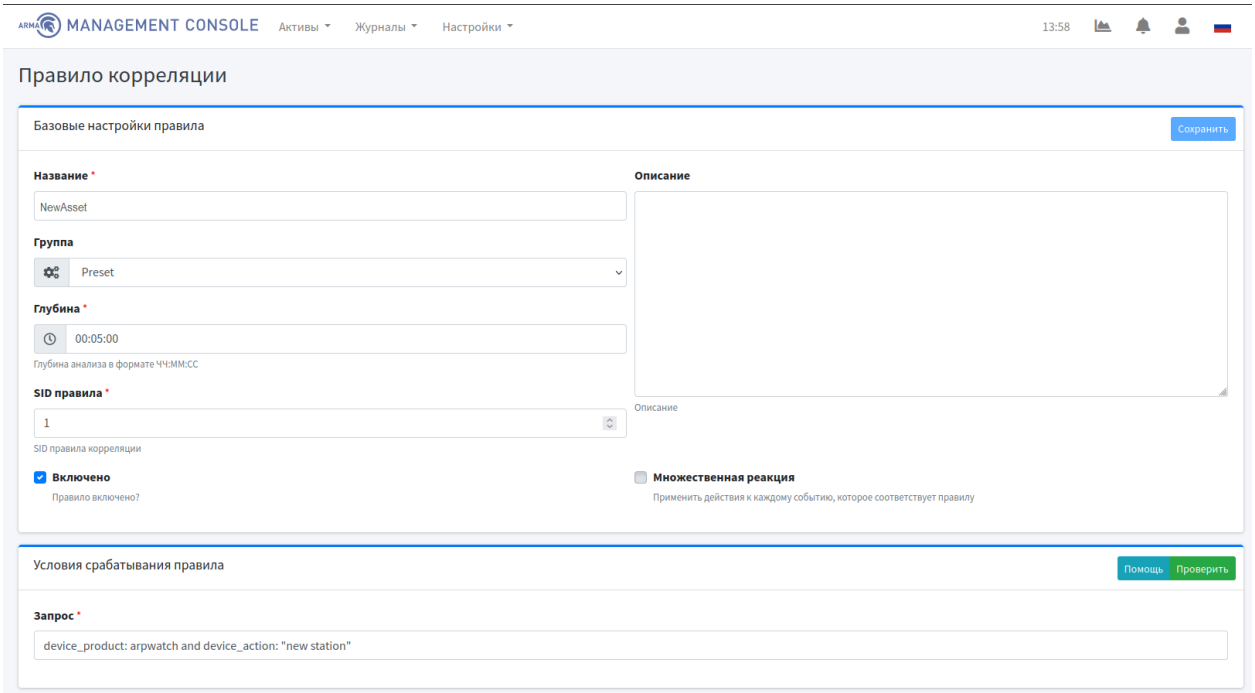


Рисунок 63 – Базовые настройки и условия срабатывания правила корреляции «Новый актив»

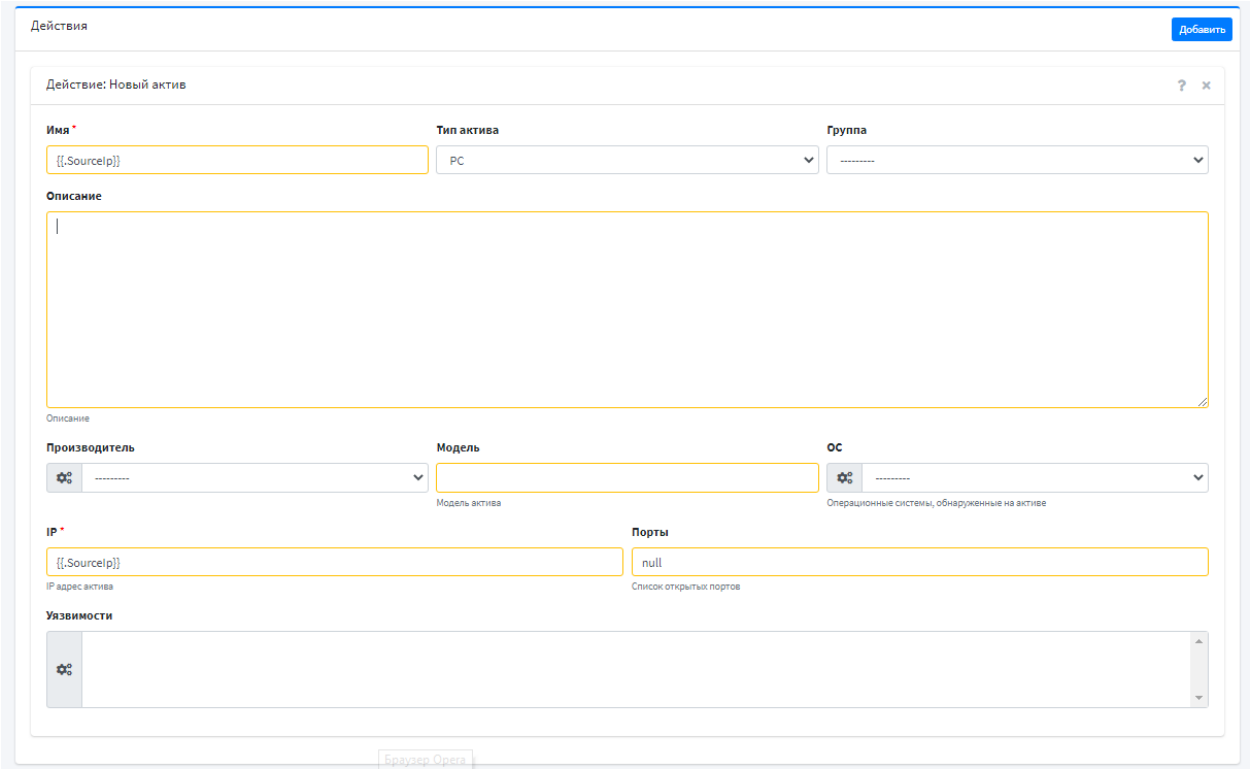


Рисунок 64 – Настройка действия «Новый актив»

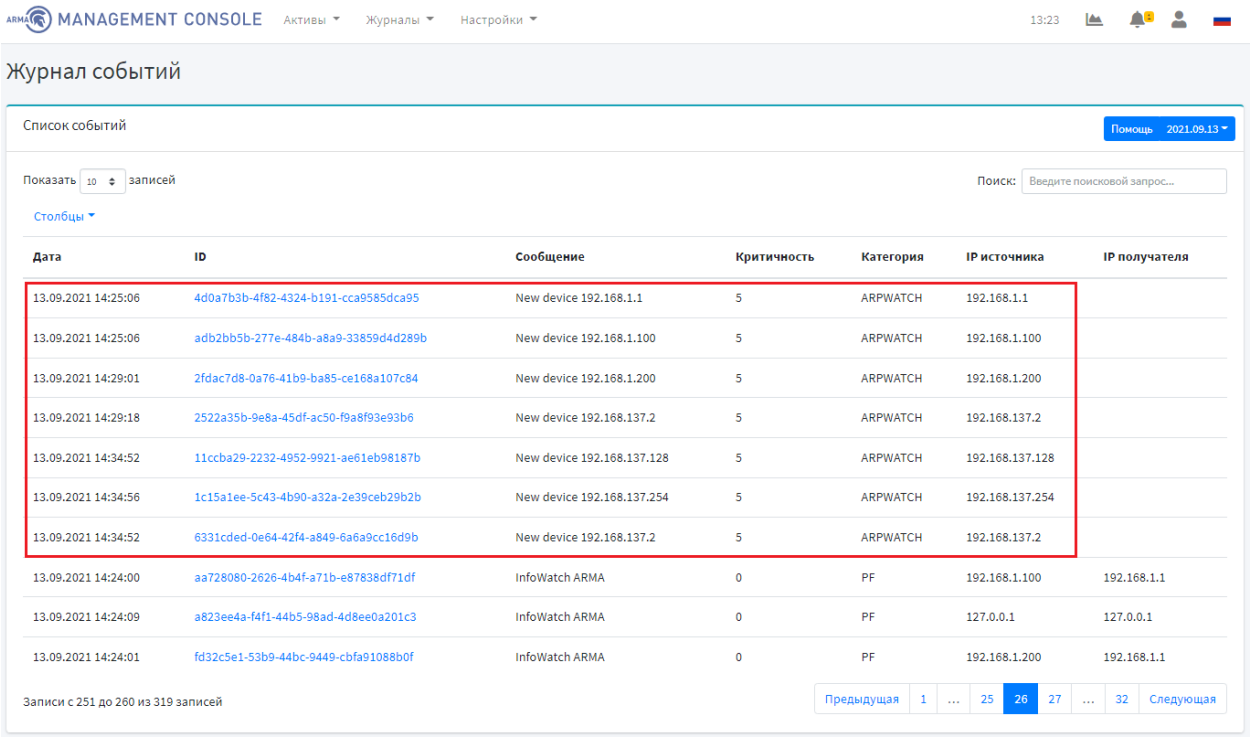


Рисунок 65 – Результат срабатывания правила корреляции с действием «Новый актив»

5.1.7 Правило корреляции с типом действия «Правило межсетевого экрана»

Действие «Правило межсетевого экрана» позволяет на определенное событие создавать правило межсетевого экрана (разрешающее, блокирующее и запрещающее).

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «Правило межсетевого экрана» как показано на рисунках (Рисунок 66, Рисунок 67).

2. Сгенерировать событие (в данном случае, появление новых устройств в сети). Для этого необходимо в ARMA IF перейти в раздел обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), установить флажок **«Включить»**, выбрать прослушиваемые интерфейсы и нажать **кнопку «Сохранить»**.

3. Убедиться, что в разделе API правил ARMA Industrial Firewall (**«Межсетевой экран» - «API правила»**) появилось правило с заданными параметрами (Рисунок 68).

Примечание – при редактировании созданного правила корреляции с типом действия «Правило межсетевого экрана» при выборе другого МЭ в поле «ARMA IF» текущие настройки будут сброшены.

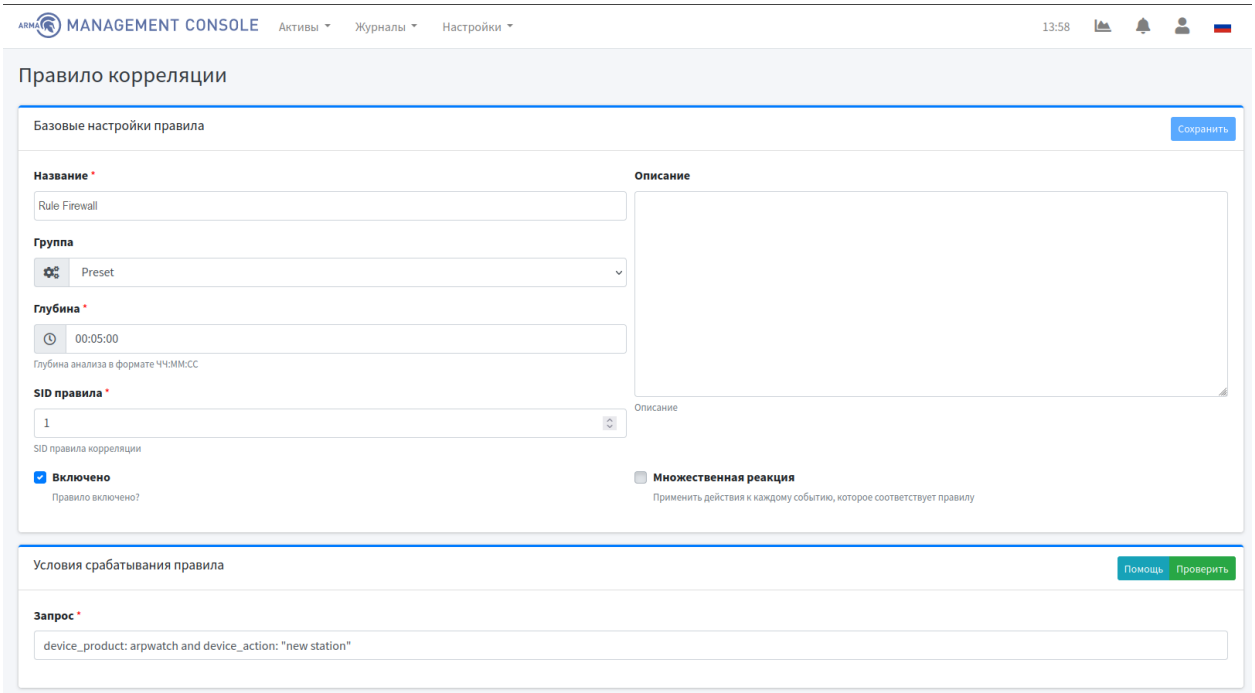


Рисунок 66 – Базовая настройка и условия срабатывания правила корреляции с действием «Правило межсетевого экрана»

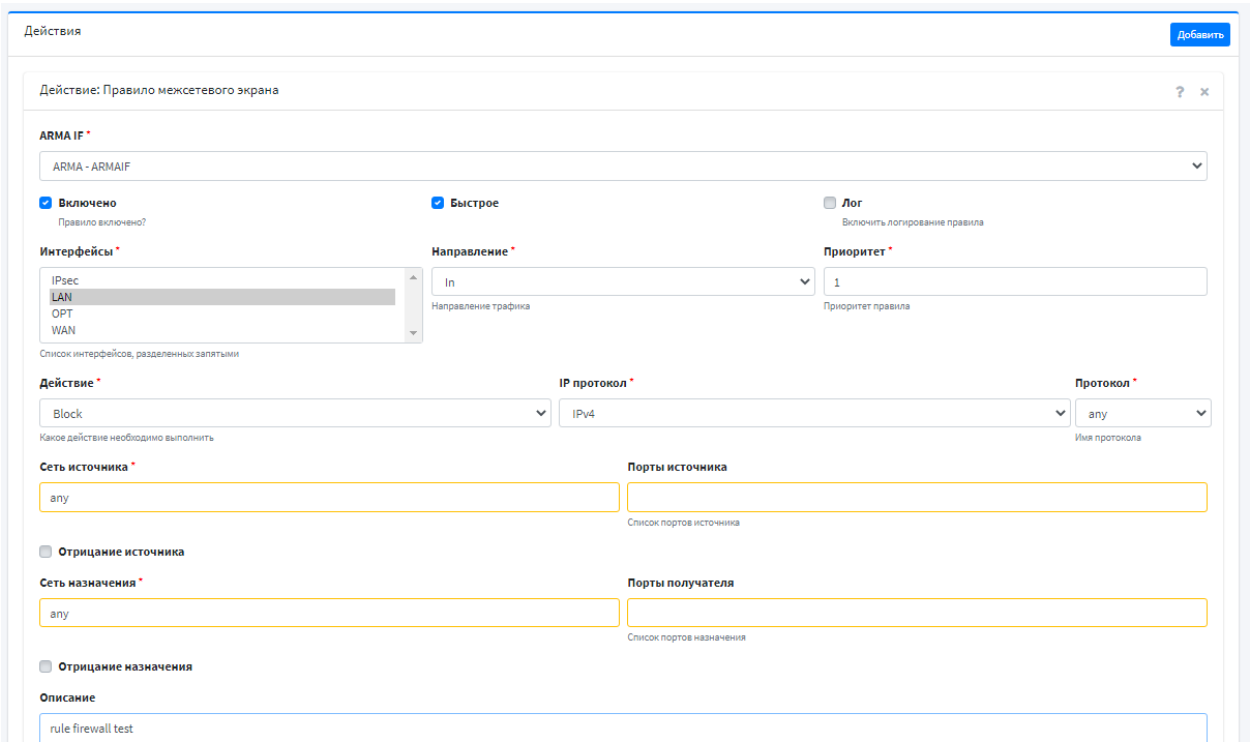


Рисунок 67 – Действие «Правило межсетевого экрана»

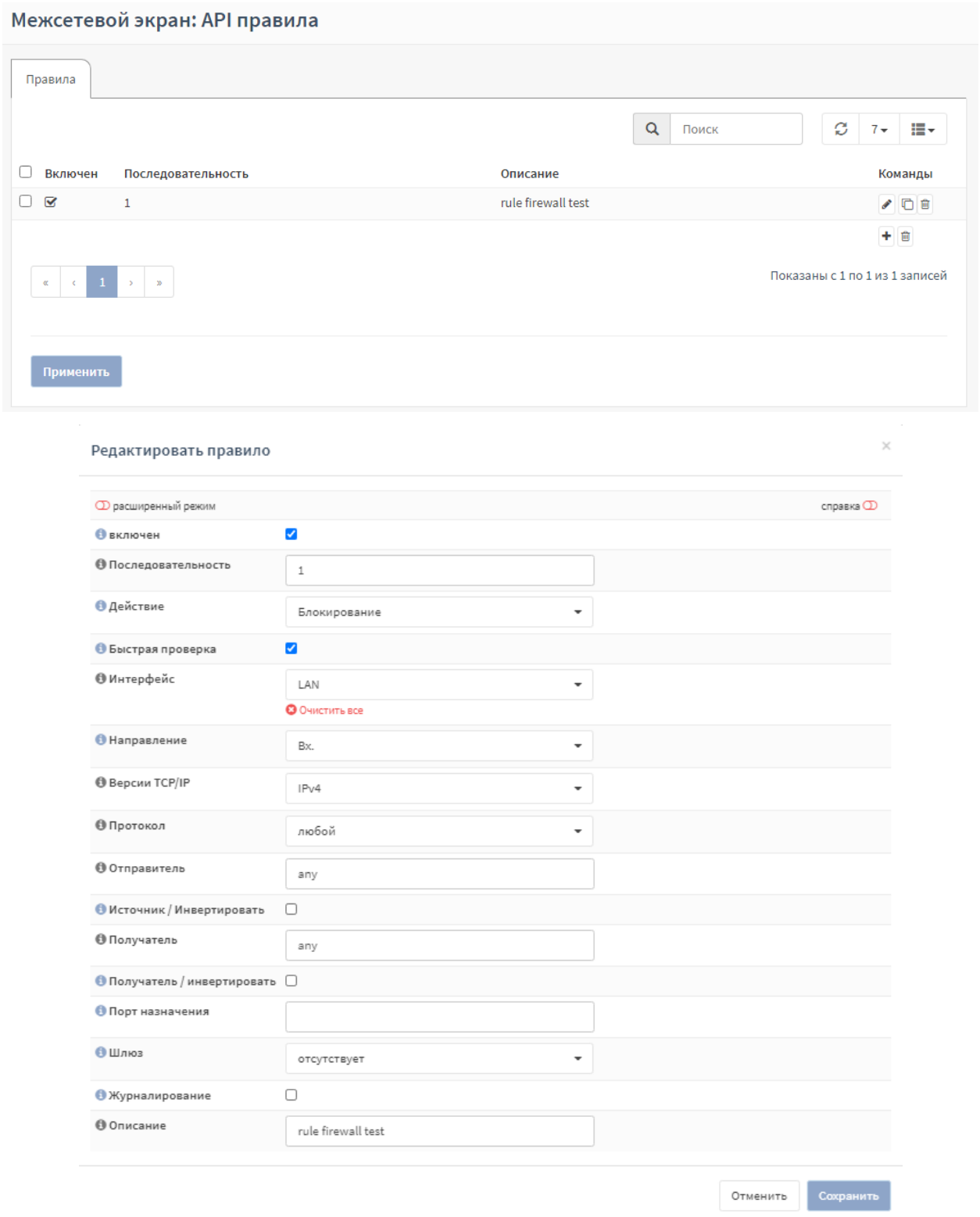


Рисунок 68 – Результат срабатывания правила корреляции с действием «Правило межсетевого экрана»

5.2 Настройка ротации журналов

Текущий раздел позволяет настраивать ротацию журнала инцидентов и журнала событий (Рисунок 69).

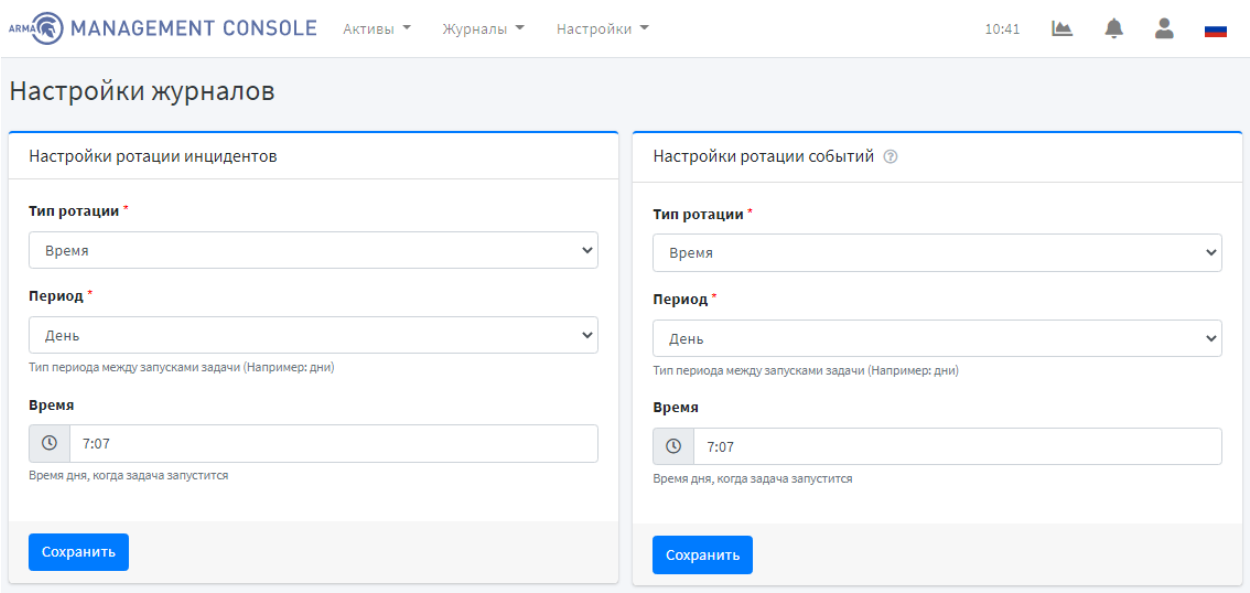


Рисунок 69 – Настройки ротации инцидентов/событий по времени

В поле «Тип ротации» необходимо выбрать один из типов ротации – «Время», «Размер», «Отключено».

При выборе типа ротации «Время» в поле «Период» необходимо выбрать один из периодов времени – «День», «Неделя», «Месяц». При выборе периода «День» в поле «Время» необходимо указать время дня, когда будет запущена задача и нажать на кнопку Сохранить. При выборе периода «Неделя» необходимо выбрать день недели, в который будет запущена задача и нажать на кнопку Сохранить. При выборе периода «Месяц» необходимо выбрать месяц, в котором будет запущена задача и нажать на кнопку Сохранить.

При выборе типа ротации «Размер» в поле «Размер таблицы, когда происходит ротация» необходимо указать размер таблицы и нажать на кнопку (Рисунок 70).

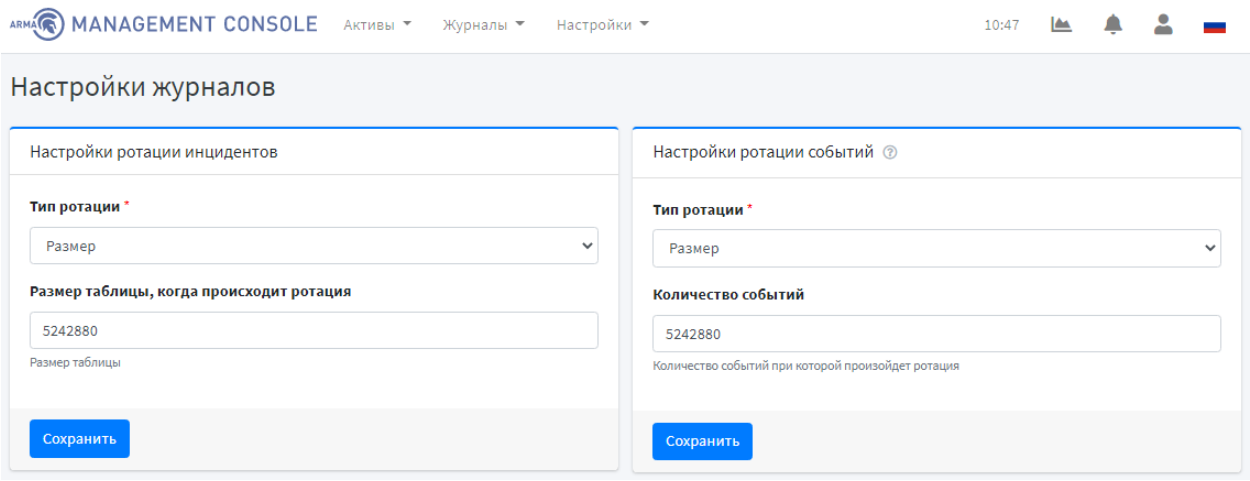


Рисунок 70 – Настройки ротации инцидентов/событий по размеру

Для отключения ротации журналов необходимо выбрать тип ротации «Отключено» и нажать на кнопку Сохранить.

Примечание – при срабатывании ротации инцидентов ротируются инциденты только со статусом «Решен» и «Ложное срабатывание».

При настройке ротации событий, нажав на кнопку , появится окно справки (Рисунок 71).

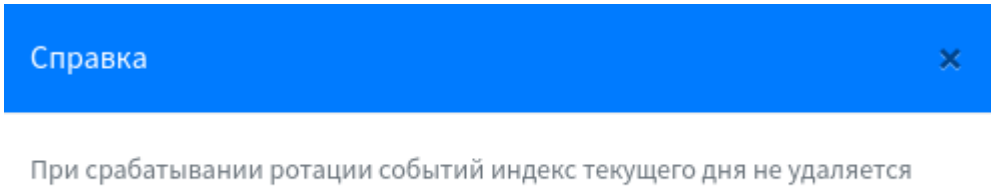


Рисунок 71 – Окно справки в настройках ротации событий

5.3 Настройка экспорта инцидентов

Текущий раздел позволяет настраивать экспорт событий по протоколам OPC UA и Syslog (Рисунок 72).

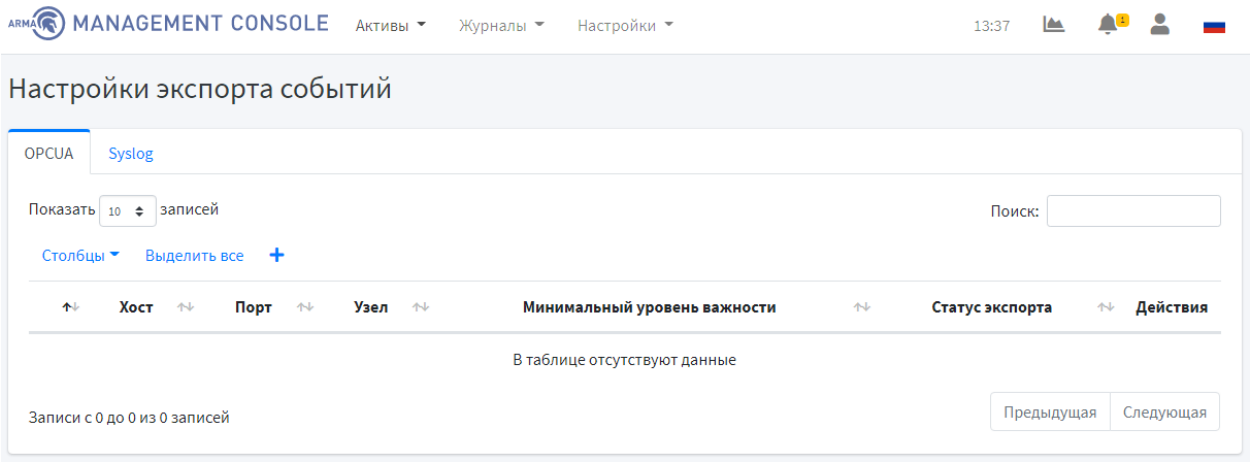


Рисунок 72 – Страница экспорта событий

Для настройки экспорта событий по протоколам OPC UA и Syslog необходимо добавить получателя, нажав на кнопку . В открывшейся форме заполнить поля (Рисунок 73, Рисунок 74).

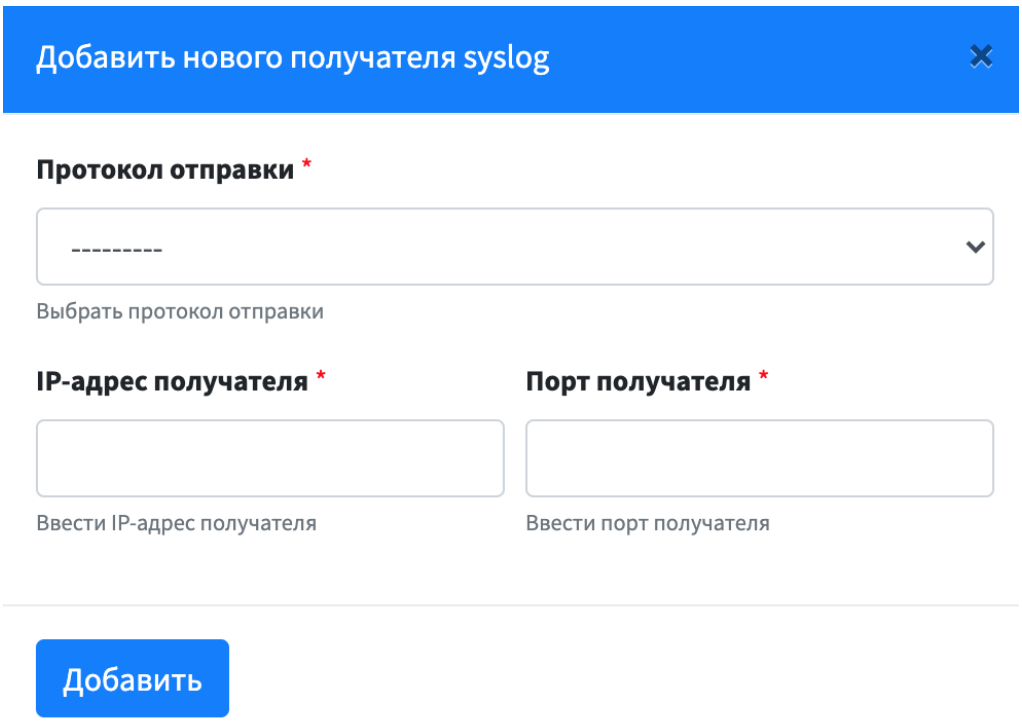
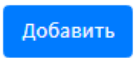


Рисунок 73 – Добавление получателя (Syslog)

В поле «Протокол отправки» необходимо выбрать протокол отправки, в поле «IP-адрес получателя» ввести IP-адрес получателя, в поле «Порт получателя» ввести порт получателя и нажать на кнопку 

.

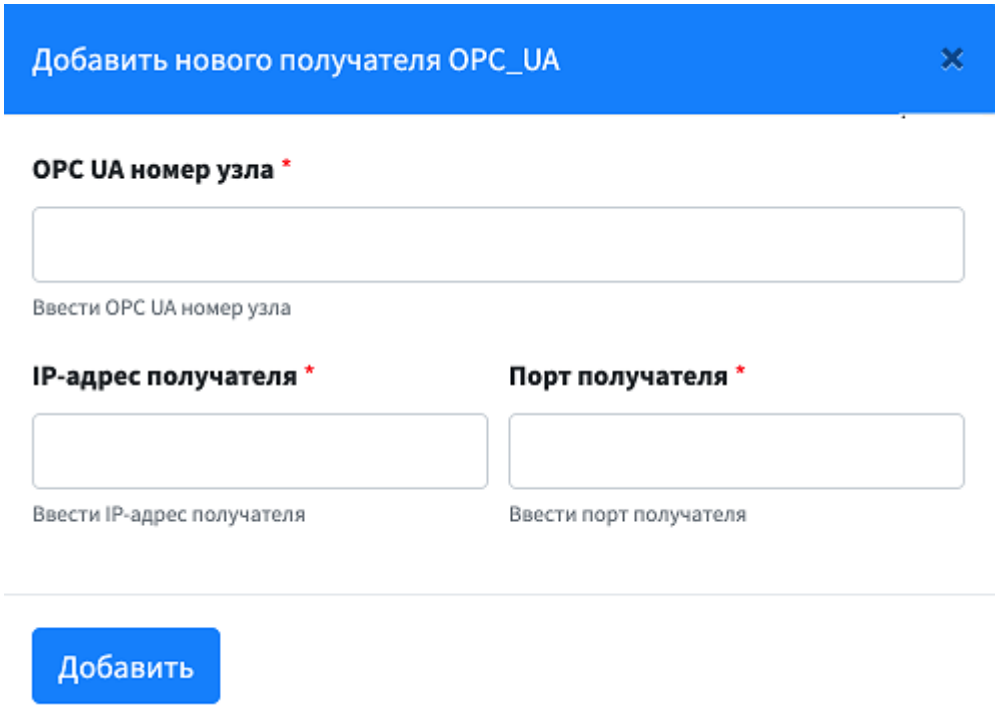
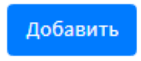


Рисунок 74 – Добавление получателя (OPC_UA)

В поле «OPC UA номер узла» необходимо указать номер узла, в поле «IP-адрес получателя» ввести IP-адрес получателя, в поле «Порт получателя» ввести порт получателя и нажать на кнопку 

.

5.3.1 Формат сообщений при экспорте инцидентов через Syslog

5.3.1.1 Формат основного сообщения

<DateTime> <Host/IP> AMC: <MessageBody>

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

Пример такого 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

5.3.1.2 Формат вложенного сообщения CEF

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

- **<Version>** - версия CEF
- **<Device Vendor>** - производитель источника логов (всегда InfoWatch ARMA)
- **<Device Product>** - название продукта, источника логов (всегда InfoWatch ARMA Management Console)
- **<Device Version>** - версия продукта, источника логов.
- **<Device Event Class ID>** - тип сообщения, всегда равен Incident
- **<Name>** - название инцидента
- **<Severity>** - серьезность 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 (пример: 1608216295000)
  - **cs1** - уникальный идентификатор инцидента (пример: 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 (пример: 1608216295000)
- **end** - время появления последнего события для текущего инцидента в формате unixtime в миллисекундах (пример: 1608216295000)
- **msg** - описание инцидента, зависит от сформировавшего инцидент правила корреляции. Применяется экранирование символов \, = с помощью постановки символа \ перед такими символами

Пример такого сообщения:

CEF:0|InfoWatch ARMA|ARMAMC|1.0.1|Incident|test|5|cnt=1 rt=1608216295000 cs1=1c5f4516-27cb-4714-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

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

5.3.2 Формат сообщений при экспорте инцидентов через OPCUA

Формат основного сообщения и вложенного сообщения CEF при экспорте инцидентов через OPCUA аналогичен формату сообщений при экспорте инцидентов через Syslog, который представлен в подразделах 5.3.1.1 и 5.3.1.2.

При экспорте инцидентов по OPCUA будет осуществляться выгрузка не всех инцидентов, а только последнего, так как новый экспортируемый инцидент будет заменять предыдущий инцидент.

Пример сообщения:

AMC: CEF:0|InfoWatch ARMA|ARMAMC|1.1.0-rc20|Incident|inc_100|1|cnt=1 rt=1638433303000 cs1=1bbf23d7-46a3-4af3-a01a-2d18bbed47a9 cs1Label=IncidentID start=1638432975000 end=1638432975000

Примечание – экспорт инцидентов всегда осуществляется в переменную с индексом [0] в рамках объекта с индексом [1].

5.4 Настройка TLS сертификата

Текущий раздел позволяет настраивать режим работы ARMA Management Console по HTTPS.

Блок настроек «TLS сертификат» позволяет включать TLS, генерировать сертификат безопасности и ключ к нему (Рисунок 75).

Действующий сертификат и ключ, которые можно скачать, нажав на certificate.crt и certificate.key, сгенерированы со сроком действия 1 год. После окончания срока действия текущего сертификата и ключа необходимо сгенерировать новый, нажав на кнопку Создать новый.

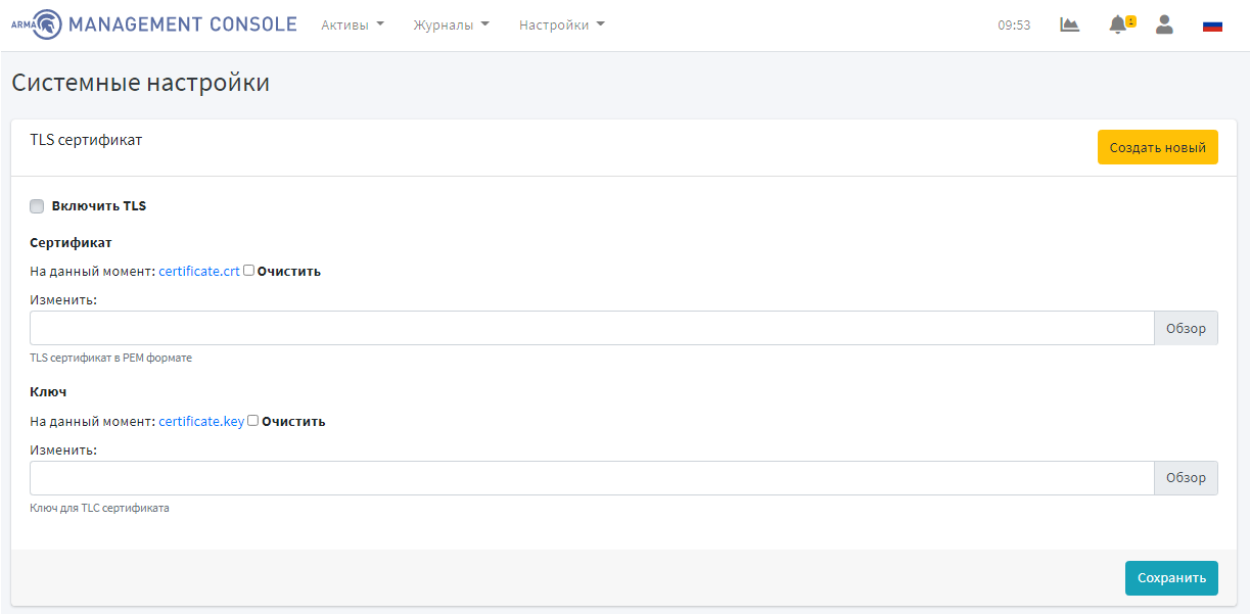


Рисунок 75 – Системные настройки. TLS сертификат

Блок настроек «Настройки аутентификации» позволяет задавать количество допустимых попыток входа в систему и время, в течение которого пользователю будет отказано в аутентификации после превышения попыток входа (Рисунок 76). Значение количества допустимых попыток входа в систему должно быть больше либо равно 0.

Примечание – по прошествии времени, указанного в поле «Тайм-аут попыток аутентификации», пользователю снова будет доступен вход в систему.

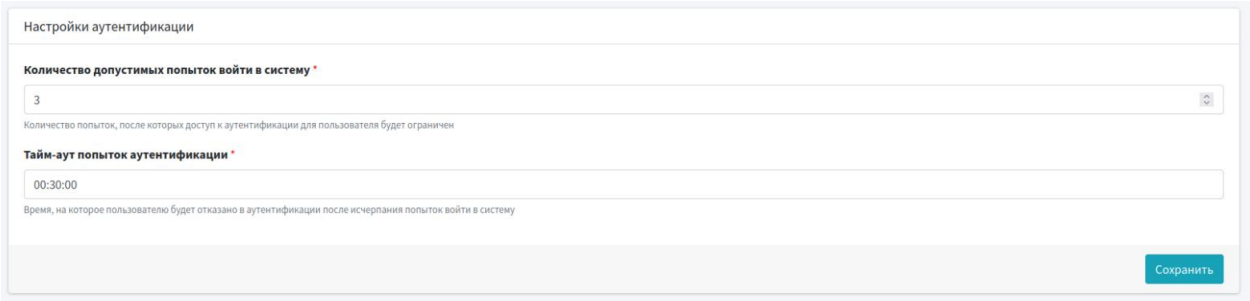


Рисунок 76 – Системные настройки. Настройки аутентификации

5.5 Управление лицензиями

Текущий раздел позволяет просматривать информацию о действующей лицензии, а также активировать новую.

Для просмотра информации о действующей лицензии необходимо перейти на страницу «Настройки» - «Лицензия» - «Информация о лицензии». Информация о лицензии включает в себя (Рисунок 77):

– основную информацию;
– функционал лицензии;
– опции лицензии.

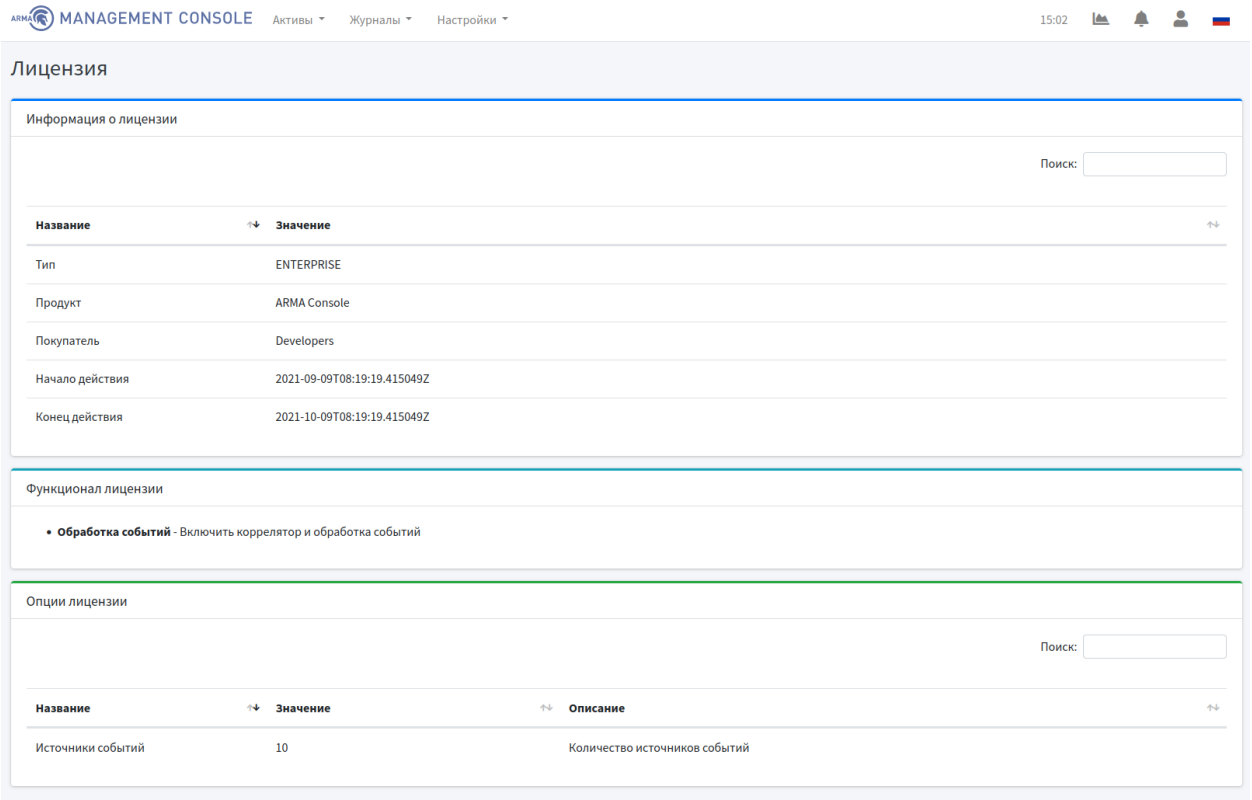


Рисунок 77 – Информация о действующей лицензии

В ARMA Management Console предусмотрены следующие типы лицензий:

1. ENTERPRISE базовая. Предоставляет доступ ко всем функциям ARMA Management Console, кроме тех, что входят в тип лицензии «ENTERPRISE базовая + обработка инцидентов». Срок лицензии не ограничен.

2. ENTERPRISE базовая + обработка инцидентов. Включает в себя все функции ARMA Management Console, а также предоставляет доступ к дополнительным функциям:

– формирование правил корреляции (создание, импорт и экспорт правил);
– работа с инцидентами (просмотр журнала инцидентов, расследование инцидентов, настройка экспорта инцидентов по протоколам OPC UA и Syslog).

Срок лицензии не ограничен.

3. TRIAL. Предоставляет доступ ко всем функциям ARMA Management Console. Срок лицензии ограничен.

Для активации новой лицензии необходимо перейти на страницу «Настройки» - «Лицензия» - «Активировать новую» и активировать лицензию

одним их предложенных способов. Подробный процесс активации лицензии описан в п. 2.4.1 и 2.4.2 настоящего руководства.

6 УПРАВЛЕНИЕ СИСТЕМАМИ ЗАЩИТЫ

Текущий раздел доступен пользователям с правом доступа «Может просматривать список систем защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для просмотра систем защиты необходимо перейти на страницу «Активы» - «Системы защиты» (Рисунок 78).

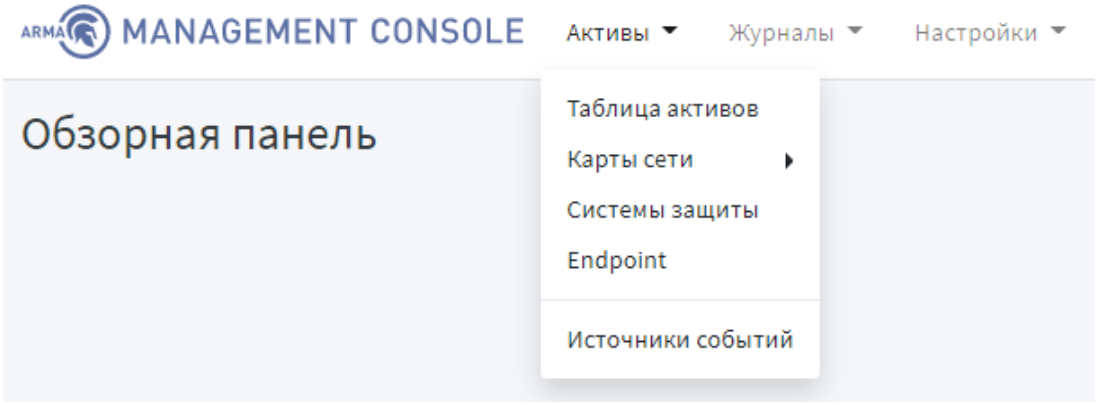


Рисунок 78 – Переход на страницу систем защиты

6.1 Описание таблицы систем защиты

Страница «Системы защиты» позволяет просматривать системы защиты в формате таблицы, которая содержит следующие данные (Рисунок 79):

- статус;
- тип системы защиты;
- имя узла;
- IP-адрес;
- действия (отображаются только для пользователя с правом «Может управлять системами защиты»):
  - : информация о системе защиты;
  -
  - езагрузка системы управления;
  - : скачивание конфигурации на устройство;
  - : скачивание баз решающих правил СОВ;
  - : редактирование информации о системе защиты;
  - : удаление системы защиты из списка.

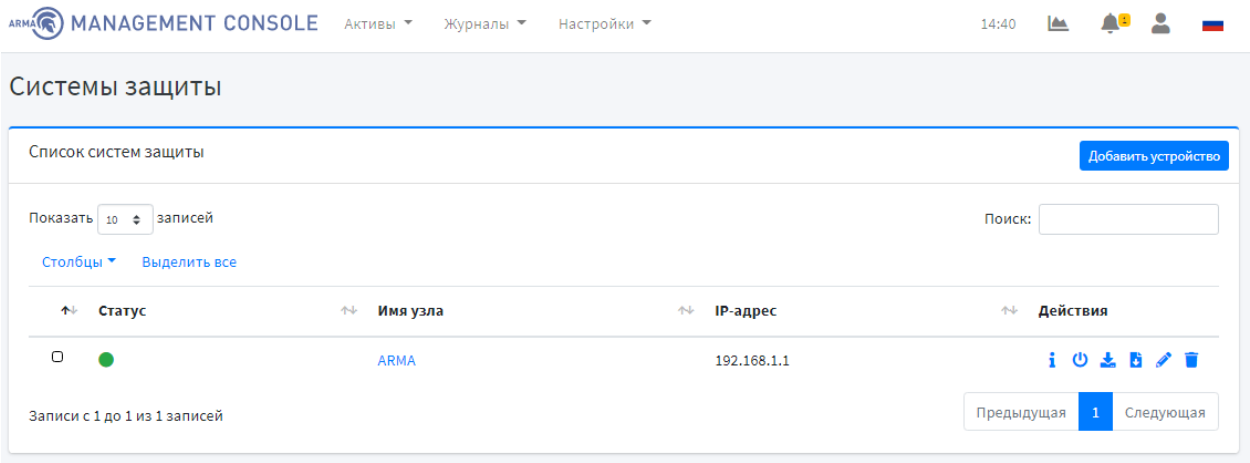


Рисунок 79 – Системы защиты

Для выбора количества записей, отображаемых в таблице систем защиты на странице «Активы» - «Системы защиты» необходимо нажать на кнопку  в левом в верхнем углу страницы.

Поле «Поиск» вверху таблицы систем защиты позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку  рядом с названием соответствующего столбца.

Для изменения столбцов, отображаемых в таблице, необходимо нажать на кнопку  .

Действия доступные для применения к нескольким системам защиты следующие (отображается только для пользователя с правом «Может управлять сенсорами»):

–  : загрузка конфигурации на устройство;

–  : загрузка баз решающих правил СОВ;

 : удаление системы защиты из списка.

Для применения действий ко всем системам защиты необходимо нажать на кнопку «Выделить все». Для применения действий к нескольким системам защиты необходимо поставить флажок в левом столбце напротив соответствующих систем защиты.

В столбце «Статус» отображается статус добавленных систем защиты, такие как:

–  : в сети – система защиты включена и доступна;

– : не в сети – система защиты не доступна;

– : ошибка – произошла ошибка при подключении к системе защиты.

6.2 Добавление системы защиты

Текущий подраздел доступен только для пользователя с правом «Может добавлять системы защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для добавления системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать на кнопку Добавить устройство.

Всплывающее окно позволяет ввести необходимую информацию для подключения новой системы защиты (Рисунок 80).

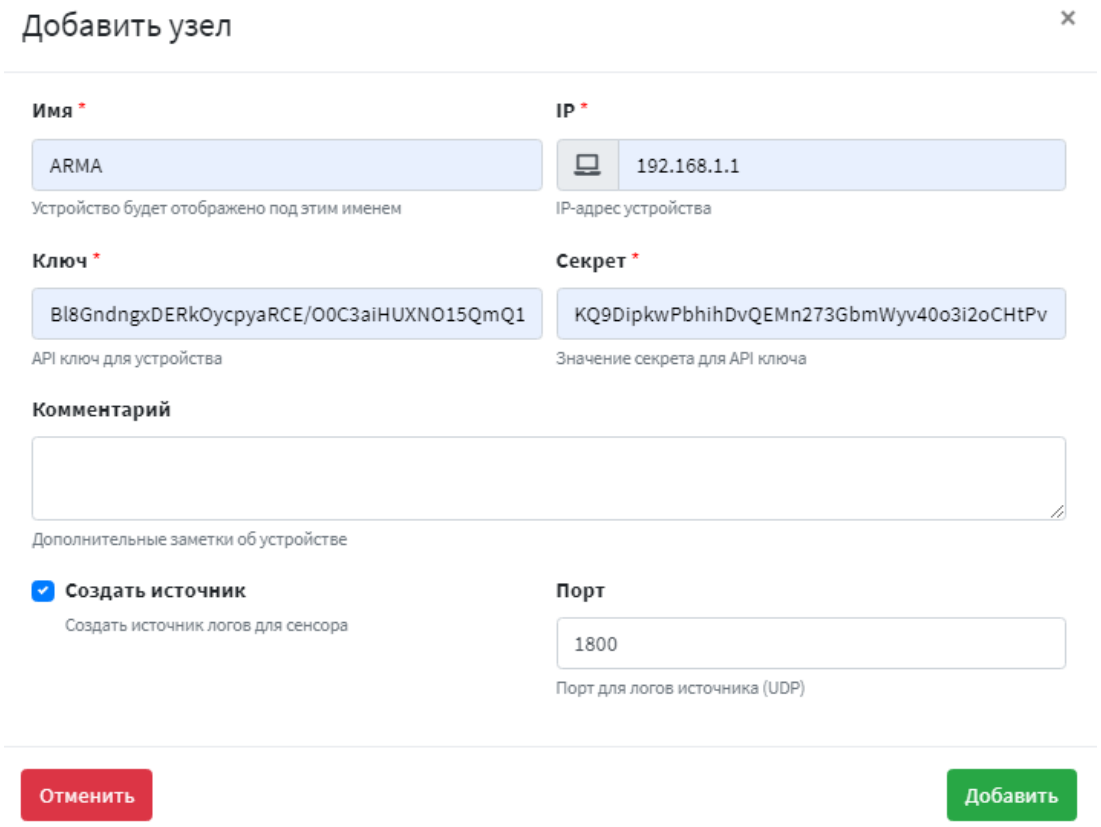


Рисунок 80 – Добавление нового устройства

В поле «Имя» необходимо ввести название системы защиты. В поле «IP» необходимо ввести IP-адрес или домен подключаемой системы. В поле «Ключ» необходимо ввести ключ авторизации. В поле «Секрет» необходимо ввести «секрет» для API ключа. В поле «Комментарий» необходимо ввести комментарий к системе защиты. Для создания источника события для системы защиты необходимо поставить галочку в поле «Создать источник». В поле «Порт» необходимо указать порт для входящих логов.

Примечание – в поле «Порт» необходимо указать любой произвольный, но свободный порт, начиная с 1500.

Для сохранения информации и добавления системы защиты необходимо нажать на кнопку Добавить. Для отмены добавления нового устройства необходимо нажать на кнопку Отменить.

При добавлении системы защиты ARMA Management Console выполняет проверку совместимости версий продуктов. В случае, если версии продуктов не совместимы, то отобразится уведомление об этом (Рисунок 150).

6.3 Удаление системы защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять системами защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для удаления системы защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо нажать на кнопку напротив системы защиты, которую собираетесь удалить. После нажатия на кнопку необходимо подтвердить удаление, нажав во всплывающем окне кнопку «Да».

Для удаления нескольких систем защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо выбрать несколько систем защиты (для выбора всех систем защиты нажать на кнопку «Выделить все» вверху таблицы) и нажать на кнопку вверху таблицы. После нажатия на кнопку необходимо подтвердить удаление, нажав во всплывающем окне кнопку «Да».

6.4 Редактирование основной информации о системе защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять системами защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для редактирования системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать на кнопку напротив системы защиты.

Всплывающее окно позволяет изменить необходимую информацию системы защиты (Рисунок 81).

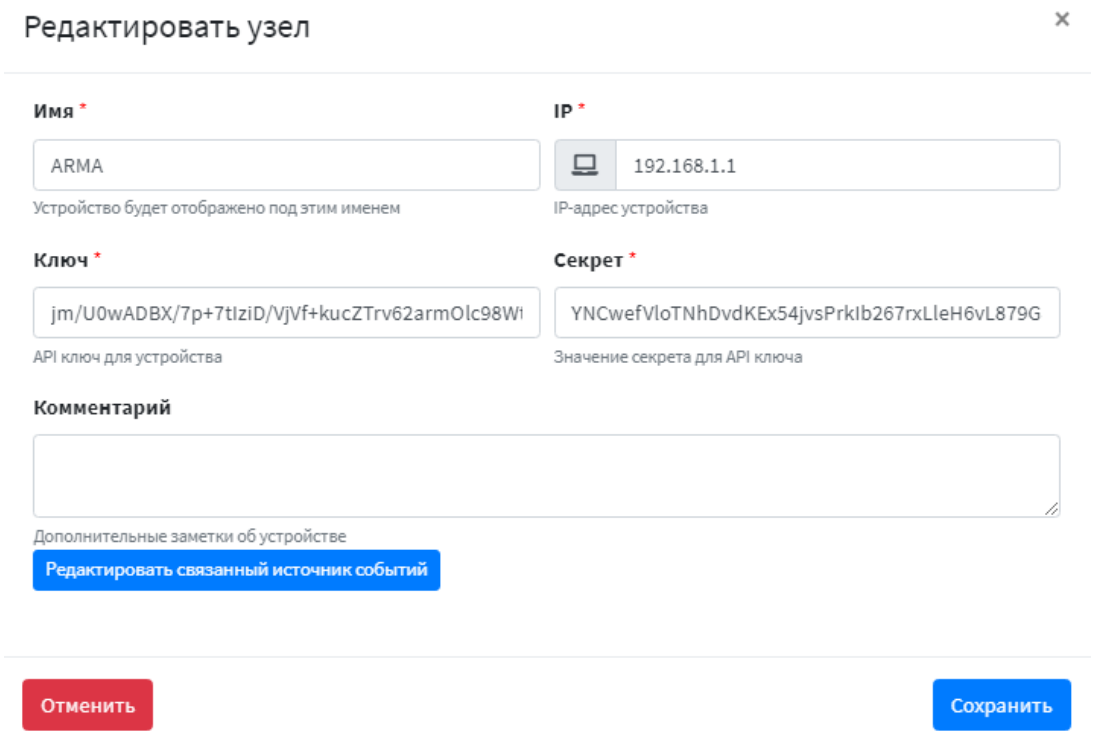


Рисунок 81 – Окно редактирования системы защиты

Для сохранения изменения информации о системе защиты необходимо нажать на кнопку Сохранить. Для отмены изменений необходимо нажать на кнопку Отменить.

6.5 Работа с конфигурациями систем защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять системами защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

6.5.1 Скачивание конфигурации системы защиты

Для скачивания конфигурации системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать на кнопку напротив системы защиты. При успешном скачивании файла конфигурации появится всплывающее уведомление об этом.

6.5.2 Загрузка конфигурации на систему/системы защиты

Для загрузки файла конфигурации системы защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо выбрать системы защиты (для выбора всех систем защиты необходимо нажать на кнопку «Выделить все») и нажать на кнопку вверху таблицы. После нажатия на кнопку необходимо выбрать файл конфигурации. При успешной загрузке

конфигурации на систему/системы защиты в верхнем правом углу появится уведомление об этом.

6.6 Работа с правилами СОВ систем защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять системами защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

6.6.1 Скачивание правил СОВ системы защиты

Для скачивания привил СОВ системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать на кнопку  напротив соответствующей системы защиты. При успешном скачивании файла правил СОВ появится всплывающее уведомление об этом.

6.6.2 Загрузка правил СОВ на систему/системы защиты

Для загрузки файла правил СОВ системы защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо выбрать соответствующие системы защиты (для выбора всех систем защиты необходимо нажать на кнопку «Выделить все») и нажать на кнопку  вверху таблицы. После нажатия на кнопку  необходимо выбрать файл правил СОВ. При успешной загрузке правил СОВ на систему/системы защиты в верхнем правом углу появится уведомление об этом.

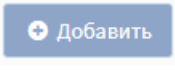
6.7 Добавление ARMA Industrial Firewall

Для успешной обработки событий от ARMA Industrial Firewall в ARMA Management Console необходимо чтобы дата и время были точно синхронизированы между устройствами.

Для подключения ARMA Industrial Firewall к ARMA Management Console необходимо выполнить следующие шаги:

1. В ARMA Industrial Firewall создать пользователя с правами администратора и с ключом API.
2. В ARMA Management Console добавить устройство защиты.
3. В ARMA Industrial Firewall настроить экспорт событий по Syslog.

6.7.1 Создание пользователя

В ARMA Industrial Firewall перейти в раздел доступа к системе («Система» - «Доступ» - «Пользователи») и нажать на кнопку 

.

В поле «Имя пользователя» необходимо ввести имя «arma». В поле «Пароль» необходимо задать пароль и подтвердить его. В пункте «Участники группы» выбрать группу «admins» и, нажав на стрелочку «вправо», добавить группу для создаваемого пользователя и нажать на «Сохранить». После сохранения данных страница с настройками обновится и появится возможность добавления ключа API.

Для создания ключа необходимо в пункте «Ключ API» нажать на +, после чего будет скачан файл в формате apikey.txt.

6.7.2 Добавление устройства защиты

В ARMA Management Console необходимо перейти на страницу «Активы» - «Системы защиты», нажать на кнопку Добавить устройство, заполнить поля согласно рисунку (Рисунок 82) и нажать на кнопку Добавить.

Примечание – в поле «Порт» необходимо указать любой произвольный, но свободный порт, начиная с 1500.

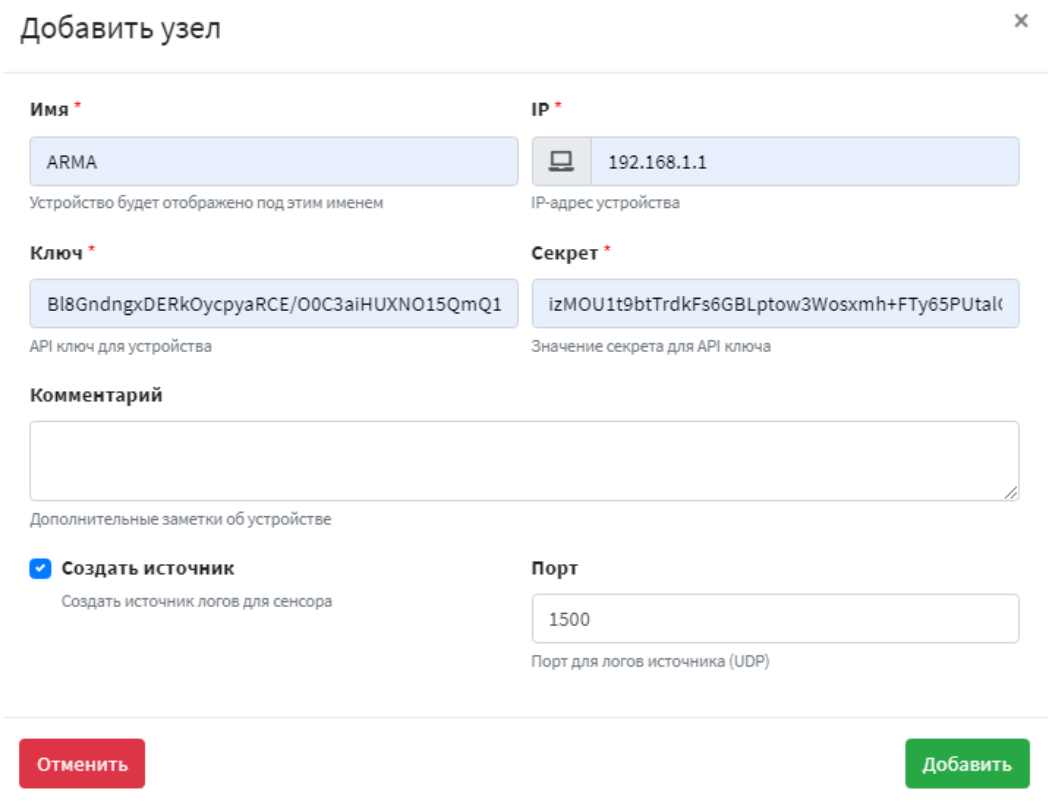


Рисунок 82 – Добавление нового устройства

Устройство добавлено и отображается в списке систем защиты (Рисунок 83).

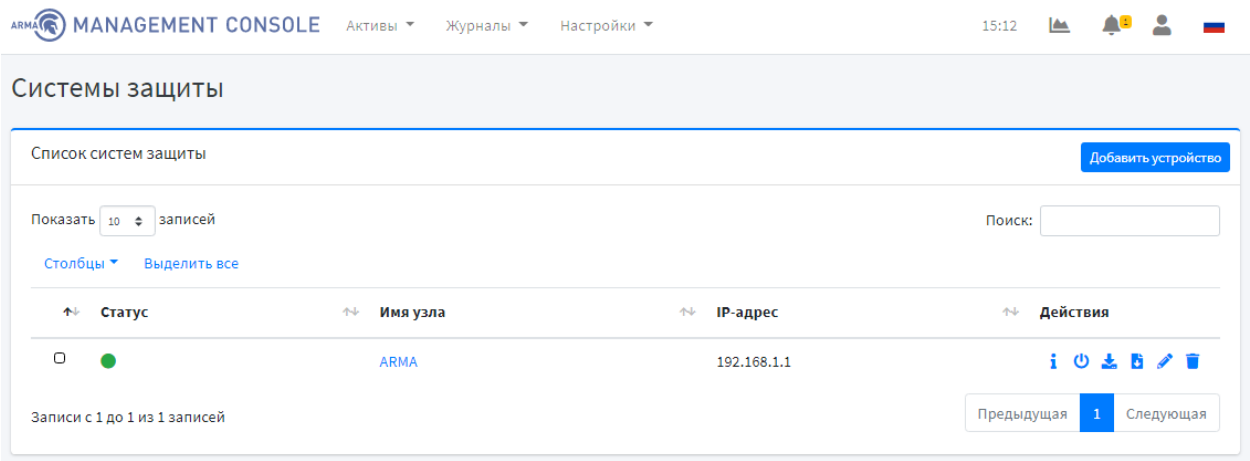


Рисунок 83 – Список систем защиты

6.7.3 Настройка экспорта событий по Syslog

В ARMA Industrial Firewall перейти в раздел настройки экспорта событий по Syslog («Система» - «Настройки» - «Экспорт событий»), нажать на +, заполнить поля согласно рисунку (Рисунок 84), нажать на Сохранить, а затем на кнопку Применить.

Примечание – в поле «Имя хоста» необходимо прописывать заданный адрес ARMA Management Console.

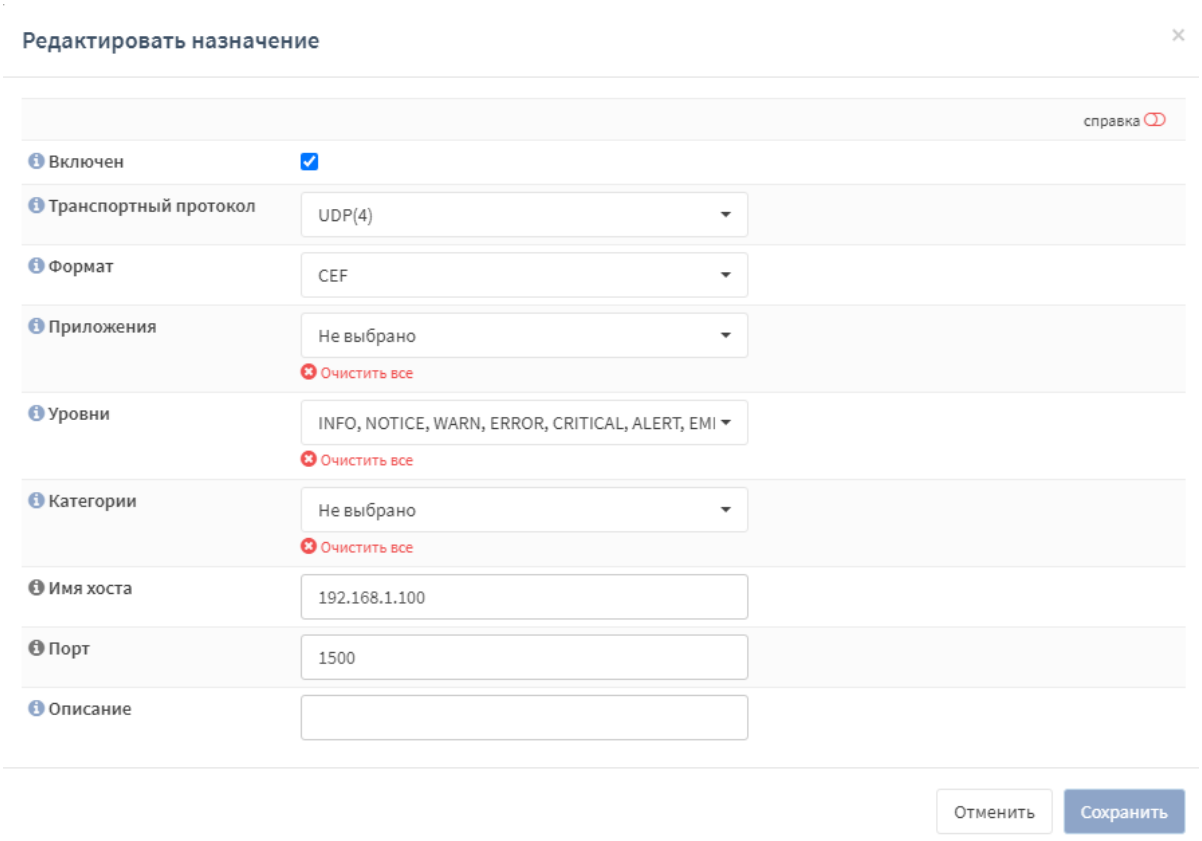


Рисунок 84 – Настройка экспорта событий по Syslog

6.7.4 Настройка обнаружения устройств

В ARMA Industrial Firewall перейти в раздел настроек сети («Сеть» - «Обнаружение устройств» - «Общие настройки»), включить сервис ARPwatch, выбрать прослушиваемые интерфейсы и нажать на кнопку Сохранить (Рисунок 85).

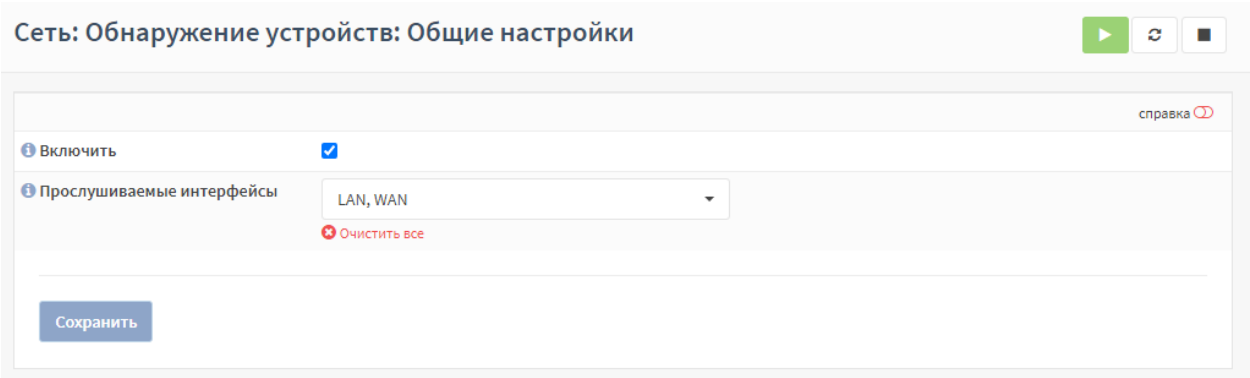


Рисунок 85 – Настройка обнаружения устройств

7 УПРАВЛЕНИЕ ENDPOINT

Текущий раздел доступен пользователям с правом доступа «Может просматривать список Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для просмотра систем защиты необходимо перейти на страницу «Активы» - «Endpoint» (Рисунок 86).

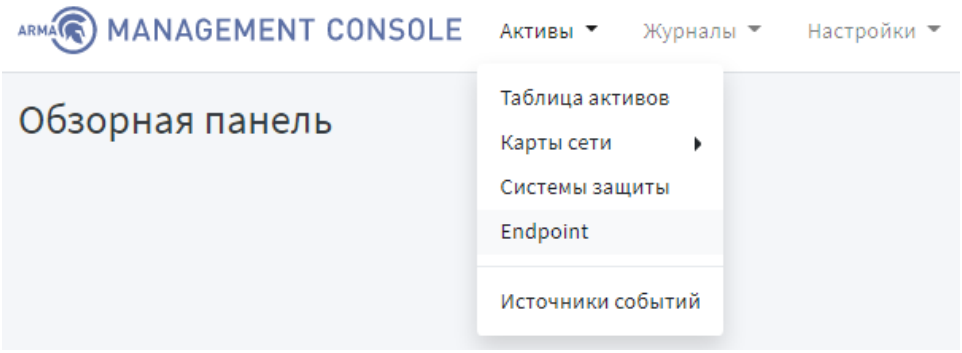


Рисунок 86 – Переход на страницу Endpoint

7.1 Описание таблицы Endpoint

Страница «Endpoint» позволяет просматривать Endpoint в формате таблицы, которая содержит следующие данные (Рисунок 87):

- статус;
- имя;
- дата и время обновления;
- действия:
  -
  - : скачивание конфигурации Endpoint;
  -
  - : редактирование Endpoint;
  - : удаление Endpoint из списка.

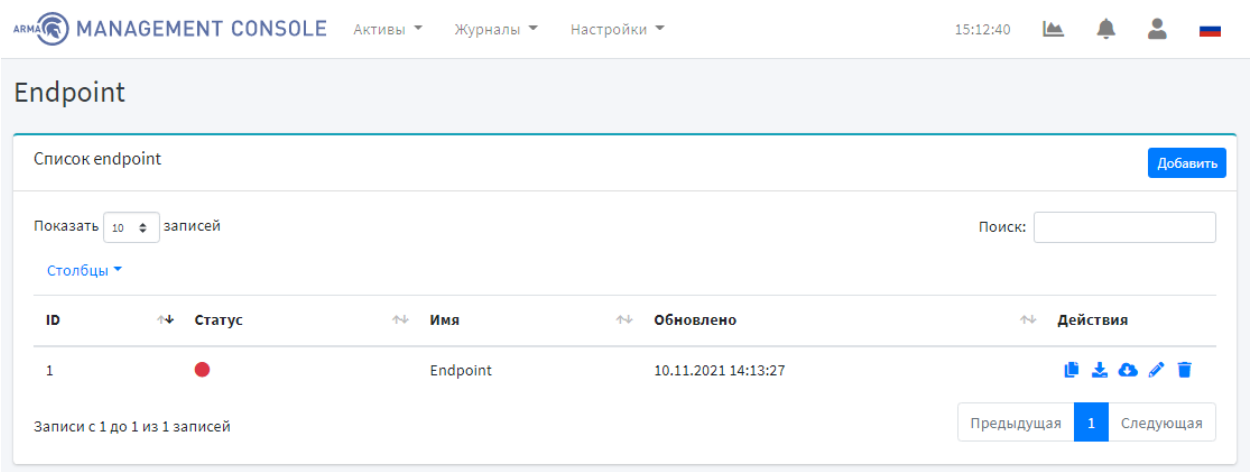


Рисунок 87 – Endpoint

Для выбора количества записей, отображаемых в таблице Endpoint на странице «Активы» - «Endpoint» необходимо нажать на кнопку 10 в левом в верхнем углу страницы.

Поле «Поиск» вверху таблицы позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

Для изменения столбцов, отображаемых в таблице, необходимо нажать на кнопку Столбцы .

В столбце «Статус» отображается статус добавленных Endpoint, такие как:

– : в сети – Endpoint включен и доступен;

– : не в сети – Endpoint не доступен;

– : ошибка – произошла ошибка при подключении к Endpoint. При нажатии на текущий статус во всплывающем окне будет отображена подробная информация об ошибке (Рисунок 151).

7.2 Добавление Endpoint

Текущий подраздел доступен только для пользователя с правом «Может просматривать Endpoint» и «Может добавлять Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для добавления Endpoint необходимо перейти на страницу «Активы» - «Endpoint» и нажать на кнопку Добавить (Рисунок 88).

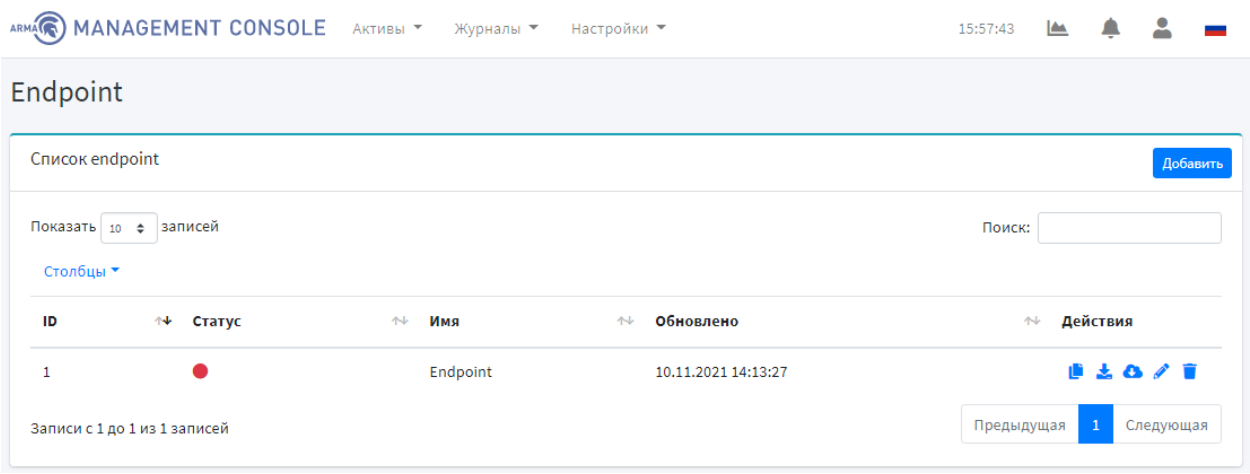


Рисунок 88 – Страница Endpoint

В поле «Имя» необходимо задать имя Endpoint. В поле «Описание» необходимо добавить описание Endpoint. Для создания источника события для Endpoint необходимо поставить галочку в поле «Создать источник». В поле «Порт» необходимо указать порт для входящих логов. В поле «IP» необходимо ввести IP-адрес или домен устройства (Рисунок 89).

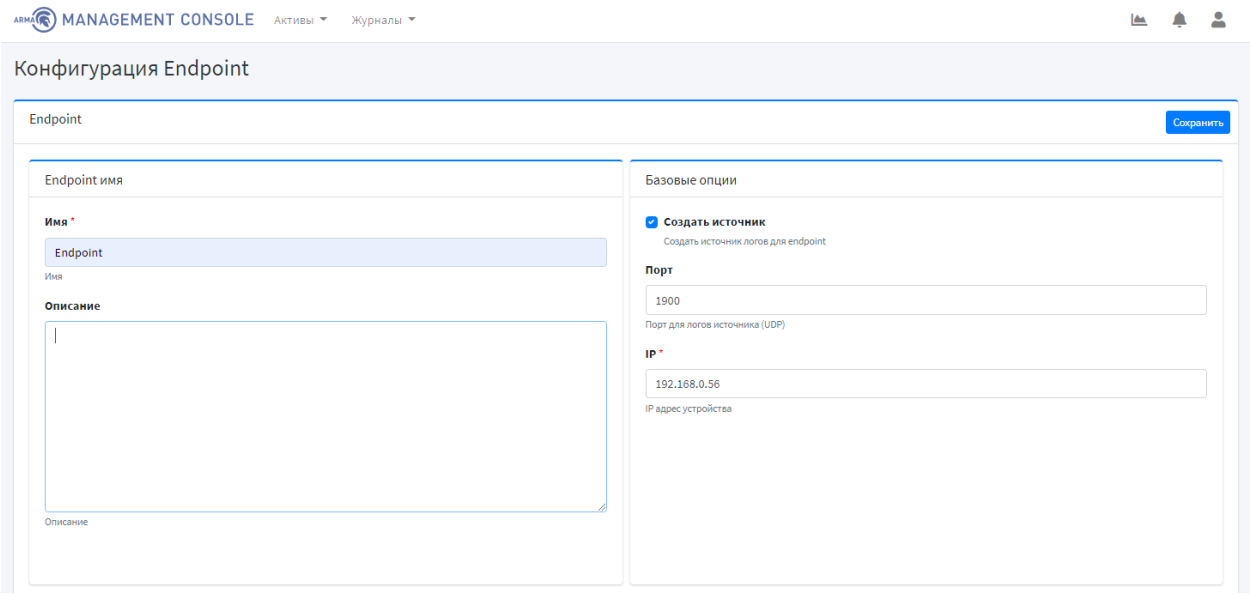


Рисунок 89 – Добавление Endpoint

В блоке «Директории сканирования при запуске» необходимо добавить путь к файлу или папке, который будет сканироваться. Для включения контроля целостности необходимо установить галочку в соответствующем поле «Включить контроль целостности». В поле «Период буферизации событий» необходимо задать частоту периодического сканирования директории (Рисунок 90).

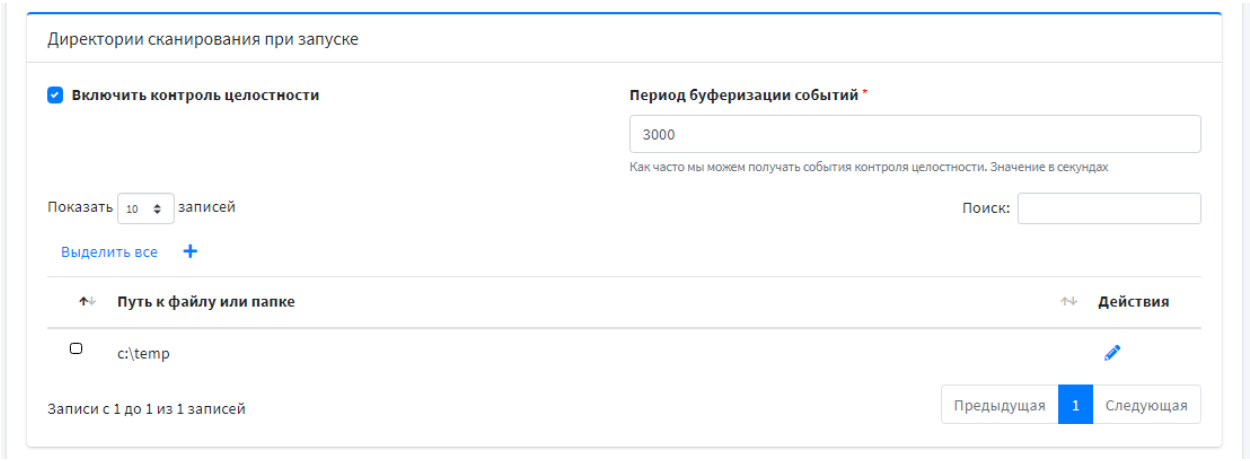


Рисунок 90 – Добавление Endpoint. Директории сканирования при запуске

В блоке «Белый список приложений» необходимо указать путь к файлу или папке, доступ к которому будет разрешен. По умолчанию заданы пути, указанные на рисунке ниже (Рисунок 91). Для включения белого списка необходимо установить галочку в соответствующем поле «Включить белый список». При необходимости разрешения локальному администратору игнорировать белый список необходимо установить галочку в поле «Локальный администратор игнорирует белый список» (Рисунок 91).

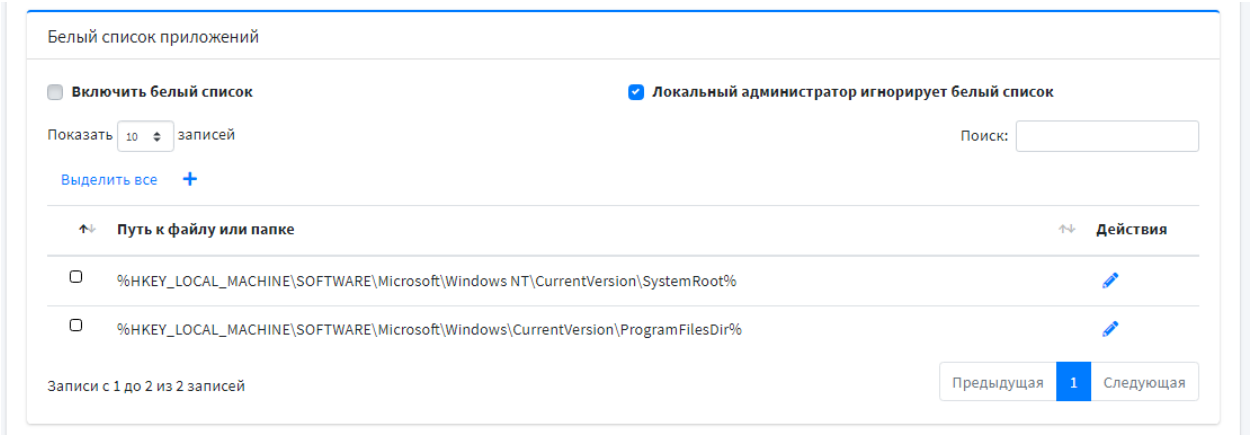


Рисунок 91 – Добавление Endpoint. Белый список приложений

Блок «Настройки управления устройствами» позволяет управлять контролем устройств (Рисунок 92). Для включения контроля устройств и USB устройств необходимо установить галочки в соответствующих полях «Включить управление устройствами» и «Блокировка USB устройств». Для запрета чтения и записи CD/DVD необходимо установить галочку в поле «Запрет доступа на чтение CD/DVD».

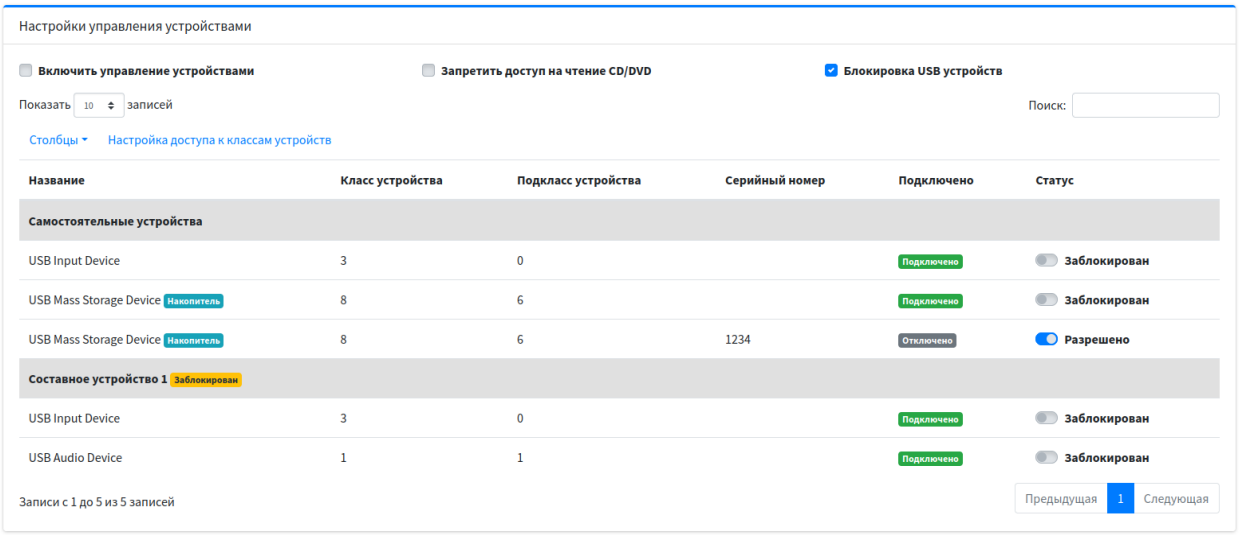


Рисунок 92 – Добавление Endpoint. Настройка управления устройствами

Нажав на кнопку «Настройка доступа к классам устройств» можно настроить доступ к классам/подклассам USB-устройств (Рисунок 93).

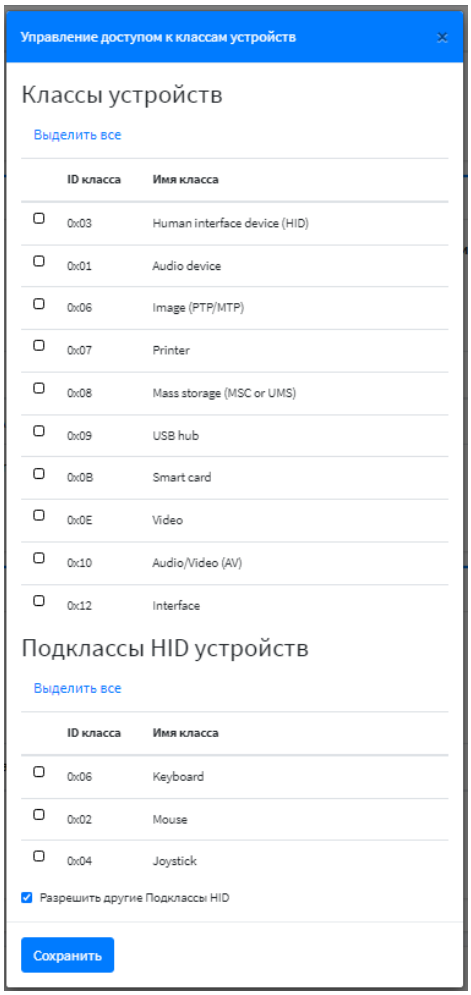


Рисунок 93 – Управление доступом к классам устройств

Установленный флажок в поле «Разрешить другие Подклассы HID» позволяет настраивать дополнительные классы/подклассы для HID устройств.

7.3 Редактирование Endpoint

Текущий подраздел доступен пользователям с правом доступа «Может редактировать Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для редактирования Endpoint необходимо перейти на страницу «Активы» - «Endpoint» и нажать на кнопку напротив Endpoint.

7.4 Копирование конфигурации Endpoint

Текущий подраздел доступен пользователям с правом доступа «Может добавлять Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для копирования Endpoint необходимо перейти на страницу «Активы» - «Endpoint» и нажать на кнопку напротив Endpoint.

Результатом копирования конфигурации Endpoint будет появление в общем списке конфигурации Endpoint с пометкой «копия» (Рисунок 94), а также в списке источников событий («Активы» - «Источники событий»).

Примечание – при копировании конфигурации Endpoint порт нового источника событий будет отличаться от исходного на +1.

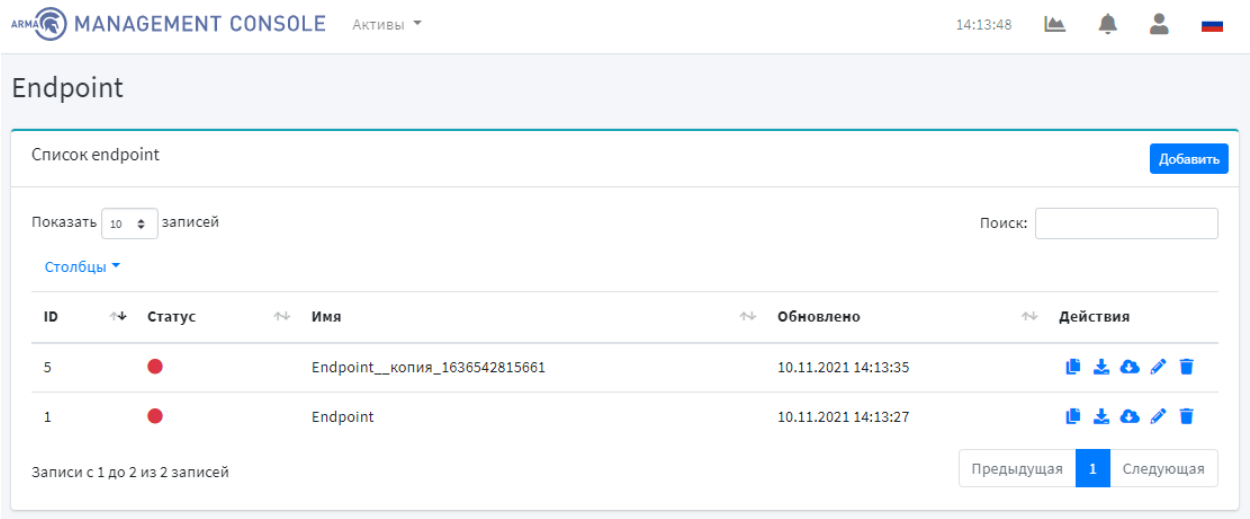


Рисунок 94 – Копирование конфигурации Endpoint

7.5 Скачивание конфигурации Endpoint

Текущий подраздел доступен пользователям с правом доступа «Может скачивать конфигурацию Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для скачивания конфигурации Endpoint необходимо перейти на страницу «Активы» - «Endpoint» и нажать на кнопку напротив Endpoint. При успешном скачивании файла конфигурации появится всплывающее уведомление об этом.

7.6 Обновление конфигурации с Endpoint

Текущий подраздел доступен пользователям с правом доступа «Может просматривать список Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для обновления конфигурации с Endpoint необходимо перейти на страницу «Активы» - «Endpoint» и нажать на кнопку  напротив Endpoint.

7.7 Удаление Endpoint

Текущий подраздел доступен пользователям с правом доступа «Может удалять Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для скачивания конфигурации Endpoint необходимо перейти на страницу «Активы» - «Endpoint», нажать на кнопку  напротив Endpoint и подтвердить удаление, нажав во всплывающем окне кнопку «Да».

8 УПРАВЛЕНИЕ ИСТОЧНИКАМИ СОБЫТИЯ

Текущий раздел позволяет настраивать связи логирования.

Для просмотра списка источников логов необходимо перейти на страницу «Активы» - «Источники событий» (Рисунок 95).

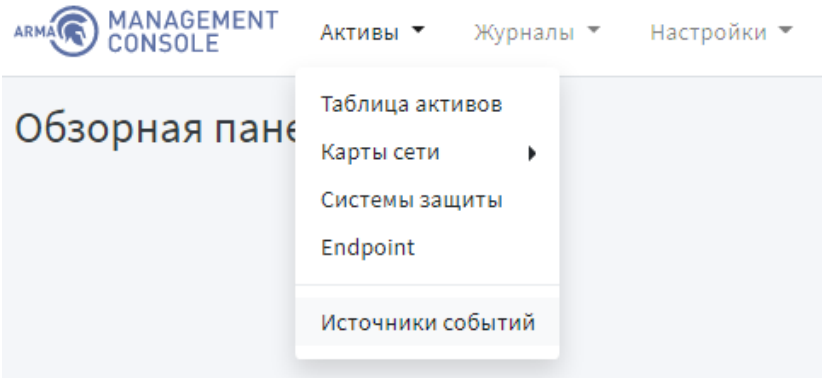


Рисунок 95 – Переход на страницу источников событий

Страница «Источники событий» позволяет просматривать список источников логов в формате таблицы (Рисунок 96).

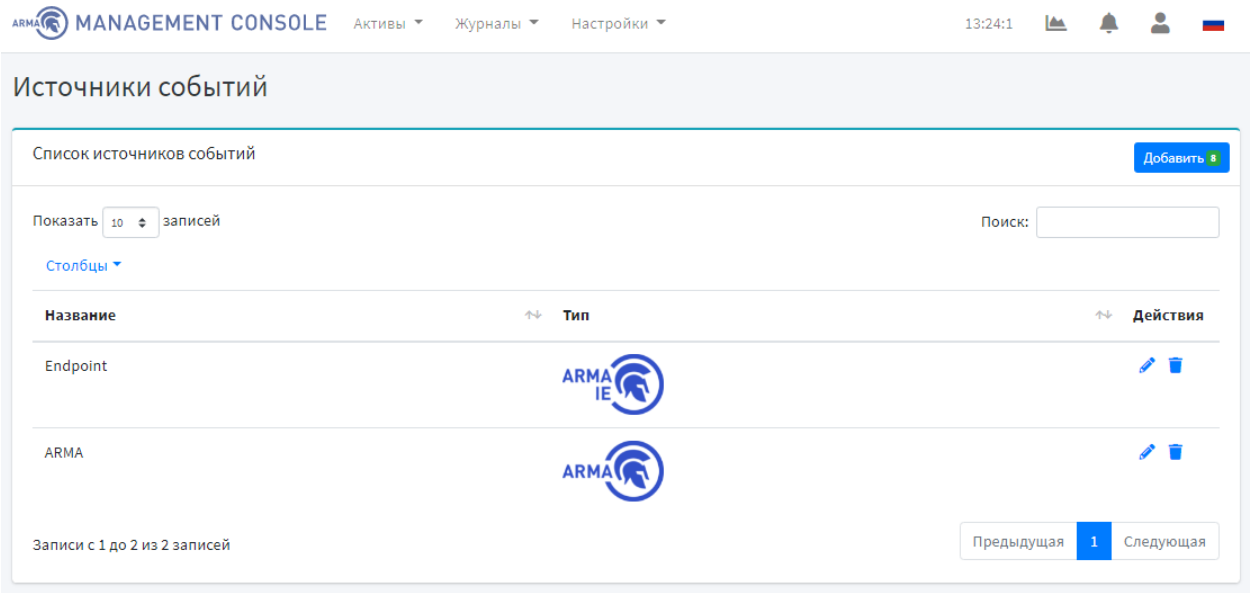


Рисунок 96 – Список источников логов

8.1 Добавление источника события

Для создания источника события необходимо нажать на кнопку Добавить. В поле «Имя» необходимо ввести название источника. В поле «Тип» необходимо выбрать тип источника логов. В поле «Настройка даты и времени» выбрать параметр «локальный» или «без изменений» (Рисунок 97).

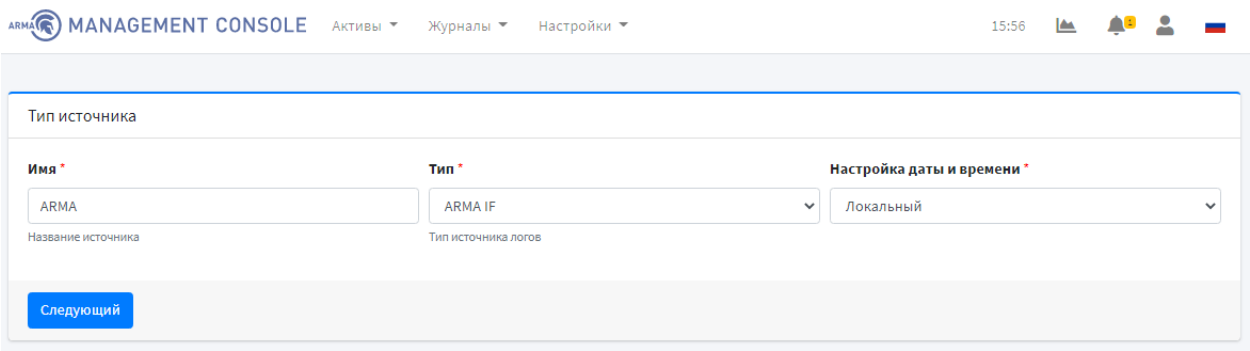


Рисунок 97 – Добавление источника события

Для перехода на второй шаг («Входные данные логов ARMA IF») необходимо нажать на кнопку Следующий, в поле «Порт» указать номер порта источника и затем нажать на кнопку Сохранить (Рисунок 98). Для возврата к предыдущему шагу необходимо нажать на соответствующую кнопку Предыдущий шаг.

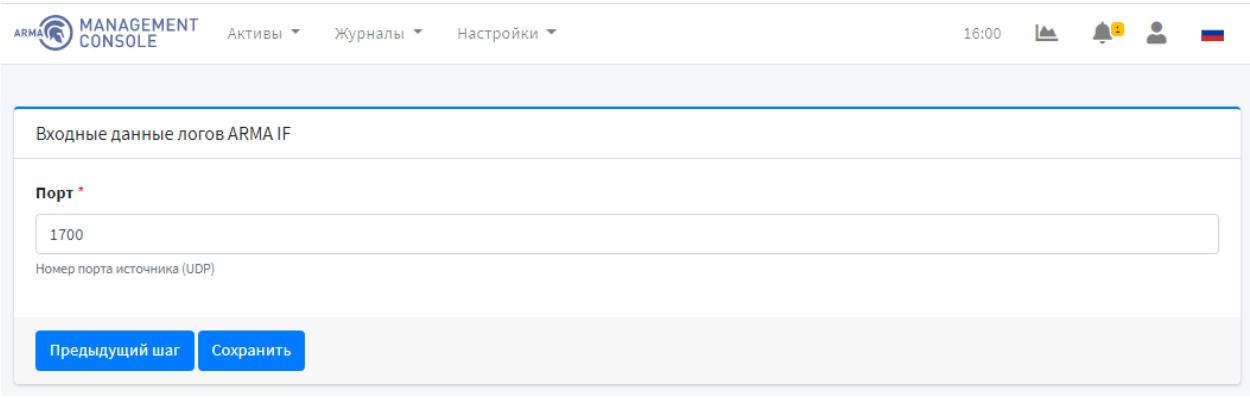


Рисунок 98 – Входные данные логов ARMA IF

9 УПРАВЛЕНИЕ СПИСКОМ УСТРОЙСТВ СЕТИ

Текущий раздел доступен пользователям с правом доступа «Может просматривать активы». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для просмотра устройств сети необходимо перейти на страницу «Активы» - «Таблица активов» (Рисунок 99).

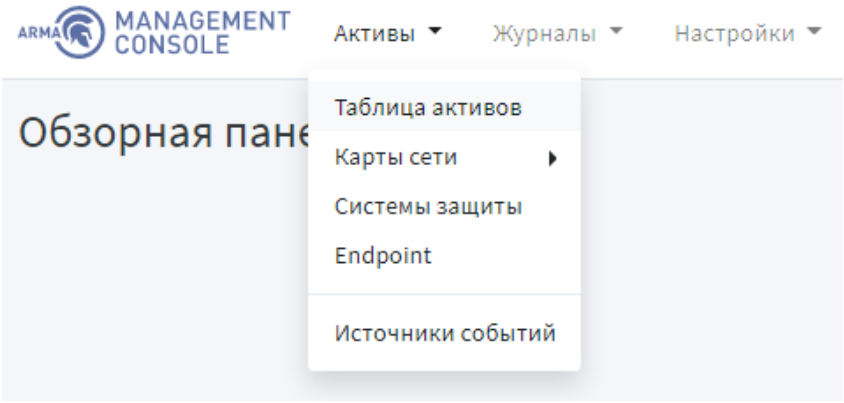


Рисунок 99 – Переход на страницу таблицы активов

9.1 Описание таблицы устройств сети

Страница «Таблица активов» позволяет просматривать активы в формате таблицы, которая содержит следующие данные (Рисунок 100):

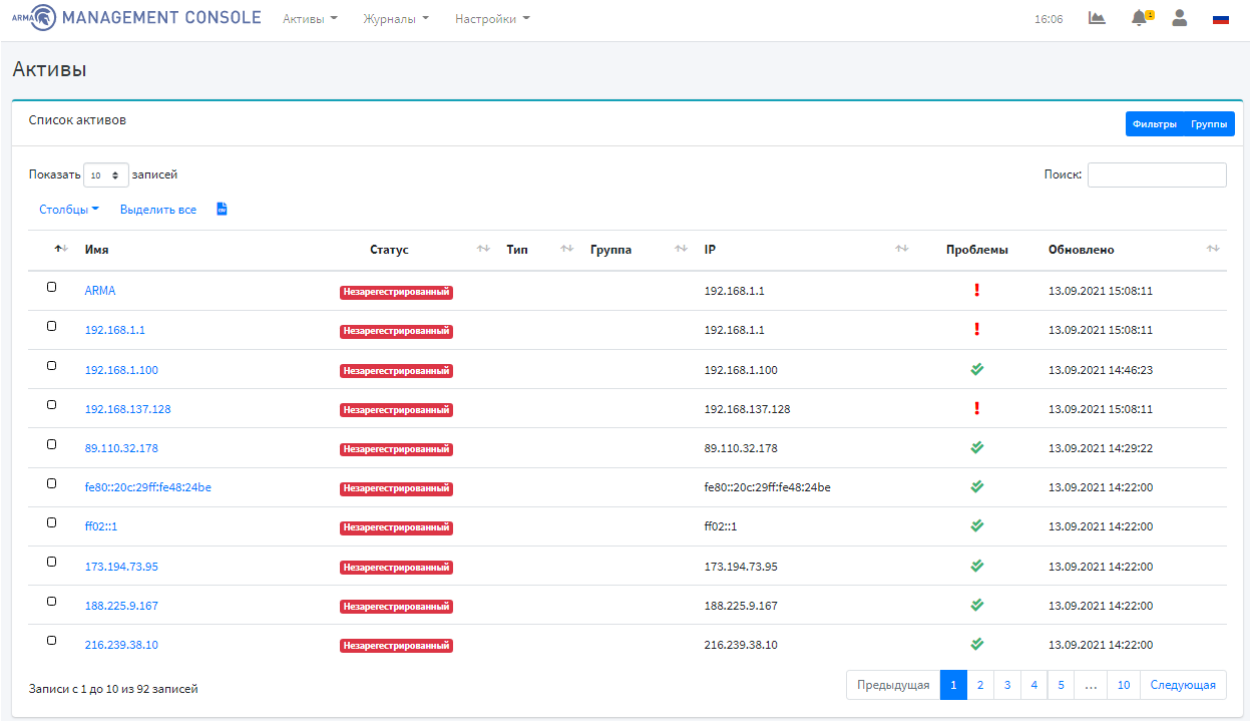


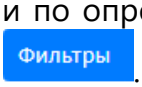
Рисунок 100 – Таблица активов

Для выбора количества записей, отображаемых в таблице на странице «Таблица активов» необходимо нажать на кнопку 

в верхнем левом углу страницы.

9.2 Поиск, сортировка и фильтрация устройств сети

Поле «Поиск» вверху таблицы инцидентов позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Для фильтрации по определенным столбцам таблицы событий необходимо нажать на кнопку 

. Всплывающее окно позволяет задать фильтры отображения таблицы активов (Рисунок 101):

- группа;
- операционная система;
- тип и статус актива;
- время обновления.

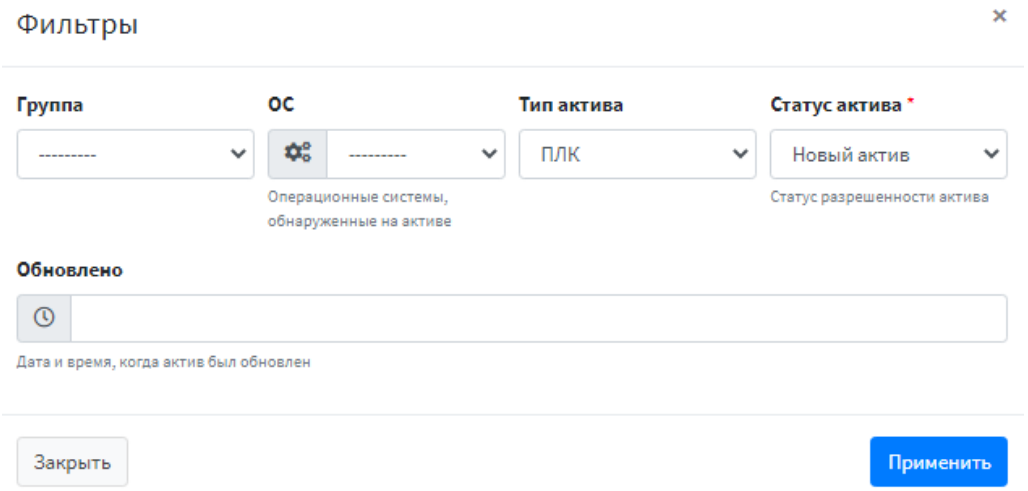


Рисунок 101 – Фильтрация списка активов

В поле «ОС» необходимо выбрать ОС устройства сети или добавить новое, нажав на кнопку  , а затем на кнопку + (Рисунок 102, Рисунок 103).

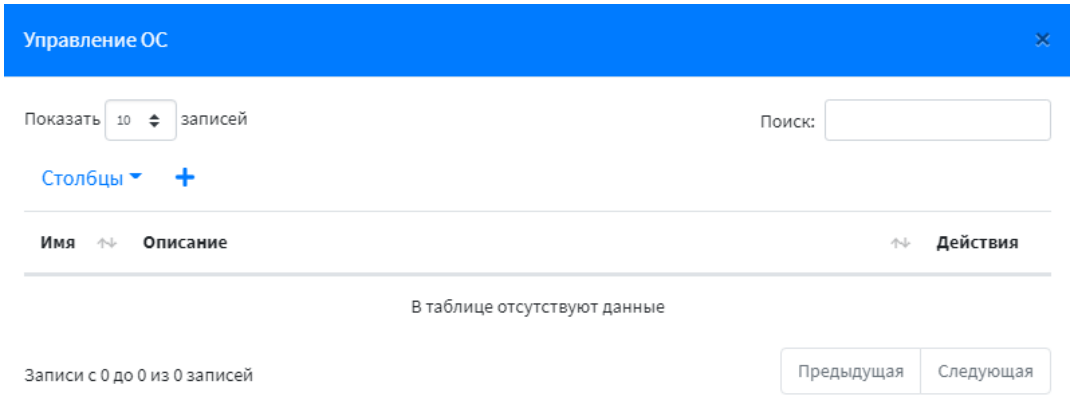


Рисунок 102 – Управление ОС

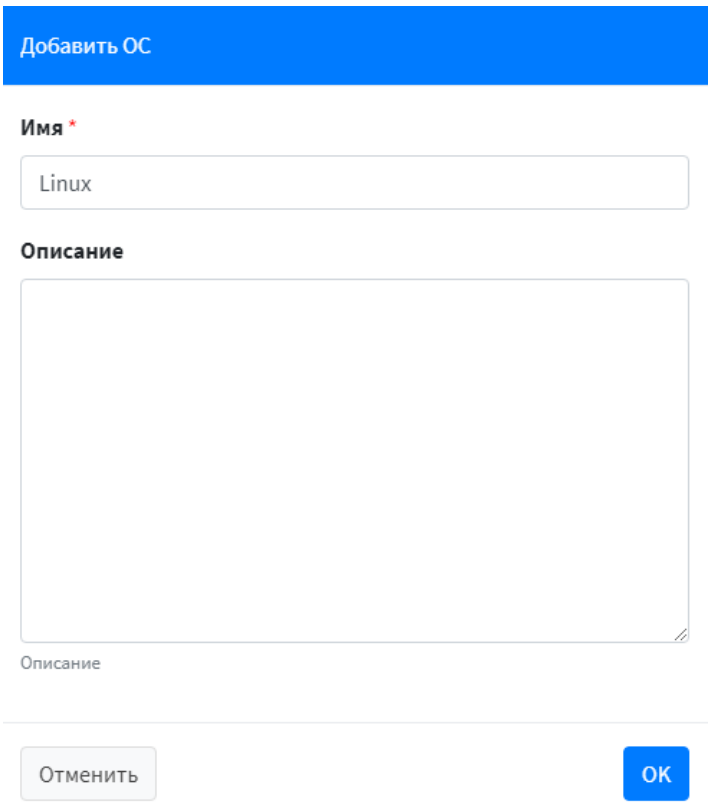


Рисунок 103 – Добавление ОС

Для сохранения и применения фильтров необходимо нажать на кнопку Применить. Для закрытия окна задания фильтра необходимо нажать на кнопку Закрыть.

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку ↑↓ рядом с названием соответствующего столбца.

9.3 Редактирование основной информации об устройстве сети

Для редактирования основной информации об устройстве необходимо перейти на страницу «Активы» - «Таблица активов». В таблице активов необходимо нажать на ссылку названия этого устройства сети в столбце «Имя», например, 192.168.1.1. При нажатии на название устройства сети ARMA Management Console отобразит страницу подробной информации об устройстве, которую можно редактировать (Рисунок 104). Для сохранения изменений необходимо нажать на кнопку Сохранить.

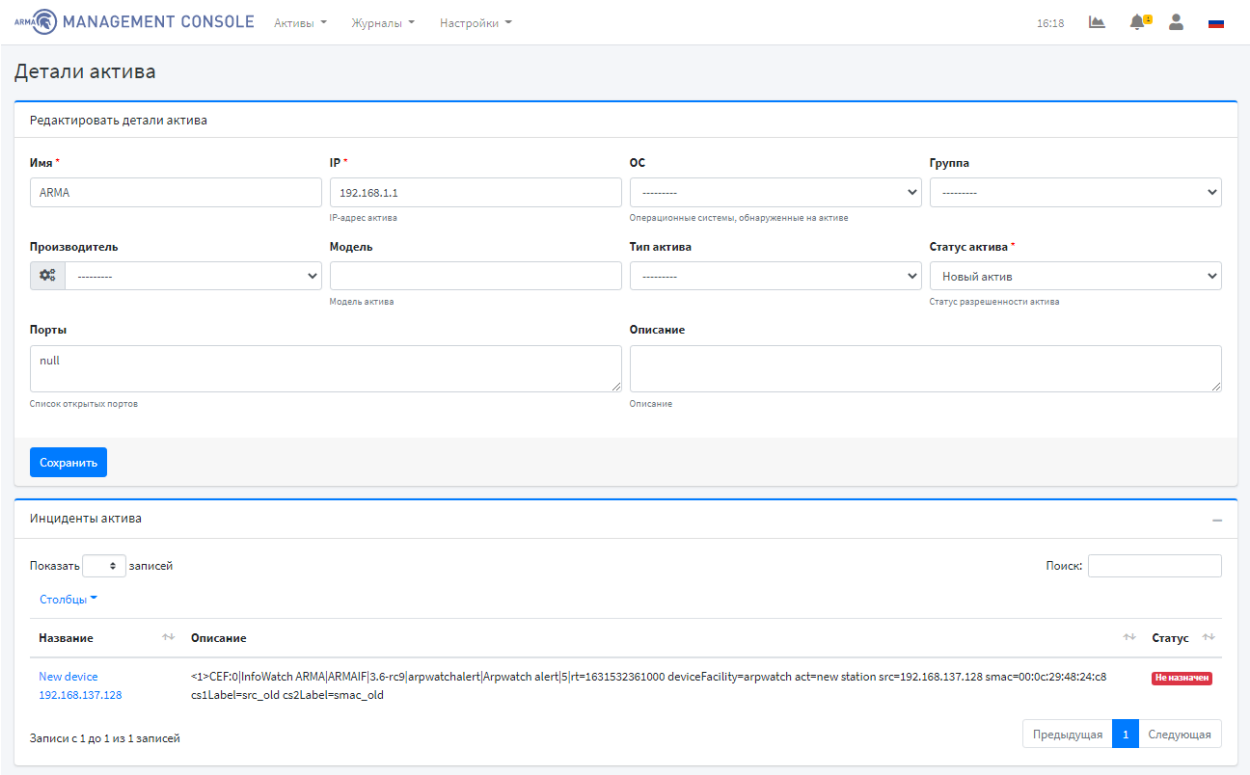


Рисунок 104 – Детали актива

9.4 Добавление группы устройств сети

Текущий подраздел доступен пользователям с правом доступа «Может редактировать группы активов». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для добавления группы систем защиты необходимо перейти на страницу «Активы» - «Таблица активов» и нажать на кнопку Группы. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп (Рисунок 105). Для добавления новой группы необходимо нажать на кнопку Добавить.

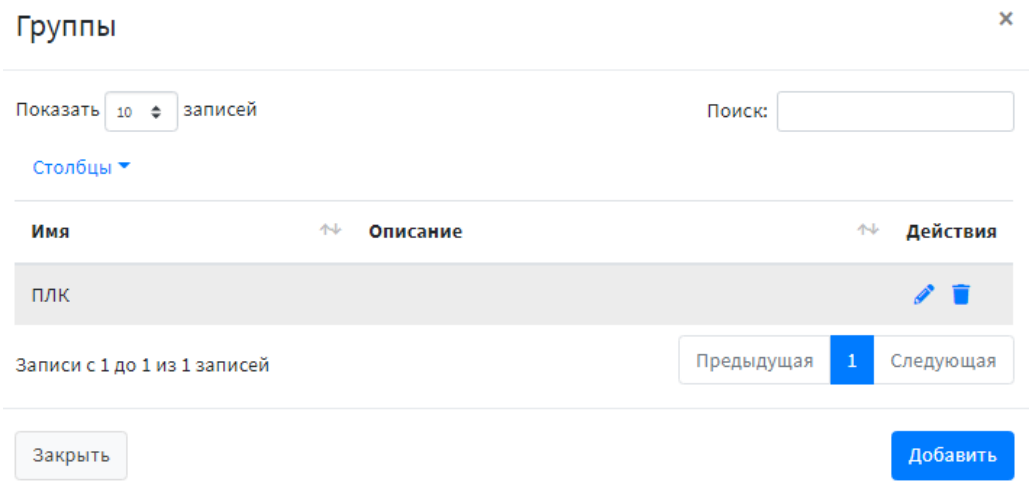


Рисунок 105 – Список групп активов

Окно добавления группы (Рисунок 106) позволяет ввести необходимую информацию для создания новой группы. Для сохранения группы устройств сети необходимо нажать на кнопку Сохранить изменения. Для закрытия окна добавления группы необходимо нажать на кнопку Закрыть. В случае успешного добавления группы появится уведомление об этом (Рисунок 148).

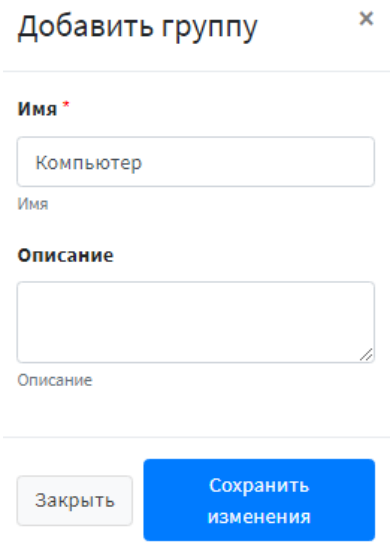


Рисунок 106 – Добавление группы устройств сети

9.5 Удаление группы устройств сети

Текущий подраздел доступен пользователям с правом доступа «Может редактировать группы активов». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для удаления группы необходимо перейти на страницу «Активы» - «Таблица активов» и нажать на кнопку Группы. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп. Для удаления пользовательской группы необходимо нажать на кнопку напротив соответствующей группы и подтвердить удаление во всплывающем окне. В случае успешного удаления группы появится уведомление об этом.

9.6 Редактирование групп

Текущий подраздел доступен пользователям с правом доступа «Может редактировать группы активов». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для редактирования группы необходимо перейти на страницу «Активы» - «Таблица активов» и нажать на кнопку Группы. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и

пользовательских групп. Для редактирования пользовательской группы необходимо нажать на кнопку напротив группы.

Окно редактирования группы (Рисунок 107) позволяет ввести необходимую информацию о группе. Для сохранения группы устройств сети необходимо нажать на кнопку Сохранить изменения. Для закрытия окна редактирования группы необходимо нажать на кнопку Закрыть. В случае успешного добавления группы появится уведомление об этом (Рисунок 149).

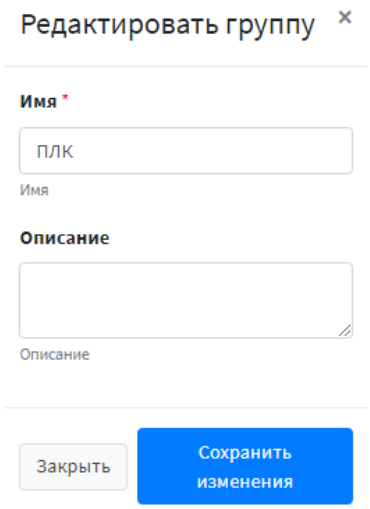


Рисунок 107 – Редактирование группы устройств сети

10 НАСТРОЙКА КАРТЫ СЕТИ

Текущий раздел доступен пользователям с правом доступа «Может просматривать структуру сети». Описание добавления пользователя и назначение прав доступа приведены в разделе 11 настоящего руководства.

Для просмотра устройств сети необходимо перейти на страницу «Активы» - «Карта сети» - «Статическая» (Рисунок 108).

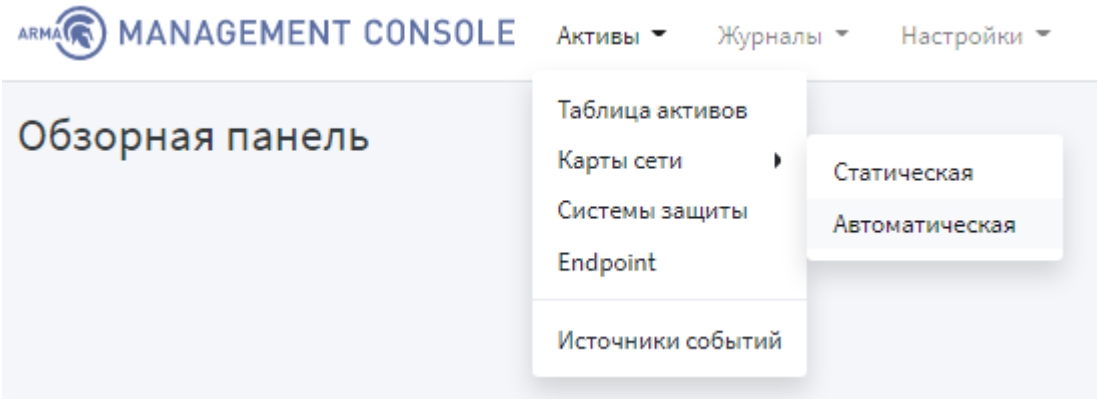


Рисунок 108 – Переход на карту сети

10.1 Описание карты сети

На странице «Активы» - «Карта сети» - «Статическая» отображаются устройства сети и их связи (Рисунок 109) в соответствие с таблицей устройств сети на странице «Активы» - «Таблица активов» (Рисунок 100). Карта сети позволяет:

- просматривать все устройства сети;
- просматривать связи между устройствами сети;
- перемещать устройства сети;
- просматривать подробную информацию об устройстве сети.
- выбирать масштаб отображения карты сети;
- добавлять/удалять связи между устройствами;
- добавлять фоновое изображение для карты сети;
- добавлять карту сети.

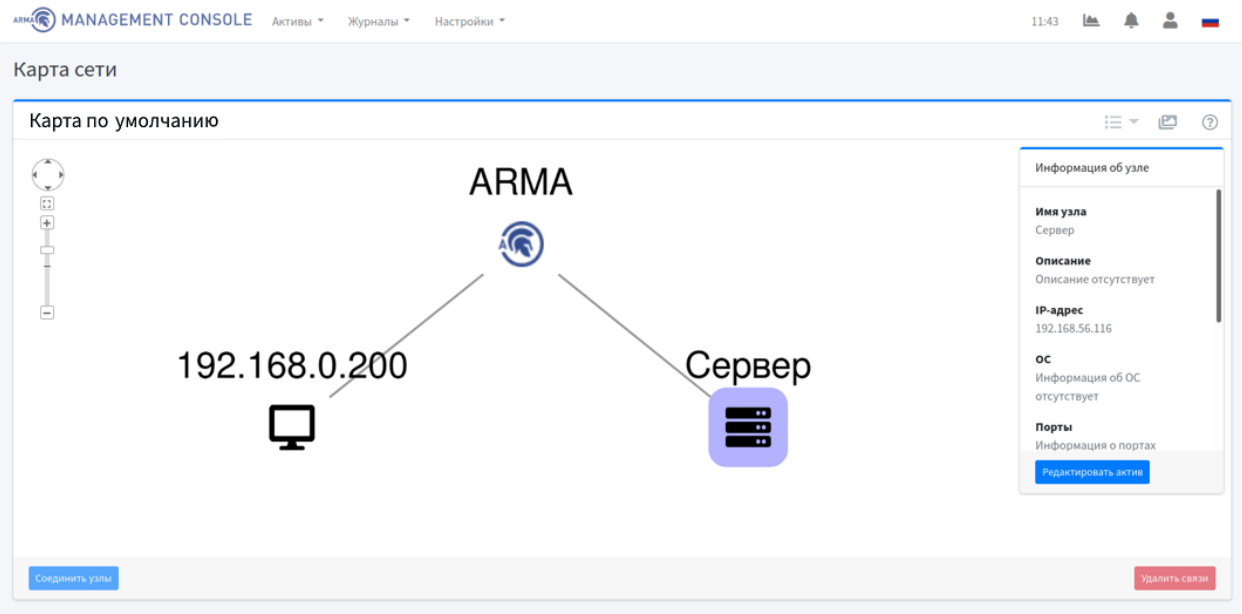


Рисунок 109 – Карта сети

При нажатии на устройство сети открывается окно со следующей информацией:

- название узла;
- описание;
- IP-адрес узла;
- ОС;
- порты;
- обновлено;
- инциденты;
- уязвимости (отображаются только пользователю с правом доступа «Может просматривать уязвимости»).

Выполнение действий на карте сети представлено в инструкции, которую можно открыть, нажав на кнопку (Рисунок 110).

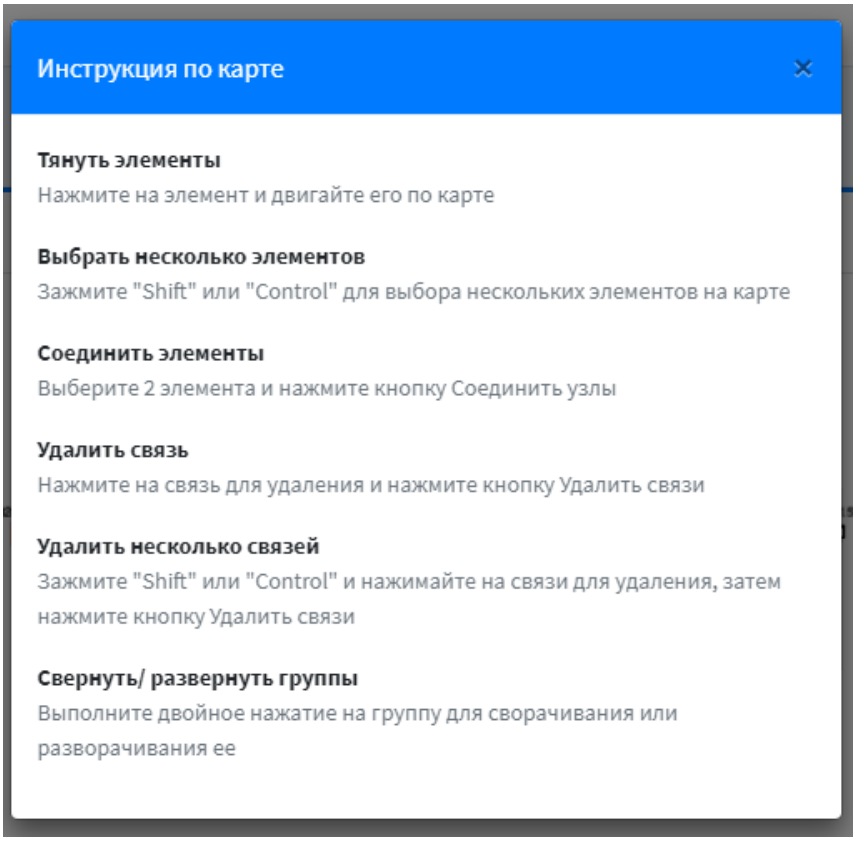


Рисунок 110 – Инструкция по карте сети

Для любой карты сети можно установить фоновое изображение, нажав на кнопку . Во всплывающем окне нажать на кнопку + и добавить фоновое изображение (Рисунок 111, Рисунок 112).

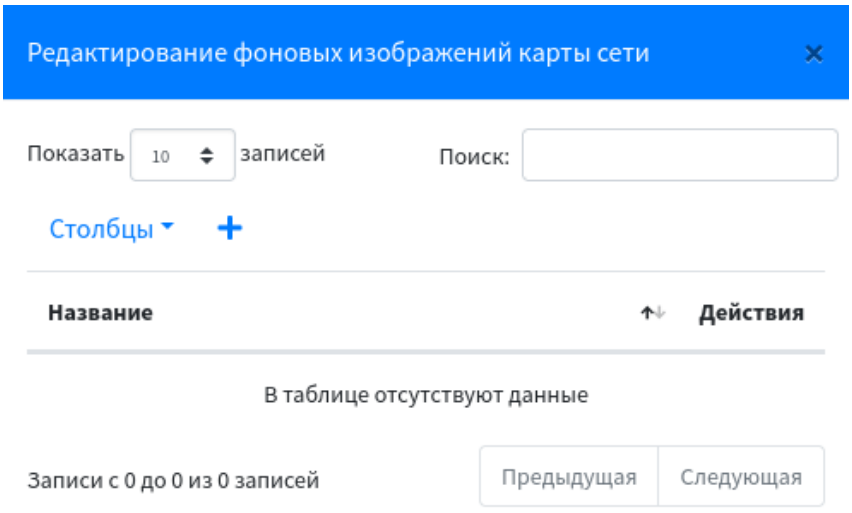


Рисунок 111 – Список фоновых изображений

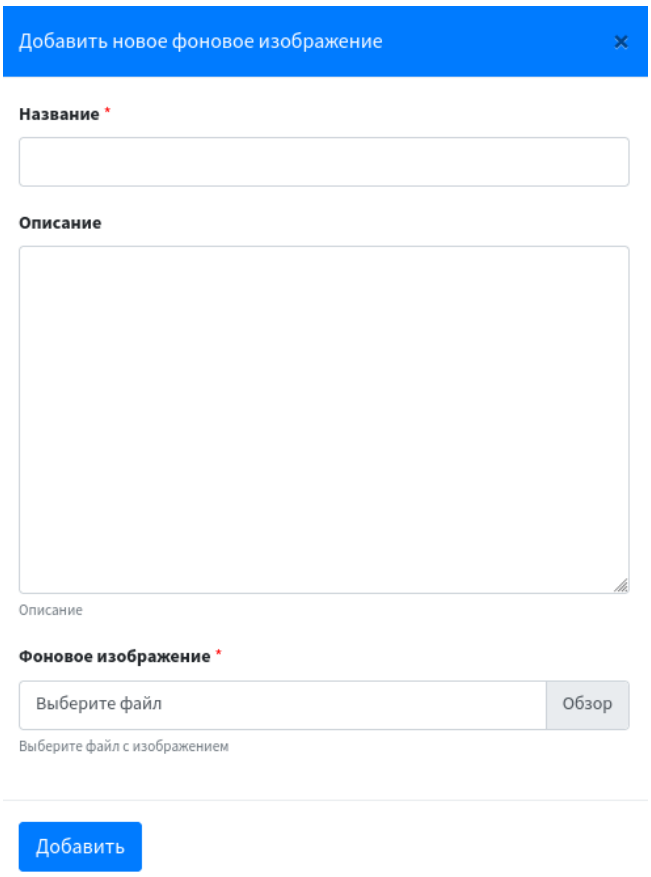


Рисунок 112 – Добавление фонового изображения

Фоновое изображение можно масштабировать и передвигать по карте сети (Рисунок 113).

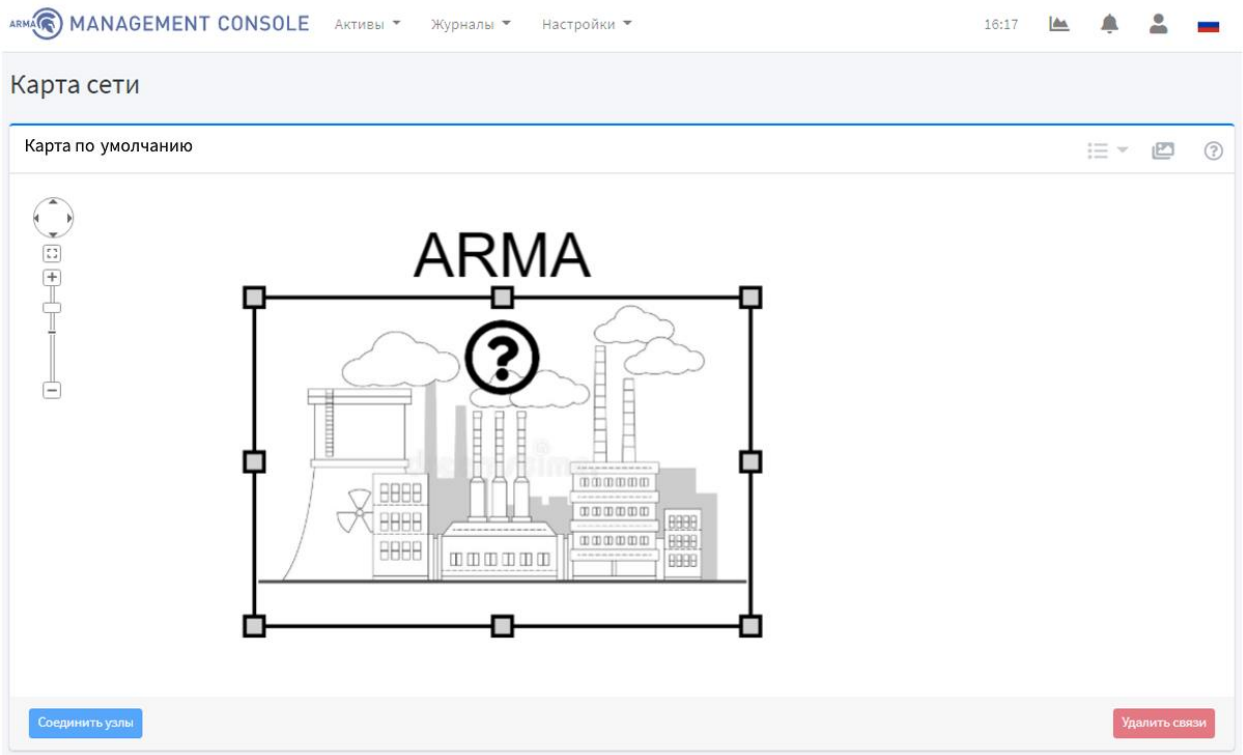


Рисунок 113 – Пример фонового изображения на карте сети

10.1.1 Создание и удаление связей устройств

Для создания связей устройств сети необходимо перейти на страницу «Активы» - «Карта сети», выбрать устройства сети, которые необходимо соединить, и нажать на кнопку Соединить узлы. Появится связь между устройствами.

Для удаления связей между устройствами сети необходимо перейти на страницу «Активы» - «Карта сети», выбрать устройства сети, связь между которыми необходимо удалить, и нажать на кнопку Удалить связи.

10.1.2 Добавление карты сети

Для добавления новой карты сети необходимо нажать на кнопку и в выпадающем списке выбрать пункт «Добавить новую карту». Во всплывающем окне ввести необходимую информацию о новой карте сети и нажать на кнопку Добавить (Рисунок 114).

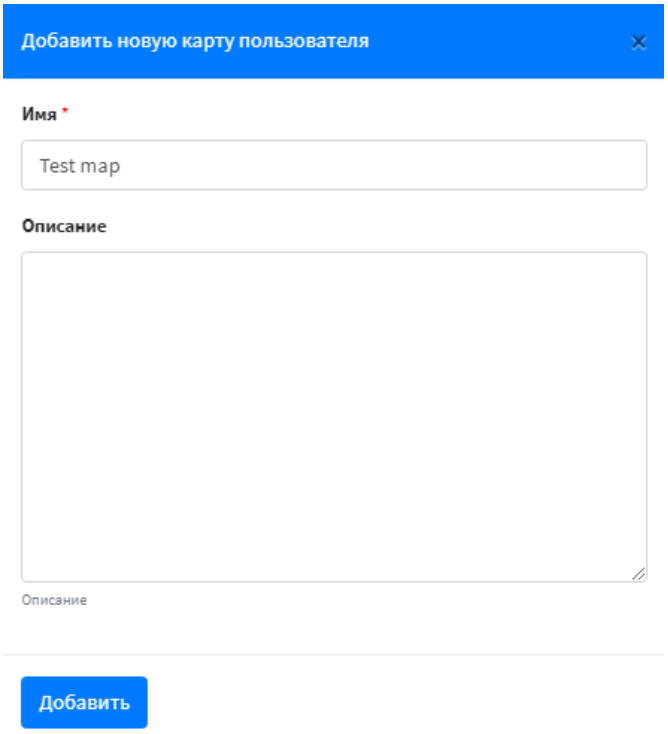


Рисунок 114 – Добавление карты сети

10.2 Описание карты сетевых взаимодействий

На странице «Активы» - «Карта сети» - «Автоматическая» отображается информация о сетевых потоках между узлами сети (Рисунок 115) в соответствие с таблицей устройств сети на странице «Активы» - «Таблица активов» (Рисунок 100).

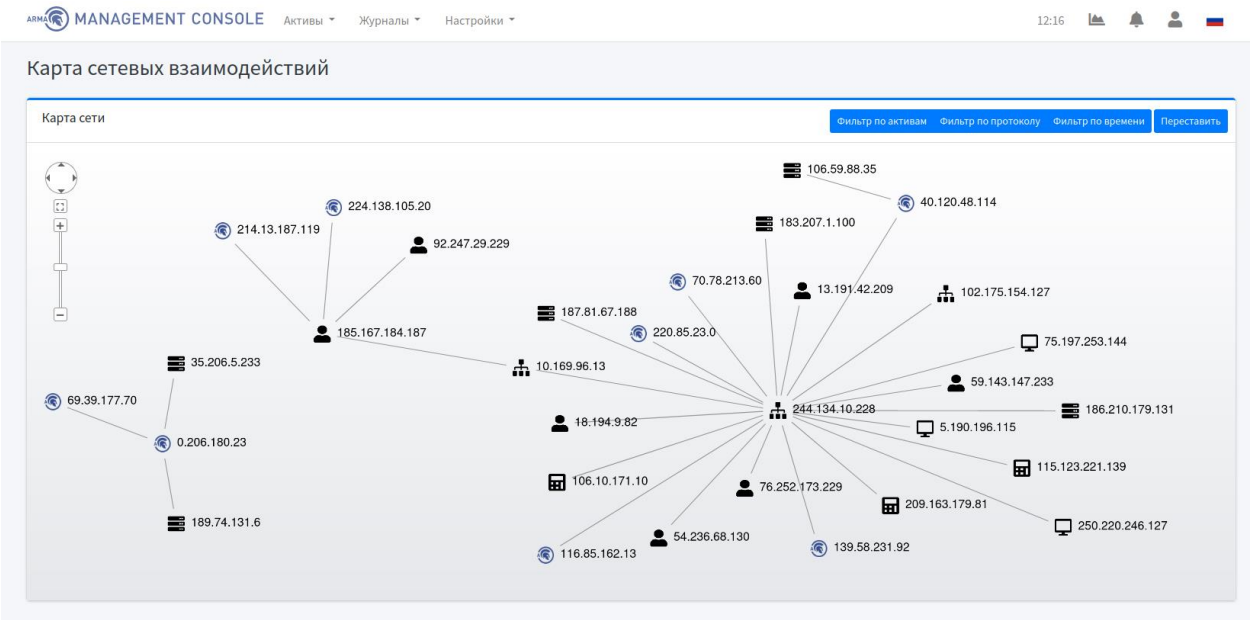


Рисунок 115 – Карта сетевых взаимодействий

Карта сетевых взаимодействий позволяет:

– автоматически формировать карту на основе активов и соединений;

– отображать взаимодействие активов;

– формировать сетевые соединения посредством анализа поступающих событий от устройства;

– фильтровать соединения по времени и типу протокола;

– фильтровать активы;

– отображать «соседей» выбранных активов, то есть показывать активы, с которыми есть связь у выбранных пользователем активов;

– отображать информацию о компонентах сети (активов, соединений);

– переставлять элементы на карте.

10.2.1 Фильтрация соединений по времени и типу протокола

Для фильтрации соединений по времени и типу протокола необходимо нажать на соответствующие кнопки Фильтр по протоколу и Фильтр по времени.

При фильтрации по времени необходимо указать временной диапазон и нажать на кнопку Применить, а затем на кнопку Добавить (Рисунок 116).

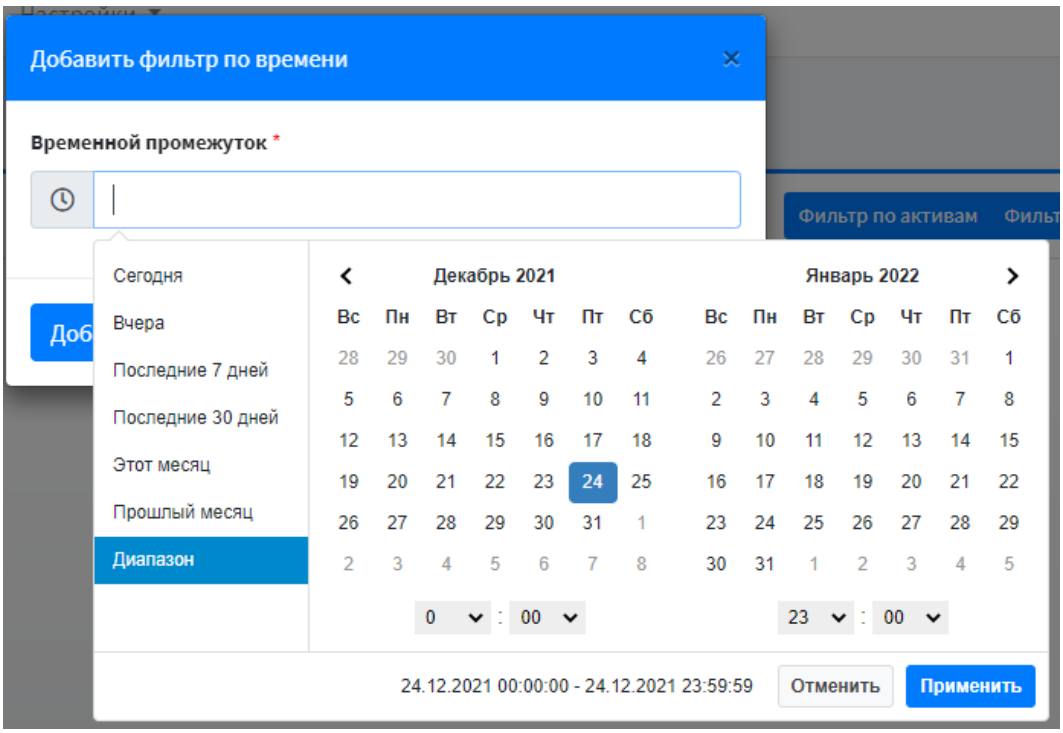


Рисунок 116 – Фильтрация соединений по времени

При фильтрации по типу протокола необходимо выбрать один из протоколов (TCP/UDP) и нажать на кнопку Добавить (Рисунок 117).

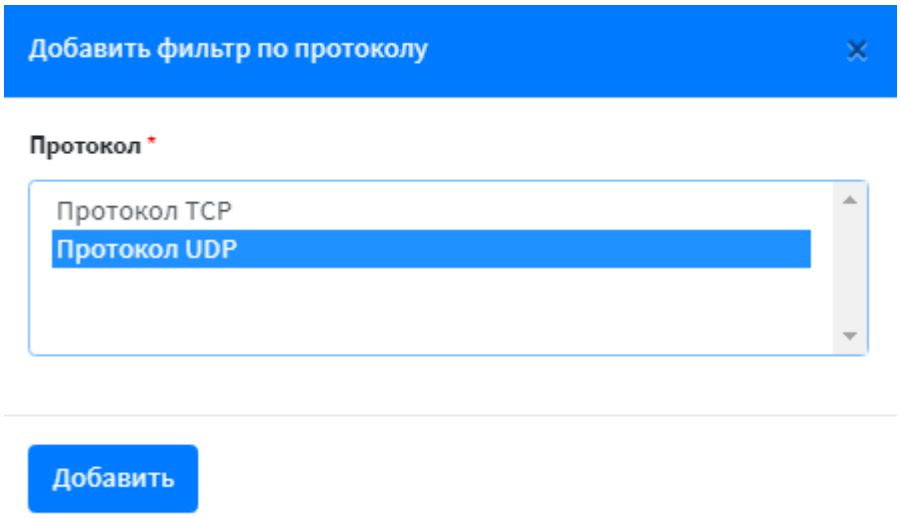


Рисунок 117 – Фильтрация по типу протокола

10.2.2 Фильтрация по активам

Для фильтрации по активам необходимо нажать на кнопку Фильтр по активам. В появившемся окне выбрать необходимые активы и нажать на кнопку Добавить. При необходимости отобразить «соседей» активов необходимо установить флажок в поле «Отображать соседей» (Рисунок 118).

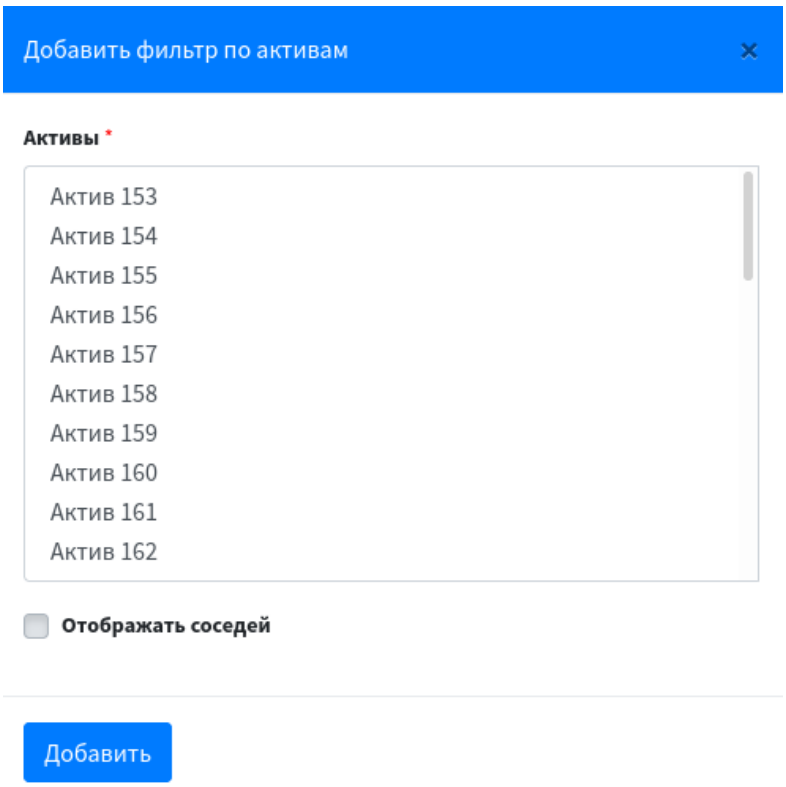


Рисунок 118 – Фильтрация по активам

10.2.3 Перестановка элементов на карте

Для применения различных вариантов расстановки элементов на карте сетевых взаимодействий необходимо нажать на кнопку Переставить.

11 УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ И ПРАВАМИ ДОСТУПА СИСТЕМЫ

11.1 Профиль пользователя

Для перехода на страницу «Профиль пользователя» необходимо нажать на в верхнем меню, а затем выбрать пункт «Профиль пользователя» (Рисунок 119).

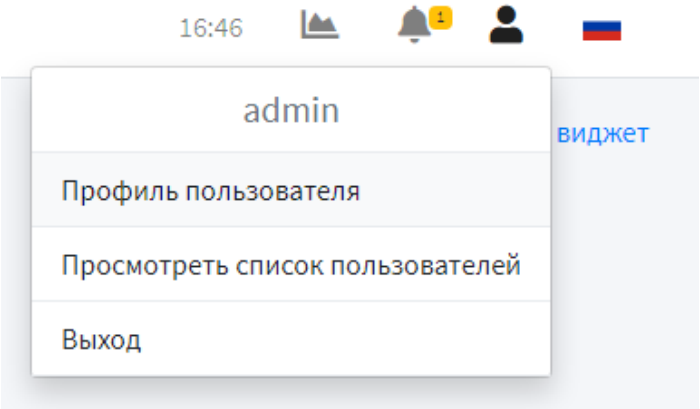


Рисунок 119 – Переход на страницу профиля пользователя

Страница «Профиль пользователя» позволяет просматривать следующие данные о текущем пользователе (Рисунок 120).

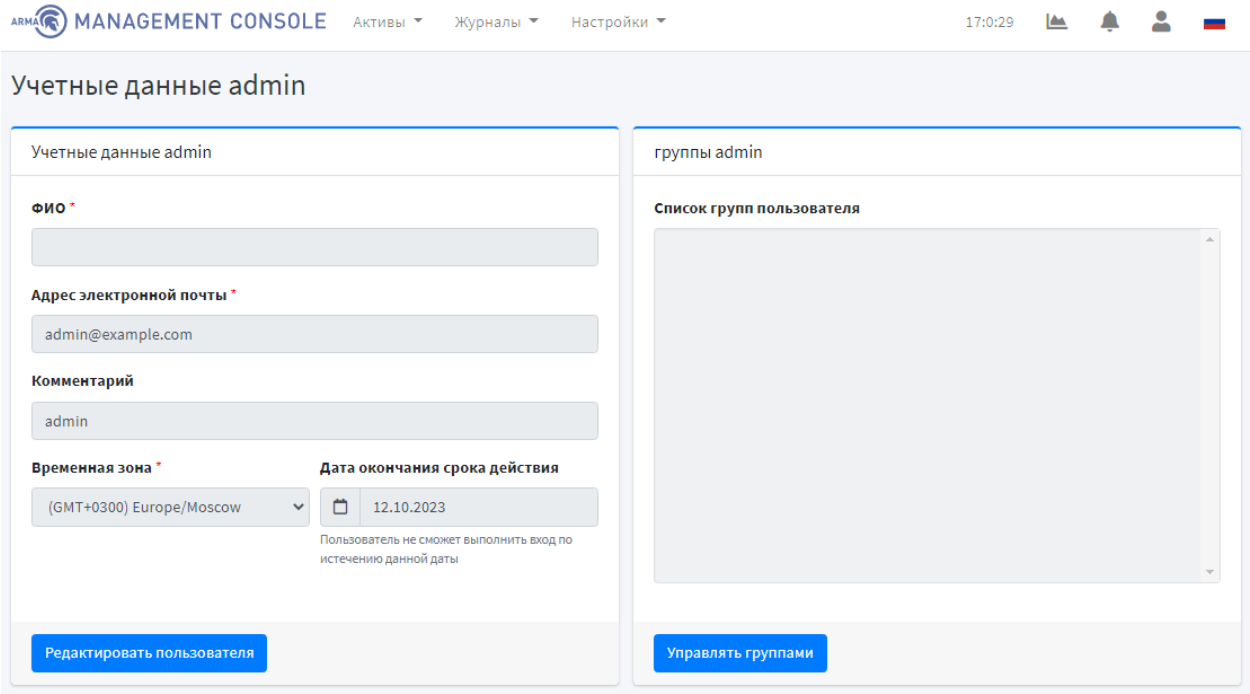


Рисунок 120 – Профиль текущего пользователя (просмотр)

11.2 Список пользователей

Текущий подраздел доступен пользователю с правом доступа «Может просматривать список пользователей». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 11.2.2, п. 11.3).

Для перехода на страницу «Список пользователей» необходимо нажать на в верхнем меню, а затем выбрать пункт «Просмотреть список пользователей» (Рисунок 119).

Страница «Список пользователей» позволяет просматривать список учетных записей пользователей в формате таблицы, которая содержит следующие записи (Рисунок 121):

– имя пользователя (в виде ссылки отображается только пользователю с правом доступа «Может просматривать учетные данные пользователя»);

– имя;

– действия:

– : редактировать;

– : редактировать группы пользователя (отображается только пользователю с правом доступа «Может редактировать учетные данные пользователя»);

– : удалить (отображается только пользователю с правом доступа «Может удалять пользователя»).

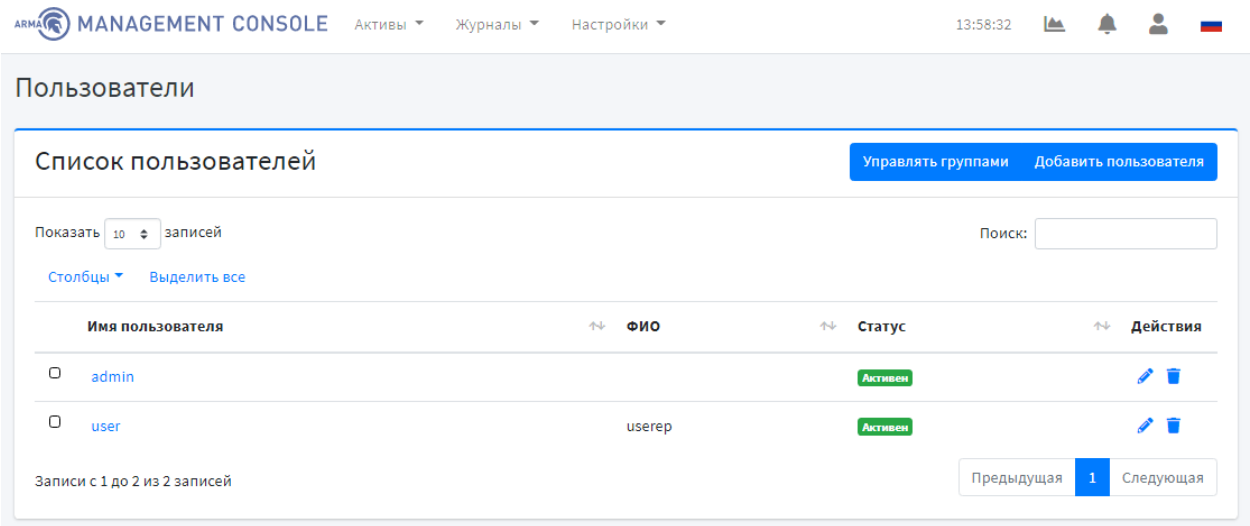


Рисунок 121 – Список пользователей

Для выбора количества записей, отображаемых в таблице пользователей необходимо нажать на кнопку 10 в левом в верхнем углу страницы.

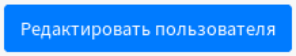
Поле «Поиск» вверху таблицы позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку  рядом с названием соответствующего столбца.

11.2.1 Просмотр учетной записи пользователя

Текущий подраздел доступен пользователю с правом доступа «Может просматривать учетные данные пользователя». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 11.2.2, п. 11.3).

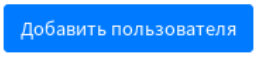
Для просмотра информации учетной записи пользователя необходимо перейти на страницу списка пользователей, нажав на  в верхнем меню и, выбрав пункт «Просмотреть список пользователей». Затем в таблице пользователей нажать на ссылку в столбце «Имя пользователя» соответствующего пользователя, после чего откроется страница «Учетные данные [имя пользователя]» (Рисунок 120).

Для пользователя с правом доступа «Может редактировать учетные данные пользователя» на странице будет отображаться кнопка 

. При нажатии на кнопку отображается страница «Редактировать пользователя» (подробнее описано в подразделе 11.2.3).

11.2.2 Добавление учетной записи пользователя

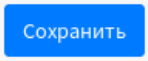
Текущий подраздел доступен пользователю с правом доступа «Может добавлять новых пользователей». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 11.2.2, п. 11.3).

Для добавления учетной записи пользователя необходимо перейти на страницу списка пользователей, нажав на  в верхнем меню и, выбрав пункт «Просмотреть список пользователей» и нажать на кнопку 

(Рисунок 121).

Страница «Добавить нового пользователя» позволяет ввести необходимую информацию для добавления учетной записи пользователя (Рисунок 122). Пароль учетной записи пользователя должен содержать не менее 8 символов, цифры, прописные и строчные буквы.

Примечание – необходимо, чтобы имя пользователя было оригинальным в ARMA Management Console, так как имя пользователя является идентификатором пользователя в ARMA Management Console.

Для сохранения и добавления пользователя необходимо нажать на кнопку 

.

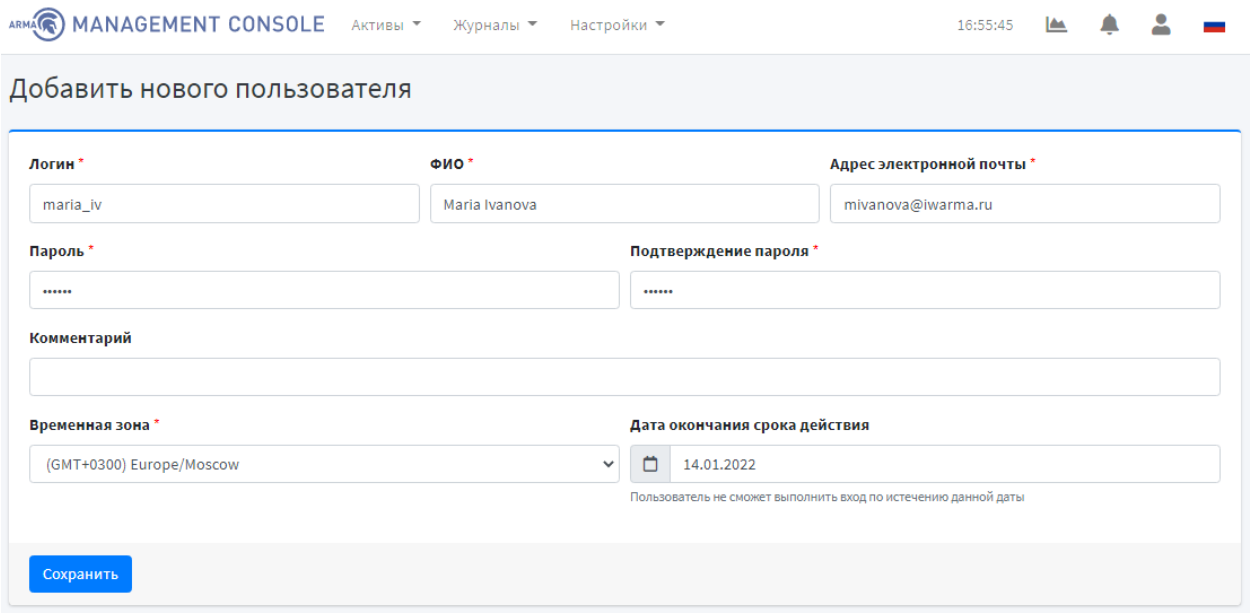


Рисунок 122 – Добавление пользователя

11.2.3 Редактирование учетной записи пользователя

Для редактирования учетной записи пользователей необходимо перейти на страницу списка пользователей, нажав на в верхнем меню и, выбрав пункт «Просмотреть список пользователей». Затем в таблице пользователей нажать на кнопку в столбце «Действия» соответствующего пользователя.

Страница «Редактирование пользователя» позволяет редактировать информацию учетной записи пользователя (Рисунок 123).

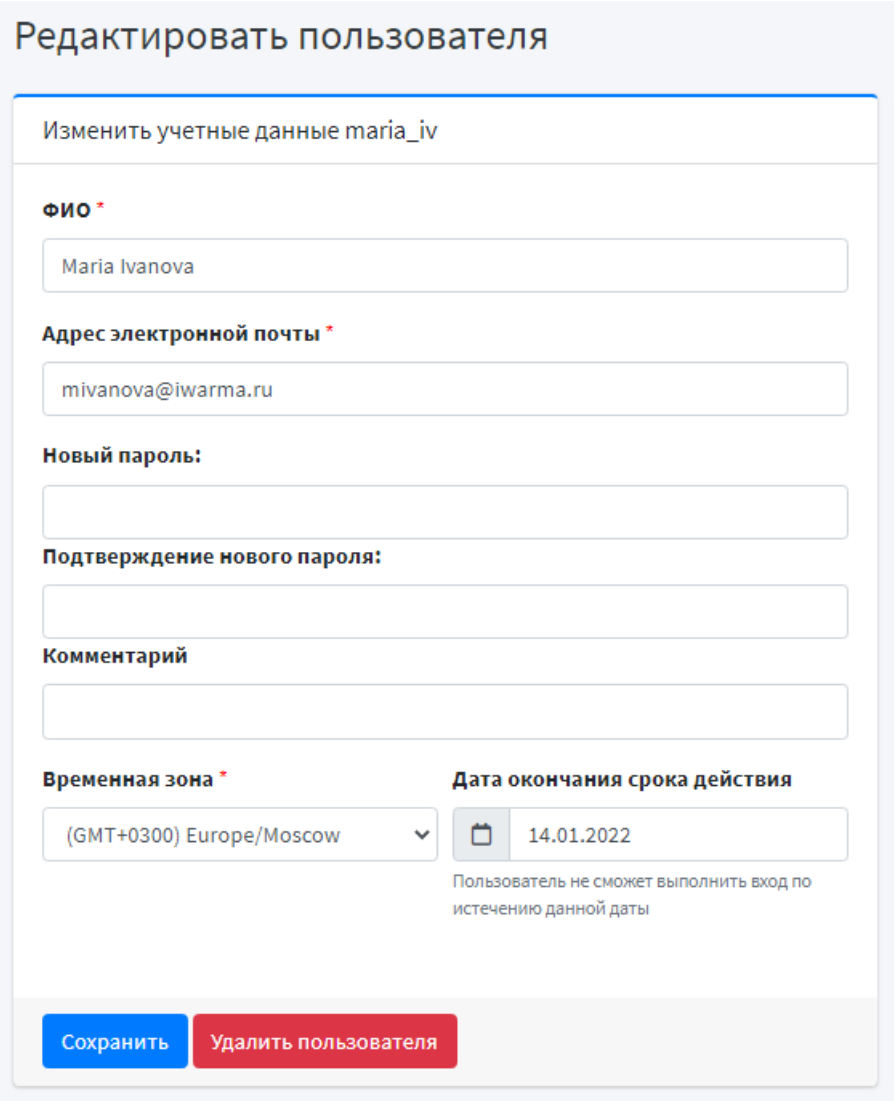


Рисунок 123 – Редактирование учетной записи пользователя

Для сохранения изменений учетной записи пользователя необходимо нажать на кнопку Сохранить.

Для удаления пользователя необходимо нажать на кнопку Удалить пользователя, а затем подтвердить удаление (Рисунок 135).

11.2.4 Удаление учетной записи

Текущий подраздел доступен пользователю с правом доступа «Может удалить пользователя». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 11.2.2, п. 11.3).

Для удаления учетной записи пользователей необходимо перейти на страницу списка пользователей, нажав на в верхнем меню и, выбрав пункт «Просмотреть список пользователей» (Рисунок 121).

Для удаления одной учетной записи пользователя в таблице пользователей необходимо нажать на кнопку в столбце «Действия» соответствующего пользователя и подтвердить удаление во всплывающем окне (Рисунок 133). В

случае успешного удаления учетной записи пользователя появится уведомление об этом (Рисунок 144).

Для удаления нескольких учетных записей пользователя в таблице пользователей необходимо выбрать соответствующих пользователей (Рисунок 124), нажать на кнопку и подтвердить удаление во всплывающем окне.

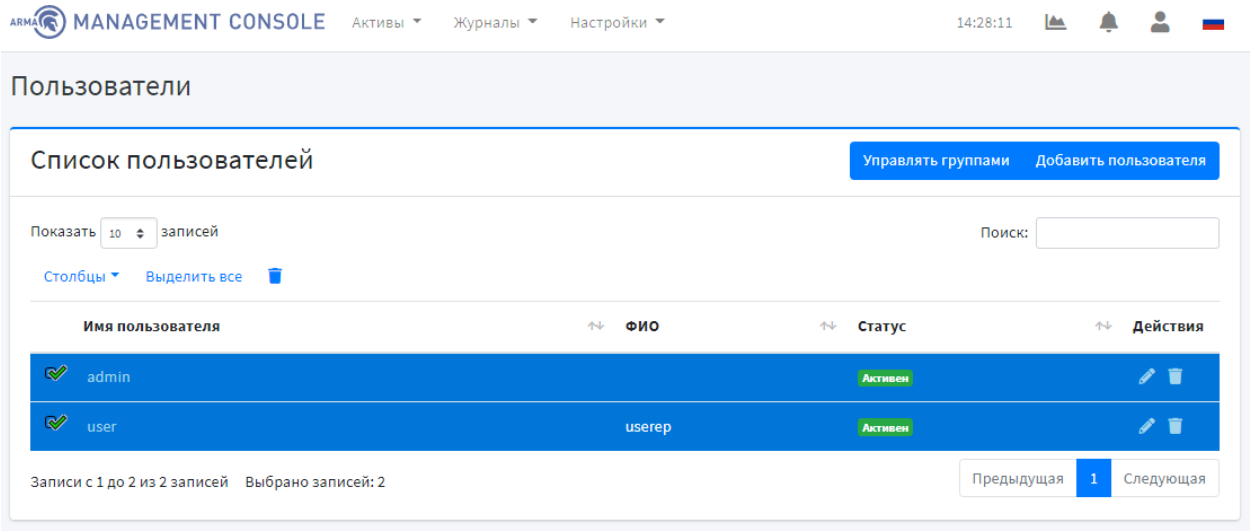


Рисунок 124 – Выбор нескольких учетных записей пользователей

11.3 Управление привилегиями групп пользователей

Текущий подраздел доступен пользователю с привилегией «Может редактировать группы».

Для возможности управления группами пользователей необходимо перейти на страницу списка пользователей, нажав на в верхнем меню и, выбрав пункт «Просмотреть список пользователей». Затем в таблице пользователей нажать на кнопку в столбце «Действия» соответствующего пользователя.

На странице «Редактировать пользователя» нажать на кнопку Управлять группами. При нажатии на кнопку отображается страница «Управлять группами» (Рисунок 125).

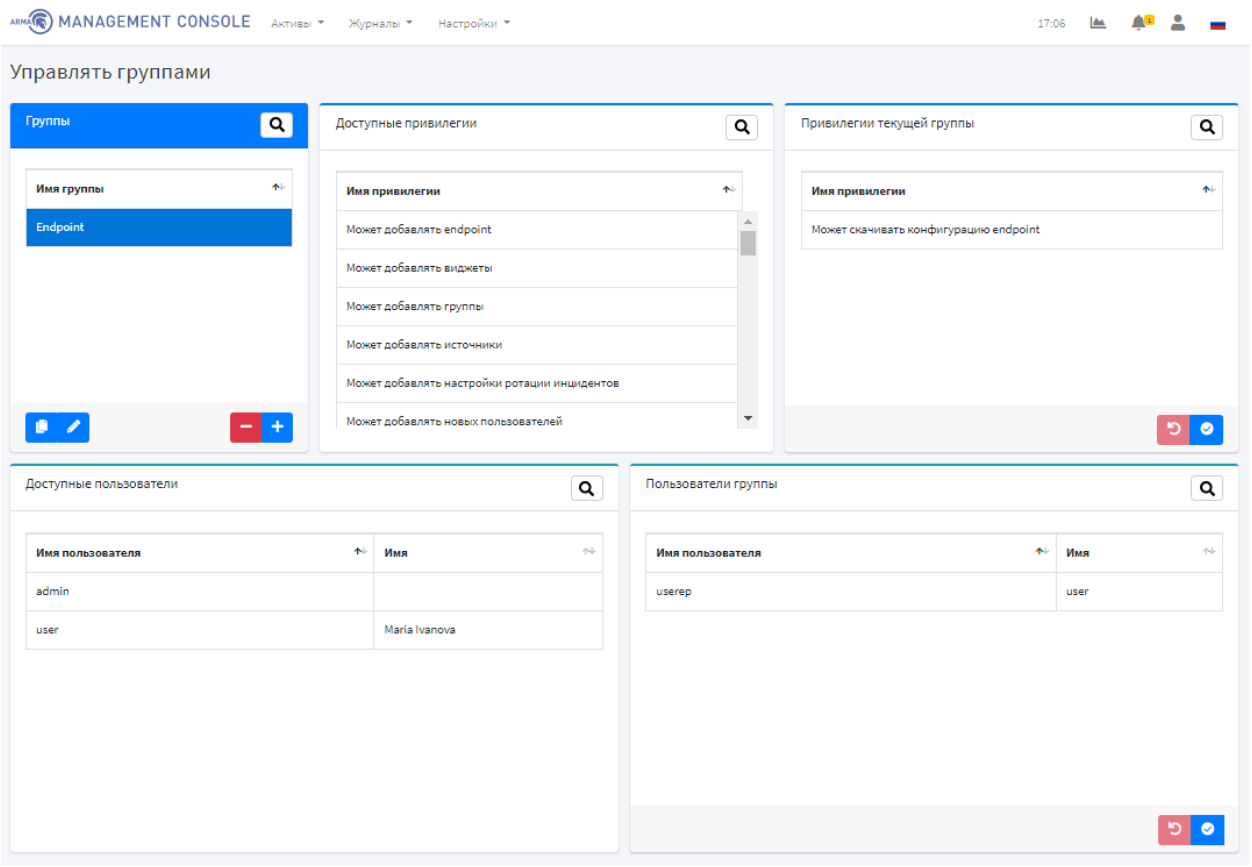


Рисунок 125 – Управление группами

Кнопка позволяет осуществлять сквозной поиск по всем полям соответствующих таблиц. Для выполнения поиска необходимо нажать на кнопку и ввести строку совпадения в поле «Поиск».

Все таблицы позволяют производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

Таблица «Группы» страницы «Управлять группами» отображает список настроенных групп. Возможны следующие действия с элементами таблицы:

– : скопировать выбранную группу;
– : редактировать выбранную группу;
– : удалить выбранную группу;
– : добавить новую группу.

Таблица «Доступные привилегии» отображает невыбранные привилегии для просматриваемой группы. Для выбора привилегий необходимо нажать на привилегию. При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы».

Таблица «Привилегии текущей группы» отображает привилегии для просматриваемой группы. Для удаления привилегий из группы необходимо нажать на привилегию. При нажатии привилегия исчезнет из таблицы «Привилегии

текущей группы» и появится в таблице «Доступные привилегии». Для сохранения изменений привилегий группы необходимо нажать на кнопку  . Для отмены изменения привилегий в группе необходимо нажать на кнопку  .

Таблица «Доступные пользователи» отображает список пользователей, которые не являются участниками просматриваемой группы. Для добавления пользователя в группу необходимо нажать на этого пользователя. При нажатии пользователь исчезнет из таблицы «Доступные пользователи» и появится в таблице «Пользователи группы».

Таблица «Пользователи группы» отображает список пользователей, состоящих в просматриваемой группе. Для удаления пользователя из группы необходимо нажать на пользователя. При нажатии пользователь исчезнет из таблицы «Пользователи группы» и появится в таблице «Доступные пользователи». Для сохранения изменений необходимо нажать на кнопку  . Для отмены изменения необходимо нажать на кнопку  .

11.3.1 Привилегии доступа в системе

В ARMA Management Console доступны следующие привилегии:

1. Управление пользователями:

- может просматривать список пользователей;
- может просматривать учетные данные пользователя;
- может редактировать учетные данные пользователя;
- может удалить пользователя;
- может добавлять новых пользователей.

2. Управление группами пользователей:

- может добавлять группы.

3. Работа с инцидентами:

- может просматривать список инцидентов;
- может назначать инциденты;
- может работать с инцидентами;
- может изменять решенные инциденты;
- может просматривать инциденты (действует при включенной привилегии **«Может работать с инцидентами»**);
- может экспортировать списки инцидентов.

4. Доступ к системным данным:

- может просматривать информацию о системе.

5. Работа с источниками событий:

- может просматривать список источников;
- может редактировать карточку источника;
- может добавлять источники;
- может удалять источники.

6. Работа с сетевыми устройствами:

- может просматривать список активов;
- может просматривать карточку актива;

- может редактировать актив;
- может создавать актив;
- может удалить актив;
- может редактировать группы активов;
- может экспортировать списки активов.

7. Карта сети:

- может просматривать структуру сети.

8. Работа с системами защиты:

- может просматривать список систем защиты;
- может просматривать системы защиты;
- может редактировать системы защиты;
- может добавлять системы защиты;
- может управлять системами защиты;
- может удалить систему защиты.

9. Ротация:

- может изменять настройки ротации;
- может скачивать файлы ротации.

10. Работа с журналом событий:

- может просматривать список событий;
- может просматривать карточку события;
- может экспортировать журналы событий.

11. Endpoint:

- может добавлять Endpoint;
- может редактировать Endpoint;
- может просматривать список Endpoint;
- может скачивать конфигурацию Endpoint;
- может удалять Endpoint.

12. Правила корреляции:

- может просматривать список правил корреляции;
- может просматривать карточку правила корреляции;
- может создавать и редактировать правила корреляции;
- может удалять правила корреляции;
- может создавать, редактировать и удалять группы правил корреляции.

13. Хранилище:

- может просматривать хранилище и скачивать доступные файлы.

14. Системные настройки:

- может просматривать системные настройки;
- может изменять системные настройки.

15. Управление виджетами:

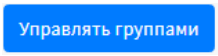
- может добавлять виджеты.

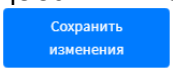
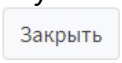
16. Другие привилегии:

- может просматривать сетевые атаки.

11.3.2 Добавление группы пользователей

Для добавления группы пользователей необходимо перейти на страницу списка пользователей, нажав на  в верхнем меню и, выбрав пункт «Просмотреть список пользователей». Затем в таблице пользователей нажать на кнопку  в столбце «Действия» соответствующего пользователя.

На странице «Редактировать пользователя» нажать на кнопку  . При нажатии на кнопку отображается страница «Управлять группами» (Рисунок 125).

Для добавления группы пользователей в таблице «Группы» необходимо нажать на кнопку  , во всплывающем окне «Добавить новую группу» (Рисунок 126) ввести название группы и нажать на кнопку  . Для отмены создания новой группы необходимо нажать на кнопку  .

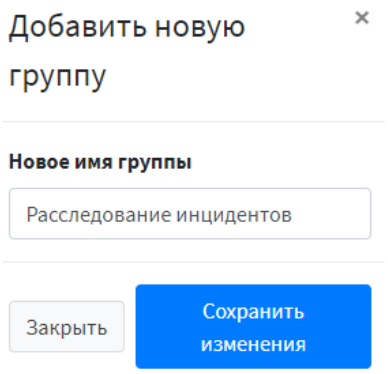


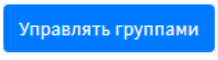
Рисунок 126 – Добавление группы пользователей

При успешном создании группы пользователей появится уведомление об этом, и группа появится в таблице «Группы». Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Добавление пользователей в группу и добавление привилегий группам пользователям описано в п. 11.3.5 и 11.3.6 настоящего руководства.

11.3.3 Редактирование группы пользователя

Для редактирования группы пользователей необходимо перейти на страницу списка пользователей, нажав на  в верхнем меню и, выбрав пункт «Просмотреть список пользователей». Затем в таблице пользователей нажать на кнопку  в столбце «Действия» соответствующего пользователя.

На странице «Редактировать пользователя» нажать на кнопку  . При нажатии на кнопку отображается страница «Управлять группами» (Рисунок 125).

Для редактирования группы пользователей необходимо выбрать (нажать) группу пользователей, нажать на кнопку , во всплывающем окне «Переименовать группу» (Рисунок 127) ввести новое название группы и нажать на кнопку Применить. Для отмены редактирования группы пользователей необходимо нажать на кнопку Закрыть.

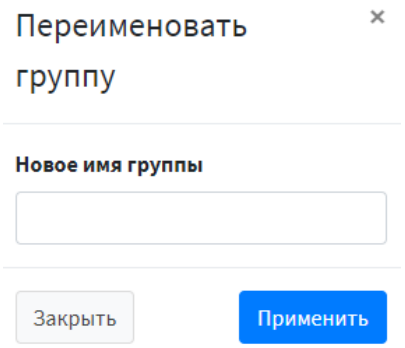


Рисунок 127 – Редактирование группы пользователей

При успешном изменении группы пользователей появится уведомление об этом. Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Добавление пользователей в группу и добавление привилегий группам пользователям описано в п. 11.3.5 и 11.3.6 настоящего руководства.

11.3.4 Удаление группы пользователей

Для удаления группы пользователей необходимо перейти на страницу списка пользователей, нажав на в верхнем меню и, выбрав пункт «Просмотреть список пользователей». Затем в таблице пользователей нажать на кнопку в столбце «Действия» соответствующего пользователя.

На странице «Редактировать пользователя» нажать на кнопку Управлять группами. При нажатии на кнопку отображается страница «Управлять группами» (Рисунок 125).

Для удаления группы пользователей необходимо выбрать (нажать) группу пользователей, нажать на кнопку и подтвердить удаление во всплывающем окне, нажав на кнопку «Да» (Рисунок 128).

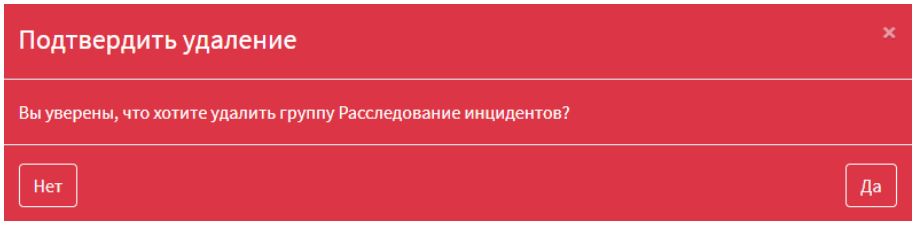


Рисунок 128 – Подтверждение удаления группы пользователей

11.3.5 Добавление пользователей в группу

Добавление пользователей в группу в ARMA Management Console производится посредством добавления групп пользователей (п. 11.3.2 настоящего руководства).

Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Таблица «Доступные пользователи» отображает список пользователей, которые не являются участниками просматриваемой группы. Для добавления пользователя в группу необходимо нажать на этого пользователя. При нажатии пользователь исчезнет из таблицы «Доступные пользователи» и появится в таблице «Пользователи группы».

Таблица «Пользователи группы» отображает список пользователей, состоящих в просматриваемой группе. Для удаления пользователя из группы необходимо нажать на пользователя. При нажатии пользователь исчезнет из таблицы «Пользователи группы» и появится в таблице «Доступные пользователи». Для сохранения изменений необходимо нажать на кнопку  . Для отмены изменения необходимо нажать на кнопку  .

11.3.6 Добавление привилегий группам пользователей

Добавление привилегий группам пользователей в ARMA Management Console производится посредством добавления групп пользователей (п. 11.3.2 настоящего руководства).

Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Для выбора привилегий необходимо нажать на привилегию в таблице «Доступные привилегии». При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы».

Для удаления привилегий из группы необходимо нажать на привилегию в таблице «Доступные привилегии». При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы». Для сохранения изменений привилегий группы необходимо нажать на кнопку  . Для отмены изменений привилегий группы необходимо нажать на кнопку  .

12 УПРАВЛЕНИЕ СТАРТОВОЙ ПАНЕЛЬЮ

Для просмотра страницы «Обзорная панель» необходимо нажать на кнопку  в верхнем меню или на логотип ARMA Management Console.

Страница «Обзорная панель» (Рисунок 129) позволяет просматривать виджеты со следующей информацией:

– системная информация (отображается только для пользователя с правом доступа «Может просматривать информацию о системе»):
  – использование процессора;
  – информация об объеме памяти;
  – использование памяти;
– системные службы;
– инциденты по категории/времени/важности;
– активы по инцидентам;
– статус коррелятора.

ARMA Management Console позволяет каждому пользователю настраивать индивидуальное отображение виджетов – выбирать удобное местоположение виджетов на странице, а также их масштаб.

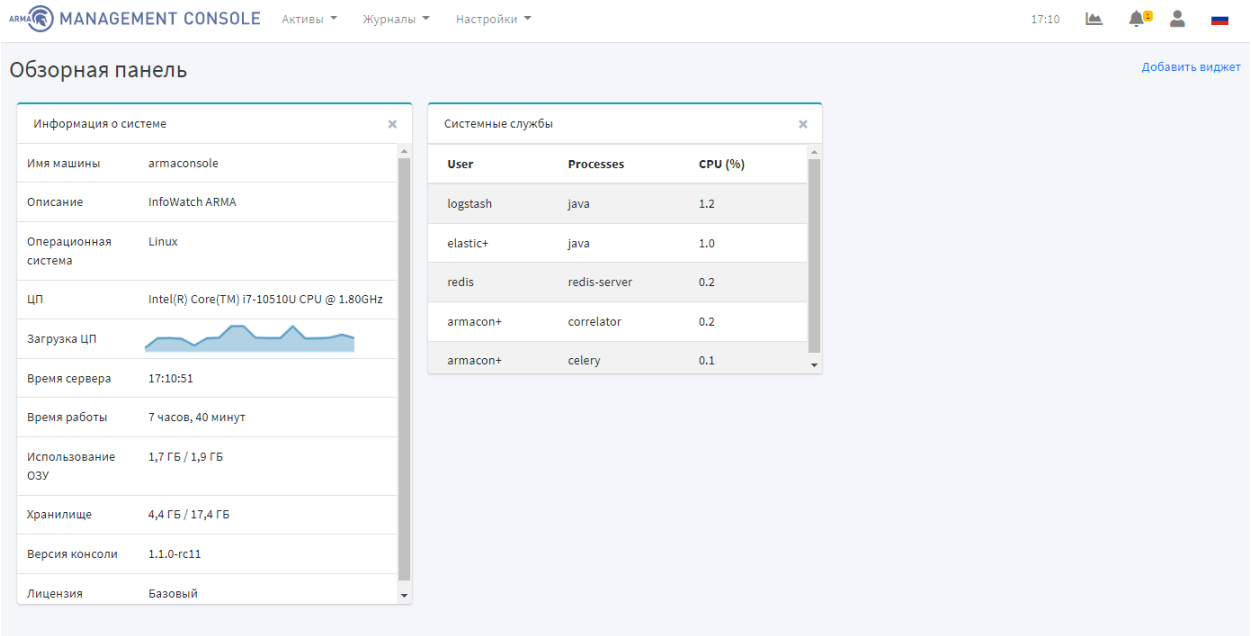


Рисунок 129 – Обзорная панель

Для добавления нового виджета необходимо нажать на кнопку 

. Во всплывающем окне «Добавить новый виджет» в поле «Тип виджета» необходимо выбрать тип добавляемого виджета (Рисунок 130).

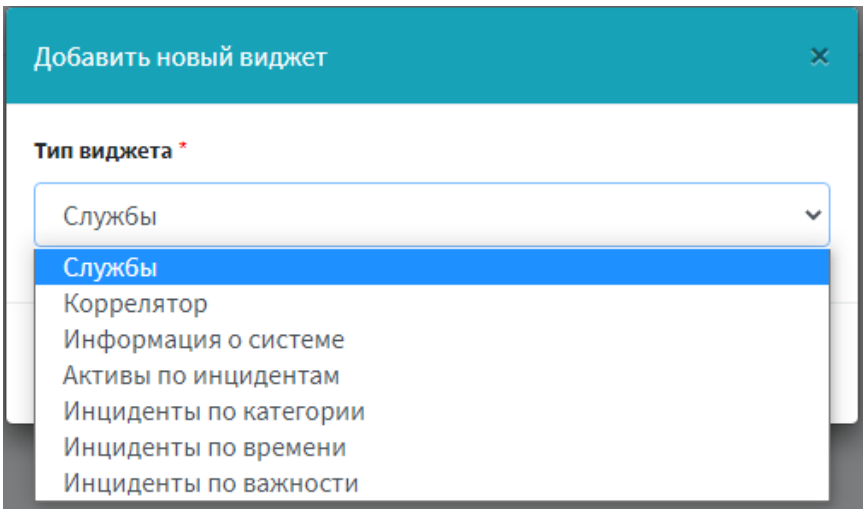


Рисунок 130 – Типы виджетов

Для добавления виджета необходимо нажать на кнопку Добавить (Рисунок 131).

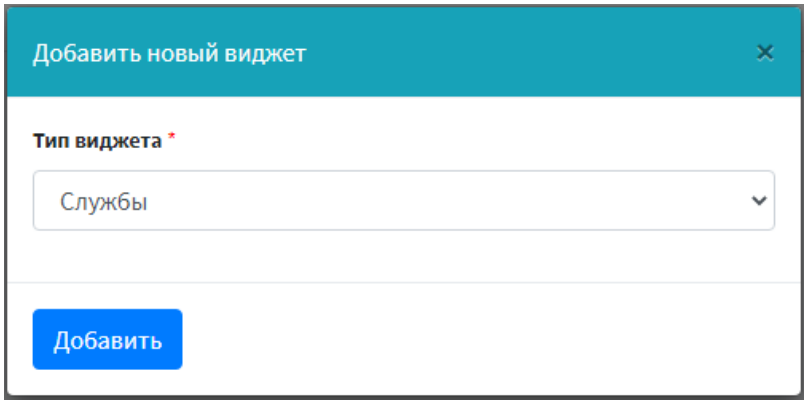


Рисунок 131 – Добавление виджета

13 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

13.1 Предупреждения всплывающие при необходимости подтверждения действий

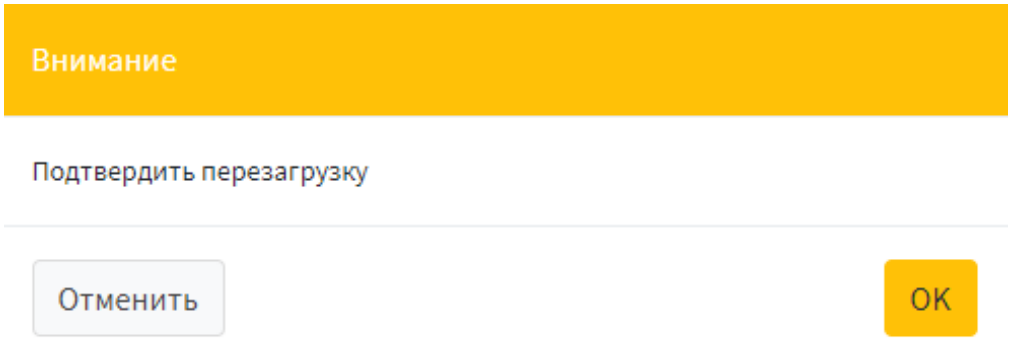


Рисунок 132 – Подтверждение перезагрузки

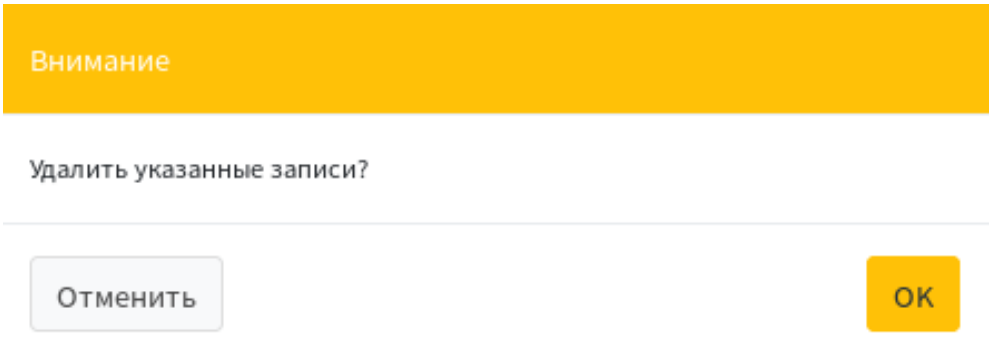


Рисунок 133 – Подтверждение удаления записей

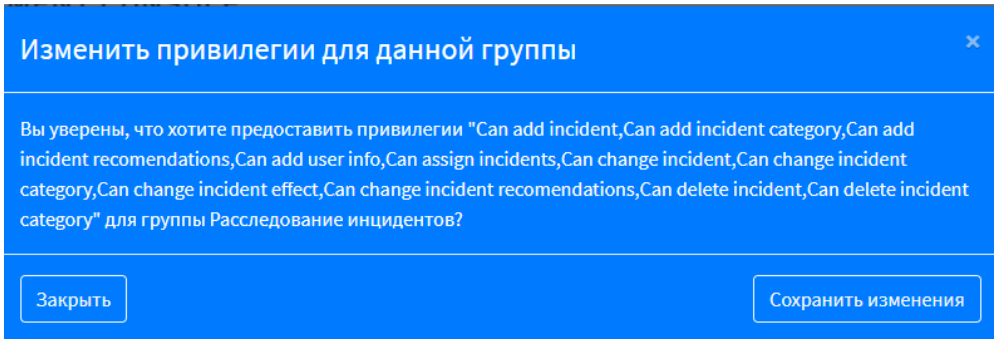


Рисунок 134 – Подтверждение изменений привилегий для группы

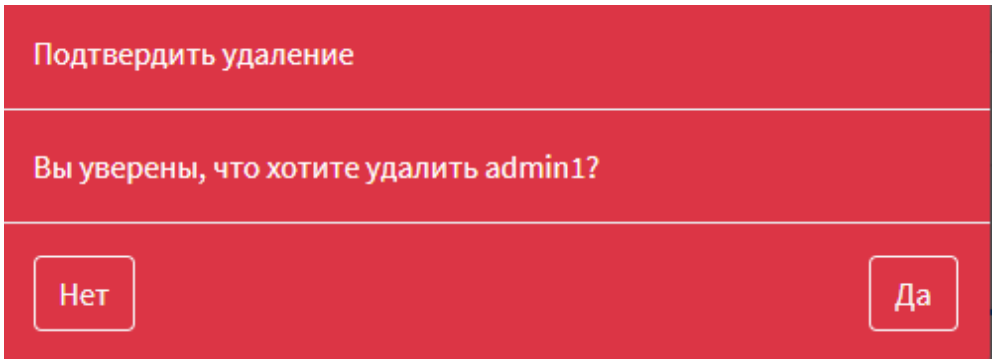


Рисунок 135 – Подтверждение удаления пользователя

13.2 Предупреждения при любом неправильном вводе в поле

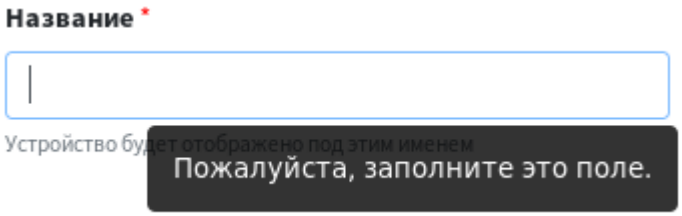


Рисунок 136 – Предупреждение о неправильном вводе в поле (1)

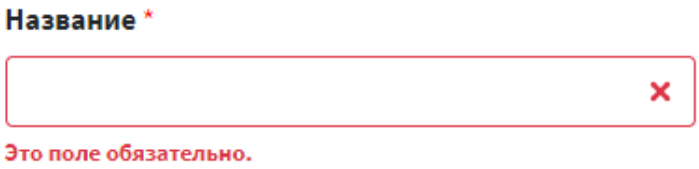


Рисунок 137 – Предупреждение о неправильном вводе в поле (2)

Рисунок 138 – Предупреждение о неправильном вводе в поле (3)

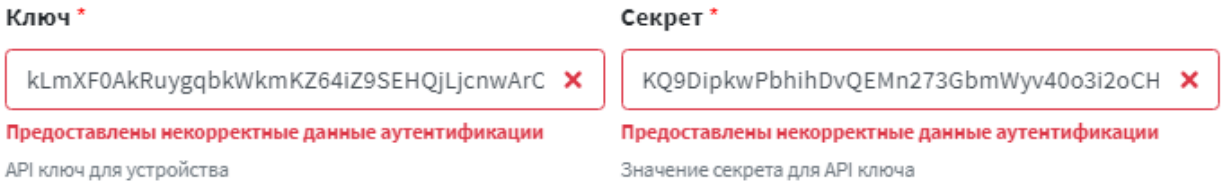


Рисунок 139 – Предупреждение о неправильном вводе в поле (4)

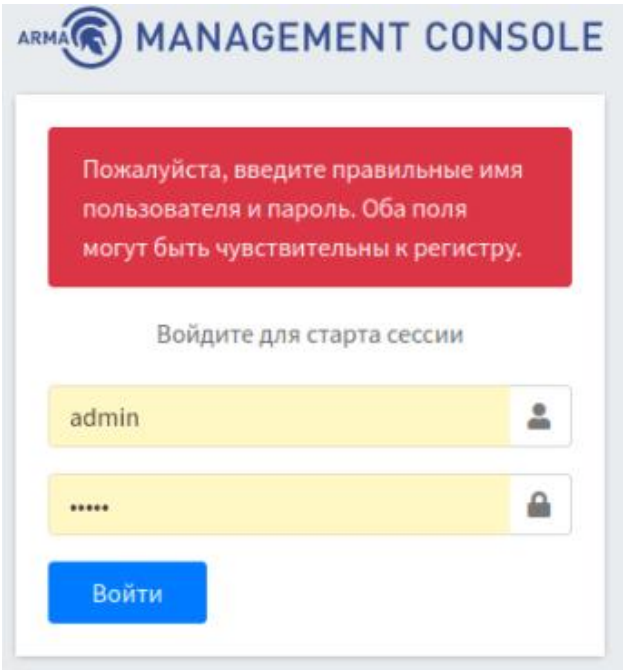


Рисунок 140 – Предупреждение о неправильном вводе в поле (5)

13.3 Предупреждения при применении настроек

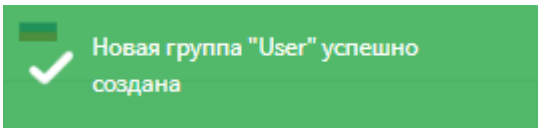


Рисунок 141 – Добавление группы пользователей

Рисунок 142 – Обновление актива

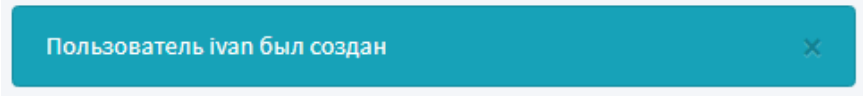


Рисунок 143 – Создание пользователя

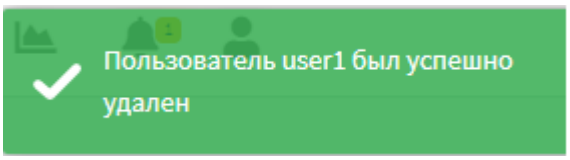


Рисунок 144 – Удаление пользователя

Рисунок 145 – Загрузка конфигурации/правил СОВ

Рисунок 146 – Ожидание скачивания

Рисунок 147 – Неуспешная активация лицензии

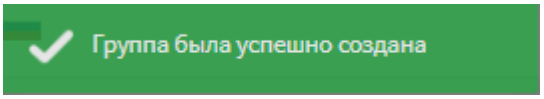


Рисунок 148 – Добавление группы активов

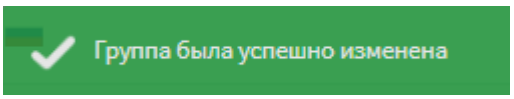


Рисунок 149 – Редактирование группы активов

13.4 Уведомление о несовместимости версий продуктов

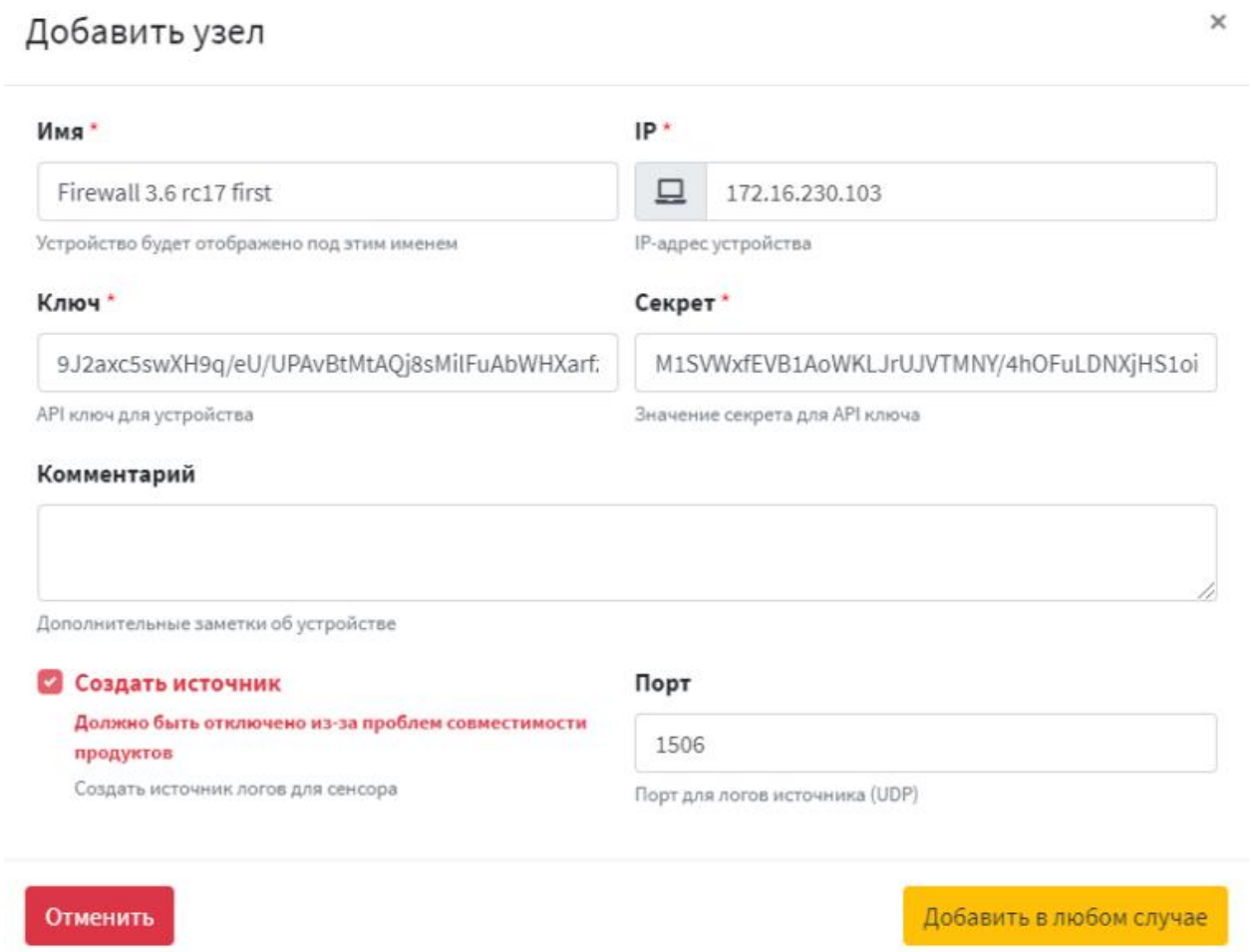


Рисунок 150 – Уведомление о несовместимости версий продуктов

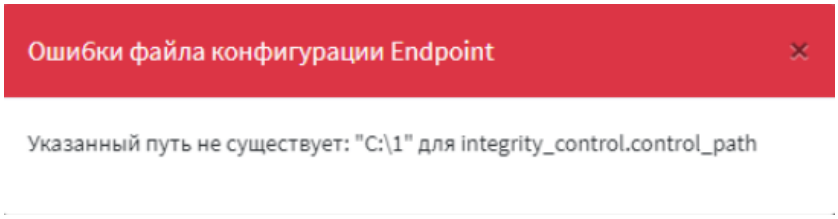


Рисунок 151 – Ошибки файла конфигурации Endpoint