



INFOWATCH ARMA MANAGEMENT CONSOLE



Руководство пользователя по эксплуатации

версия 33 ред. от 26.04.2022

Листов 121

ОГЛАВЛЕНИЕ

Термины и сокращения	6
Аннотация.....	7
1 Назначение программы	8
1.1 Общие сведения	8
1.2 Требования к среде функционирования	8
1.2.1 Требования к аппаратной платформе	8
1.2.2 Требования к виртуальной платформе	9
2 Начало работы.....	10
2.1 Установка	10
2.2 Базовая настройка сетевых интерфейсов.....	14
2.3 Изменение пароля по умолчанию.....	15
2.4 Подключение к ARMA MC.....	16
2.4.1 Активация лицензии с доступом в Интернет.....	17
2.4.2 Активация лицензии без доступа в Интернет	17
3 Просмотр журналов событий.....	21
3.1 Описание журнала событий.....	21
3.2 Поиск событий.....	22
3.3 Просмотр подробной информации о событии	24
4 Расследование инцидентов	27
4.1 Уведомление о нерешенных инцидентах.....	27
4.2 Описание журнала инцидентов	27
4.3 Поиск, сортировка и фильтрация инцидентов.....	28
4.4 Просмотр подробной информации об инциденте	30
4.5 Экспорт инцидентов	32
4.6 Управление инцидентами	32
4.6.1 Назначение пользователя для решения инцидента.....	32
4.6.2 Внесение результата проведенного расследования	33
4.7 Просмотр архивов	33
5 Настройки.....	36

5.1	Настройка правил корреляции.....	36
5.1.1	Правило корреляции с типом действия «Syslog»	40
5.1.2	Правило корреляции с типом действия «HTTP»	42
5.1.3	Правило корреляции с типом действия «Инцидент»	44
5.1.4	Правило корреляции с типом действия «Bash скрипт»	47
5.1.5	Правило корреляции с типом действия «Запустить исполняемый файл» 49	49
5.1.6	Правило корреляции с типом действия «Новый актив»	50
5.1.7	Правило корреляции с типом действия «Правило межсетевого экрана» 52	52
5.2	Настройка ротации журналов.....	54
5.3	Настройка экспорта инцидентов	56
5.3.1	Формат сообщений при экспорте инцидентов через Syslog	57
5.3.2	Формат сообщений при экспорте инцидентов через OPCUA	59
5.4	Настройка TLS сертификата	59
5.5	Управление лицензиями.....	60
6	Управление системами защиты	63
6.1	Описание таблицы систем защиты	63
6.2	Добавление системы защиты	65
6.3	Удаление системы защиты	66
6.4	Редактирование основной информации о системе защиты	66
6.5	Работа с конфигурациями систем защиты	67
6.5.1	Скачивание конфигурации системы защиты	67
6.5.2	Загрузка конфигурации на систему/системы защиты.....	67
6.6	Работа с правилами COB систем защиты	68
6.6.1	Скачивание правил COB системы защиты	68
6.6.2	Загрузка правил COB на систему/системы защиты.....	68
6.7	Добавление ARMA IF	68
6.7.1	Создание пользователя.....	68
6.7.2	Добавление устройства защиты.....	69
6.7.3	Настройка экспорта событий по Syslog.....	70

7	Управление Endpoint.....	71
7.1	Описание таблицы Endpoint	71
7.2	Добавление Endpoint.....	72
7.3	Редактирование Endpoint.....	75
7.4	Копирование конфигурации Endpoint.....	76
7.5	Скачивание конфигурации Endpoint.....	76
7.6	Обновление конфигурации с Endpoint	76
7.7	Удаление Endpoint	77
8	Управление источниками события.....	78
8.1	Добавление источника события	78
9	Управление списком устройств сети	80
9.1	Описание таблицы устройств сети.....	80
9.2	Поиск, сортировка и фильтрация устройств сети	81
9.3	Редактирование основной информации об устройстве сети	82
9.4	Добавление группы устройств сети.....	83
9.5	Удаление группы устройств сети.....	84
9.6	Редактирование групп	84
10	Настройка карты сети	86
10.1	Описание карты сети	86
10.1.1	Создание и удаление связей устройств	90
10.1.2	Добавление карты сети	90
10.2	Описание карты сетевых взаимодействий.....	90
10.2.1	Фильтрация соединений по времени и типу протокола.....	91
10.2.2	Фильтрация по активам	92
10.2.3	Перестановка элементов на карте.....	93
11	Управление учетными записями и правами доступа системы	94
11.1	Профиль пользователя.....	94
11.2	Список пользователей.....	95
11.2.1	Просмотр учетной записи пользователя.....	96
11.2.2	Добавление учетной записи пользователя	96

11.2.3	Редактирование учетной записи пользователя.....	97
11.2.4	Удаление учетной записи.....	98
11.3	Управление привилегиями групп пользователей.....	99
11.3.1	Привилегии доступа в системе.....	103
11.3.2	Добавление группы пользователей.....	106
11.3.3	Редактирование группы пользователя.....	107
11.3.4	Удаление группы пользователей.....	107
11.3.5	Добавление пользователей в группу.....	108
11.3.6	Добавление привилегий группам пользователей.....	108
12	ГосСОПКА.....	110
13	Управление стартовой панелью.....	115
14	Сообщения пользователю.....	117
14.1	Предупреждения всплывающие при необходимости подтверждения действий.....	117
14.2	Предупреждения при любом неправильном вводе данных в поле.....	118
14.3	Предупреждения при применении настроек.....	119
14.4	Уведомление о несовместимости версий продуктов.....	120
14.5	Уведомление об ошибке файла конфигурации Endpoint.....	121

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Таблица 1
Термины и сокращения

Термины и сокращения	Значение
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак
КИИ	Критическая информационная инфраструктура
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
ОС	Операционная система
ПК	Программный комплекс
СОБ	Система обнаружения вторжений
ARMA IF	InfoWatch ARMA Industrial Firewall
ARMA MC	InfoWatch ARMA Management Console
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 MC v. 1.3.2**.

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 MC**.

Перед эксплуатацией **ARMA MC** пользователю необходимо изучить настоящее руководство.

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Общие сведения

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

- a. расследование инцидентов **ARMA IF**;
- b. централизованное управление **ARMA IF**;
- c. доступ к веб-интерфейсу управляемых устройств **ARMA IF**;
- d. управление правилами COB на **ARMA IF**;
- e. управление конфигурацией **ARMA IF**;
- f. управление списком устройств сети;
- g. 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);
- h. управление учетными записями и правами доступа **ARMA MC**.

1.2 Требования к среде функционирования

Установка **ARMA MC** производится на следующие типы платформ:

- аппаратная;
- виртуальная (гипервизор).

Установка на аппаратную платформу выполняется с использованием USB-накопителя, на который должен быть записан образ **ARMA MC** 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 MC** на аппаратную платформу необходимо использовать микропроцессорную архитектуру **x64** или **Байкал-М (ARMv8)**.

Для аппаратной платформы, на которую устанавливается **ARMA MC** достаточно руководствоваться минимальными требованиями к аппаратному обеспечению (см. Таблица 2).

Таблица 2
Минимальные требования к аппаратному обеспечению

Название оборудования	Требования
Процессор	2,0 ГГц, четырехъядерный, x64 или Байкал-М (ARMv8)

Название оборудования	Требования
ОЗУ	16 ГБ
Интерфейсы, необходимые для установки программного обеспечения	Последовательная консоль или видеовыход (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 MC** 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 MC** предъявляются следующие минимальные требования к виртуальной среде (см. Таблица 3).

*Таблица 3
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:

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

2 НАЧАЛО РАБОТЫ

2.1 Установка

Установка **ARMA MC** 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 **кнопку «Enter»** (см. [Рисунок 1](#)).

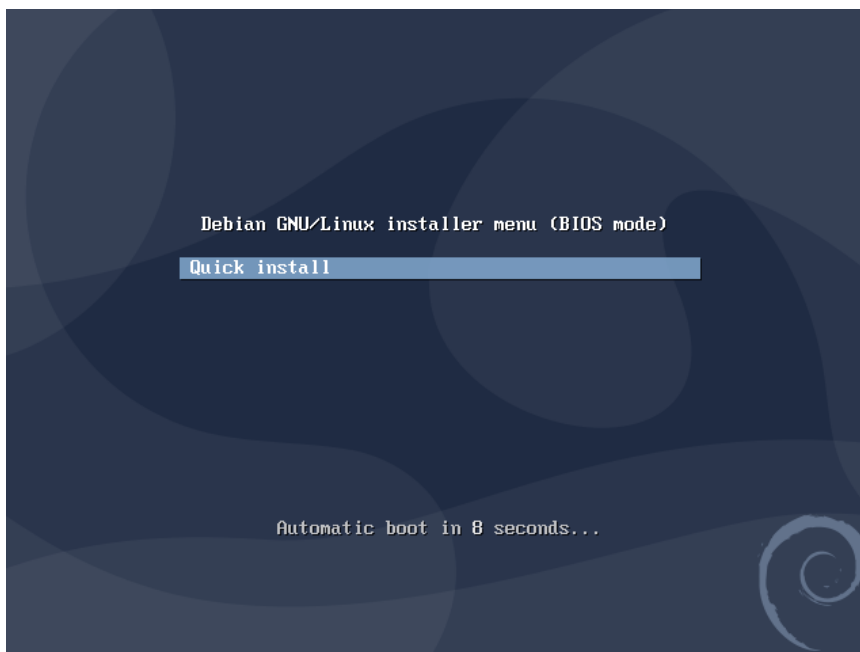


Рисунок 1 – Выбор типа установки

Затем запустится загрузка списка пакетов для установки системы (см. [Рисунок 2](#)).

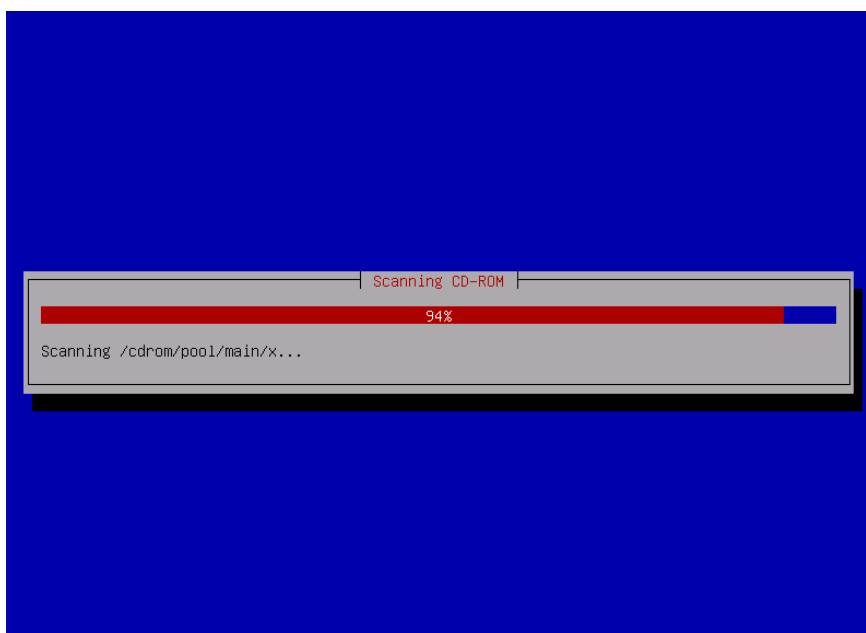


Рисунок 2 – Загрузка списка пакетов

Далее необходимо ввести имя хоста для системы или оставить его по умолчанию и нажать **кнопку «Enter»** (см. [Рисунок 3](#))

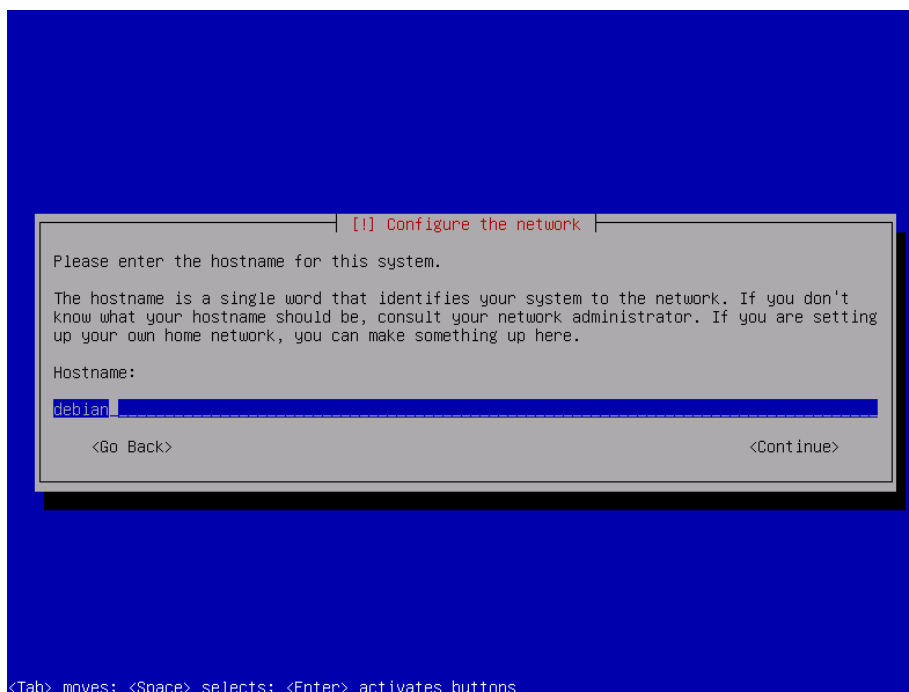


Рисунок 3 – Настройка сети. Выбор имени хоста

После выбора имени хоста необходимо задать доменное имя или оставить его по умолчанию и нажать **кнопку «Enter»** (см. [Рисунок 4](#)).

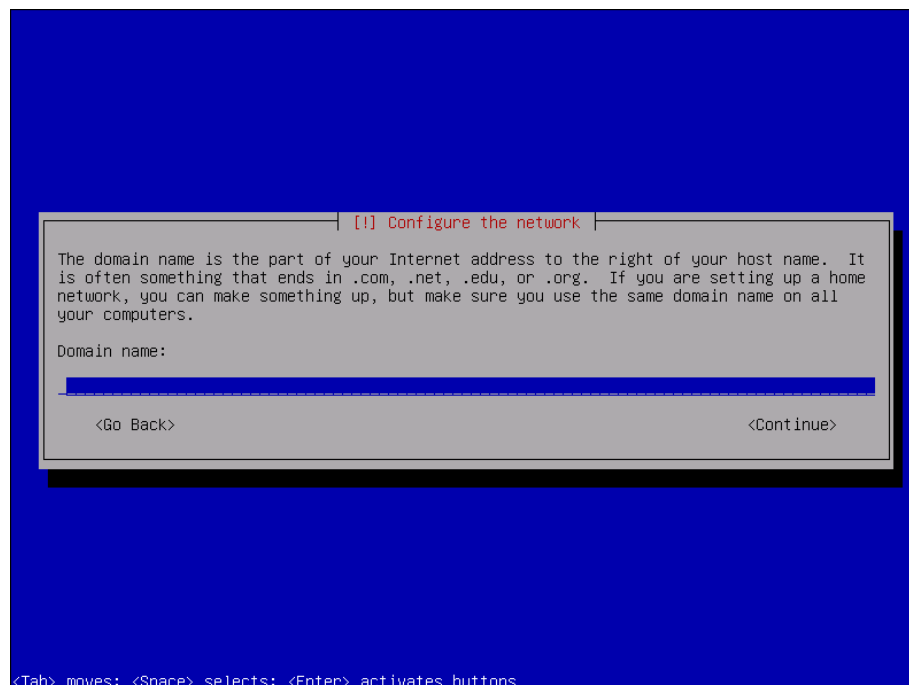


Рисунок 4 – Настройка сети. Выбор доменного имени

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

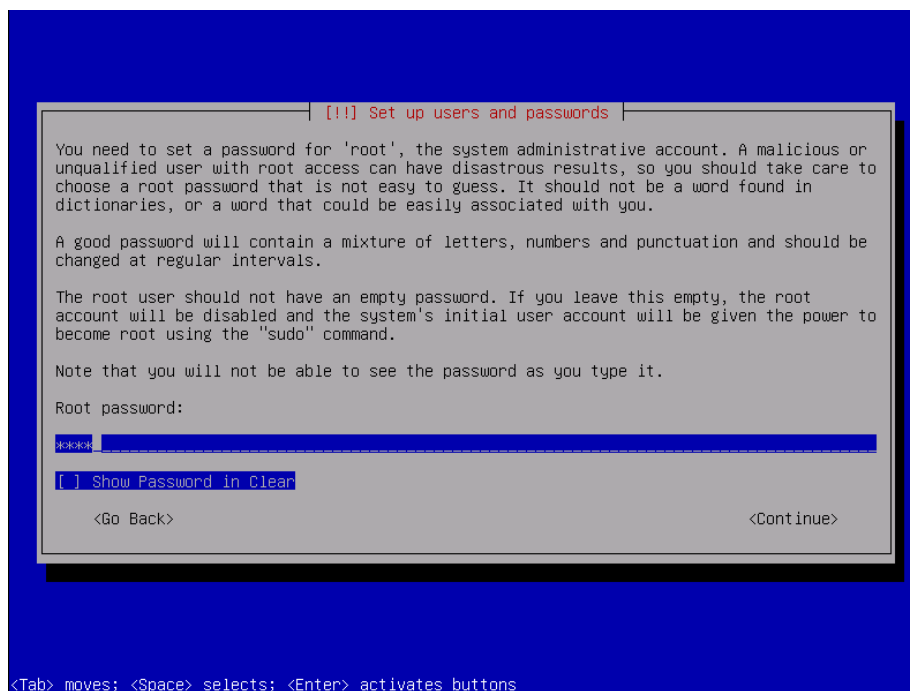


Рисунок 5 – Настройка пользователей и паролей. Ввод пароля

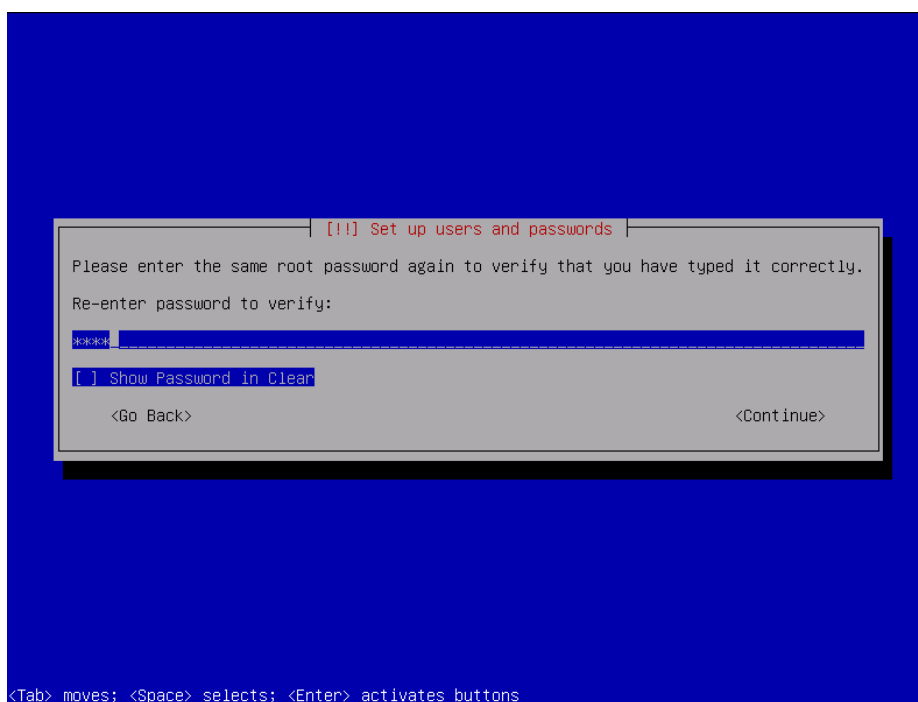


Рисунок 6 – Настройка пользователей и паролей. Повтор пароля

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

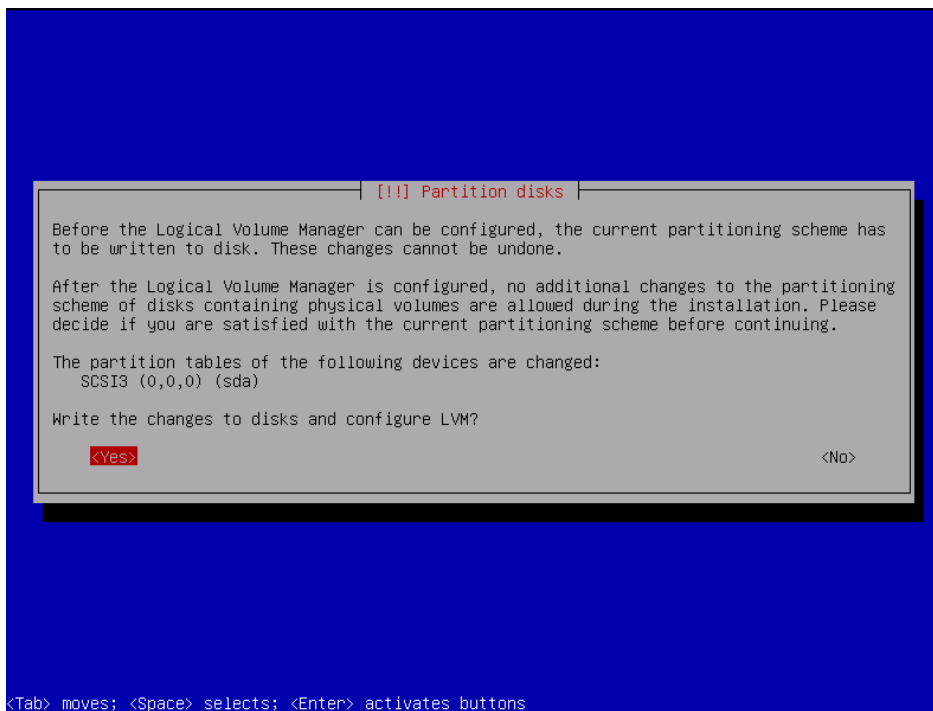


Рисунок 7 – Диски разделов

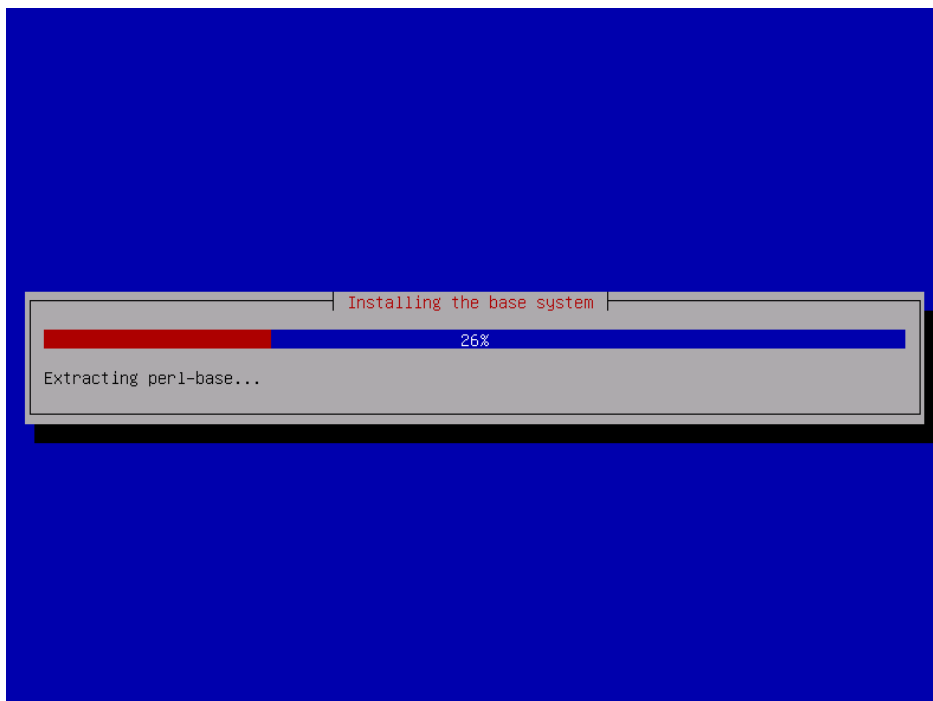


Рисунок 8 – Установка базовой системы

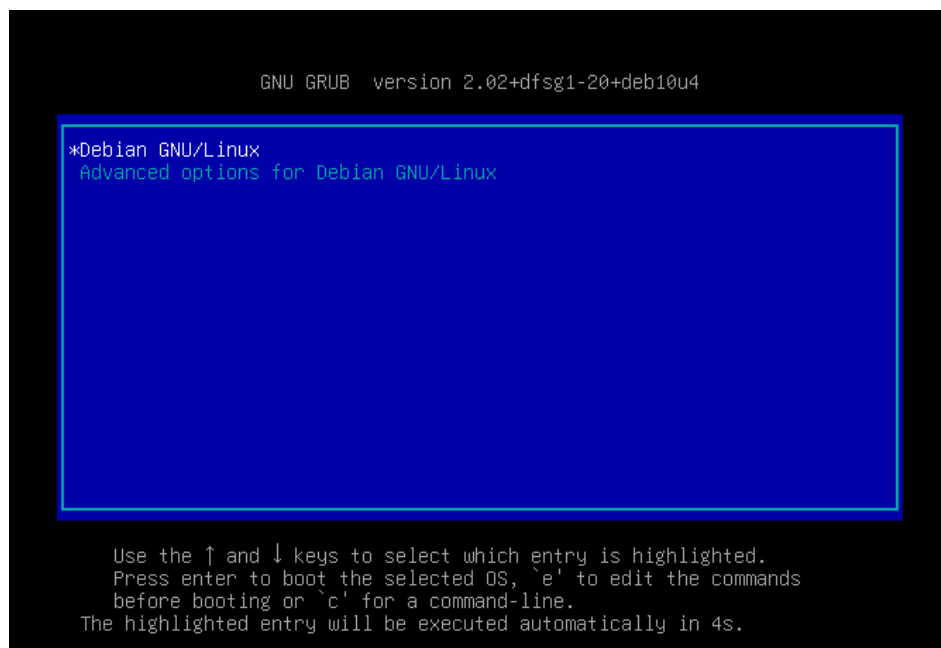


Рисунок 9 – Загрузка системы

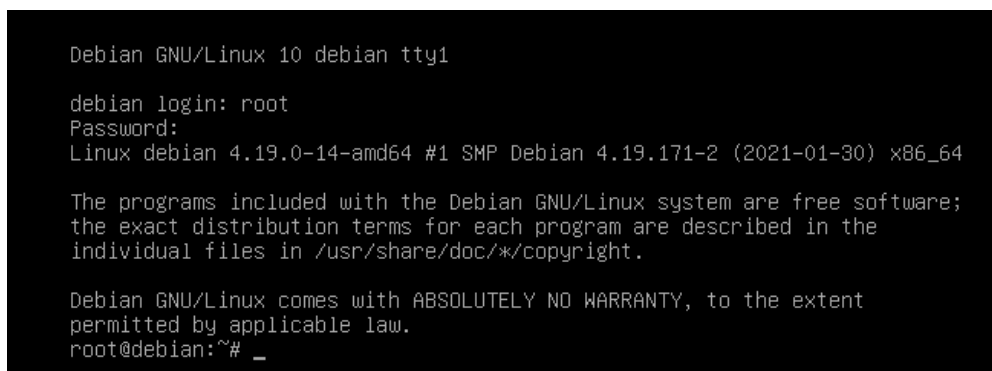


Рисунок 10 – Аутентификация в локальном (консольном) интерфейсе

2.2 Базовая настройка сетевых интерфейсов

Адрес по DHCP по умолчанию выдается для первого сетевого интерфейса **ARMA MS**.

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

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

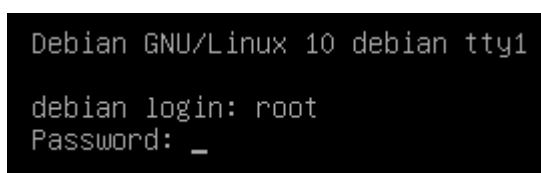
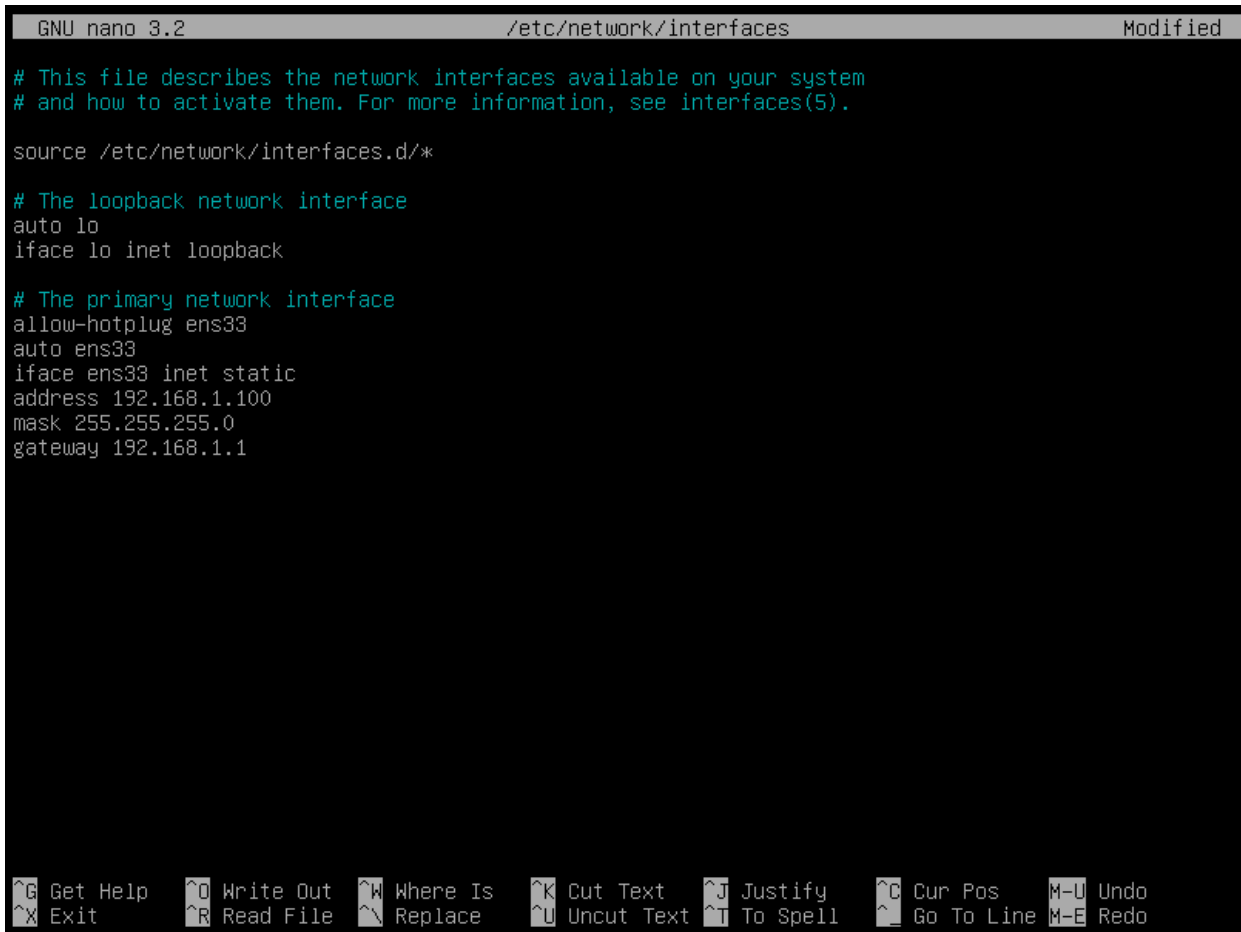


Рисунок 11 – Вход в локальный (консольный) интерфейс

- b. Выполнить команду `nano /etc/network/interfaces`.

- c. Задать параметры в секции **#The primary network interface** согласно рисунку (см. [Рисунок 12](#)) и сохранить изменения, нажав комбинации клавиш **«Ctrl+O»**, а затем **«Ctrl+X»**.



```

GNU nano 3.2 /etc/network/interfaces Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
auto ens33
iface ens33 inet static
address 192.168.1.100
mask 255.255.255.0
gateway 192.168.1.1
    
```

Рисунок 12 – Настройка сетевого интерфейса

- d. Выполнить команду `service networking restart`.
 e. 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 MC**, используя пользователя по умолчанию (логин – **root**, пароль – **root**). После успешного входа необходимо выполнить команду `passwd`, указать новый пароль, нажать **кнопку «Enter»**, а затем повторить пароль и нажать **кнопку «Enter»**.

Для изменения пароля по умолчанию пользователя веб-интерфейса необходимо зайти в веб-интерфейс **ARMA MC**, используя пользователя по умолчанию (логин – **admin**, пароль – **nimda**). После успешного входа перейти в раздел **«Профиль пользователя»**, нажав **кнопку «»**, нажать **кнопку «Редактировать пользователя»**, в полях **«Пароль»** и **«Подтверждение пароля»** задать новый пароль и нажать **кнопку «Сохранить»**.

2.4 Подключение к ARMA MC

Для доступа к веб-интерфейсу управления **ARMA MC** 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 MC** (по умолчанию используется получение по DHCP).

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

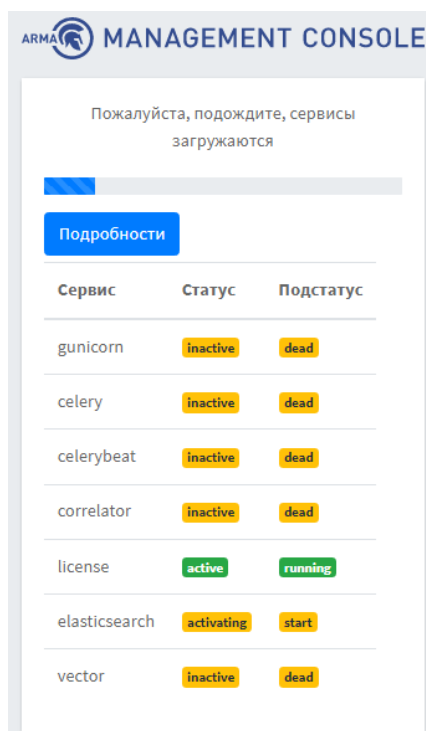


Рисунок 13 – Загрузка сервисов

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

- активация лицензии с доступом в Интернет;
- активация лицензии без доступа в Интернет.

!Важно Лицензионный ключ предоставляется согласно условиям в договоре поставки.

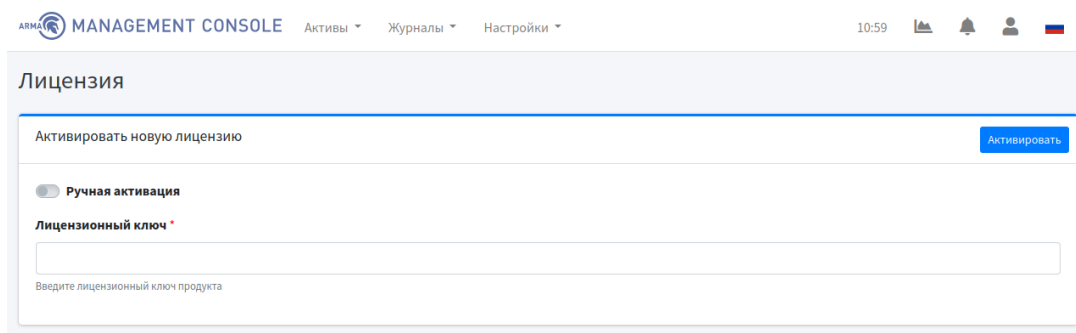


Рисунок 14 – Активация лицензии

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 **кнопку «Активировать»** (см. Рисунок 15).

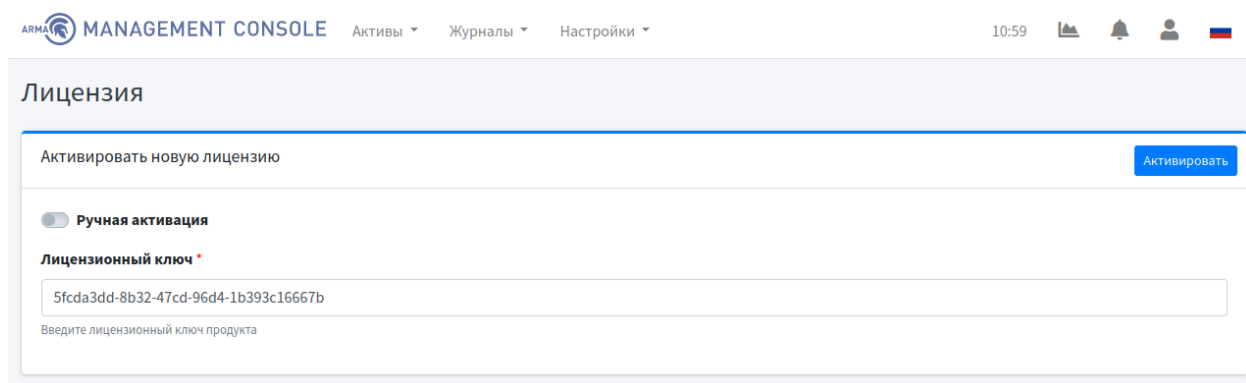


Рисунок 15 – Активация лицензии с доступом в Интернет

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 **кнопку «Получить токен»** (см. Рисунок 16).

Лицензия

Активировать новую лицензию Активировать

Ручная активация

Лицензионный ключ *

5fcd3dd-8b32-47cd-96d4-1b393c16667b Получить токен

Введите лицензионный ключ продукта

Токен

```

=====BEGIN=====
X82j3YsyR82W1Bs5PBZre+2+grsAb27qrMVK2gAZ
mdkAAAAeMiAyMSOwOSOyN1QxMD00Do1MC4wMzYyMzUyNiZa
=====END=====
    
```

Данный текст будет отправлен на сервер лицензий

Лицензия *

Выберите файл Обзор

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 кнопку «**Обзор**» в поле «Лицензия», а затем нажать кнопку «**Активировать**» (см. Рисунок 17).

Лицензия

Активировать новую лицензию Активировать

Ручная активация

Лицензионный ключ *

5fcd3dd-8b32-47cd-96d4-1b393c16667b Получить токен

Введите лицензионный ключ продукта

Токен

```

=====BEGIN=====
X82j3YsyR82W1Bs5PBZre+2+grsAb27qrMVK2gAZ
mdkAAAAeMiAyMSOwOSOyN1QxMD00Do1MC4wMzYyMzUyNiZa
=====END=====
    
```

Данный текст будет отправлен на сервер лицензий

Лицензия *

license.bin Обзор

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 кнопку «**Войти**» (см. Рисунок 18).

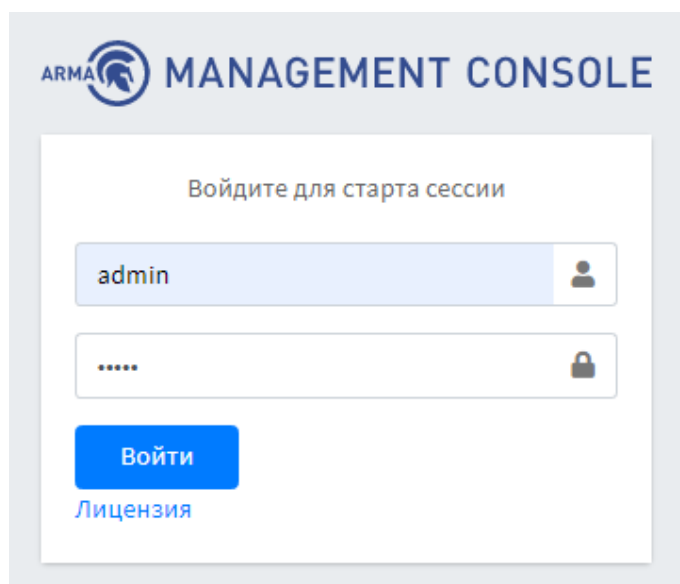


Рисунок 18 – Вход в систему

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

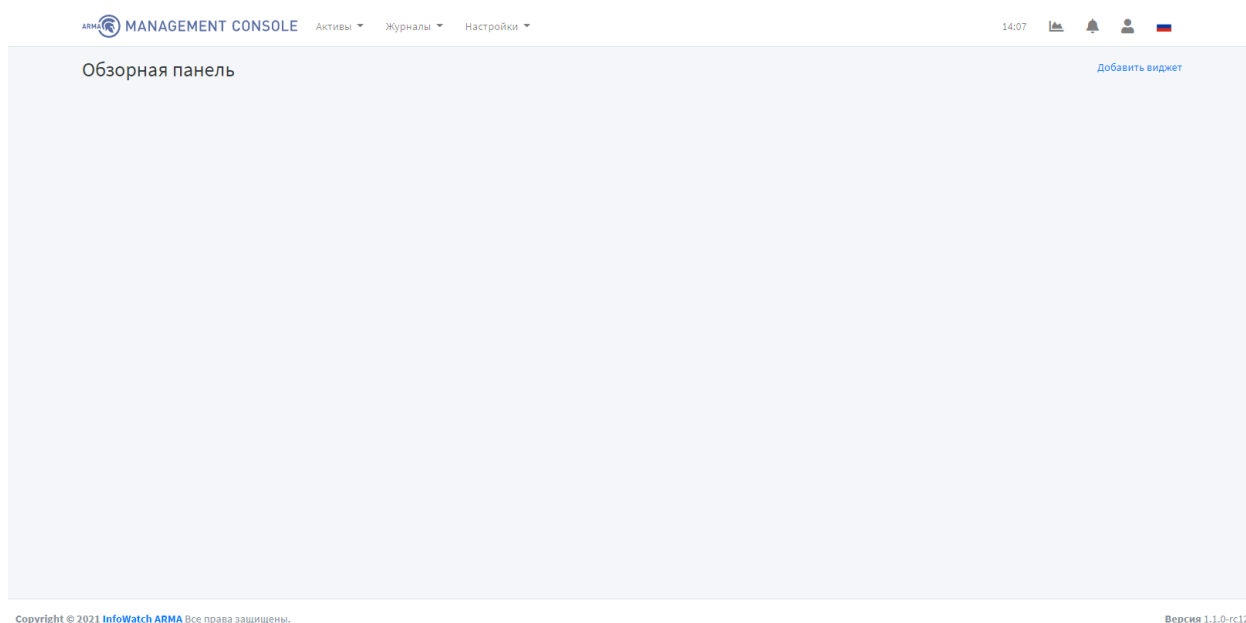


Рисунок 19 – Обзорная панель

Информация о порядке работы в **ARMA MC** 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 ГосСОПКой (раздел 12);
- Управление стартовой панелью (раздел 13);
- Сообщения пользователю (раздел 14).

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 11 настоящего руководства.

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



Рисунок 20 – Переход на страницу событий

3.1 Описание журнала событий

В журнале событий отображаются события систем защиты, подключенных к **ARMA MS**.

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

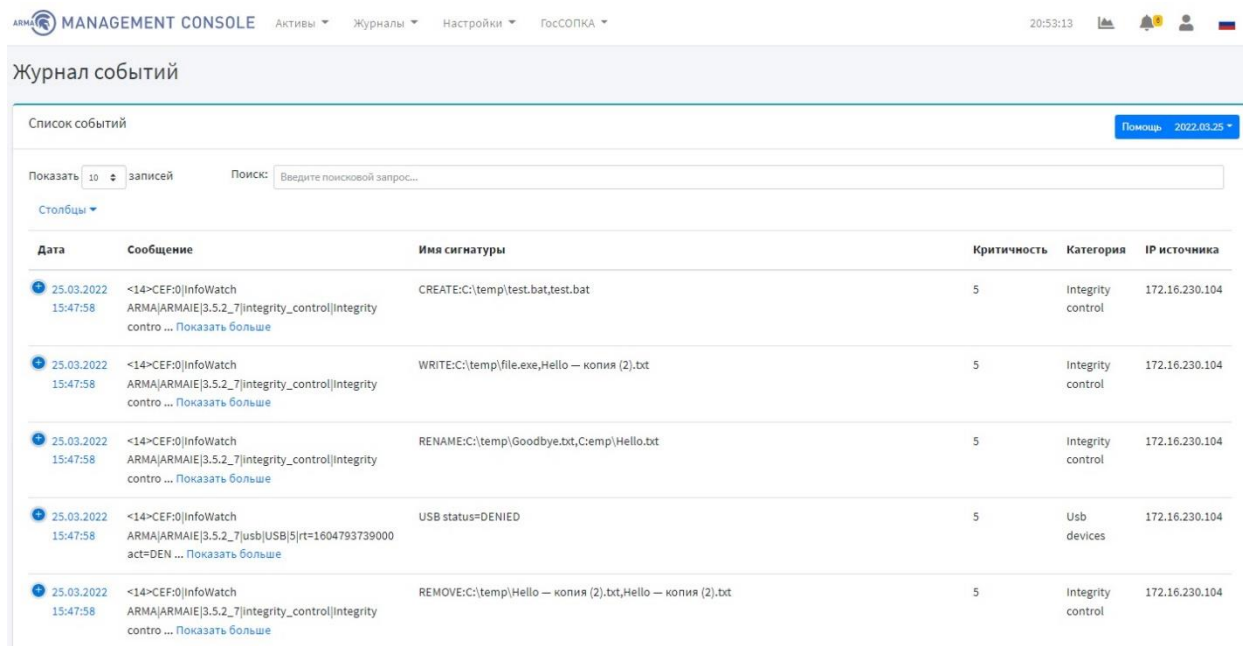


Рисунок 21 – Журнал событий

Данные о событиях можно настраивать вручную. Для этого необходимо нажать **кнопку «Столбцы»** в левом верхнем углу формы и в выпадающем списке выбрать/убрать данные, которые будут отображаться в таблице (см. [Рисунок 22](#)).

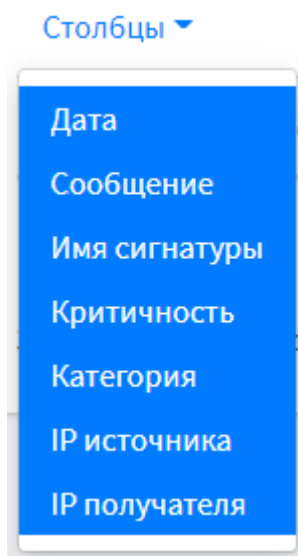


Рисунок 22 – Выбор данных о событиях

Для выбора конкретной даты отображения данных таблицы событий необходимо нажать **кнопку «2020.10.22»** в правом верхнем углу формы.

Для выбора количества записей, отображаемых в таблице событий необходимо нажать **кнопку «10»** в левом в верхнем углу формы.

3.2 Поиск событий

Поле **«Поиск»** сверху таблицы событий позволяет осуществлять сквозной поиск по всем полям таблицы.

Для выполнения поиска необходимо ввести одно из доступных полей, которые можно посмотреть, нажав **кнопку «Помощь»**, во вкладке **«Поля»** (см. [Рисунок 23](#)), и строку совпадения в поле **«Поиск»**. Например, `sign_name:idsalert`.

Помощь по коррелятору
✕

Синтаксис
Поля

Строка запроса разбивается на ряд терминов и операторов. Термин может состоять из одного слова - **quick** или **brown** - или фраза, заключенная в двойные кавычки - "**quick brown**" - поиск всех слов в заданном порядке.

Имена полей

Вы можете указать поля для поиска в синтаксисе запроса:

```
status: active           # поле статуса содержит активные
title:(quick OR brown)  # поле заголовка содержит быстрое или коричневое
author: "John Smith"    # поле author содержит точную фразу "john smith"
```

Диапазоны

Можно указать диапазоны для полей даты, числовых или строковых полей. Включаемые в диапазоны значения указываются в квадратных скобках **[min TO max]**, не включаемые в фигурных скобках **{min TO max}**.

Примеры:

```
count: [1 TO 5]         # Числа 1..5
date: {* TO 2012-01-01} # Даты до 2012 г.
count: [от 1 до 5]     # чисел от 1 до 5, но не включая 5
age: > 10
age: >= 10
age: <10
age: <= 10
```

Логические операторы

Предпочтительные операторы: + (это слово должно присутствовать) и - (это слово должно отсутствовать). Все остальные условия необязательны. Например, такой запрос:

```
quick brown + fox -news
```

будет искать:

- слово **fox** должно присутствовать
- слово **news** должно отсутствовать
- слова **quick** и **brown** необязательны - их присутствие увеличивает релевантность.

Знакомые логические операторы **AND**, **OR** и **NOT** (также записываются как **&&**, **||** и **!**) также поддерживаются, но имейте в виду, что они не соблюдают обычные правила приоритета, поэтому следует использовать круглые скобки если несколько операторов используются вместе. Например, предыдущий запрос можно переписать как:

```
((quick AND fox) OR (brown AND fox) OR fox) AND NOT news
```

Рисунок 23 – Синтаксис коррелятора

Во вкладке «Поля» представлены возможные поля для поиска запроса в синтаксисе (см. Таблица 4).

Таблица 4
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





Имя	Описание
event_count	Количество событий в правиле
event_timestamp	Дата и время, когда правило вызвало срабатывание действия
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 MC** отобразит страницу подробной

информации о событии со следующими разделами (см. Рисунок 24, Рисунок 25, Рисунок 26).

ARMA  MANAGEMENT CONSOLE Активы ▾ Журналы ▾   

Детали события

Основные

Поиск:

Имя	↕	Значение	↕
Протокол события		udp	
Последнее событие		2021-06-10T09:22:06.714Z	
Порт источника		53131	
Первое событие		2021-06-10T09:22:06.714Z	
Имя сигнатуры		InfoWatch ARMA	
IP источника		127.0.0.1	

Рисунок 24 – Детали события. Основные

Дополнительные

Поиск:

Имя	↕	Значение	↕
Число событий		1	
Порт получателя		53	
Критичность события		0	
Категория сигнатуры		PF	
IP получателя		127.0.0.1	
ID сигнатуры		77	

Рисунок 25 – Детали события. Дополнительные


Технические

Поиск:

Имя	↕	Значение	↕
Производитель устройства		InfoWatch ARMA	
Модуль устройства		ARMAIF	
Исходное сообщение события		<1>CEF:0 InfoWatch ARMA ARMAIF 3.6-rc4 pfalert PF rule alert 0 cs1=77 deviceInboundInterface=lo0 act=pass deviceDirection=0 proto=udp rt=1623316926000 deviceFacility=filterlog src=127.0.0.1 dst=127.0.0.1 spt=53131 dpt=53 cs1Label=RuleNumber	Скрыть текст
Действие устройства		pass	
Версия устройства		3.6-rc4	
ID события		76b7507c-28d2-438e-8851-eabe40fa64b7	

Рисунок 26 – Детали события. Технические

Поле **«Поиск»** сверху 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 **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 11 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**» (см. Рисунок 27).

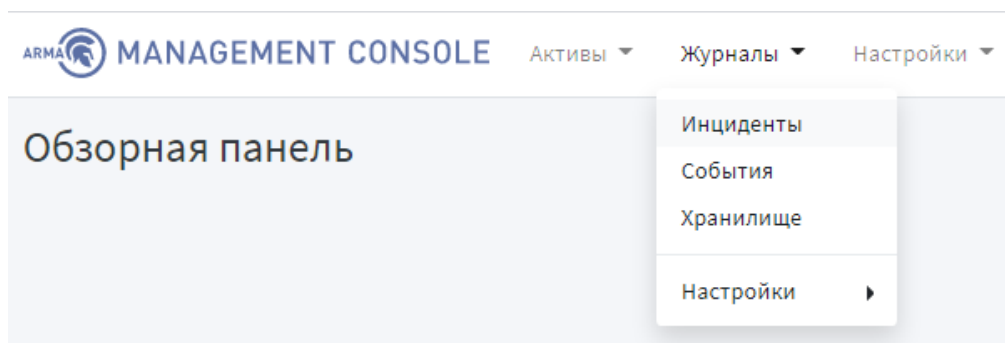




Рисунок 27 – Переход на страницу инцидентов

4.1 Уведомление о нерешенных инцидентах

Кнопка «» в верхнем меню позволяет просматривать все уведомления **ARMA MC**.

При наличии/появлении нерешенных инцидентов появится уведомление об этом.

Для просмотра нерешенных инцидентов, необходимо нажать кнопку «», а затем выбрать уведомление об инцидентах (см. Рисунок 28). При нажатии на уведомление о нерешенных инцидентах **ARMA MC** отобразит страницу «**Журналы**» - «**Инциденты**» (см. Рисунок 29).

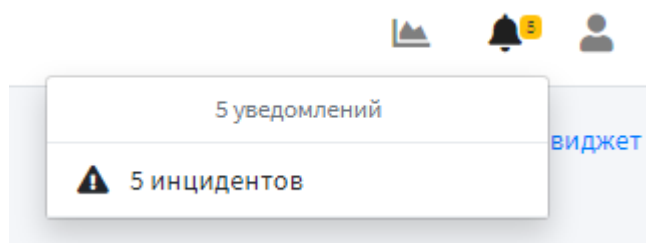


Рисунок 28 – Уведомление об инцидентах

4.2 Описание журнала инцидентов

В журнале инцидентов отображаются инциденты систем защиты, подключенных к **ARMA MC**.

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

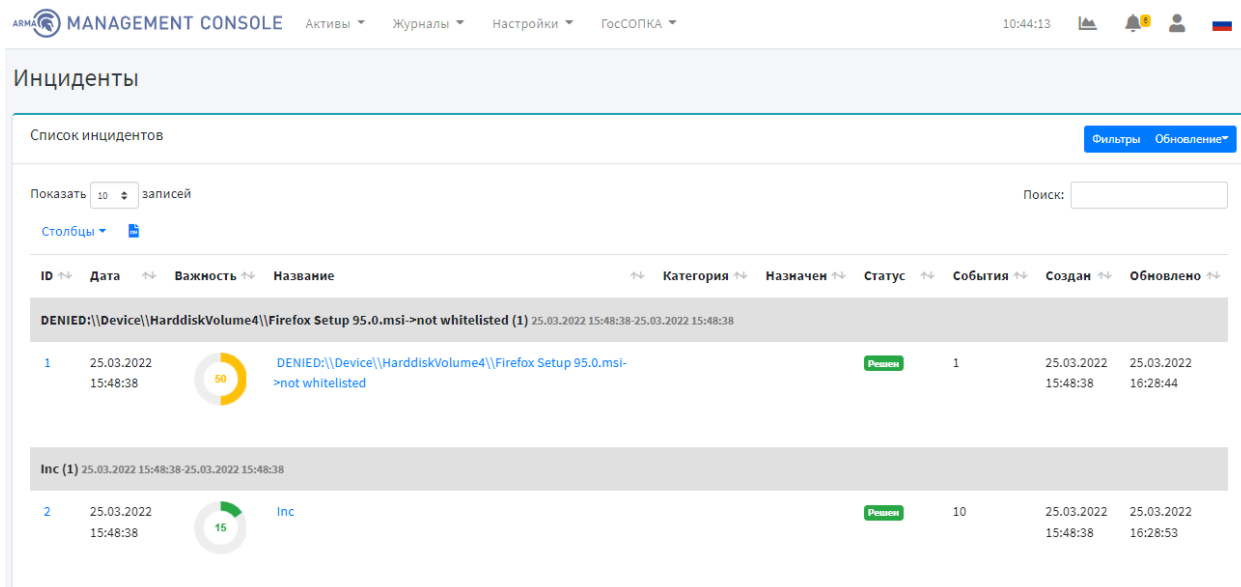


Рисунок 29 – Журнал инцидентов

ARMA MC поддерживает автоматическую группировку инцидентов.

Для выбора промежутка обновления данных таблицы инцидентов необходимо нажать **кнопку «Обновление»** в правом верхнем углу формы и выбрать частоту обновления данных. При выборе частоты обновления данных кнопка сменит вид на «**Обновление: 5 сек**».

Для выбора количества записей, отображаемых в таблице инцидентов необходимо нажать **кнопку «10»** в левом в верхнем углу формы.

4.3 Поиск, сортировка и фильтрация инцидентов

Поле «**Поиск**» вверху таблицы событий 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 **кнопку «Фильтры»**. Всплывающее окно позволяет задать фильтры отображения таблицы инцидентов (см. [Рисунок 30](#)):

- дата;
- важность;
- категория;
- назначен;
- статус.

Фильтры ✕

Дата *

🕒
01.09.2021 00:00:00 - 30.09.2021 23:59:59

Дата и время, когда произошел инцидент

Важность *

0
10
50
100

Уровень опасности инцидента

Категория

⚙️
Нарушение правил доступа
▾

Категория инцидента

Назначен

▾
admin
▾

Пользователь, назначенный на решение инцидента

Статус *



▾
Назначен

Список инцидентов

Сбросить

Применить

Рисунок 30 – Фильтры журнала инцидентов

В поле «**Категория**» необходимо выбрать категорию инцидента или создать новую, нажав **кнопку** «», а затем **кнопку** «» (см. Рисунок 31, Рисунок 32).

Управление категориями инцидентов ✕

Показать 10 записей Поиск:

Столбцы ▾ +

Имя ↕	Описание ↕	Действия ↕
Нарушение правил доступа		✎ 🗑️

Записи с 1 до 1 из 1 записей

Предыдущая
1
Следующая

Рисунок 31 – Управление категориями инцидентов

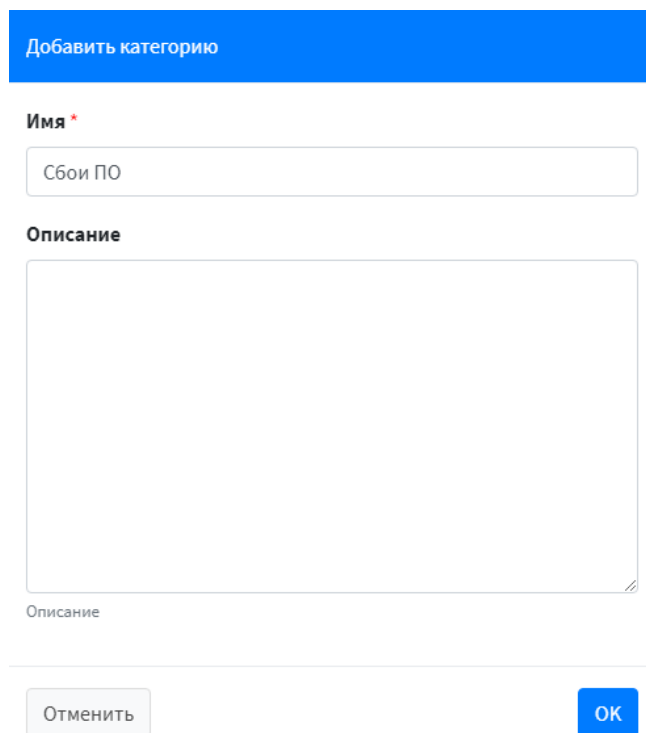



Рисунок 32 – Добавление категории

Для сброса фильтров необходимо нажать **кнопку «Сбросить»**.

Для сохранения и применения фильтров необходимо нажать **кнопку «Применить»**.

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать **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 MC** отобразит страницу подробной информации об инциденте (см. [Рисунок 33](#)). 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.

Далее отображается список событий, из которых сформирован инцидент, представленный в виде таблице со следующей информацией (см. [Рисунок 34](#)).

Затем отображаются рекомендации по закрытию инцидента и последствия инцидента (см. [Рисунок 35](#)).

Для сохранения изменений на странице **«Детали инцидента»** необходимо нажать **кнопку «Сохранить»**.

При решении инцидента необходимо нажать **кнопку «Решить»** или выбрать статус **«Решен»** из выпадающего списка.

Для просмотра подробной информации о системе защиты, с которой был обнаружен инцидент, необходимо нажать **кнопку «Посмотреть систему защиты»**.

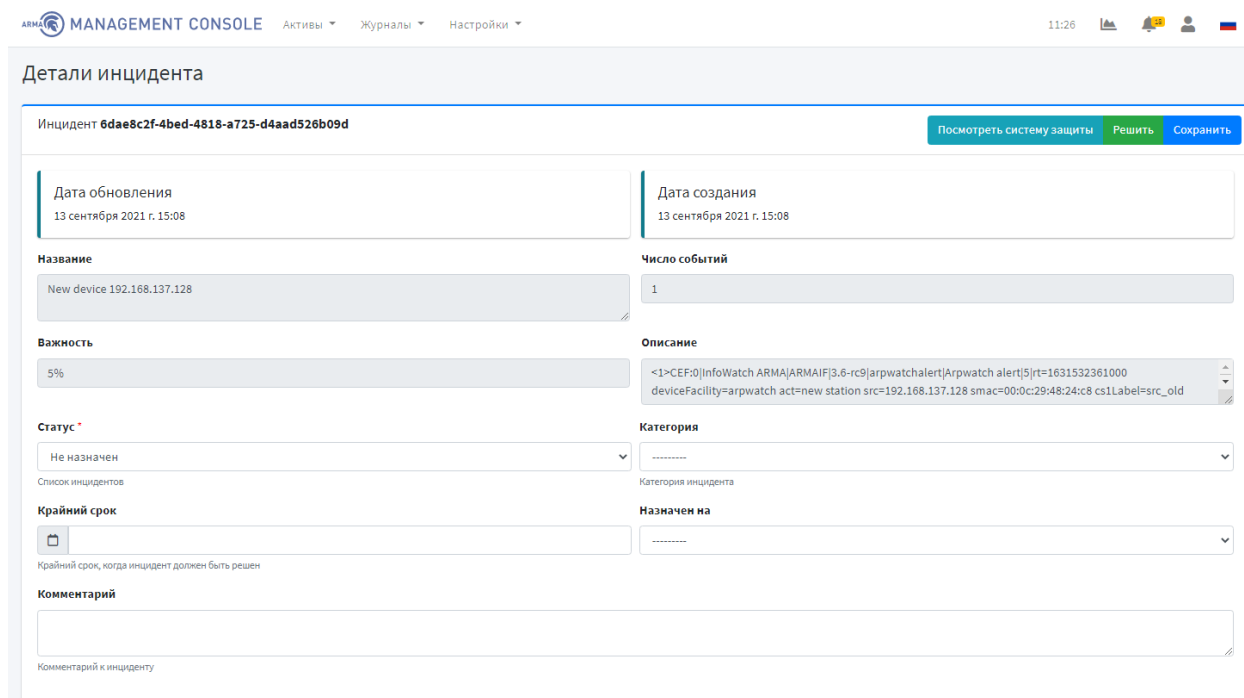


Рисунок 33 – Детали инцидента (1)

События

Показать 10 записей

Поиск:

Столбцы

#	Дата	Сообщение	Продукт	IP источника	IP получателя
0	13.09.2021 14:28:01	New device 192.168.137.128	ARMAIF	192.168.137.128	

Записи с 1 до 1 из 1 записей


Предыдущая 1 Следующая

Рисунок 34 – Детали инцидента (2)

<p>Рекомендации по решению</p> <p>Заблокировать устройство</p>	<p>Последствия инцидента</p> <p>Утечка служебной информации</p>
--	---

Рисунок 35 – Детали инцидента (3)

4.5 Экспорт инцидентов

Для того чтобы скачать таблицу инцидентов необходимо нажать **кнопку** «  » в левом верхнем углу таблицы (см. [Рисунок 29](#)).

4.6 Управление инцидентами

Для работы с инцидентами с помощью **ARMA MC** 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 MC** отобразит страницу подробной информации об инциденте (см. [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 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 MC** отобразит страницу подробной информации об инциденте (см. [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 инцидента и в поле **«Комментарий»** необходимо ввести комментарий к инциденту.

Для сохранения изменений необходимо нажать кнопку **«Сохранить»**.

В случае положительного решения инцидента, отметить инцидент как решенный, нажав кнопку **«Решить»**.

4.7 Просмотр архивов

Страница **«Хранилище»** позволяет просматривать архивы собранных инцидентов и событий (см. [Рисунок 36](#)).

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

Хранилище

CSV экспорт

Показать 10 записей Поиск:

Столбцы ▾

Формат	Создан	Размер (МБ)	Описание	Действия
CSV	14.09.2021 11:24:39	0.03	Exported incident data	
CSV	14.09.2021 11:28:56	0.03	Exported incident data	
CSV	14.09.2021 11:29:00	0.03	Exported incident data	

Записи с 1 до 3 из 3 записей Предыдущая 1 Следующая

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 (см. [Рисунок 37](#)).

MANAGEMENT CONSOLE Активы Журналы Настройки 11:58

Хранилище

Дамп БД CSV экспорт

Показать 10 записей Поиск:

Столбцы ▾

Формат	Создан	Размер (МБ)	Описание	Действия
JSON	14.09.2021 11:35:00	0.04	Table rotation incident	
JSON	14.09.2021 11:40:00	0.01	Table rotation incident	
JSON	14.09.2021 11:45:00	0.00	Table rotation incident	
JSON	14.09.2021 11:50:00	0.00	Table rotation incident	
JSON	14.09.2021 11:55:00	0.00	Table rotation incident	

Записи с 1 до 5 из 5 записей (отфильтровано из 8 записей) Предыдущая 1 Следующая

Рисунок 37 – Хранилище. Дамп БД

Для редактирования описания хранилища необходимо нажать **кнопку** « » напротив соответствующего хранилища и в разделе «**Редактировать**» изменить описание, а затем нажать **кнопку** «**Сохранить**» (см. [Рисунок 38](#)).

Для скачивания архива необходимо нажать **кнопку** « » (см. [Рисунок 36](#)) либо **кнопку** «**Скачать**» (см. [Рисунок 38](#)).

ARMA MANAGEMENT CONSOLE Активы Журналы Настройки 11:59 🔔 👤 🇷🇺

Детали хранилища

Редактировать

Описание

Table rotation incident

Описание

[Сохранить](#)

Просмотреть

Поиск:

Имя	Значение
Формат	JSON
Файл	Скачать
Тип	Дамп БД
Создан	14 сентября 2021 г. 11:35
Размер	36411
Последний доступ	14 сентября 2021 г. 11:35
Дата высвобождения	None
CRC	True

Рисунок 38 – Детали хранилища

5 НАСТРОЙКИ

5.1 Настройка правил корреляции

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

Текущий раздел позволяет создавать и настраивать правила корреляции (см. Рисунок 39).

По умолчанию в **ARMA MC** предустановлено два правила корреляции – «**NewAsset**» и «**Serious event**».

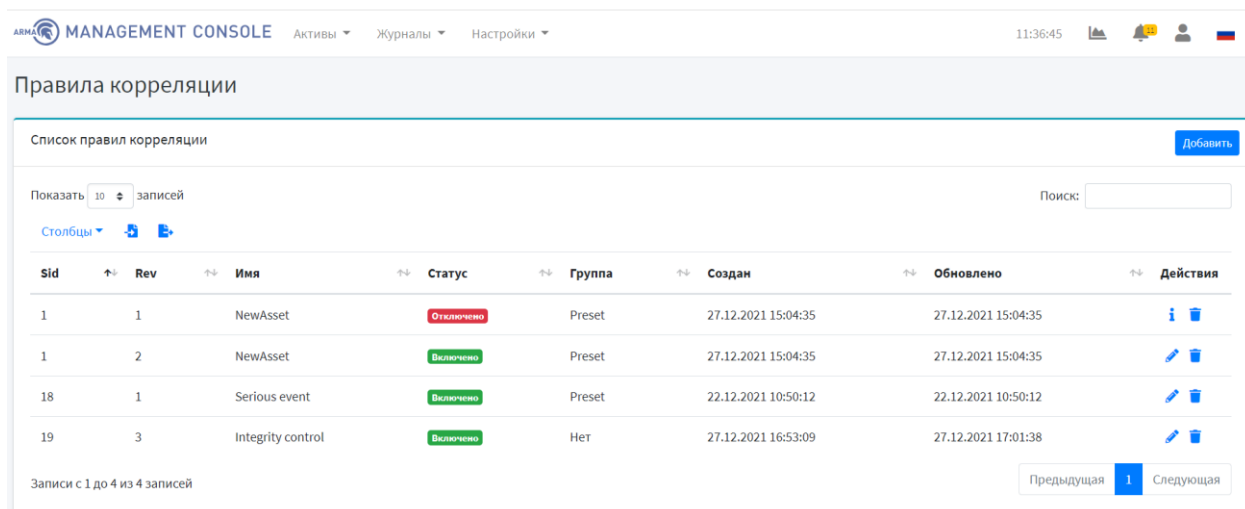


Рисунок 39 – Правила корреляции

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

Так же есть возможность импорта и экспорта правил корреляции.

Для импорта правил корреляции необходимо нажать **кнопку** «», выбрать файл в формате JSON и нажать **кнопку** «**Импорт**» (см. Рисунок 40).

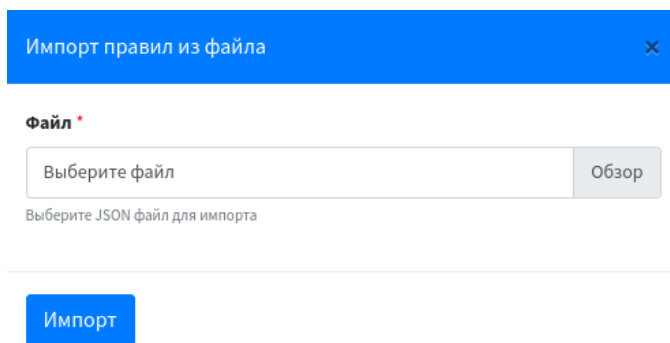


Рисунок 40 – Импорт правил корреляции

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

Отчет по импорту

Показать 10 записей Поиск:

Столбцы

Правило	Статус	Отчет
NewAsset	Импортировано	Правило успешно импортировано
Serious event	Импортировано	Правило успешно импортировано

Записи с 1 до 2 из 2 записей

Предыдущая 1 Следующая

Рисунок 41 – Успешный импорт правил корреляции

Отчет по импорту

Показать 10 записей Поиск:

Столбцы

Правило	Статус	Отчет
NewAsset	Не импортировано	NewAsset не импортировано, так как такое-же правило уже есть в базе данных
Serious event	Не импортировано	Serious event не импортировано, так как такое-же правило уже есть в базе данных



Записи с 1 до 2 из 2 записей

Предыдущая 1 Следующая

Рисунок 42 – Неуспешный импорт правил корреляции

Для экспорта правил корреляции необходимо нажать **кнопку** «».

Для добавления правила корреляции необходимо нажать **кнопку** «**Добавить**».

В блоке «**Базовые настройки**» задаются общие настройки правила – имя, группа, глубина анализа и описание правила (см. Рисунок 46). Группу правила можно выбирать из существующих, а также добавлять новые, нажав **кнопку** «» и затем **кнопку** «» (см. 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).

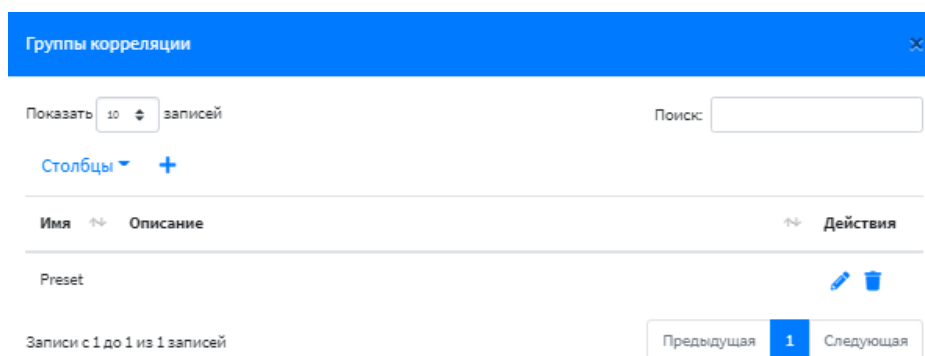


Рисунок 43 – Группы корреляции

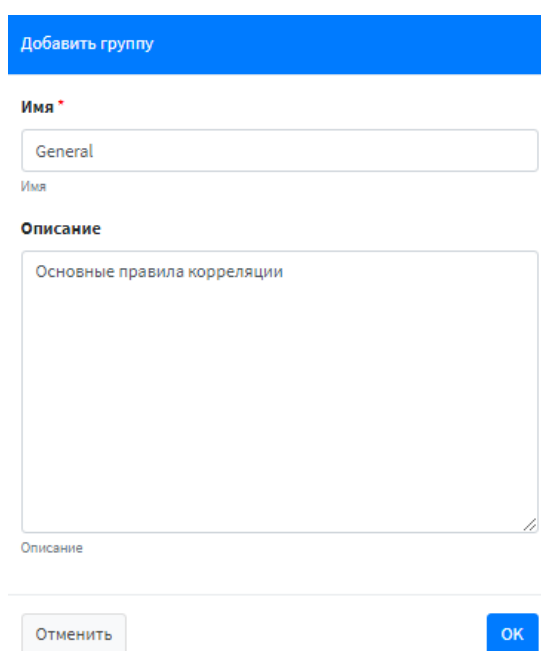


Рисунок 44 – Добавление группы корреляции

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

!Важно Условия задаются на основании деталей события, на которое создается то или иное правило корреляции.

Для проверки срабатывания условия правила корреляции необходимо нажать **кнопку «Проверить»**. Если в списке событий есть подходящие события под заданное условие, то они отобразятся в виде таблицы (см. [Рисунок 45](#)).

Query results ✕

Показать записей

Столбцы ▾

Дата	ID	Сообщение	Критичность	Категория	IP источника	IP получателя
13.09.2021 14:38:07	6fef7ef0-91f5-4f42-a07f-6ebea7735689	New device 192.168.1.200	5	ARPWATCH	192.168.1.200	
13.09.2021 14:34:56	1c15a1ee-5c43-4b90-a32a-2e39ceb29b2b	New device 192.168.137.254	5	ARPWATCH	192.168.137.254	
13.09.2021 14:34:52	11ccba29-2232-4952-9921-ae61eb98187b	New device 192.168.137.128	5	ARPWATCH	192.168.137.128	
13.09.2021 14:34:52	6331cded-0e64-42f4-a849-6a6a9cc16d9b	New device 192.168.137.2	5	ARPWATCH	192.168.137.2	
13.09.2021 14:31:47	0146f23e-ea05-428e-9f6b-a75378754ec1	New device 192.168.137.1	5	ARPWATCH	192.168.137.1	
13.09.2021 14:31:05	7179f235-01d0-45b9-a2b5-42d8d1109703	New device 192.168.1.100	5	ARPWATCH	192.168.1.100	

Рисунок 45 – Результаты проверки срабатывания условий правила корреляции

!Важно 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 **кнопку «Добавить»**, выбрать одно из предложенных действий (см. [Рисунок 47](#)) и нажать **кнопку «Добавить»**.

MANAGEMENT CONSOLE Активы Журналы Настройки 13:58

Правило корреляции

Базовые настройки правила Сохранить

Название *

Группа

Глубина *

Глубина анализа в формате ЧЧ:ММ:СС

SID правила *

SID правила корреляции

Включено
Правило включено?

Множественная реакция
Применить действия к каждому событию, которое соответствует правилу

Описание

Описание

Условия срабатывания правила Помощь Проверить

Запрос *

Рисунок 46 – Добавление правила корреляции

Тип действия ✕

Тип *

- Syslog
- HTTP
- Инцидент
- Bash скрипт
- Запустить исполняемый файл
- Новый актив
- Правило межсетевое экрана

Рисунок 47 – Типы действий

!Важно Для проверки работоспособности правил корреляции необходимо подключиться к **ARMA IF** (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 (см. 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 (см. Рисунок 50).

The screenshot displays the 'Правило корреляции' (Correlation Rule) configuration page in the ARMA IF Management Console. The page is divided into two main sections: 'Базовые настройки правила' (Basic rule settings) and 'Условия срабатывания правила' (Rule triggering conditions).

Базовые настройки правила:

- Название:** Syslog
- Группа:** Preset
- Глубина:** 00:05:00 (Depth of analysis in HH:MM:SS format)
- SID правила:** 1
- Включено:** Checked (Rule is enabled)
- Множественная реакция:** Unchecked (Apply actions to each event that matches the rule)

Условия срабатывания правила:

- Запрос:** device_product: arpwatch and device_action: "new station"

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

Рисунок 49 – Действие «Syslog»

Visual Syslog Server 1.6.3

Time	IP	Host	Facility	Priority	Tag	Message
Mar 02 17:21:13	192.168.1.100		local0	info	2021-03-02T17:21:13+03:00	с ARPWatch
Mar 02 17:21:13	192.168.1.100		local0	info	2021-03-02T17:21:13+03:00	с ARPWatch
Mar 02 17:21:14	192.168.1.100		local0	info	2021-03-02T17:21:14+03:00	с ARPWatch
Mar 02 17:21:14	192.168.1.100		local0	info	2021-03-02T17:21:14+03:00	с ARPWatch
Mar 02 17:21:43	192.168.1.100		local0	info	2021-03-02T17:21:43+03:00	с ARPWatch
Mar 02 17:22:43	192.168.1.100		local0	info	2021-03-02T17:22:43+03:00	с ARPWatch

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

5.1.2 Правило корреляции с типом действия «НТТР»

Действие «НТТР» 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 «НТТР» как показано на рисунках (см. 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 (см. Рисунок 53).

The screenshot displays the 'Правило корреляции' (Correlation Rule) configuration page in the ARMA IF Management Console. The page is divided into two main sections: 'Базовые настройки правила' (Basic rule settings) and 'Условия срабатывания правила' (Rule trigger conditions).

Базовые настройки правила:

- Название:** HTTP
- Группа:** Preset
- Глубина:** 00:05:00 (Depth of analysis in HH:MM:SS format)
- SID правила:** 1
- Включено:** (Rule is enabled)
- Множественная реакция:** (Apply actions to each event that matches the rule)

Условия срабатывания правила:

Запрос: device_product: arpwatch and device_action: "new station"

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

Рисунок 52 – Действие «HTTP»

```

C:\Users\Server\Downloads\http_test.exe
time="2021-03-03T13:32:30+03:00" level=info msg="Starting server on port: 7788"
time="2021-03-03T13:34:33+03:00" level=info msg="Start request from 192.168.1.200:7788"
time="2021-03-03T13:34:33+03:00" level=info msg="Headers:"
time="2021-03-03T13:34:33+03:00" level=info msg="Content-Type: application/json"
time="2021-03-03T13:34:33+03:00" level=info msg="Accept-Encoding: gzip"
time="2021-03-03T13:34:33+03:00" level=info msg="User-Agent: Go-http-client/1.1"
time="2021-03-03T13:34:33+03:00" level=info msg="Content-Length: 319"
time="2021-03-03T13:34:33+03:00" level=info msg="Body:"
time="2021-03-03T13:34:33+03:00" level=info msg="Body: <1>CEF:0|armaif|ARMPwatch|3.5.2_7|New station|arpwatch|5|unixdate=1614767652 log_from=arpwatch cid=None message=new station ip_src=192.168.1.100 ip_src_old=None mac_src=00:0c:29:73:ed:b8 mac_src_old=None mechanic=Arpwatch description=Unauthorized device connection detected with IP: 192.168.1.100, MAC: 00:0c:29:73:ed:b8"
    
```

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

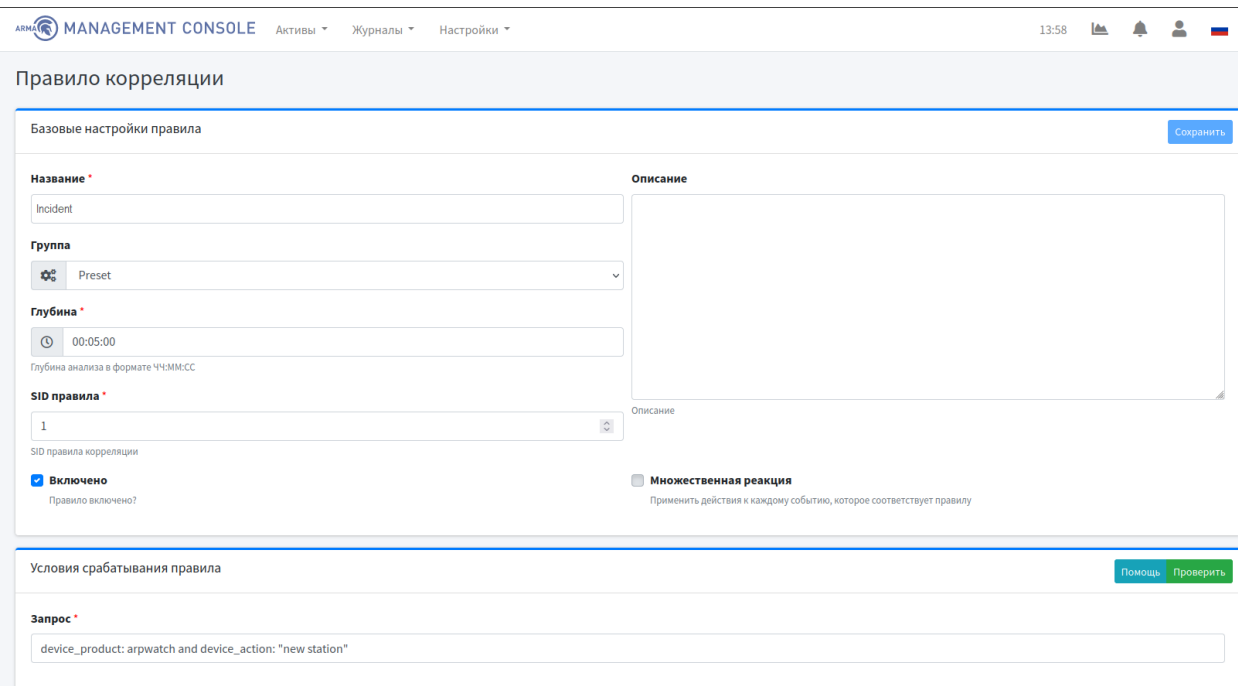
5.1.3 Правило корреляции с типом действия «Инцидент»

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

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «Инцидент» как показано на рисунках (см. 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».

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



MANAGEMENT CONSOLE Активы Журналы Настройки 13:58

Правило корреляции

Базовые настройки правила Сохранить

Название *
Incident

Группа
Preset

Глубина *
00:05:00
Глубина анализа в формате ЧЧ:ММ:СС

SID правила *
1
SID правила корреляции

Включено
Правило включено?

Множественная реакция
Применить действия к каждому событию, которое соответствует правилу

Описание

Описание

Условия срабатывания правила Помощь Проверить




Запрос *
device_product: arpwatch and device_action: "new station"

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 (см. Таблица 5).

Таблица 5
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	

ARMA MANAGEMENT CONSOLE Активы Журналы Настройки

Инциденты

Список инцидентов Фильтры Экспорт Обновление

Показать 10 записей Поиск:

Столбцы

ID	Дата	Важность	Название	Категория	Назначен	Статус	События	Создан	Обновлено
New device 192.168.137.128 (1) 13.09.2021 15:08:11-13.09.2021 15:08:11									
18	13.09.2021 15:08:11	5	New device 192.168.137.128			Не назначен	1	13.09.2021 15:08:11	13.09.2021 15:08:11

Записи с 1 до 1 из 1 записей

Предыдущая 1 Следующая

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 (см. [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 совпадающим по имени сигнатуры самого события, как прописано в сценарии скрипта bash (см. [Рисунок 59](#)).

MANAGEMENT CONSOLE Активы Журналы Настройки 13:58

Правило корреляции

Базовые настройки правила Сохранить

Название *
Bash script

Описание

Группа
Preset

Глубина *
00:05:00
Глубина анализа в формате ЧЧ:ММ:СС

SID правила *
1
SID правила корреляции

Включено
Правило включено?

Множественная реакция
Применить действия к каждому событию, которое соответствует правилу

Условия срабатывания правила Помощь Проверить

Запрос *
device_product: arpwatch and device_action: "new station"

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

Действия Добавить

Действие: Bash скрипт ? x

Тело *

```
#!/bin/bash

# Place you script here
echo "{.SignName}"> /tmp/{.SignName}_.txt
```

Тело bash скрипта

Рисунок 58 – Сценарий Bash скрипта

```
root@debian:/tmp# ls
2021-02-17-15:17:06.txt  hperfdata_logstash
2021-02-17-15:17:36.txt  jruby-387
2021-02-17-15:18:06.txt  pypm-alzuhjiu
2021-02-17-15:18:36.txt  systemd-private-0b2c2fb2bd5c406eac3f83b5f06f81eb-elasticsearch.service-803zII
2021-02-17-15:19:06.txt  systemd-private-0b2c2fb2bd5c406eac3f83b5f06f81eb-redis-server.service-caf70I
2021-02-17-15:19:36.txt  systemd-private-0b2c2fb2bd5c406eac3f83b5f06f81eb-systemd-timesyncd.service-o1Ss2J
hperfdata_elasticsearch  tmux-0
root@debian:/tmp#
```

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 (см. 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 созданся текстовый документ «1.txt» с заданными параметрами из правила корреляции (см. Рисунок 62).

The screenshot shows the 'Правило корреляции' (Correlation Rule) configuration page in the ARMA Management Console. The top navigation bar includes 'MANAGEMENT CONSOLE', 'Активы', 'Журналы', and 'Настройки'. The main content area is titled 'Правило корреляции' and contains two sections:

- Базовые настройки правила** (Basic rule settings):
 - Название *** (Name): Executable file
 - Группа** (Group): Preset
 - Глубина *** (Depth): 00:05:00 (Depth of analysis in HH:MM:SS format)
 - SID правила *** (Rule SID): 1
 - Включено** (Enabled): Правило включено?
 - Множественная реакция** (Multiple reaction): Применить действия к каждому событию, которое соответствует правилу
 - Описание** (Description): Empty text area.
- Условия срабатывания правила** (Rule trigger conditions):
 - Запрос *** (Request): device_product: arpwatch and device_action: "new station"

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

Рисунок 61 – Действие «Запустить исполняемый файл»

```

root@debian:/tmp/1# ls
script.sh
root@debian:/tmp/1# ls
1.txt script.sh
root@debian:/tmp/1# cat 1.txt
AAA BBB RRR /tmp/1
root@debian:/tmp/1# _
    
```

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 IF** отправлять об этом события в журнал событий **ARMA MC**.

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «**Новый актив**» как показано на рисунках (см. [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 (см. Рисунок 65).

The screenshot shows the 'Правило корреляции' (Correlation Rule) configuration page. The 'Базовые настройки правила' (Basic rule settings) section includes:

- Название:** NewAsset
- Группа:** Preset
- Глубина:** 00:05:00 (Depth of analysis in HH:MM:SS format)
- SID правила:** 1
- Включено** (Rule is enabled)
- Множественная реакция** (Apply actions to each event that matches the rule)

The 'Условия срабатывания правила' (Rule trigger conditions) section shows the request: `device_product: arpwatch and device_action: "new station"`.

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

The screenshot shows the 'Действия' (Actions) configuration page for the 'Новый актив' (New Asset) action. The configuration includes:

- Имя:** {{SourceIp}}
- Тип актива:** PC
- Группа:** -----
- Описание:** (Empty text area)
- Производитель:** -----
- Модель:** (Empty text field)
- ОС:** -----
- IP:** {{SourceIp}}
- Порты:** null
- Уязвимости:** (Empty list)

Рисунок 64 – Настройка действия «Новый актив»

MANAGEMENT CONSOLE Активы Журналы Настройки 13:23

Журнал событий

Список событий Помощь 2021-09-13

Показать 10 записей Поиск:

Столбцы

Дата	ID	Сообщение	Критичность	Категория	IP источника	IP получателя
13.09.2021 14:25:06	4d0a7b3b-4f82-4324-b191-cca9585dca95	New device 192.168.1.1	5	ARPCWATCH	192.168.1.1	
13.09.2021 14:25:06	adb2bb5b-277e-484b-a8a9-33859d4d289b	New device 192.168.1.100	5	ARPCWATCH	192.168.1.100	
13.09.2021 14:29:01	2fdac7d8-0a76-41b9-ba85-ce168a107c84	New device 192.168.1.200	5	ARPCWATCH	192.168.1.200	
13.09.2021 14:29:18	2522a35b-9e8a-45df-ac50-f9a8f93e93b6	New device 192.168.137.2	5	ARPCWATCH	192.168.137.2	
13.09.2021 14:34:52	11ccba29-2232-4952-9921-ae61eb98187b	New device 192.168.137.128	5	ARPCWATCH	192.168.137.128	
13.09.2021 14:34:56	1c15a1ee-5c43-4b90-a32a-2e39ceb29b2b	New device 192.168.137.254	5	ARPCWATCH	192.168.137.254	
13.09.2021 14:34:52	6331cde4-0e64-42f4-a849-6a6a9cc16d9b	New device 192.168.137.2	5	ARPCWATCH	192.168.137.2	
13.09.2021 14:24:00	aa728080-2626-4b4f-a71b-e87838df71df	InfoWatch ARMA	0	PF	192.168.1.100	192.168.1.1
13.09.2021 14:24:09	a823ee4a-f4f1-44b5-98ad-4d8ee0a201c3	InfoWatch ARMA	0	PF	127.0.0.1	127.0.0.1
13.09.2021 14:24:01	fd32c5e1-53b9-44bc-9449-cbfa91088b0f	InfoWatch ARMA	0	PF	192.168.1.200	192.168.1.1

Записи с 251 до 260 из 319 записей

Предыдущая 1 ... 25 **26** 27 ... 32 Следующая

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

5.1.7 Правило корреляции с типом действия «Правило межсетевое экрана»

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

Для проверки работоспособности правила необходимо выполнить следующие шаги:

1. Настроить правило корреляции с действием «**Правило межсетевое экрана**» как показано на рисунках (см. [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 IF** («**Межсетевой экран**» - «**API правила**») появилось правило с заданными параметрами (см. [Рисунок 68](#)).

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

MANAGEMENT CONSOLE Активы Журналы Настройки 13:58 🔔 👤 🇷🇺

Правило корреляции

Базовые настройки правила Сохранить

<p>Название * Rule Firewall</p> <p>Группа Preset</p> <p>Глубина * 00:05:00 <small>Глубина анализа в формате ЧЧ:ММ:СС</small></p> <p>SID правила * 1 <small>SID правила корреляции</small></p> <p><input checked="" type="checkbox"/> Включено <small>Правило включено?</small></p>	<p>Описание</p> <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> <p><small>Описание</small></p> <p><input type="checkbox"/> Множественная реакция <small>Применить действия к каждому событию, которое соответствует правилу</small></p>
---	---

Условия срабатывания правила Помощь Проверить

Запрос *
device_product: arpwatch and device_action: "new station"

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

Действия

Действие: Правило межсетевого экрана ? ✕

ARMA IF *
ARMA - ARMAIF

Включено Правило включено? **Быстрое** **Лог** Включить логирование правила

<p>Интерфейсы * IPsec LAN OPT WAN <small>Список интерфейсов, разделенных запятыми</small></p>	<p>Направление * In <small>Направление трафика</small></p>	<p>Приоритет * 1 <small>Приоритет правила</small></p>
--	---	--

<p>Действие * Block <small>Какое действие необходимо выполнить</small></p>	<p>IP протокол * IPv4</p>	<p>Протокол * алу <small>Имя протокола</small></p>
---	--------------------------------------	---

<p>Сеть источника * алу</p>	<p>Порты источника <small>Список портов источника</small></p>
<p><input type="checkbox"/> Отрицание источника</p>	
<p>Сеть назначения * алу</p>	<p>Порты получателя <small>Список портов назначения</small></p>
<p><input type="checkbox"/> Отрицание назначения</p>	

Описание
rule firewall test

Рисунок 67 – Действие «Правило межсетевого экрана»

Межсетевой экран: API правила

Правила

Поиск

Включен	Последовательность	Описание	Команды
<input checked="" type="checkbox"/>	1	rule firewall test	

Показаны с 1 по 1 из 1 записей

Применить

Редактировать правило

расширенный режим справка

включен

Последовательность: 1

Действие: Блокирование

Быстрая проверка

Интерфейс: LAN ✖ Очистить все

Направление: Вх.

Версии TCP/IP: IPv4

Протокол: любой

Отправитель: any

Источник / Инвертировать:

Получатель: any

Получатель / инвертировать:

Порт назначения:

Шлюз: отсутствует

Журналирование:

Описание: rule firewall test

Отменить Сохранить

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 по двум типам:


- по времени (день/неделя/месяц) (см. Рисунок 69);
- по размеру (см. Рисунок 70).

Рисунок 69 – Настройки ротации инцидентов/событий по времени

Рисунок 70 – Настройки ротации инцидентов/событий по размеру

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

!Важно При срабатывании ротации инцидентов ротируются инциденты только со статусом «Решен» и «Ложное срабатывание».

При настройке ротации событий, нажав кнопку «», появится окно справки (см. Рисунок 71).



При срабатывании ротации событий индекс текущего дня не удаляется

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** (см. Рисунок 72).

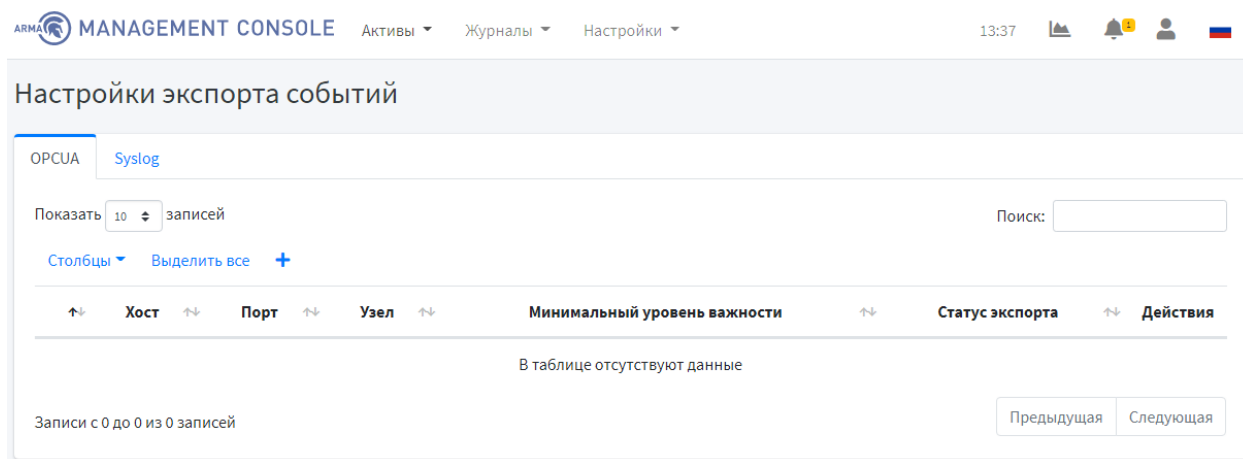


Рисунок 72 – Страница экспорта событий

Для настройки экспорта событий по протоколам OPC UA и Syslog необходимо добавить получателя, нажав **кнопку «+»**.

В открывшейся форме заполнить поля, указав минимальный уровень важности события для отправки, протокол отправки/номер узла, IP-адрес и порт получателя и нажать **кнопку «Добавить»** (см. Рисунок 73, Рисунок 74).

Добавить нового получателя syslog
✕

Протокол отправки *

▼

Выбрать протокол отправки

IP-адрес получателя *

Ввести IP-адрес получателя

Порт получателя *

Ввести порт получателя

Добавить

Рисунок 73 – Добавление получателя (Syslog)

Добавить нового получателя OPC-UA
✕

OPC UA номер узла *

Ввести OPC UA номер узла

IP-адрес получателя *

Ввести IP-адрес получателя

Порт получателя *

Ввести порт получателя

Добавить

Рисунок 74 – Добавление получателя (OPC-UA)

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 MC**)
- **<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-2d18bbbed47a9 cs1Label=IncidentID
start=1638432975000 end=1638432975000
```

!Важно 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 MC** по протоколу **HTTPS**.

Блок настроек «**TLS сертификат**» позволяет включить TLS, генерировать сертификат безопасности и ключ к нему (см. [Рисунок 75](#)).

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

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 кнопку «Создать новый».

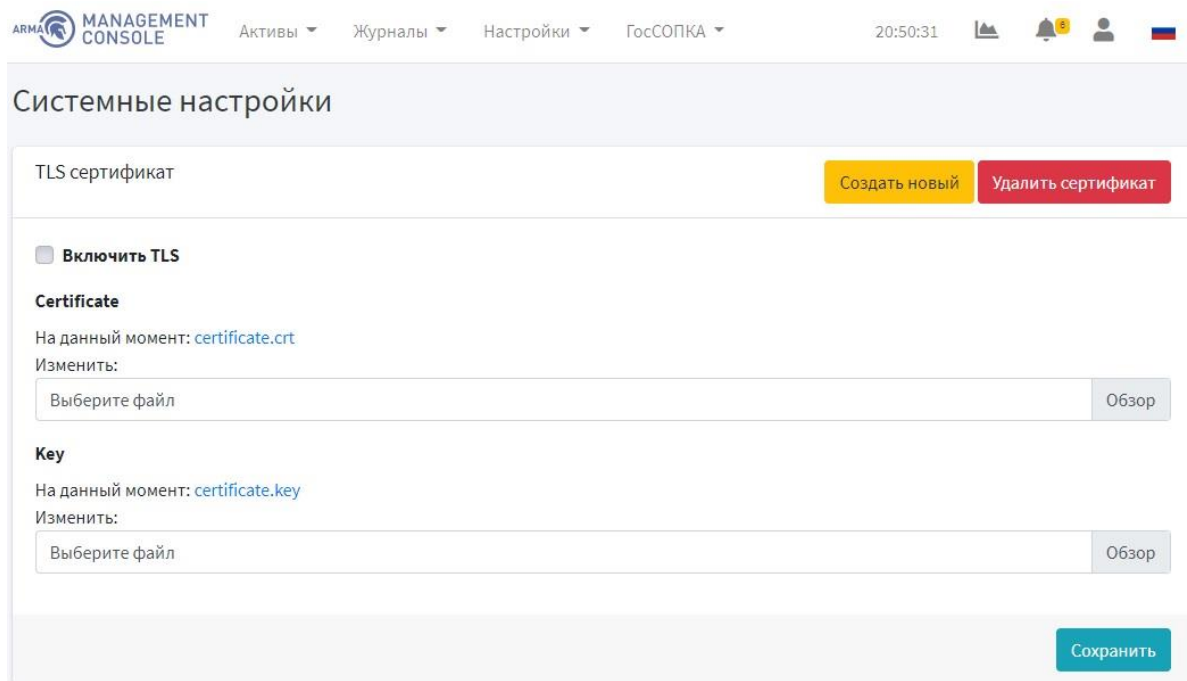


Рисунок 75 – Системные настройки. TLS сертификат

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 (см. Рисунок 76). Значение количества допустимых попыток входа в систему должно быть больше либо равно 0.

!Важно По прошествии времени, указанного в поле «**Тайм-аут попыток аутентификации**», пользователю снова будет доступен вход в систему.

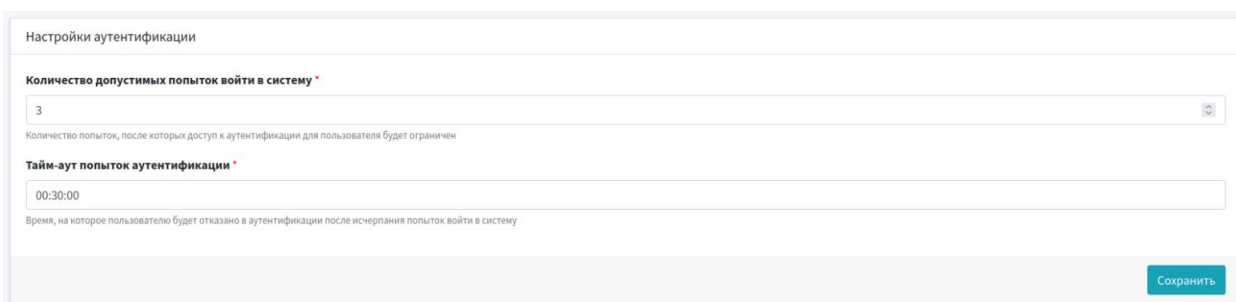


Рисунок 76 – Системные настройки. Настройки аутентификации

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 (см. [Рисунок 77](#)):

- основную информацию;
- функционал лицензии;
- опции лицензии.

The screenshot shows the 'Лицензия' (License) page in the ARMA Management Console. The page is divided into three main sections:

- Информация о лицензии** (License Information): A table with columns 'Имя' (Name) and 'Значение' (Value).

Имя	Значение
Тип	ENTERPRISE
Продукт	ARMA Console
Покупатель	Testers
Начало действия	2022-04-26T05:48:18.336562Z
Конец действия	2022-05-26T05:48:18.336562Z
- Функционал лицензии** (License Functionality): A list of options, including 'Обработка событий' (Event Processing) which is checked.
- Опции лицензии** (License Options): A table with columns 'Имя' (Name), 'Значение' (Value), and 'Описание' (Description).

Имя	Значение	Описание
Источники событий	10	Количество источников событий

Рисунок 77 – Информация о действующей лицензии

В **ARMA MC** предусмотрены следующие типы лицензий:

1. ENTERPRISE базовая. Предоставляет доступ ко всем функциям **ARMA MC**, 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 MC**, 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 MC**. Срок лицензии ограничен.

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

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»** (см. Рисунок 78).

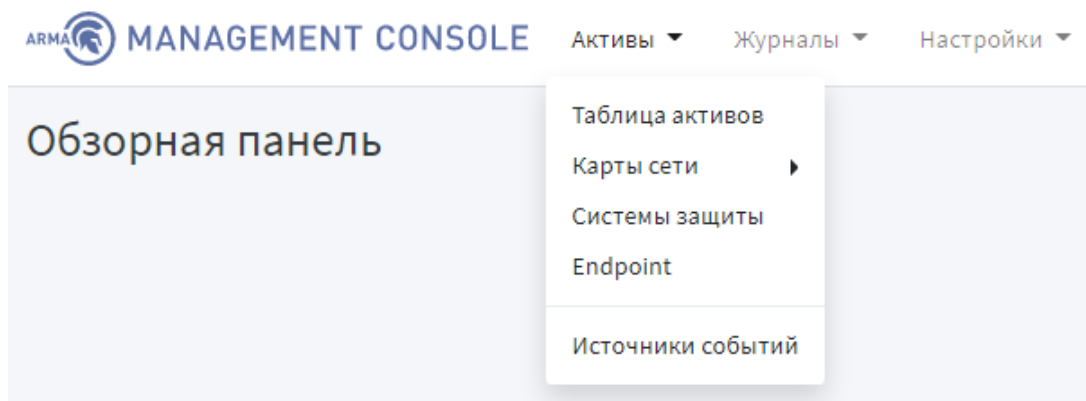








Рисунок 78 – Переход на страницу систем защиты

6.1 Описание таблицы систем защиты

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

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

Системы защиты

Список систем защиты Добавить устройство

Показать записей Поиск:

[Столбцы](#) [Выделить все](#)

Статус	Имя узла	IP-адрес	Действия
<input type="checkbox"/>	ARMA	192.168.1.1	

Записи с 1 до 1 из 1 записей Предыдущая **1** Следующая

Рисунок 79 – Системы защиты

Для выбора количества записей, отображаемых в таблице систем защиты на странице «Активы» - «Системы защиты» необходимо нажать на кнопку « 10 » в левом в верхнем углу формы.

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 кнопку «Столбцы» в левом верхнем углу формы.



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

- «»: загрузка конфигурации на устройство;
- «»: загрузка баз решающих правил СОВ;
- «»: удаление системы защиты из списка.

Для применения действий ко всем системам защиты необходимо нажать 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:

- «»: 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 **кнопку «Добавить устройство»**.

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

Добавить узел
✕

Имя *

Устройство будет отображено под этим именем

IP *

IP-адрес устройства

Ключ *

API ключ для устройства

Секрет *

Значение секрета для API ключа

Комментарий

Дополнительные заметки об устройстве

Создать источник

Создать источник логов для сенсора

Порт

Порт для логов источника (UDP)

Отменить

Добавить

Рисунок 80 – Добавление нового устройства

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.

Для создания источника события для системы защиты необходимо поставить галочку в поле **«Создать источник»** и в поле **«Порт»** указать порт для входящих логов.

!Важно В поле «**Порт**» необходимо указать любой произвольный, но свободный порт, начиная с 1500.


Для сохранения информации и добавления системы защиты необходимо нажать **кнопку «Добавить»**.


Для отмены добавления нового устройства необходимо нажать **кнопку «Отменить»**.

При добавлении системы защиты **ARMA MC** выполняет проверку совместимости версий продуктов. В случае, если версии продуктов не совместимы, отобразится уведомление об этом (см. [Рисунок 157](#)).

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 кнопку «» напротив системы защиты, которую собираетесь удалить и подтвердить удаление во всплывающем окне.

Для удаления нескольких систем защиты в таблице систем защиты необходимо выбрать несколько систем защиты (для выбора всех систем защиты нажать **кнопку «Выделить все»** сверху таблицы) и нажать **кнопку «»** сверху таблицы и подтвердить удаление во всплывающем окне.

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 **кнопку «»** напротив системы защиты. Всплывающее окно позволяет изменить необходимую информацию системы защиты (см. [Рисунок 81](#)).

Редактировать узел
✕

Имя *

Устройство будет отображено под этим именем

IP *

192.168.1.1

IP-адрес устройства

Ключ *

API ключ для устройства

Секрет *

Значение секрета для API ключа

Комментарий

Дополнительные заметки об устройстве

Редактировать связанный источник событий

Отменить

Сохранить

Рисунок 81 – Окно редактирования системы защиты

Для сохранения изменения информации о системе защиты необходимо нажать кнопку **«Сохранить»**.

Для отмены изменений необходимо нажать **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 **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 **кнопку «Выделить все»**) и нажать **кнопку** «» сверху таблицы и выбрать файл


конфигурации. При успешной загрузке конфигурации на систему/системы защиты в верхнем правом углу страницы появится уведомление об этом.

!Важно После загрузки файла конфигурации необходимо перезагрузить систему защиты.

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

!Важно ARMA IF по умолчанию не содержит дополнительных правил СОВ в связи с чем есть вероятность скачивания пустого файла архива.

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 **кнопку «Выделить все»**) и нажать **кнопку**  **»** сверху таблицы и 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 IF

Для успешной обработки событий от **ARMA IF** в **ARMA MC** необходимо чтобы дата и время были точно синхронизированы между устройствами.

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

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

!Важно Для взаимодействия **ARMA MC** (версий 1.3.x) и **ARMA IF** необходимо, чтобы **ARMA IF** был подключен по протоколу HTTPS.

6.7.1 Создание пользователя

В **ARMA IF** перейти в раздел доступа к системе (**«Система» - «Доступ» - «Пользователи»**) и нажать **кнопку «Добавить»**.

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 кнопку «**→**», добавить группу для создаваемого пользователя и нажать кнопку «**Сохранить**».

После сохранения данных страница с настройками обновится и появится возможность добавления ключа API.

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

6.7.2 Добавление устройства защиты

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

!Важно В поле «**Порт**» необходимо указать любой произвольный, но свободный порт, начиная с 1500.

Добавить узел

Имя *
 ARMA
 Устройство будет отображено под этим именем

IP *
 192.168.1.1
 IP-адрес устройства

Ключ *
 kLmXF0AkRuYgqbkWkmKZ64iZ9SEHQjLjcnwArCalW
 API ключ для устройства

Секрет *
 KQ9DipkwPbhivDvQEMn273GbmWyv40o3i2oCHtPv
 Значение секрета для API ключа

Комментарий
 Дополнительные заметки об устройстве

Создать источник
 Создать источник логов для сенсора

Порт
 1500
 Порт для логов источника (UDP)

Отменить Добавить

Рисунок 82 – Добавление нового устройства

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

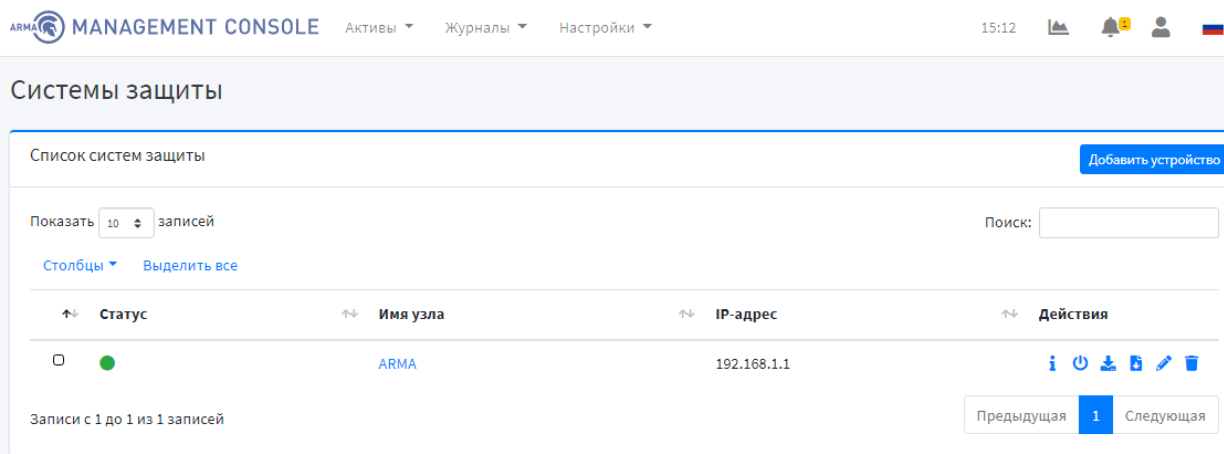


Рисунок 83 – Список систем защиты

6.7.3 Настройка экспорта событий по Syslog

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

!Важно В поле «Имя хоста» необходимо прописывать заданный адрес ARMA MC.

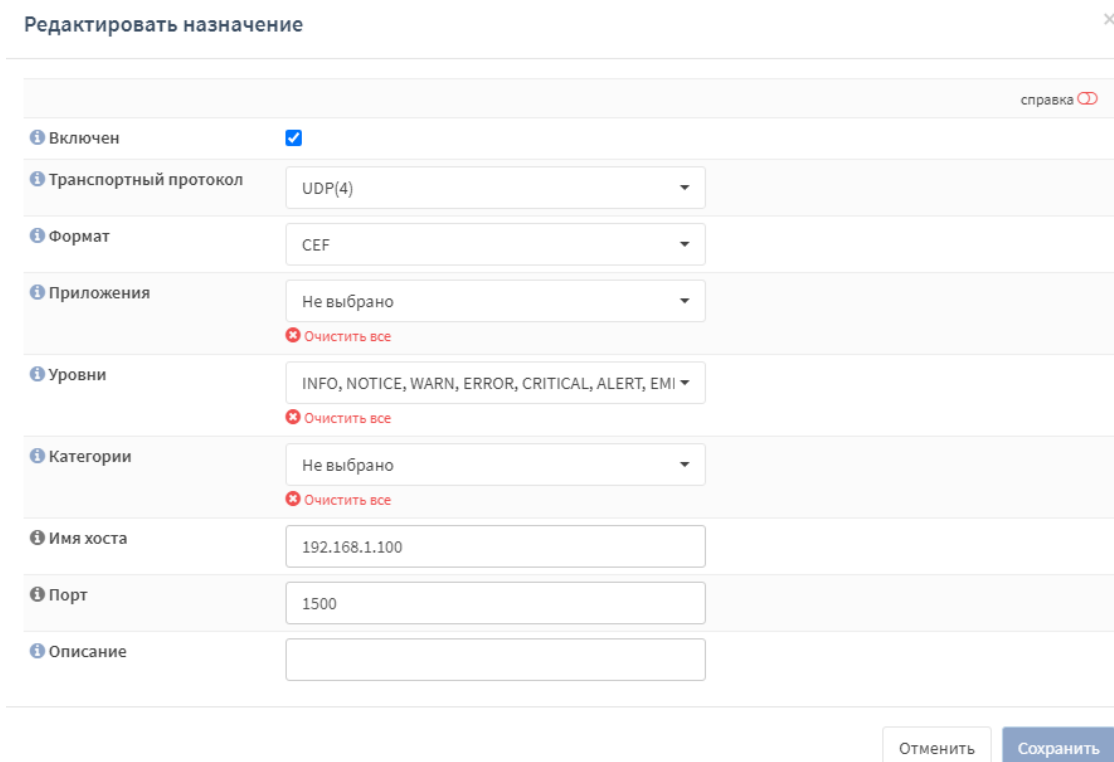


Рисунок 84 – Настройка экспорта событий по Syslog

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**» (см. Рисунок 85).

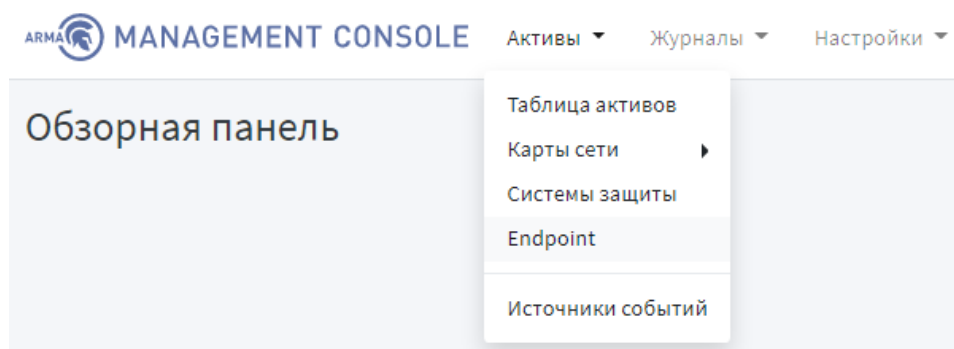







Рисунок 85 – Переход на страницу Endpoint

7.1 Описание таблицы Endpoint

Страница «**Endpoint**» позволяет просматривать Endpoint в формате таблицы, которая содержит следующие данные (см. Рисунок 86):

- a. ID;
- b. статус;
- c. имя;
- d. обновлено;
- e. действия:
 - «  »: копирование конфигурации Endpoint;
 - «  »: скачивание конфигурации Endpoint;
 - «  »: обновление конфигурации с Endpoint;
 - «  »: редактирование Endpoint;
 - «  »: удаление Endpoint из списка.

Endpoint

Список endpoint Добавить

Показать записей Поиск:

Столбцы ▾

ID	Статус	Имя	Обновлено	Действия
1	●	Endpoint	10.11.2021 14:13:27	

Записи с 1 до 1 из 1 записей Предыдущая **1** Следующая

Рисунок 86 – Endpoint

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

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 кнопку « » рядом с названием соответствующего столбца.

Для изменения столбцов, отображаемых в таблице, необходимо нажать 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 (см. Рисунок 158).

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», нажать **кнопку «Добавить»** и ввести необходимую информацию (см. Рисунок 87, Рисунок 88).

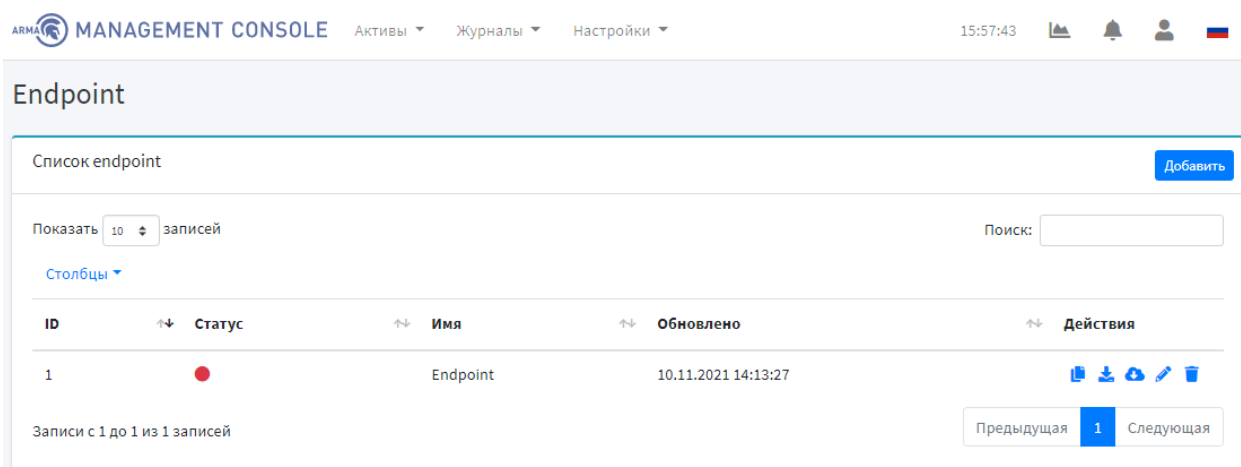


Рисунок 87 – Страница Endpoint

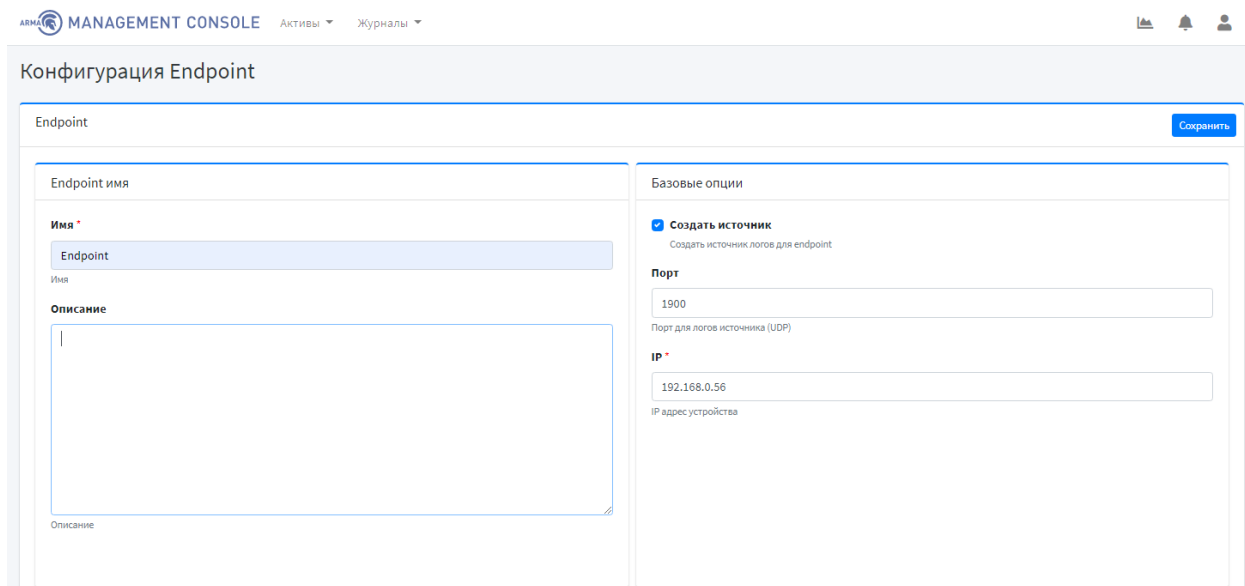


Рисунок 88 – Добавление Endpoint

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 (см. Рисунок 89).

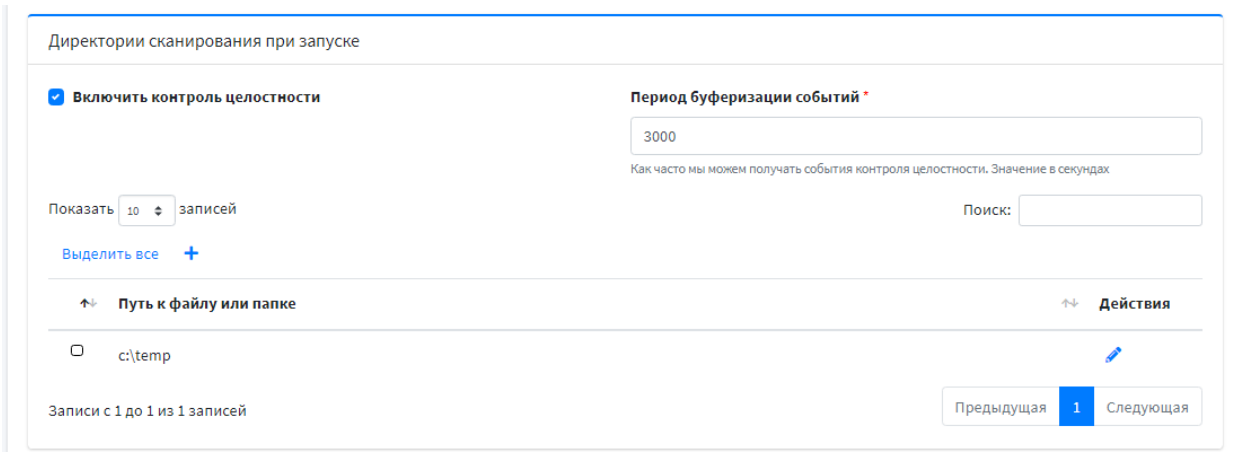


Рисунок 89 – Добавление Endpoint. Директории сканирования при запуске

В блоке **«Белый список приложений»** необходимо указать путь к файлу или папке, доступ, к которому будет разрешен. По умолчанию заданы пути, указанные на рисунке (см. Рисунок 90).

Для включения белого списка необходимо установить галочку в соответствующем поле **«Включить белый список»**.

Для разрешения локальному администратору игнорировать белый список в поле **«Локальный администратор игнорирует белый список»** установлена галочка, которая не подлежит изменению (см. Рисунок 90).

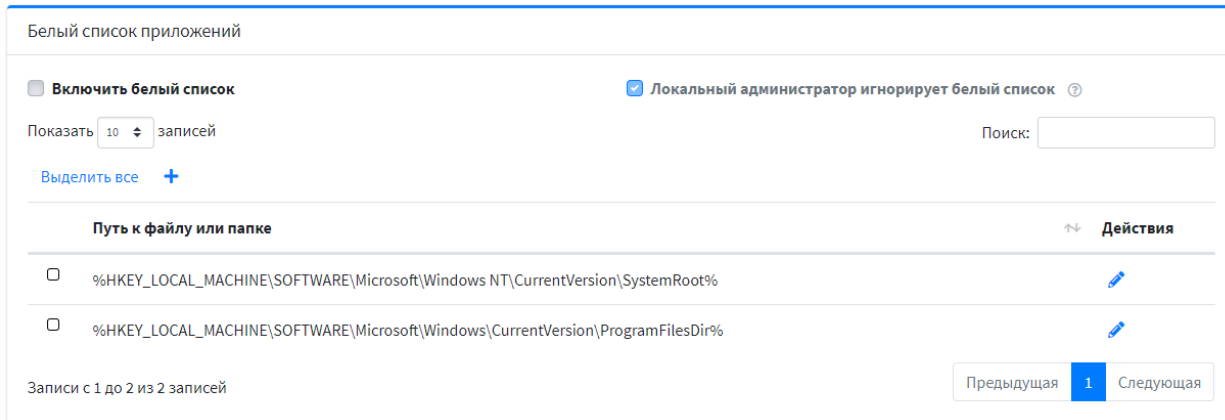


Рисунок 90 – Добавление Endpoint. Белый список приложений

Блок **«Настройки управления устройствами»** позволяет управлять контролем устройств (см. Рисунок 91).

Для включения контроля устройств и USB устройств необходимо установить галочку в соответствующем поле **«Включить управление устройствами»**.

Для запрета чтения и записи CD/DVD или USB необходимо установить галочку в поле **«Запрет доступа на чтение CD/DVD»** или **«Блокировка USB устройств»**.

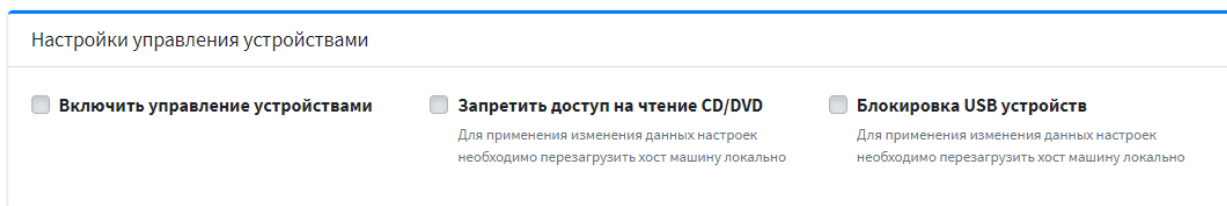


Рисунок 91 – Добавление Endpoint. Настройки управления устройствами

Блок «**Настройки ротации событий**» позволяет настраивать ротацию событий **ARMA IE** по двум типам (см. Рисунок 92):

- по времени (каждый день/неделя/месяц);
- по размеру.

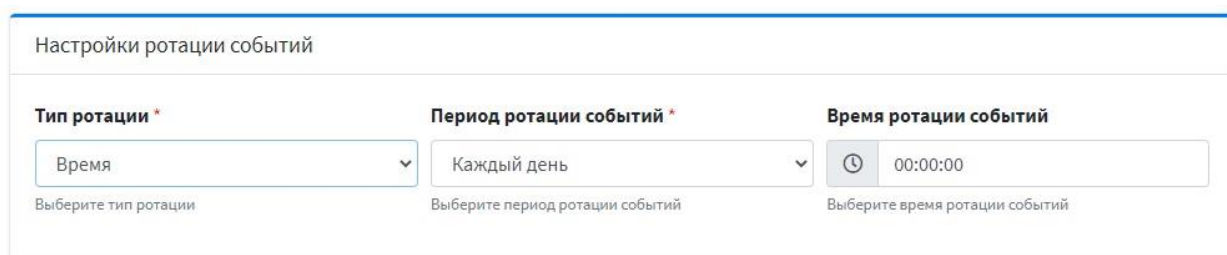


Рисунок 92 – Добавление Endpoint. Настройки ротации событий

Блок «**Настройки антивируса**» позволяет включать/отключать антивирус и добавлять пути сканирования (см. Рисунок 93).

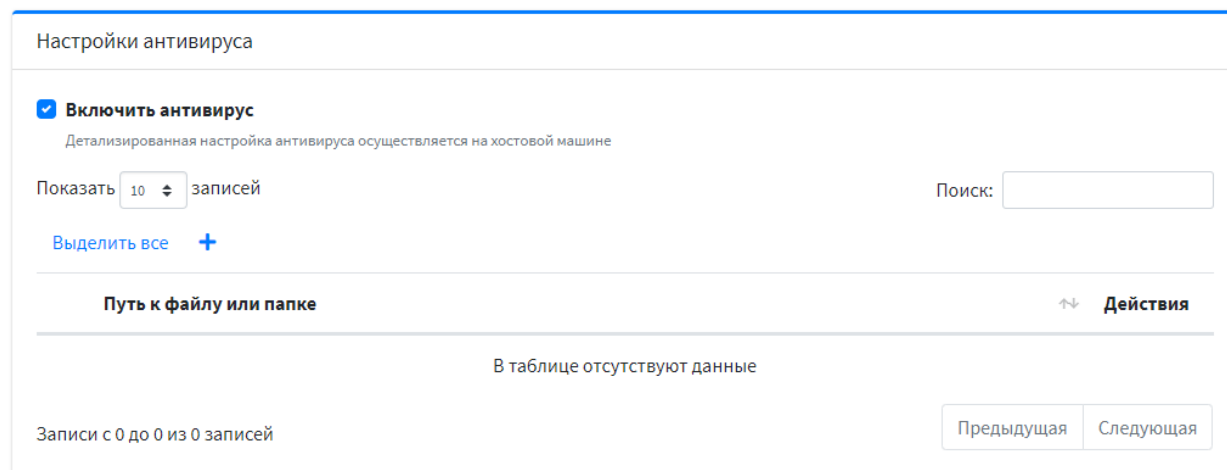



Рисунок 93 – Добавление Endpoint. Настройки антивируса


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 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 кнопку **«**  **»** напротив Endpoint.

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

!Важно При копировании конфигурации Endpoint порт нового источника событий будет отличаться от исходного на +1.

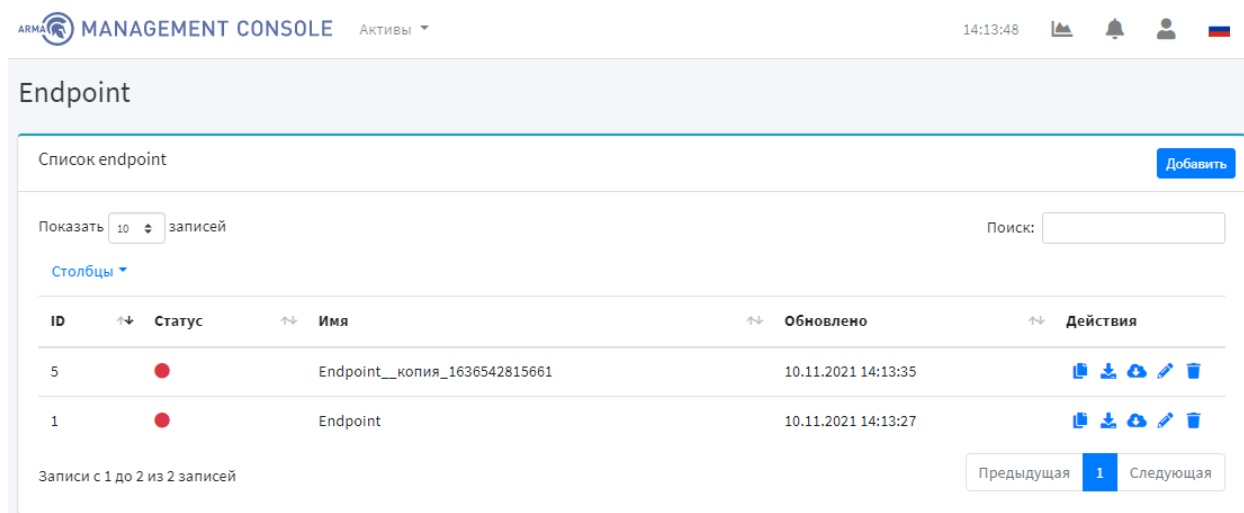



Рисунок 94 – Копирование конфигурации Endpoint

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 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 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 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» (см. Рисунок 95).

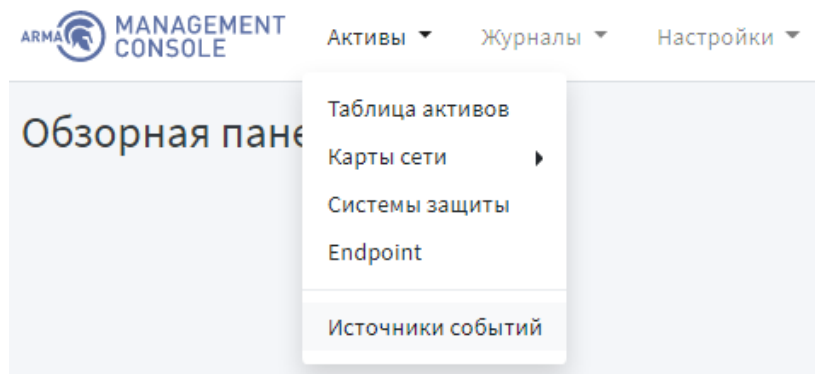


Рисунок 95 – Переход на страницу источников событий

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

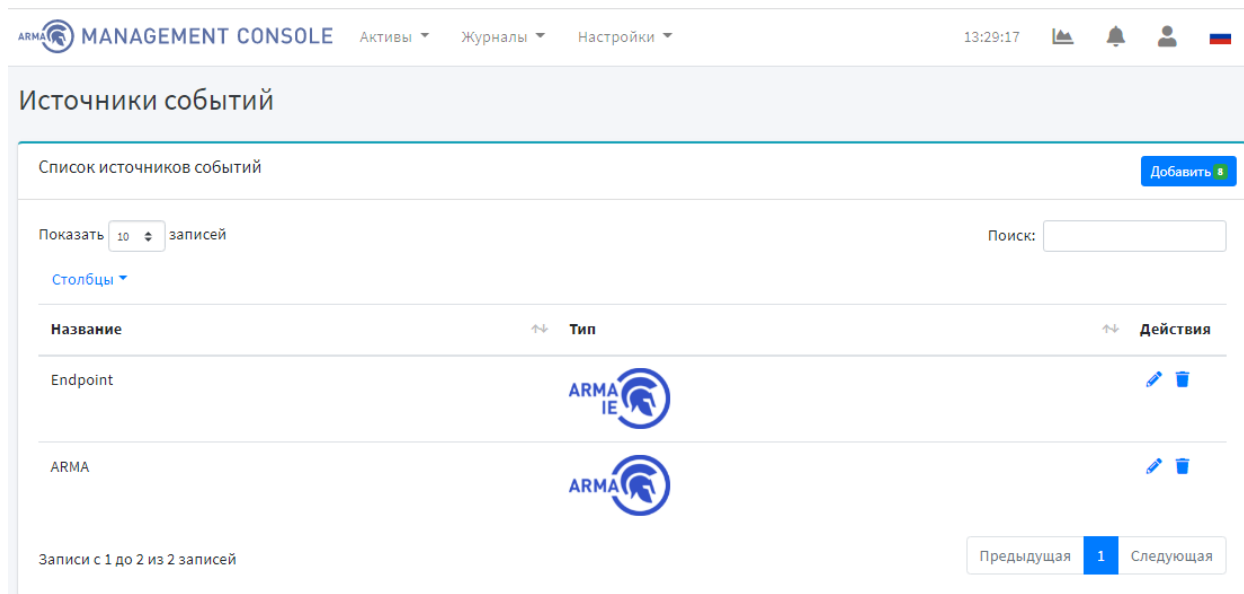


Рисунок 96 – Список источников логов

8.1 Добавление источника события

Для создания источника события необходимо нажать кнопку «Добавить», указать имя и тип источника логов и в поле «Настройка даты и времени» выбрать параметр «локальный» или «без изменений» (см. Рисунок 97).

ARMA MANAGEMENT CONSOLE Активы ▾ Журналы ▾ Настройки ▾ 15:56 [Icons]

Тип источника

Имя * Тип * Настройка даты и времени *

ARMA ARMA IF Локальный

Название источника Тип источника логов

Следующий

Рисунок 97 – Добавление источника события

Для перехода на второй шаг («Входные данные логов ARMA IF») необходимо нажать **кнопку «Следующий»**, указать номер порта источника и затем нажать **кнопку «Сохранить»** (см. Рисунок 98).

Для возврата к предыдущему шагу необходимо нажать **кнопку «Предыдущий шаг»**.

ARMA MANAGEMENT CONSOLE Активы ▾ Журналы ▾ Настройки ▾ 16:00 [Icons]

Входные данные логов ARMA IF

Порт *

1700

Номер порта источника (UDP)

Предыдущий шаг Сохранить

Рисунок 98 – Входные данные логов ARMA IF

9 УПРАВЛЕНИЕ СПИСОКОМ 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**» (см. Рисунок 99).

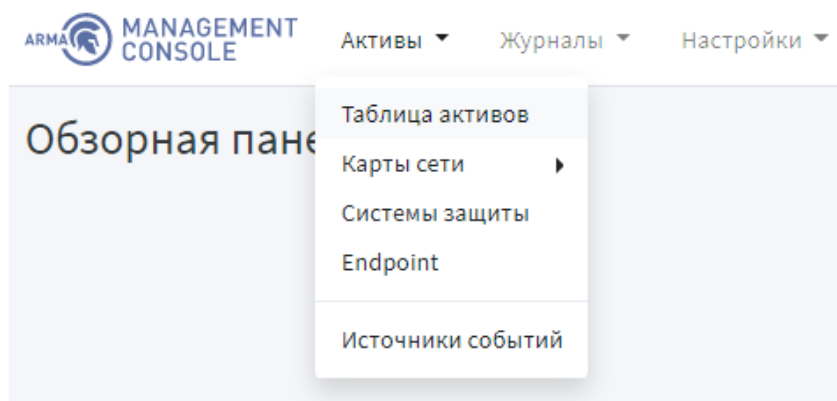



Рисунок 99 – Переход на страницу таблицы активов

9.1 Описание таблицы устройств сети

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


Имя	Статус	Тип	Группа	IP	Проблемы	Обновлено
ARMA	Незарегистрированный			192.168.1.1	!	13.09.2021 15:08:11
192.168.1.1	Незарегистрированный			192.168.1.1	!	13.09.2021 15:08:11
192.168.1.100	Незарегистрированный			192.168.1.100	✓	13.09.2021 14:46:23
192.168.137.128	Незарегистрированный			192.168.137.128	!	13.09.2021 15:08:11
89.110.32.178	Незарегистрированный			89.110.32.178	✓	13.09.2021 14:29:22
fe80::20c:29ffe48:24be	Незарегистрированный			fe80::20c:29ffe48:24be	✓	13.09.2021 14:22:00
ff02::1	Незарегистрированный			ff02::1	✓	13.09.2021 14:22:00
173.194.73.95	Незарегистрированный			173.194.73.95	✓	13.09.2021 14:22:00
188.225.9.167	Незарегистрированный			188.225.9.167	✓	13.09.2021 14:22:00
216.239.38.10	Незарегистрированный			216.239.38.10	✓	13.09.2021 14:22:00

Рисунок 100 – Таблица активов

Для выбора количества записей, отображаемых в таблице необходимо нажать кнопку «  » в левом верхнем углу формы.

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**».

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

Для фильтрации по определенным столбцам таблицы событий необходимо нажать кнопку «**Фильтры**». Всплывающее окно позволяет задать фильтры отображения таблицы активов (см. [Рисунок 101](#)):

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

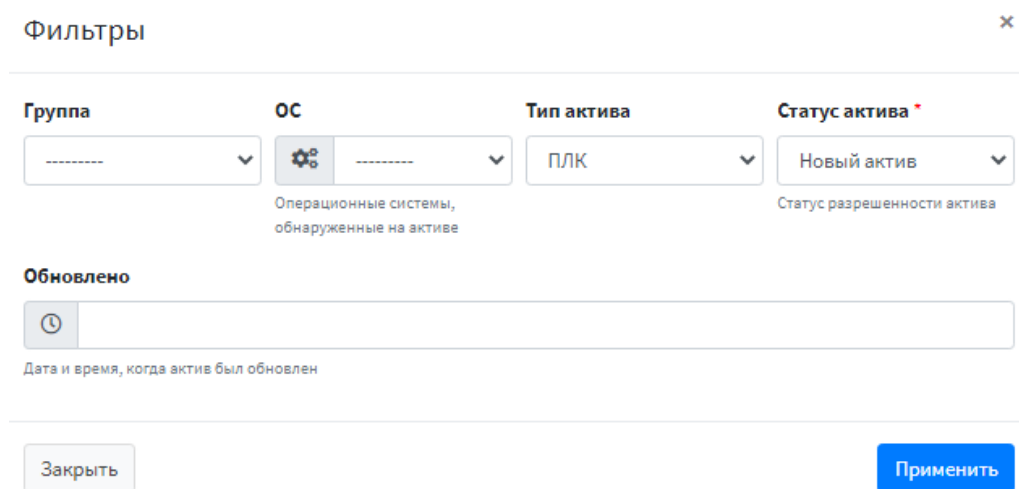




Рисунок 101 – Фильтрация списка активов

В поле «**ОС**» необходимо выбрать операционную систему устройства сети или добавить новую, нажав кнопку «  », а затем кнопку «  » (см. [Рисунок 102](#), [Рисунок 103](#)).

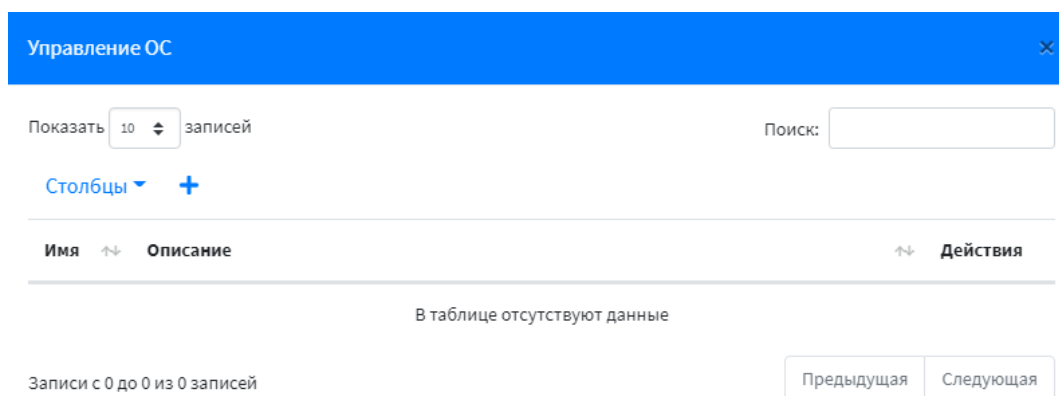


Рисунок 102 – Управление ОС

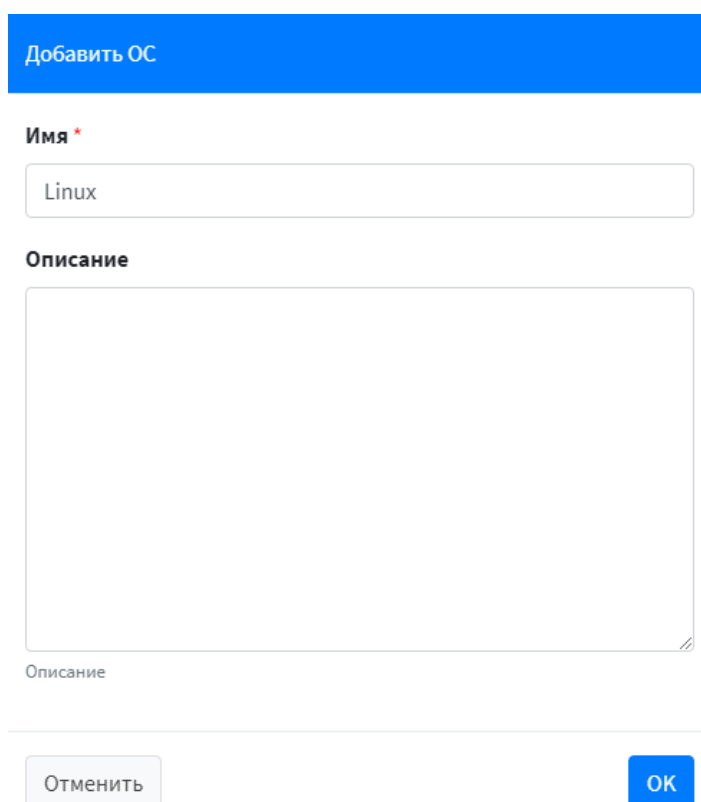


Рисунок 103 – Добавление ОС

Для сохранения и применения фильтров необходимо нажать **кнопку «Применить»**.

Для закрытия окна задания фильтра необходимо нажать **кнопку «Закрыть»**.

9.3 Редактирование основной информации об устройстве сети

Для редактирования основной информации об устройстве необходимо перейти на страницу **«Активы» - «Таблица активнов»**. В таблице активнов необходимо нажать на ссылку названия этого устройства сети в столбце **«Имя»**, например, [192.168.1.1](#). При нажатии на название устройства сети **ARMA MC** отобразит страницу подробной информации об устройстве, которую можно редактировать (см. [Рисунок 104](#)).

Для сохранения изменений необходимо нажать **кнопку «Сохранить»**.

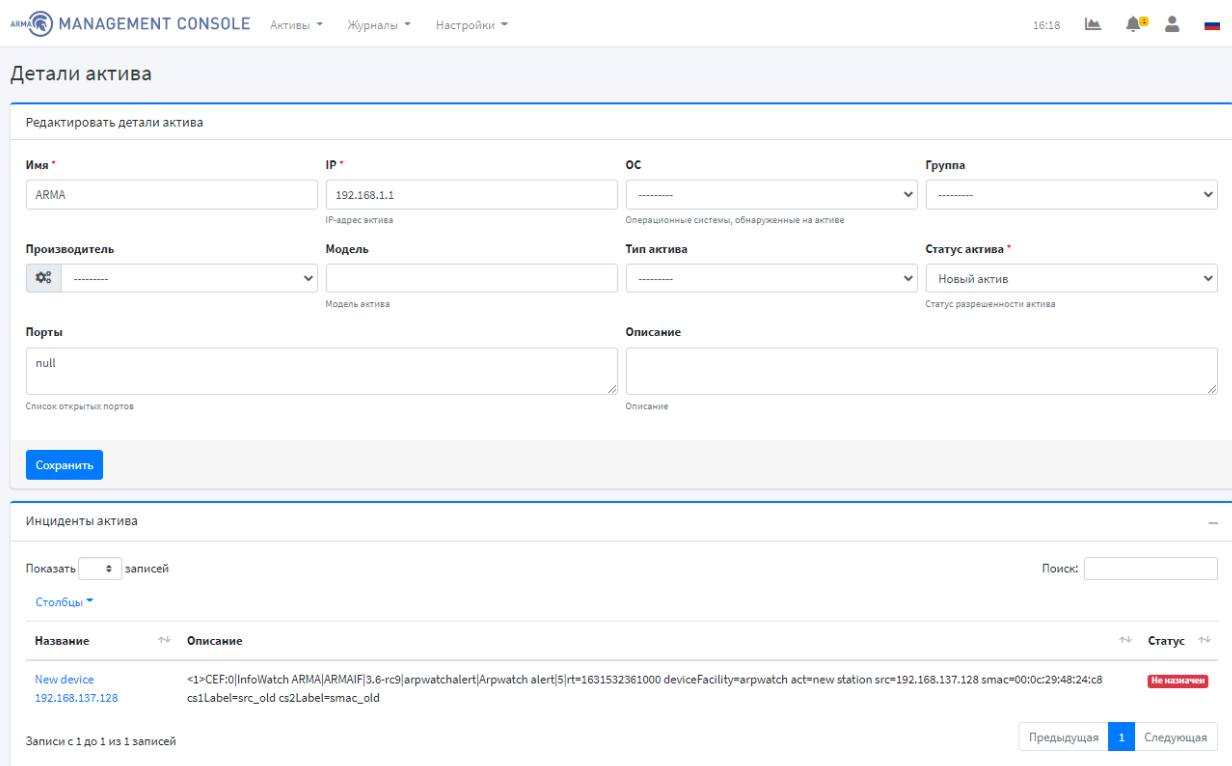


Рисунок 104 – Детали актива

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 **кнопку «Группы»**. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп (см. Рисунок 105). Для добавления новой группы необходимо нажать **кнопку «Добавить»**.

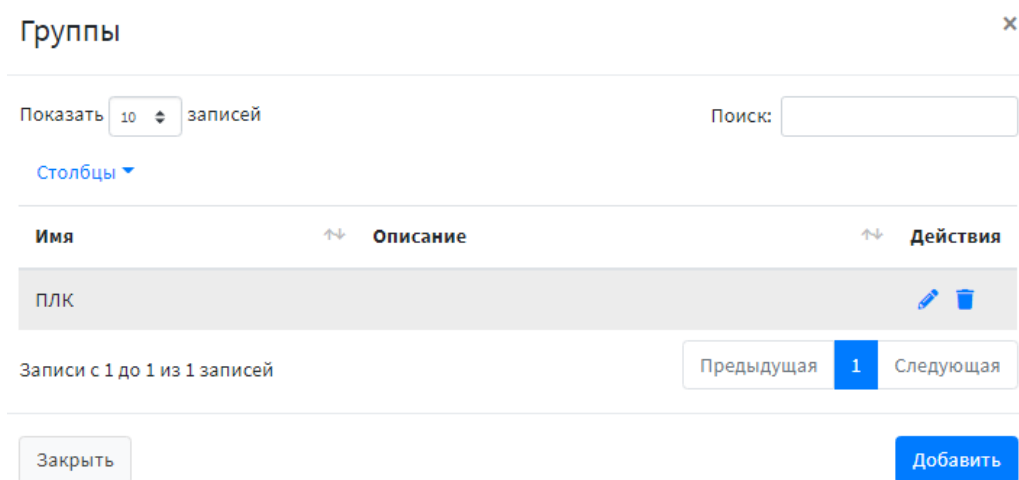


Рисунок 105 – Список групп активов

Окно добавления группы (см. [Рисунок 106](#)) позволяет ввести необходимую информацию для создания новой группы.

Для сохранения группы устройств сети необходимо нажать **кнопку «Сохранить изменения»**.

Для закрытия окна добавления группы необходимо нажать **кнопку «Закрыть»**. В случае успешного добавления группы появится уведомление об этом (см. [Рисунок 154](#)).

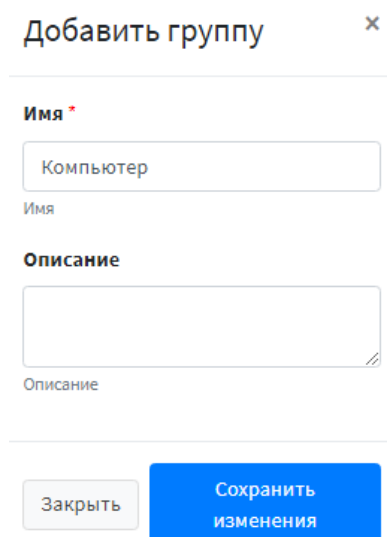



Рисунок 106 – Добавление группы устройств сети

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 **кнопку «Группы»**. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп. Для удаления пользовательской группы необходимо нажать **кнопку «»** напротив соответствующей группы и подтвердить удаление во всплывающем окне.

В случае успешного удаления группы появится уведомление об этом.

9.6 Редактирование групп

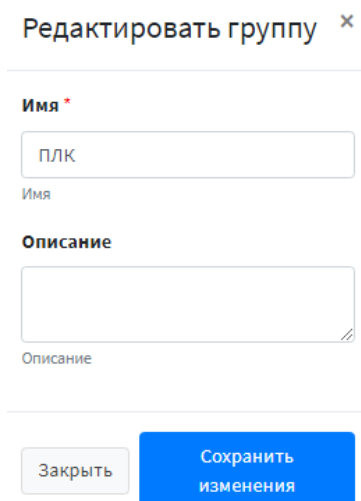
Текущий подраздел доступен пользователям с правом доступа **«Может редактировать группы активов»**. Описание добавления пользователя и назначение прав доступа приведены в разделе [11](#) настоящего руководства.

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

Окно редактирования группы (см. Рисунок 107) позволяет ввести необходимую информацию о группе.

Для сохранения группы устройств сети необходимо нажать кнопку «Сохранить изменения».

Для закрытия окна редактирования группы необходимо нажать кнопку «Закрыть». В случае успешного редактирования группы появится уведомление об этом (см. Рисунок 155).



Редактировать группу ✕

Имя *

ПЛК

Имя

Описание

Описание

Закрыть

Сохранить изменения

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» / «Автоматическая»** (см. Рисунок 108).

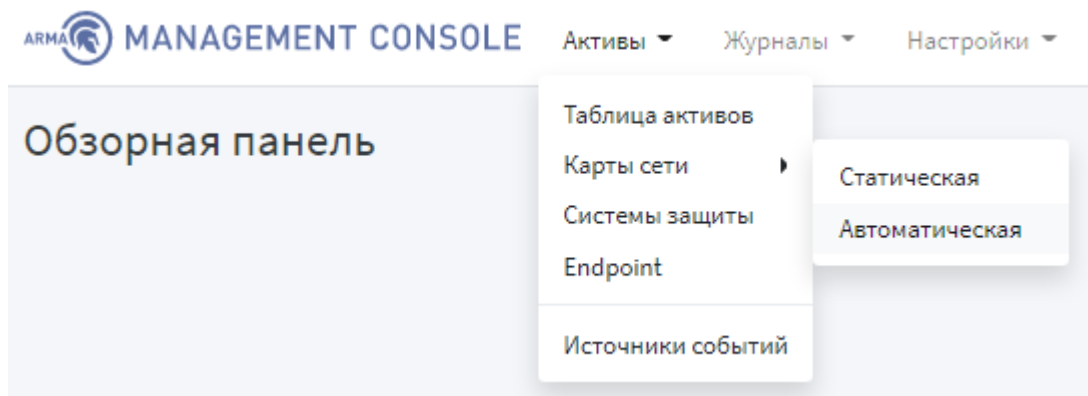


Рисунок 108 – Переход на карту сети

10.1 Описание карты сети

На странице **«Активы» - «Карта сети» - «Статическая»** отображаются устройства сети и их связи (см. Рисунок 109) в соответствии с таблицей устройств сети на странице **«Активы» - «Таблица активов»** (см. 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.

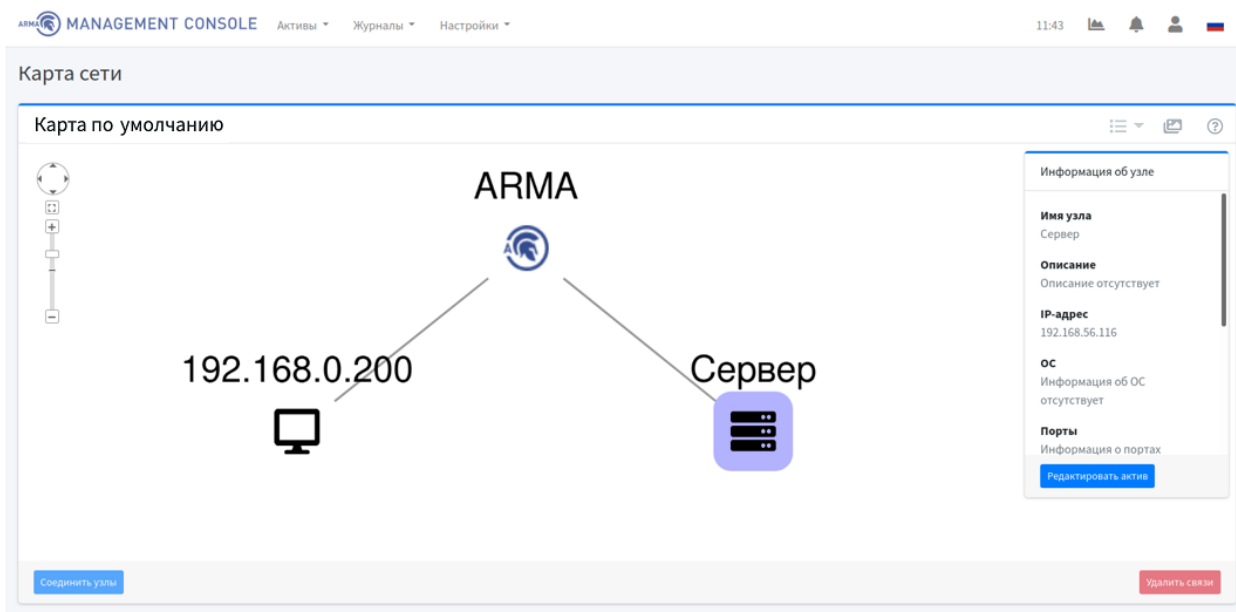



Рисунок 109 – Карта сети

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 **кнопку** «» (см. Рисунок 110).

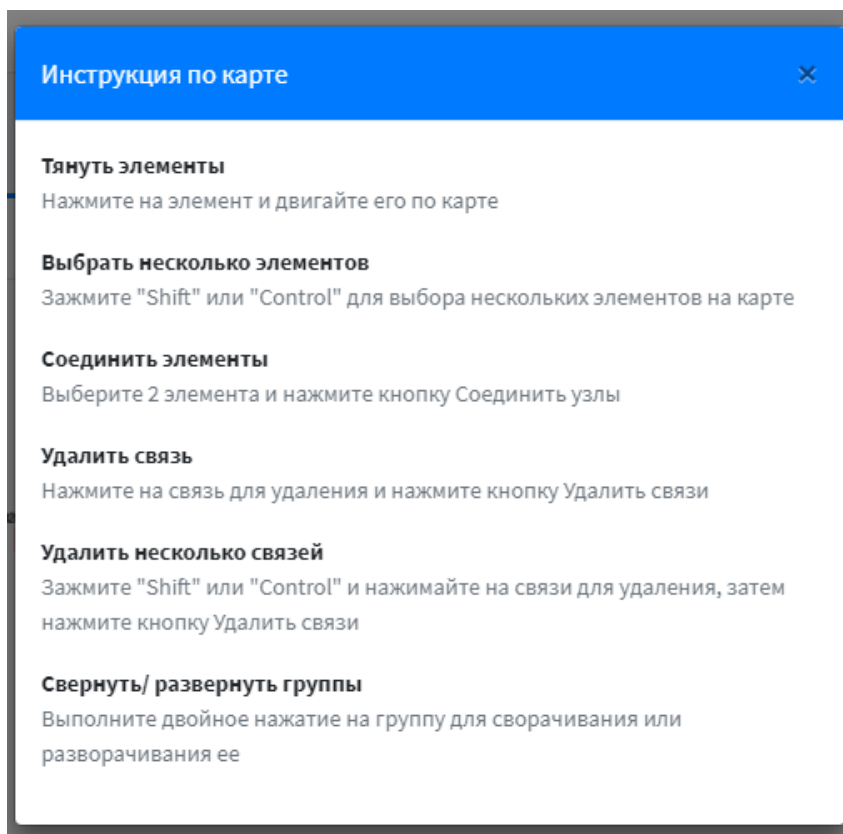




Рисунок 110 – Инструкция по карте сети

Для любой карты сети можно установить фоновое изображение, нажав **кнопку** «»». Во всплывающем окне нажать **кнопку** «» и добавить фоновое изображение (см. Рисунок 111, Рисунок 112).

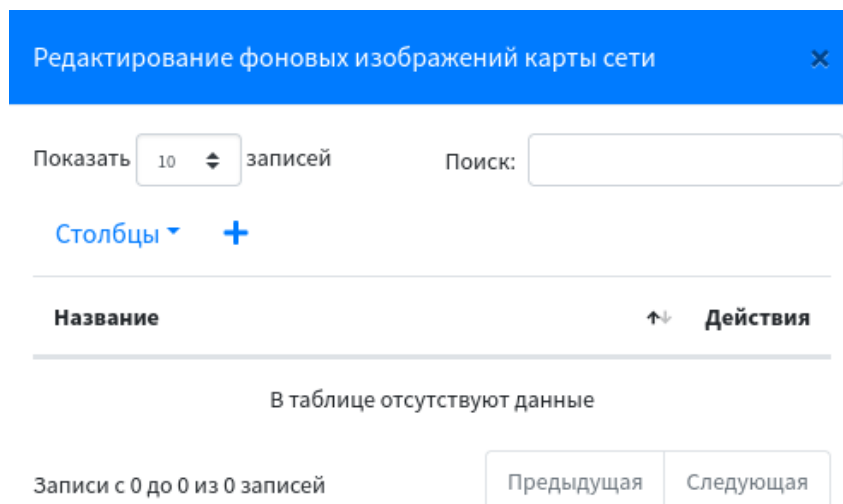


Рисунок 111 – Список фоновых изображений

Добавить новое фоновое изображение
✕

Название *

Описание

Описание

Фоновое изображение *

Выберите файл
Обзор

Выберите файл с изображением

Добавить

Рисунок 112 – Добавление фонового изображения

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

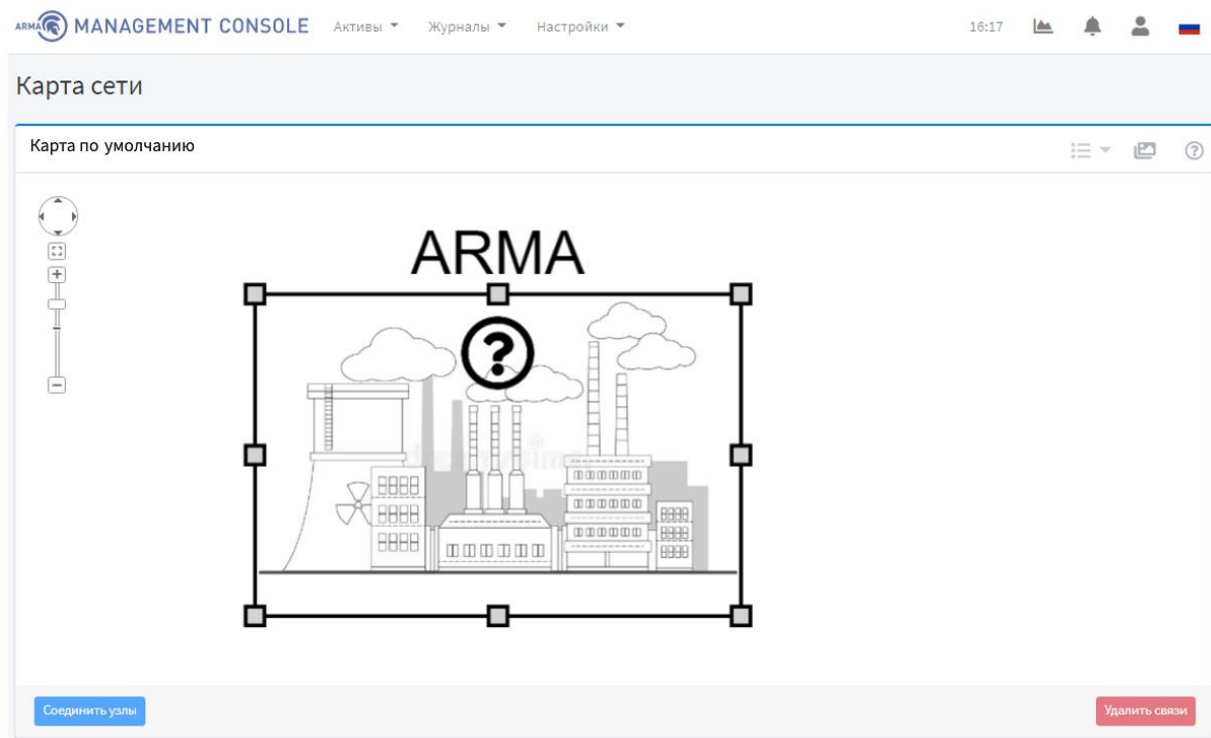


Рисунок 113 – Пример фонового изображения на карте сети

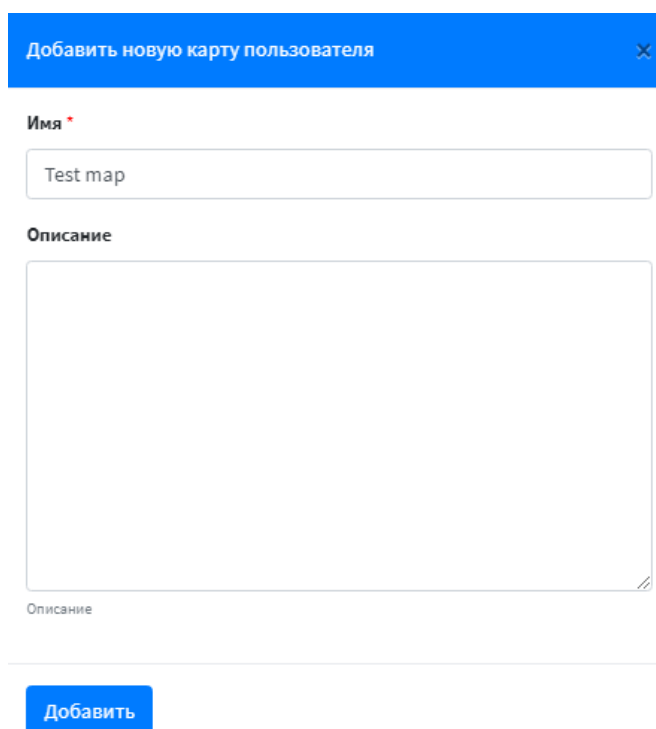
10.1.1 Создание и удаление связей устройств

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

Для удаления связей между устройствами сети необходимо выбрать устройства сети, связь между которыми необходимо удалить, и нажать **кнопку «Удалить связи»**.

10.1.2 Добавление карты сети

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



Добавить новую карту пользователя

Имя *

Test map

Описание

Описание

Добавить

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 (см. Рисунок 115) в соответствие с таблицей устройств сети на странице «**Активы**» - «**Таблица активов**» (см. Рисунок 100).

Карта сетевых взаимодействий

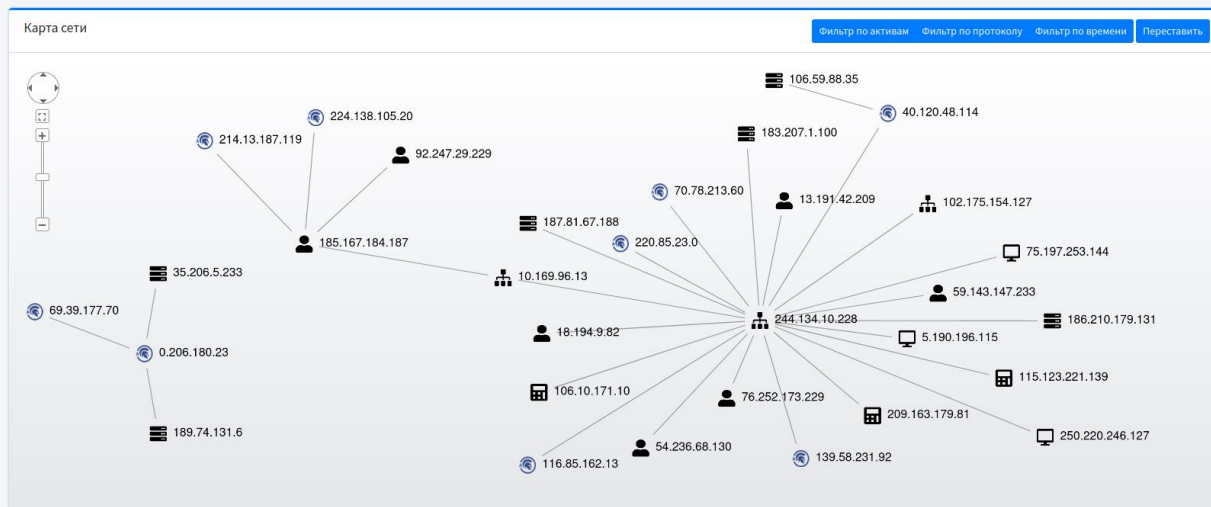


Рисунок 115 – Карта сетевых взаимодействий

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 кнопку «**Применить**», а затем кнопку «**Добавить**» (см. Рисунок 116).

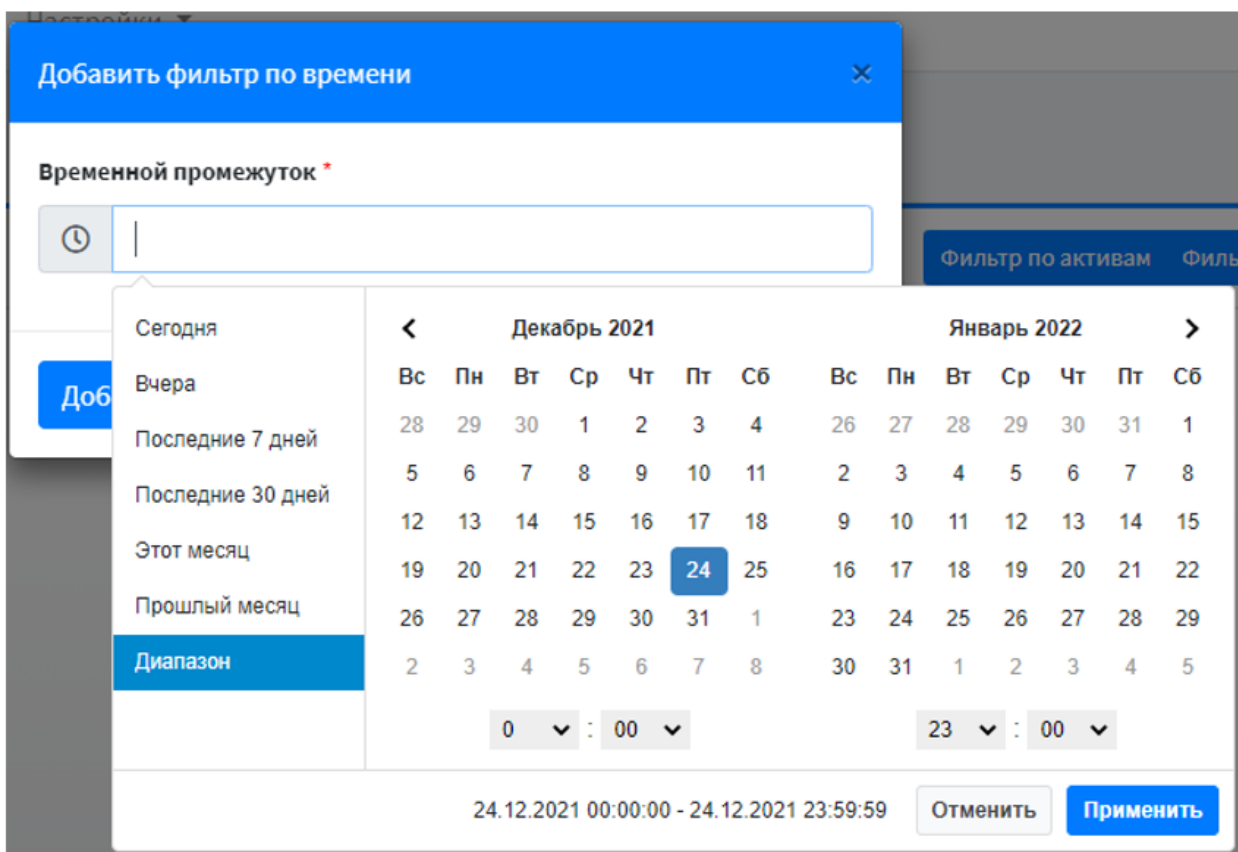


Рисунок 116 – Фильтрация соединений по времени

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

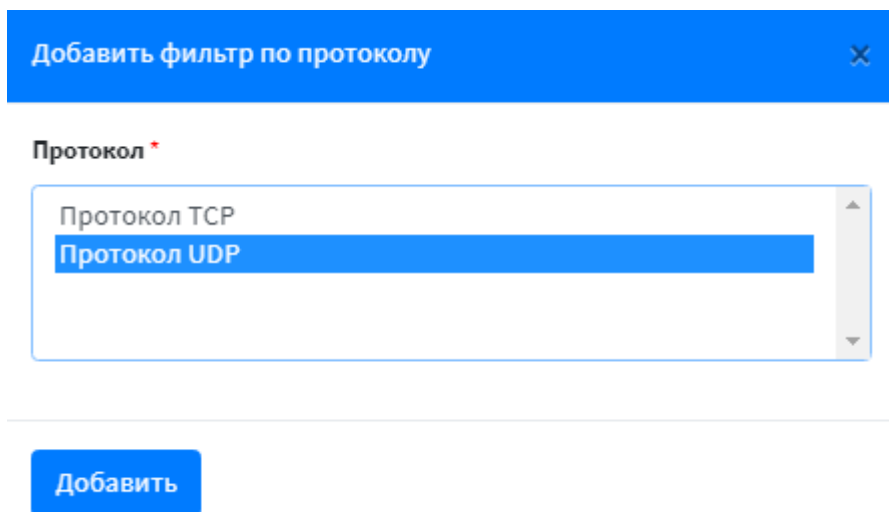


Рисунок 117 – Фильтрация по типу протокола

10.2.2 Фильтрация по активам

Для фильтрации по активам необходимо нажать **кнопку «Фильтр по активам»**. В появившемся окне выбрать необходимые активы и нажать **кнопку «Добавить»**.

При необходимости отобразить «соседей» активов необходимо установить флажок в поле «**Отображать соседей**» (см. Рисунок 118).

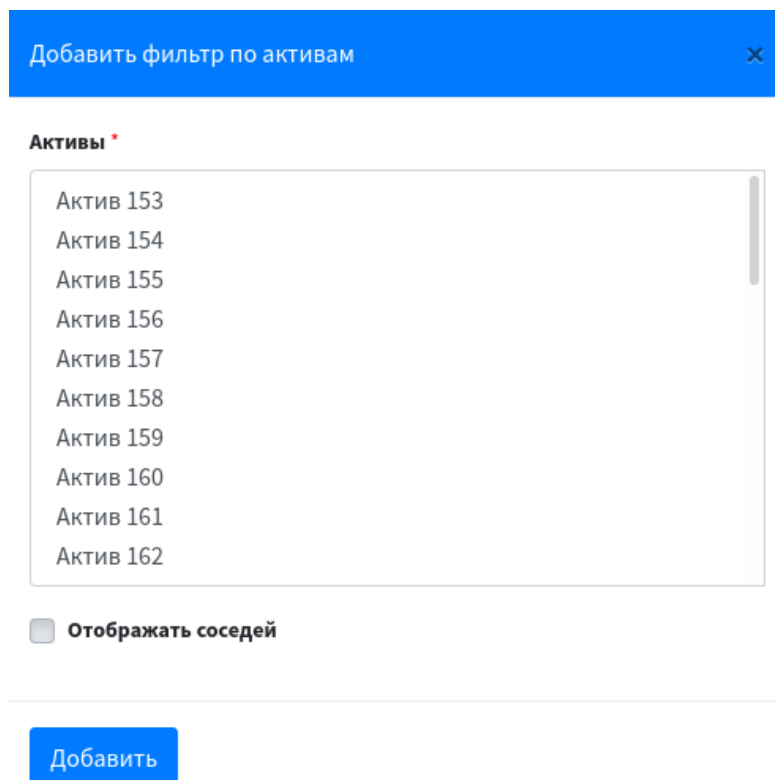



Рисунок 118 – Фильтрация по активам

10.2.3 Перестановка элементов на карте

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

11 УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ И ПРАВАМИ ДОСТУПА СИСТЕМЫ

11.1 Профиль пользователя

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

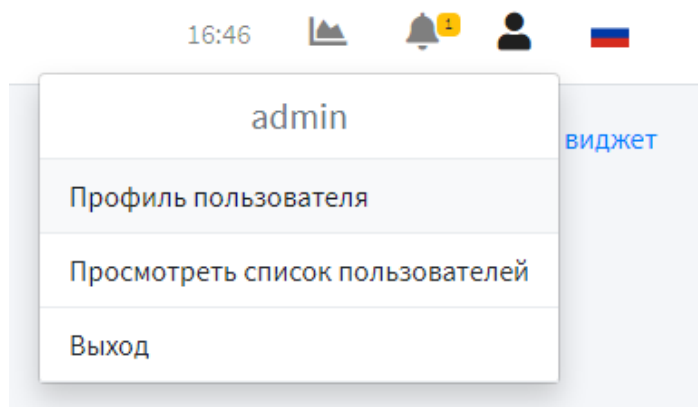


Рисунок 119 – Переход на страницу профиля пользователя

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

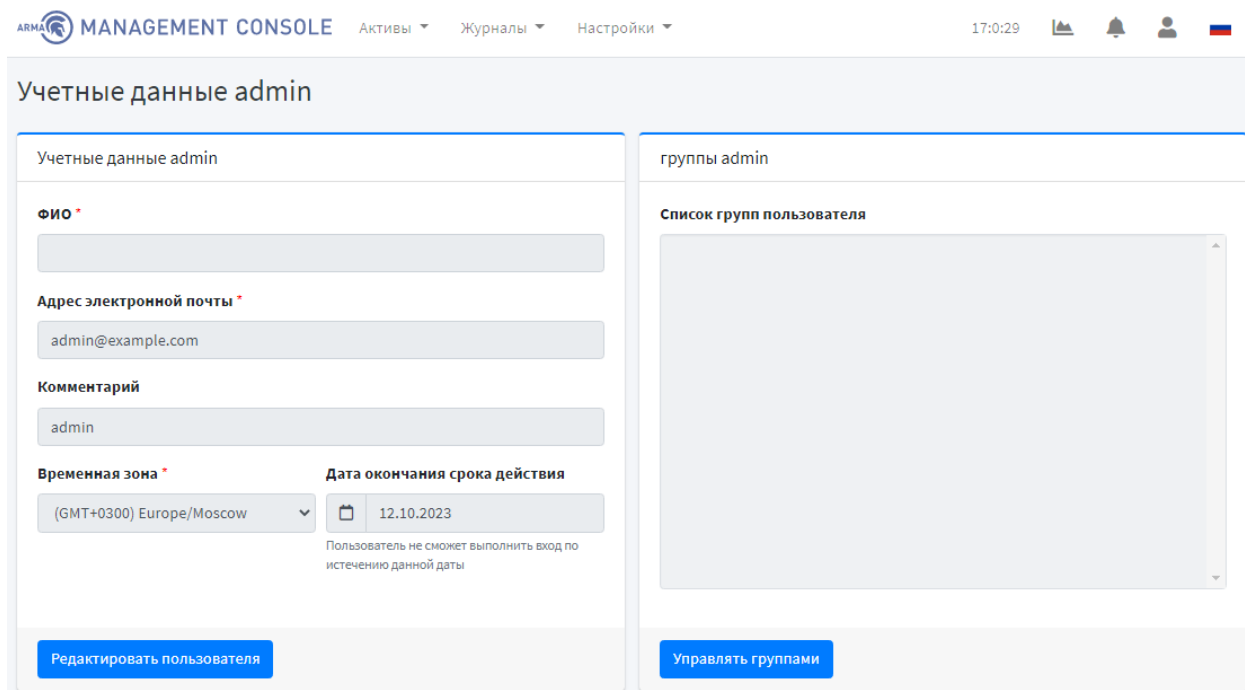






Рисунок 120 – Профиль текущего пользователя (просмотр)

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 **кнопку «»** в верхнем меню, а затем выбрать пункт **«Просмотреть список пользователей»** (см. Рисунок 119).

Страница **«Список пользователей»** позволяет просматривать список учетных записей пользователей в формате таблицы, которая содержит следующие записи (см. 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»**).

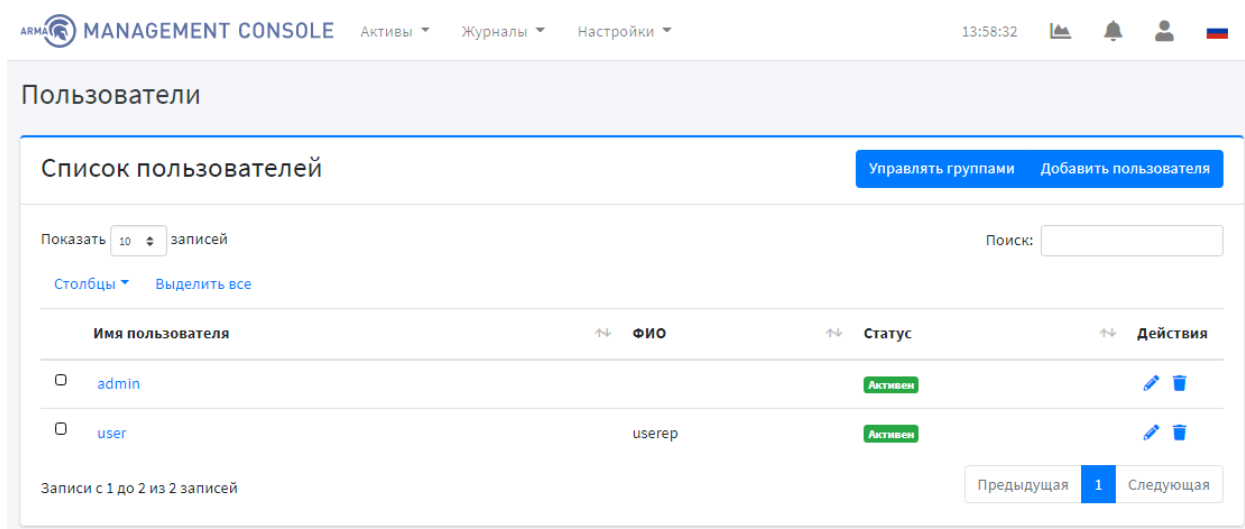




Рисунок 121 – Список пользователей


Для выбора количества записей, отображаемых в таблице пользователей, необходимо нажать **кнопку** «  » в левом верхнем углу формы.

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 **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 **кнопку** «  » 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]»** (см. Рисунок 120).

Для пользователя с правом доступа **«Может редактировать учетные данные пользователя»** на странице будет отображаться **кнопка** **«Редактировать пользователя»**. При нажатии на кнопку отображается страница **«Редактировать пользователя»** (подробнее описано в п. 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 **кнопку** «  » в верхнем меню и, выбрав пункт **«Просмотреть список пользователей»** и нажать **кнопку** **«Добавить пользователя»** (см. Рисунок 121).

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

!Важно Необходимо, чтобы имя пользователя было оригинальным в **ARMA MC**, так как имя пользователя является идентификатором пользователя в **ARMA MC**.

Для сохранения и добавления пользователя необходимо нажать **кнопку «Сохранить»**.

The screenshot shows the 'Добавить нового пользователя' (Add new user) form in the ARMA MANAGEMENT CONSOLE. The form contains the following fields and options:



- Логин ***: Input field with value 'maria_iv'.
- ФИО ***: Input field with value 'Maria Ivanova'.
- Адрес электронной почты ***: Input field with value 'mivanova@iwarma.ru'.
- Пароль ***: Password input field (masked with dots).
- Подтверждение пароля ***: Confirm password input field (masked with dots).
- Активный**: A checked checkbox with the label 'Активный'. Below it, a note reads: 'Отметьте, если пользователь должен считаться активным. Уберите эту отметку вместо удаления учётной записи.'
- Комментарий**: A large empty text area for additional notes.
- Временная зона ***: A dropdown menu showing '(GMT+0300) Europe/Moscow'.
- Дата окончания срока действия**: A date picker showing '30.06.2022'. Below it, a note reads: 'Пользователь не сможет выполнить вход по истечению данной даты'.
- Сохранить**: A blue button at the bottom left of the form.

Рисунок 122 – Добавление пользователя

Установленный флажок в поле **«Активный»** предоставляет пользователю доступ к системе, снятый флажок – блокирует доступ к системе.

Возможность **блокировки** и **разблокировки** доступа пользователя к **ARMA MC** доступна пользователю с привилегией **«Может редактировать учетные данные пользователя»**.

11.2.3 Редактирование учетной записи пользователя

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

Страница **«Редактирование пользователя»** позволяет редактировать информацию учетной записи пользователя (см. [Рисунок 123](#)).

Редактировать пользователя

Изменить учетные данные maria_iv

Заблокирован

ФИО *

Maria Ivanova

Адрес электронной почты *

mivanova@iwarma.ru

Новый пароль:

Подтверждение нового пароля:

Комментарий

Временная зона * **Дата окончания срока действия**

(GMT+0300) Europe/Moscow 30.06.2022

Пользователь не сможет выполнить вход по истечению данной даты


Рисунок 123 – Редактирование учетной записи пользователя


Для сохранения изменений учетной записи пользователя необходимо нажать **кнопку «Сохранить»**.


Для удаления пользователя необходимо нажать **кнопку «Удалить пользователя»**, а затем подтвердить удаление во всплывающем окне (см. [Рисунок 141](#)).

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 **кнопку** «  » в верхнем меню и, выбрав пункт «**Просмотреть список пользователей**» (см. [Рисунок 121](#)).

Для удаления одной учетной записи пользователя в таблице пользователей необходимо нажать **кнопку** «  » в столбце «**Действия**» соответствующего пользователя и подтвердить удаление во всплывающем окне (см. [Рисунок 139](#)). В случае успешного удаления учетной записи пользователя появится уведомление об этом (см. [Рисунок 150](#)).

Для удаления нескольких учетных записей пользователя в таблице пользователей необходимо выбрать соответствующих пользователей (см. [Рисунок 124](#)), нажать **кнопку** «  » и подтвердить удаление во всплывающем окне.

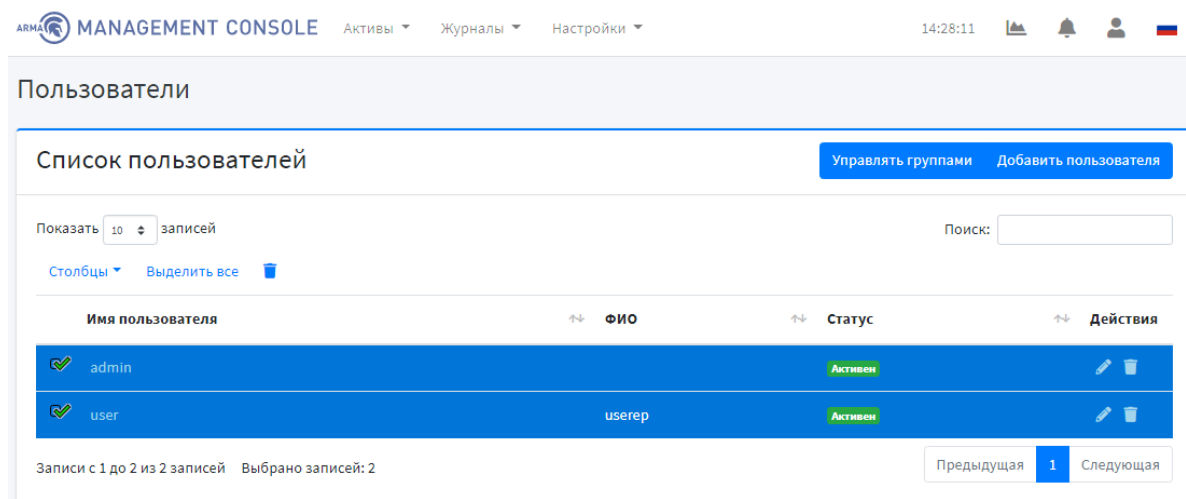




Рисунок 124 – Выбор нескольких учетных записей пользователей

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 **кнопку** «  » в верхнем меню и, выбрав пункт «**Просмотреть список пользователей**». Затем в таблице пользователей нажать **кнопку** «  » в столбце «**Действия**» соответствующего пользователя.

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

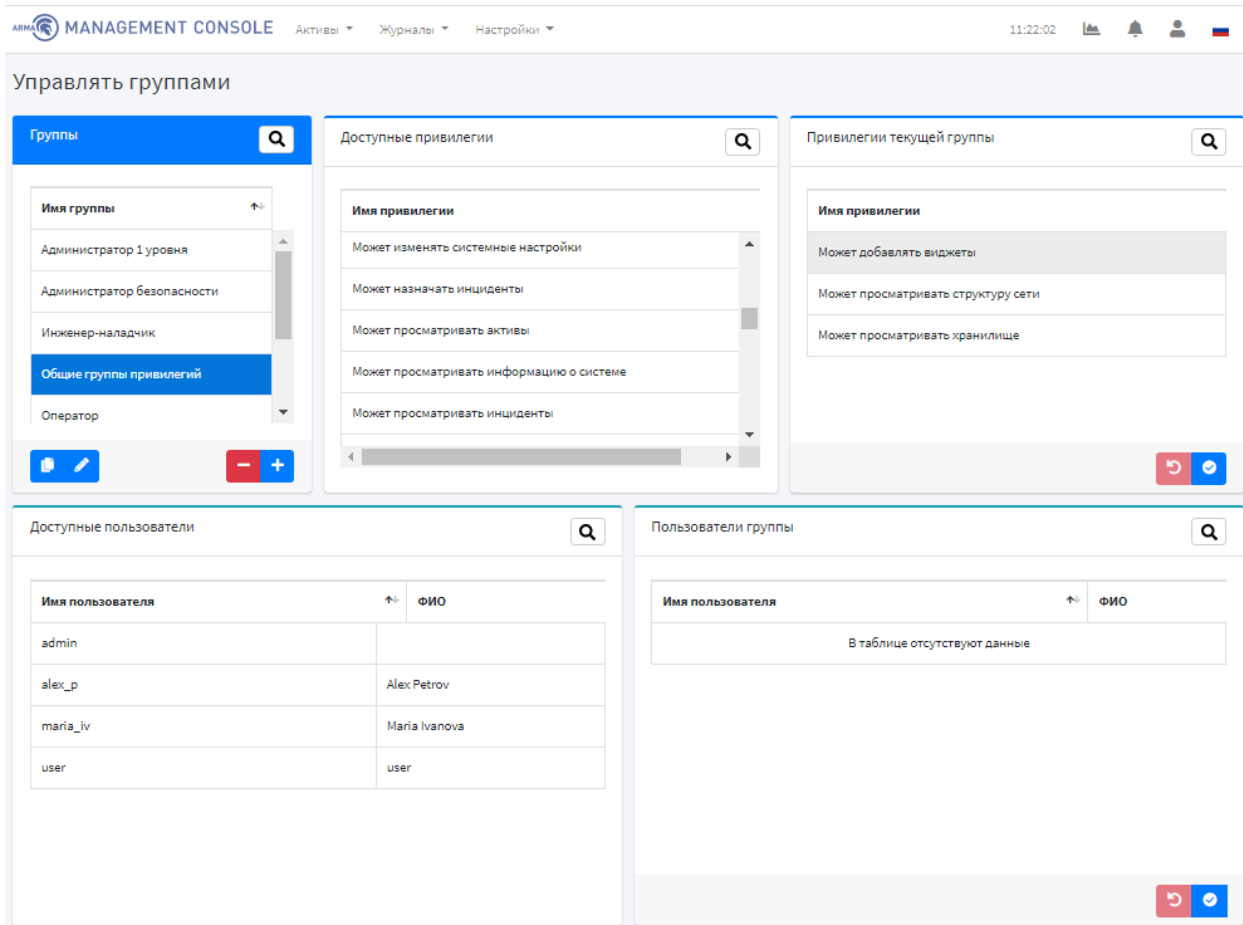




Рисунок 125 – Управление группами

В **ARMA MC** имеются заранее настроенные группы пользователей (см. Таблица 6).

Таблица 6
Настроенные группы пользователей

Группа пользователей	Описание	Примечание
Администратор безопасности	Администратор, которому доступны все привилегии	Доступны все привилегии
Администратор 1 уровня	Администратор ограниченными правами	с Доступны все привилегии, кроме: <ul style="list-style-type: none"> • может удалять правила корреляции; • может удалять Endpoint; • может удалять систему защиты; • может удалять актив; • может удалять пользователя.

Группа пользователей	Описание	Примечание
Инженер-наладчик	Может настраивать средства защиты и источники событий, но не может работать с инцидентами	Доступны все привилегии, кроме привилегий следующих разделов: <ul style="list-style-type: none"> • работы с активами; • работы с системами защиты; • работы с источниками событий • работы с Endpoint.
Super	Инженерный пользователь для проведения восстановительных работ при внештатных ситуациях	Доступны все привилегии (расширенный режим работы с программой)
Оператор	Может видеть инциденты, но не может их обрабатывать	Доступна привилегия «Может просматривать инциденты»
Офицер безопасности 1 уровня	Может обрабатывать инциденты, но не может их назначать	Доступны привилегии: <ul style="list-style-type: none"> • может работать с инцидентами; • может просматривать карточку событий; • может просматривать карточку актива.
Офицер безопасности 2 уровня	Может обрабатывать и назначать инциденты	Доступны привилегии офицера безопасности 1 уровня и привилегия «Может назначать инциденты»
Офицер безопасности 3 уровня	Может создавать правила корреляции	Доступны привилегии офицера безопасности 1 и 2 уровня и следующие привилегии: <ul style="list-style-type: none"> • раздела правил корреляции; • может изменять решенные инциденты.

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


Все таблицы позволяют производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать **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 **кнопку** «».


Для отмены изменения привилегий в группе необходимо нажать **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 **кнопку** «».

Для отмены изменения необходимо нажать **кнопку** «».

11.3.1 Привилегии доступа в системе

В **ARMA MC** доступны следующие привилегии (см. Таблица 7).

Таблица 7
Привилегии доступа в системе



Привилегия	Примечание
1. Управление пользователями:	
может просматривать список пользователей	
может просматривать учетные данные пользователя	
может редактировать учетные данные пользователя	Доступна блокировка/разблокировка доступа пользователя к ARMA MC
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	

Привилегия	Примечание
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	Доступно создание и удаление 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	Доступна кнопка «Информация по системе»
может редактировать системы защиты	Доступна кнопка «Редактирование»
может добавлять системы защиты	
может управлять системами защиты	Доступны кнопки «Перезагрузка», «Скачать конфигурацию» и «Скачать наборы правил СОВ»
может удалить систему защиты	Доступны кнопки удаления и множественного удаления систем защиты
9. Ротация:	
может изменять настройки ротации	
может скачивать файлы ротации	
10. Работа с журналом событий:	
может просматривать список событий	
может просматривать карточку события	


Привилегия	Примечание
может экспортировать журналы событий	
11. Endpoint:	
может добавлять Endpoint	При отсутствии привилегий « Может просматривать список событий » и « Может просматривать карточку события » недоступна кнопка « Просмотр событий антивируса Endpoint »
может редактировать Endpoint	
может просматривать список Endpoint	
может скачивать конфигурацию Endpoint	
может удалять Endpoint	
может просматривать хранилище	
12. Правила корреляции:	
может просматривать список правил корреляции	
может просматривать карточку правила корреляции и список групп 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:	

Привилегия	Примечание
может просматривать сетевые атаки	
17. ГосСОПКА	
может просматривать карточку компании	
может редактировать карточку компании	
может просматривать карточку сообщений	
может редактировать карточку сообщений	
может просматривать список сообщений	

11.3.2 Добавление группы пользователей

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

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

Для добавления группы пользователей в таблице «**Группы**» необходимо нажать **кнопку** «», во всплывающем окне «**Добавить новую группу**» (см. [Рисунок 126](#)) ввести название группы и нажать **кнопку** «**Сохранить изменения**».

Для отмены создания новой группы необходимо нажать **кнопку** «**Заккрыть**».

Добавить новую группу
×

Новое имя группы

Расследование инцидентов

Заккрыть
Сохранить изменения



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 **кнопку** «» в верхнем меню и, выбрав пункт «**Просмотреть список пользователей**». Затем в таблице пользователей нажать **кнопку** «» в столбце «**Действия**» соответствующего пользователя.

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

Для редактирования группы пользователей необходимо выбрать (нажать на) группу пользователей, нажать **кнопку** «», во всплывающем окне «**Переименовать группу**» (см. [Рисунок 127](#)) ввести новое название группы и нажать **кнопку** «**Применить**».

Для отмены редактирования группы пользователей необходимо нажать **кнопку** «**Заккрыть**».

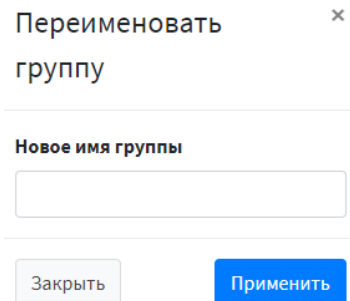




Рисунок 127 – Редактирование группы пользователей

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 **кнопку** «» в верхнем меню и, выбрав пункт «**Просмотреть**

список пользователей». Затем в таблице пользователей нажать **кнопку** «  » в столбце «**Действия**» соответствующего пользователя.

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

Для удаления группы пользователей необходимо выбрать (нажать на) группу пользователей, нажать **кнопку** «  » и подтвердить удаление во всплывающем окне (см. [Рисунок 128](#)).

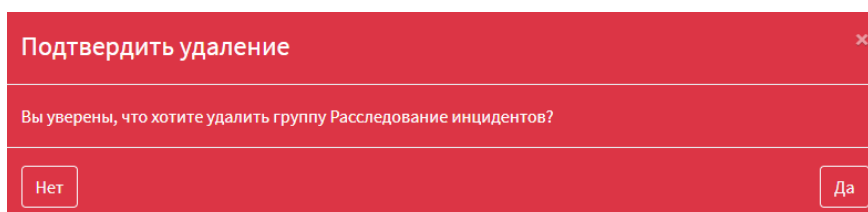


Рисунок 128 – Подтверждение удаления группы пользователей

11.3.5 Добавление пользователей в группу


Добавление пользователей в группу производится посредством добавления групп пользователей (см. [11.3.2](#)).

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 **кнопку** «  ».

Для отмены изменения необходимо нажать **кнопку** «  ».


11.3.6 Добавление привилегий группам пользователей

Добавление привилегий группам пользователей производится посредством добавления групп пользователей (см. [11.3.2](#)).

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 **кнопку** «».

Для отмены изменений привилегий группы необходимо нажать **кнопку** «».

12 ГОССОПКА

Раздел «ГосСОПКА» реализован в рамках исполнения следующих приказов:

- Ф3 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 года;
- ФСБ РФ № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» от 19.06.2019 года.

Текущий раздел позволяет информировать НКЦКИ о произошедших инцидентах.

Вкладка «Уведомления» отображает список уведомлений ГосСОПКА (см. Рисунок 129).

The screenshot shows the 'ГосСОПКА' management console interface. At the top, there is a navigation bar with 'MANAGEMENT CONSOLE', 'Активы', 'Журналы', 'Настройки', and 'ГосСОПКА'. The main content area is titled 'ГосСОПКА' and contains a section 'Список уведомлений ГосСОПКА'. This section includes a search bar, a 'Показать 10 записей' dropdown, and a table of notifications. The table has columns for ID, Инцидент, Идентификатор, Статус активности, Статус уведомления, Обновления, and Комментарии. Three notifications are listed with their respective details. To the right of the table is a 'Комментарии' section with a text input field and an 'Отправить' button. Below the table, there are navigation buttons for 'Предыдущая', '1', and 'Следующая'.

ID	Инцидент	Идентификатор	Статус активности	Статус уведомления	Обновления	Комментарии
5	73ed9bb4-86ed-4d5f-aa2f-f78127e45da3	INC-22-03-149	Меры приняты	Отправлено в архив	2022-03-25T16:19:34.575000+03:00	🔔
6	d7f49cf8-e248-4e33-aa31-cfa8edc5d02	INC-22-03-150	Меры приняты	Требуется дополнение	2022-03-25T16:22:07.803000+03:00	🔔
7	f474f2fe-1ee5-47dc-9d49-997a17de8cf7	INC-22-03-151	Меры приняты	Проверка НКЦКИ	2022-03-29T01:28:04.578000+03:00	🔔

Рисунок 129 – Список уведомлений ГосСОПКА

При поступлении комментария по конкретному уведомлению появляется цифра в столбце «Комментарии», нажав на которую в блоке «Комментарии» появится сообщение/комментарий от НКЦКИ в формате переписки.

Пользователь имеет возможность отвечать сотрудникам НКЦКИ на их сообщения/комментарии. Для этого необходимо ввести информацию в поле «Сообщение в ГосСОПКА» и нажать кнопку «Отправить».

При нажатии на инцидент осуществляется переход на страницу с деталями инцидента (см. Рисунок 130).

MANAGEMENT CONSOLE Активы Журналы Настройки ГосСОПКА 20:35:55 🔔 👤 🇷🇺

Детали инцидента

Инцидент **f474f2fe-1ee5-47dc-9d49-997a17de8cf7** Отправить в ГосСОПКА Решить Сохранить

Дата обновления 25 марта 2022 г. 16:29	Дата создания 25 марта 2022 г. 15:48
Название USB status=DENIED	Число событий 1
Важность 50%	Описание <14>CEF:0 InfoWatch ARMA ARMAIE 2.3.4 usb USB 6 rt=1639592452 act=DENIED cs1Label=pid cs1=1000 cs2Label=vid cs2=8564 cs3Label=serial_number cs3=JKPQMZ1G msg=class:8 subclass:6;class:0
Статус * Решен	Категория
Крайний срок 📅	Назначен на
Комментарий Комментарий к инциденту	

Рисунок 130 – Детали инцидента ГосСОПКА

Для отправки уведомления об инциденте в НКЦКИ необходимо нажать **кнопку «Отправить в ГосСОПКА»** и заполнить соответствующую форму (см. [Рисунок 131](#), [Рисунок 132](#)).

Уведомления ГосСОПКА ✕

Категория *
Уведомление о компьютерном инциденте

Тип *
Вовлечение контролируемого ресурса в инфраструктуру BI

Статус активности *
Проводятся мероприятия по реагированию

Статус приватности *
Для ограниченного распространения внутри организации

Название затронутой системы
.....

Категория затронутой системы *
Объект КИИ второй категории значимости

Краткое описание события ИБ
.....

Рисунок 131 – Форма заполнения уведомления в ГосСОПКА (1)

Наличие подключения к сети Интернет
 Помощь ГосСОПКА

Последствия целостности *

Отсутствует

Последствия доступности *

Отсутствует

Последствия конфиденциальности *

Отсутствует

Настраиваемое последствие

Отправить

Рисунок 132 – Форма заполнения уведомления в ГосСОПКА (2)

Поля, выделенные серым цветом недоступны для заполнения, остальные поля заполняются либо вручную, либо выбором необходимого варианта из выпадающего списка.

Во вкладке **«Карточка компании»** заполняется общая информация об организации, необходимая для отправки каждого уведомления в ГосСОПКА (см. Рисунок 133):

- наименование организации;
- код страны/региона;
- принадлежность к субъектам КИИ;
- город;
- сфера деятельности компании;
- токен для доступа к аппарату ГосСОПКА.

Компания

Карточка компании

Перейти в персональный аккаунт ГосСОПКА
?

Наименование организации *

Субъект КИИ

Код Страны/Региона *

Город *

Сфера деятельности компании *

Токен *

Токен для доступа к аппарату ГосСОПКА

Сохранить

Рисунок 133 – Карточка компании

Кнопка «Перейти в персональный аккаунт ГосСОПКА» перенаправляет пользователя в личный кабинет ГосСОПКА.

Для подключения к сервисам ГосСОПКА необходимо руководствоваться инструкцией, которая открывается при нажатии **кнопки «?**» (см. Рисунок 134).

Для подключения к сервисам ГосСОПКА, Вам необходимо:



1. Написать официальный запрос на имя Директора НКЦКИ (Скрябин Олег Валерьевич). <https://cert.gov.ru>

2. Развернуть С-Терра Шлюз 100 (версия 4.3). Всю информацию по настройке можно найти [тут](#)

3. На email network@cert.gov.ru написать письмо с темой «Подключение к ТИ НКЦКИ С-Терра», в котором предоставить информацию:

- контактные данные лиц (ФИО, должность, телефон, e-mail),
- ответственных за взаимодействие с НКЦКИ по вопросу организации защищенного канала,
- краткое наименование организации,
- количество и адреса узлов, с которых планируется осуществлять доступ к ТИ НКЦКИ,
- файл запроса на сертификат (+ контрольную сумму).

В ответ, Вам присылают корневой сертификат для построения тоннеля. Информацию о примерах построения тоннеля Вы можете найти [тут](#)

5. Для получения доступа в личный кабинет на портале ГосСОПКА, необходимо написать запрос на электронную почту info@cert.gov.ru с просьбой предоставить логин/пароль от личного кабинета, а также, сгенерировать API для удаленного подключения. К письму необходимо прикрепить заполненный [файл](#) с данными о Вашей организации.

6. После получения данных для входа в личный кабинет ГосСОПКА переходите на страницу авторизации, нажав на кнопку "Переход в личный кабинет ГосСОПКА".

7. В личном кабинете ГосСОПКА, на вкладке "Настройки-Общие-Мой профиль", скопировать "Токен API".


8. Вставить скопированный "Токен API" в строку Токен на странице "Карточка организации" ARMA Management Console.

9. Сохранить настройки.

Для отправки инцидентов в ГосСОПКА необходимо корректно заполнить все поля на странице "Карточка организации" ARMA Management Console.

Рисунок 134 – Инструкция по подключению к сервисам ГосСОПКА

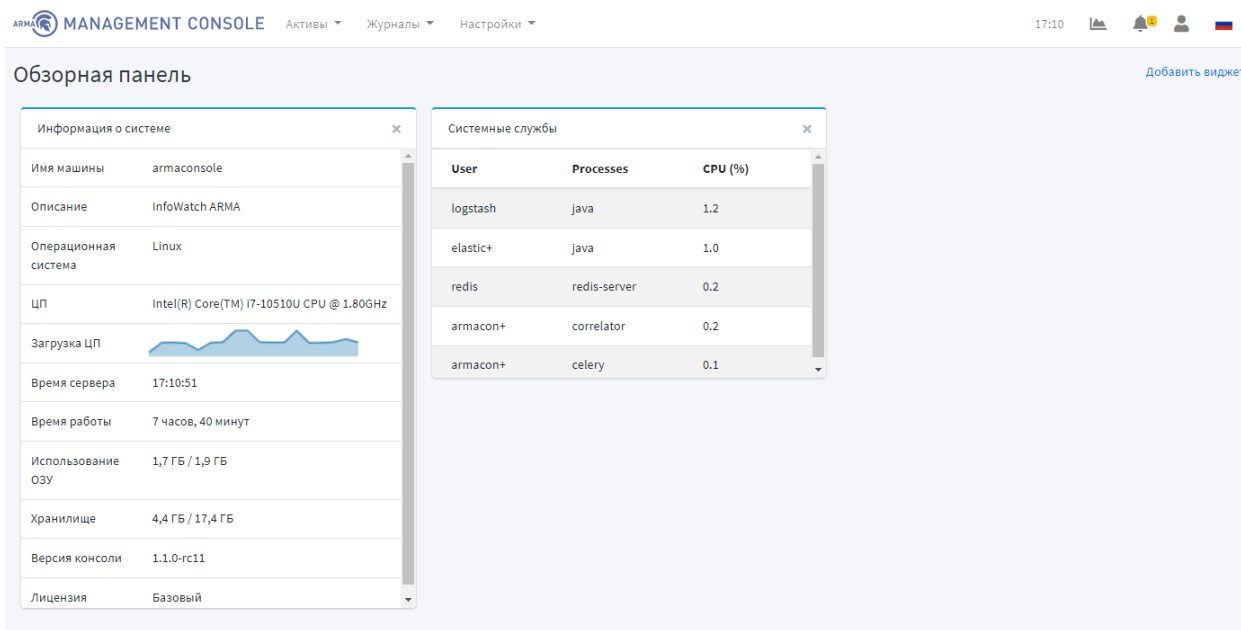
13 УПРАВЛЕНИЕ СТАРТОВОЙ ПАНЕЛЬЮ

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

Страница «**Обзорная панель**» (см. [Рисунок 135](#)) 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 MC позволяет каждому пользователю настраивать индивидуальное отображение виджетов – выбирать удобное местоположение виджетов на странице, а также их масштаб.



The screenshot shows the 'Обзорная панель' (Dashboard) in the ARMA MC Management Console. The interface includes a top navigation bar with 'MANAGEMENT CONSOLE', 'Активы', 'Журналы', and 'Настройки'. The dashboard contains two main widgets:

- Информация о системе** (System Information): A table with the following data:

Имя машины	armaconsole
Описание	InfoWatch ARMA
Операционная система	Linux
ЦП	Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz
Загрузка ЦП	
Время сервера	17:10:51
Время работы	7 часов, 40 минут
Использование ОЗУ	1,7 Гб / 1,9 Гб
Хранилище	4,4 Гб / 17,4 Гб
Версия консоли	1.1.0-rc11
Лицензия	Базовый
- Системные службы** (System Services): A table showing active services:

User	Processes	CPU (%)
logstash	java	1.2
elastic+	java	1.0
redis	redis-server	0.2
armacon+	correlator	0.2
armacon+	celery	0.1

Рисунок 135 – Обзорная панель

Для добавления нового виджета необходимо нажать **кнопку** «**Добавить виджет**» и во всплывающем окне выбрать тип виджета (см. [Рисунок 136](#)).

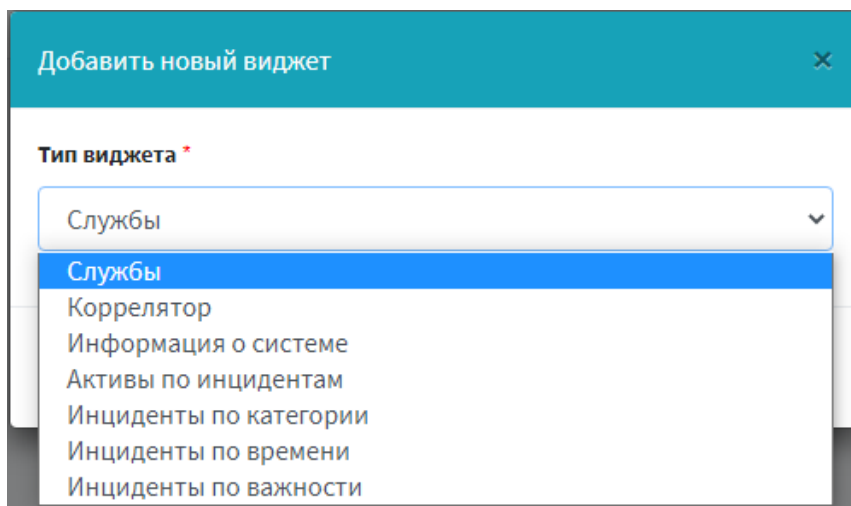


Рисунок 136 – Типы виджетов

Для добавления виджета необходимо нажать **кнопку «Добавить»** (см. Рисунок 137).

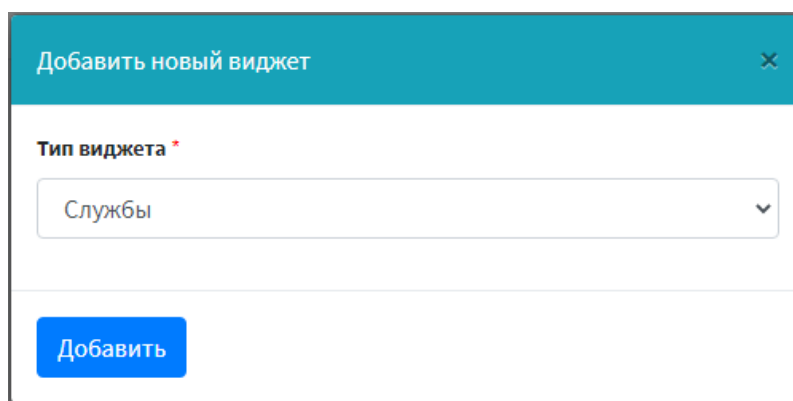


Рисунок 137 – Добавление виджета

Для добавления конкретного виджета необходима отдельная привилегия (см. Таблица 8).

Таблица 8
Привилегии для добавления виджетов

Виджет	Привилегия
Коррелятор	Может просматривать список правил корреляции
Информация о системе	Может просматривать информацию о системе
Службы	Может просматривать информацию о системе
Активы по инцидентам	Может просматривать инциденты, Может просматривать список активов
Инциденты по категории	Может просматривать инциденты
Инциденты по времени	Может просматривать инциденты
Инциденты по важности	Может просматривать инциденты

14 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

14.1 Предупреждения всплывающие при необходимости подтверждения действий

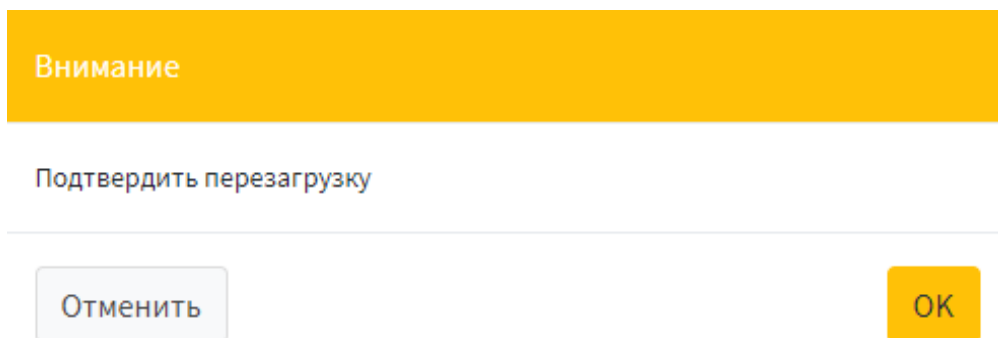


Рисунок 138 – Подтверждение перезагрузки

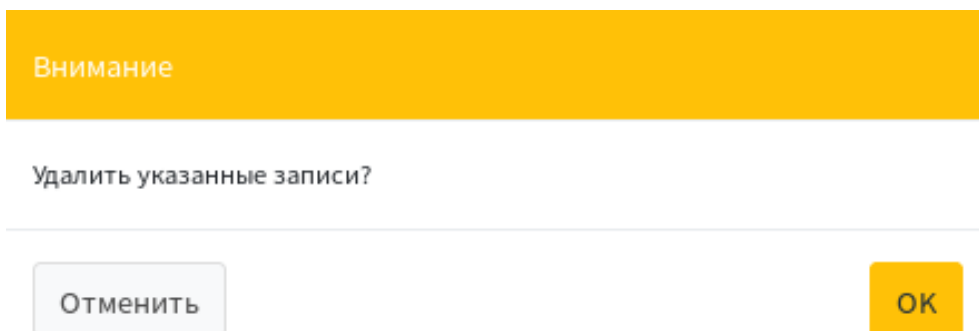


Рисунок 139 – Подтверждение удаления записей

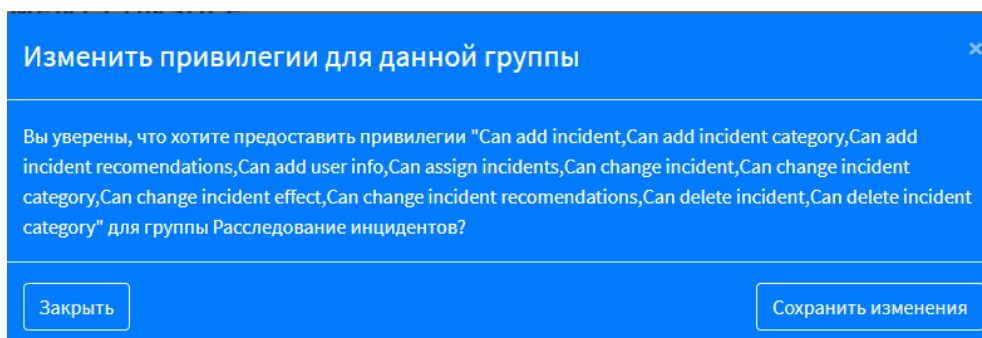


Рисунок 140 – Подтверждение изменений привилегий для группы

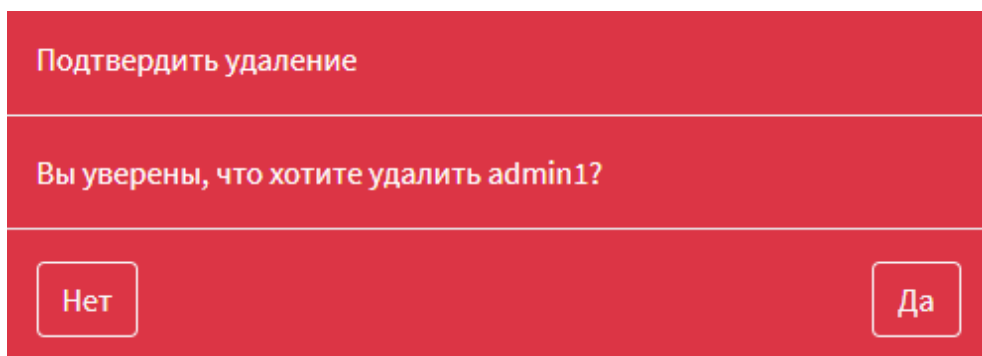


Рисунок 141 – Подтверждение удаления пользователя

14.2 Предупреждения при любом неправильном вводе данных в поле

Название *

Устройство будет отображено под этим именем

Пожалуйста, заполните это поле.

Рисунок 142 – Предупреждение о неправильном вводе в поле (1)

Название *

Это поле обязательно.

Рисунок 143 – Предупреждение о неправильном вводе в поле (2)



Рисунок 144 – Предупреждение о неправильном вводе в поле (3)

<p>Ключ *</p> <input type="text" value="kLmXF0AkRuygqbkWkmKZ64iZ9SEHQjLjcnwArC"/> <p>Предоставлены некорректные данные аутентификации API ключ для устройства</p>	<p>Секрет *</p> <input type="text" value="KQ9DipkwPbhihDvQEMn273GbmWyv40o3i2oCH"/> <p>Предоставлены некорректные данные аутентификации Значение секрета для API ключа</p>
---	---

Рисунок 145 – Предупреждение о неправильном вводе в поле (4)

Рисунок 146 – Предупреждение о неправильном вводе в поле (5)

14.3 Предупреждения при применении настроек

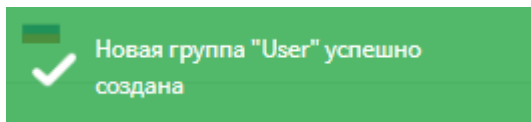


Рисунок 147 – Добавление группы пользователей



Рисунок 148 – Обновление актива



Рисунок 149 – Создание пользователя

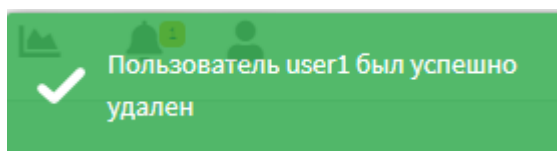


Рисунок 150 – Удаление пользователя



Рисунок 151 – Загрузка конфигурации/правил СОВ



Рисунок 152 – Ожидание скачивания

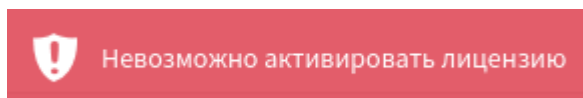


Рисунок 153 – Неуспешная активация лицензии

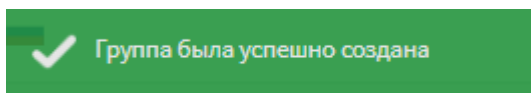


Рисунок 154 – Добавление группы активов

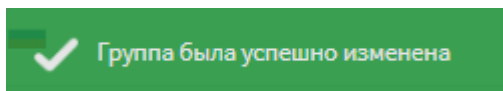


Рисунок 155 – Редактирование группы активов

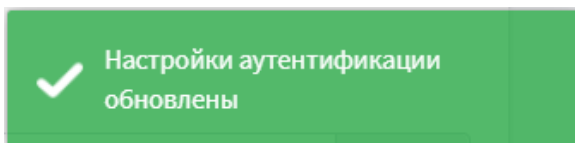


Рисунок 156 – Обновление параметров аутентификации

14.4 Уведомление о несовместимости версий продуктов

Добавить узел
✕

Имя *

Устройство будет отображено под этим именем

IP *

IP-адрес устройства

Ключ *

API ключ для устройства

Секрет *

Значение секрета для API ключа

Комментарий

Дополнительные заметки об устройстве

Создать источник

Должно быть отключено из-за проблем совместимости продуктов

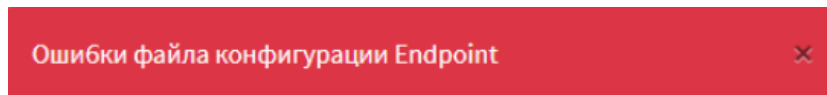
Создать источник логов для сенсора

Порт

Порт для логов источника (UDP)

Рисунок 157 – Уведомление о несовместимости версий продуктов

14.5 Уведомление об ошибке файла конфигурации Endpoint



Указанный путь не существует: "C:\1" для integrity_control.control_path

Рисунок 158 – Ошибки файла конфигурации Endpoint