Руководство администратора

версия 7 ред. от 26.11.2024

Листов 36

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Таблица «Термины и сокращения»

Термины и сокращения	Значение
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
DHCP	Сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
ЛКИ	Локальный консольный интерфейс
УЗ	Учётная запись
ARMA MC	InfoWatch ARMA Management Console

АННОТАЦИЯ

Настоящее руководство администратора по эксплуатации предназначено для администратора, который устанавливает и проводит начальную настройку **ARMA Management Console v.1.7**.

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

ARMA MC выполняет следующие функции:

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

Настоящее руководство администратора по эксплуатации содержит описание:

- установки и настройки **ARMA MC**;
- работы в локальном консольном интерфейсе **ARMA MC**;
- возможных проблем и их решение **ARMA MC**.

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

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

Таблица «Смежные документы»

Сокращенное наименование	Полное наименование
Руководство администратора ARMA MC	Руководство администратора InfoWatch ARMA Management Console

1 СЦЕНАРИИ НАСТРОЙКИ И ЭКСПЛУАТАЦИИ

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

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

- ознакомление с требования к среде функционирования (см. Требований к среде функционирования);
- установка, первоначальная настройка и смена пароля УЗ (см. Установка и первоначальная настройка системы);
- активация и просмотр информации лицензии (см. Управление лицензиями);
- настройка через локальный консольный интерфейс и управление сервисами (см. Описание локального консольного интерфейса);
- решение возможных проблем при работе с **ARMA MC** (см. Возможные проблемы и их решение).

1.1 Пользовательские роли

В **ARMA MC** доступны пользовательские роли, указанные ниже.

Таблица «Пользовательские роли»

Роль	Примечание
Администратор безопасности	Доступны все разделы
Офицер безопасности	Доступны разделы: - **«Обзорная панель»**; - **«Хранилище»**; - **«Профиль пользователя»**; - **«Активы»**; - **«События»**; - **«Инциденты»**; - **«ГосСОПКА»**; - **«Правила корреляции»**; - **«Карта сети»**.

2 ТРЕБОВАНИЙ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

В настоящем разделе представлено описание требований к среде функционирования **ARMA MC**.

Установка **ARMA MC** производится на аппаратную или виртуальную платформы.

Установка на аппаратную платформу производится с использованием USB-накопителя с записанным образом **ARMA MC** в формате «ISO».

Установка на виртуальную платформу производится с помощью образа оптического диска в формате «ISO».

При любом из вариантов установки, для корректного отображения веб-интерфейса, к веб-браузерам предъявляются следующие требования:

- Необходимо иметь последнюю версию ОС и используемого браузера:
  - для ОС семейства Windows – Chrome, Яндекс браузер;
  - для ОС семейства Linux – Chrome, Яндекс браузер.

Примечание:

Во избежание некорректной работы **ARMA MC** не рекомендуется допускать незапланированные отключения питания оборудования.

Примечание:

Рекомендуемый минимальный свободный объем дискового пространства 10 Гб. В случае когда на сервере **ARMA MC** остается менее 10 Гб дискового пространства, появится соответствующее уведомление (см. Рисунок – Переполнение дискового пространства).

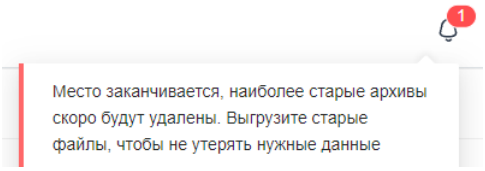

Рисунок – Переполнение дискового пространства

2.1 Требования к аппаратной платформе

При установке **ARMA MC** на аппаратную платформу необходимо использовать микропроцессорную архитектуру x64.

Минимальные технические требования, предъявляемые к аппаратной платформе, представлены ниже.

Таблица «Минимальные технические требования к аппаратной платформе»

Название оборудования	Требования
Процессор	2,0 ГГц, четырёхъядерный, x64

Название оборудования	Требования
ОЗУ	8 ГБ
Интерфейсы	Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры
Жесткий диск	512 ГБ, SSD
Сетевые интерфейсы	Не менее 4 x Ethernet 100/1000 Мбит/сек

2.2 Требования к виртуальной платформе

Виртуализация **ARMA MC** поддерживается для следующих гипервизоров:

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

Минимальные технические требования, предъявляемые к виртуальной платформе, представлены ниже.

Таблица «Минимальные технические требования к виртуальной платформе»

Параметр	Значение
Количество процессоров	4
Объём оперативной памяти	8 ГБ
Размер виртуального диска	512 ГБ
Количество сетевых интерфейсов	Не менее 4

Для корректной работы **ARMA MC** при настройке виртуальной машины рекомендуется выбрать режим загрузки **«Legacy»**.

3 УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ

В настоящем разделе представлено описание установки и первоначальной настройки **ARMA MC**.

3.1 Установка

Установка **ARMA MC** производится со следующих носителей:

- образ диска в формате «ISO» для ВМ;
- USB-накопитель;
- DVD-диск.

При первоначальной загрузке с установочного носителя запустится режим автоустановки (см. Рисунок – Установка ARMA MC). В данном режиме будут выполнены следующие действия:

- установка **ARMA MC** на первый определившийся жесткий диск;
- попытка автоконфигурирования первого сетевого интерфейса;
- перезагрузка **ARMA MC** с отключением установочного носителя.

Рисунок – Установка ARMA MC

Автоконфигурирование первого сетевого интерфейса производится по DHCP, в случае невозможности получить сетевые настройки посредством DHCP необходимо выполнить ручную настройку сетевого интерфейса (см. Ручная настройка сетевого интерфейса во время установки).

После завершения установки и перезагрузки **ARMA MC** будет отображено приглашение авторизации в локальном консольном интерфейсе (см. Рисунок – Приглашение авторизации в локальном консольном интерфейсе).

Рисунок – Приглашение авторизации в локальном консольном интерфейсе

3.1.1 Авторизация в локальном консольном интерфейсе

Для входа в локальный консольный интерфейс необходимо указать учетные данные и нажать **клавишу «ENTER»** после каждого ввода:

- **«login:»** – по умолчанию **«root»**;
- **«password:»** – по умолчанию **«root»**.

  Примечание:

  Пароль пользователя не отображается при наборе.

После успешной аутентификации будет отображен интерфейс командной строки (см. Рисунок – Интерфейс командной строки).

Рисунок – Интерфейс командной строки

3.1.2 Ручная настройка сетевого интерфейса во время установки

В случае невозможности получить сетевые настройки посредством DHCP будет выведено соответствующее уведомление (см. Рисунок – Уведомление о необходимости настроить сеть).

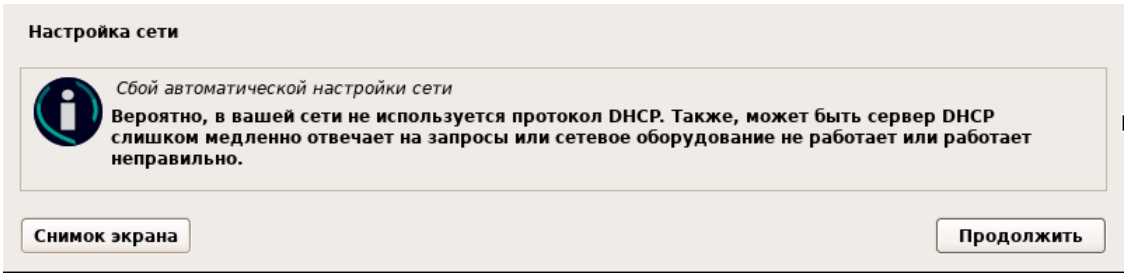

Рисунок – Уведомление о необходимости настроить сеть

Для ручной настройки сетевого интерфейса необходимо нажать **кнопку «Продолжить»** и следовать шагам:

1. Выбрать **«Настроить сеть вручную»** и нажать **кнопку «Продолжить»** (см. Рисунок – Выбор способа настройки сети).

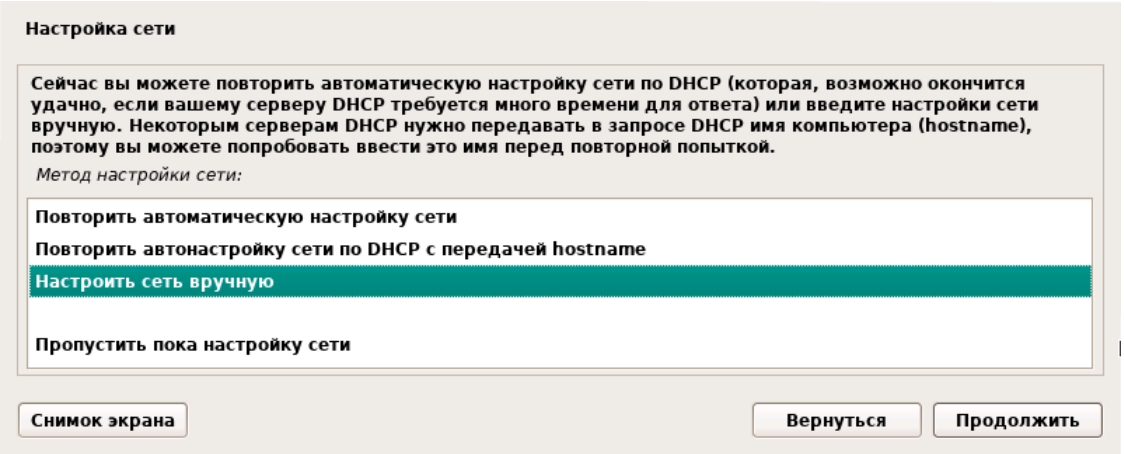

Рисунок – Выбор способа настройки сети

2. Указать IP-адрес и нажать **кнопку «Продолжить»** (см. Рисунок – Указание IP-адреса).

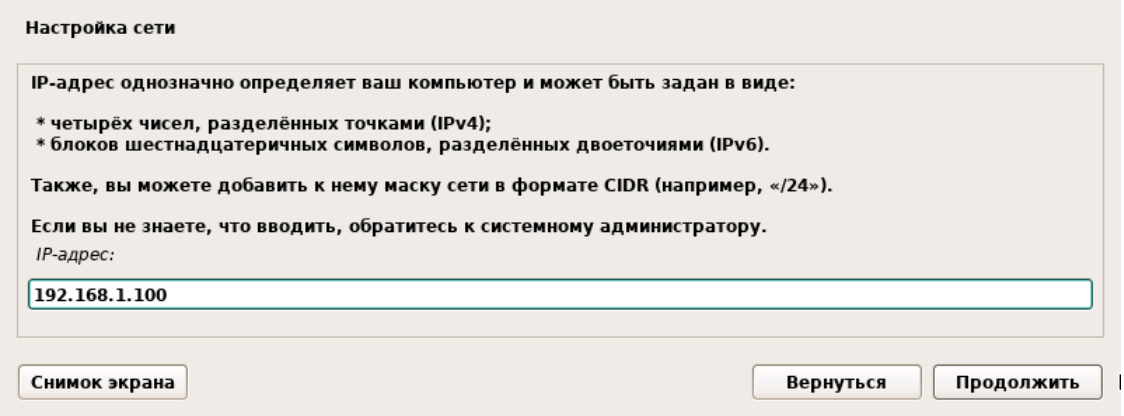

Рисунок – Указание IP-адреса

3. Указать маску подсети и нажать **кнопку «Продолжить»** (см. Рисунок – Указание маски подсети).

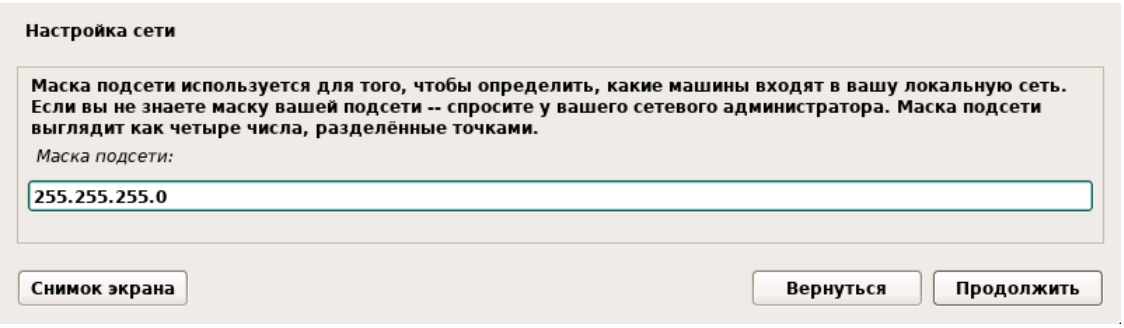

Рисунок – Указание маски подсети

4. Указать шлюз и нажать **кнопку «Продолжить»** (см. Рисунок – Указание шлюза).

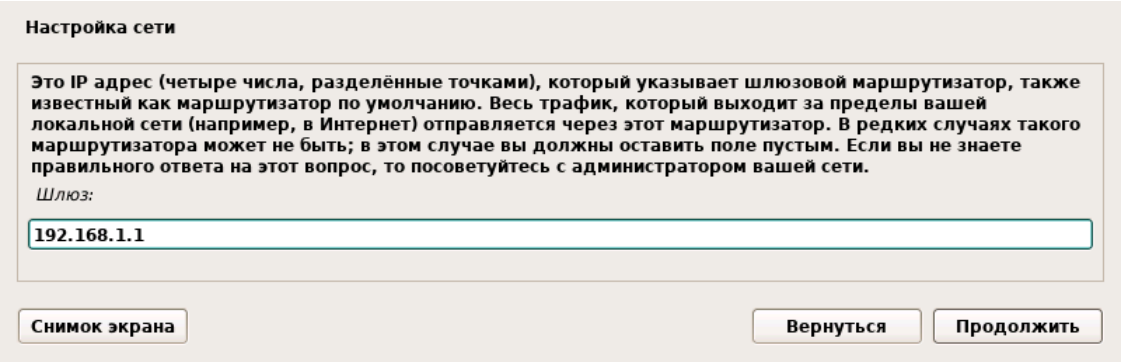

Рисунок – Указание шлюза

5. После окончания ручной настройки сетевого подключения **ARMA MC** произведёт попытку определения наличия подключения на сетевом интерфейсе и установка продолжится (см. Рисунок – Определение наличия подключения на сетевом интерфейсе).

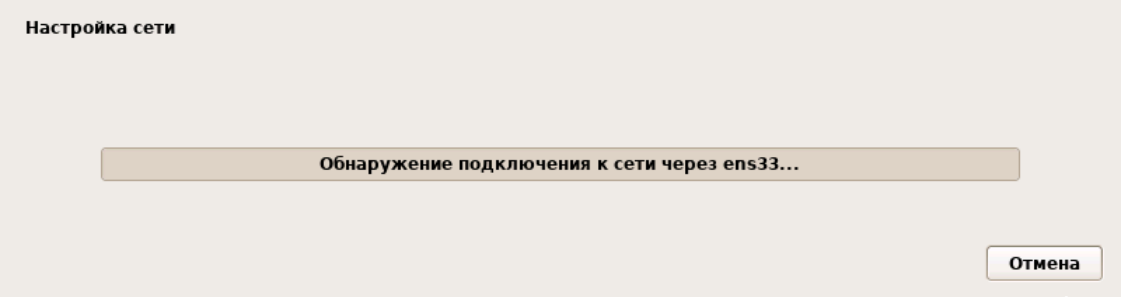

Рисунок – Определение наличия подключения на сетевом интерфейсе

3.2 Базовая настройка сетевых интерфейсов

Для определения IP-адреса, полученного посредством DHCP необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«ip a»** и нажать **клавишу «ENTER»** для получения информации о настройках сетевых интерфейсов. На рисунке ниже указан IP-адрес, полученный посредством DHCP (см. Рисунок – Полученный посредством DHCP IP-адрес ARMA MC):
   - «192.168.1.102».

   Примечание:

   Полученный посредством DHCP IP-адрес приведен в виде примера и может отличаться в зависимости от настроек сети и заданного диапазона IP-адресов.

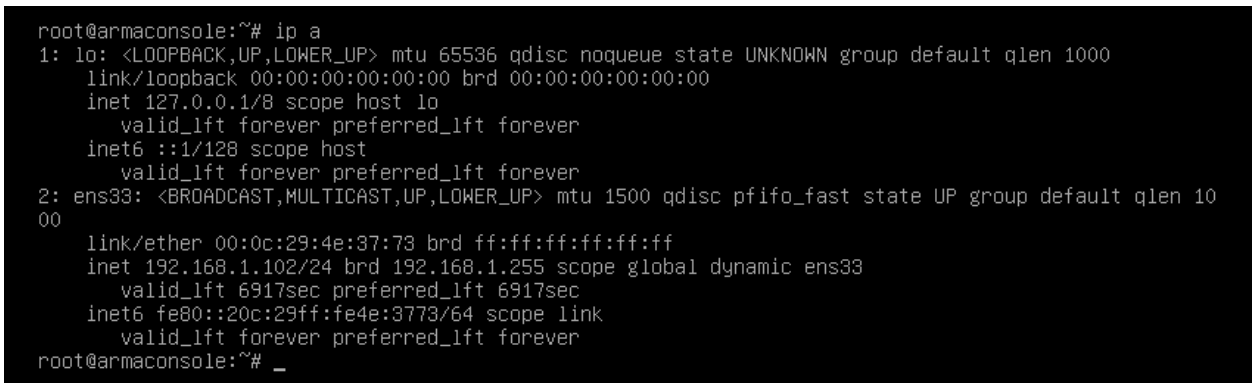

Рисунок – Полученный посредством DHCP IP-адрес ARMA MC

Для ручной настройки параметров сетевого интерфейса необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«nano /etc/network/interfaces»** и нажать **клавишу «ENTER»** для открытия конфигурационного файла сетевых интерфейсов в текстовом редакторе (см. Рисунок – Конфигурационный файл сетевых интерфейсов).

   Перемещение курсора осуществляется **клавишами со стрелками вверх и вниз**.

Рисунок – Конфигурационный файл сетевых интерфейсов

3. В блоке **«#The primary network interface»** (см. Рисунок – Указание параметров сетевого адаптера):
   - добавить строку **«auto ens33»**;
   - изменить значение **«dhcp»** на **«static»**;
   - добавить строки:
     - **«address <IP-адрес>»** – указать требуемый IP-адрес;
     - **«mask <Маска подсети>»** – указать требуемую маску подсети;
     - **«gateway <IP-адрес шлюза>»** – указать требуемый шлюз.

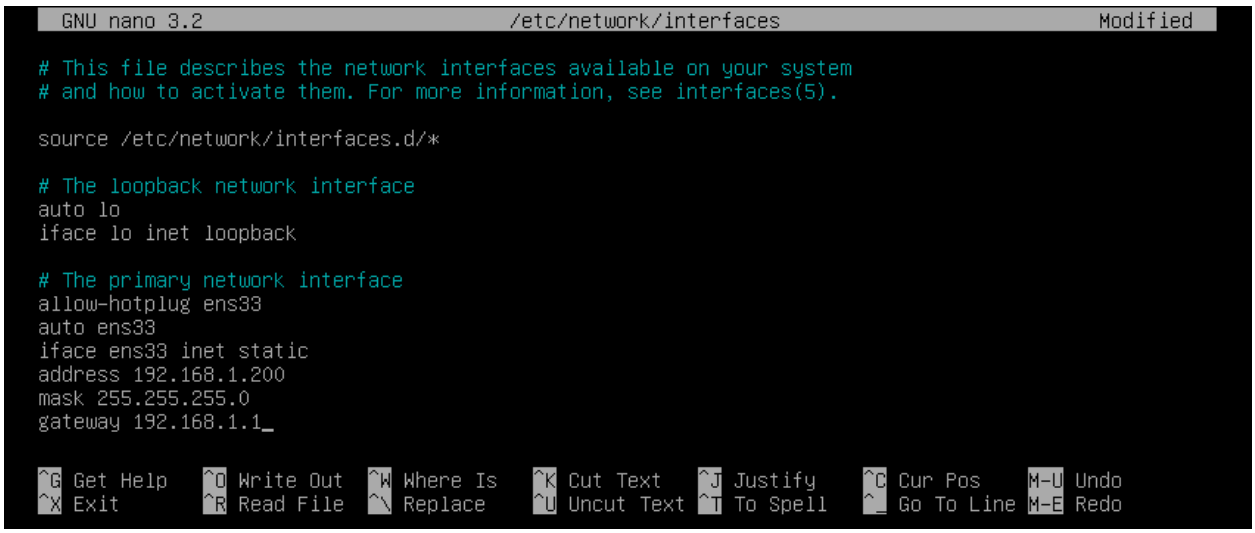

Рисунок – Указание параметров сетевого адаптера

4. Нажать комбинацию **клавиш «Ctrl+S»** для сохранения изменений, а затем нажать комбинацию **клавиш «Ctrl+X»** для выхода из текстового редактора.
5. Ввести команду **«service networking restart»** и нажать **клавишу «ENTER»** для перезапуска сетевого сервиса.
6. Ввести команду **«ip a»** и нажать **клавишу «ENTER»** для получения информации о настройках сетевого адаптера. Убедиться, что IP-адрес изменён на корректный (см. Рисунок – Статический IP-адрес ARMA MC).

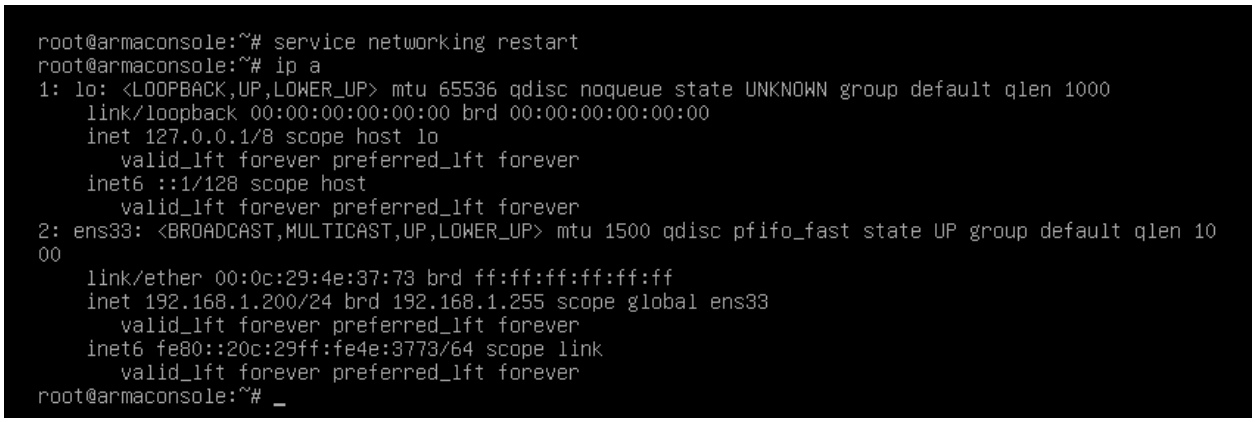

Рисунок – Статический IP-адрес ARMA MC

3.3 Подключение к веб-интерфейсу

Для подключения к веб-интерфейсу необходимо открыть веб-браузер и ввести IP-адрес хоста, указанный в локальном консольном интерфейсе (см. Базовая настройка сетевых интерфейсов) в результате будет отображена страница авторизации в веб-интерфейсе (см. Рисунок – Страница авторизации в веб-интерфейсе).

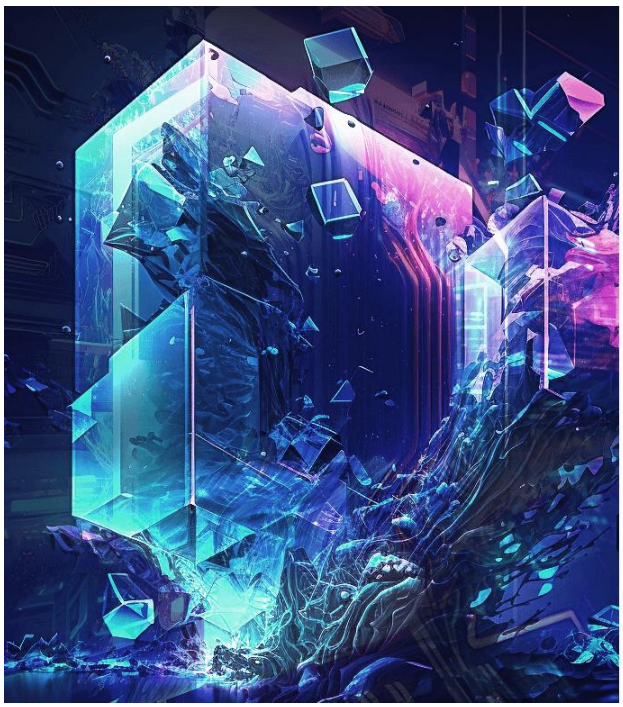

Рисунок – Страница авторизации в веб-интерфейсе

Для входа в веб-интерфейс необходимо указать учетные данные:

- **«Логин»** – по умолчанию **«admin»**;
- **«Пароль»** – по умолчанию **«nimda»**;

и нажать **кнопку «Войти»**.

> **Примечание:**
>
> Указанные выше логин и пароль являются установленными по умолчанию и используются при первоначальном входе. С целью обеспечения ИБ следует изменить данные после первоначального входа.

После успешной аутентификации будет отображен раздел меню **«Обзорная панель»** (см. Рисунок – Обзорная панель).

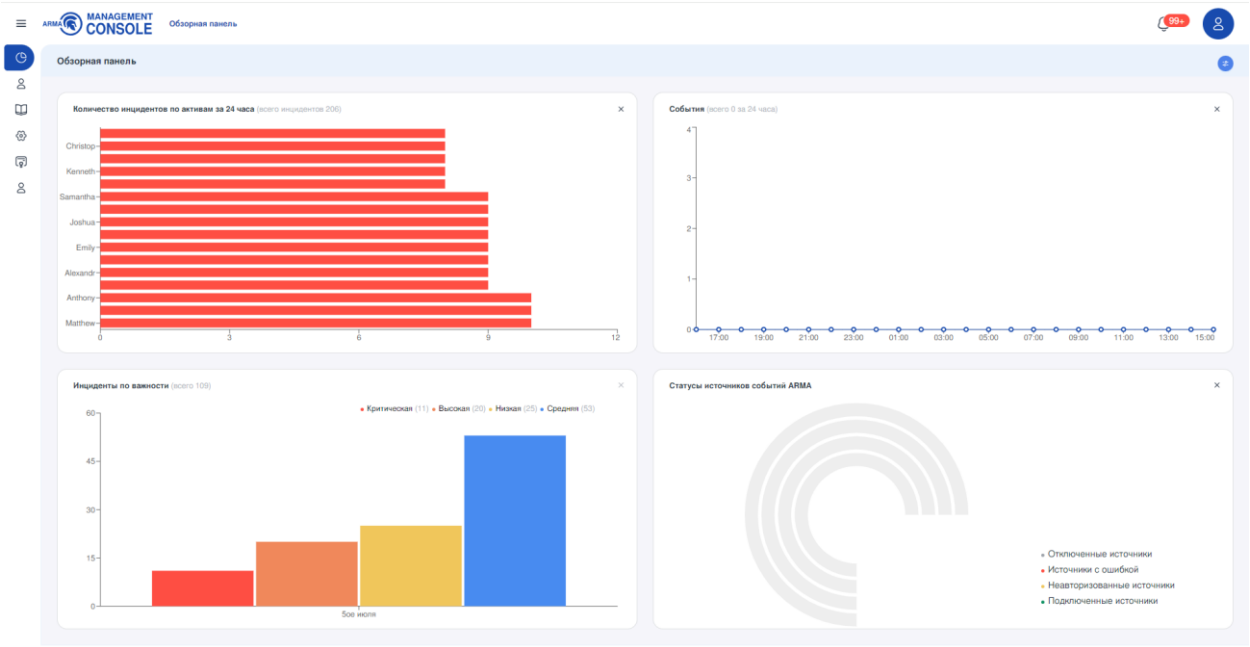

Рисунок – Обзорная панель

Примечание:

При первом подключении для успешной авторизации в **ARMA MC** необходимо активировать лицензию одним из способов, представленных в разделе Активация лицензии.

3.4 Изменение пароля по умолчанию

С целью обеспечения ИБ следует изменить пароли от системных УЗ:

- **«root»** для локального консольного интерфейса;
- **«admin»** для веб-интерфейса.

3.4.1 Изменение пароля УЗ локального консольного интерфейса

Для изменения пароля УЗ локального консольного интерфейса необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«passwd»** и нажать **клавишу «ENTER»**.
3. Ввести новый пароль на запрос **«Новый пароль:»** и нажать **клавишу «ENTER»**.
4. Повторить ввод нового пароля на запрос **«Повторите ввод нового пароля:»** и нажать **клавишу «ENTER»**. В результате корректного ввода пароль будет изменён (см. Рисунок – Изменение пароля УЗ локального консольного интерфейса).

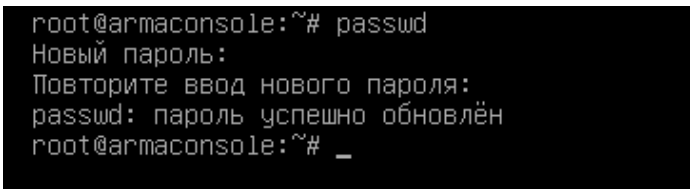

Рисунок – Изменение пароля УЗ локального консольного интерфейса

3.4.2 Изменение пароля УЗ веб-интерфейса

Для изменения пароля УЗ веб-интерфейса необходимо выполнить следующие действия:

1. Выполнить авторизацию в веб-интерфейсе (см. Подключение к веб-интерфейсу).
2. Открыть профиль пользователя, нажав на **кнопку** « ».
3. Пройти по ссылке **«Управление профилем»** « Управление профилем ».
4. На открывшейся странице профиля пользователя (см. Рисунок – Профиль пользователя) нажать на **кнопку «Изменить пароль»**.

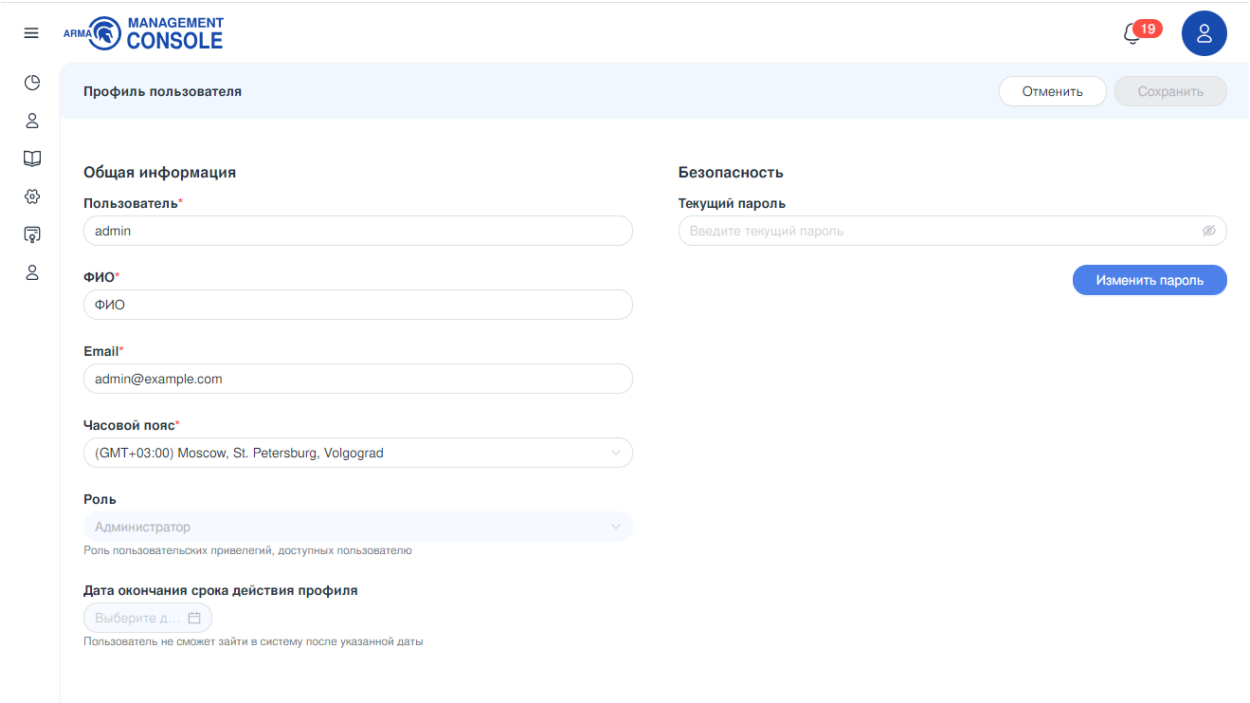

Рисунок – Профиль пользователя

5. В поле **«Текущий пароль»** ввести действующий пароль.
6. В поле **«Новый пароль»** ввести новый пароль.

Примечание:

Предъявляются следующие требования к сложности пароля:

- разрешено использование только латиницы;
- должен содержать как минимум одну цифру;

- должен содержать как минимум одну букву в верхнем регистре;
- должен содержать как минимум одну букву в нижнем регистре;
- должен содержать как минимум один спецсимвол;
- пароль может содержать от 8-ми до 32-х символов;
- новый пароль не может совпадать с текущим паролем.

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

3.5 Подключение к ARMA MC по SSH

3.5.1 Настройка «nftables»

Для настройки сервиса **«nftables»** необходимо выполнить следующие действия:

1. Открыть конфигурационный файл, выполнив команду:

```
nano /etc/nftables.conf
```

2. В области **«type filter hook input priority filter; policy drop;»** в параметре порта назначения **«tcp dport»** вписать порт **«22»** (см. Рисунок – Значение параметра «tcp dport»).

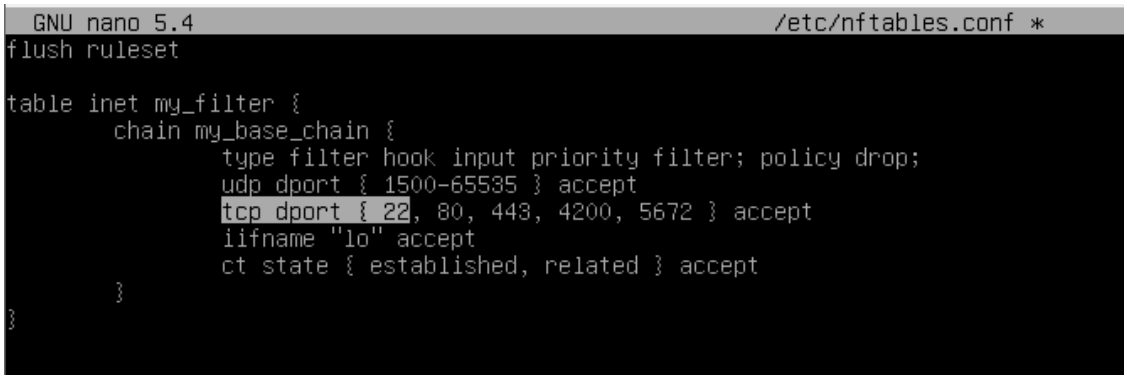

Рисунок – Значение параметра «tcp dport»

3. Сохранить изменения в файле комбинацией **клавиш «CTRL+O»**.
4. Выйти из режима изменения комбинацией **клавиш «CTRL+X»**.
5. Перезагрузить службу **«nftables»**, выполнив команду:

```
systemctl restart nftables
```

При необходимости получения доступа с конкретных IP-адресов или сетей, в конфигурационном файле необходимо указать следующую команду:

```
ip saddr [IP-адрес источника] accept
```

[IP-адрес источника] может быть представлен следующими вариантами:

- IP-адресом узла (см. Рисунок – IP-адрес узла);

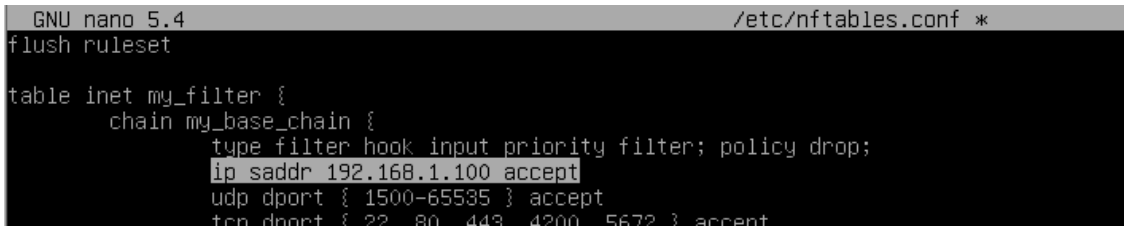

Рисунок – IP-адрес узла

- Группой IP-адресов (см. Рисунок – Группа IP-адресов);

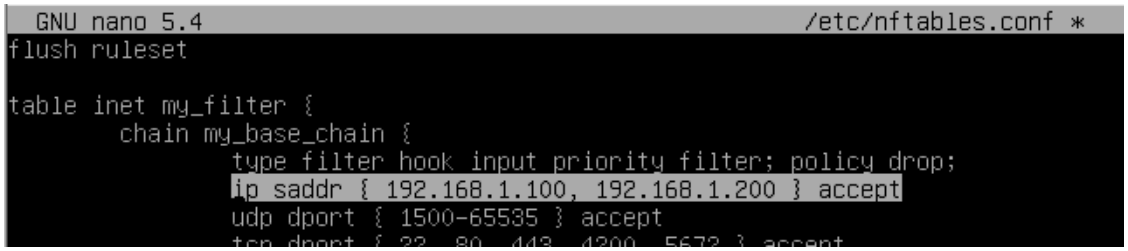

Рисунок – Группа IP-адресов

- IP-адресом сети (см. Рисунок – IP-адрес сети);

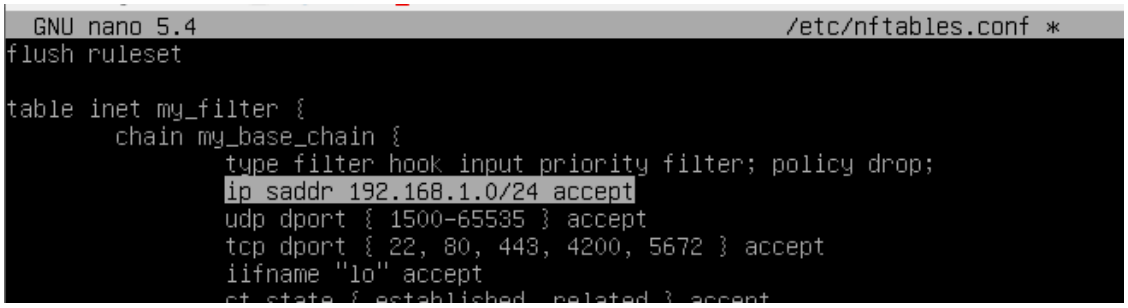

Рисунок – IP-адрес сети

- Комбинацией IP-адреса узла и сети (см. Рисунок – Комбинация IP-адреса узла и сети).

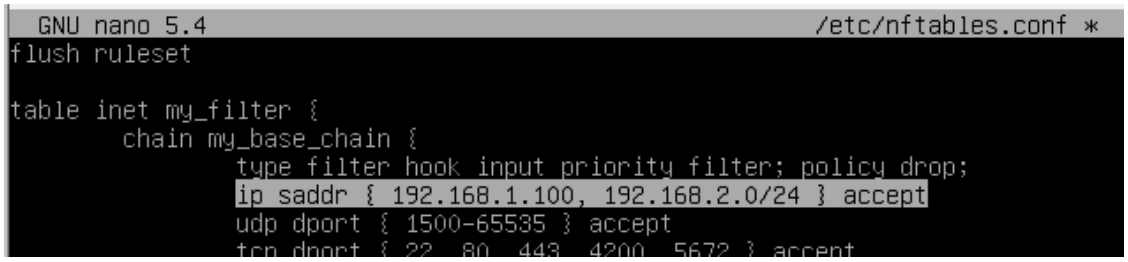

Рисунок – IP-адрес сети

3.5.2 Конфигурирование демона SSH

Для конфигурирования демона **SSH** необходимо выполнить следующие действия:

1. В файле конфигурации демона **SSH** ввести пользователей, с логином которых можно будет удаленно подключаться к **ARMA MC**:

```
nano /etc/ssh/sshd_config
```

2. В случае, если в параметре **«AllowUsers»** был указан администратор **«root»** (см. Рисунок – Значение параметра «AllowUsers»),

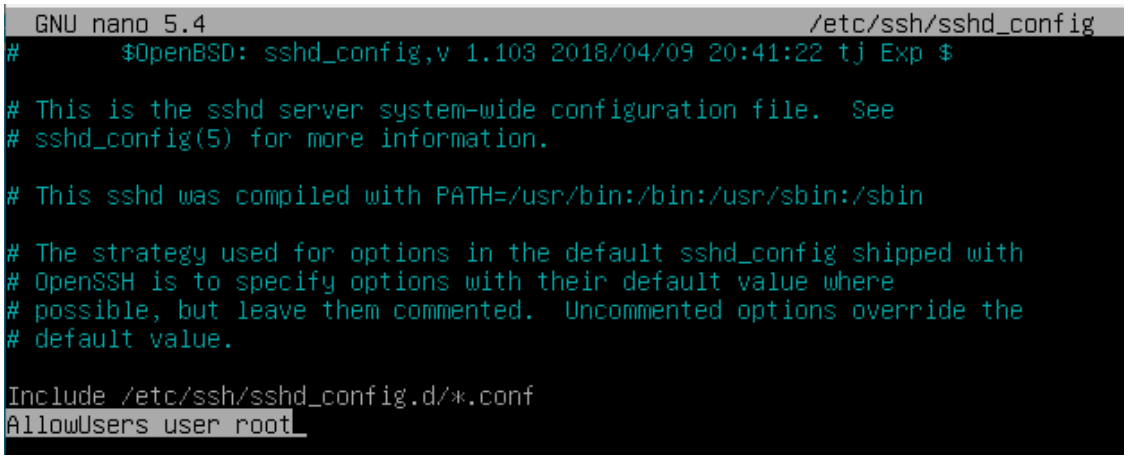

Рисунок – Значение параметра «AllowUsers»

необходимо изменить значение параметра **«PermitRootLogin»** со значения **«no»** на значение **«yes»** в конце файла (см. Рисунок – Значение параметра «PermitRootLogin»).

Рисунок – Значение параметра «PermitRootLogin»

3. Перезагрузить службу **SSH**, выполнив команду:

```
systemctl restart ssh
```

4. Проверить подключение по **SSH**.

3.5.3 Проверка и управление состоянием служб

Для проверки состояния службы необходимо выполнить команду (см. Рисунок – Проверка состояния службы):

```
systemctl status [название службы]
```

Рисунок – Проверка состояния службы

Для перезагрузки службы необходимо выполнить команду:

```
systemctl restart [название службы]
```

Для остановки службы необходимо выполнить команду:

```
systemctl stop [название службы]
```

Для старта службы необходимо выполнить команду:

```
systemctl start [название службы]
```

3.6 Подключение к ARMA MC с применением двухфакторной аутентификации

Для подключения к **ARMA MC** с применением двухфакторной аутентификации необходимо настроить доступ к порталу авторизации **ARMA IFW**:

1. Перейти в веб-интерфейс **ARMA IFW**.
2. Создать разрешающие правила МЭ для необходимого интерфейса и применить изменения (см. раздел Настройка правил МЭ «Руководства пользователя по эксплуатации **ARMA FW»**). Параметры правил представлены в списке (в качестве примера взят интерфейс OPT1):
    - Доступ к порталу авторизации:
        - **«Действие»** – «Разрешить (Pass)»;
        - **«Интерфейс»** – «OPT1»;
        - **«Протокол»** – «TCP»;
        - **«Отправитель»** – «OPT1 сеть»;
        - **«IP-адрес назначения»** – «Этот межсетевой экран»;
        - **«Диапазон портов назначения»** – «Другое/8000»;
        - **«Описание»** – «Доступ к порталу авторизации»;
    - Доступ к веб-серверу по HTTP:
        - **«Действие»** – «Разрешить (Pass)»;
        - **«Интерфейс»** – «OPT1»;
        - **«Протокол»** – «TCP»;
        - **«Отправитель»** – «OPT1 сеть»;
        - **«IP-адрес назначения»** – «[IP-адрес ARMA MC]»;
        - **«Диапазон портов назначения»** – «HTTP»;
        - **«Описание»** – «Разрешающее правило HTTP»;

- Доступ к веб-серверу по HTTPS:
    - **«Действие»** – «Разрешить (Pass)»;
    - **«Интерфейс»** – «OPT1»;
    - **«Протокол»** – «TCP»;
    - **«Отправитель»** – «OPT1 сеть»;
    - **«IP-адрес назначения»** – «[IP-адрес ARMA MC]»;
    - **«Диапазон портов назначения»** – «HTTPS»;
    - **«Описание»** – «Разрешающее правило HTTPS».

3. Настроить Radius-сервер (см. раздел Radius Руководства пользователя **ARMA IFW**).
4. Добавить зону авторизации (см. раздел Добавление портала авторизации Руководства пользователя **ARMA IFW**).

   Обязательные параметры зоны представлены в списке:

   - **«Интерфейсы»** – «OPT1»;
   - **«Аутентификация через»** – выбрать созданный Radius-сервер;
   - **«Описание»** – заполнить описание.

5. Ввести в адресную строку веб-браузера IP-адрес **ARMA MC**.
6. В появившейся форме входа ввести имя пользователя и пароль.
7. Подтвердить вход в **ARMA MC** с помощью зарегистрированного второго фактора.

4 УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

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

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

Активация лицензии автоматическим способом производится при наличии доступа к сети Интернет.

Активация лицензии ручным способом производится без доступа к сети Интернет.

4.1 Активация лицензии

При первоначальном входе необходимо произвести активацию лицензии **ARMA MC**.

При первом подключении к **ARMA MC** после авторизации, окно запроса на активацию лицензии будет выведено автоматически (см. Рисунок – Активация новой лицензии).

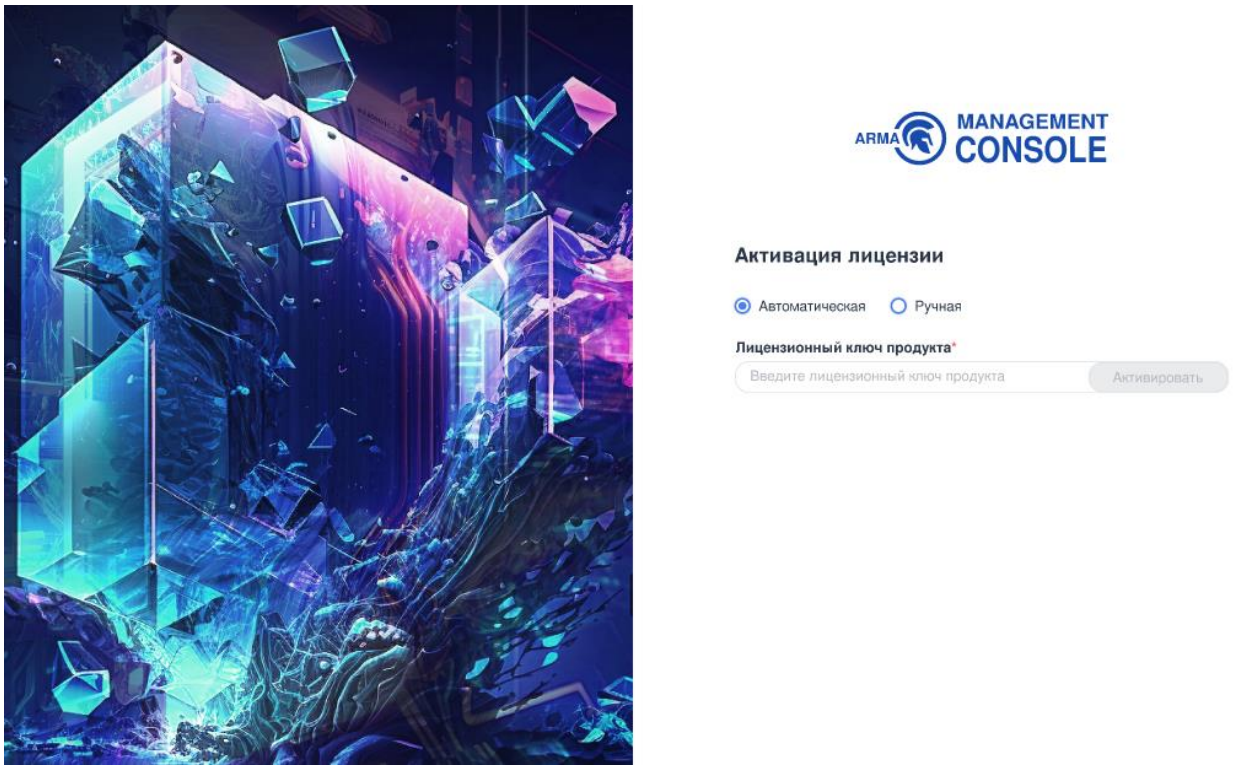

Рисунок – Активация новой лицензии

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

Примечание:

Активировать лицензию возможно только обладая УЗ, наделенной правами администратора безопасности.

4.1.1 Автоматическая активация лицензии

Система предлагает активировать лицензию автоматически сразу после успешной авторизации при первом входе. Для автоматической активации лицензии необходимо выполнить следующие действия:

1. Убедиться, что в секции **«Активация лицензии»** выбран пункт **«Автоматическая»** (см. Рисунок – Автоматическая активация).

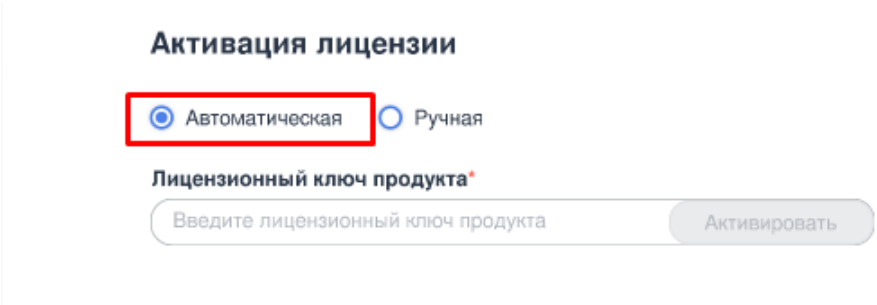

Рисунок – Автоматическая активация

2. В поле **«Лицензионный ключ»** указать лицензионный ключ и нажать **кнопку «Активировать»** (см. Рисунок – Лицензионный ключ).

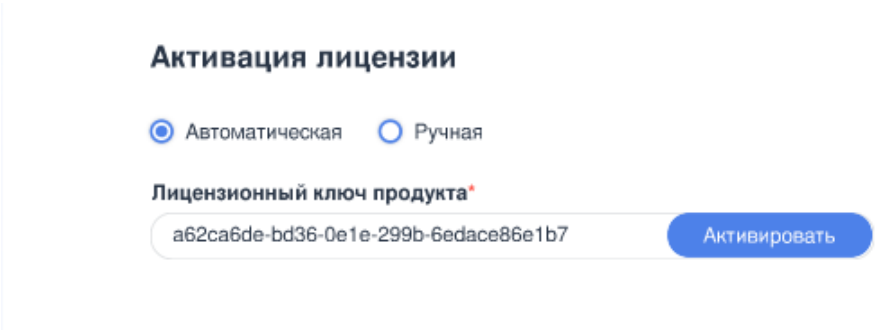

Рисунок – Лицензионный ключ

3. После успешной активации лицензии произойдёт перенаправление на страницу с информацией о текущей лицензии, и отобразится всплывающее уведомление об активации лицензии (см. Рисунок – Информация о лицензии).

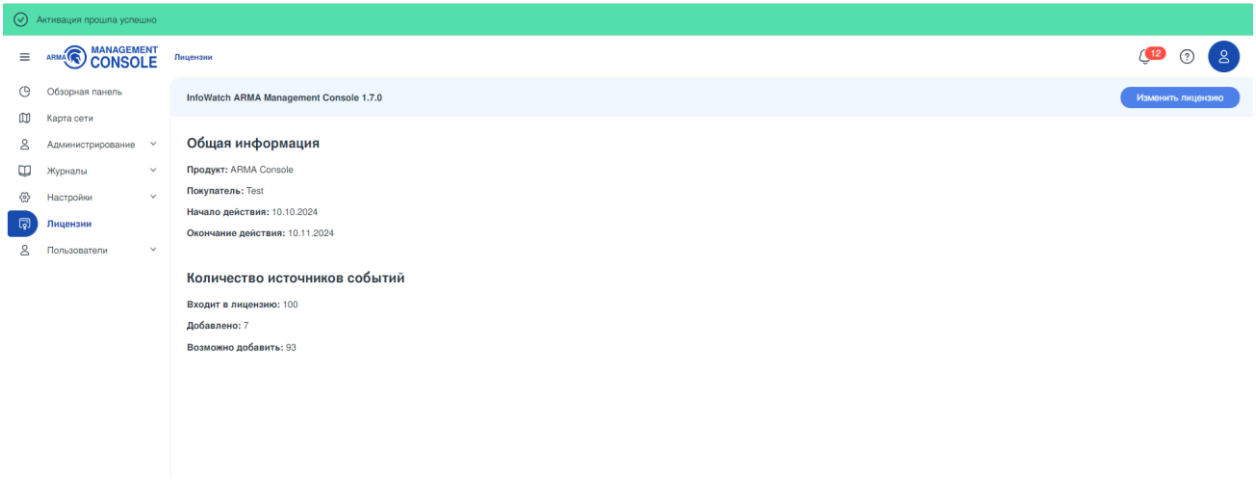

Рисунок – Информация о лицензии

При вводе некорректного лицензионного ключа отобразится соответствующее уведомление (см. Рисунок – Некорректный ключ).

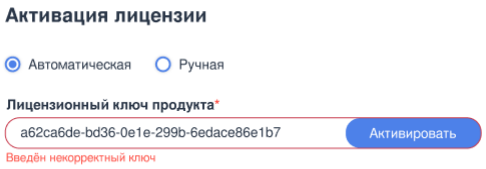

Рисунок – Некорректный ключ

4.1.2 Ручная активация лицензии

Для ручной активации лицензии необходимо выполнить следующие действия:

1. В секции **«Активация лицензии»** выбрать пункт **«Ручная»**.
2. В поле **«Лицензионный ключ»** указать лицензионный ключ и нажать **кнопку «Получить токен»** (см. Рисунок – Лицензионный ключ).

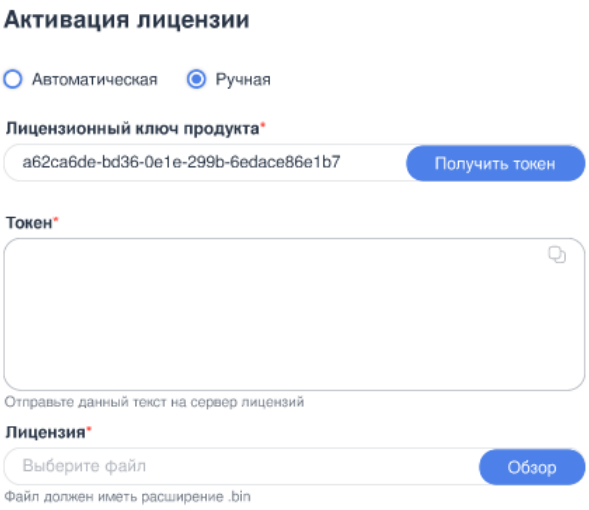

Рисунок – Лицензионный ключ

3. Скопировать значение поля параметра **«Токен»** (см. Рисунок – Получение токена для активации лицензии) и направить в техподдержку **ООО «ИнфоВотч АРМА»** для получения файла лицензии **«license.bin»**.

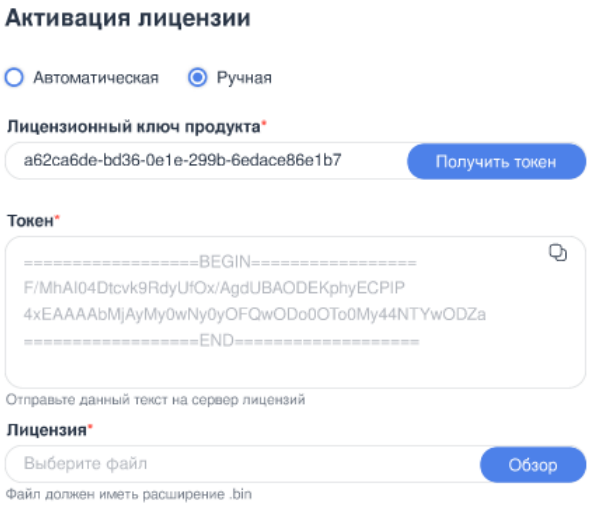

Рисунок – Получение токена для активации лицензии

4. В секции **«Лицензия»** нажать на **кнопку «Обзор»**, в открывшемся окне проводника выбрать полученный файл **«license.bin»**, нажать **кнопку «Открыть»**. **Кнопка «Активировать»** станет активной (см. Рисунок – Кнопка «Активировать»). Нажать **кнопку «Активировать»**.

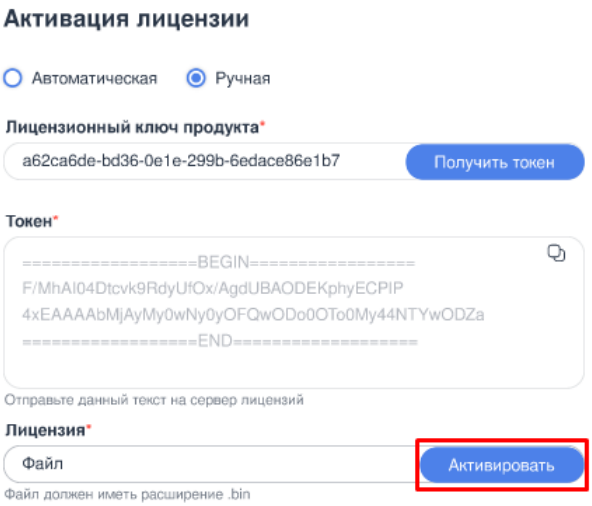

Рисунок – Кнопка «Активировать»

5. После успешной активации лицензии произойдёт перенаправление на страницу с информацией о текущей лицензии, и отобразится всплывающее уведомлении об активации лицензии (см. Рисунок – Информация о лицензии).

При попытке загрузки некорректного формата файла лицензии (см. Рисунок – Некорректный формат файла лицензии) или файла лицензии с некорректным

содержимым (см. Рисунок – Некорректное содержимое файла лицензии) отобразится соответствующее уведомление.

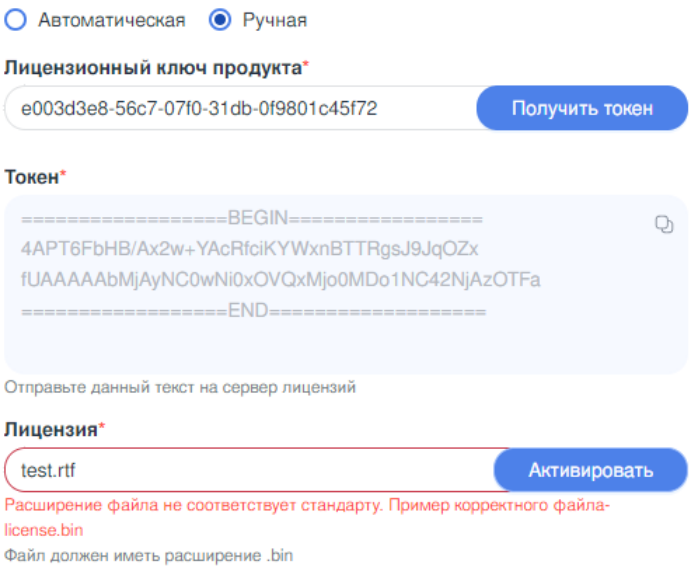

Рисунок – Некорректный формат файла лицензии

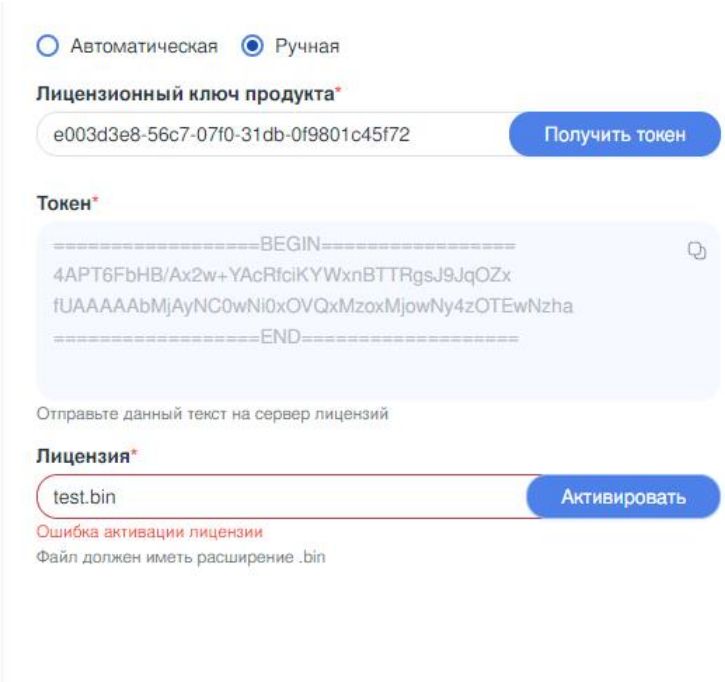

Рисунок – Некорректное содержимое файла лицензии

4.2 Информация о текущей лицензии

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

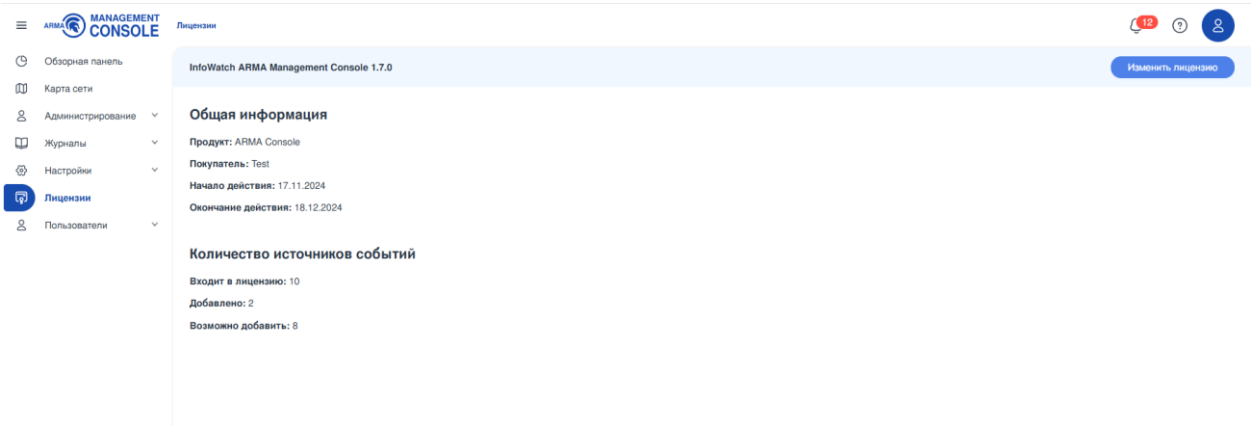

Рисунок – Текущая лицензия

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

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

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

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

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

4.2.1 Изменение лицензии

Для изменения лицензии на панели навигации необходимо выбрать раздел **«Лицензии»**. На открывшейся странице в правом верхнем углу нажать **кнопку «Изменить лицензию»**.

Шаги по автоматической активации описаны в разделе Автоматическая активация лицензии.

Шаги по ручной активации описаны в разделе Ручная активация лицензии.

5 ОПИСАНИЕ ЛОКАЛЬНОГО КОНСОЛЬНОГО ИНТЕРФЕЙСА

В настоящем разделе представлено описание ЛКИ. Управление в ЛКИ происходит только с использованием клавиатуры.

5.1 Выключение ARMA MC

Для выключения **ARMA MC** необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«poweroff»** и нажать **клавишу «ENTER»**.

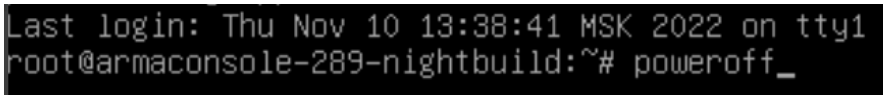

Рисунок – Выключение ARMA MC

5.2 Перезагрузка ARMA MC

Для перезагрузки **ARMA MC** необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«reboot»** и нажать **клавишу «ENTER»**.

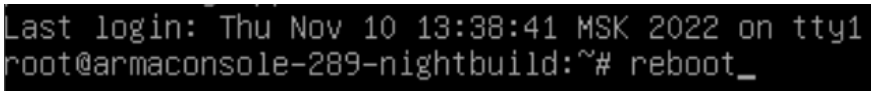

Рисунок – Перезагрузка ARMA MC

5.2.1 Проверка доступности хоста ОС Windows

Для проверки доступности хоста необходимо выполнить следующие действия:

1. Открыть командную строку Windows.
2. Ввести команду **«ping [IP-адрес хоста]»**, в примере используется 87.250.250.242 и нажать **клавишу «ENTER»**.
3. По результатам проверки будет выведено сообщение:
   - если хост доступен (см. Рисунок – Хост доступен);
   - если хост не доступен (см. Рисунок – Хост недоступен).

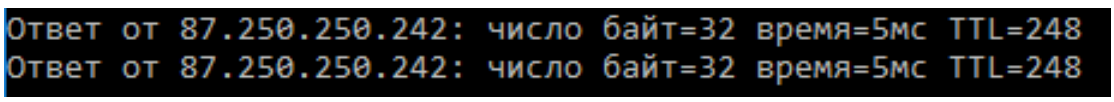

Рисунок – Хост доступен

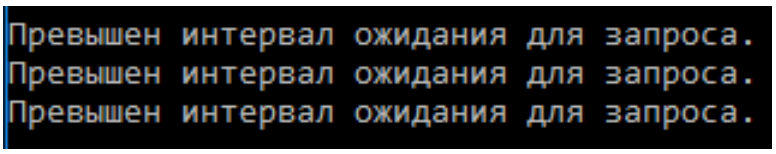

Рисунок – Хост недоступен

Примечание:

IP-адрес хоста приведен в виде примера и может отличаться в зависимости от настроек сети и заданного диапазона IP-адресов.

5.2.2 Проверка доступности хоста ОС Linux

Для проверки доступности хоста необходимо выполнить следующие действия:

1. Открыть командную строку Linux.
2. Ввести команду **«ping [IP-адрес хоста]»**, в примере используется 10.0.2.15 и нажать **клавишу «ENTER»**.
3. По результатам проверки будет выведено сообщение:
   - если хост доступен (см. Рисунок – Хост доступен);
   - если хост не доступен (см. Рисунок – Хост недоступен).

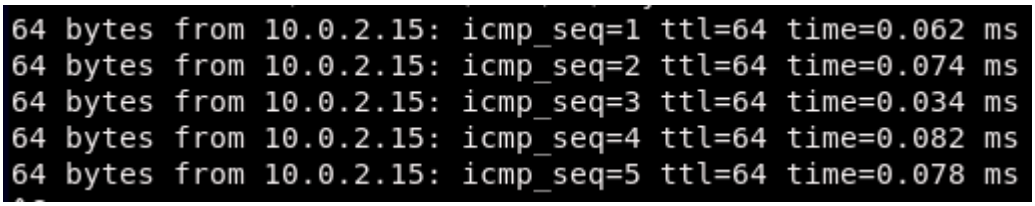

Рисунок – Хост доступен

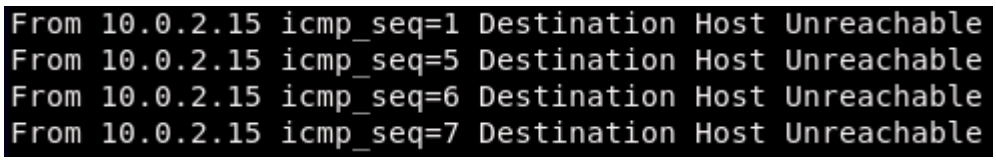

Рисунок – Хост недоступен

Примечание:

IP-адрес хоста приведен в виде примера и может отличаться в зависимости от настроек сети и заданного диапазона IP-адресов.

Примечание:

Показателем отсутствия связи с хостом является ответ от хоста «destination host unreachable», «конечный узел недоступен».

5.3 Обновление ARMA MC

Обновление **ARMA MC** с версии 1.6 на версию 1.7 возможно осуществить через:

- веб-интерфейс (см. Обновление версии);
- локальный консольный интерфейс (ЛКИ).

Для обновления через ЛКИ необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Перейти в директорию **«/opt»** и создать пустой каталог, например **«amc»**:

```
cd /tmp/opt
mkdir amc
```

3. Распаковать архив командой **«tar -xzf [название архива] -C [название каталога]»**, например:

```
tar -xzf armaconsole_1.7.0_amd64.tar.gz -C amc
```

4. Перейти в каталог **«amcansible»**, например:

```
cd ./amc/amcansible
```

5. Сравнить версию установленной **ARMA MC**, указанной в левом нижнем углу веб-интерфейса, с версией обновления. Для проверки версии обновления ввести команду:

```
sudo ./setup.sh -v
```

   Версия обновления будет указана в строке **«This package can be used as update for versions»**.

6. Если версия установленной **ARMA MC** больше или равна версии, указанной в строке **«This package can be used as update for versions»**, выполнить команду:

```
sudo ./setup.sh -u
```

   В консоли появится надпись **«Installation completed»** и **ARMA MC** перезагрузится.

7. После перезагрузки проверить в браузере доступность веб-интерфейса.

Примечание:

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

5.3.1 Автоматическое резервное копирование

После запуска команды **«sudo ./setup.sh -u»** (см. п.6 Обновление ARMA MC) запускается механизм создания резервной копии **ARMA MC**.

Резервная копия создается в папке **«backup»**, которая располагается на одном уровне с файлом **«setup.sh»**. В случае обновления **ARMA MC** через веб-интрефейс (см. Обновление версии), резервная копия сохранится в директории **«/opt/armaupdate/backup»**.

5.3.2 Возможные проблемы и их решения

В случае отсутствия ответа **ARMA MC** рекомендуется:

1. Выполнить установку текущей версии (см. Установка).
2. Скопировать папку **«backup»** в директорию с файлом **«setup.sh»** и выполнить команду восстановления:

```
sudo ./setup.sh -r
```

Примечание:

В случае возникновения любых ошибок при обновлении рекомендуется скопировать папку **«backup»** на отдельный диск, а также отправить файл **«/var/log/armaconsole/setup.log»** в **INFOWATCH ARMA**.

5.4 Резервное копирование и восстановление ARMA MC

Резервную копию возможно использовать для восстановления конфигурации при её повреждении, отката изменений конфигурации или переноса конфигурации на новое устройство.

Для создания локальной резервной копии конфигурации необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Перейти в директорию с файлом **«setup.sh»**.
3. Выполнить команду:

```
sudo ./setup.sh -b
```

В результате выполнения данной команды будет создана папка с резервной копией на одном уровне с файлом **«setup.sh»**.

Восстановление резервной копии запускается командой:

```
sudo ./setup.sh -r
```

Примечание:

Механизм восстановления может быть применён только для той версии **ARMA MC**, для которой была сделана резервная копия.

5.5 Сервисы ARMA MC

ARMA MC включает в себя следующие сервисы:

Таблица «Сервисы ARMA MC»

Название сервиса	Полное наименование сервиса	Путь к журналу сервиса
amccelery	amccelery.service	/var/log/armaconsole/celeryd.log
amccelerybeat	amccelerybeat.service	/var/log/armaconsole/celerybeat.log
amcchecker	amcchecker.service	Журнал отсутствует
amcclient	amcclient.service	/var/log/armaconsole/license.log
amccore	amccore.service	var/log/armaconsole/console.log
amccorrelator	amccorrelator.service	/var/log/armaconsole/correlator.log
amcvector	mcvector.service	Журнал отсутствует
elasticsearch	elasticsearch.service	/var/log/elasticsearch
nginx	nginx.service	/var/log/nginx
postgresql@13-main	postgresql@13-main.service	/var/log/postgresql/postgresql-13-main.log
postgresql	postgresql.service	/var/log/postgresql
rabbitmq-server	rabbitmq-server.service	/var/log/rabbitmq/rabbit@amcdebian.log
redis-server	redis-server.service	/var/log/redis/redis-server.log

5.5.1 Перезагрузка сервисов

Для перезагрузки сервиса необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«systemctl restart [servicename]»**, где:

   [servicename] – это название сервиса (см. Сервисы ARMA MC).

   Например, для перезагрузки сервиса «amccelery», необходимо ввести команду **«systemctl restart amccelery»** и нажать **клавишу «ENTER»**.

Результат выполнения команды будет следующим:

- в случае успешного перезапуска сервиса в командной строке сообщений не будет;

- в случае безуспешного перезапуска сервиса будет выведено сообщение об ошибке, которая возникла при попытке перезапуска.

5.5.2 Просмотр журналов сервисов

Для просмотра журналов сервисов необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду:
   - vim [path_to_log_file] – для редактора **«Vim»**;
   - nano [path_to_log_file] – для редактора **«Nano»**;
   - cat [path_to_log_file] – для утилиты **«Cat»**, где:

     [path_to_log_file] – это название сервиса (см. Сервисы ARMA MC).

     Например, для просмотра журнала сервиса «amcclient», необходимо ввести команду **«vim /var/log/armaconsole/license.log»**.
3. Нажать **клавишу «ENTER»**.

5.6 Работа с SSH

В **ARMA MC** протокол SSH по умолчанию включен.

Чтобы произвести удалённое подключение и управление сервером **ARMA MC** необходимо сконфигурировать **nftables**.

Для включения сервиса «SSH» необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«sudo systemctl enable sshd»** и нажать **клавишу «ENTER»**.

Для выключения сервиса «SSH» необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«systemctl stop sshd»** и нажать **клавишу «ENTER»**.

6 ВОЗМОЖНЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЕ

В настоящем разделе представлено описание возможных проблем при работе с **ARMA MC** и их решения.

6.1 Выход ARMA MC из строя

Для получения подробных логов по возможным ошибкам, которые могли повлечь за собой отключение **ARMA MC**, необходимо проверить файлы журналов основных сервисов **ARMA MC**, указанных в разделе Сервисы ARMA MC. Инструкция просмотра журналов сервисов описана в разделе Просмотр журналов сервисов

6.2 Ошибка «elasticsearch»

Для устранения ошибок с сервисом «elasticsearch» необходимо перезагрузить **ARMA MC** (см. Перезагрузка ARMA MC).

6.3 Не срабатывает правило коррелятора

Для выяснения причин, по которым могут не работать правила корреляции, необходимо посмотреть файл журнала сервиса «amccorrelator» (см. Просмотр журналов сервисов).

6.4 Недостаточно места на диске

Для анализа дискового пространства необходимо выполнить следующие действия:

1. Выполнить авторизацию в ЛКИ (см. Авторизация в локальном консольном интерфейсе).
2. Ввести команду **«df -h»** и нажать **клавишу «ENTER»**.
3. Результатом выполнения команды будет отчет о заполненности накопителей устройства. Необходимо обратить внимание на заполненность файловой системы /dev/sda1.

```
root@armaconsole-289-nightbuild:/var/log/redis# df -h
Файловая система Размер Использовано  Дост Использовано% Смонтировано в
udev               2,0G             0  2,0G            0% /dev
tmpfs              394M          708K  393M            1% /run
/dev/sda1           20G          4,3G   15G           23% /
tmpfs              2,0G           32K  2,0G            1% /dev/shm
tmpfs              5,0M             0  5,0M            0% /run/lock
tmpfs              394M             0  394M            0% /run/user/0
```

Рисунок – Отчет о заполненности накопителей устройства

6.5 Отсутствует доступ к веб-интерфейсу

При отсутствии доступа к веб-интерфейсу в случае корректной работы всех сервисов необходимо перезагрузить **ARMA MC** (см. Перезагрузка ARMA MC).

В случае возникновения проблем с доступом к веб-интерфейсу **ARMA MC**, установленной на виртуальную платформу, необходимо убедиться в корректности имён интерфейсов.