Руководство администратора

версия 12 ред. от 21.03.2025

Листов 28

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**.

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
Руководство пользователя ARMA FW	Руководство пользователя по эксплуатации InfoWatch ARMA Firewall

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 требованиями к среде функционирования (см. Требования 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 команд 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. ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

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

Установка **ARMA MC** производится на аппаратную или виртуальную платформу, на которой установлена ОС **«Debian 11 (русская локализация)»**.

Для установки используется установочный пакет **«InfoWatch-ARMA-Центр-Управления_[номер_версии].deb»** (здесь и далее **«[номер_версии]»** заменяется на соответствующее значение, например, **«1.8.2»**).

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;
  - для ОС семейства Linux /*nix – Chrome для Linux /*nix.

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.

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:

- **процессор** – 2,0 ГГц, четырёхъядерный, x64;
- **ОЗУ** – 8 ГБ;
- **интерфейсы** – последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры;
- **накопитель** – 512 ГБ, SSD;
- **сетевые интерфейсы** – не менее 4 x Ethernet 100/1000 Мбит/с.

2.2. Требования к виртуальной платформе

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

- Hyper-V 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:

- **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**.

Примечание:

Установка должна проводиться от имени УЗ с ролью уровня «**Администратор ОС**».

3.1. Установка

Примечание:

Для корректной установки **ARMA MC** на ОС должна быть установлена русская локаль **«ru_RU.UTF-8»** и все пакеты ПО из следующего списка:

linux-image-amd64, lsb-release, acl, open-vm-tools, curl, jq, vim, gnupg, tcpdump, nginx, python3, python3-apt, python3-pip, python3-venv, python3-dev, postgresql, postgresql-contrib, rabbitmq-server, redis, redis-server, gcc, make, libpq-dev, openssl, ca-certificates, bash, default-jre, apt-utils, sudo, gettext, golang, elasticsearch (версия 7.12.0).

Загрузите установочный пакет **ARMA MC** – **«InfoWatch-ARMA-Центр-Управления_[номер_версии].deb»**.

Запустите установку **ARMA MC**, выполнив команду:

```
dpkg -i InfoWatch-ARMA-Центр-Управления_[номер_версии].deb
```

По окончании процесса установки будет выведено сообщение **«Installation completed.»**.

3.2. Подключение к веб-интерфейсу

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

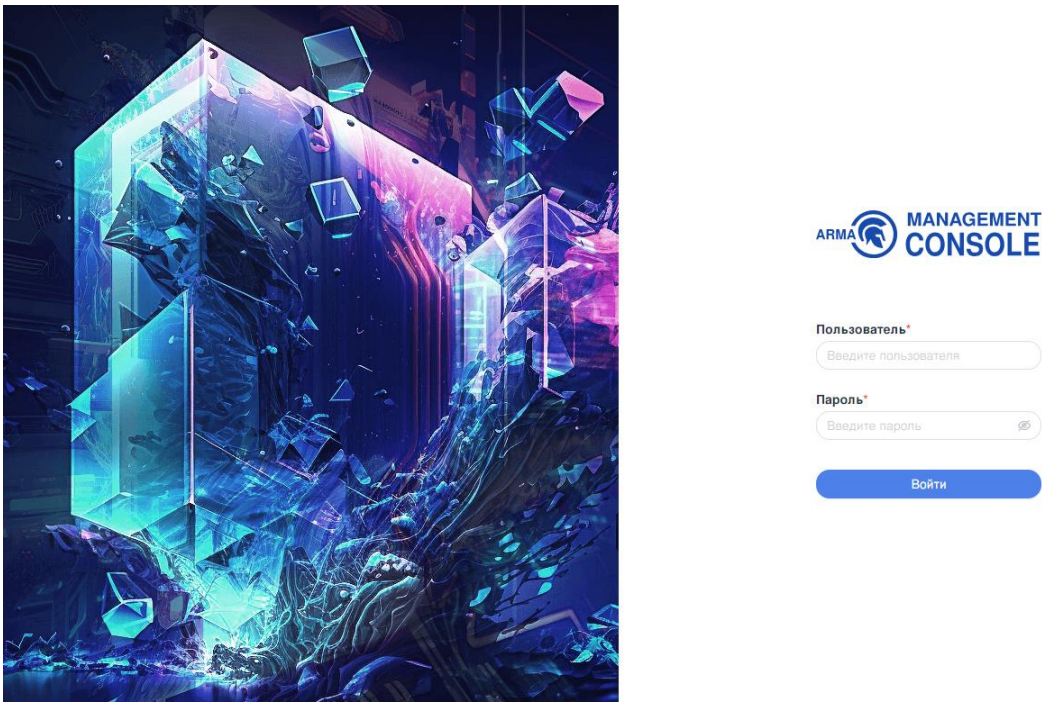


Рисунок – Страница авторизации в веб-интерфейсе

Примечание:

Из соображений безопасности добавлено ограничение на период бездействия пользователя в веб-интерфейсе. Если авторизованный пользователь неактивен в течение 15 минут, сессия будет разорвана и потребуется повторная авторизация.

Для входа в веб-интерфейс необходимо указать учётные 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 отображён раздел меню **«Обзорная панель»** (см. Рисунок – Обзорная панель).

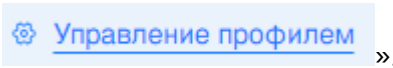
Рисунок – Обзорная панель

Примечание:

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

3.2.1. 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»** « 

».
4. На открывшейся странице профиля пользователя (см. Рисунок – Профиль пользователя) нажать на **кнопку «Изменить пароль»**.

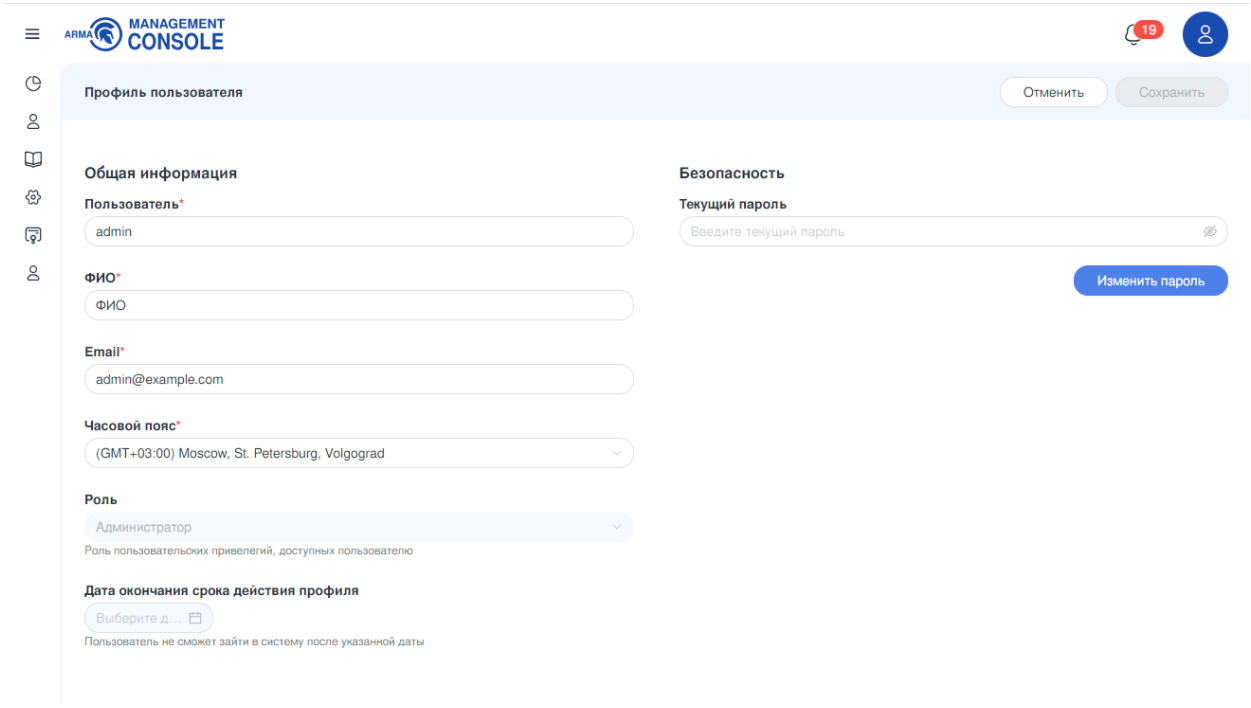


Рисунок – Профиль пользователя

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»**.

3.3. Подключение к ARMA MC по SSH

3.3.1. Настройка «nftables»

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

1. Открыть конфигурационный файл, введя команду:

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

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

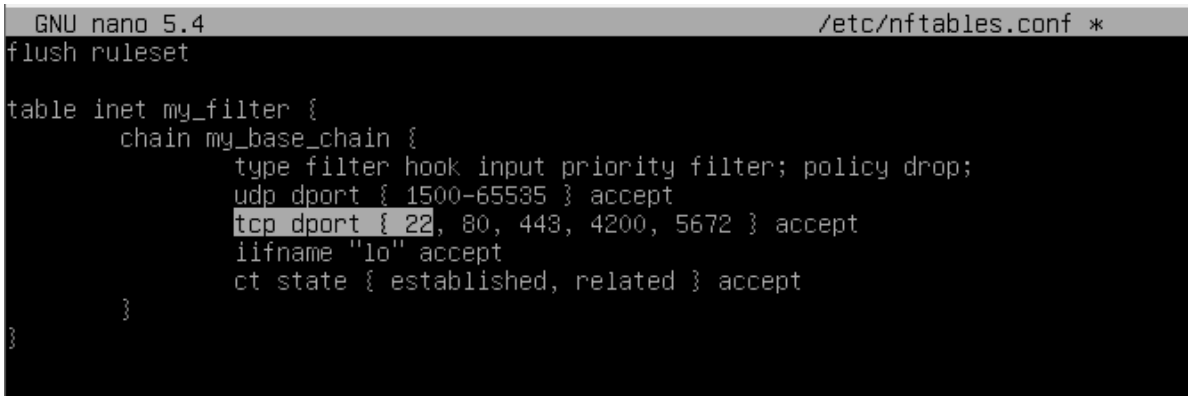


Рисунок – Значение параметра «tcp dport»

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

```
systemctl restart nftables
```

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

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

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

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

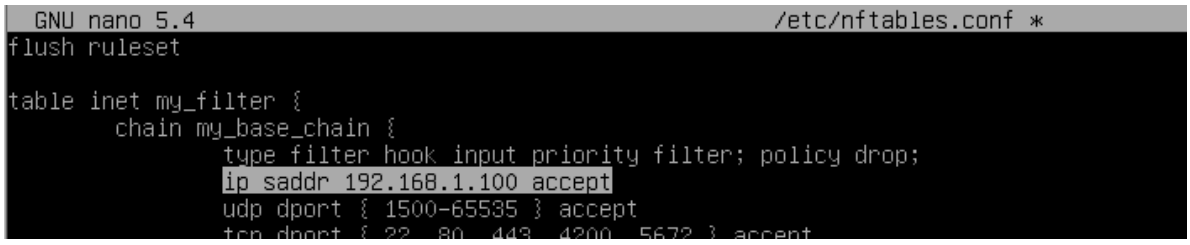


Рисунок – IP-адрес узла

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

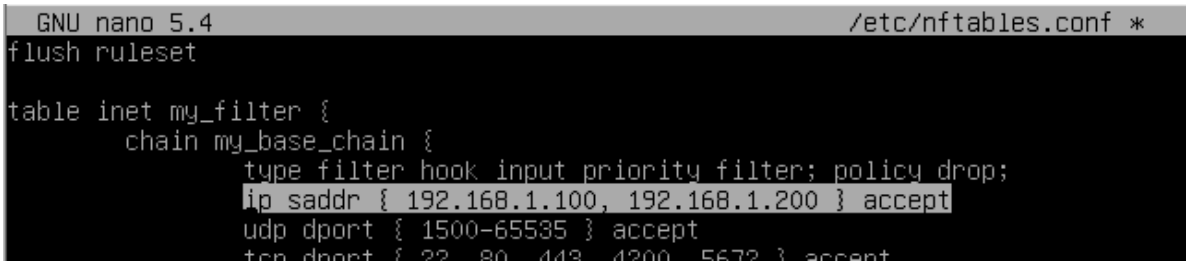


Рисунок – Группа IP-адресов

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

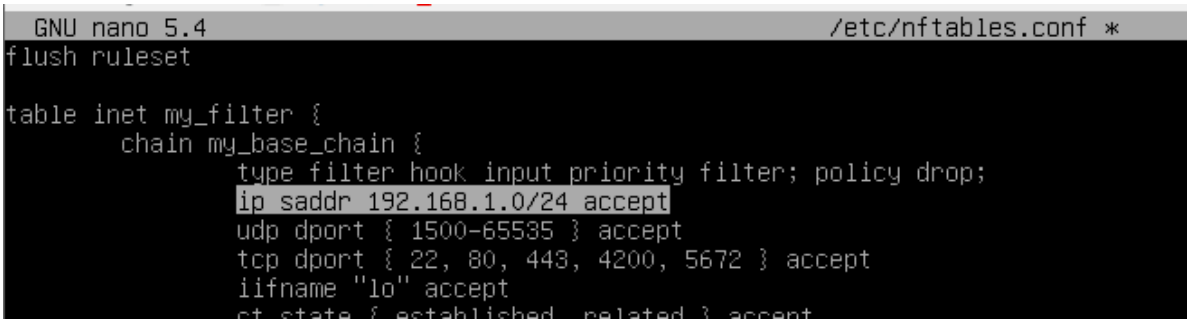


Рисунок – IP-адрес сети

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

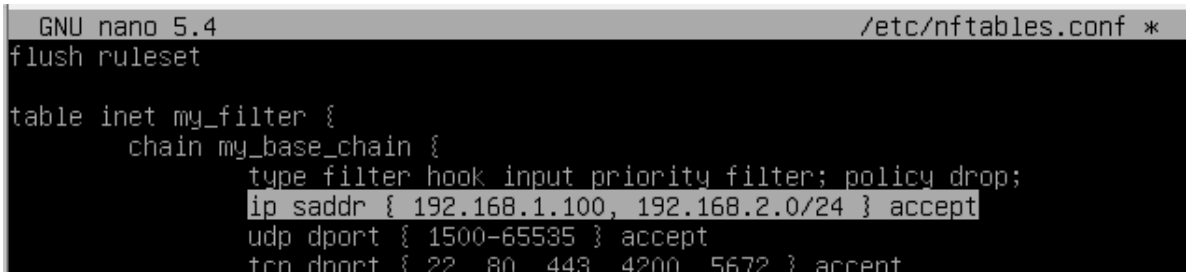


Рисунок – IP-адрес сети

3.4. Подключение к ARMA MC с применением двухфакторной аутентификации

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

1. Перейти в веб-интерфейс **ARMA FW**.
2. Создать разрешающие правила МЭ для необходимого интерфейса и применить изменения (см. раздел Настройка правил МЭ «Руководства пользователя **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 Радиус Руководства пользователя **ARMA FW**).
4. Добавить зону авторизации (см. раздел Добавление портала авторизации` Руководства пользователя **ARMA FW**).

   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).

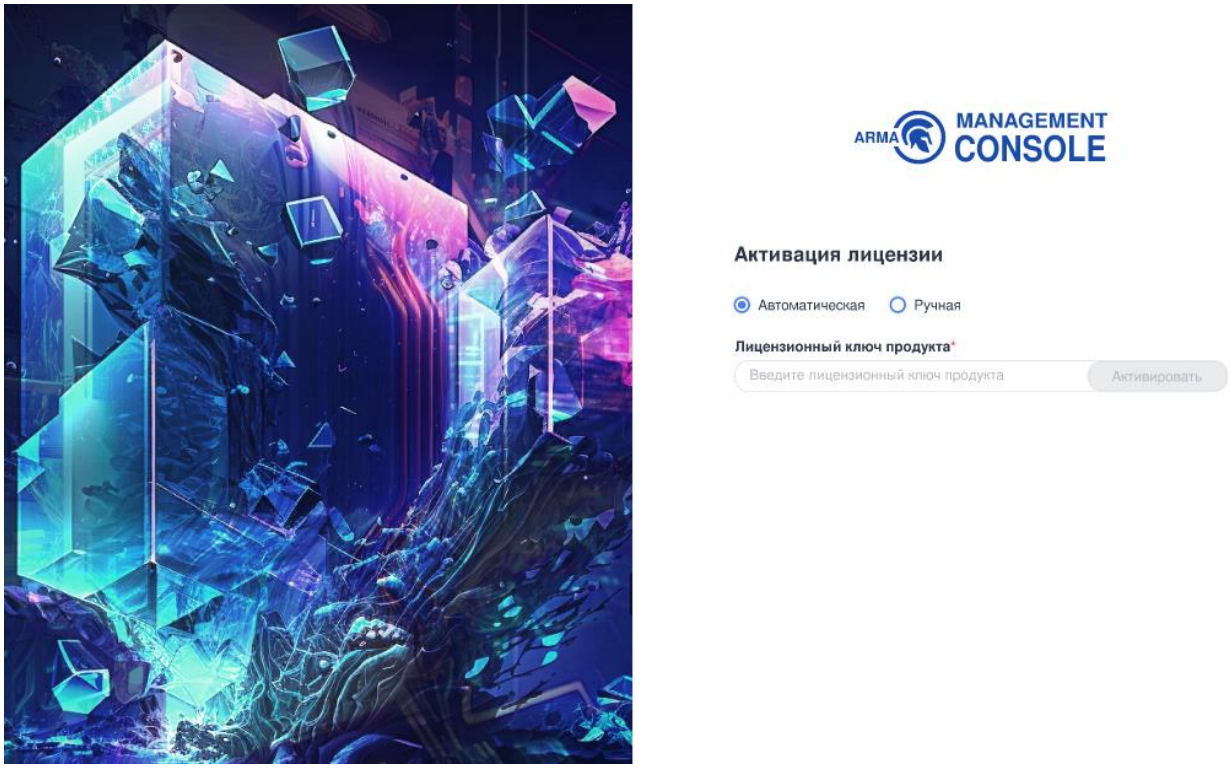


Рисунок – Активация новой лицензии

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).

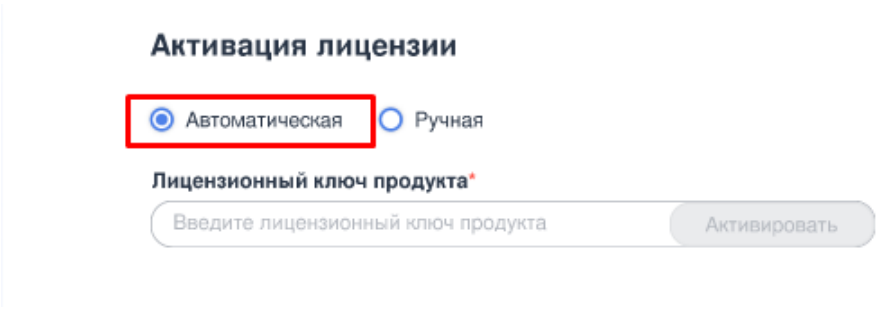


Рисунок – Автоматическая активация

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

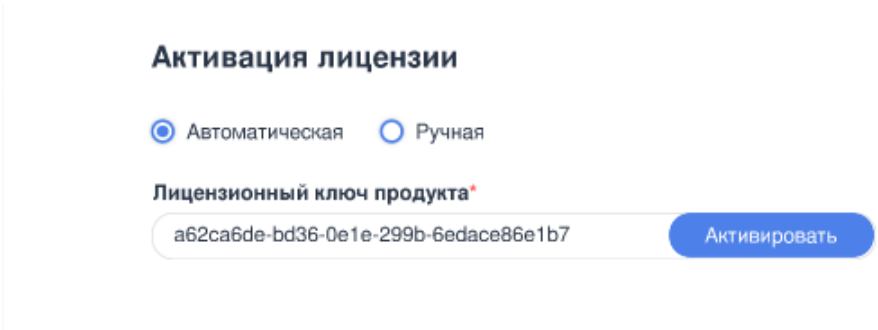


Рисунок – Лицензионный ключ

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).

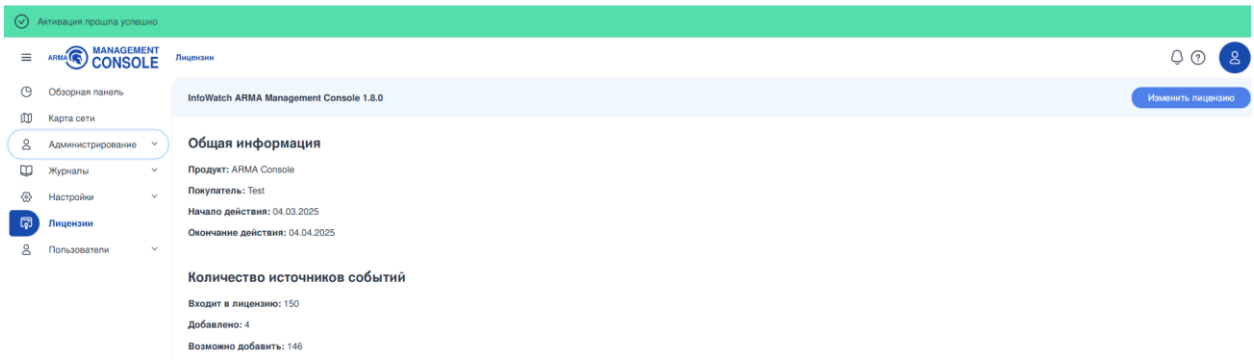


Рисунок – Информация о лицензии

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

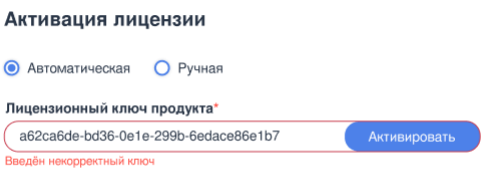


Рисунок – Некорректный ключ

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).

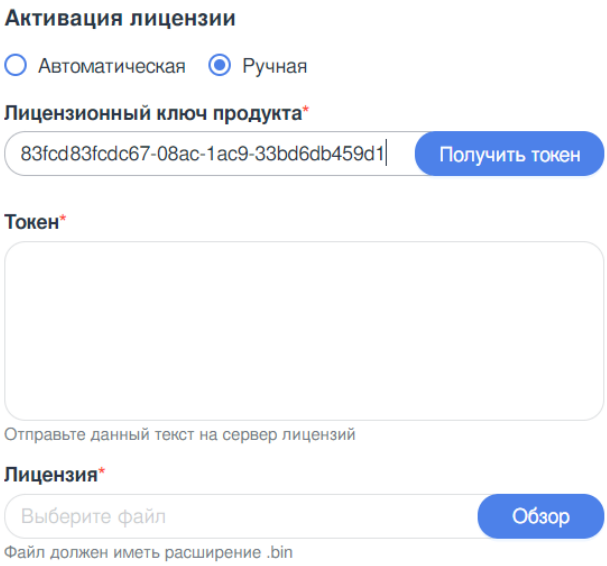


Рисунок – Лицензионный ключ

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»**.

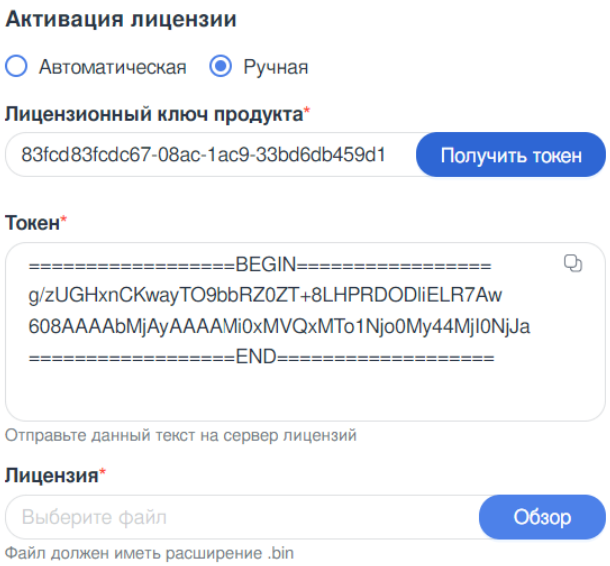


Рисунок – Получение токена для активации лицензии

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»**.

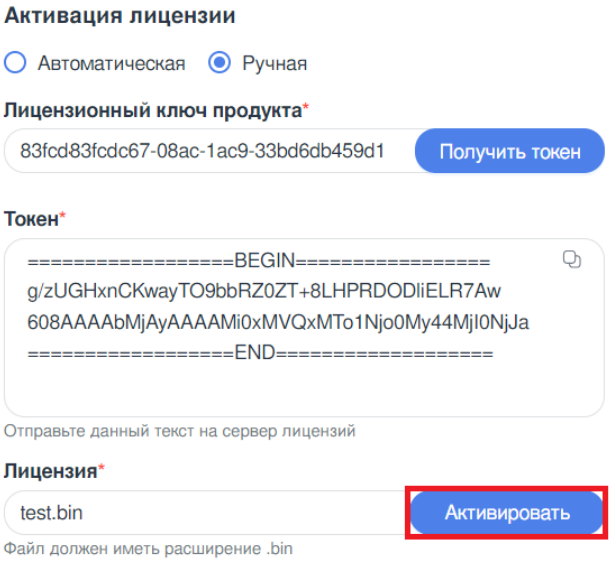


Рисунок – Кнопка «Активировать»

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.

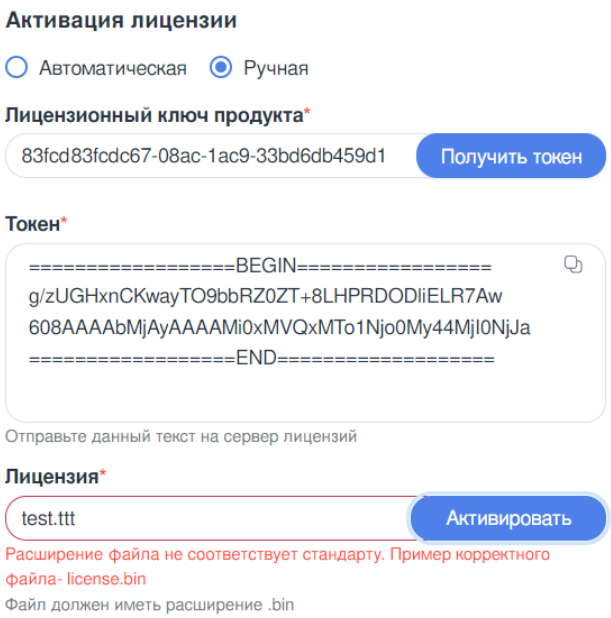


Рисунок – Некорректный формат файла лицензии

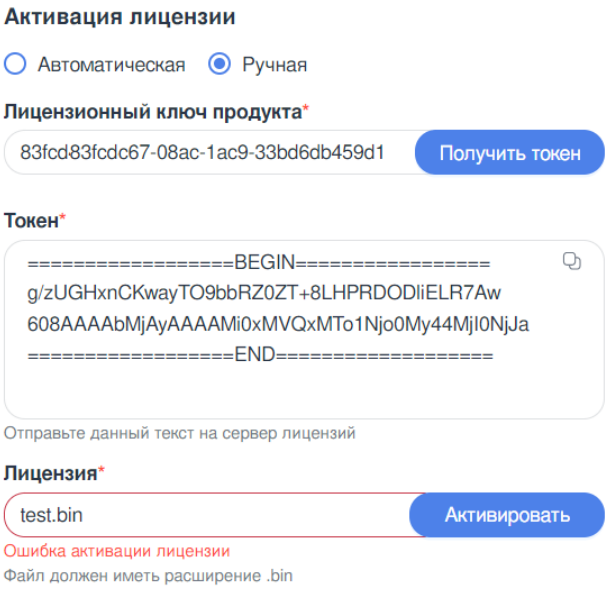


Рисунок – Некорректное содержимое файла лицензии

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).

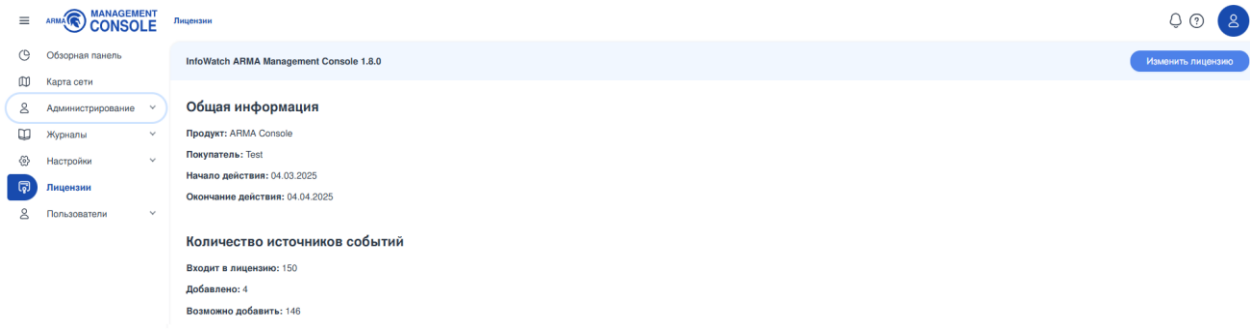


Рисунок – Текущая лицензия

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 КОМАНД ЛОКАЛЬНОГО КОНСОЛЬНОГО ИНТЕРФЕЙСА

В настоящем разделе представлено описание команд локального консольного интерфейса (ЛКИ).

5.1. Обновление ARMA MC

Обновление **ARMA MC** возможно осуществить через:

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

Для обновления через ЛКИ необходимо выполнить следующие действия:

1. Перейти в директорию **«/opt»** и создать пустой каталог, например **«amc»**:

```
cd opt
mkdir amc
```

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

```
tar -xzf InfoWatch-ARMA-Центр-Управления_1.8.0.tar.gz -C amc
```

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

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

4. 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»**.

5. 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.

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

Примечание:

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

5.1.1. 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 создаётся в папке **«backup»**, которая располагается на одном уровне с файлом **«setup.sh»**. В случае обновления **ARMA MC** через веб-интерфейс (см. Обновление ARMA MC), резервная копия сохранится в директории **«/opt/amcbackup»**.

5.1.2. 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 ввести 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**.

5.2. 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. Перейти в директорию **«/opt/armaupdate/amcansible/»**, которая содержит файл **«setup.sh»**.
2. Ввести команду:

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

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

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.

В текущей реализации производится резервное копирование и восстановление баз данных **«PostgreSQL»** и **«Elasticsearch»**.

5.3. 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
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
amc-storage-event-listener	amc-storage-event-listener.service	/var/log/syslog
amc-gateway.service	amc-gateway.service.service	/var/log/syslog
amc-device	amc-device.service	/var/log/syslog

Название сервиса	Полное наименование сервиса	Путь к журналу сервиса
amc-event	amc-event.service	/var/log/syslog
amc-license	amc-license.service	/var/log/syslog
amc-notification	amc-notification.service	/var/log/syslog

5.3.1. Перезагрузка сервисов

Для перезагрузки сервиса необходимо 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.

5.3.2. Просмотр журналов сервисов

Для просмотра журналов сервисов необходимо выполнить следующие действия:

1. 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»**.
2. Нажать **клавишу «ENTER»**.

5.4. Работа с SSH

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

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

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**.

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. Отсутствует доступ к веб-интерфейсу

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

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

ПРИЛОЖЕНИЕ А ЗАПУСК ARMA MC НА «ASTRA LINUX»

В качестве альтернативы установка **ARMA MC** может производится на аппаратную или виртуальную платформу с предустановленной ОС **«Astra Linux»**.

Для ОС **«Astra Linux»** должны соблюдаться следующие условия:

- версия ОС: **«Astra Linux SE 1.7»**;
- уровень защищенности: **Базовый («Орёл»)**.

Остальные настройки рекомендуется оставить по умолчанию.

Для установки используется установочный пакет **«InfoWatch-ARMA-Центр-Управления_ASTRA_[номер_версии].deb»**. Данная версия установочного пакета является **бета-версией**, поэтому должна использоваться только квалифицированными специалистами.

В остальном порядок установки **ARMA MC** не отличается от описанного ранее (см. Установка).