Руководство администратора

версия 17 ред. от 02.12.2025

Листов 31

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.2.1**.

ARMA MC является единым центром управления системой защиты, агрегирует информацию с подключённых средств защиты и позволяет оперативно оценить текущую защищённость 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 пользователя ARMA MC	Руководство пользователя по эксплуатации 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**.

ARMA MC совместима со следующими версиями продуктов **ARMA**:

- **«ARMA Стена (NGFW)»** версии **«4.5 (ФСТЭК)»** и **«4.7»**;
- **«Industrial Firewall (IFW)»** версии **«3.14»** и **«3.15»**;
- **«Industrial EndPoint Linux (IEL)»** версии **«3.0»**;
- **«Industrial EndPoint Windows (IEW)»** версии **«2.7»**.

Примечание:

При использовании **ARMA MC** совместно с сертифицированной по 4 уровню доверия, классам Б, Д и СОВ версией **«ARMA Стена (NGFW) 4.5»** необходимо обеспечить использование **ARMA MC** исключительно внутри доверенного контура.

При нарушении данного требования **InfoWatch ARMA** не может гарантировать безопасное и бесперебойное взаимодействие **ARMA MC** и **ARMA Стена** в соответствии со следующими требованиями ФСТЭК России: «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Д» четвертого класса защиты. ИТ.МЭ.Д4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

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

Примечание:

Рекомендуемая версия: **«Debian GNU/Linux 11.11»**
Минимально поддерживаемая версия: **«Debian GNU/Linux 11.9»**

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.

2.1 Требования к аппаратной платформе

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

Технические требования, предъявляемые к аппаратной платформе:

- **процессор** – 3,2 ГГц, восьмиядерный, x64;
- **ОЗУ** – 32 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** – минимум 2 Ethernet 100/1000 Мбит/с:
  - 1 для консольного порта (с которого производится управление),
  - минимум 1 для подключения сетевой инфраструктуры (итоговое число определяется количеством изолированных сегментов сети).

Примечание:

Для стабильной работы **ARMA MC** рекомендуется использовать аппаратную платформу **«Trinity 8S»**, обладающую следующими основными параметрами:

Процессор: AMD EPYC 7262 8-Core Processor (сокетов: 1, физ.ядер: 8, потоков: 16, потоков/ядро: 2)
ОЗУ: 32 ГБ
Накопитель: SSD 512 ГБ (SAMSUNG_MZ7LH240HAHQ-00005)
Видеокарта: ASPEED Technology, Inc. ASPEED Graphics Family (rev 41)

2.2 Требования к виртуальной платформе

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

- **«Hyper-V Generation 1»** и **«Hyper-V Generation 2»**;
- **«VirtualBox»** версии 6.0.4 и выше;
- **«VMware ESXi»** версии 7 обновления 2 и выше.

Примечание:

Тестирование **ARMA MC** производилось на **«VMware ESXi»** версии 7 обновления 2. Для обеспечения стабильной работы рекомендуется использовать именно этот вариант.

Минимальные технические требования, предъявляемые к виртуальной платформе:

- **количество процессоров** – 4;
- **объём оперативной памяти** – 8 ГБ;
- **размер виртуального диска** – 512 ГБ;
- **сетевые интерфейсы** – минимум 1 (итоговое число определяется количеством изолированных сегментов сети).

3 УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ

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

Примечание:

Перед установкой следует убедиться, что **ARMA MC** находится в защищённом межсетевым экраном контуре, из которого исключён прямой (без защиты МЭ) доступ **ARMA MC** к сети Интернет.

Только после изменения предустановленного пароля значением, соответствующим актуальным требованиям ИБ, допускается использование **ARMA MC** с непосредственным доступом к сети Интернет.

Примечание:

Если требуется установить **ARMA MC** в полностью закрытом контуре (без доступа в Интернет), следует обратиться в службу поддержки для получения дополнительных пакетов и инструкций.

Примечание:

Установка должна проводиться от имени УЗ с ролью уровня **«Администратор ОС»** на чистую систему, не содержащую элементов предыдущей установки **ARMA MC** (если необходимо возобновить прерванную установку см. Не удалось установить ARMA MC настоящего руководства).

3.1 Установка

Примечание:

Для корректной установки **ARMA MC** на ОС должна быть установлена русская локаль **«ru_RU.UTF-8»**.

Порядок установки:

1. Подключить сетевые репозитории в **«/etc/apt/sources.list»**, если они были отключены.
2. Установить необходимое ПО командой:

```
apt update && apt upgrade -y && apt install lsb-release bash curl jq gnupg nginx python3 python3-apt python3-pip python3-venv postgresql postgresql-contrib rabbitmq-server redis redis-server libpq-dev openssl ca-certificates sudo wget -y
```

Примечание:

Для работы **ARMA MC** требуется **«rsyslog»**. В большинстве дистрибутивов **«Linux»** пакет предустановлен, в ином случае его следует установить. Например, командой **«apt install rsyslog»**.

После завершения необходимо убедиться, что версия Debian больше или равна **«11.9»**. Например, воспользовавшись командой:

```
cat /etc/debian_version
```

3. Скачать и установить **«elasticsearch»** версии **«7.12.0»**. Например, воспользовавшись командой:

```
wget https://mirror.yandex.ru/mirrors/elastic/7/pool/main/e/elasticsearch/elasticsearch-7.12.0-amd64.deb && dpkg -i elasticsearch-7.12.0-amd64.deb
```

Примечание:

Приведённый в примере выше репозиторий является лишь одним из возможных вариантов. Выбор источника установки зависимостей остаётся на усмотрение администратора системы.

Примечание:

Если при установленном **«elasticsearch»** выполнить обновление пакетов (например, **«apt upgrade»**), **«elasticsearch»** обновится до последней версии. В этом случае необходимо вернуть версию **«7.12.0»**, повторно запустив установку пакета **«elasticsearch-7.12.0-amd64.deb»**.

4. Установить **«UFW»**:

```
sudo apt install ufw
```

Примечание:

Проверить наличие и активный статус службы UFW можно командой: systemctl status ufw

В выдаче должно присутствовать **«Active: active»**

5. Загрузить установочный пакет **ARMA MC** – **«InfoWatch-ARMA-Центр-Управления_[номер_версии].deb»**.
6. Запустить 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).

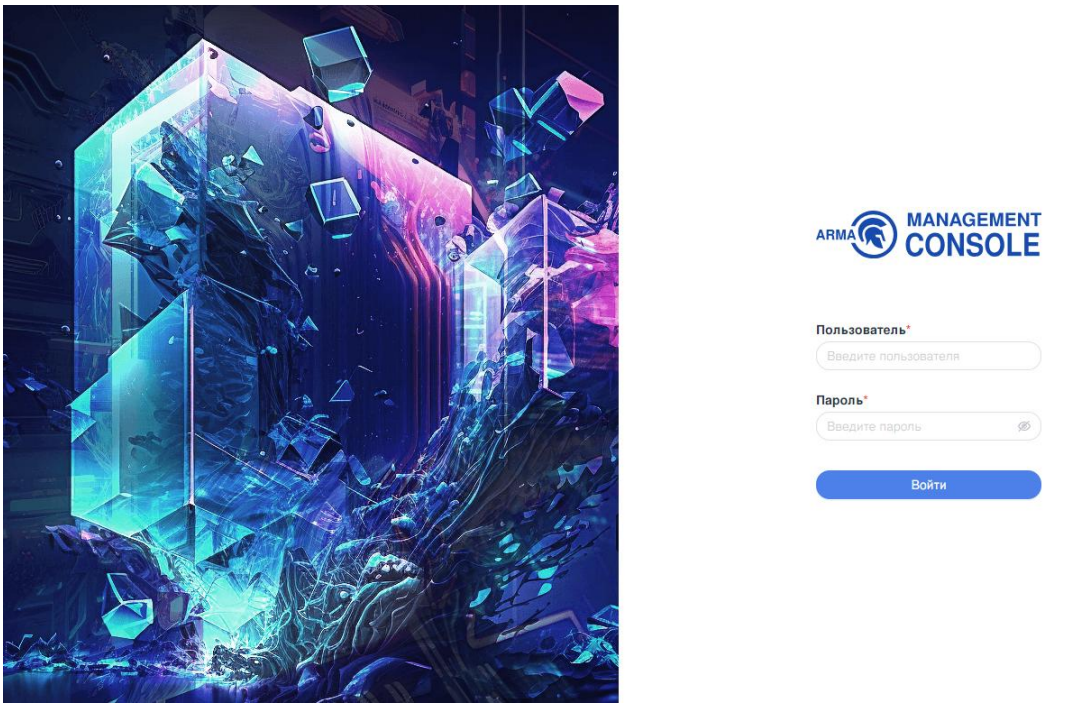

Рисунок – Страница авторизации в веб-интерфейсе

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 необходимо изменить данные после первоначального входа (см. Изменение пароля УЗ веб-интерфейса настоящего руководства).

В случае превышения допустимого количества неудачных попыток входа в систему пользователь будет временно заблокирован. Количество попыток и время блокировки пользователя задаётся в интерфейсе **ARMA MC**, описанном в разделе Аутентификация Руководства пользователя по эксплуатации **ARMA MC**.

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

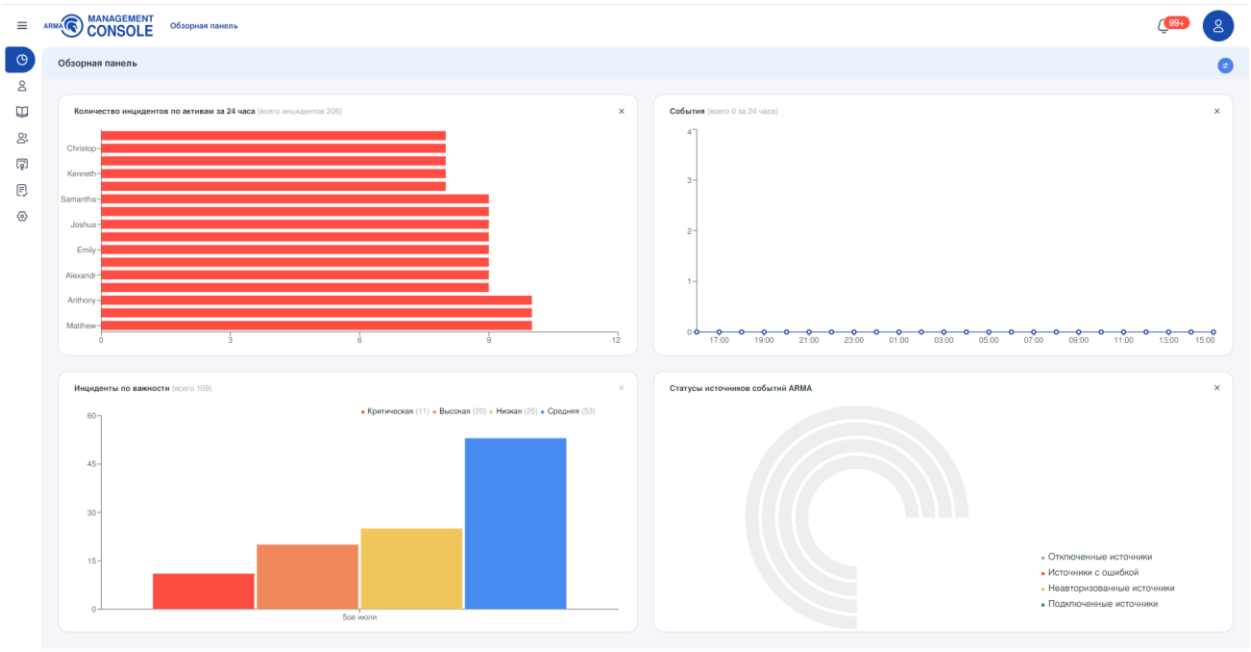

Рисунок – Обзорная панель

Примечание:

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

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 настоящего руководства).
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»**.

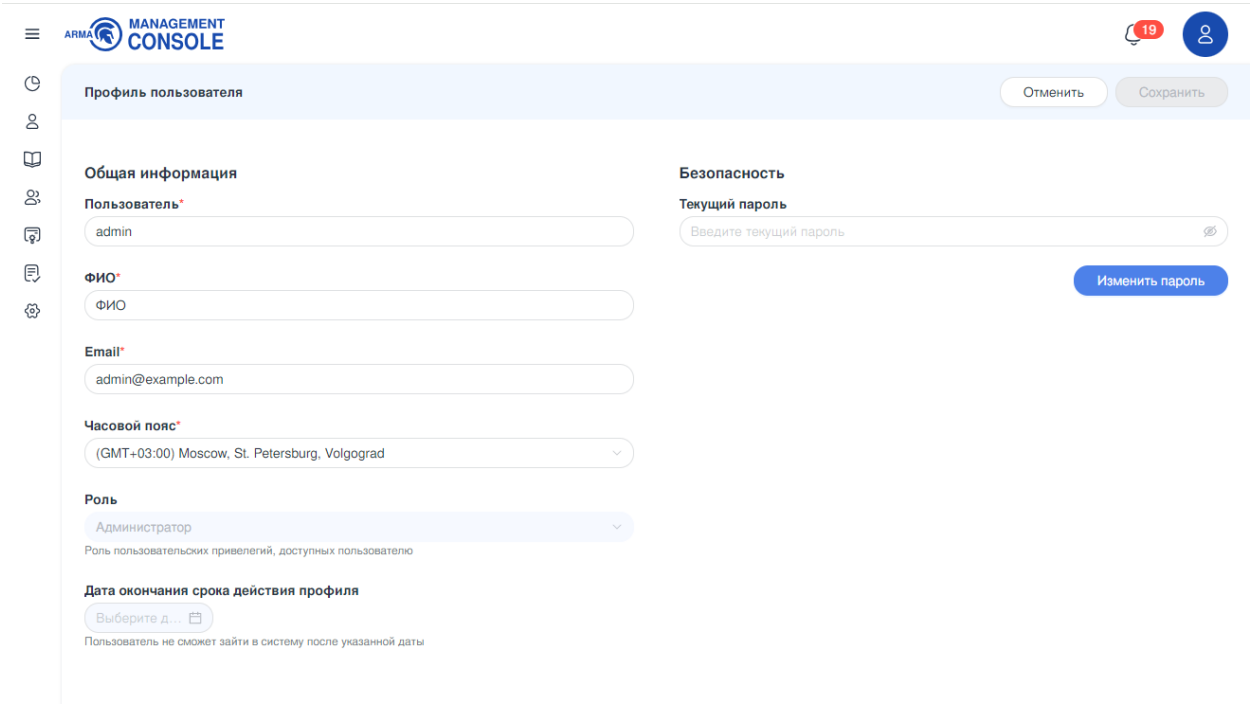

Рисунок – Профиль пользователя

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»**.

3.3 Подключение к ARMA MC по SSH

3.3.1 Настройка «UFW»

Разрешить входящие SSH-соединения возможно вводом следующей команды:

```
sudo ufw allow ssh
```

Для проверки состояния UFW необходимо ввести следующую команду:

```
sudo ufw status verbose
```

Если UFW включён, то в консоли будут перечисляться заданные правила.

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 Radius 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.

3.5 Монтирование внешнего ресурса

Внешний ресурс (система хранения данных) может использоваться для сохранения архивов в процессе ротации (см. раздел Экспорт файлов ротации Руководства пользователя **ARMA MC**).

> **Примечание:**
>
> Важно правильно подключить внешний ресурс. Если ресурс будет недоступен в момент ротации, архив, который требовалось перенести на внешний ресурс, будет удалён.

ARMA MC не предъявляет особых требований к подключаемому ресурсу, но в целях обеспечения безопасности и корректной работы рекомендуется:

1. Установить пакет **«cifs-utils»**, если он не был установлен. Пакет можно установить, например, командой **«apt install cifs-utils»**.

   Примечание:

   В средах без доступа к внешним репозиториям пакет **«cifs-utils»** устанавливается из локального репозитория, зеркала или вручную из .deb пакетов. Рекомендуется заранее убедиться, что пакет присутствует в локальном репозитории. Для проверки наличия установленного пакета можно выполнить команду dpkg -l | grep cifs-utils.

2. Задать **«uid»** и **«gid»** пользователя, из-под которого работает **ARMA MC**. **«uid»** может быть **«armaconsole»** или числовой идентификатор, а **«gid»** – **«www-data»** или число. Данные для этого можно получить командой **«id»**.
3. Выставить права **«644»** для файлов и **«755»** для директории.
4. Сохранить данные авторизации (логин и пароль), создать файл (например, по пути **«/etc/samba/»**, если директория отсутствует, её можно создать самостоятельно) и записать туда эти данные.

   Пример файла:

```
# /etc/samba/smbcreds
username=user
password=12345
```

   Примечание:

   Для дополнительной безопасности можно файлу **«/etc/samba/smbcreds»** выдать права **«600»** и **«chown root»**.

6. Создать mount файлы. Имена файлов **«.mount»** и **«.automount»** должны содержать путь к точке монтирования в которой все слеши, кроме начального, заменяются на дефис. Например, для точки монтирования **«/mnt/nfs/backups»** имя файла должно быть **«mnt-nfs-backups.mount»**.

   Пример итогового mount файла:

```
# /etc/systemd/system/mnt-smb-backups.mount
[Unit]
Description=Automount SMB Fresh series

[Mount]
What=//172.16.241.74/secure_share
Where=/mnt/smb/backups
Type=cifs
Options=_netdev,iocharset=utf8,rw,file_mode=0644,dir_mode=0755,uid=armacons
ole,gid=www-data,credentials=/etc/samba/smbcreds
TimeoutSec=10

[Install]
WantedBy=multi-user.target
```

```
# /etc/systemd/system/mnt-smb-backups.automount
[Unit]
Description=Automount SMB SAN

[Automount]
Where=/mnt/smb/backups
TimeoutIdleSec=60

[Install]
WantedBy=multi-user.target
```

Примечание:

В примерах выше **«What»** – адрес smb/конечная папка, **«Where»** – точка монтирования.

7. Для включения автомонтирования необходимо запустить automount unit файл, используя следующие команды:

```
systemctl daemon-reload
systemctl enable --now mnt-smb-backups.automount
```

Примечание:

В mount файле кроме пути к папке необходимо задавать адрес самой SMB. Например, **«//ip-smb/folder/name/»**.

После того как автомонтирование запущено, его статус можно проверить командой systemctl status mnt-smb-backups.automount. В выводе команды должен быть активный статус (**«Active: active»**).

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).

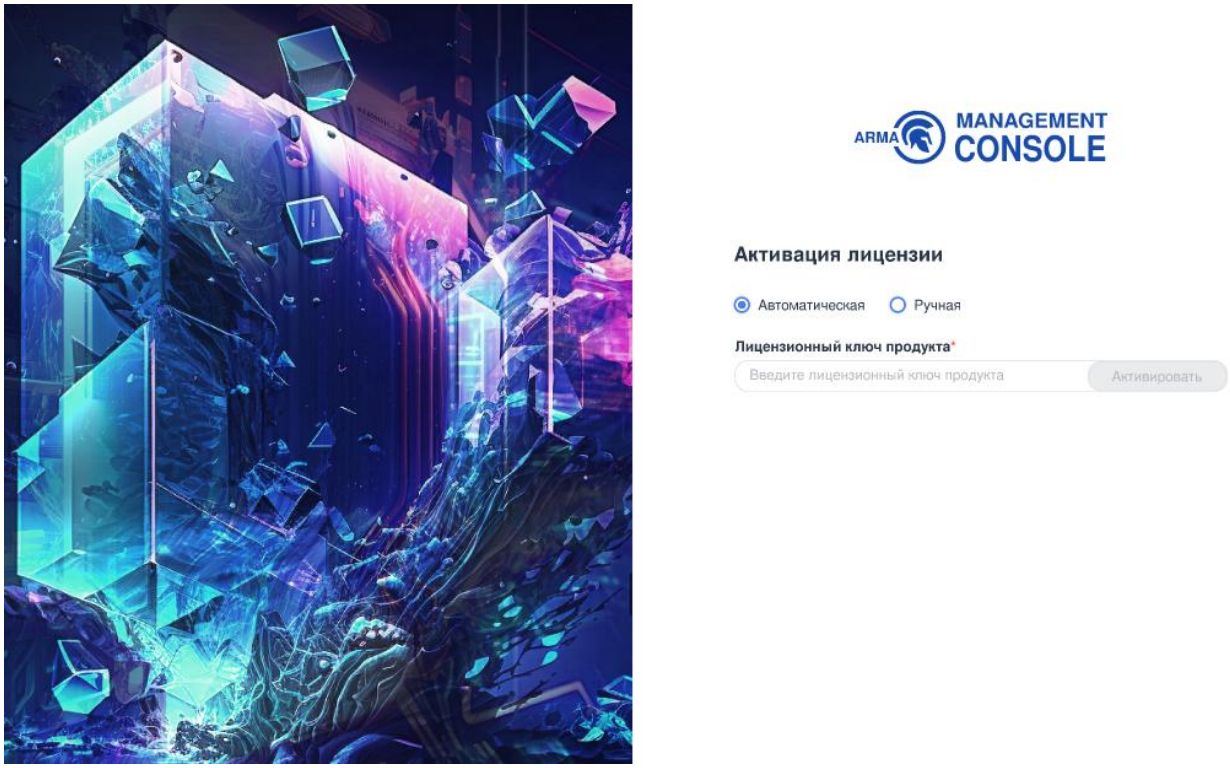

Рисунок – Активация новой лицензии

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

Примечание:

Активировать лицензию возможно только обладая УЗ, наделённой 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).

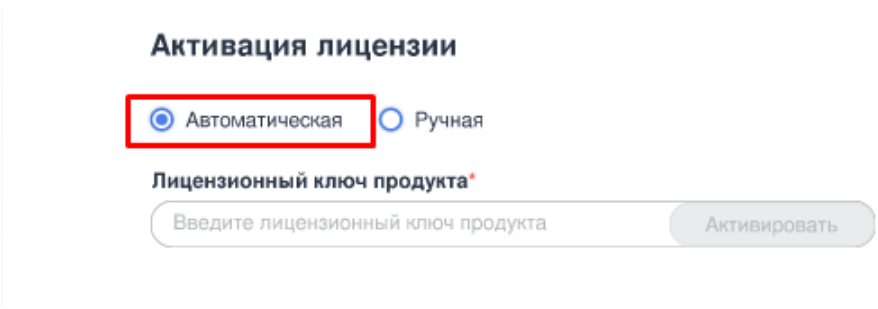

Рисунок – Автоматическая активация

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

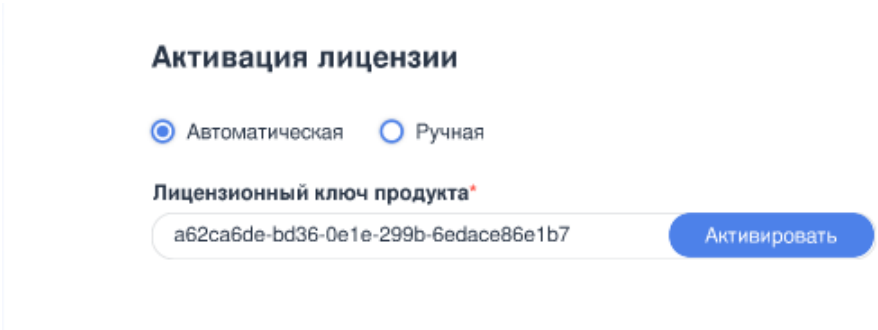

Рисунок – Лицензионный ключ

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).

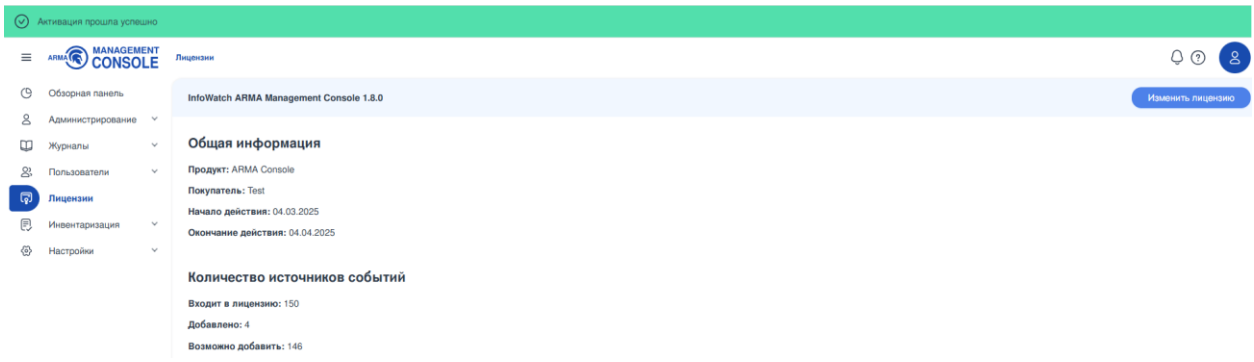

Рисунок – Информация о лицензии

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

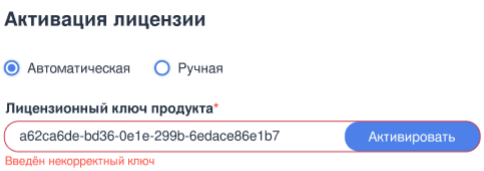

Рисунок – Некорректный ключ

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).

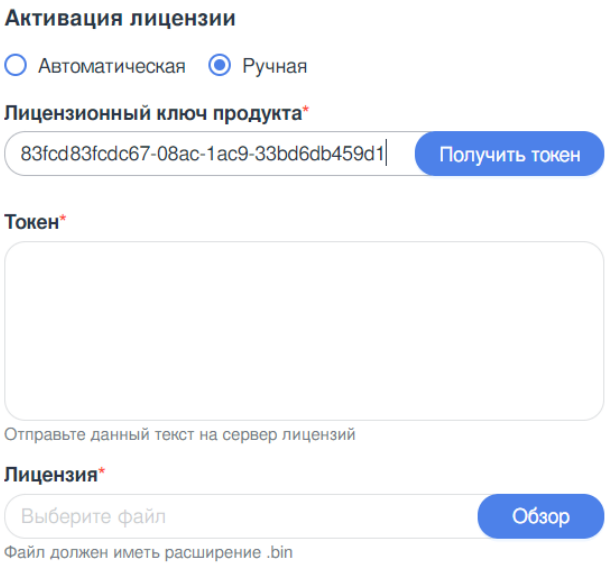

Рисунок – Лицензионный ключ

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»**.

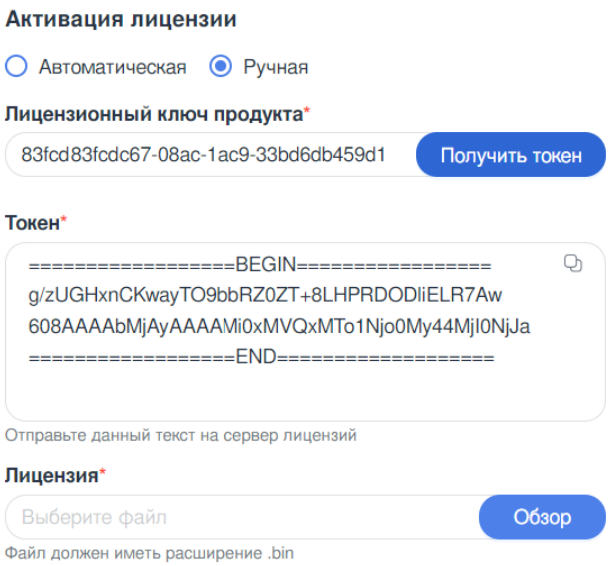

Рисунок – Получение токена для активации лицензии

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»**.

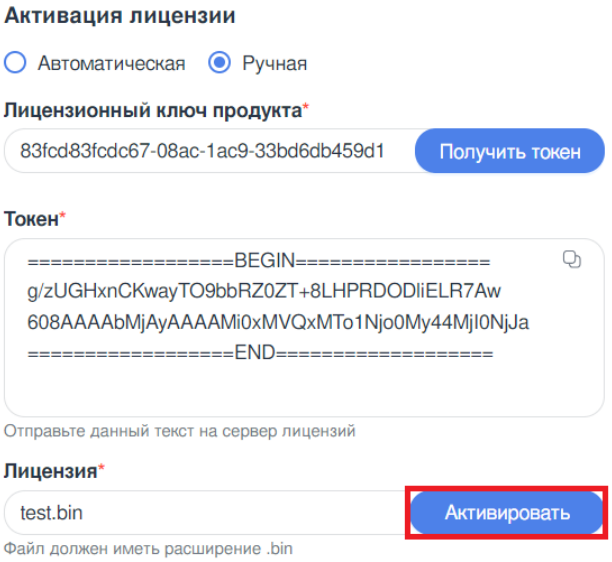

Рисунок – Кнопка «Активировать»

5. После успешной активации лицензии произойдёт перенаправление на страницу с информацией о текущей лицензии, и отобразится всплывающее уведомление 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.

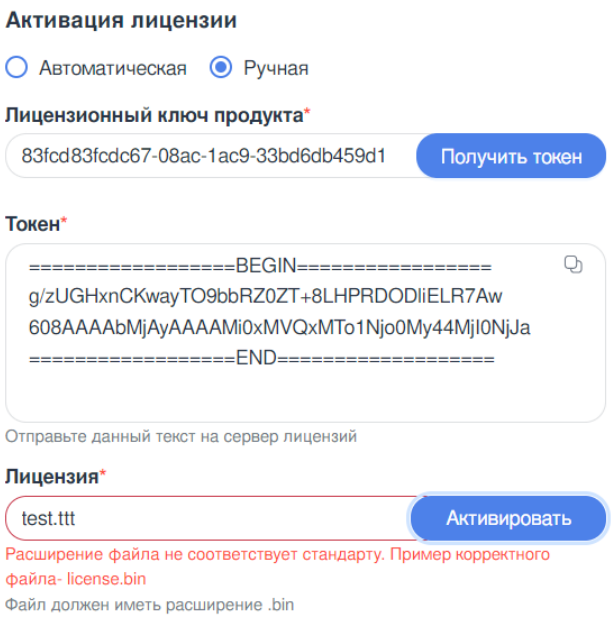

Рисунок – Некорректный формат файла лицензии

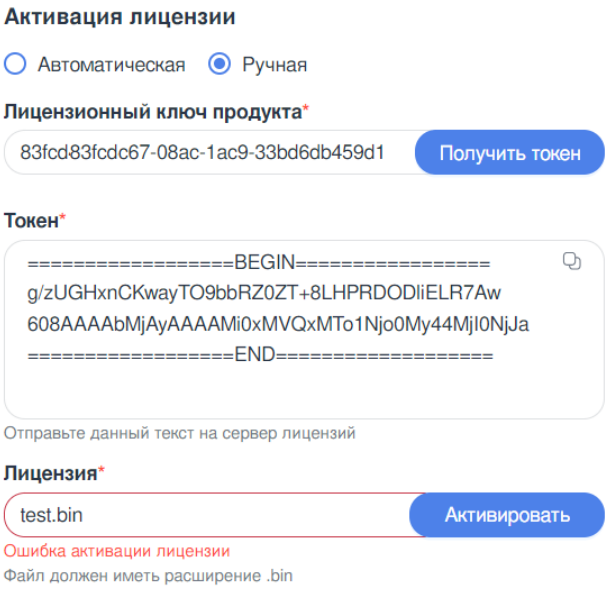

Рисунок – Некорректное содержимое файла лицензии

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).

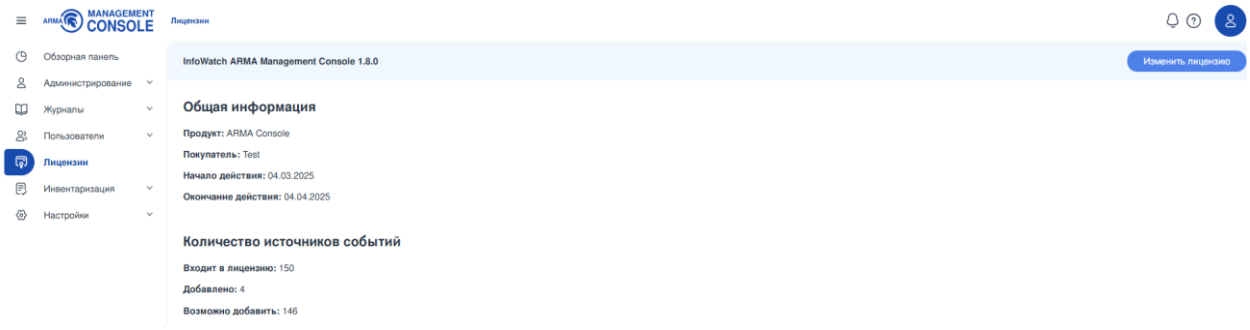

Рисунок – Текущая лицензия

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 Руководства пользователя **ARMA MC**);
- **«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 настоящего руководства.

Шаги по ручной активации описаны в разделе Ручная активация лицензии настоящего руководства.

5 ОПИСАНИЕ КОМАНД ЛОКАЛЬНОГО КОНСОЛЬНОГО ИНТЕРФЕЙСА

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

5.1 Обновление ARMA MC

Обновление **ARMA MC** производится через веб-интерфейс (см. раздел Обновление версии Руководства пользователя **ARMA MC**).

> **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**.

5.1.1 Удаление устаревших данных после обновления

После обновления **ARMA MC** на версию **«2.1»** в хранилище могут остаться данные, которые не будут доступны через веб-интерфейс, но при этом будут занимать место на диске.

Для удаления данных по окончании обновления следует:

1. Перейти в директорию:

```
cd /usr/local/armaconsole/app/
```

2. Запустить скрипт командой:

```
bash delete-old-storage-archives.sh
```

5.2 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

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

5.2.1 Перезагрузка сервисов

Для перезагрузки сервиса необходимо ввести команду **«systemctl restart [servicename]»**, где:

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

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.

5.2.2 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 настоящего руководства).

  Например, для просмотра журнала сервиса «amcclient», необходимо ввести команду:

  ```
  vim /var/log/armaconsole/license.log
  ```

2. Нажать клавишу **«ENTER»**.

5.3 Выгрузка диагностической информации

Диагностическую информацию **ARMA MC** следует выгружать при возникновении внештатной ситуации, чтобы получить данные, необходимые для диагностики проблемы.

Для выгрузки диагностической информации необходимо из-под **«root»** пользователя запустить скрипт командой:

```
bash /opt/armaupdate/amcansible/scripts/diag.sh
```

Архив с диагностической информацией будет расположен по следующему пути:

```
/tmp/amc_system_info_${CURRENT_DATE}.tar.gz
```

где **{CURRENT_DATE}** – текущая дата вида ГГГГ-ММ-ДД, например, 2025-04-25.

5.4 Снятие блокировки пользователя

ARMA MC поддерживает возможность снятия блокировки пользователя, заблокированного по причине превышения допустимого количества попыток аутентификации с вводом неверных учётных данных.

Для снятия блокировки необходимо из-под **«root»** пользователя ввести следующую команду:

```
/usr/local/armaconsole/app/scripts/faillock --reset --user [blocked_user]
```

где **[blocked_user]** – имя заблокированного пользователя, например, **«usertest»**.

В результате пользователь будет сразу разблокирован без необходимости ожидания установленного времени блокировки.

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 настоящего руководства. Инструкция просмотра журналов сервисов описана в разделе Просмотр журналов сервисов настоящего руководства.

6.2 Ошибка «elasticsearch»

Для устранения ошибок с сервисом «elasticsearch» необходимо перезагрузить **ARMA MC**.

6.3 Не срабатывает правило корреляции

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

6.4 Не включается правило корреляции

При включении какого-либо правила корреляции может появиться предупреждение о наличии включённого ранее правила с идентичным SID. Данная ситуация возникает вследствие наличия нескольких правил корреляции отличающихся версий, но с одинаковым SID (см. Рисунок – Правила корреляции с идентичными SID).

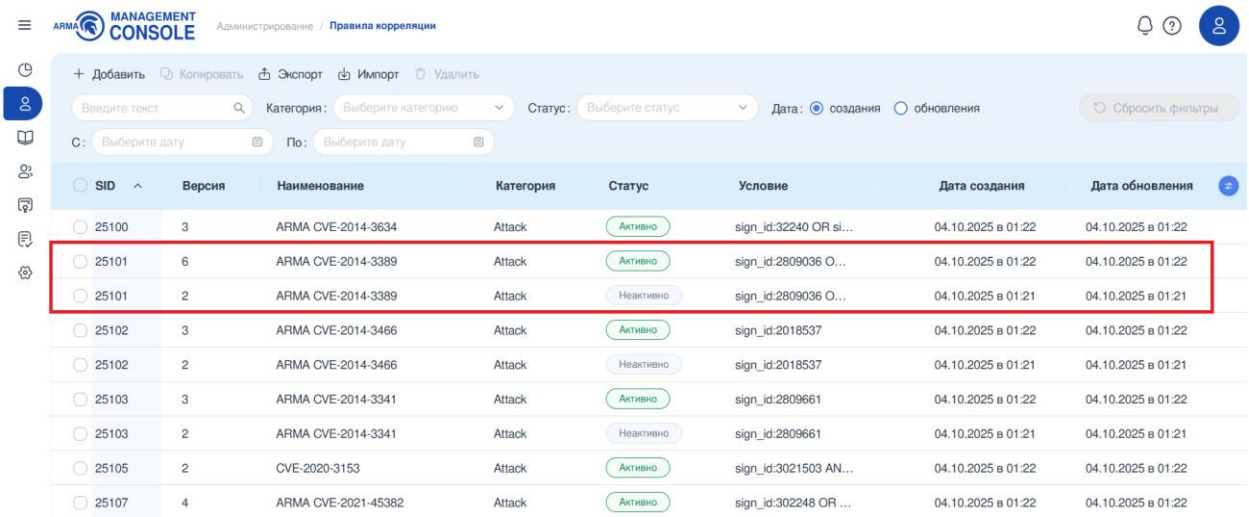

Рисунок – Правила корреляции с идентичными SID

На рисунке выше активное правило версии «6» блокирует включение правила версии «2».

Для включения требуемого правила необходимо предварительно отключить правило, препятствующее включению, с идентичным SID.

6.5 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.

6.6 Не удалось установить ARMA MC

Если установка **ARMA MC** не была завершена корректно, для повторной установки необходимо полностью удалить **ARMA MC** из системы.

Для удаления **ARMA MC** достаточно запустить скрипт **«uninstall.sh»**, находящийся по пути **«opt/armaupdate/amcansible/scripts»**.

> **Примечание:**
>
> После удаления **ARMA MC** можно повторно выполнить установку, как это описано в разделе Установка, за исключением того, что из пакетов ПО для Linux необходимо будет переустановить только **«elasticsearch»**, остальные пакеты ПО (если они были ранее успешно установлены) переустанавливать не требуется.

6.7 Веб-интерфейс перестал реагировать на нажатия

Если через некоторое время после обновления веб-интерфейс перестал отвечать, следует перезагрузить **ARMA MC**.

6.8 Сообщение о невозможности проведения экстренной очистки дискового пространства

ARMA MC автоматически очищает дисковое пространство при достижении минимального объема свободного места (см. раздел Нехватка места на диске и автоматическая очистка Руководства пользователя **ARMA MC**). В редких случаях после успешного выполнения очистки выводится сообщение о том, что очистка невозможна или не выполнена.

Если вы столкнулись с такой ситуацией, рекомендуется определить фактический размер свободного места на диске средствами ОС (например, с помощью утилиты **«df»**). Если в результате выяснится, что свободно более **«7,5%»** от объема диска,

можно продолжать работу как обычно. Если свободное место составляет менее **«7,5%»**, необходимо освободить место средствами ОС.