Руководство пользователя по эксплуатации

версия 1 ред. от 03.03.2025

Листов 33

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
ПЛК	Программируемый логический контроллер

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Industrial Endpoint Linux v.3.0** (далее **ARMA IEL**).

ARMA IEL является средством защиты рабочих станций и серверов автоматизированной системы управления технологическим процессом от угроз на уровне диспетчерского управления.

ARMA IEL обеспечивает защиту от таких угроз, как запуск вредоносного ПО, подключение нежелательных устройств, утечка конфиденциальной информации и подмена программ ПЛК.

ARMA IEL выполняет следующие функции:

- взаимодействие с **ARMA Management Console**;
- контроль целостности файлов;
- управление запуском приложений;
- контроль подключения USB-устройств и CD/DVD-носителей.

Руководство пользователя по эксплуатации содержит описание:

- принципов работы **ARMA IEL**;
- настройки и использования доступных функций **ARMA IEL**.

Пользователю **ARMA IEL** 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 IEL	Руководство администратора InfoWatch ARMA Industrial Endpoint Linux
Руководство пользователя по эксплуатации ARMA MC	Руководство пользователя по эксплуатации InfoWatch ARMA Management Console

1 ОБЩИЕ НАСТРОЙКИ

Для перехода в модуль **«Общие настройки»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника типа **«IEL»**.
2. В карточке источника выбрать модуль **«Общие настройки»** (см. Рисунок – Общие настройки).

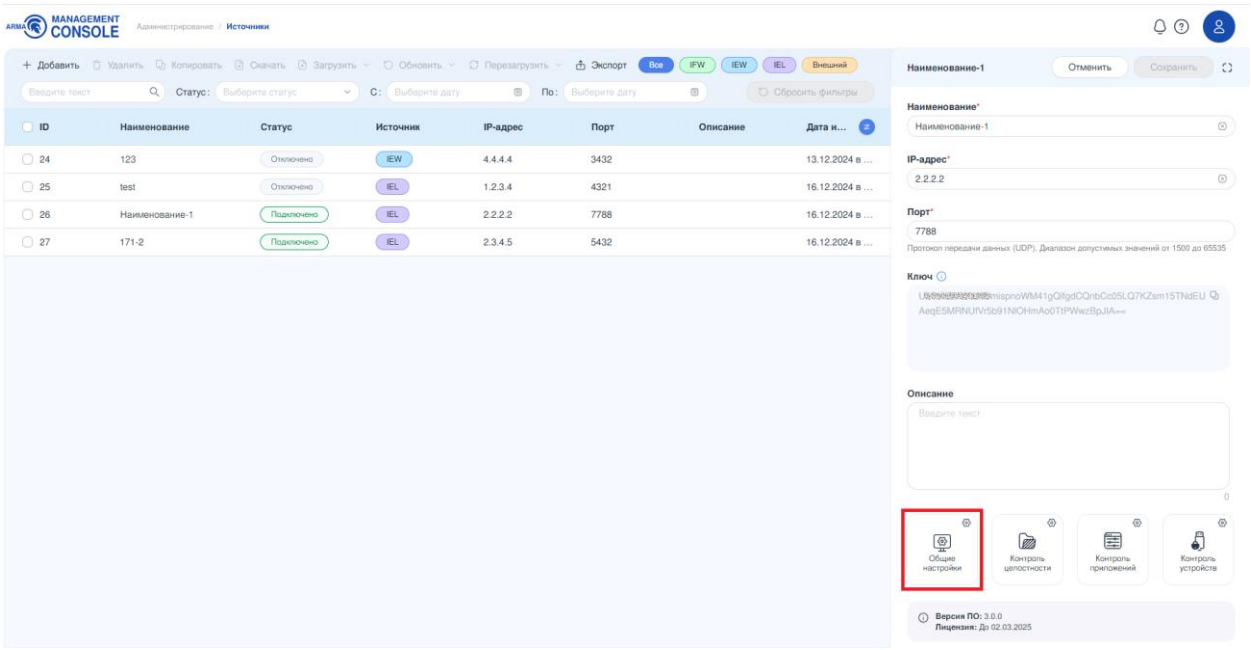

Рисунок – Общие настройки

В модуле **«Общие настройки»** существует возможность посмотреть информацию и произвести настройки (см. Рисунок – Параметры настроек):

- журналирования;
- логирования;
- сетевого журнала;
- ротации журнала событий.

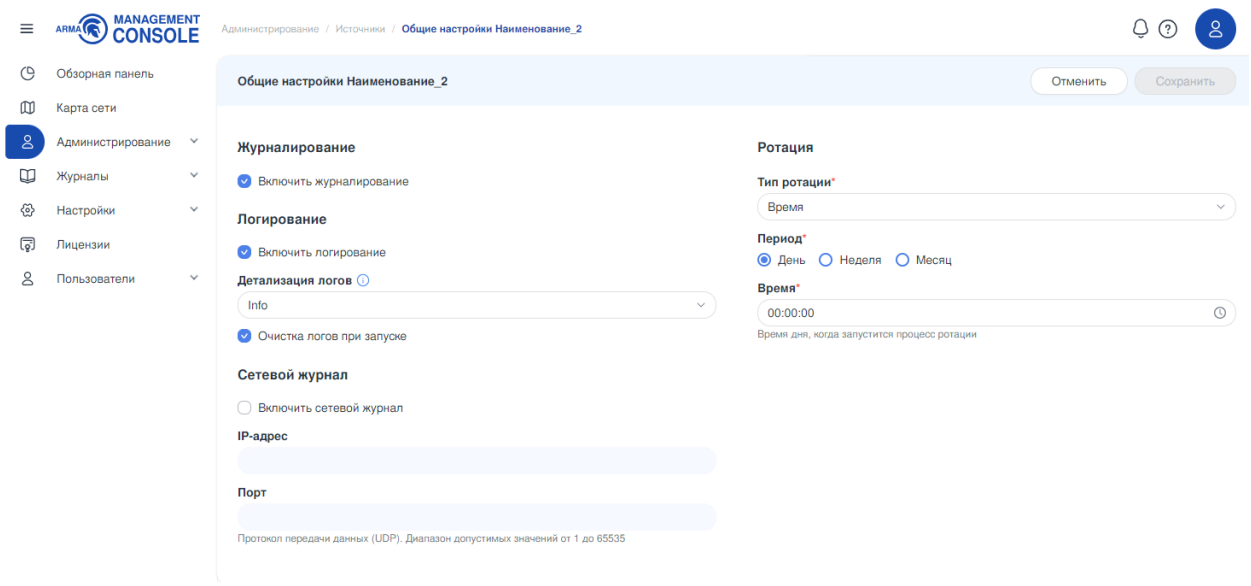

Рисунок – Параметры настроек

1.1 Журналирование

Функция журналирования отвечает за запись событий (см. раздел События Руководства пользователя **ARMA MC**) в базу данных **ARMA IEL** и по умолчанию включена. В случае разрыва связи с **ARMA MC**, события продолжают регистрироваться в базе данных **ARMA IEL**. После восстановления соединения зарегистрированные события отправляются в **ARMA MC**.

Для включения/выключения журналирования необходимо установить/снять флажок в чекбоксе **«Включить журналирование»**.

1.2 Логирование

Функция логирования отвечает за запись логов в файл **«endpoint.log»** (см. раздел Руководства администратора **ARMA IEL** Расположение ключевых артефактов ARMA IEL) и по умолчанию включена.

Доступны следующие настройки логирования:

- включение/выключение логирования;
- настройка уровня детализации событий;
- включение/выключение очистки журнала при запуске.

Для включения/выключения логирования необходимо установить/снять флажок в чек-боксе **«Включить логирование»**. При выключенном логировании в файл **«endpoint.log»** перестаёт записываться отладочная информация.

Для того чтобы задать уровень детализации логов, необходимо выбрать значение в выпадающем списке **«Детализация логов»**. Доступны следующие варианты детализации записываемых событий:

- **«Trace»** – записывает каждое действие **ARMA IEL**;
- **«Debug»** – записывает события, считающимися полезными во время отладки **ARMA IEL**;
- **«Info»** – записывает события информативного характера. Детализация по умолчанию;
- **«Warning»** – записывает непредвиденные события, которые в дальнейшем могут нарушить работу одного из процессов **ARMA IEL**;
- **«Error»** – записывает прикладные ошибки в работе **ARMA IEL**;
- **«Fatal»** – записывает события, сообщающие о неработоспособности одной или нескольких ключевых бизнес-функций **ARMA IEL**.

Для включения/выключения очистки журнала при каждом запуске **ARMA IEL** необходимо установить/снять флажок в чек-боксе **«Очистка логов при запуске»**. Очистка журнала по умолчанию включена.

1.3 Сетевой журнал

В **ARMA IEL** существует возможность экспорта событий в сторонние системы.

Для настройки экспорта событий по сети необходимо в блоке настроек **«Сетевой журнал»** выполнить следующие действия:

1. Установить флажок в чек-бокс параметра **«Включить сетевой журнал»**.
2. Указать значения для параметров:
   - **«IP-адрес»** – IP-адрес устройства, на которое будут отправляться события;
   - **«Порт»** – порт UDP, по которому будут отправляться события. Доступно указание значения в диапазоне от «1» до «65535».
3. Нажать кнопку **«Сохранить»**.

1.4 Ротация журнала

Ротация журнала событий отвечает за удаление устаревших накопленных событий, отправленных в **ARMA MC**, во избежание переполнения базы данных.

> **Примечание:**
>
> Форсированная ротация. Вне зависимости от факта отправки в **ARMA MC** событие подпадает под ротацию принудительно, если хранится в базе дольше 30 дней. Период можно изменить в файле конфигурации (см. раздел Руководства администратора **ARMA IEL** Управление ARMA IEL с помощью файлов конфигурации).

Ротация журнала событий доступна по следующим типам:

- **«Количество»** – определяет, при достижении какого количества записей в базе данных будет выполняться процесс ротации;
- **«Время»** – определяет время запуска процесса ротации.

Для запуска ротации журнала событий по типу **«Количество»** необходимо выполнить следующие действия:

1. В поле **«Тип ротации»** установить значение **«Количество»**.
2. В поле **«Количество записей»** ввести количество событий в базе данных, при котором должна выполняться ротация. Диапазон допустимых значений от 100 до 100000.
3. Нажать кнопку **«Сохранить»**.

Для запуска ротации журнала событий по типу **«Время»** необходимо выполнить следующие действия:

1. В поле **«Тип ротации»** установить значение **«Время»**.
2. Установить необходимое значение для параметра **«Период»**. Допустимые значения:
   - **«День»** – ротация будет запускаться каждый день;
   - **«Неделя»** – ротация будет запускаться по понедельникам;
   - **«Месяц»** – ротация будет запускаться 1 числа каждого месяца.
3. В поле **«Время»** ввести время, в которое будет запускаться ротация, в формате «чч:мм:сс».
4. Нажать кнопку **«Сохранить»**.

Ротированные записи хранятся в формате **«json»** по пути **«/var/lib/iwarma-endpoint/rotation»** с указанием даты и времени ротации в имени файла, например:

```
event-rotation_11.12.2024_15:50:24
```

Записи содержат полную информацию о событии (см. Руководство пользователя **ARMA MC** раздел ch_mc_rp_events) и недоступны для редактирования.

2 КОНТРОЛЬ ЦЕЛОСТНОСТИ

Функция **«Контроль целостности»** предназначена для отслеживания действий, выполняемых с файлами и директориями в области мониторинга.

Для перехода в модуль **«Контроль целостности»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника типа **«IEL»**.
2. В карточке источника выбрать настройку **«Контроль целостности»** (см. Рисунок – Настройка «Контроль целостности»).

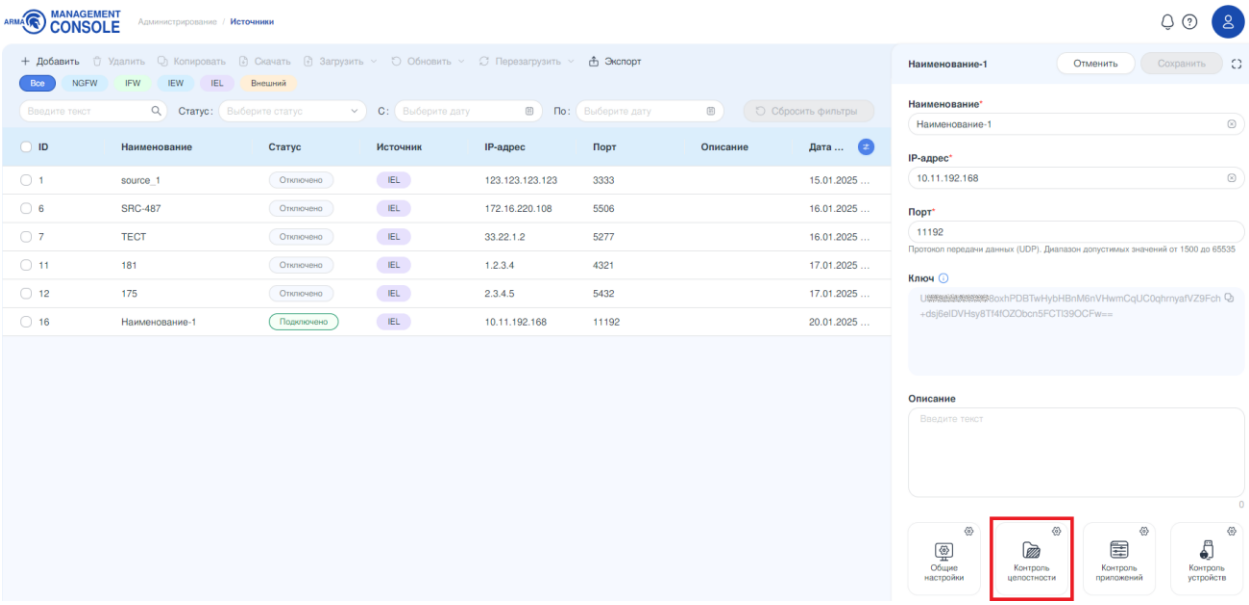

Рисунок – Настройка «Контроль целостности»

Список файлов и директорий, подлежащих контролю целостности, представлен в формате таблицы и состоит из следующих столбцов:

- **«Путь к файлу/папке»** – содержит путь к файлу или директории источника событий;
- **«Статус»** – отображает состояние записи.

В столбце **«Статус»** могут отображаться следующие состояния:

- **«Не сохранено»** – данный статус присваивается автоматически после ручного добавления пути. При закрытии экранной формы, путь с этим статусом исчезнет из списка;
- **«Загружается»** – данный статус присваивается автоматически после сохранения пути;
- **«Успешно»** – процесс проверки прошёл успешно, целостность папки/файла не нарушена;

- **«Неуспешно»** – папка/файл не прошла проверку целостности, т.к. были произведены изменения;
- **«Ошибка»** – как правило, статус присваивается в случае, когда система не смогла проверить выбранную папку ввиду большого объёма данных или отсутствия пути.

Примечание:

Статус **«Неуспешно»** может появиться вследствие копирования в контролируемый путь большого количества элементов. В таком случае выполните действие **«Проверить по базе»** для данного пути. Статус изменится на **«Ошибка»**.

Для устранения ошибки нажмите кнопку **«Обновить эталонные образы»** (см. Настройка контроля целостности).

2.1 Настройка контроля целостности

Для включения функции **«Контроль целостности»** и добавления файла или директории, подлежащей контролю целостности в перечень контролируемых, необходимо выполнить следующие действия:

1. Перейти к настройке **«Контроль целостности»** необходимого источника типа **«IEL»**.
2. Включить функцию **«Контроль целостности»**, установив флажок в чек-бокс параметра **«Включить контроль целостности»**.
3. Нажать кнопку **«Добавить»** на панели инструментов.
4. Выбрать в открывшемся окне проводника необходимую директорию или файл и нажать кнопку **«Выбрать»** (см. Рисунок – Добавление пути к файлу/директории).

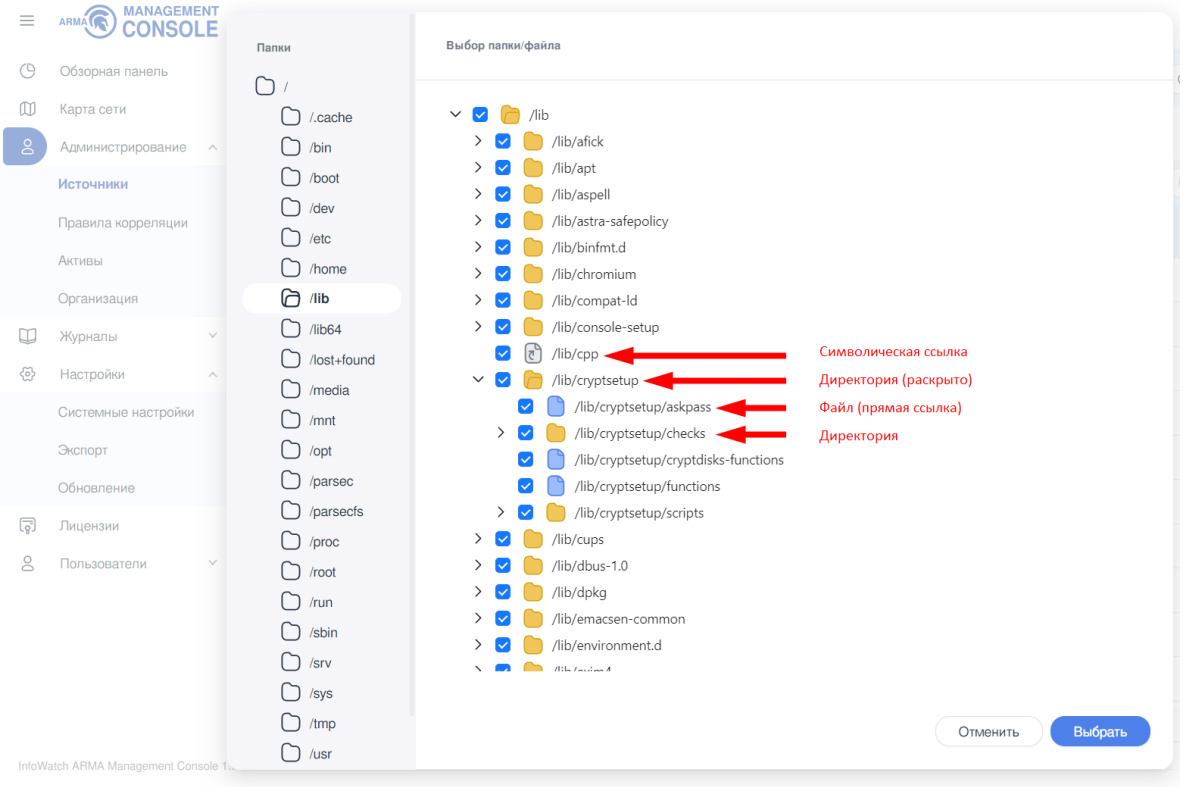

Рисунок – Добавление пути к файлу/директории

5. Нажать кнопку **«Сохранить»** в правом верхнем углу экрана.

После сохранения внесённых изменений появится соответствующее уведомление.

> **Примечание:**
>
> Путь к директории/файлу не будет добавлен в контроль целостности, если путь к вышестоящей директории уже находится в списке.

В случае любых изменений в контролируемых каталогах, необходимо запустить обновление эталонных образов нажатием кнопки **«Обновить эталонные образы»** во избежание блокировки белого списка.

Кнопка **«Проверить по базе»** применяется для сверки эталонных контрольных сумм, хранящихся в базе, и актуальных.

Для удаления путей к файлу или директории следует:

1. Выбрать необходимый элемент, установив флажок в чек-бокс элемента.
2. Нажать кнопку **«Удалить»** на панели инструментов.
3. Подтвердить удаление, нажав кнопку **«Удалить»** во всплывающем окне.
4. Нажать кнопку **«Сохранить»** в правом верхнем углу окна для подтверждения изменений.

3 КОНТРОЛЬ УСТРОЙСТВ

Функция **«Контроль устройств»** отвечает за ограничение подключаемых USB-устройств и CD/DVD-носителей.

Для перехода в модуль **«Контроль устройств»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника типа **«IEL»**.
2. В карточке источника выбрать настройку **«Контроль устройств»** (см. Рисунок – Настройка «Контроль устройств»).

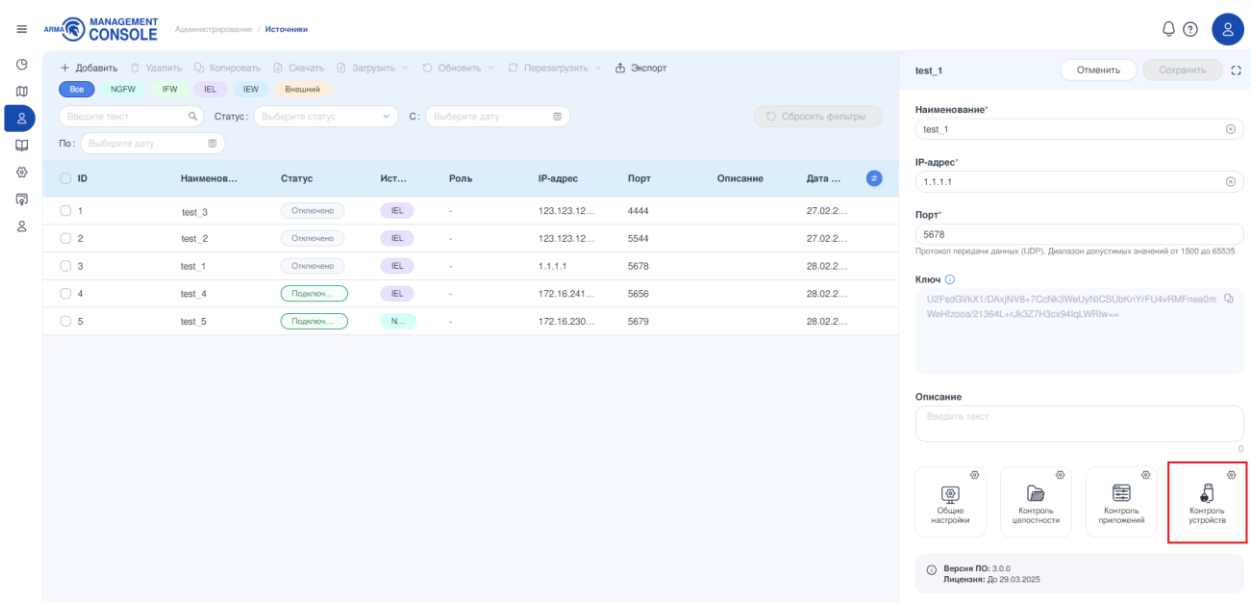

Рисунок – Настройка «Контроль устройств»

Модуль **«Контроль устройств»** содержит два основных блока настроек:

- **«Настройка разрешенных USB устройств»**;
- **«Подключенные устройства»**.

Блок настроек **«Настройка разрешенных USB устройств»** содержит перечень типов устройств, включающий в себя следующие типы (см. Рисунок – Блок «Настройка разрешенных USB устройств»):

- **«Неопределенное USB устройство»**;
- **«Устройство ввода информации»**;
- **«Аудио/Видео (камера, наушники, в том числе составные устройства)»**;
- **«Накопитель данных (flash-накопитель и card reader)»**;
- **«Устройство чтения Smart card»**;
- **«USB-хаб»**;

- **«Принтер»**;
- **«Смартфон»**;
- **«Bluetooth»**.

Примечание:

Устройство, включающее в себя несколько интерфейсов, будет заблокировано целиком, если хотя бы один из интерфейсов запрещен (не разрешен).

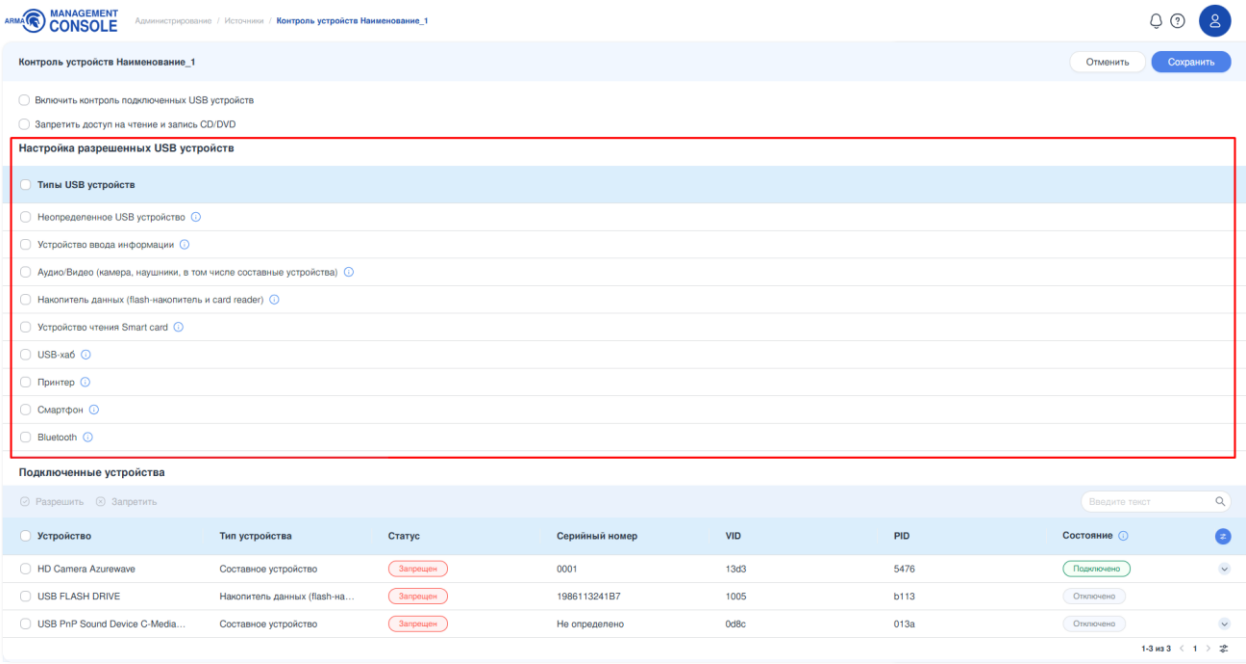

Рисунок – Блок «Настройка разрешенных USB устройств»

Блок **«Подключенные устройства»** содержит в себе все определённые **ARMA IEL** подключённые в данный момент устройства, а также устройства, подключённые ранее. Информация об устройствах представлена в формате таблицы, состоящей из следующих столбцов (см. Рисунок – Блок «Подключенные устройства»):

- **«Устройство»** – сочетание значений «наименование производителя» + «наименование продукта» устройства. В случае отсутствия производителя и продукта, поле приобретёт значение «Не определено»;
- **«Тип устройства»** – тип устройства, соответствует типам, указанным в разделе **«Настройка разрешенных USB устройств»**, определяется автоматически;
- **«Статус»** – статус устройства («Запрещен»/«Разрешен»);
- **«Серийный номер»** – серийный номер устройства, определяется автоматически. Если у подключённого устройства невозможно определить серийный номер, поле приобретёт значение «Не определено»;

- **«VID»** – VID устройства, определяется автоматически;
- **«PID»** – PID устройства, определяется автоматически;
- **«Состояние»** – состояние подключения устройства («Отключено»/«Подключено»), определяется автоматически. Под «Отключено» может подразумеваться как физическое отключение устройства от машины, так и программное, например, вследствие блокировки.

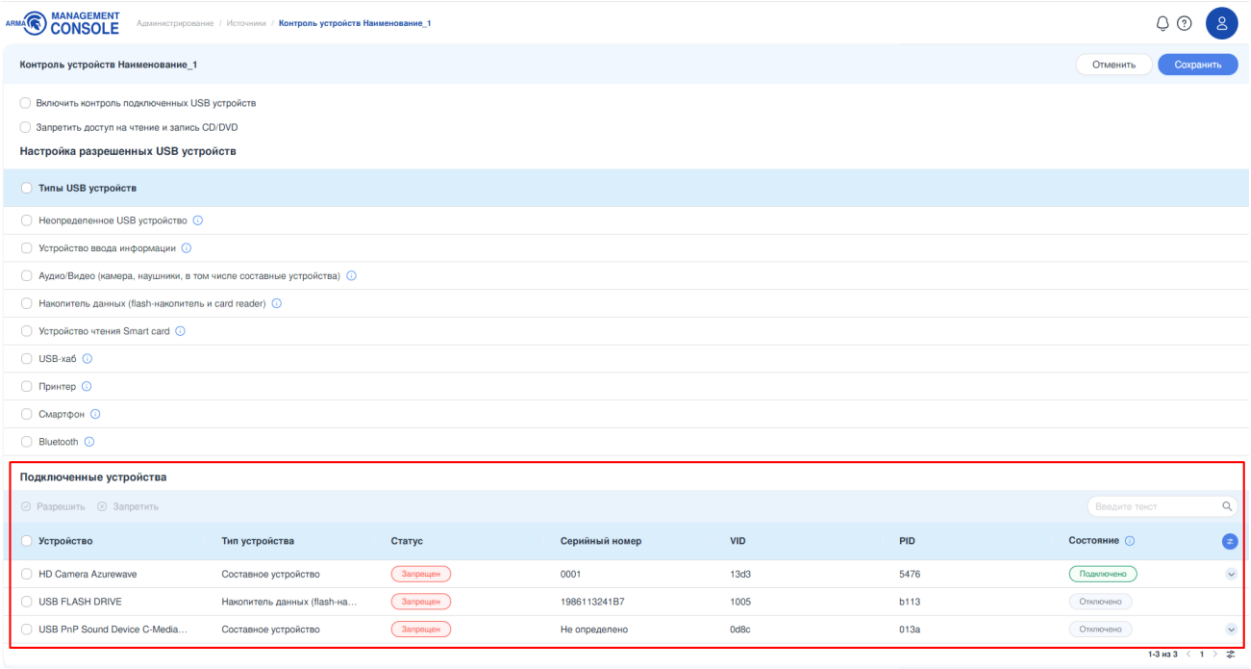

Рисунок – Блок «Подключенные устройства»

В случае подключения многосоставного устройства в столбце **«Тип устройства»** отобразится значение **«Составное устройство»**. Для просмотра состава устройства необходимо нажать кнопку « » в строке этого устройства (см. Рисунок – Составное устройство).

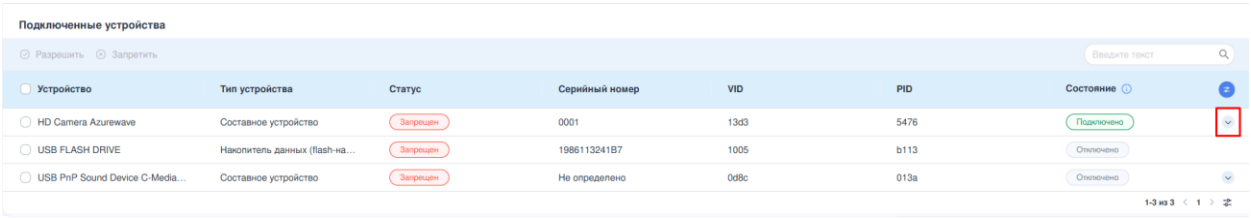

Рисунок – Составное устройство

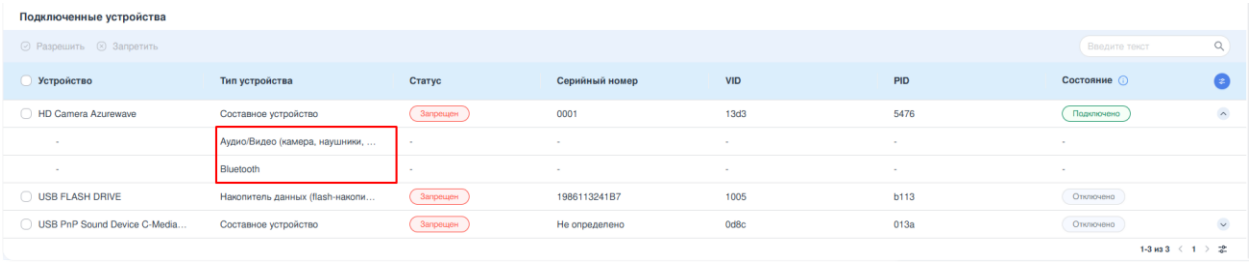

Рисунок – Состав устройства

3.1 Настройка контроля устройств по типу устройства

Для включения функции **«Контроль устройств»** и указания типов разрешённых устройств необходимо выполнить следующие действия (см. Рисунок – Контроль устройств по типу устройства):

1. Установить флажок в чек-бокс **«Включить контроль подключенных USB-устройств»**.
2. При необходимости установить флажок в чек-бокс **«Запретить доступ на чтение и запись CD/DVD»**.

   Примечание:

   Если режим **«Запретить доступ на чтение и запись CD/DVD»** активен, любой вставленный диск немедленно извлекается из устройства автоматически.

3. В блоке **«Настройка разрешенных USB устройств»** выбрать необходимые устройства из списка **«Типы USB устройств»**.
4. Нажать кнопку **«Сохранить»** в правом верхнем углу экрана.

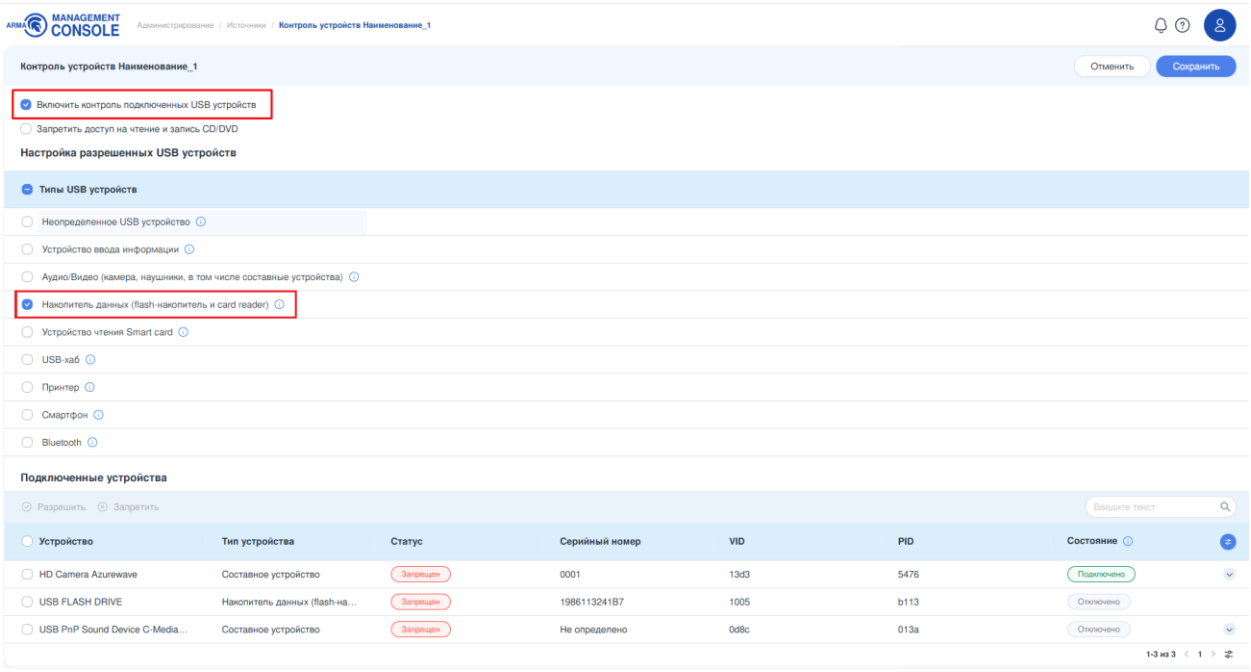

Рисунок – Контроль устройств по типу устройства

После сохранения внесённых изменений появится соответствующее уведомление (см. Рисунок – Изменение статуса устройства). Устройства, подключённые после указания типов разрешённых устройств, отобразятся в таблице **«Подключенные устройства»** в статусе **«Разрешен»**.

Примечание:

Разрешения из списка **«Типы USB устройств»** для устройств, которые были подключены до внесения изменений, применятся при их следующем подключении.

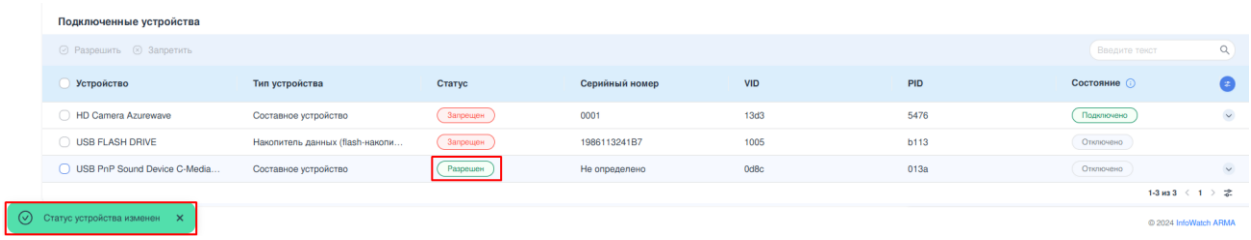

Рисунок – Изменение статуса устройства

3.2 Настройка контроля устройств по конкретному устройству

Для разрешения конкретного подключённого устройства без привязки к типам устройств необходимо выполнить следующие действия (см. Рисунок – Контроль устройств по выбранному устройству):

1. Установить флажок в чек-бокс необходимого устройства.
2. На панели инструментов нажать кнопку **«Разрешить»**.

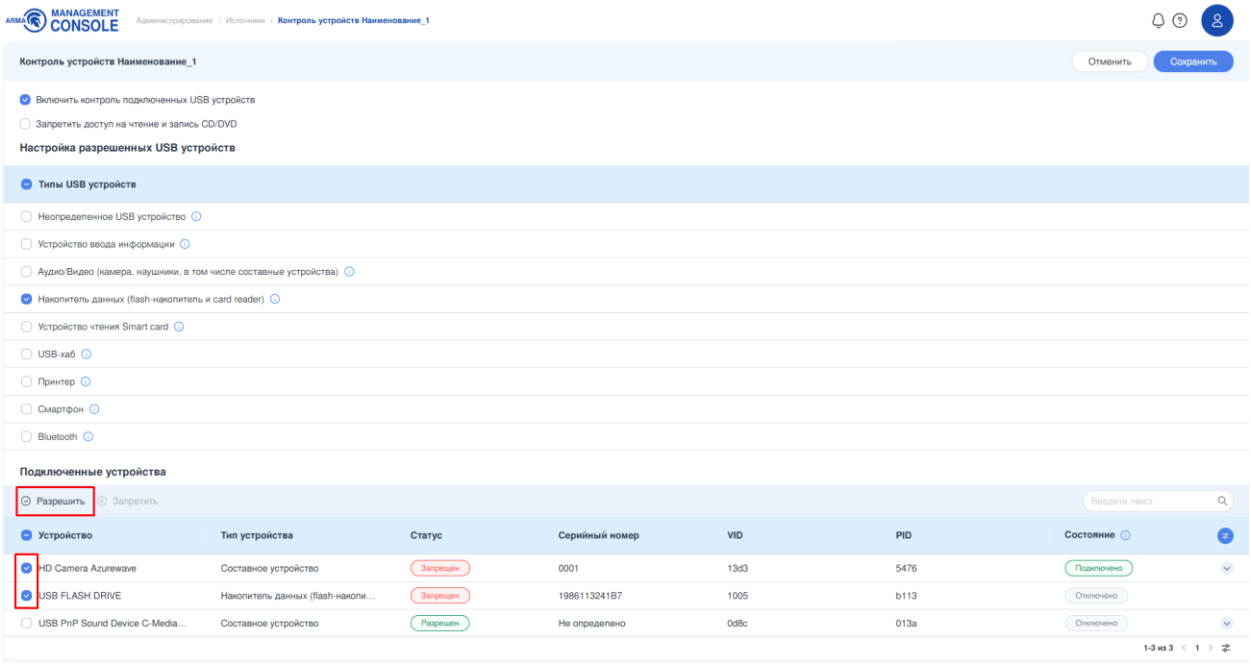

Рисунок – Контроль устройств по выбранному устройству

3. Нажать кнопку **«Сохранить»**.

После перехода подключённого устройства в статус **«Разрешен»**, появится соответствующее уведомление (см. Рисунок – Уведомление об успешном изменении статуса подключённого устройства).

Рисунок – Уведомление об успешном изменении статуса подключённого устройства

Для блокировки подключённого устройства необходимо выполнить следующие действия (см. Рисунок – Блокировка устройства):

1. Установить флажок в чек-бокс необходимого устройства.
2. На панели инструментов нажать кнопку **«Запретить»**.

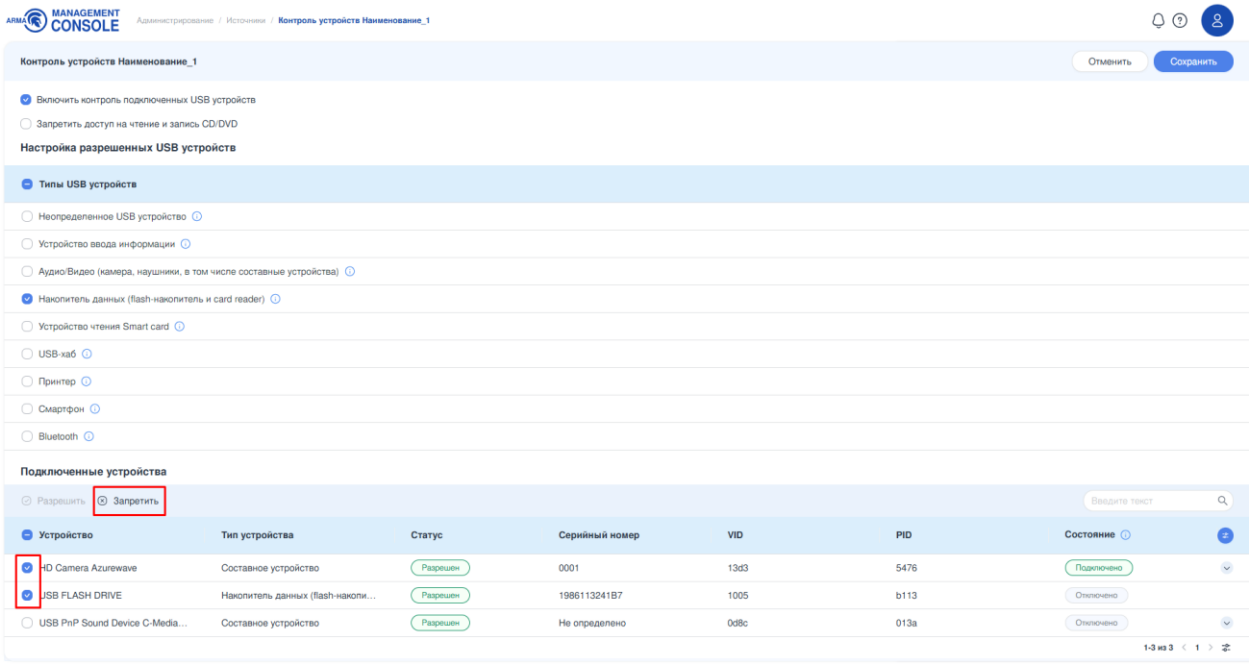

Рисунок – Блокировка устройства

3. Нажать кнопку **«Сохранить»**.

После перехода подключённого устройства в статус **«Запрещен»**, появится соответствующее уведомление (см. Рисунок – Уведомление об успешном изменении статуса подключённого устройства).

Примечание:

Правила контроля устройств имеют следующие приоритеты:

- Разрешения, заданные в блоке **«Типы USB устройств»**, имеют самый низкий приоритет.
- Изменение статуса устройства в блоке **«Подключенные устройства»** имеет более высокий приоритет по сравнению с ограничением, заданным в блоке **«Типы USB устройств»**.
- Наивысший приоритет дает добавление VID и PID устройства в конфигурационный файл (см. раздел Руководства администратора **ARMA IEL** Контроль устройств).

4 КОНТРОЛЬ ПРИЛОЖЕНИЙ

Функция **«Контроль приложений»** управляет запуском приложений на компьютерах пользователей, что позволяет выполнить политику безопасности организации при использовании приложений и снижает риск заражения компьютера, ограничивая доступ к ним.

Для перехода в модуль **«Контроль приложений»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника типа **«IEL»**.
2. В карточке источника выбрать настройку **«Контроль приложений»** (см. Рисунок – Настройка «Контроль приложений»).

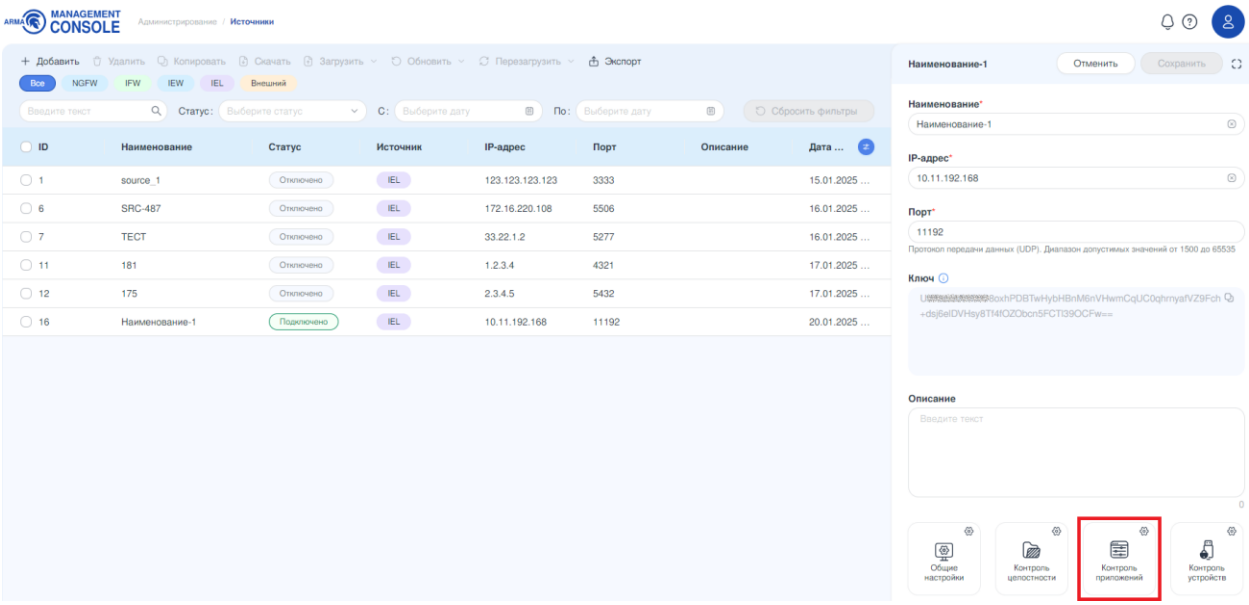

Рисунок – Настройка «Контроль приложений»

Список файлов и директорий, подлежащих контролю приложений, представлен в формате таблицы и состоит из следующих столбцов:

- **«Путь к файлу/папке»** – содержит путь к файлу или директории источника событий;
- **«Статус»** – отображает состояние записи.

В столбце **«Статус»** могут отображаться следующие состояния:

- **«Не сохранено»** – данный статус присваивается автоматически после ручного добавления пути. При закрытии экранной формы, путь с этим статусом исчезнет из списка;
- **«Новый»** – данный статус присваивается автоматически после добавления пути с помощью режима обучения;

- **«Разрешен»** – данный путь или папка доступны для открытия, просмотра или запуска;
- **«Запрещен»** – данный статус присваивается автоматически, в случае нарушения целостности файла/папки. При переводе статуса на **«Разрешен»**, произойдёт пересчёт контрольных сумм.

В столбце **«Контроль целостности файла/папки»** (см. Контроль целостности белого списка) могут отображаться следующие состояния:

- **«Включено»** – выбранный путь добавлен в список **«Контроль целостности»**;
- **«Выключено»** – выбранный путь не добавлен в список **«Контроль целостности»**.

4.1 Добавление пути к файлу/директории

Для ручного указания списка файлов и директорий, запуск которых разрешён в системе, необходимо выполнить следующие действия:

1. Перейти к настройке **«Контроль приложений»** необходимого источника типа **«IEL»** (см. Рисунок – Настройка «Контроль приложений»).
2. Установить флажок в чек-бокс параметра **«Включить контроль приложений»**.
3. При необходимости снять флажок с чек-бокса параметра **«Разрешить пользователю root игнорировать правила белого списка»**, чтобы не позволять пользователю root игнорировать правила, добавленные в список.
4. Нажать кнопку **«Добавить»** на панели инструментов. В открывшемся окне проводника выбрать необходимую директорию или файл и нажать кнопку **«Выбрать»** (см. Рисунок – Выбор файла/директории).

Примечание:

В связи с особенностью обработки операционной системой символических ссылок есть вероятность того, что система позволит запустить исполняемый файл, отсутствующий в белом списке. Рекомендуется добавлять в список и прямые ссылки, и символические ссылки на них, если такие имеются.

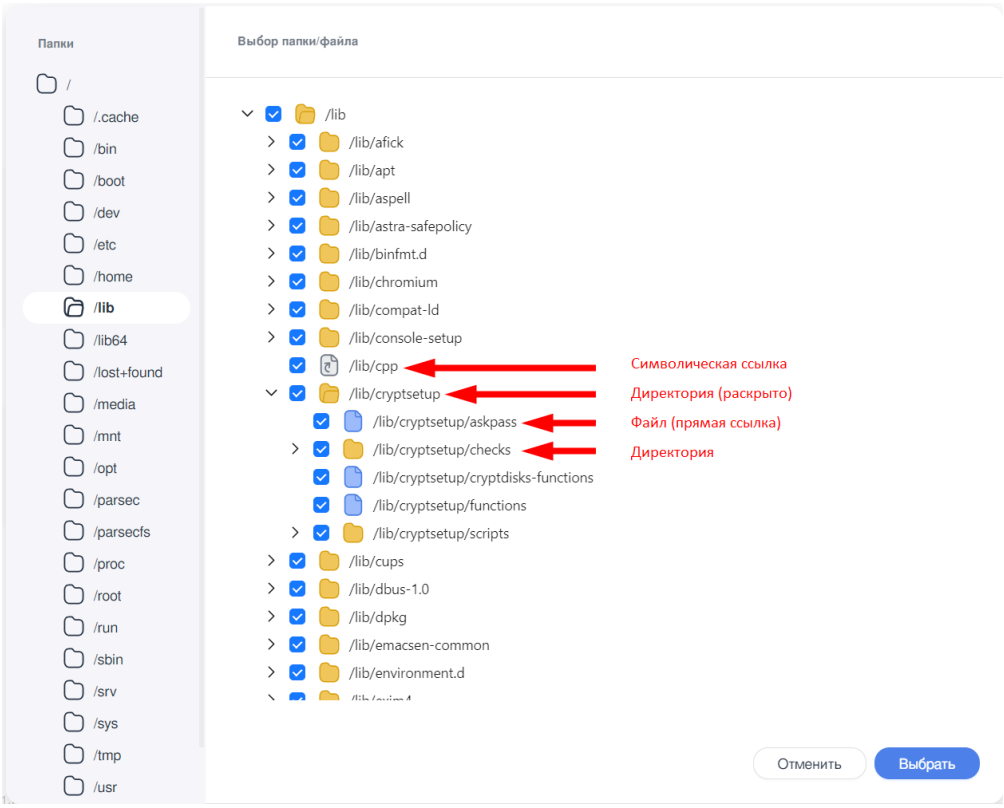

Рисунок – Выбор файла/директории

5. Нажать кнопку **«Сохранить»** в правом верхнем углу экрана.

После сохранения внесённых изменений появится соответствующее уведомление.

Примечание:

Разрешения распространяются на вложенные директории. Например, если разрешен путь **«/usr»**, то разрешены **«/usr/bin»**, **«/usr/bin/su»** и так далее.

Путь к директории/файлу не будет добавлен в контроль целостности, если путь к вышестоящей директории уже находится в списке.

4.2 Удаление пути к файлу/директории

Для удаления путей к файлу или директории следует:

1. Выбрать необходимый элемент, установив флажок в чек-бокс элемента.
2. Нажать кнопку **«Удалить»** на панели инструментов.
3. Подтвердить удаление, нажав кнопку **«Удалить»** во всплывающем окне.

Примечание:

Удаление следующих директорий может привести к частичной или полной неработоспособности ОС и **ARMA IEL**:

- **«/usr»** – содержит приложения, библиотеки, документацию и другие файлы;
- **«/root»** – директория администратора, в которой обычно хранятся файлы и конфигурации, относящиеся к администратору ОС;
- **«/lib/systemd/system»** – содержит скрипт для запуска службы «system ctl».

При попытке удаления любой из этих директорий появится уведомление **«Опасное действие! Удаление выбранного пути может нарушить работу операционной системы и IEL. Вы действительно хотите совершить действие?»**. В случае необходимости удаления директории подтвердите действие, нажав кнопку **«Удалить»** (см. Рисунок – Удаление критических директорий).

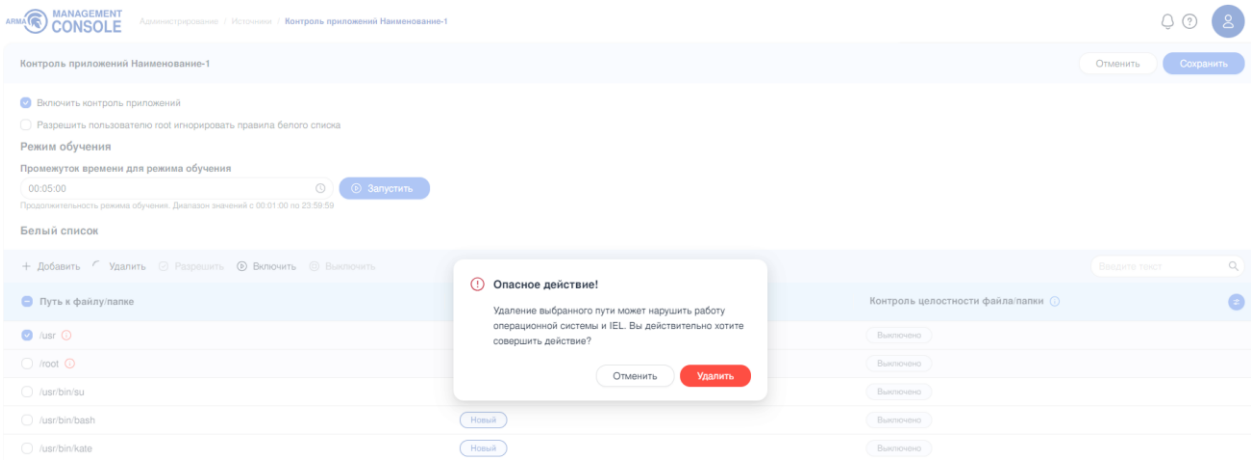

Рисунок – Удаление критических директорий

4. Для подтверждения изменений нажмите кнопку **«Сохранить»** в правом верхнем углу окна.

4.3 Режим обучения

Режим обучения для функции **«Контроль приложений»** автоматически сканирует запущенное ПО, давая пользователю возможность включить используемые приложения в белый список. Для использования режима обучения необходимо выполнить следующие действия:

1. Перейти к настройке **«Контроль приложений»** необходимого источника типа **«IEL»**.
2. Убедиться в отсутствии флажка в чек-боксе параметра **«Включить контроль приложений»**.

3. При необходимости ввести в поле **«Промежуток времени для режима обучения»** временной диапазон в формате «чч:мм:сс». Доступный диапазон от 00:01:00 до 23:59:59.

4. Нажать кнопку **«Запустить»** (см. Рисунок – Запуск режима обучения).

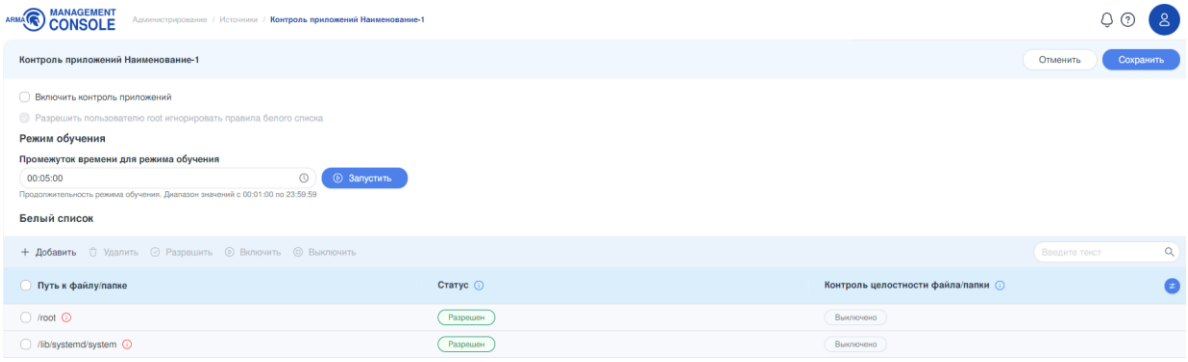

Рисунок – Запуск режима обучения

Примечание:

Запуск режима обучения при наличии несохранённых изменений в списке файлов и директорий приведёт к сохранению этих изменений. В этом случае после нажатия кнопки **«Запустить»** появится окно с уведомлением **«Запуск режима обучения приведёт к сохранению экранной формы. Вы уверены, что хотите совершить данное действие?»**.

5. Когда обучение закончится, будет выведено соответствующее уведомление, а в область **«Белый список»** добавятся пути к исполняемым файлам процессов, выполнявшихся в период действия режима обучения. В поле **«Статус»** для таких путей будет значение **«Новый»**. Чтобы открыть пути для просмотра и запуска, следует выбрать их, установив флажки в чек-боксы, и нажать кнопку **«Разрешить»** (см. Рисунок – Обучение завершено).

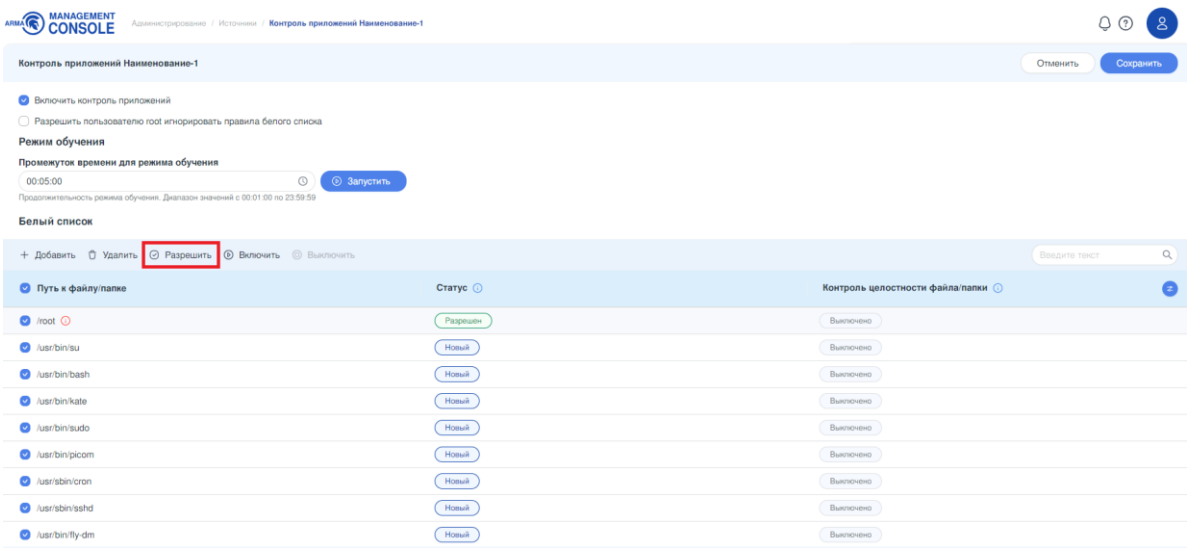

Рисунок – Обучение завершено

6. После того как все необходимые пути разрешены, установите флажок в чек-бокс параметра **«Включить контроль приложений»**.

При необходимости принудительного завершения режима обучения следует нажать кнопку **«Остановить»** (см. Рисунок – Остановка режима обучения).

Примечание:

Режим обучения позволяет найти пути до приложений, которые еще не попали в белый список.

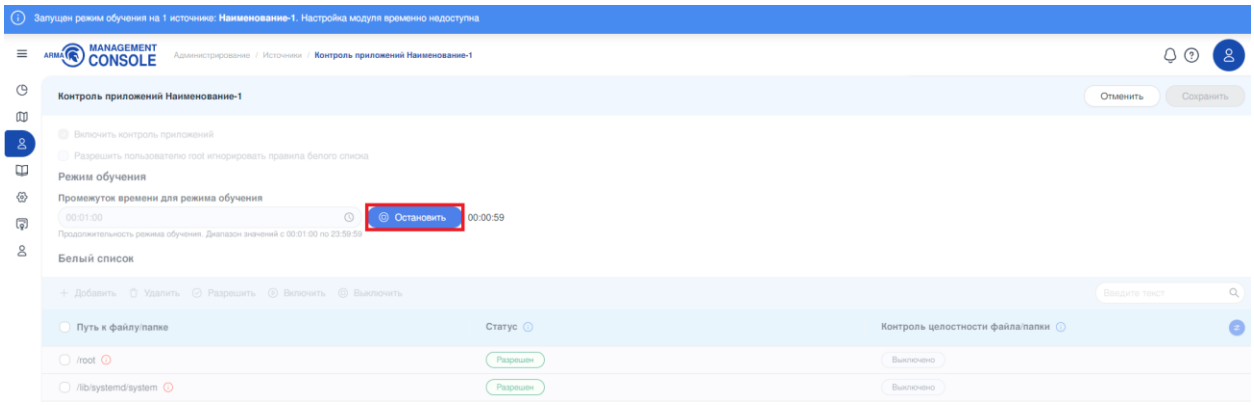

Рисунок – Остановка режима обучения

В случае изменения IP-адреса Центра Управления или перезапуска IEL во время активированного режима обучения, будет выполнена остановка режима обучения, без его автоматического возобновления.

4.4 Контроль целостности белого списка

Существует возможность включения контроля целостности для белого списка приложений. Для включения необходимо выполнить следующие действия:

1. Выделить необходимую строку или строки таблицы.

2. На панели инструментов нажать кнопку **«Включить»** (см. Рисунок – Включение КЦ).

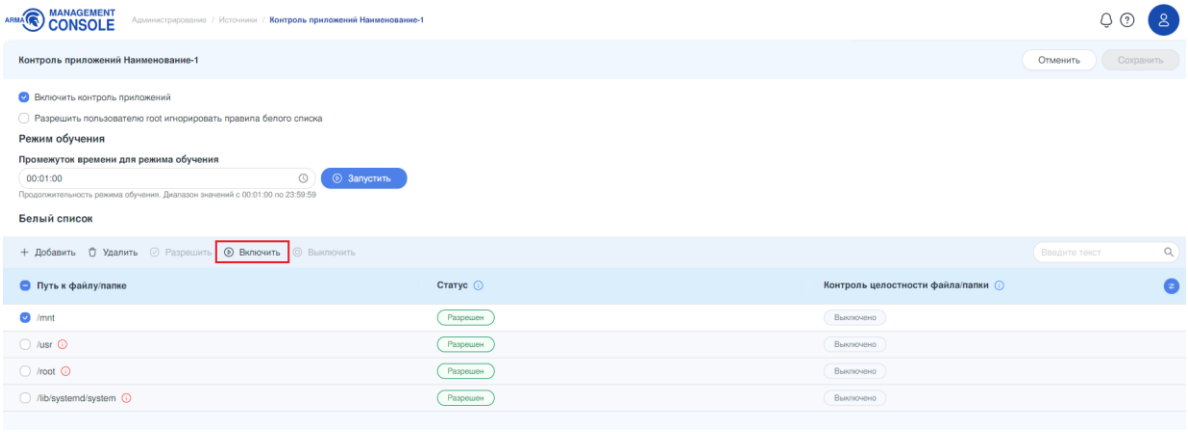

Рисунок – Включение КЦ

В случае если модуль **«Контроль целостности»** был выключен, в появившемся окне (см. Рисунок – Включение модуля КЦ) необходимо подтвердить включение модуля, нажав кнопку **«Активировать»**.

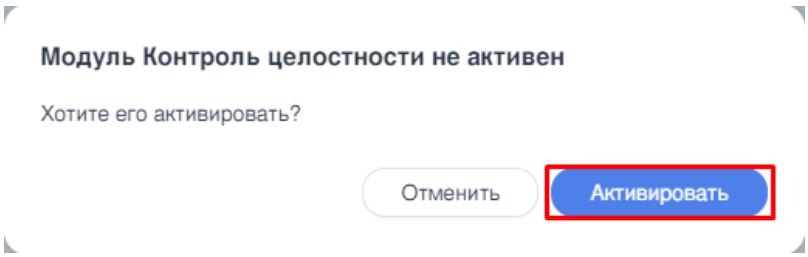

Рисунок – Включение модуля КЦ

3. Нажать кнопку **«Сохранить»** в правом верхнем углу экрана.

После включения контроля целостности выбранные записи будут добавлены в список контроля целостности, статусы записей в белом списке изменятся на **«Включено»** (см. Рисунок – Статус КЦ).

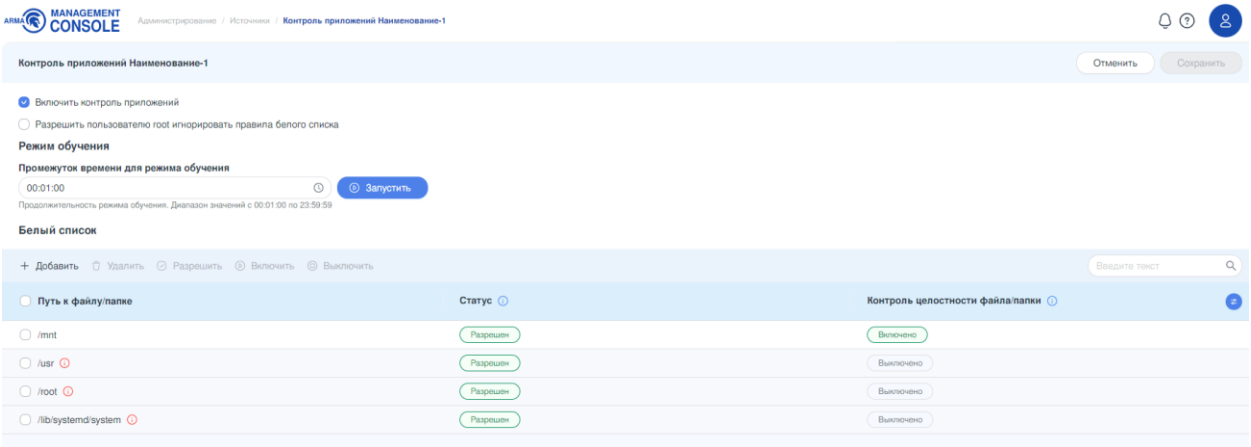

Рисунок – Статус КЦ

Для выключения контроля целостности необходимо выбрать запись или записи и нажать кнопку **«Выключить»** на панели инструментов. При выключении путь будет удалён из списка контролируемых модулем **«Контроль целостности»**.

Примечание:

Существует возможность включить запись в белый список, если её по какой-либо причине заблокировал модуль **«Контроль целостности»**. Для этого необходимо выбрать запись и нажать кнопку **«Разрешить»**.

5 СОБЫТИЯ

При успешной синхронизации **ARMA IEL** с **ARMA MC** все события, зафиксированные модулями **«Контроль приложений»**, **«Контроль целостности»** и **«Контроль устройств»**, а также изменения в конфигурации фиксируются в **ARMA MC** в формате **«cef»**.

При потере связи с **ARMA MC ARMA IEL** продолжает работать автономно по заданным конфигурациям, регистрируя события в базе данных при включенном журналировании. После восстановления связи события будут отправлены в **ARMA MC**.

Для просмотра списка событий необходимо открыть **ARMA MC**, выбрать раздел меню **«Журналы»**, затем – подраздел **«События»**.

Примечание:

Порядок работы с событиями и просмотра подробной информации о них представлен в разделе ch_mc_rp_events Руководства пользователя **ARMA MC**.

5.1 Формат вложенного сообщения «cef»

Формат вложенного сообщения **«cef»** имеет следующий вид:

```
«CEF:<Version>|<Device Vendor>|<Device Product>|<Device Version>
|<Device Event Class ID>|<Name>|<Priority>|<Extension>»
```

где:

- **«<Version>»** – версия формата **«cef»**;
- **«<Device Vendor>»** – производитель источника логов, всегда **InfoWatch ARMA**;
- **«<Device Product>»** – название продукта источника логов, **ARMA IEL**;
- **«<Device Version>»** – версия продукта источника логов;
- **«<Device Event Class ID>»** – идентификатор события:
  - «white_list»;
  - «integrity_control»;
  - «device_control»;
  - «config_file»;
- **«<Name>»** – описание события;
  - «White list»;

- «Integrity control»;
- «USB»;
- «Config file»;

- **«<Priority>»** – приоритет события от «1» до «6»;
- **«<Extension>»** – дополнительные поля, представляющие собой пары ключ=значение, в значении допускаются пробелы.

5.1.1 Ключи блока «<Extension>»

- **«rt»** – время в формате unix timestamp;
- **«suser»** – пользователь, инициировавший событие;
- **«act»** – действие, которое было совершено:
  - «act=DENIED» – запрещено;
  - «act=ALLOWED» – разрешено;
  - «act=REMOVE» – удаление;
  - «act=WRITE» – изменение;
  - «act=CREATE» – создание;
  - «act=CHMOD» – изменение прав доступа;
  - «act=CHANGE» – изменение;
- **«filePath»** – путь расположения файла, над которым было совершено действие;
- **«fname»** – наименование файла («FILE» – файл, «DIR» – папка);
- **«fileType»** – тип файла;
- **«cat»** – категория действия;
- **«cs1»** – PID или наименование подключённого устройства (USB или CD/DVD);
- **«cs1Label»** – наименование «pid» или «device»;
- **«cs2»** – VID подключенного устройства;
- **«cs2Label»** – наименование «vid»;
- **«cs3»** – серийный номер подключенного устройства;
- **«cs3Label»** – наименование «serial_number».

5.2 Примеры «cef» сообщений

5.2.1 Сообщения модуля «Контроль приложений»

1. Модуль **«Контроль приложений»** заблокировал пользователю **«simpleuser»** доступ к файлу **«test.txt»**, расположенному в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|white_list|White list|4|rt=1717764281
suser=simpleuser act=DENIED
cat=Blocked by app control filePath=/mnt/TEST/folder fname=test.txt
```

2. Модуль **«Контроль целостности»** заблокировал пользователю **«simpleuser»** доступ к файлу **«test.txt»**, расположенному в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|white_list|White list|4|rt=1717764281
suser=simpleuser act=DENIED
cat=Blocked by integrity control filePath=/mnt/TEST/folder
fname=test.txt
```

5.2.2 Сообщения модуля «Контроль целостности»

1. Удалена папка **«folder»**, располагавшаяся в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=REMOVE
filePath=/mnt/TEST/folder fname=folder
```

2. Удалён файл **«test.txt»**, располагавшийся в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=REMOVE
filePath=/mnt/TEST/test.txt fname=test.txt
```

3. Изменён **«test.txt»**, расположенный в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=WRITE
filePath=/mnt/TEST/test.txt fname=test.txt fileType=FILE
```

4. В **«/mnt/TEST/»** создана папка **«folder»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=CREATE
filePath=/mnt/TEST/folder fname=folder fileType=DIR
```

5. В **«/mnt/TEST/»** создан файл **«test.txt»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=CREATE
filePath=/mnt/TEST/test.txt fname=test.txt fileType=FILE
```

6. Перемещена папка **«folder»**, располагавшаяся в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=MOVE
filePath=/mnt/TEST/folder fname=folder fileType=DIR
```

7. Перемещён файл **«test.txt»**, располагавшийся в **«/mnt/TEST/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=MOVE
filePath=/mnt/TEST/test.txt fname=test.txt fileType=FILE
```

8. Изменены права доступа к папке **«folder»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=CHMOD
filePath=/mnt/TEST/folder fname=folder fileType=DIR
```

9. Изменены права доступа к файлу **«test.txt»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|integrity_control|Integrity control|5|rt=1717764281
act=CHMOD
filePath=/mnt/TEST/test.txt fname=test.txt fileType=FILE
```

5.2.3 Сообщения модуля «Контроль устройств»

1. Заблокировано подключение устройства с PID «1111a», VID «22b» и серийным номером «333333333»:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|device_control|USB|4|rt=1717764281 act=DENIED
cs1=1111a cs2=22b
cs1Label=pid cs2Label=vid cs3Label=serial_number cs3=333333333
```

2. Успешное подключение устройства с PID «1111a», VID «22b» и серийным номером «333333333»:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|device_control|USB|6|rt=1717764281
act=ALLOWED cs1=111a cs2=22b
cs1Label=pid cs2Label=vid cs3Label=serial_number cs3=333333333
```

5.2.4 Сообщение об изменении конфигурационного файла

1. Пользователь **«simpleuser»** внёс изменения в файл **«integrity-control-config.yaml»**, расположенный в **«/etc/iwarma-endpoint/»**:

```
CEF:0|InfoWatch ARMA|ARMAIEL|3.0|config_file|Config file|5|rt=1717764281
suser=simpleuser act=CHANGE
filePath=/etc/iwarma-endpoint/integrity-control-config.yaml fname=integrity-control-config.yaml
fileType=FILE
```

6 СВЕДЕНИЯ О ЛИЦЕНЗИИ И ВЕРСИИ ПО

Для просмотра информации о лицензии и версии ПО источника достаточно открыть карточку необходимого источника типа **«IEL»**. Искомая информация отображается в нижней части карточки (см. Рисунок – Сведения о лицензии и версии ПО).

Примечание:

При необходимости содержимое карточки можно прокрутить вниз с помощью колесика мыши или полосы прокрутки.

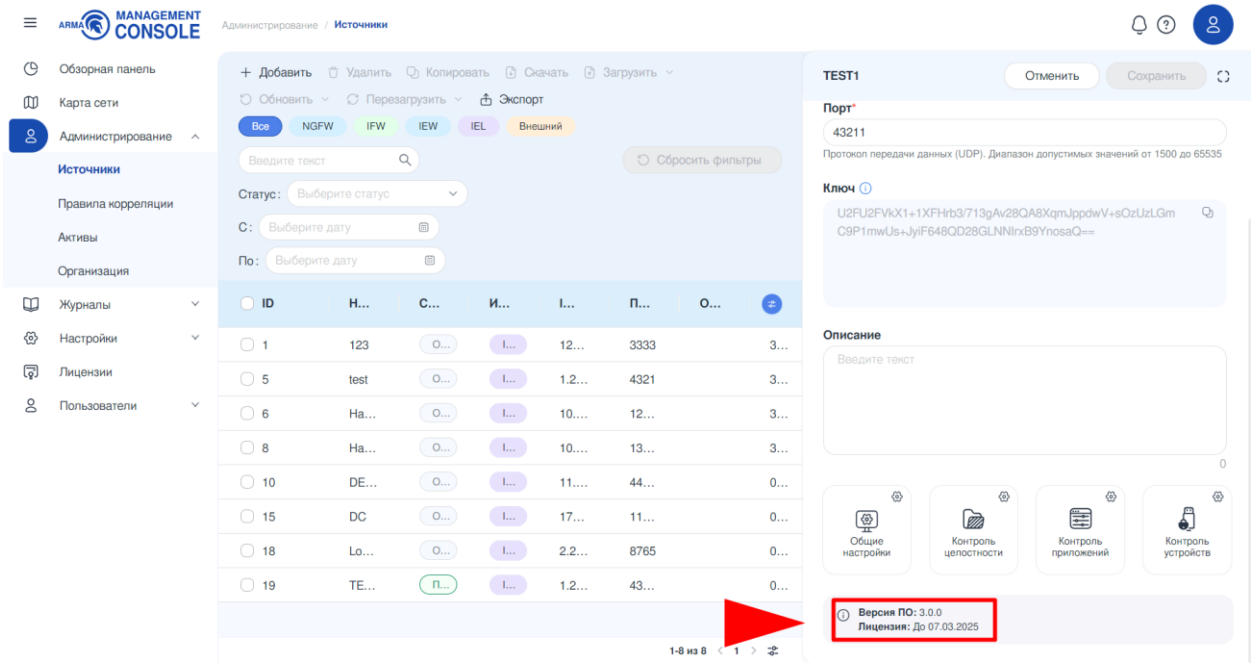

Рисунок – Сведения о лицензии и версии ПО

Если лицензия не активирована, ПО **ARMA IEL** не может выполнять свои функции. Модули не отображаются, а в поле «**Лицензия**» выводится значение «**Не определено**» (см. Рисунок – Лицензия не активирована).

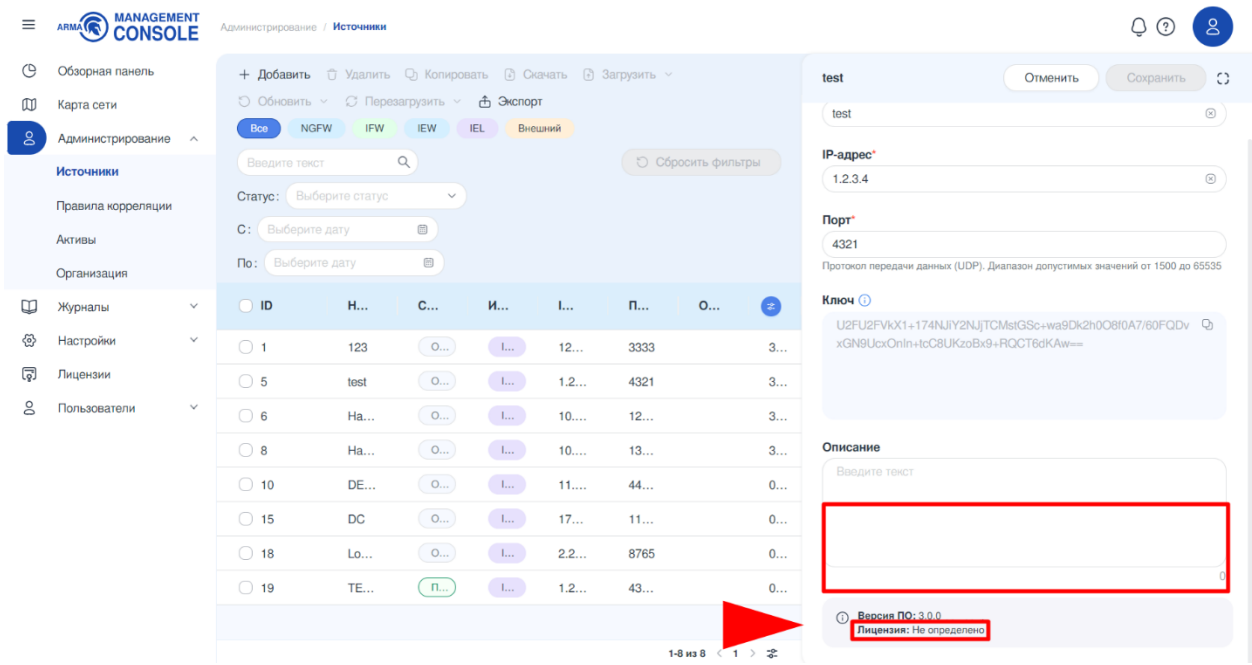

Рисунок – Лицензия не активирована