Руководство пользователя по эксплуатации

версия 9 ред. от 14.04.2022

Листов 43

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Таблица 1
Термины и сокращения

Термины и сокращения	Значение
БД	База данных
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
ЧПУ	Числовое программное управление
ARMA IE	InfoWatch ARMA Industrial Endpoint
ARMA MC	InfoWatch ARMA Management Console
ID	Идентификатор

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, которые выполняют конфигурирование и мониторинг работы **ARMA IE v.2.5.3.**

Руководство пользователя по эксплуатации содержит описание консольного интерфейса, доступных функций с подробным описанием их настройки и использования, а также принципов работы с **ARMA IE**.

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

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Общие сведения

ARMA IE представляет собой системный сервис с графическим интерфейсом пользователя.

Управление программой возможно локально или посредством **ARMA MC**.

ARMA IE предназначен для решения следующих задач:

- контроль целостности программного обеспечения;
- ограничение перечня исполняемых программ;
- ограничение подключаемых съемных носителей;
- отправка событий безопасности в централизованную консоль управления;
- обнаружение вредоносного ПО.

1.2 Требования к среде функционирования

Установка **ARMA IE** производится с помощью установщика с расширением **«.msi»**.

Подробная установка **ARMA IE** описана в п. 2.2 настоящего руководства.

Для аппаратной платформы, на которую устанавливается **ARMA IE**, достаточно руководствоваться минимальными требованиями к аппаратному обеспечению (см. Таблица 2, Таблица 3).

Таблица 2

Минимальные требования к аппаратному обеспечению

Название оборудования	Требования
Процессор	2 ГГц, одноядерный, x86 или x64
Жесткий диск	200 Мб свободной памяти на диске
ОЗУ	100 Мб свободной памяти
Операционная система	Windows 10/ Windows 10 LTSC/LTSB
Зависимости	Программная платформа .NET Framework версия 3.5

Таблица 3

Минимальные требования к аппаратному обеспечению с лицензией ENTERPRISE базовая + антивирусная защита

Название оборудования	Требования
Процессор	2 ГГц, одноядерный
Жесткий диск	6 ГБ свободной памяти на диске

Название оборудования	Требования
ОЗУ	3 ГБ свободной памяти
Операционная система	Windows 10/ Windows 10 LTSC/LTSB

2 НАЧАЛО РАБОТЫ

2.1 Настройка сервиса с ОС Windows

Для работы программы необходимо предварительно разделить права пользователей в ОС. Для обычных пользователей не рекомендуется предоставлять права администратора.

2.1.1 Создание пользователя с ограниченными правами

От имени администратора необходимо создать пользователя с ограниченными правами. Для этого следует перейти в **«Управление компьютером»**, выбрать **«Локальные пользователи и группы»**, щелкнуть правой кнопкой мыши по пункту **«Пользователи»** и в контекстном меню выбрать пункт **«Новый пользователь...»** (см. Рисунок 1).

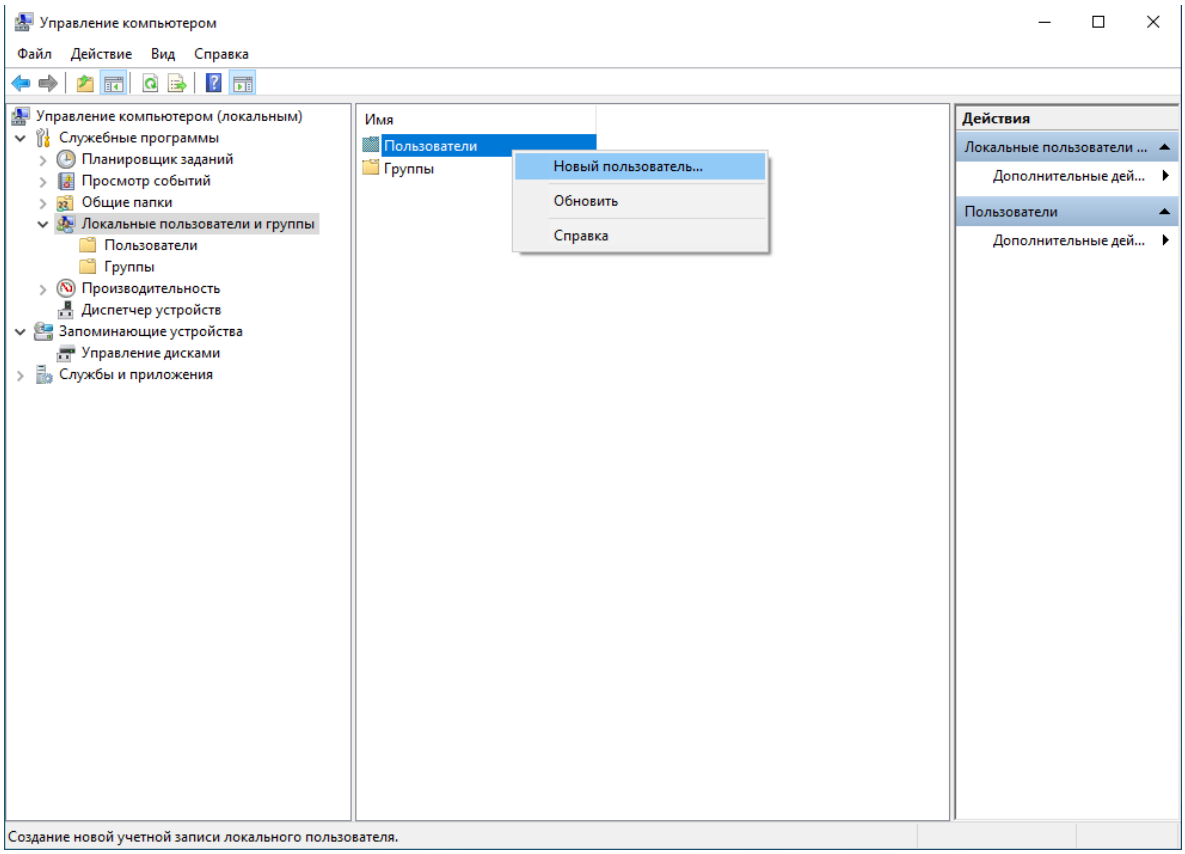

Рисунок 1 – Создание новой учетной записи локального пользователя

В появившемся окне задать имя пользователя (в примере, «userep») и пароль, установить галочку в пункте **«Срок действия пароля не ограничен»** и нажать **кнопку «Создать»**, а затем **кнопку «Закрыть»** (см. Рисунок 2).

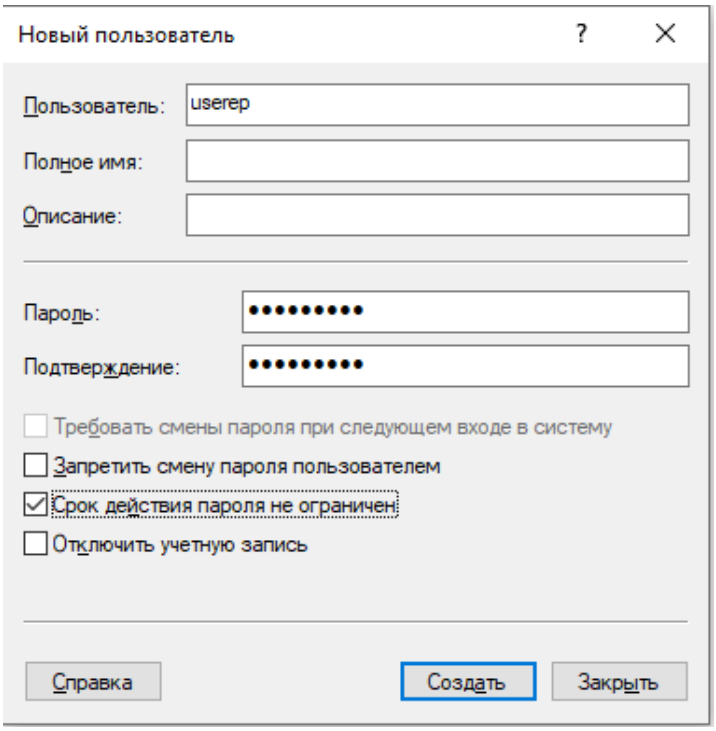

Рисунок 2 – Добавление пользователя

Для того чтобы убедиться, что учетная запись «userep» не обладает правами администратора необходимо зайти в учетные записи пользователей (**«Управление компьютером» - «Локальные пользователи и группы» - «Пользователи»**) и у пользователя «userep» открыть **«Свойства» - «Членство в группах»** (см. Рисунок 3).

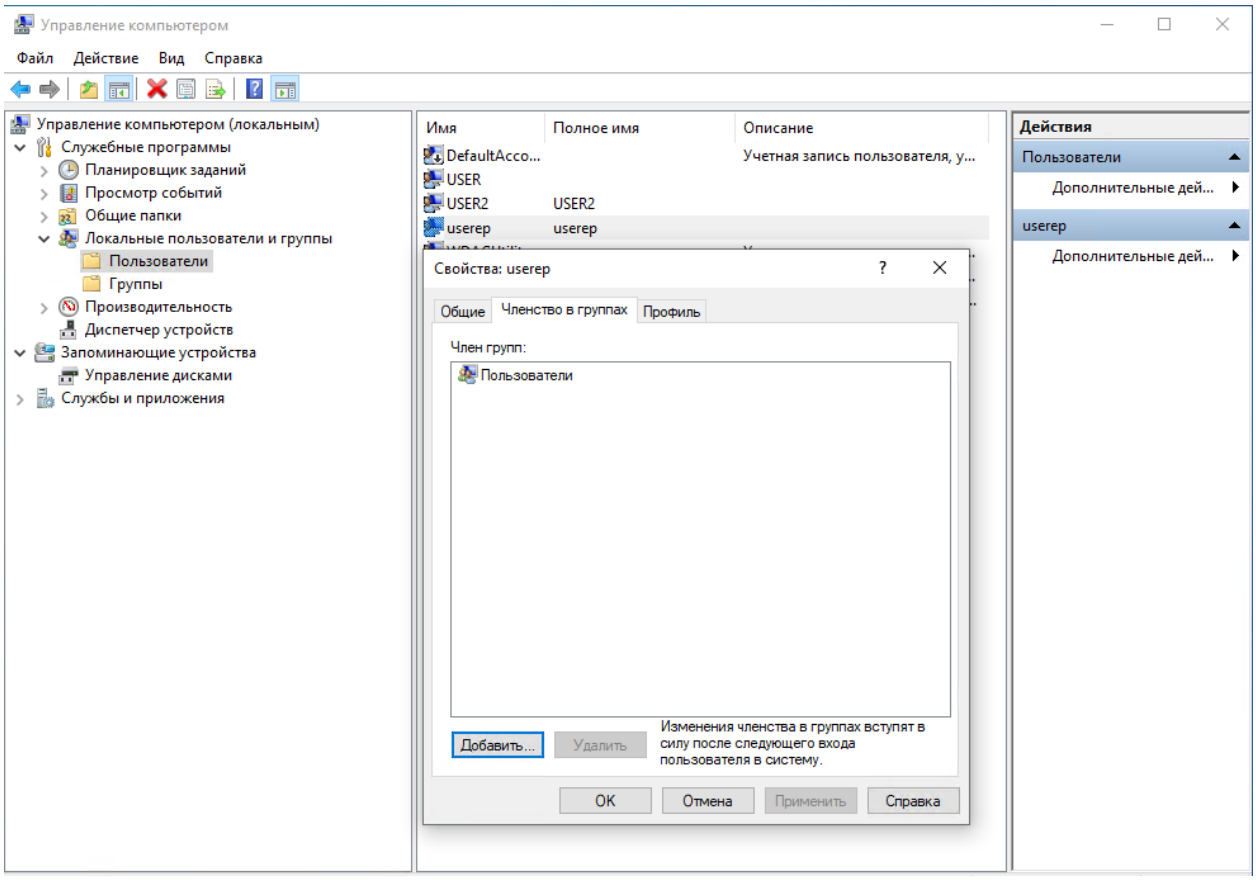

Рисунок 3 – Свойства учетной записи

2.2 Установка сервиса

Для установки сервиса **ARMA IE**, используя учетную запись администратора, необходимо запустить установщик **«ARMA Industrial Endpoint installer.msi»** и установить, следуя подсказкам мастера установки (см. Рисунок 4, Рисунок 5, Рисунок 6, Рисунок 7).

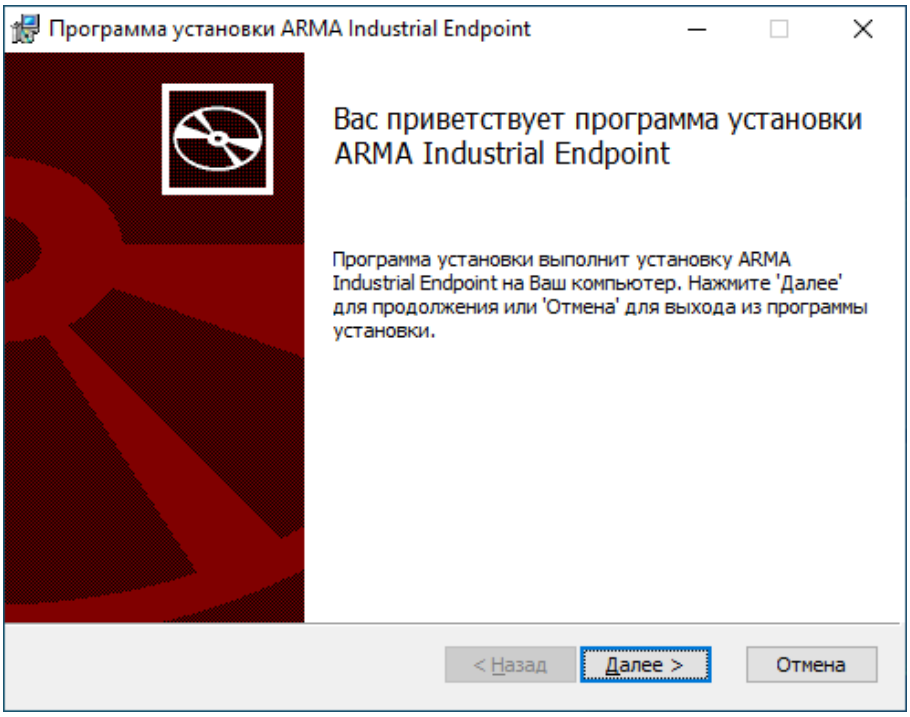

Рисунок 4 – Установка ARMA IE (1)

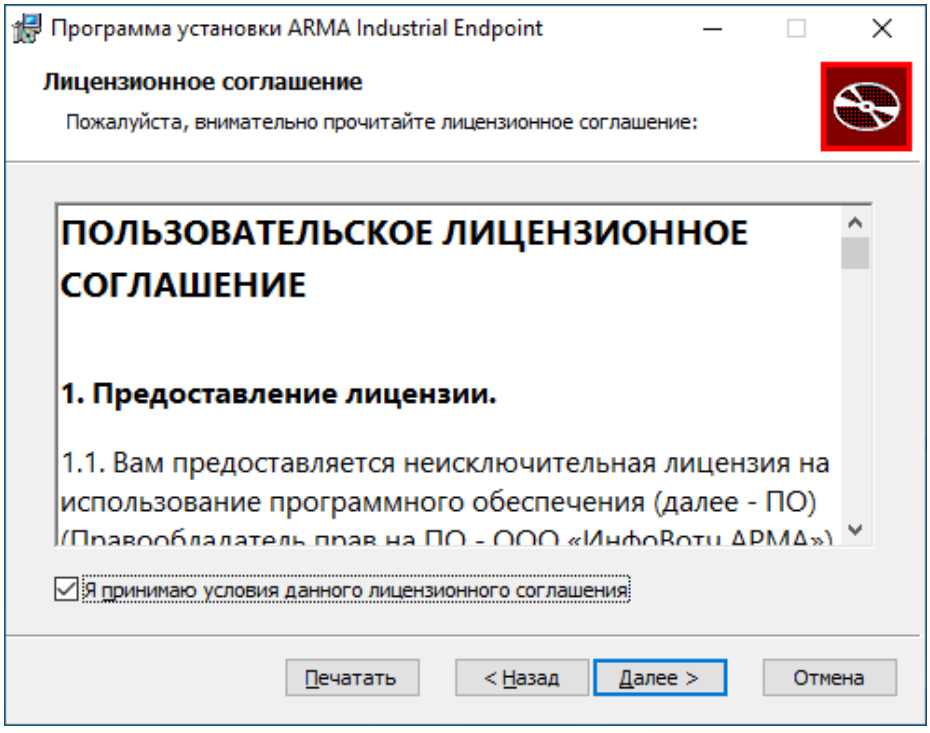

Рисунок 5 – Установка ARMA IE (2)

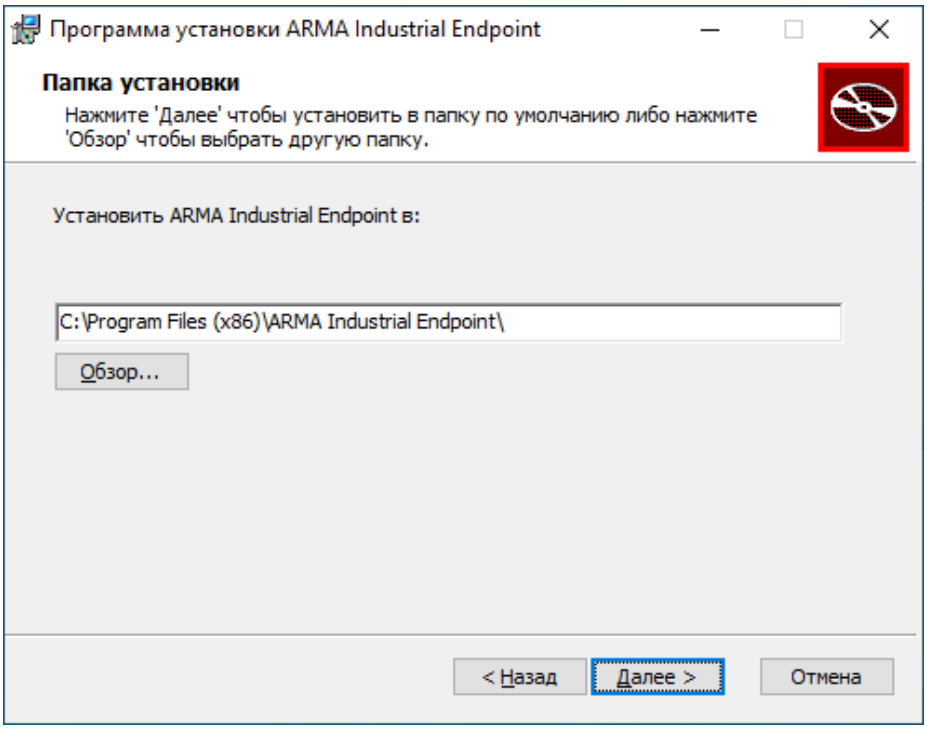

Рисунок 6 – Установка ARMA IE (3)

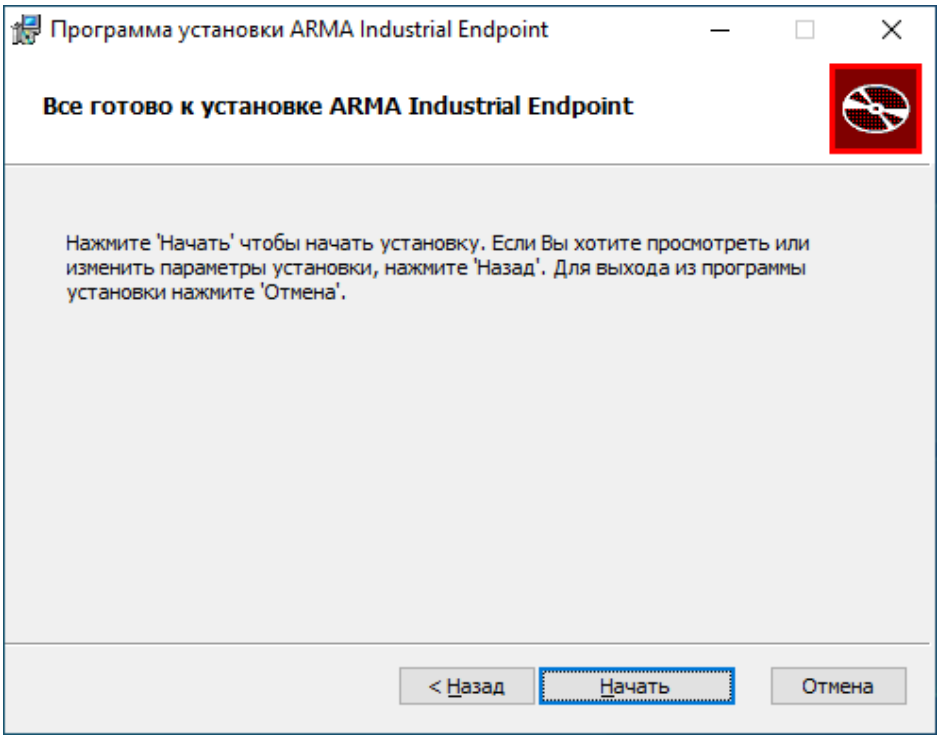

Рисунок 7 – Установка ARMA IE (4)

После нажатия **кнопки «Начать»** во всплывающем окне нужно подтвердить действие, после чего запустится установка. После завершения установки и нажатия **кнопки «Готово»** во всплывающем окне будет предложено перезагрузить компьютер (см. Рисунок 8).

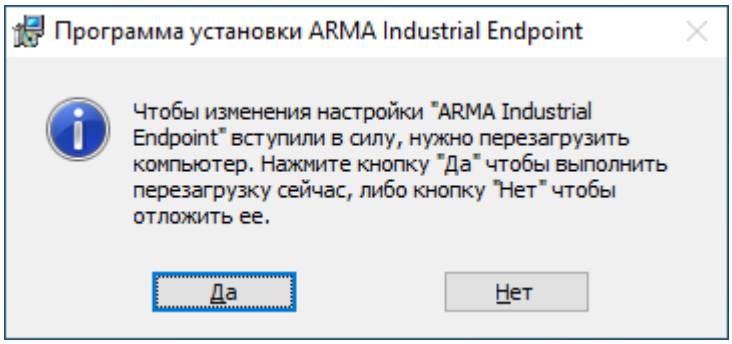

Рисунок 8 – Всплывающее окно перезагрузки

После установки **ARMA IE** и перезагрузки компьютера будет автоматически запущен сервис **«ARMA Industrial Endpoint»**, который можно просмотреть в службах Windows (см. Рисунок 9), и создано правило межсетевого экрана, которое можно просмотреть в Брандмауэр Защитника Windows (**«Дополнительные параметры» – «Правила для входящих подключений»**) (см. Рисунок 10).

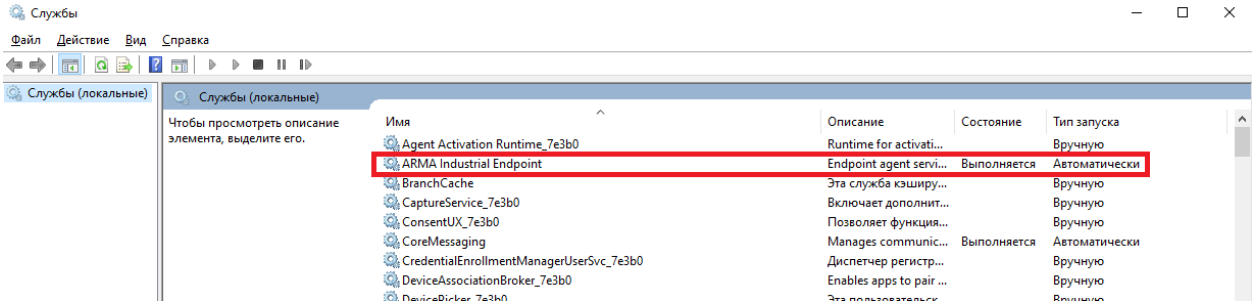

Рисунок 9 – Сервис «ARMA Industrial Endpoint»

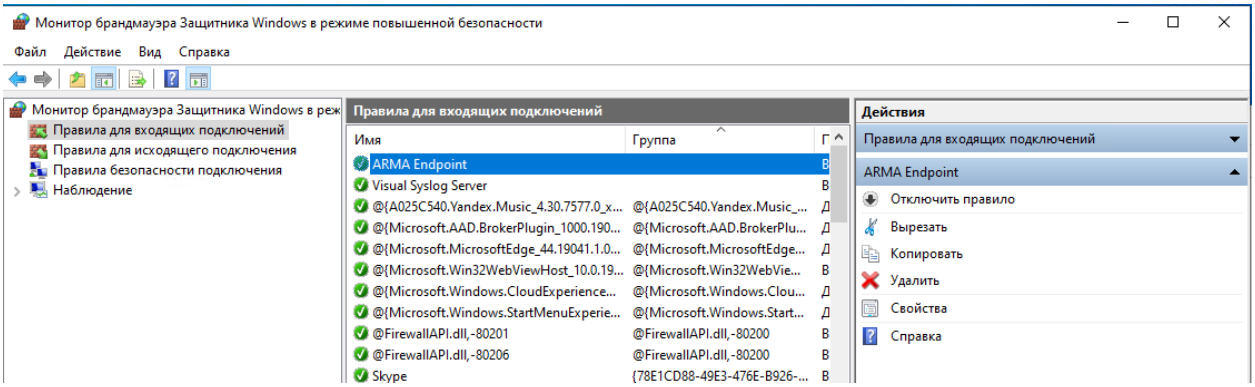

Рисунок 10 – Правило межсетевого экрана

2.3 Запуск сервиса

Для запуска сервиса **ARMA IE** необходимо открыть графический интерфейс, нажав **иконку «Endpoint»** в меню «Пуск». При первом запуске графического интерфейса пользователю будет предложено задать пароль, который в дальнейшем будет использоваться для авторизации (см. Рисунок 11).

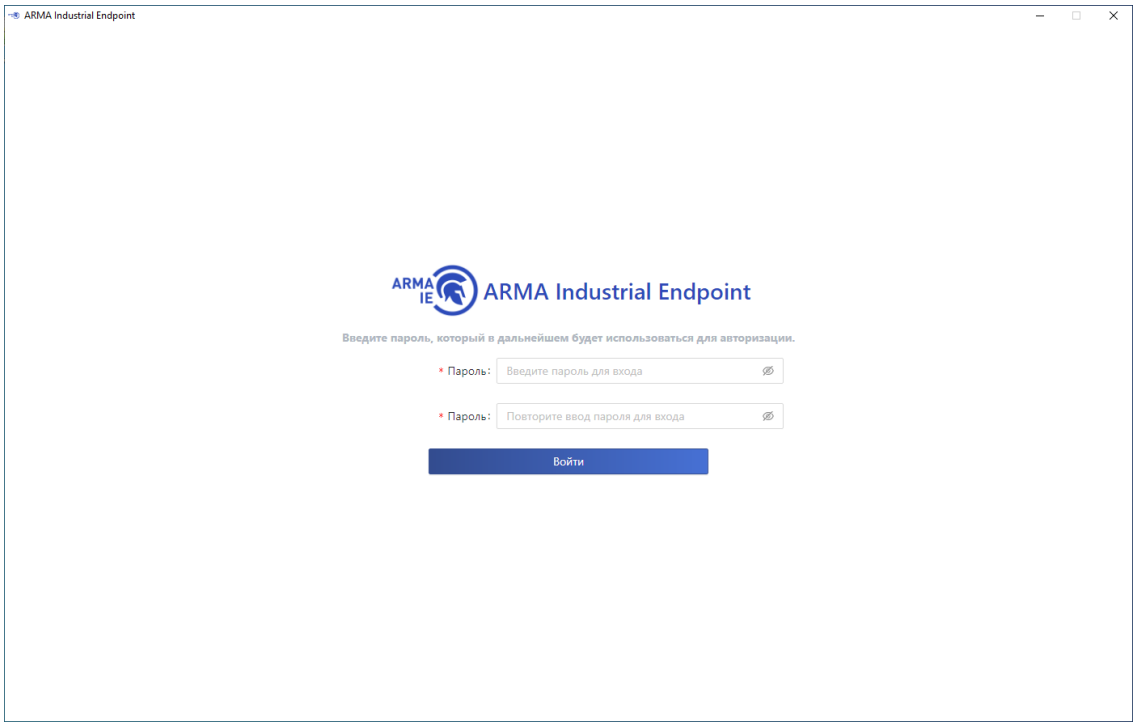

Рисунок 11 – Главное окно графического интерфейса ARMA IE

После ввода пароля необходимо активировать лицензию одним из предложенных способов (см. Рисунок 12):

- активация лицензии с доступом в Интернет (**«Активировать онлайн»**);
- активация лицензии без доступа в Интернет (**«Активировать оффлайн»**).

!Важно Лицензионный ключ предоставляется согласно условиям в договоре поставки.

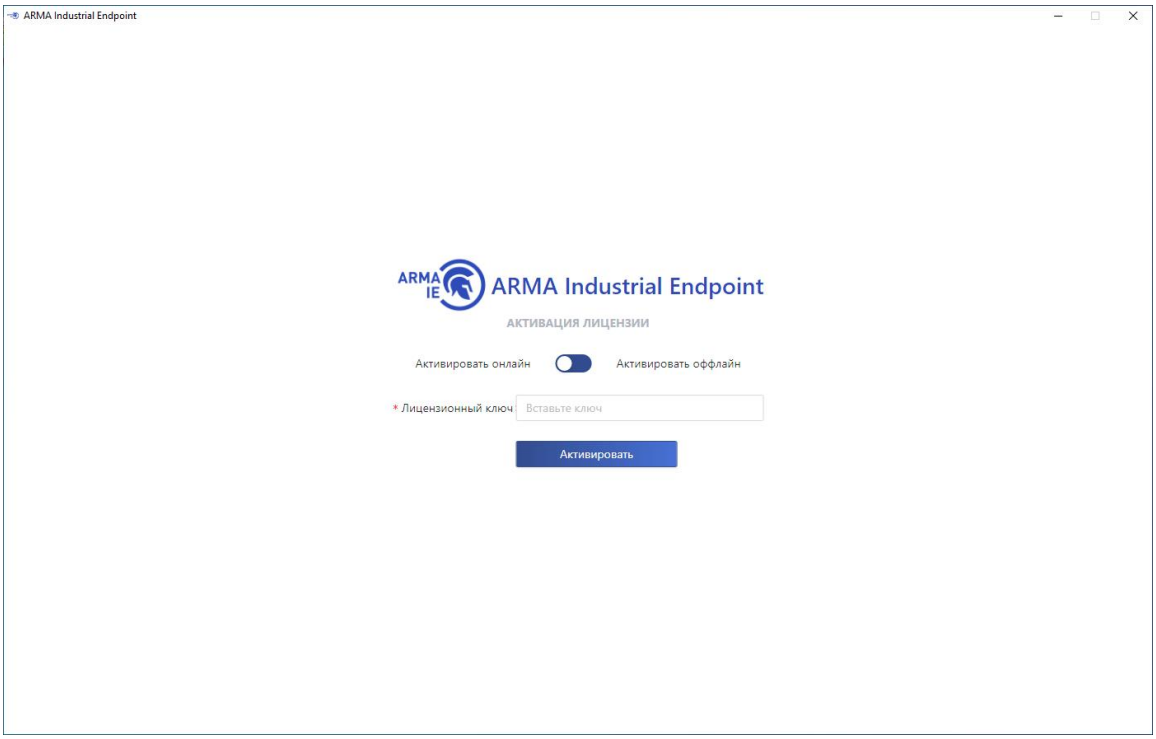

Рисунок 12 – Активация лицензии

2.3.1 Активация лицензии с доступом в Интернет

Для активации лицензии с доступом в Интернет необходимо установить ползунок в сторону **«Активировать онлайн»**, в поле **«Лицензионный ключ»** вставить ключ и нажать **кнопку «Активировать»** (см. Рисунок 13).

При успешной активации лицензии появится уведомление об этом (см. Рисунок 44).

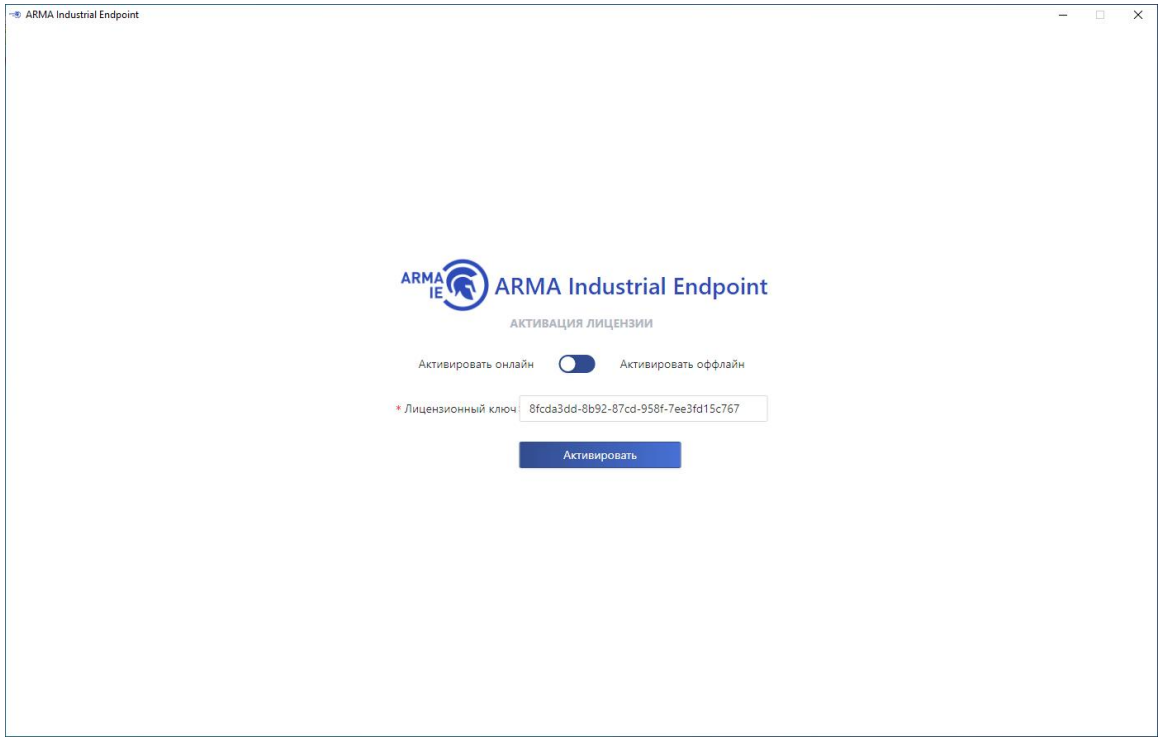

Рисунок 13 – Активация лицензии с доступом в Интернет

2.3.2 Активация лицензии без доступа в Интернет

Для активации лицензии без доступа в Интернет необходимо установить ползунок в сторону **«Активировать оффлайн»**, в поле **«Лицензионный ключ»** вставить ключ и нажать **кнопку «Получить токен»** (см. Рисунок 14).

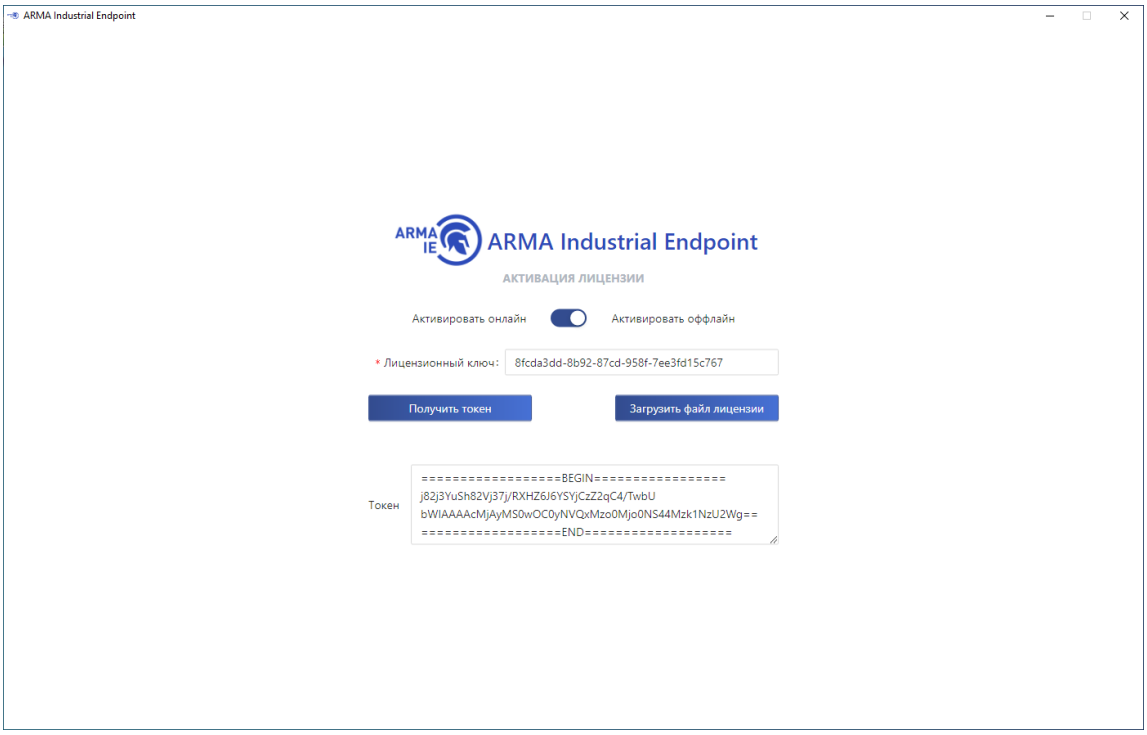

Рисунок 14 – Активация лицензии без доступа в Интернет (1)

Сгенерированный токен необходимо скопировать и направить в техподдержку **ООО «Инфовотч АРМА»**, после чего в ответ будет получен файл лицензии с названием **«license.bin»**, который необходимо загрузить, нажав **кнопку «Загрузить файл лицензии»**, а затем **кнопку «Активировать»** (см. Рисунок 15).

При успешной активации лицензии появится уведомление об этом (см. Рисунок 44).

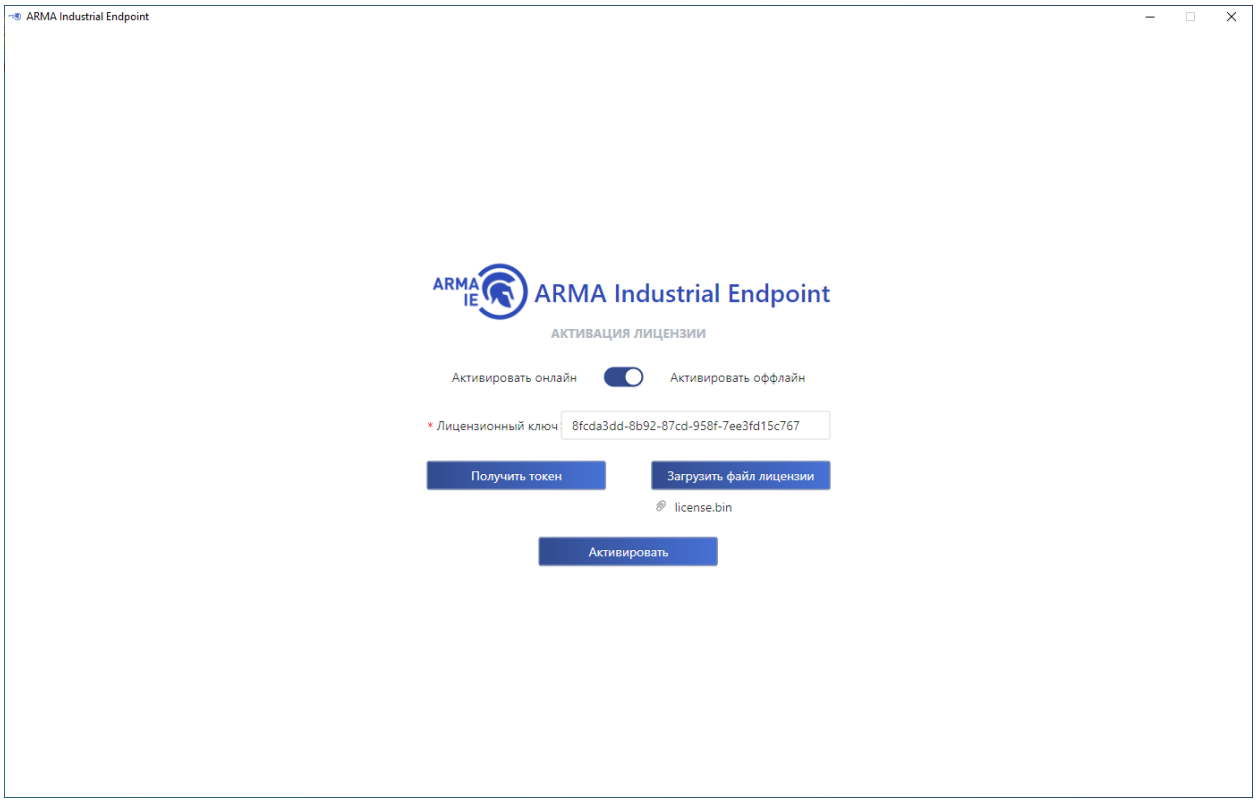

Рисунок 15 – Активация лицензии без доступа в Интернет (2)

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

1. ENTERPRISE базовая. Предоставляет доступ ко всем функциям **ARMA IE**, кроме антивирусной защиты. Срок лицензии – 1 год.

2. ENTERPRISE базовая + антивирусная защита. Предоставляет доступ ко всем функциям **ARMA IE**, включая антивирусную защиту. Срок лицензии – 1 год.

3. TRIAL. Предоставляет доступ ко всем функциям **ARMA IE**, включая антивирусную защиту. Срок лицензии ограничен по времени – 90 дней.

2.4 Настройка связи с ARMA MC

Для связи с **ARMA MC** необходимо создать технического пользователя, от лица которого будет производиться связь с **ARMA IE**.

Для добавления учетной записи пользователя в **ARMA MC** необходимо нажать **кнопку «** **»** в верхнем меню, выбрать пункт **«Просмотреть список пользователей»**, нажать кнопку **«Добавить пользователя»** и добавить пользователя согласно параметрам, представленным ниже (см. Рисунок 16).

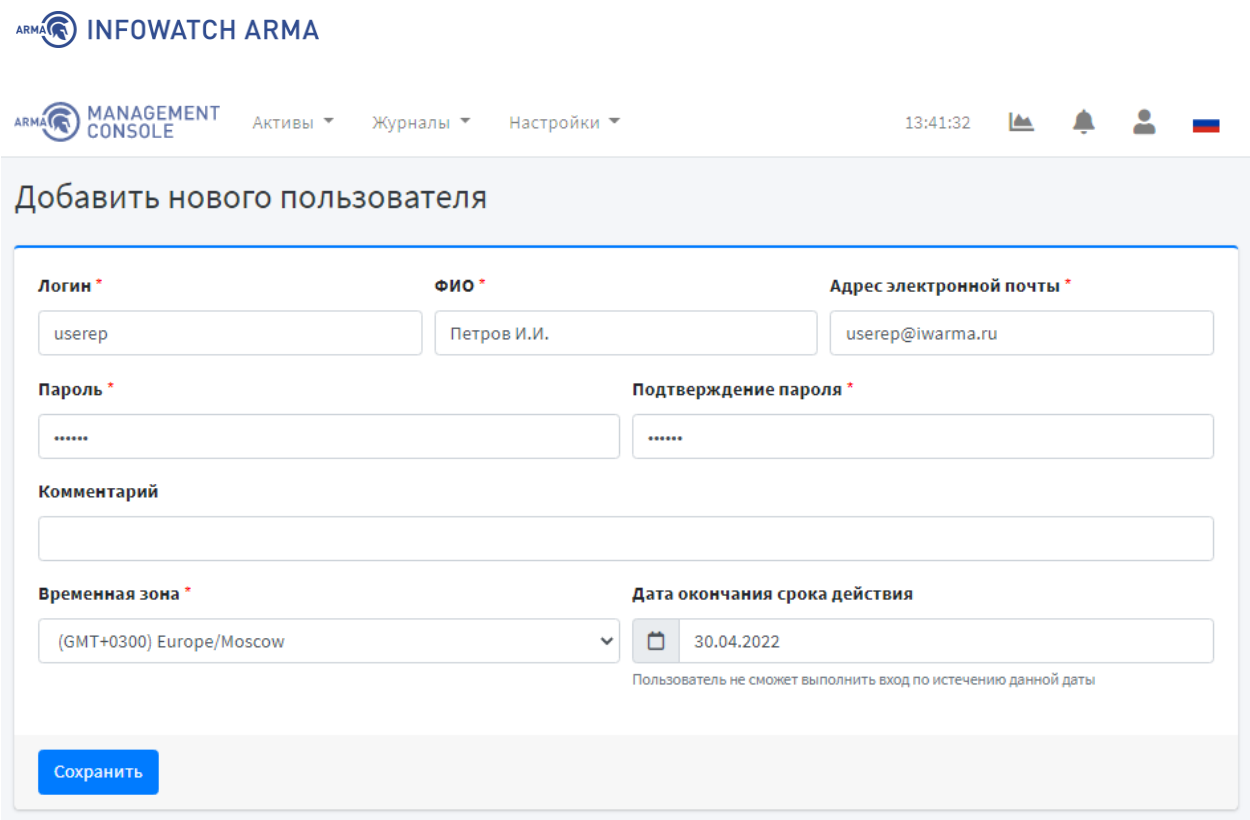

Рисунок 16 – Добавление пользователя в ARMA MC

Для того чтобы пользователю назначить привилегию **«Может скачивать конфигурацию Endpoint»** необходимо создать группу с такой привилегией и добавить туда пользователя.

Для создания группы в **ARMA MC** необходимо нажать **кнопку «** **»** в верхнем меню, выбрать пункт **«Просмотреть список пользователей»** и нажать **кнопку «Управлять группами».** Создать группу **«Endpoint»** с привилегией **«Может скачивать конфигурацию Endpoint»**, нажав **кнопку «** **»** и добавить в неё пользователя «userep» (см. Рисунок 17).

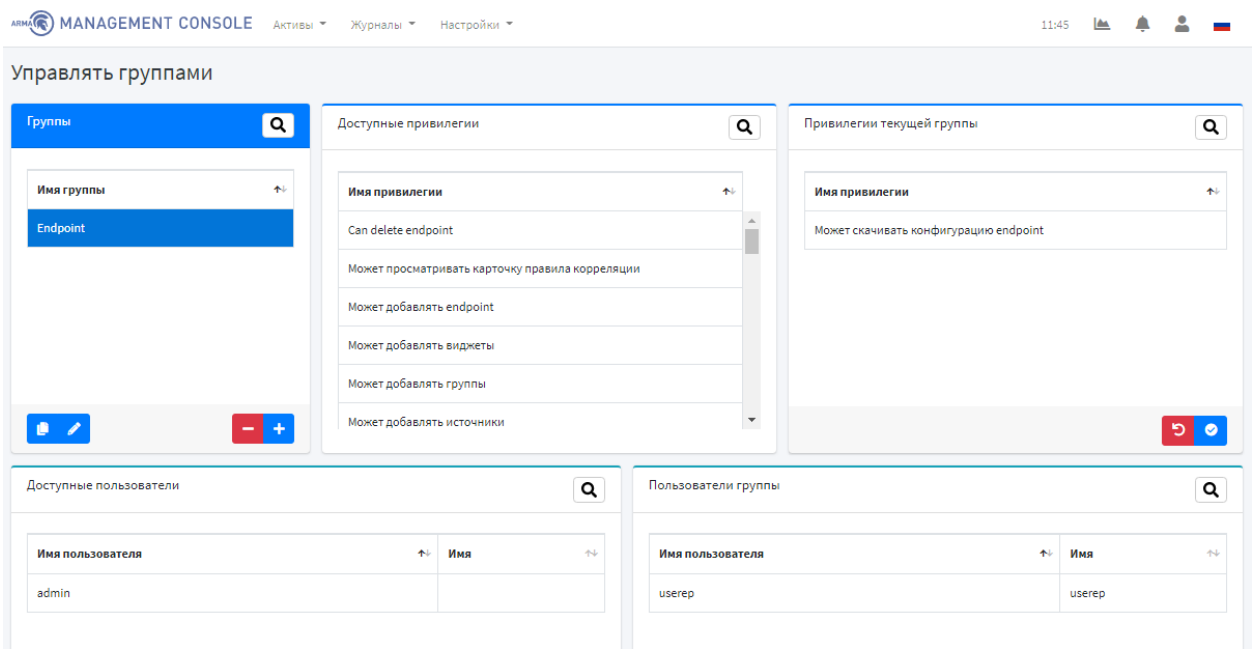

Рисунок 17 – Добавление группы в ARMA MC

2.5 Добавление и настройка Endpoint в ARMA MC

Для настройки Endpoint в **ARMA MC** необходимо перейти на страницу настроек Endpoint (**«Активы» - «Endpoint»**), нажать **кнопку «Добавить»**, настроить конфигурацию Endpoint согласно параметрам, представленным на рисунках (см. Рисунок 18, Рисунок 19,) и нажать **кнопку «Сохранить».**

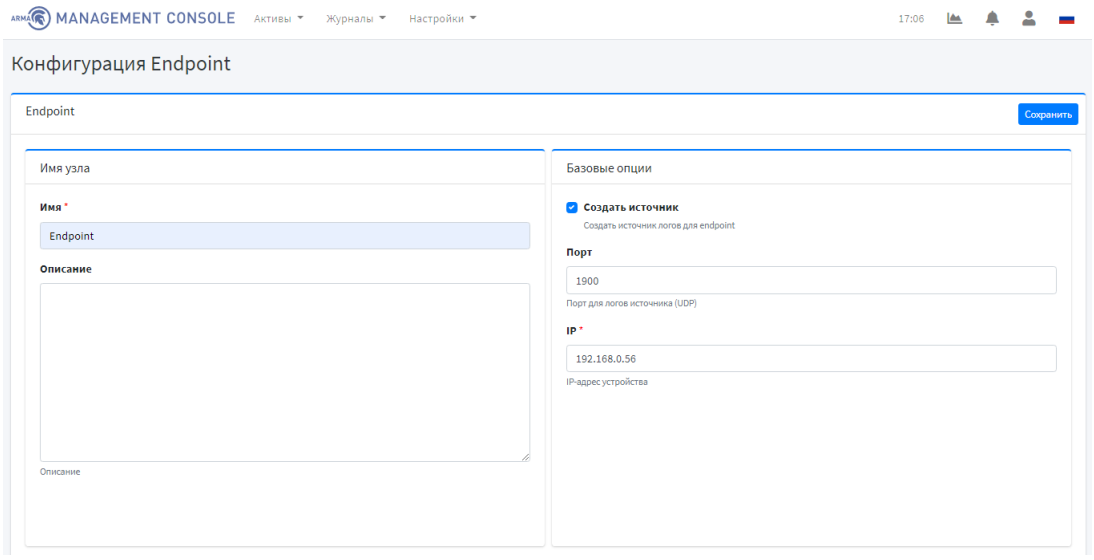

Рисунок 18 – Добавление Endpoint (1)

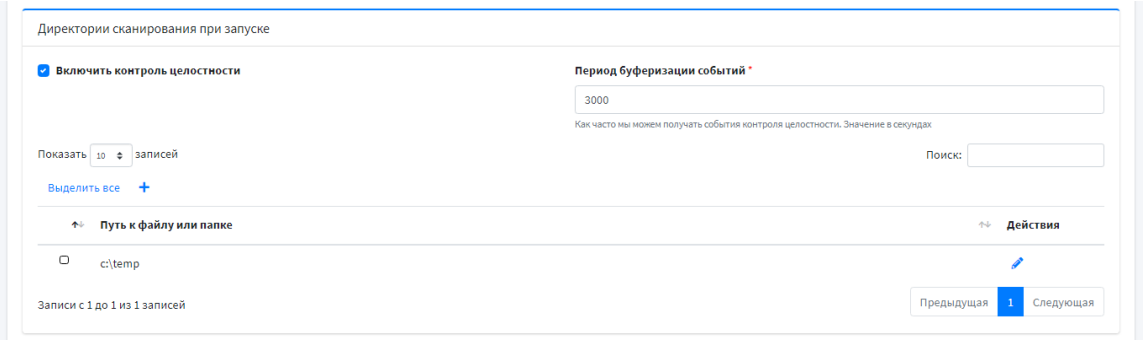

Рисунок 19 – Добавление Endpoint (2)

При добавлении сервиса Endpoint ему автоматически присваивается порядковый номер (**«ID»**), который можно увидеть в общем списке Endpoint (см. Рисунок 20), а так же при нажатии **кнопки «**  **»** напротив нужного Endpoint в адресной строке (см. Рисунок 21).

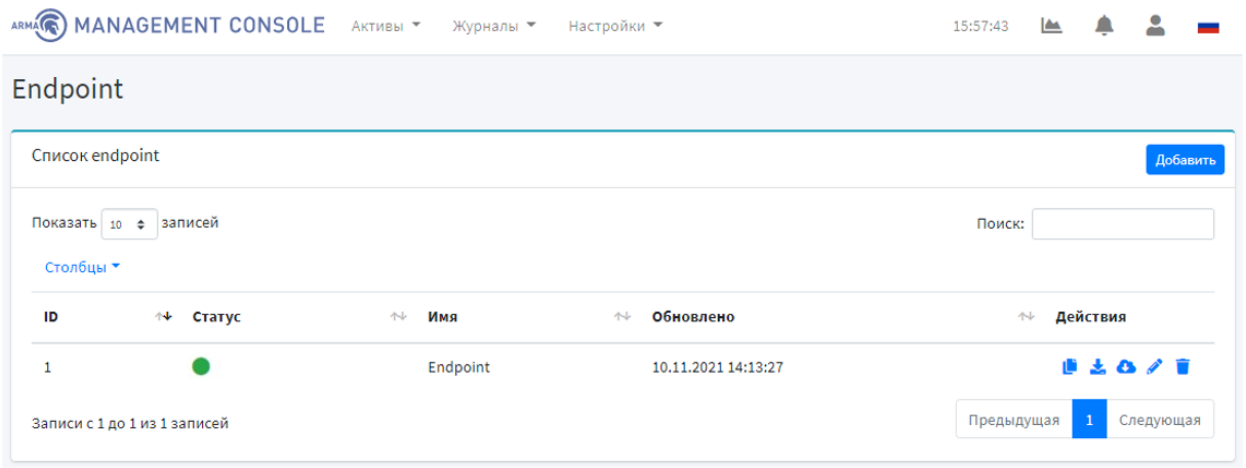

Рисунок 20 – Список Endpoint

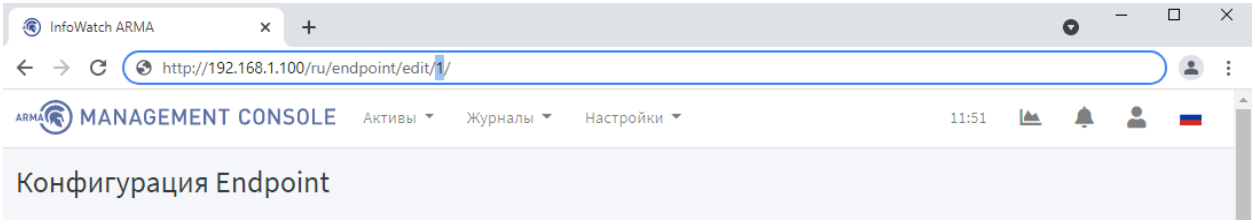

Рисунок 21 – Адрес сервиса Endpoint

Для завершения настройки связи **ARMA IE** с **ARMA MC** необходимо настроить синхронизацию с **ARMA MC** в соответствии с разделом 6 настоящего руководства.

3 УПРАВЛЕНИЕ БЕЛЫМ СПИСКОМ ПРОГРАММ

Управление белым списком программ осуществляется либо через единый центр управления **ARMA MC**, либо в графическом интерфейсе **ARMA IE**.

Для ограничения перечня исполняемых программ в **ARMA MC** в настройках Endpoint (**«Активы» - «Endpoint»**) в блоке **«Белый список приложений»** необходимо добавить путь к файлу или папке, доступ к которым будет разрешен, и нажать **кнопку «Сохранить»** (см. Рисунок 22).

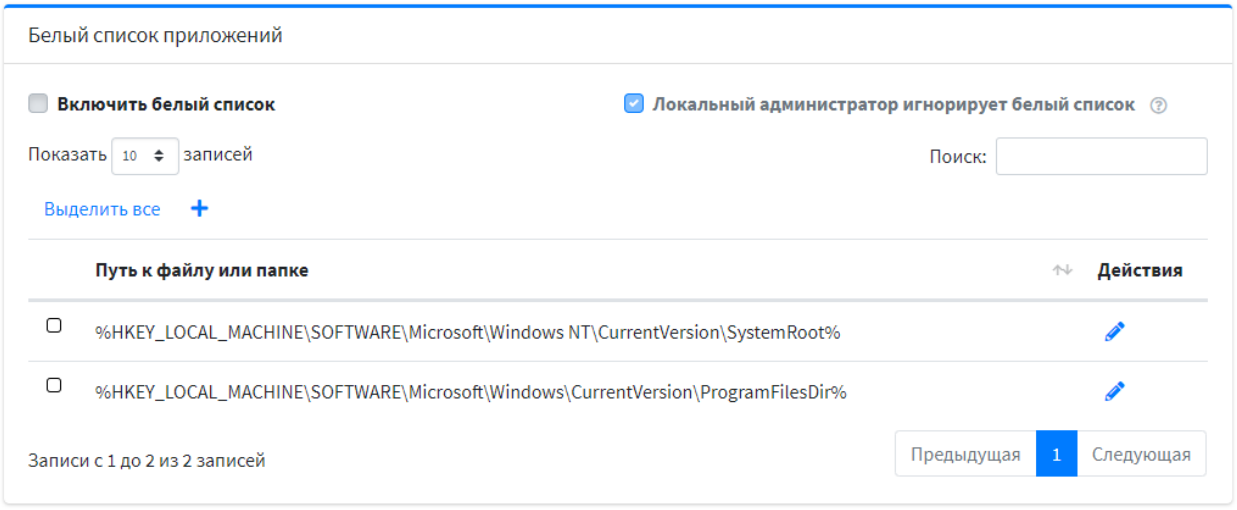

Рисунок 22 – Белый список приложений

Для ограничения перечня исполняемых программ в графическом интерфейсе **ARMA IE** во вкладке **«Белый список»** необходимо сначала включить белый список программ, после чего во всплывающем окне появится предупреждение, которое необходимо подтвердить (см. Рисунок 45).

Затем добавить путь к файлу или папке, доступ к которым будет разрешен, нажав **кнопку «**  **»**, и нажать **кнопку «Сохранить конфигурацию»** (см. Рисунок 23).

!Важно Если папка находится и в белом списке, и в контроле целостности и при этом происходит изменение одного из файлов, то папка исключается из белого списка.

Для предоставления локальному администратору возможности игнорировать правила белого списка установлена галочка в поле **«Разрешить локальному администратору игнорировать правила белого списка»** без возможности ее изменения.

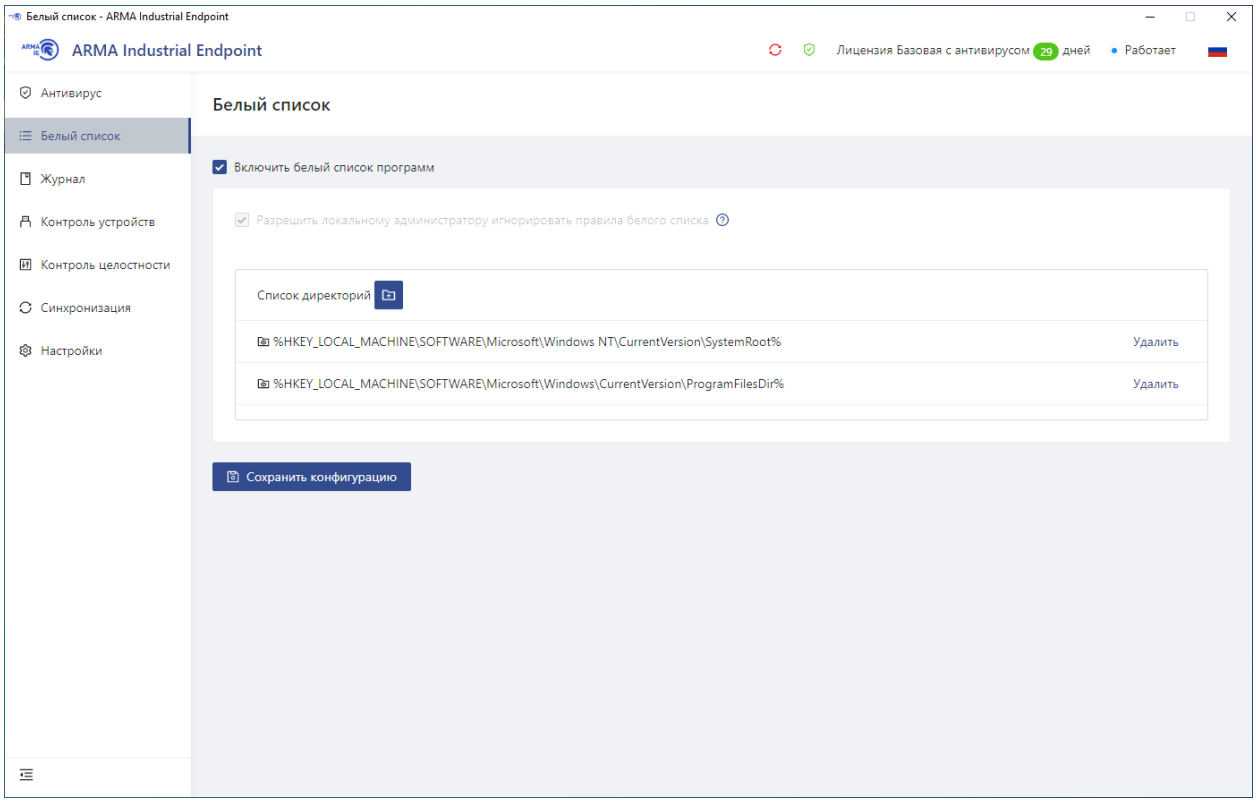

Рисунок 23 – Белый список программ

Для того чтобы проверить, что белый список приложений работает необходимо попробовать установить любую программу не входящую в этот список.

При попытке установки программы не из белого списка появится следующее сообщение (см. Рисунок 24).

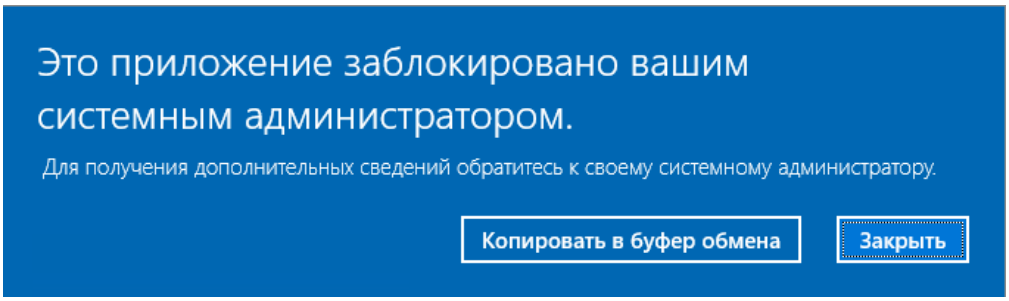

Рисунок 24 – Сообщение об ошибке

4 УПРАВЛЕНИЕ КОНТРОЛЕМ ЦЕЛОСТНОСТИ

Управление контролем целостности программного обеспечения осуществляется либо через единый центр управления **ARMA MC**, либо в графическом интерфейсе **ARMA IE**.

Для добавления директории для сканирования в **ARMA MC** в настройках Endpoint (**«Активы» - «Endpoint»**) в блоке **«Директории для сканирования»** необходимо задать путь к файлу или папке, которые необходимо сканировать (см. Рисунок 19).

Для добавления директории для сканирования в графическом интерфейсе **ARMA IE** во вкладке **«Контроль целостности»** необходимо выбрать контролируемые директории, нажав **кнопку «**  **»**, затем нажать **кнопку «Обновить эталонные образы»** и сохранить изменения, нажав **кнопку «Сохранить конфигурацию»** (см. Рисунок 25).

При первоначальной настройке контроля целостности необходимо выполнить обновление эталонных образов, нажав **кнопку «Обновить эталонные образы».** В дальнейшем, в случае любых изменений в контролируемых директориях необходимо обновлять эталонные образы во избежание блокировки белого списка.

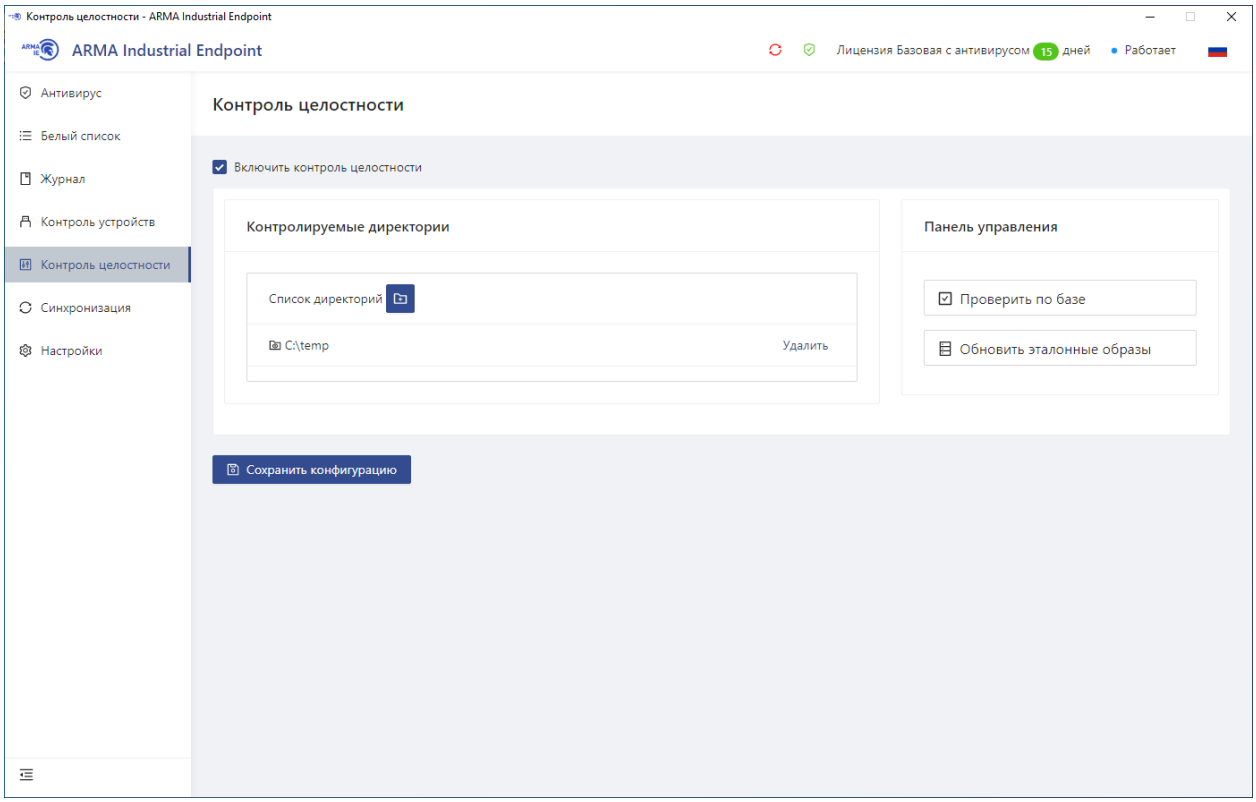

Рисунок 25 – Контроль целостности

!Важно Если на стороне **ARMA MC** в список контроля целостности добавляется или удаляется директория, то на стороне **ARMA IE** запускается механизм обновления эталонных образов и в файле **«endpoint.db»** добавляются или удаляются записи по

этой директории, остальные записи не изменяются. Для обновления эталонных образов по существующим директориям необходимо их удалить и нажать **кнопку «Сохранить конфигурацию»**, а затем заново добавить и нажать **кнопку «Сохранить конфигурацию»**.

Кнопка «Проверить по базе» применяется для сверки контрольных сумм из базы данных с теми, что имеются на диске.

!Важно При запуске процесса обновления эталонных образов и проверки по базе интерфейс **ARMA IE** полностью блокируется вплоть до окончания запущенного процесса. В связи с чем появится блокирующее окно (см. Рисунок 55, Рисунок 56).

При настроенном контроле целостности сообщения об изменениях в контролируемых директориях будут отражены в журнале событий в **ARMA MC** (**«Журналы» - «Журнал событий»**) (см. Рисунок 26) и в файле логов **«endpoint.log»** (см. Рисунок 27), расположенном в папке сервиса «ARMA Industrial Endpoint» (по умолчанию C:\Program Files (x86)\ARMA Industrial Endpoint).

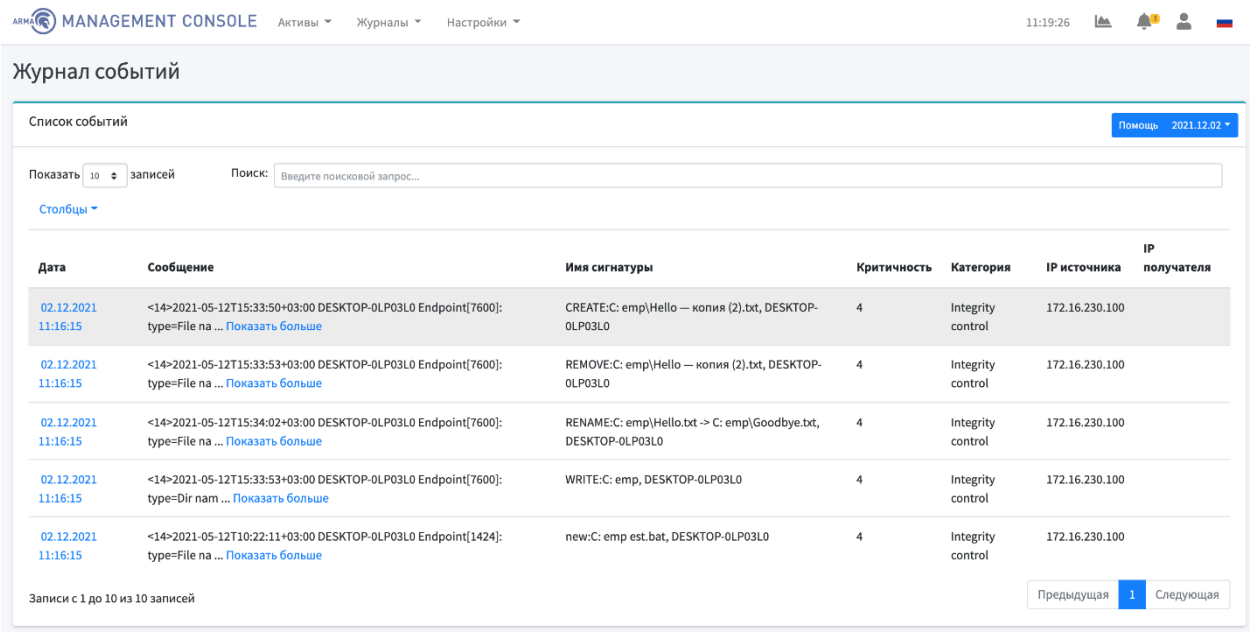

Рисунок 26 – Журнал событий ARMA MC

```
time="2020-12-08T13:13:22+03:00" level=info msg="Got event: FILE \"test.txt\" WRITE [c:\\temp\\1\\test.txt]" duration=3s part=icontrol
time="2020-12-08T13:13:28+03:00" level=info msg="Got event: DIRECTORY \"1\" WRITE [c:\\temp\\1]" duration=3s part=icontrol
time="2020-12-08T13:13:28+03:00" level=info msg="Got event: FILE \"Новый текстовый документ (2).txt\" CREATE [c:\\temp\\1\\Новый текстовый документ (2).txt]" duration=
time="2020-12-08T13:13:46+03:00" level=info msg="Got event: DIRECTORY \"1\" WRITE [c:\\temp\\1]" duration=3s part=icontrol
time="2020-12-08T13:13:46+03:00" level=info msg="Got event: FILE \"Новый текстовый документ (2).txt\" RENAME [c:\\temp\\1\\_Новый текстовый документ_.txt]" duration=3s
```

Рисунок 27 – Журнал логов «endpoint.log»

5 УПРАВЛЕНИЕ КОНТРОЛЕМ УСТРОЙСТВ

Управление контролем устройств осуществляется либо через единый центр управления **ARMA MC**, либо в графическом интерфейсе **ARMA IE**.

ARMA IE позволяет ограничивать следующие типы съемных носителей: **USB** и **CD/DVD диски.**

Для ограничения подключаемых съемных носителей в **ARMA MC** в настройках Endpoint (**«Активы» - «Endpoint»**) в блоке **«Настройки управления устройствами»** необходимо включить контроль устройств, затем установить ползунок напротив того типа съемных носителей, доступ к которым должен быть ограничен, и нажать **кнопку «Сохранить»** (см. Рисунок 28).

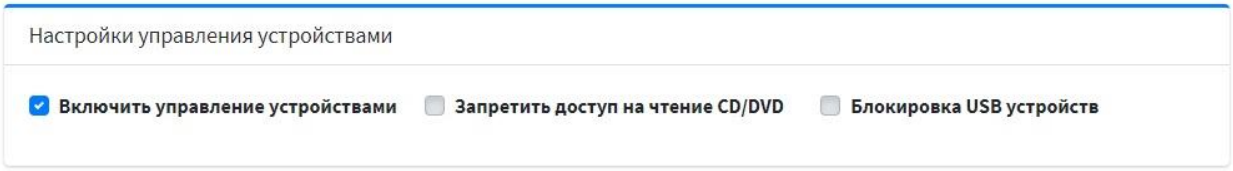

Рисунок 28 – Контроль устройствами USB

Для ограничения подключаемых съемных носителей в графическом интерфейсе **ARMA IE** во вкладке **«Контроль устройств»** необходимо включить управление устройствами, установив галочку в соответствующем поле и нажать **кнопку «Сохранить конфигурацию»** (см. Рисунок 29).

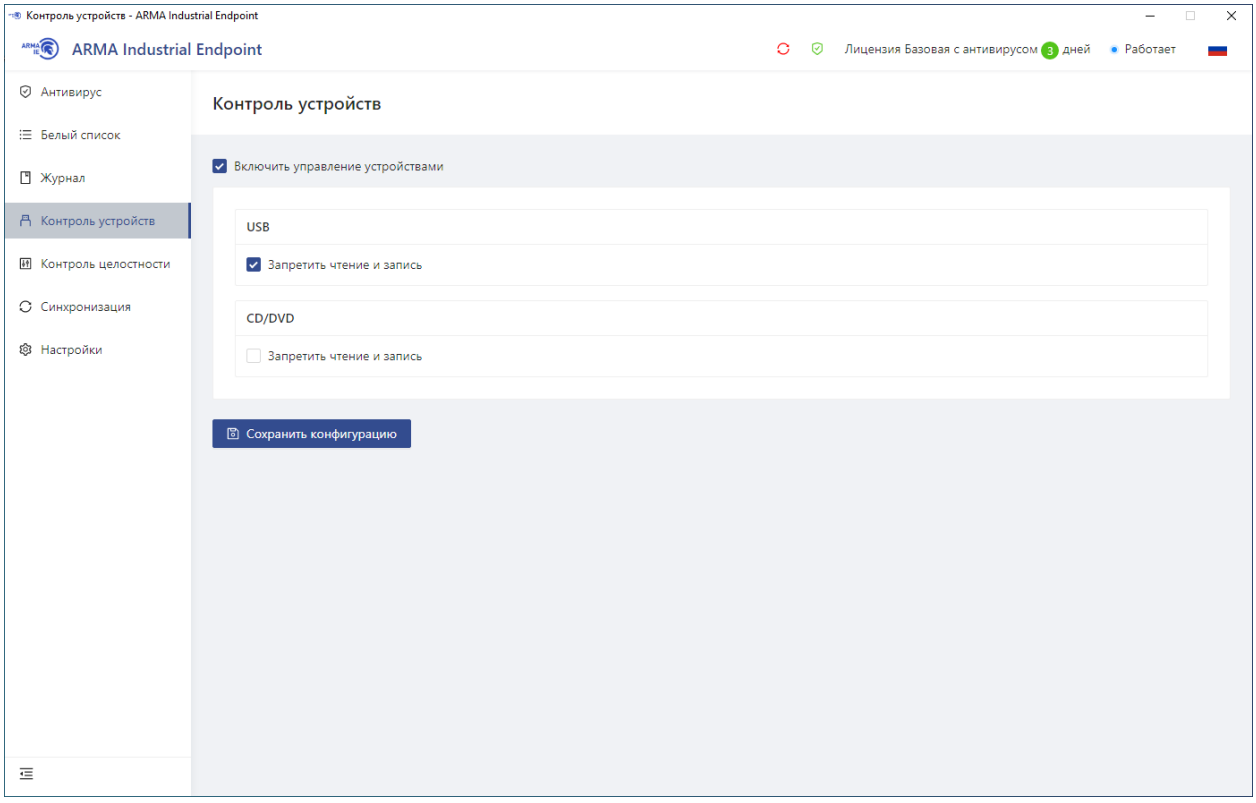

Рисунок 29 – Контроль устройств

Установленная галочка в поле **«Запретить чтение и запись»** автоматически блокирует USB/CD/DVD.

!Важно Устройства Remote USB Devices блокируются. USB-устройства без серийного номера блокироваться не будут.

Для того чтобы проверить, что ограничение записи, допустим на USB, работает, необходимо либо создать новый текстовый файл, либо скопировать любой файл на USB. При попытке это сделать появится всплывающее окно (см. Рисунок 30).

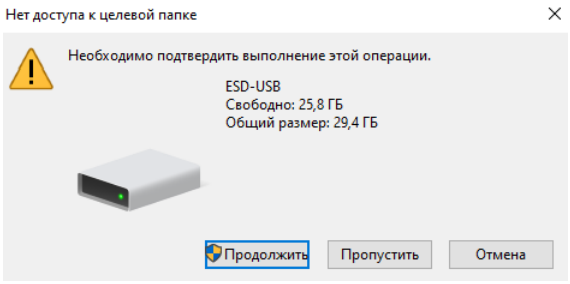

Рисунок 30 – Всплывающее окно «Нет доступа к целевой папке»

При проверке ограничения чтения на USB появится следующее всплывающее окно (см. Рисунок 31).

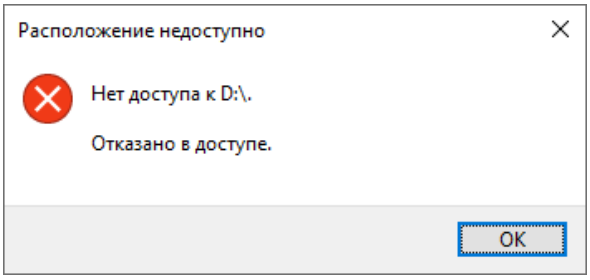

Рисунок 31 – Всплывающее окно «Расположение недоступно»

6 НАСТРОЙКА СИНХРОНИЗАЦИИ С ARMA MC

Для настройки синхронизации **ARMA IE** с **ARMA MC** необходимо в графическом интерфейсе **ARMA IE** перейти во вкладку **«Синхронизация»**, включить синхронизацию, установив галочку в соответствующем поле, ввести аутентификационные данные технического пользователя (п. 2.4 настоящего руководства), адрес **ARMA MC** и нажать **кнопку «Сохранить конфигурацию»** (см. Рисунок 32).

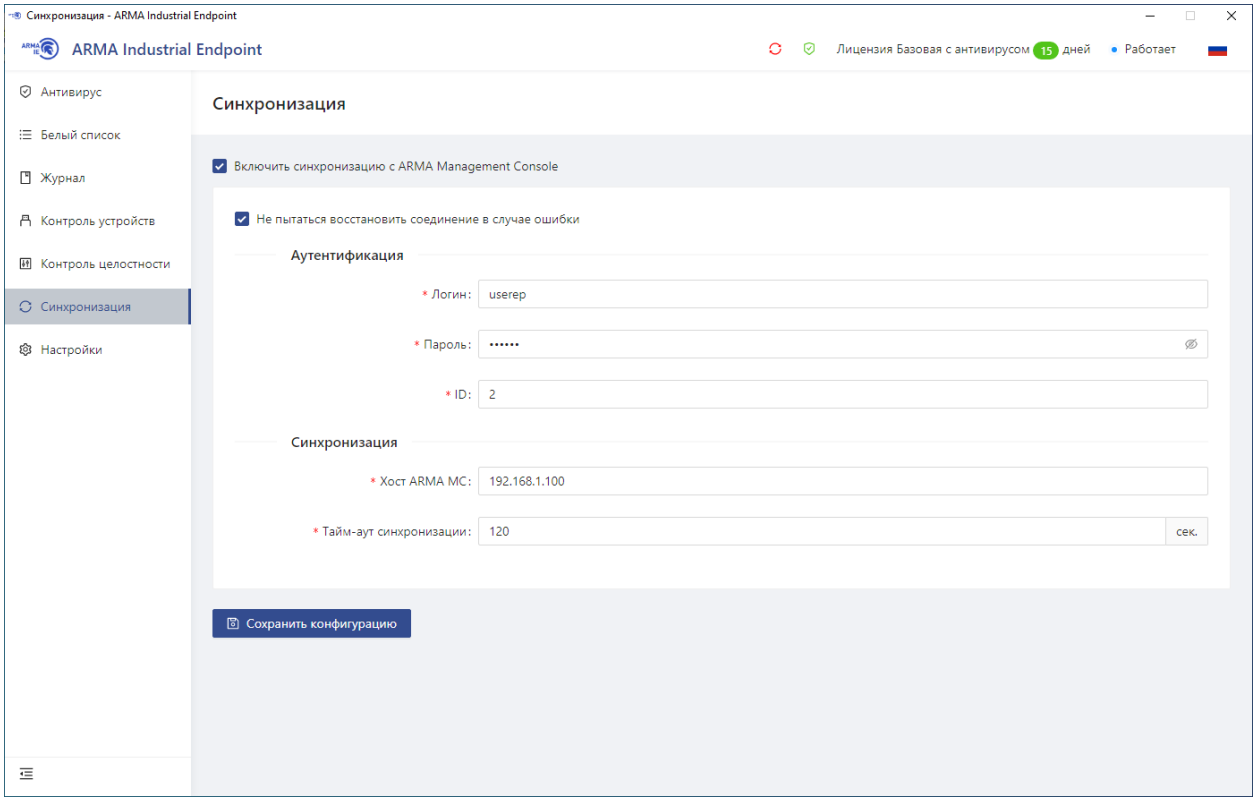

Рисунок 32 – Синхронизация

!Важно Настройки **ARMA IE** при первой синхронизации не переносятся в **ARMA MC**. Для переноса настроек необходимо после добавления **ARMA IE** в **ARMA MC** и включения синхронизации на **ARMA IE** на странице настроек Endpoint в **ARMA MC** (**«Активы» - «Endpoint»**) нажать **кнопку «** **»** для обновления конфигурации **ARMA IE** (см. раздел 2.5).

7 УПРАВЛЕНИЕ АНТИВИРУСОМ

Управление антивирусом осуществляется либо через единый центр управления **ARMA MC**, либо в графическом интерфейсе **ARMA IE**.

Для настройки антивируса в **ARMA MC** в настройках Endpoint (**«Активы» - «Endpoint»**) в блоке **«Настройки антивируса»** необходимо включить антивирус и нажать **кнопку «Сохранить»** (см. Рисунок 33).

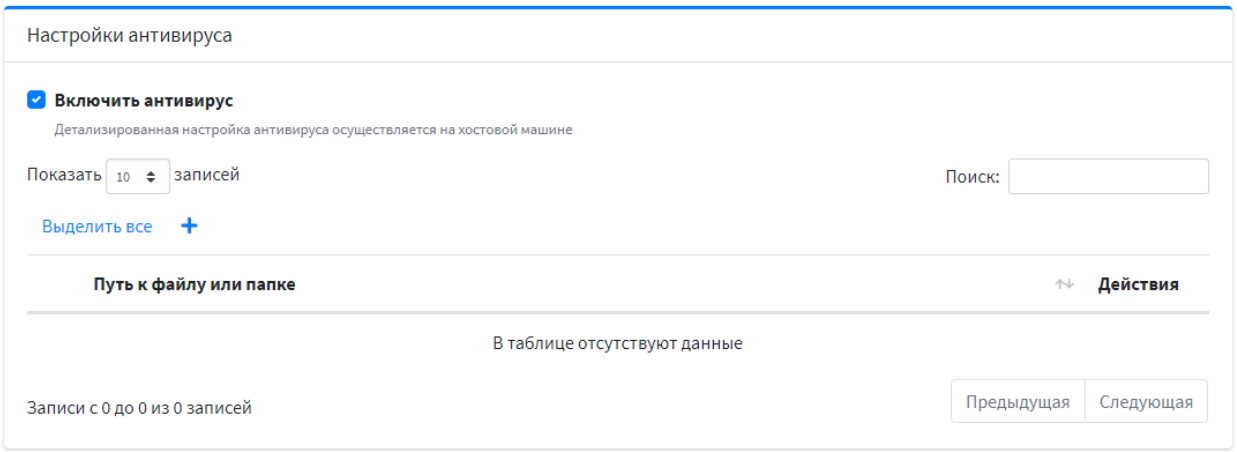

Рисунок 33 – Настройки антивируса в ARMA MC

Для включения антивирусной защиты в графическом интерфейсе **ARMA IE** во вкладке **«Антивирус»** необходимо включить антивирус, установив галочку в соответствующем поле и нажать **кнопку «Сохранить конфигурацию»** (см. Рисунок 34).

!Важно Перед началом работы с антивирусом появится уведомление о необходимости сохранения конфигурации (см. Рисунок 54), после чего произойдет автоматическое сохранение конфигурации.

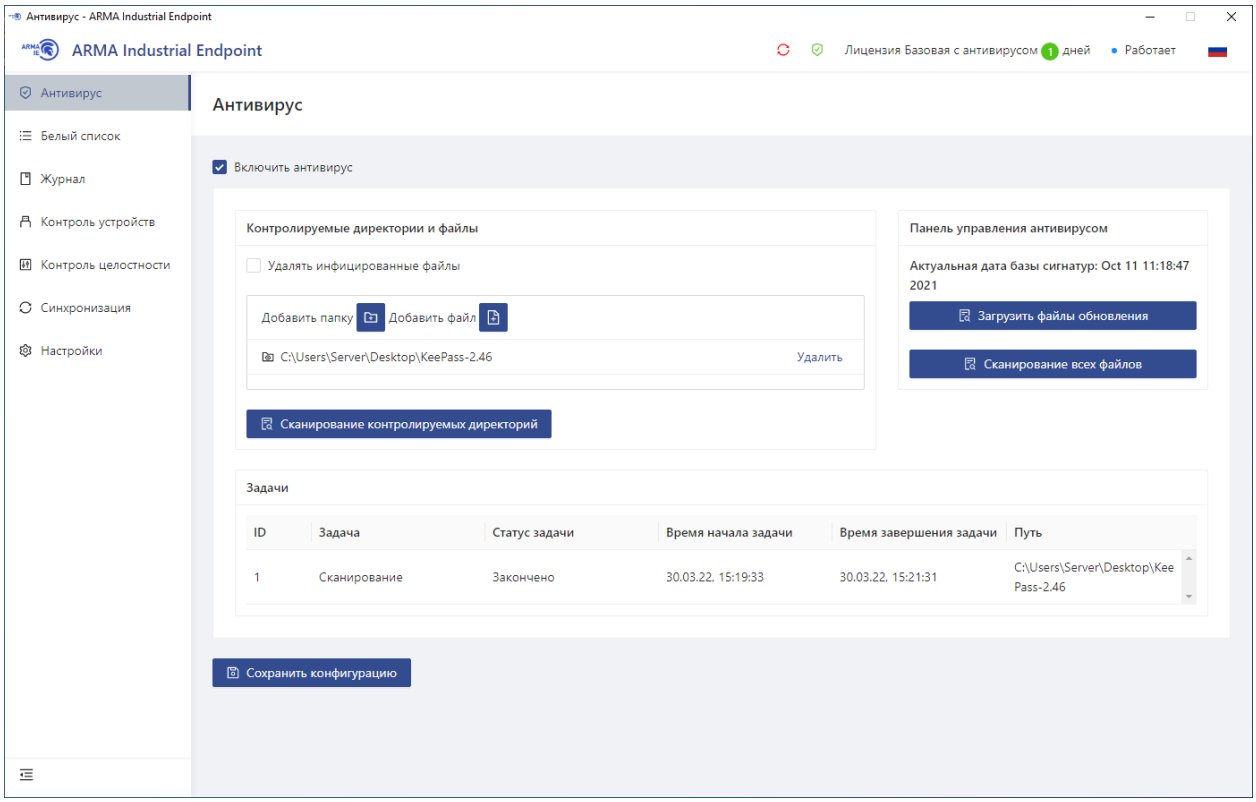

Рисунок 34 – Антивирус

Для сканирования определенных директорий и файлов необходимо их добавить, нажав на соответствующие кнопки – **«Добавить папку»** и **«Добавить файл»**, а затем нажать **кнопку «Сохранить конфигурацию»**.

!Важно Антивирус **ARMA IE** не работает с файлами на русском языке.

Кнопка «Сканирование контролируемых директорий» запускает сканирование на наличие вредоносных компьютерных программ в контролируемых директориях.

Кнопка «Сканирование всех файлов» запускает полное сканирование рабочей машины на наличие вредоносных компьютерных программ в режиме реального времени.

!Важно Сканирование заархивированных файлов возможно только при наличии в системе архиватора.

Запущенное сканирование можно остановить в любое время с помощью нажатия **кнопки «Остановить все задачи сканирования»** или **кнопки «** **»** (см. Рисунок 35).

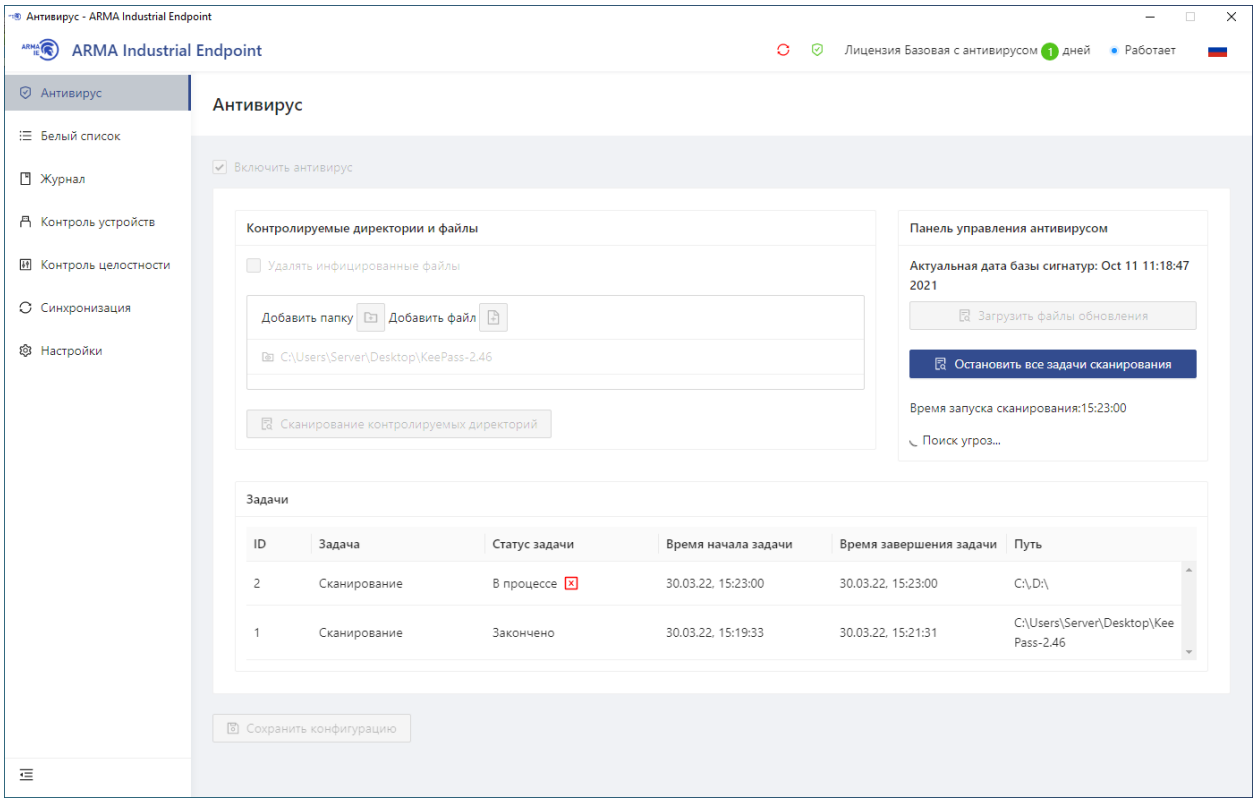

Рисунок 35 – Пример запуска сканирования

При создании, редактировании или перемещении файлов в контролируемых директориях происходит сканирование.

При подключении съемных носителей **ARMA IE** автоматически просканирует на наличие вредоносных компьютерных программ.

!Важно Подключенные съемные носители автоматически добавляются в список контролируемых директорий, после отключения – удаляются.

При обнаружении вредоносных компьютерных программ **ARMA IE** отобразит их в виде списка в блоке **«Обнаруженные угрозы»**, сформированного по дате, времени, объекте, критичности угрозы, действию и пути расположения файла (см. Рисунок 36).

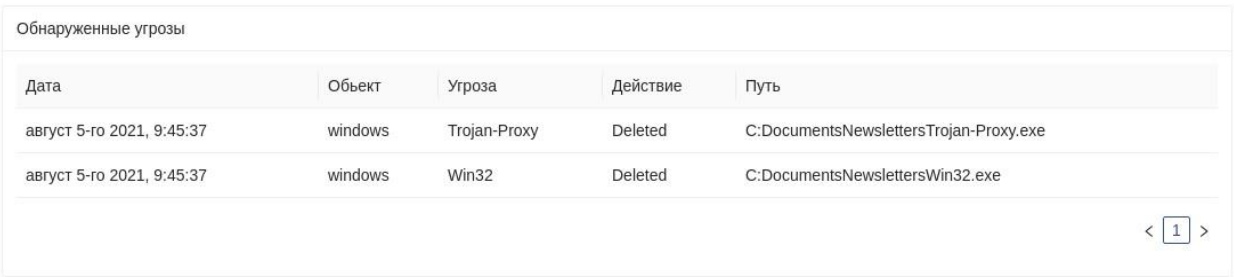

Рисунок 36 – Обнаруженные угрозы

Для автоматического удаления зараженных файлов необходимо установить галочку в соответствующем поле **«Удалять инфицированные файлы»**.

!Важно При наличии одного инфицированного файла в архиве удаляется весь архив целиком.

Обновление базы антивирусной защиты осуществляется нажатием **кнопки «Загрузить файлы обновления»**.

При обновлении базы сигнатур антивируса используется механизм ClamAV, в рамках которого осуществляется проверка по всем файлам обновления, в каждом из которых могут быть старые и новые версии. При успешном обновлении хотя бы одного файла поменяется дата обновления сигнатур.

Все события от антивируса фиксируются в **ARMA MC** в журнале событий (**«Журналы»** - **«События»**) (см. Рисунок 37).

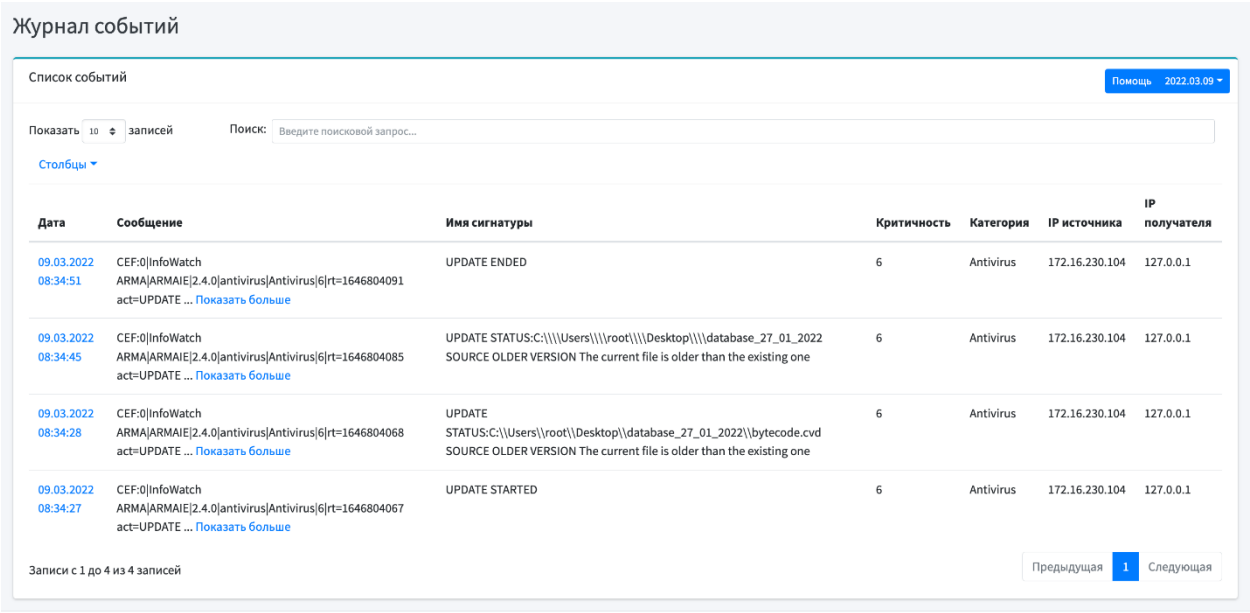

Рисунок 37 – Пример событий от антивируса в ARMA MC

8 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

8.1 Информация о состоянии и лицензии Endpoint

Информация о состоянии синхронизации с **ARMA MC**, о текущем состоянии Endpoint и действующей лицензии отображается в верхнем правом углу графического интерфейса.

Также есть возможность сменить основной язык графического интерфейса (см. Рисунок 38).

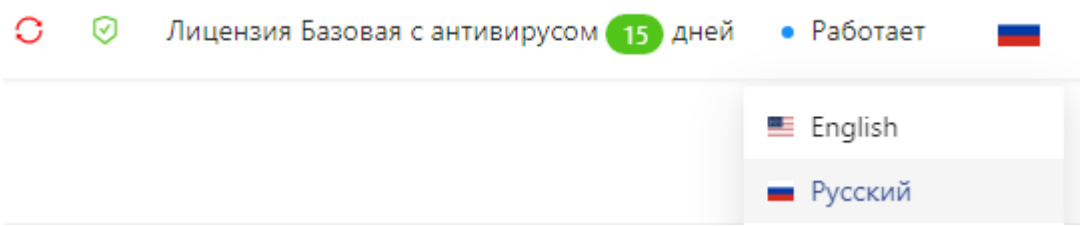

Рисунок 38 – Состояние и лицензия Endpoint

!Важно Если срок лицензии истек, то в веб-интерфейсе блокируются кнопки управления, форма данных подключения, кнопки загрузки и сохранения конфигурации, а так же блокируется контроль устройств и белый список.

8.2 Настройка управления ARMA IE

Во вкладке **«Настройки»** в блоке **«Панель управления»** предоставляется возможность управлять **ARMA IE** (см. Рисунок 39).

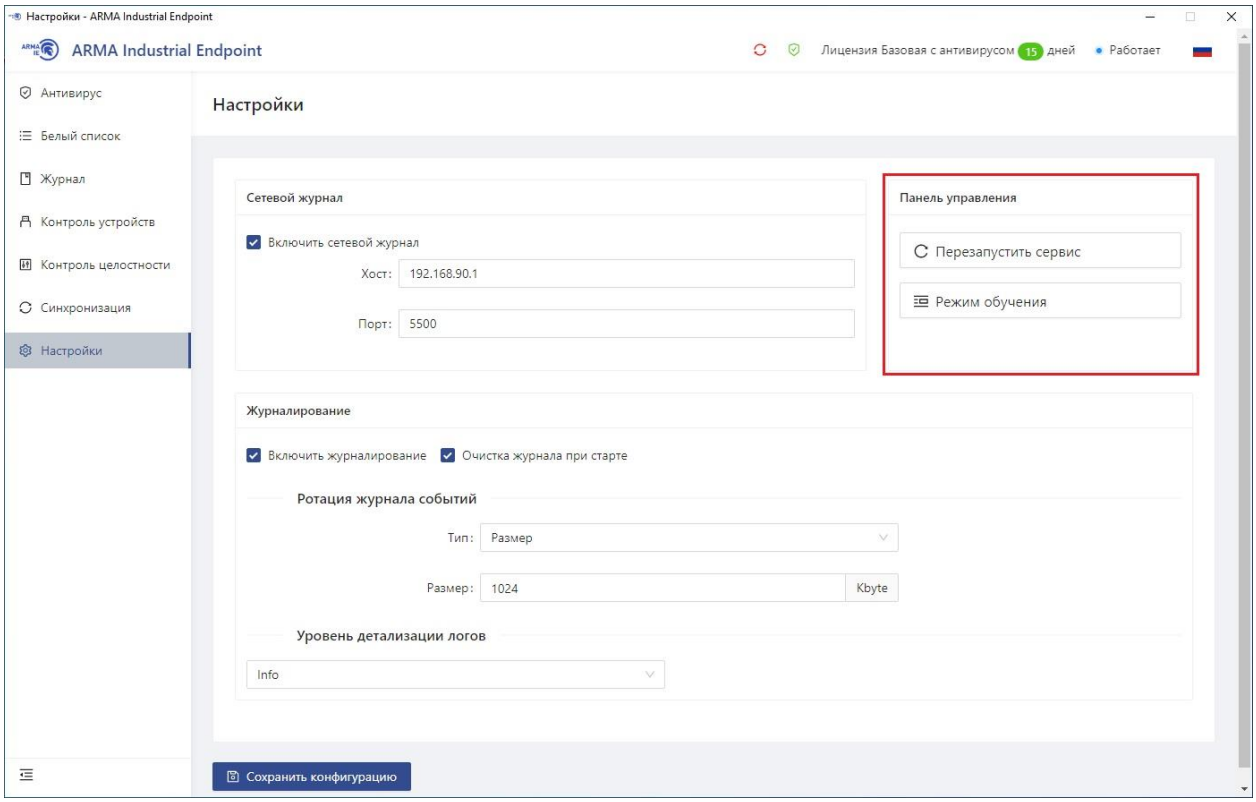

Рисунок 39 – Панель управления ARMA IE

Кнопка «Перезапустить сервис» позволяет перезапустить сервис **ARMA IE**.

8.2.1 Режим обучения

Режим обучения запускает сканирование запущенных программ и записывает их в белый список.

Для проверки режима обучения необходимо нажать **кнопку «Режим обучения»**, затем перейти на вкладку **«Белый список»** и убедиться в том, что контролируемые им папки появились в списке.

8.3 Настройка сетевого журнала

Во вкладке **«Настройки»** в блоке **«Сетевой журнал»** предоставляется возможность настроить получение событий от **ARMA IE**.

Для того чтобы настроить экспорт событий от **ARMA IE** необходимо ввести хост и порт устройства, на которое будут приходить события, а затем нажать **кнопку «Сохранить конфигурацию»** (см. Рисунок 40).

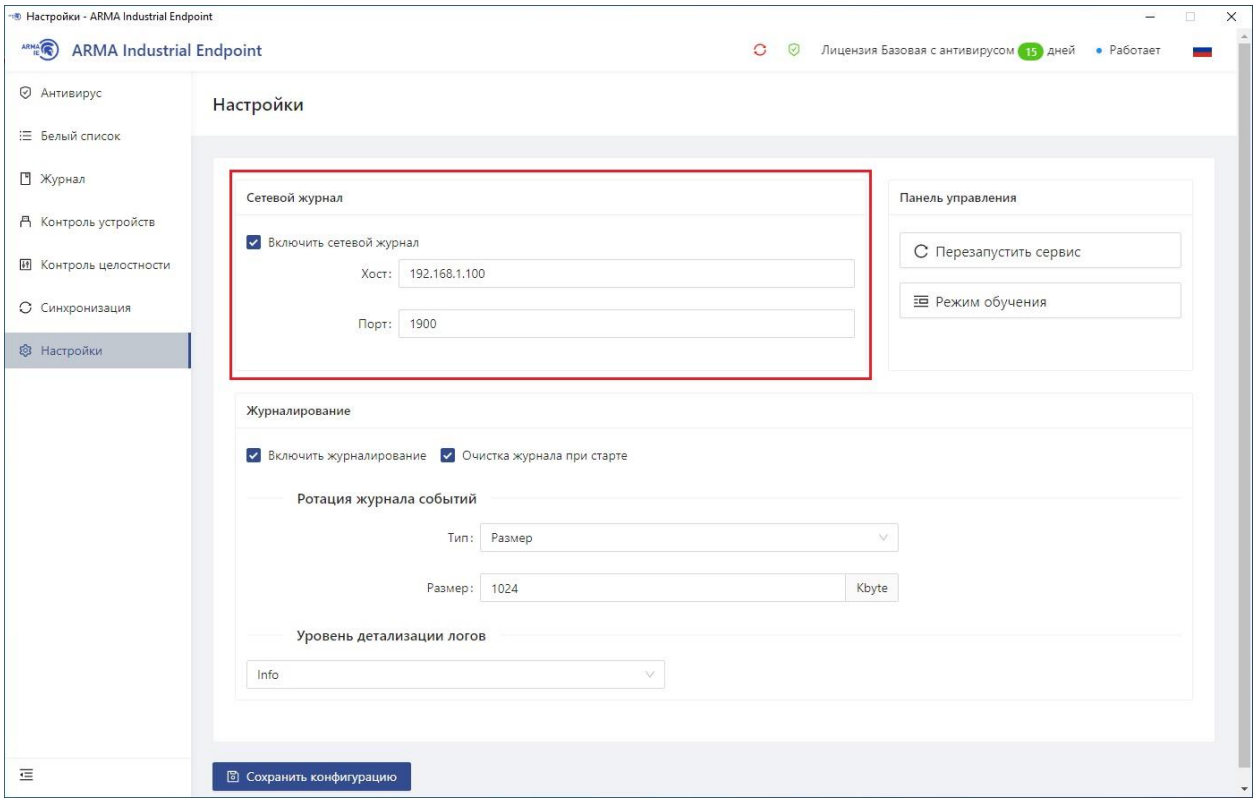

Рисунок 40 – Сетевой журнал

8.4 Настройка журналирования

Во вкладке **«Настройки»** в блоке **«Журналирование»** предоставляется возможность (см. Рисунок 41):

- включать журналирование событий;
- настраивать уровень детализации событий;
- настраивать ротацию журнала событий;
- включать очистку журнала при запуске.

!Важно При выключенном журналировании перестают записываться события в журнал **ARMA IE** (вкладка **«Журнал»**) и в файл **«endpoint.log»**.

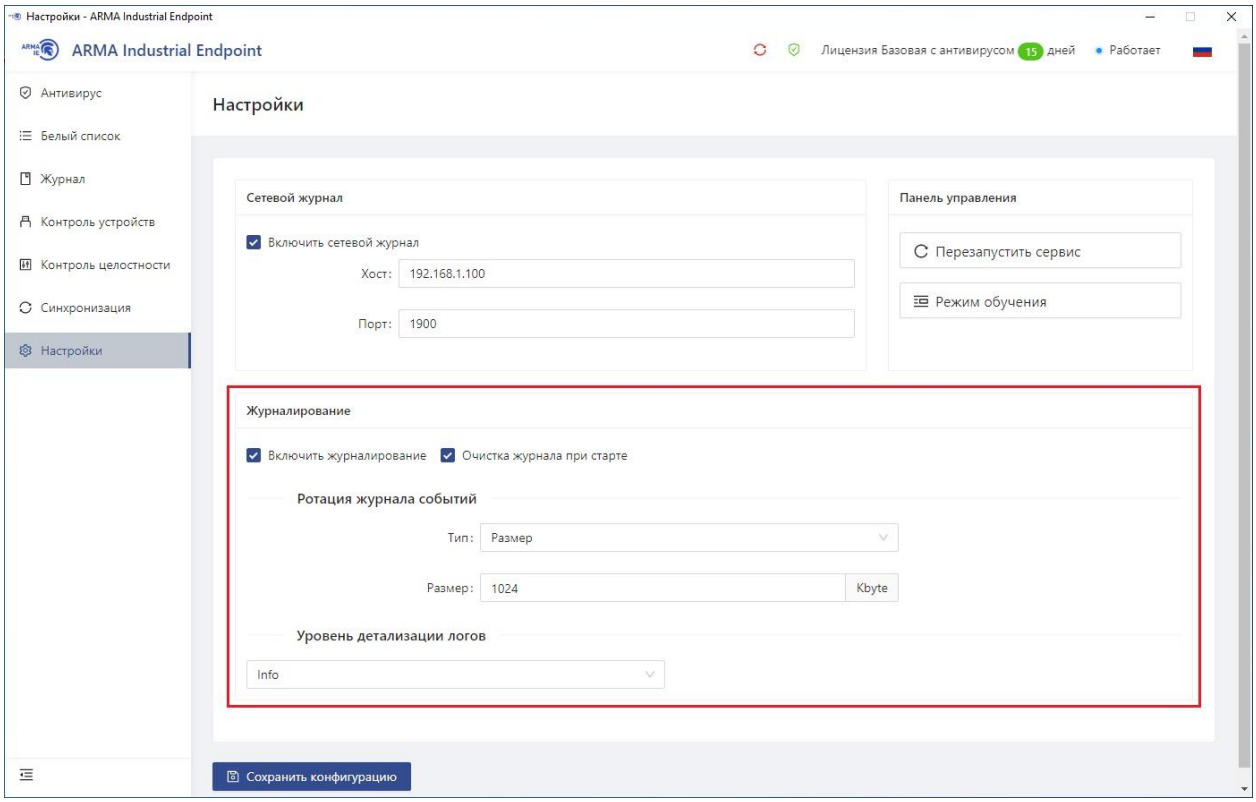

Рисунок 41 – Журналирование

Ротация журнала событий доступна по двум типам:

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

При выборе периода **«День»** типа ротации **«Время»** ротация будет запущена в определенное время.

!Важно Если время будет установлено в прошлом (допустим, текущее время 10 утра, а выбрано 8 утра) и ротации за текущий день еще не было, то ротация будет запущена. Если ротация была установлена и уже запущена, то при изменении времени ротация будет запущена относительно завтрашнего дня (допустим, ротация была запущена в 11 утра, а потом изменили время на 13 дня).

При выборе периода **«Неделя»** типа ротации **«Время»** ротация будет запущена в понедельник.

При выборе периода **«Месяц»** типа ротации **«Время»** ротация будет запущена в первый день месяца.

!Важно При настройке ротации журнала событий по размеру рекомендуется задавать значение не менее 5000-10000 Кб, так как размер определяется не размером самого журнала, а размером файла **«main.db»**.

Детализация событий доступна в следующих режимах журналирования:

- **«Info»** – записывает события информативного характера;

- **«Trace»** – записывает каждое действие в системе;
- **«Debug»** – записывает события, которые считаются полезными во время отладки ПО;
- **«Warning»** – записывает непредвиденные события, которые в дальнейшем могут нарушить работу одного из процессов системы;
- **«Error»** – записывает прикладные ошибки в работе функционала;
- **«Fatal»** – записывает события, которые сообщают о неработоспособности одной или нескольких ключевых бизнес-функций системы;
- **«Panic»** – записывает события об ошибке, которая прерывает все сессии.

Настройка журналирования в **ARMA MC** осуществляется в настройках Endpoint (**«Активы» - «Endpoint»**) в блоке **«Настройки ротации событий»** (см. Рисунок 42).

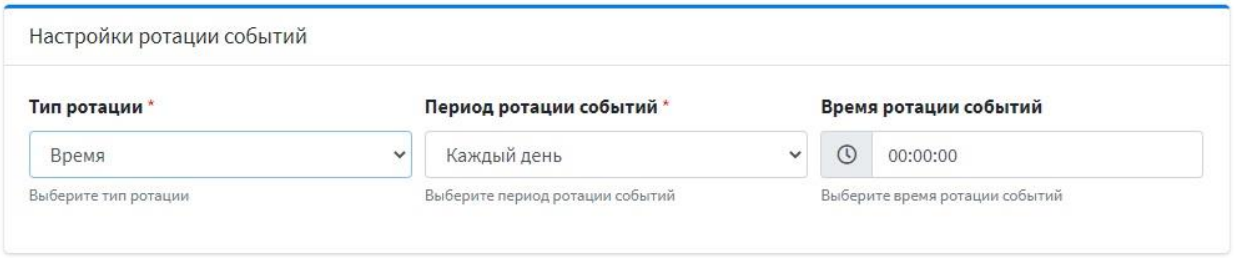

Рисунок 42 – Настройки ротации событий в ARMA MC

9 ПРОСМОТР ЖУРНАЛА СОБЫТИЙ

Во вкладке **«Журнал»** отображаются все события безопасности, зафиксированные **ARMA IE** (см. Рисунок 43).

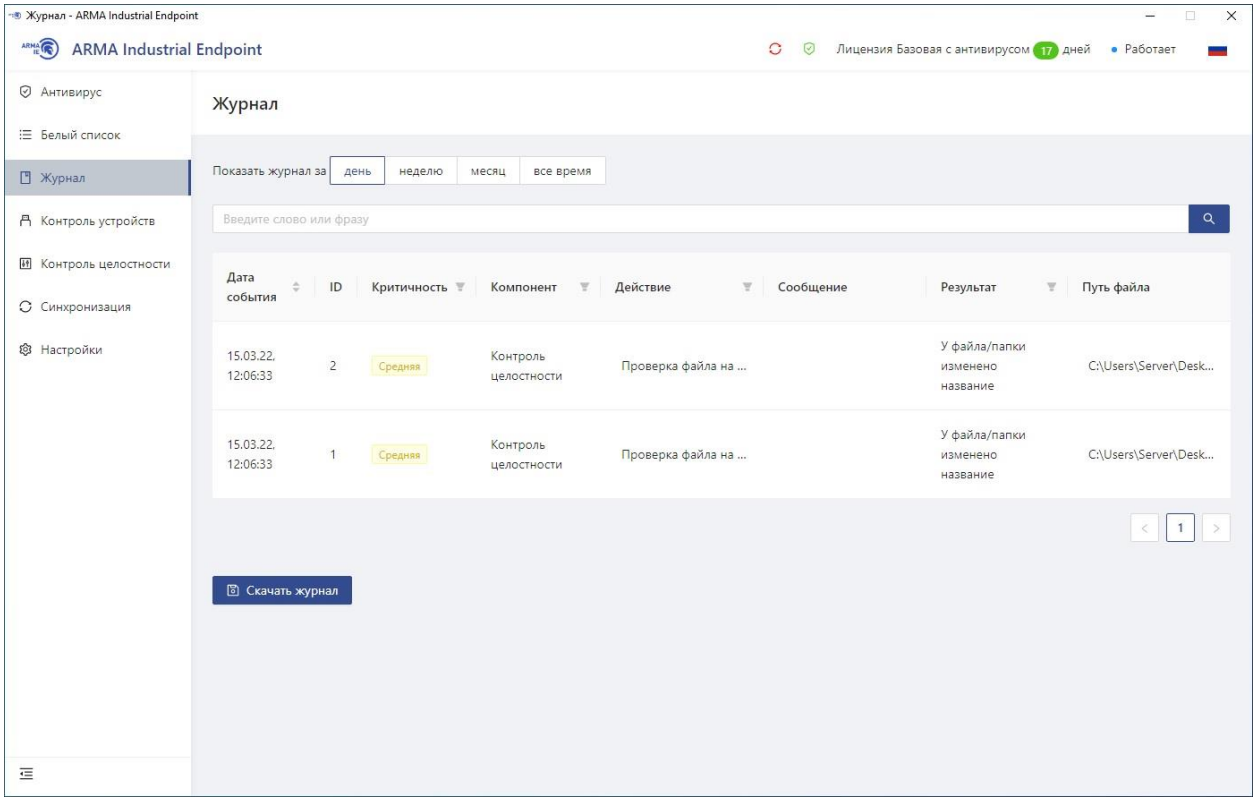

Рисунок 43 – Журнал

События безопасности сортируются по следующим уровням критичности:

- «Высокая»;
- «Средняя»;
- «Низкая».

Столбцы журнала **«Дата события»**, **«Критичность»**, **«Компонент»**, **«Действие»** и **«Результат»** можно настраивать, путем нажатия **кнопки** «».

В таблице (см. Таблица 4) представлены события, отображаемые в журнале **ARMA IE**.

Таблица 4
События безопасности, отображаемые в журнале ARMA IE

Компонент ARMA IE	Действие/результат
Белый список	
	Файл заблокирован белым списком

Компонент ARMA IE	Действие/результат
Контроль целостности	
	Файл/папка создана
	Файл/папка изменена
	Файл/папка удалена
	У файла/папки изменено название
Антивирус	
	Начало антивирусной проверки
	Окончание антивирусной проверки
	Остановка проверки по требованию пользователя
	Обнаружен вирус
	Ошибка антивирусной проверки
	Начало обновления БД
	Окончание обновления БД
	Ошибка обновления БД
Изменение настроек	
	Файл «config.json» был изменен **ARMA MC**
	Файл «config.json» был изменен в интерфейсе **ARMA IE**

Пользователю предоставляется возможность экспортировать журнал событий, нажав **кнопку «Скачать журнал»**. Экспорт журнала осуществляется в формате **«.csv»** в следующем виде:

- «Industrial Endpoint journal at 15.03.22, 12.08.59».

10 ПРОСМОТР ЖУРНАЛА СОБЫТИЙ В ФАЙЛЕ ENDPOINT.LOG

Все события, регистрируемые программой, сохраняются в файле **«endpoint.log»** и отправляются на **ARMA MC**.

В таблице (см. Таблица 5) представлены некоторые события из файла **«endpoint.log»**. Для экономии места в таблице дата и время для записей в журнале не указаны.

Таблица 5
События, регистрируемые программой

№ п.п.	Запись в журнале	Описание события
1	Runing in service mode	Сервис запущен
2	Control server started on port 4509	Сервер управления запущен на порту 4509
3	Initializing check from db	Инициализация проверки из БД
4	Got event: FILE \"test.txt\" WRITE [c:\\temp\\1\\test.txt]	Изменение файла test.txt
5	Got event: FILE \"Новый текстовый документ (2).txt\" RENAME [c:\\temp\\1\\Приказ.txt]	Добавлен новый текстовый документ с названием Приказ.txt
6	Got event: FILE \"test_1.txt\" REMOVE [c:\\temp\\1\\test_1.txt]	Удаление файла test_1.txt
7	Syslog init finish. Connected to 192.168.0.68:1800	Завершение инициализации системного журнала. Подключено к 192.168.0.68:1800
8	Config updated	Конфигурация обновлена
9	Restarting endpoint	Перезапуск endpoint
10	Starting console sync	Запуск синхронизации консоли
11	Intergrity control started	Контроль целостности запущен
12	Check done	Проверка выполнена
13	Can't verify license: license wasn't started	Невозможно проверить лицензию. Лицензия не была запущена

11 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

11.1 Уведомление об успешной активации лицензии

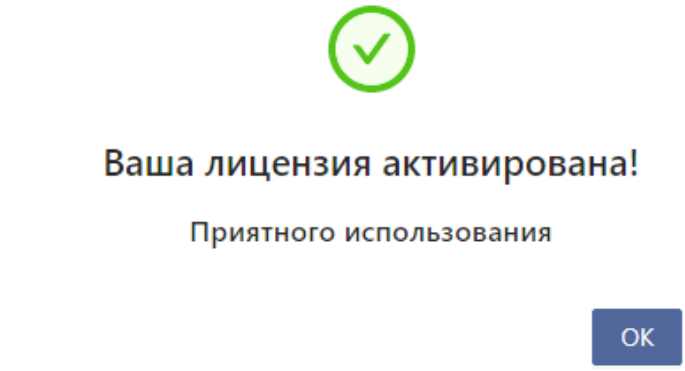

Рисунок 44 – Уведомление об успешной активации лицензии

11.2 Предупреждение о необходимости перезагрузки компьютера при включении белого списка программ и контроля устройств

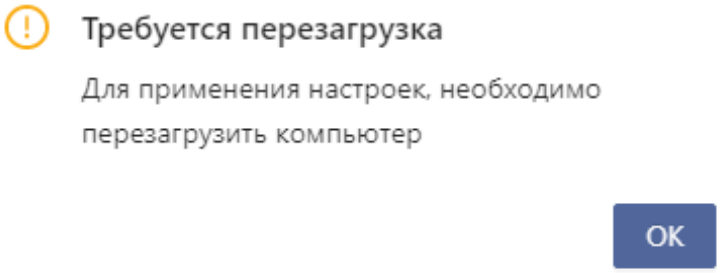

Рисунок 45 – Предупреждение о перезагрузке компьютера при включении белого списка программ и контроля устройств

11.3 Уведомление о сохранении конфигурации

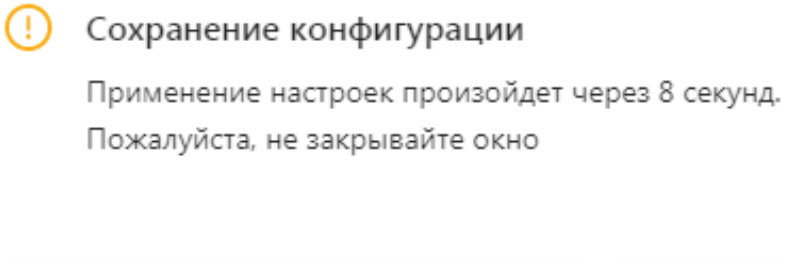

Рисунок 46 – Уведомление о сохранении конфигурации

11.4 Уведомление о несохраненных изменениях

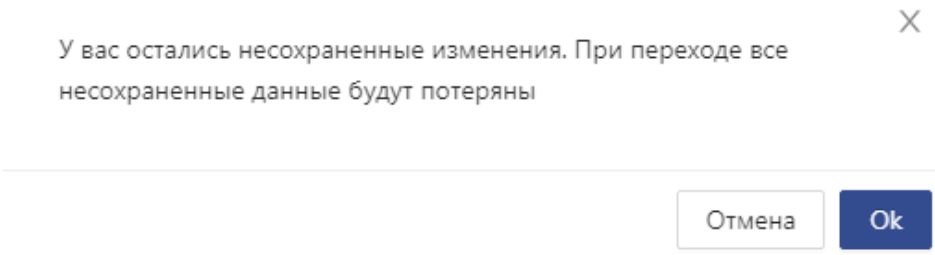

Рисунок 47 – Уведомление о несохраненных изменениях

11.5 Уведомление о перезапуске сервиса

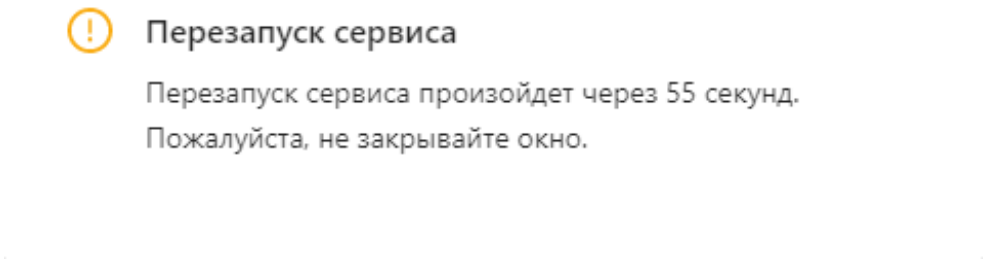

Рисунок 48 – Уведомление о перезапуске сервиса

11.6 Уведомление об обновлении эталонных образов

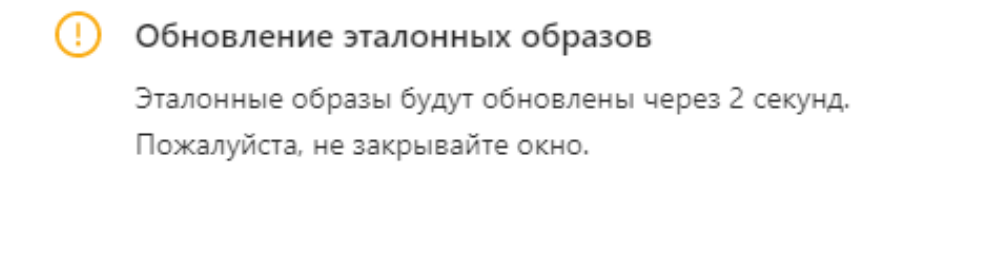

Рисунок 49 – Уведомление об обновлении эталонных образов

11.7 Уведомление о запуске проверки режима обучения

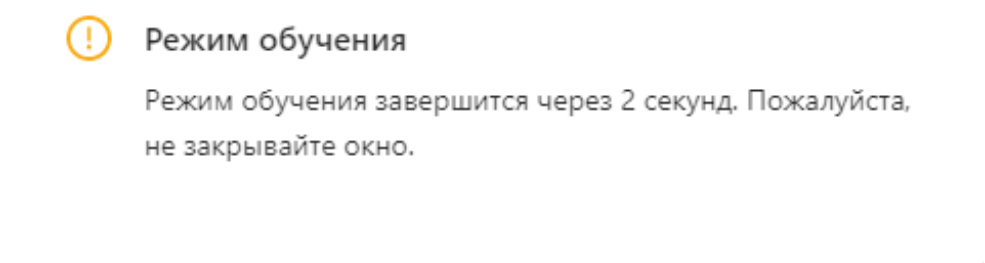

Рисунок 50 – Уведомление о запуске проверки режима обучения

11.8 Уведомление об успешной проверке контрольных сумм по базе

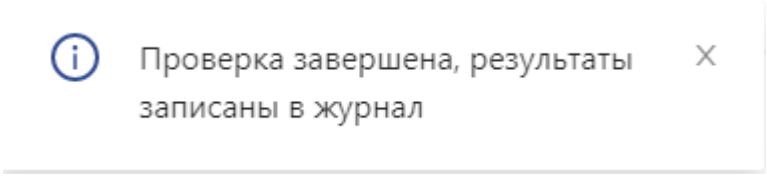

Рисунок 51 – Уведомление об успешной проверке контрольных сумм по базе

11.9 Уведомление о невозможности распознать файл лицензии

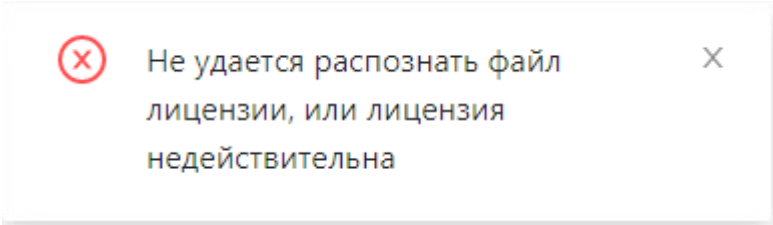

Рисунок 52 – Уведомление о невозможности распознать файл лицензии

11.10 Уведомление о некорректно введенном формате серийного номера

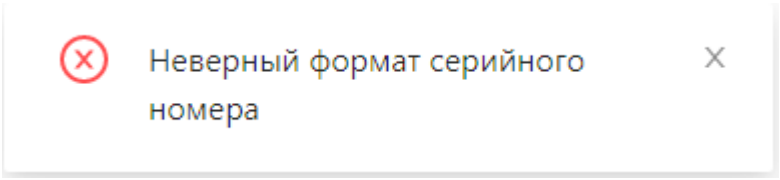

Рисунок 53 – Неверный формат серийного номера

11.11 Уведомление перед началом работы с антивирусом

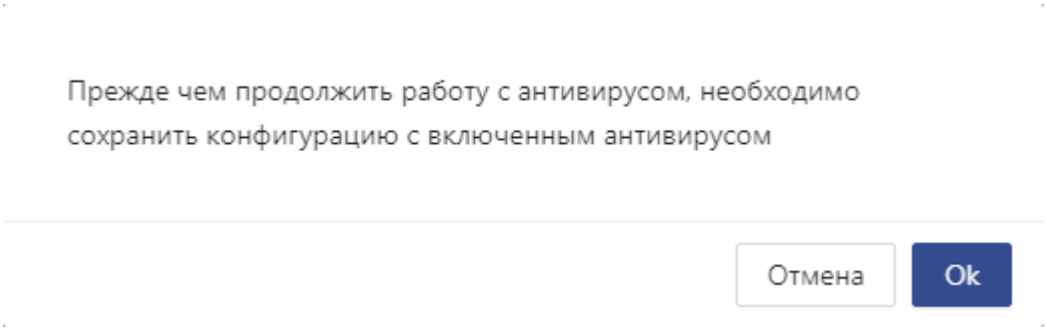

Рисунок 54 – Уведомление перед началом работы с антивирусом

11.12 Уведомление о запуске процесса обновления эталонных образов и проверки по базе

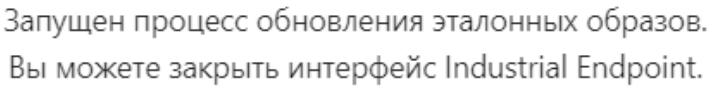

Рисунок 55 – Уведомление о процессе обновления эталонных образов

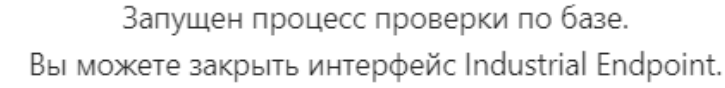

Рисунок 56 – Уведомление о процессе проверки по базе