Руководство пользователя по эксплуатации

версия 15 ред. от 16.09.2024

Листов 51

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
БД	База данных
Брандмауэр Защитника Windows	Встроенный в Microsoft Windows межсетевой экран
ГБ	Гигабайт
ГГц	Гигагерц
Мб	Мегабайт
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
УЗ	Учётная запись
ARMA IE	InfoWatch ARMA Industrial Endpoint
ARMA MC	InfoWatch ARMA Management Console
MSI	Расширение установочного пакета
USB	Последовательный интерфейс для подключения периферийных устройств
USB-носитель	Носитель данных, подключаемый с помощью интерфейса USB
Wi-Fi	Технология беспроводной локальной сети

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Industrial Endpoint v.2.7.2**.

Руководство пользователя по эксплуатации содержит описание:

- принципов работы **ARMA IE**;
- локального графического интерфейса **ARMA IE**;
- настройки и использования доступных функций **ARMA IE**.

Пользователю **ARMA IE** 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 InfoWatch ARMA Management Console

1 ОБЩИЕ СВЕДЕНИЯ

ARMA IE распространяется в виде пакета установки с расширением **«MSI»**.

Перед инсталляцией **ARMA IE** рекомендуется выполнить разграничение прав доступа в ОС. Пользователям компьютера не рекомендуется предоставлять роль уровня «Администратор ОС».

Установка и настройка **ARMA IE** производится только УЗ с ролью уровня «Администратор ОС». УЗ с ролью ниже уровня «Администратор ОС» не имеет доступа к графическому интерфейсу **ARMA IE**.

Примечание:

Не допускается использование встроенных УЗ ОС, например, «Администратор». Для проверки того, является ли УЗ встроенной, необходимо выполнить в командной строке ОС следующую команду:

- «wmic useraccount where name="%username%" get Caption, Description», где %username% – имя УЗ (см. Рисунок – Проверка параметров УЗ).

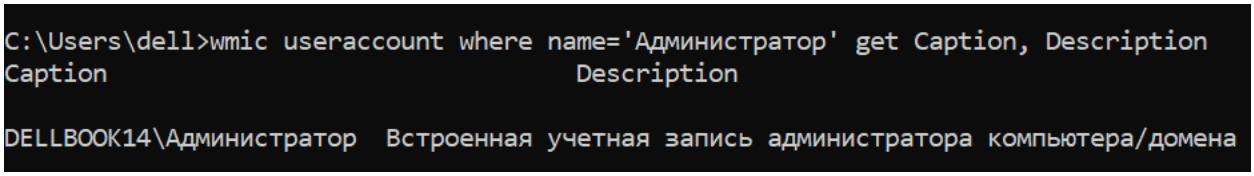

Рисунок – Проверка параметров УЗ

Подробная установка **ARMA IE** описана в разделе Установка сервиса настоящего руководства.

1.1 Требования к среде функционирования

Минимальные технические требования к аппаратному обеспечению зависят от варианта установки и представлены в таблице (см. Таблица «Минимальные требования к аппаратному обеспечению для базовой установки»).

Таблица «Минимальные требования к аппаратному обеспечению для базовой установки»

Оборудование	Требования
Процессор	2,0 ГГц, одноядерный, x86 или x64
Свободное место на жестком диске	1,6 Гб
ОЗУ	В соответствии с предъявляемыми требованиями к ОС

Оборудование	Требования
Операционная система	64-разрядная версия Windows 7 (Professional, Enterprise и Ultimate) 64-разрядная версия Windows 10
Зависимости	Программная платформа .NET Framework версия 3.5

Примечание:

Для обнаружения цифровой подписи на ОС Windows 7 необходимы обновления системы безопасности KB4474419, KB4490628 и KB2999226.

Для корректной работы **ARMA IE** необходимо установить все актуальные обновления для ОС Windows.

2 НАЧАЛО РАБОТЫ

2.1 Установка сервиса

Для установки **ARMA IE** необходимо запустить установочный файл **ARMA IE** от имени УЗ с ролью уровня «Администратор ОС» и следовать шагам мастера установки:

1. Шаг мастера – **«Приветственное сообщение»** (см. Рисунок – Приветственное сообщение).

   Нажать **кнопку «Далее >»** для продолжения установки.

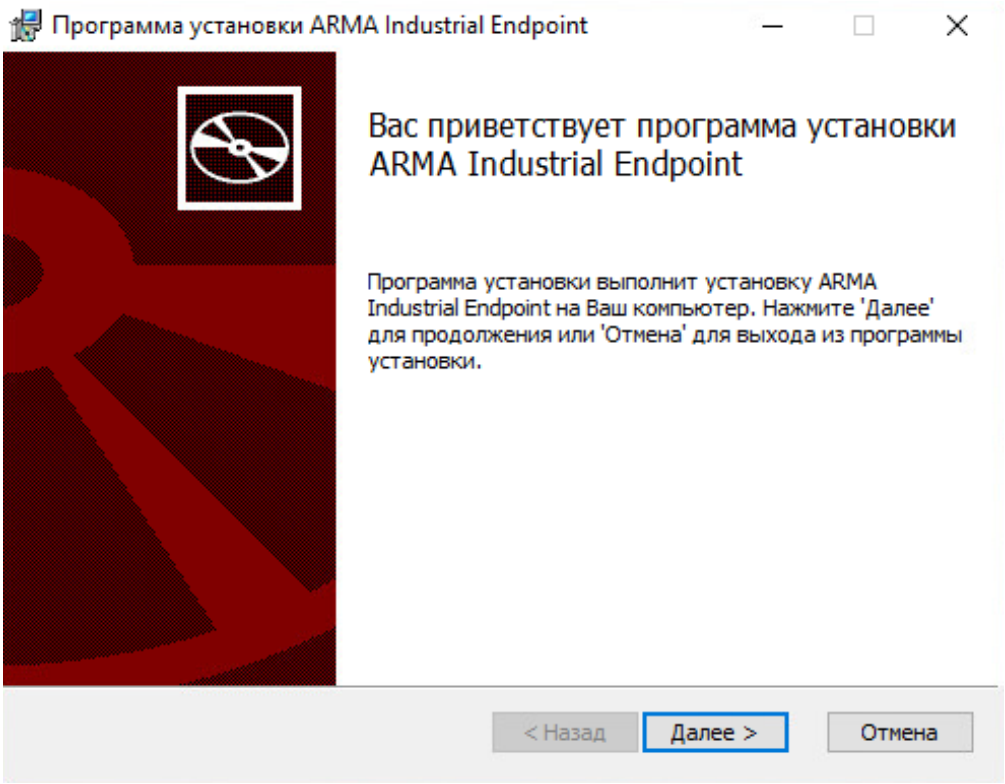

Рисунок – Приветственное сообщение

2. Шаг мастера – **«Лицензионное соглашение»** (см. Рисунок – Лицензионное соглашение).

   Ознакомиться с пользовательским соглашением, установить флажок для параметра **«Я принимаю условия данного соглашения»** и нажать **кнопку «Далее >»**.

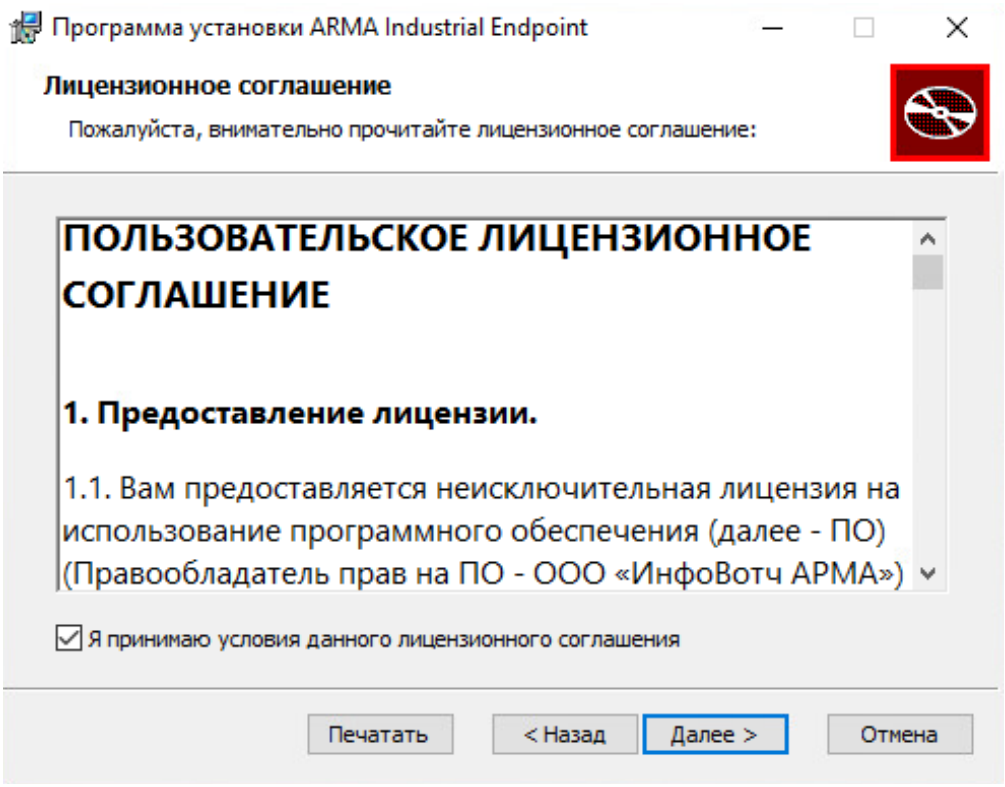

Рисунок – Лицензионное соглашение

3. Шаг мастера – **«Папка установки»** (см. Рисунок – Папка установки).

   Для установки в указанный по умолчанию каталог нажать **кнопку «Далее >»**.

   При необходимости сменить каталог установки, нажать **кнопку «Обзор...»**, выбрать требуемый каталог и нажать **кнопку «ОК»**, а затем **кнопку «Далее >»**.

   Примечание:

   Имя каталога установки не должно содержать буквы кириллического алфавита и специальные символы «!@#$^&()_+=».

   Примечание:

   В случае выбора каталога установки «Program Files», **ARMA IE** будет установлен в каталог «Program Files (x86)».

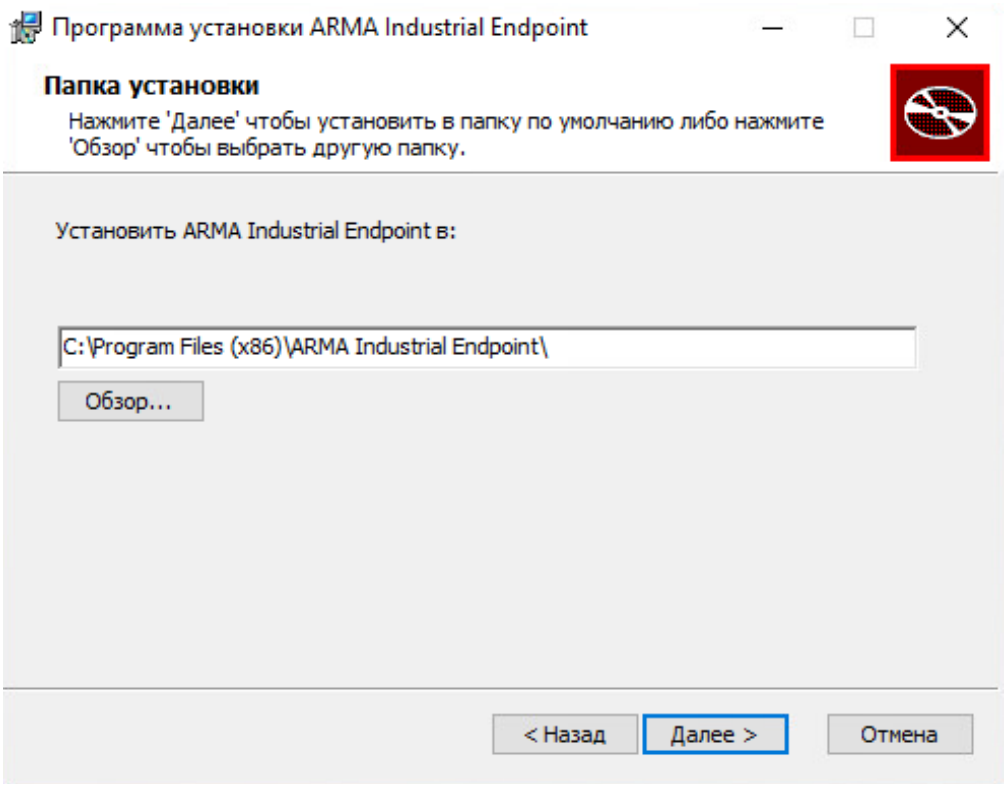

Рисунок – Папка установки

4. Шаг мастера – **«Подтверждение установки»** (см. Рисунок – Подтверждение установки).

   Для начала установки нажать **кнопку «Начать»**. Процесс установки будет отображен на полосе прогресса.

   При необходимости изменения параметров установки и возврата к предыдущим шагам мастера нажать **кнопку «< Назад»**.

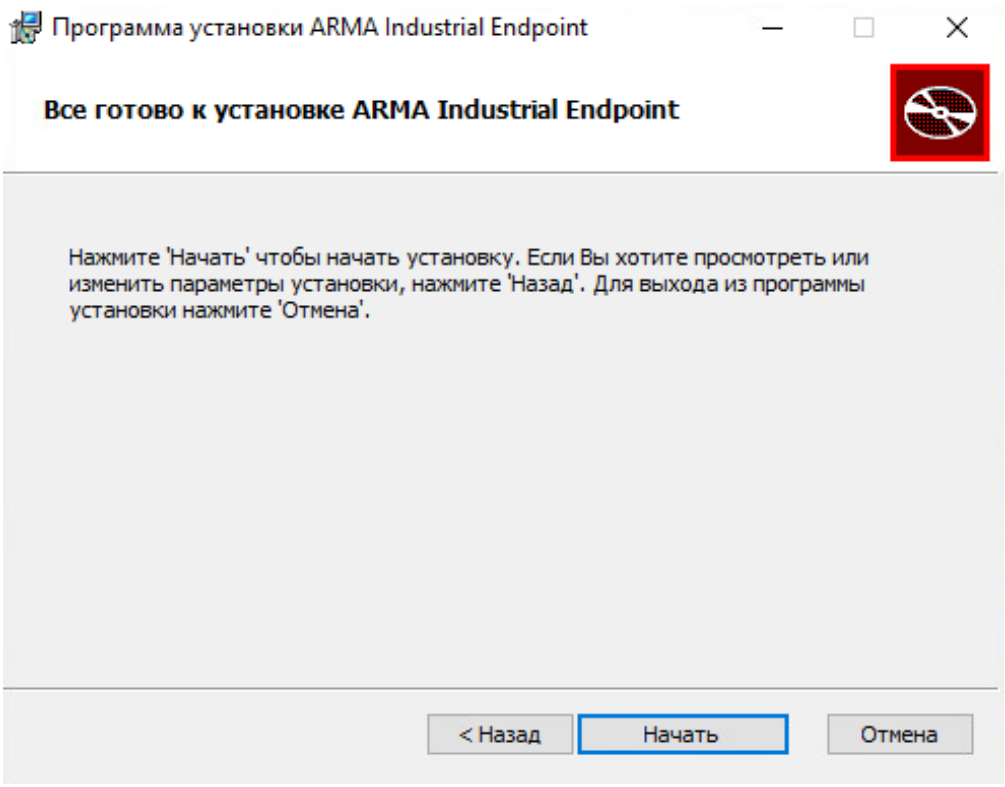

Рисунок – Подтверждение установки

5. Шаг мастера – **«Окончание установки»** (см. Рисунок – Окончание установки).

   Нажать **кнопку «Готово»** для закрытия мастера.

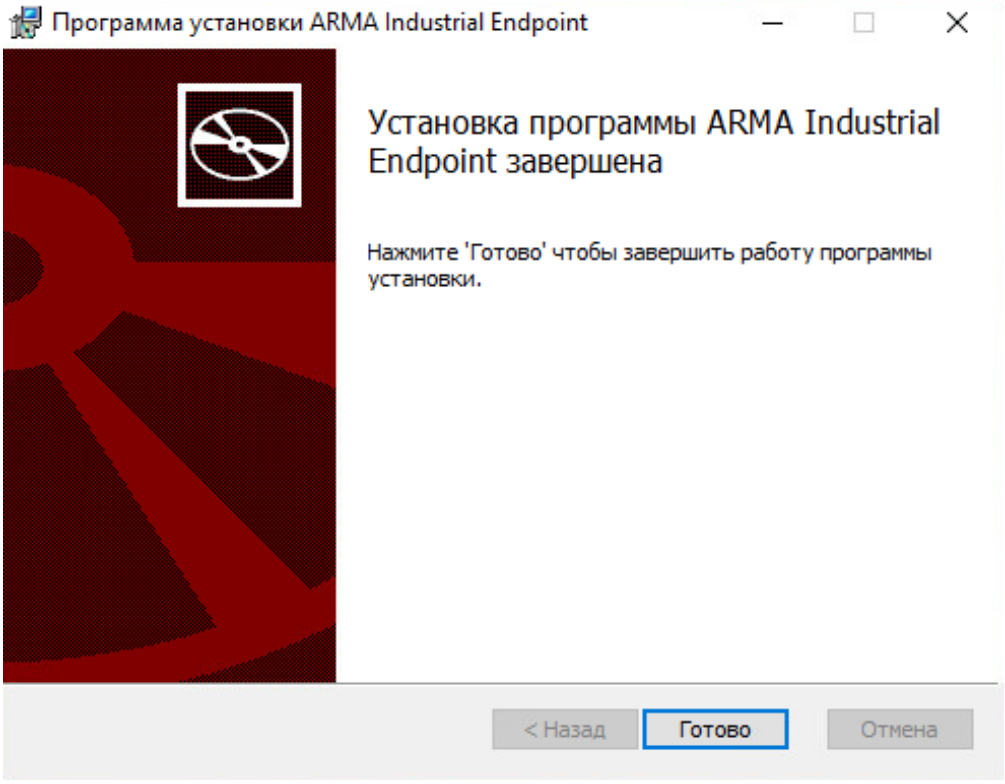

Рисунок – Окончание установки

После окончания установки будет предложено перезагрузить компьютер (см. Рисунок – Запрос перезагрузки компьютера). Рекомендуется выполнить перезагрузку, нажав **кнопку «Да»**.

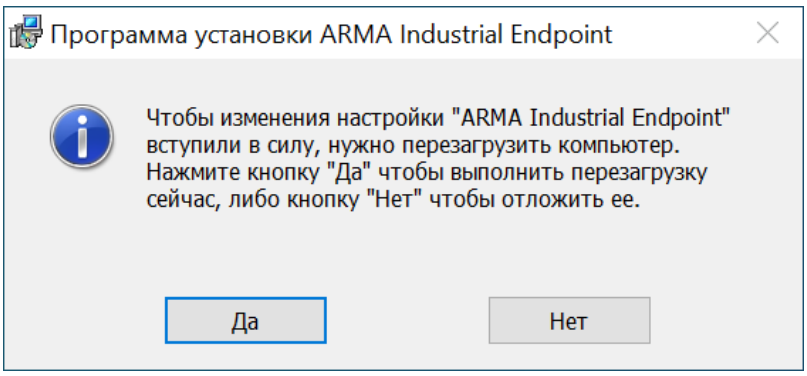

Рисунок – Запрос перезагрузки компьютера

После перезагрузки компьютера будут автоматически выполнены следующие действия:

- запущен сервис **«ARMA Industrial Endpoint»** (см. Рисунок – Сервис «ARMA Industrial Endpoint»);

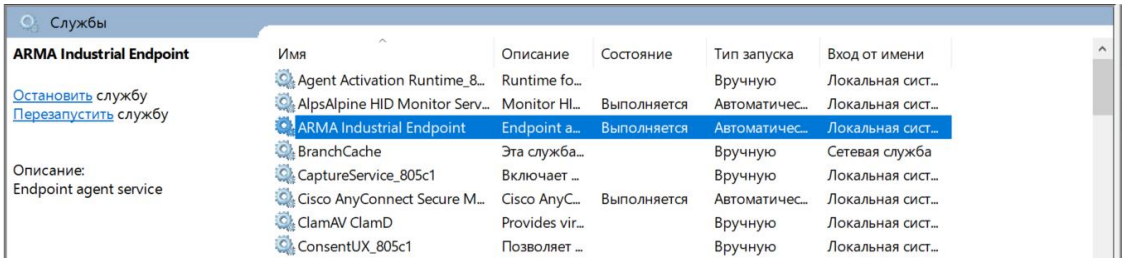

Рисунок – Сервис «ARMA Industrial Endpoint»

- создано разрешающее правило МЭ, в Брандмауэре Защитника Windows (см. Рисунок – Правило МЭ);

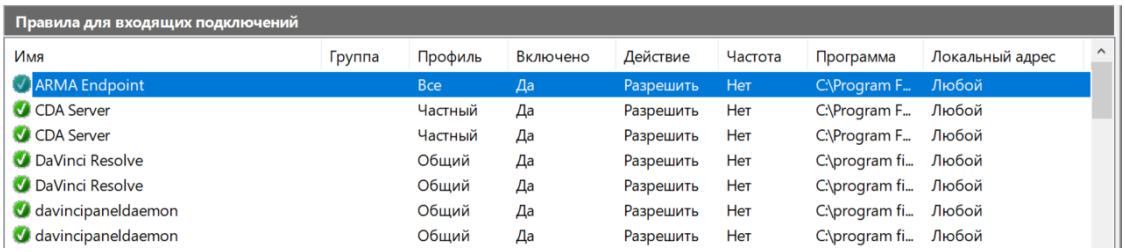

Рисунок – Правило МЭ

- в каталоге установки созданы файлы, отвечающие за хранение журнала и настроек, **«endpoint.log»** и **«main.db»** соответственно.

2.2 Запуск графического интерфейса и активация ARMA IE

Для запуска графического интерфейса **ARMA IE** необходимо выполнить следующие действия:

1. Открыть меню «Пуск», нажав **кнопку «Пуск»**, по умолчанию расположенную в левом нижнем углу экрана, или нажав на клавиатуре **клавишу с эмблемой Windows**.
2. Ввести на клавиатуре слово **«Endpoint»** и нажать **левой кнопкой мыши** любую из иконок найденного приложения (см. Рисунок – Запуск графического интерфейса).

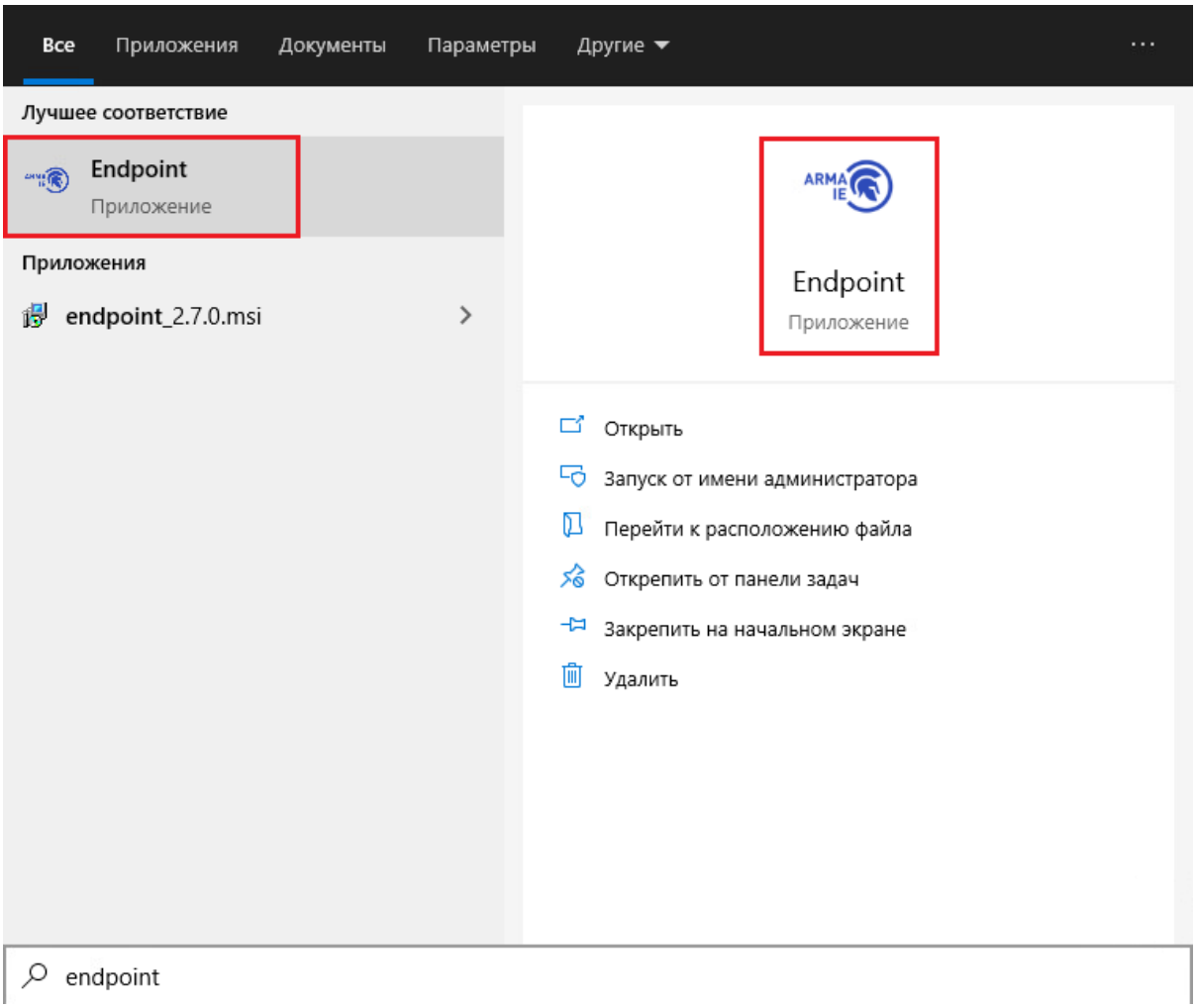

Рисунок – Запуск графического интерфейса

При первом запуске графического интерфейса пользователю будет предложено задать пароль, который в дальнейшем будет использоваться для авторизации (см. Рисунок – Указание пароля ARMA IE).

Рисунок – Указание пароля ARMA IE

После ввода пароля необходимо активировать лицензию одним из предложенных способов:

- **«Активировать онлайн»** – активация лицензии с доступом в Интернет;
- **«Активировать офлайн»** – активация лицензии без доступа в Интернет.

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

2.2.1 Активация лицензии с доступом в Интернет

Для активации лицензии с доступом в Интернет необходимо выполнить следующие действия:

1. Установить переключатель « » в сторону **«Активировать онлайн»**.
2. В поле **«Лицензионный ключ»** указать лицензионный ключ и нажать **кнопку «Активировать»** (см. Рисунок – Активация лицензии с доступом в Интернет).

Рисунок – Активация лицензии с доступом в Интернет

При успешной активации лицензии появится соответствующее уведомление (см. Рисунок – Уведомление об успешной активации лицензии).

2.2.2 Активация лицензии без доступа в Интернет

Для активации лицензии без доступа в Интернет необходимо выполнить следующие действия:

1. Установить переключатель « » в сторону **«Активировать офлайн»**.
2. В поле **«Лицензионный ключ»** указать лицензионный ключ и нажать **кнопку «Получить токен»** (см. Рисунок – Активация лицензии без доступа в Интернет).

Рисунок – Активация лицензии без доступа в Интернет

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

Рисунок – Получение токена для активации

4. Нажать **кнопку «Загрузить файл лицензии»**, в открывшемся окне проводника выбрать полученный файл **«license.bin»** и нажать **кнопку «Открыть»**, а затем **кнопку «Активировать»** (см. Рисунок – Загрузка файла лицензии).

Рисунок – Загрузка файла лицензии

При успешной активации лицензии появится соответствующее уведомление (см. Рисунок – Уведомление об успешной активации лицензии).

2.3 Типы лицензий

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

1. **«Базовая»** – предоставляет доступ ко всем функциям **ARMA IE**. Срок лицензии – 1 год.
2. **«TRIAL»** – предоставляет доступ ко всем функциям **ARMA IE**. Срок лицензии – 30 дней.

Информация о типе и сроке окончания лицензии отображается в области быстрой навигации (см. Область быстрой навигации).

Примечание:

В **ARMA IE** после окончания срока действия лицензии и перезагрузке, производится блокировка функциональности до момента продления лицензии.

2.4 Обслуживание

2.4.1 Обновление ARMA IE

Обновление **ARMA IE** производится путем удаления текущей версии и последующего запуска установочного файла **ARMA IE** новой версии.

Процесс установки описан в разделе Установка сервиса настоящего руководства.

Процесс удаления описан в разделе Удаление ARMA IE настоящего руководства.

Примечание:

Для обновления **ARMA IE** на версию 2.7 и выше с сохранением текущих настроек необходимо выполнить следующие действия:

1. Сохранить в удобный каталог копии следующих файлов: «config.json», «endpoint.log», «config.json.bak», «license.bin», «main.db». Перечисленные файлы расположены каталоге установки, указанном на шаге мастера – **«Папка установки»** (см. Рисунок – Папка установки).
2. Удалить **ARMA IE**.
3. Выполнить установку **ARMA IE**.
4. После перезагрузки компьютера подменить в каталоге установки **ARMA IE** файлы «config.json», «endpoint.log», «config.json.bak», «license.bin» и «main.db» предварительно скопированными.

2.4.2 Восстановление ARMA IE

В случае необходимости восстановления **ARMA IE**, рекомендуется выполнить следующие действия:

1. Запустить установочный файл **ARMA IE** от имени УЗ с ролью уровня «Администратор ОС» и следовать шагам мастера установки (см. Рисунок – Приветственное сообщение), учитывая следующие особенности:

   - шаг мастера – **«Изменить, восстановить или удалить программу»** (см. Рисунок – Изменить, восстановить или удалить программу) нажать **кнопку «Удалить»**;

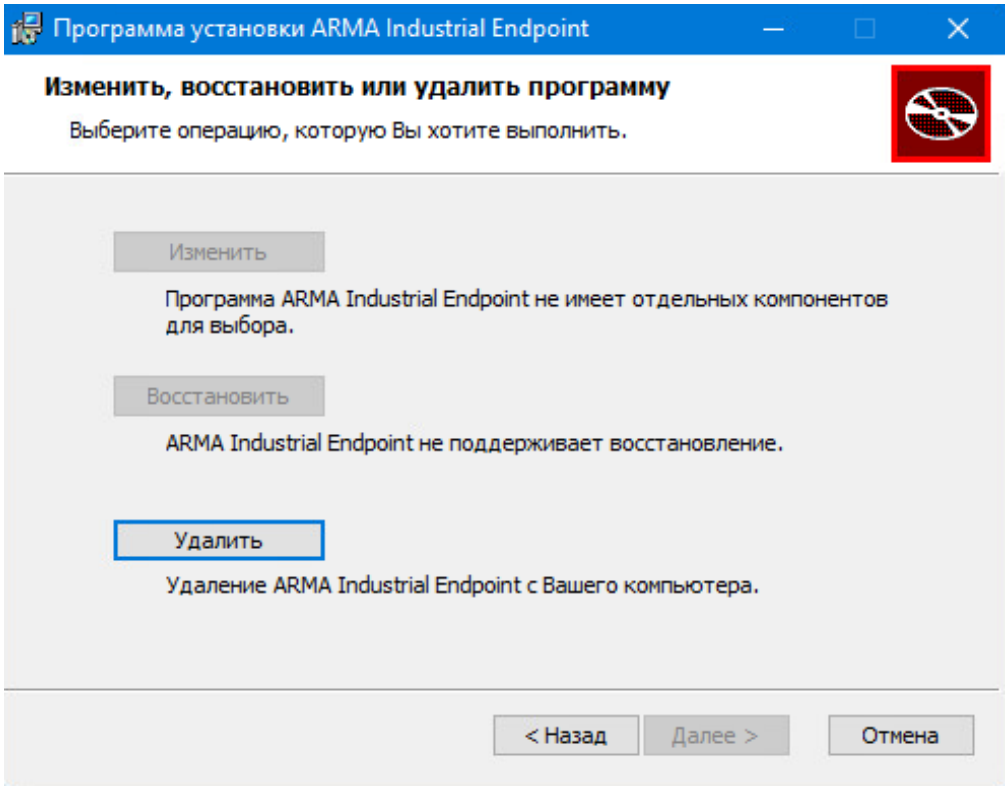

Рисунок – Изменить, восстановить или удалить программу

   - шаг мастера – **«Удаление ARMA Industrial Endpoint»** (см. Рисунок – Удаление ARMA Industrial Endpoint) нажать **кнопку «Удалить»**.

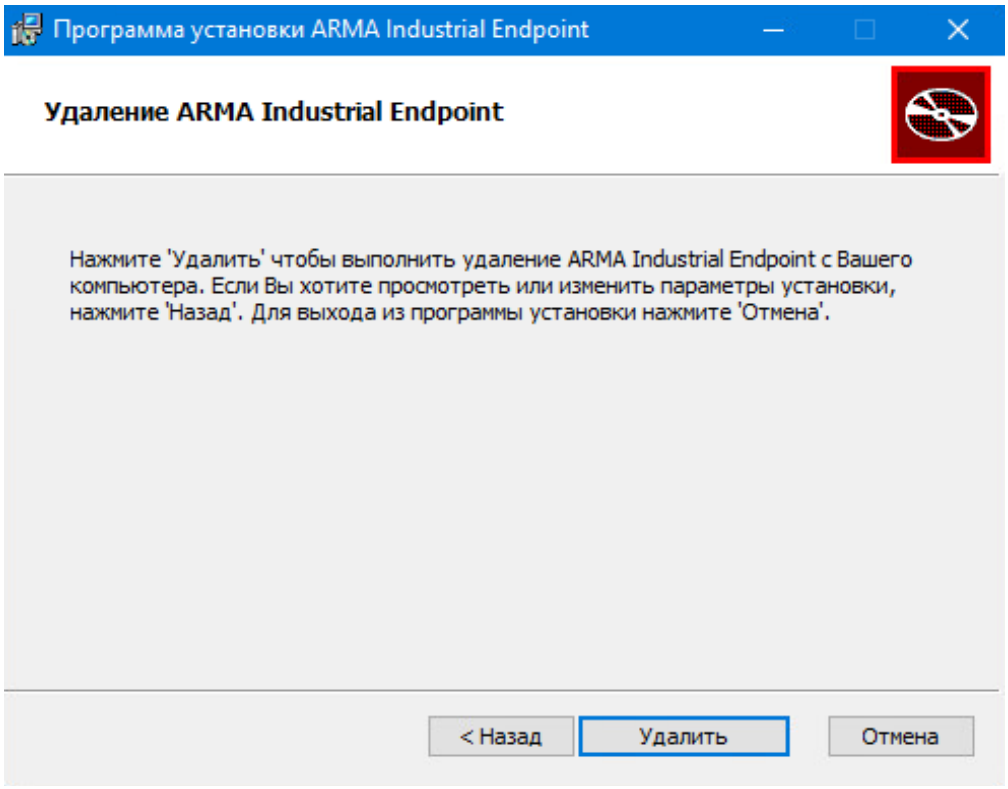

Рисунок – Удаление ARMA Industrial Endpoint

2. Выполнить перезагрузку компьютера после закрытия мастера (см. Рисунок – Окончание установки).
3. Запустить процесс установки **ARMA IE** (см. Установка сервиса).

2.4.3 Удаление ARMA IE

В случае необходимости удаления **ARMA IE**, рекомендуется выполнить следующие действия:

1. Запустить установочный файл **ARMA IE** от имени УЗ с ролью уровня «Администратор ОС» и следовать шагам мастера установки (см. Рисунок – Приветственное сообщение), учитывая следующие особенности:
   - шаг мастера – **«Изменить, восстановить или удалить программу»** (см. Рисунок – Изменить, восстановить или удалить программу) нажать **кнопку «Удалить»**;

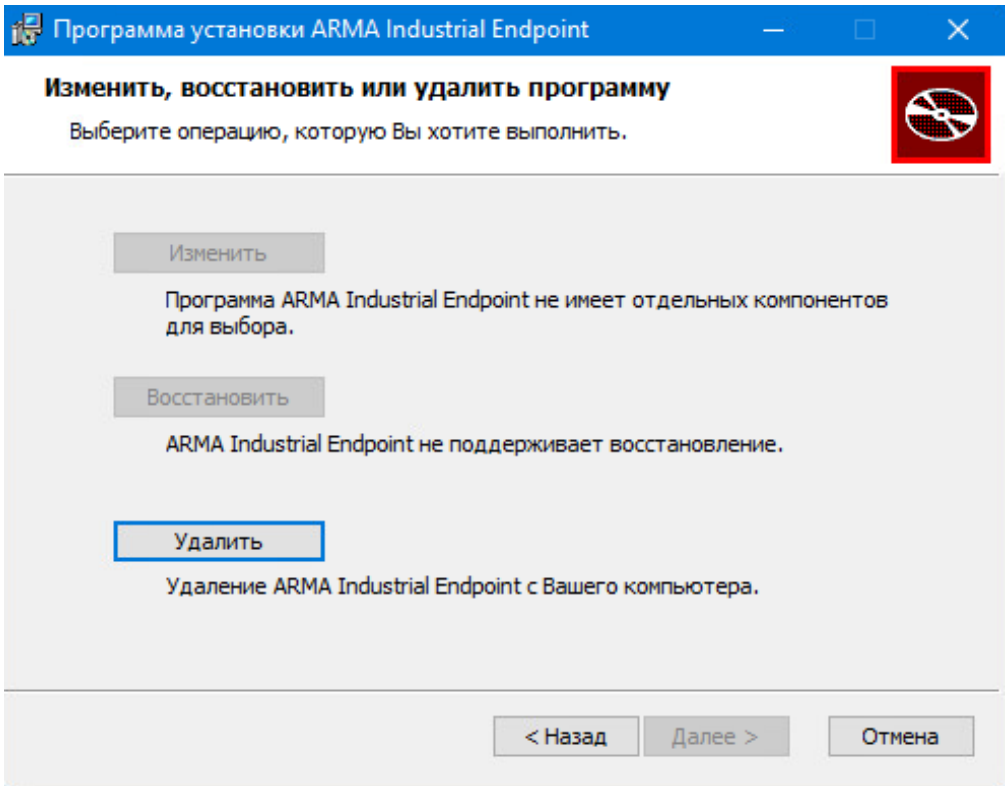

Рисунок – Изменить, восстановить или удалить программу

- шаг мастера – **«Удаление ARMA Industrial Endpoint»** (см. Рисунок – Удаление ARMA Industrial Endpoint) нажать **кнопку «Удалить»**.

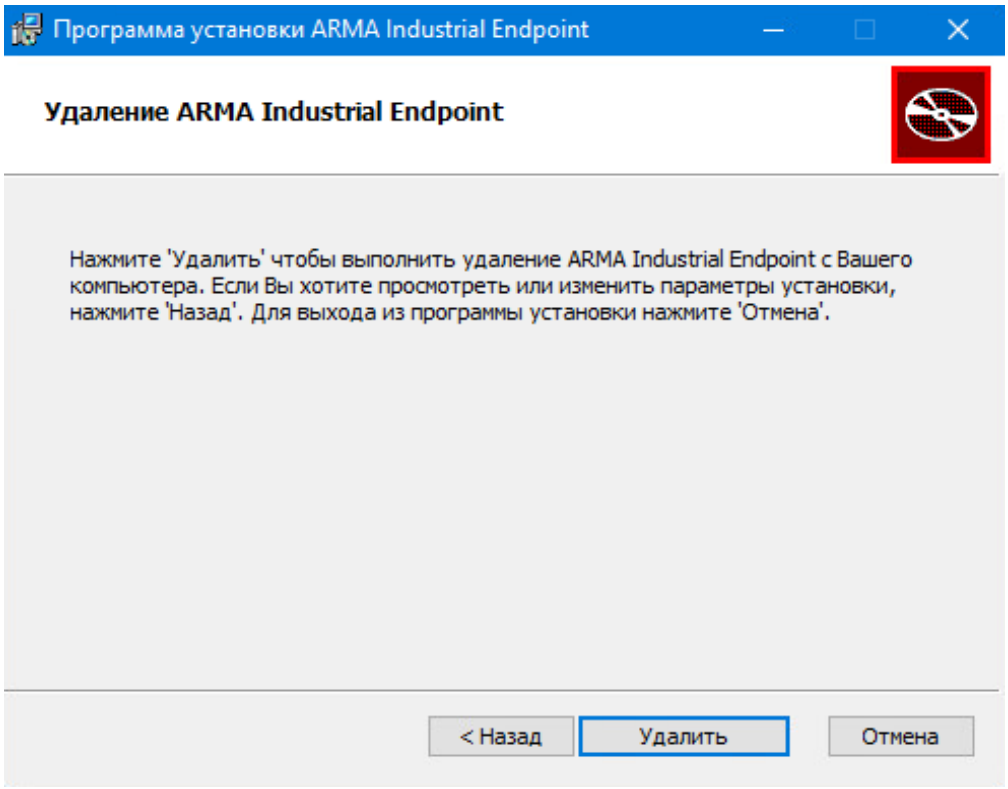

Рисунок – Удаление ARMA Industrial Endpoint

2. Выполнить перезагрузку компьютера после закрытия мастера (см. Рисунок – Окончание установки).

3 ОПИСАНИЕ ЛОКАЛЬНОГО ГРАФИЧЕСКОГО ИНТЕРФЕЙСА

Общий вид локального графического интерфейса **ARMA IE** представлен на рисунке (см. Рисунок – Локальный графический интерфейс ARMA IE).

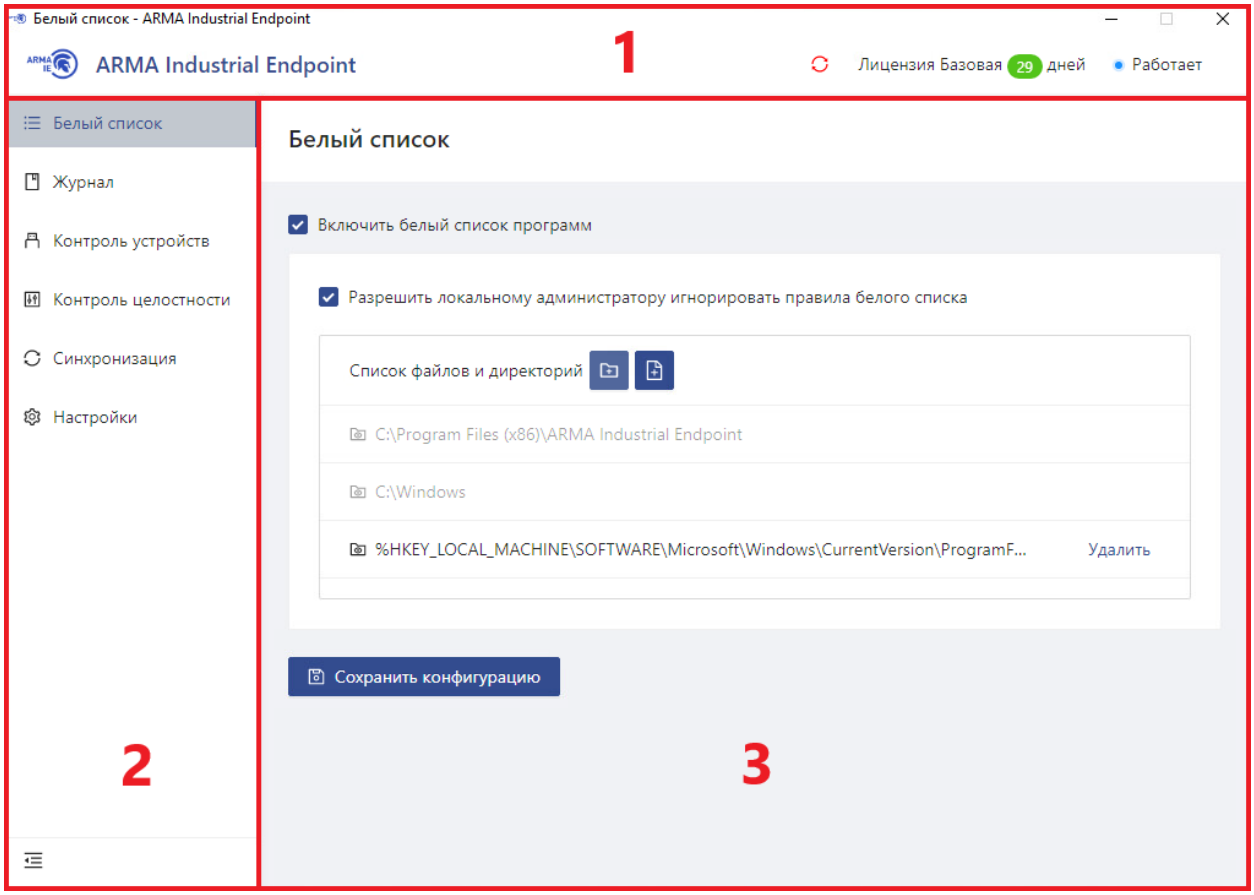

Рисунок – Локальный графический интерфейс ARMA IE

Основные разделы локального графического интерфейса:

- область быстрой навигации (**1**);
- область меню (**2**);
- форма раздела меню (**3**).

3.1 Область быстрой навигации

Область быстрой навигации **ARMA IE** представлена на рисунке (см. Рисунок – Область быстрой навигации).

Рисунок – Область быстрой навигации

Область быстрой навигации доступна в любом разделе локального графического интерфейса и содержит:

- логотип **ARMA IE** (**1**);
- индикатор статуса синхронизации с **ARMA MC** (**2**);
- информацию о лицензии **ARMA IE** (**3**);
- статус текущего состояния **ARMA IE** (**4**).

3.1.1 Логотип ARMA IE

При нажатии на логотип **ARMA IE** в любом разделе интерфейса происходит переход в раздел **«Белый список»**.

3.1.2 Индикатор статуса синхронизации с ARMA MC

Индикатор статуса синхронизации с **ARMA MC** отображает информацию о синхронизации с **ARMA MC**:

- индикатор зелёного цвета « » – синхронизация включена;
- индикатор красного цвета « » – синхронизация выключена.

3.1.3 Информация о лицензии ARMA IE

Информация о лицензии **ARMA IE** содержит:

- тип лицензии;
- срок окончания лицензии.

3.1.4 Статус текущего состояния ARMA IE

Статус текущего состояния **ARMA IE** отображает статус работы **ARMA IE**.

3.2 Область меню

Область меню (см. Рисунок – Область меню) предназначена для осуществления доступа к различным функциям **ARMA IE**, переход к которым осуществляется нажатием **левой кнопки мыши**.

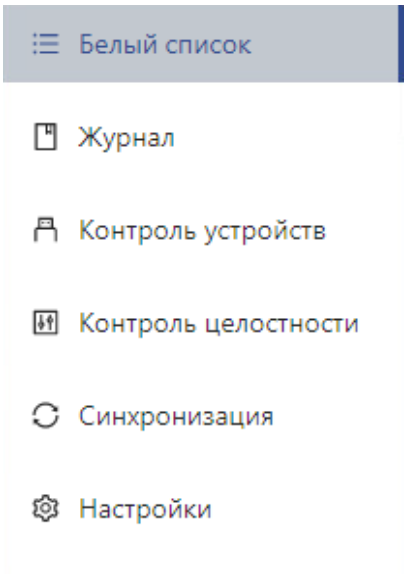

Рисунок – Область меню

3.3 Форма раздела меню

В качестве примера представлена форма раздела **«Белый список»** (см. Рисунок – Форма раздела меню).

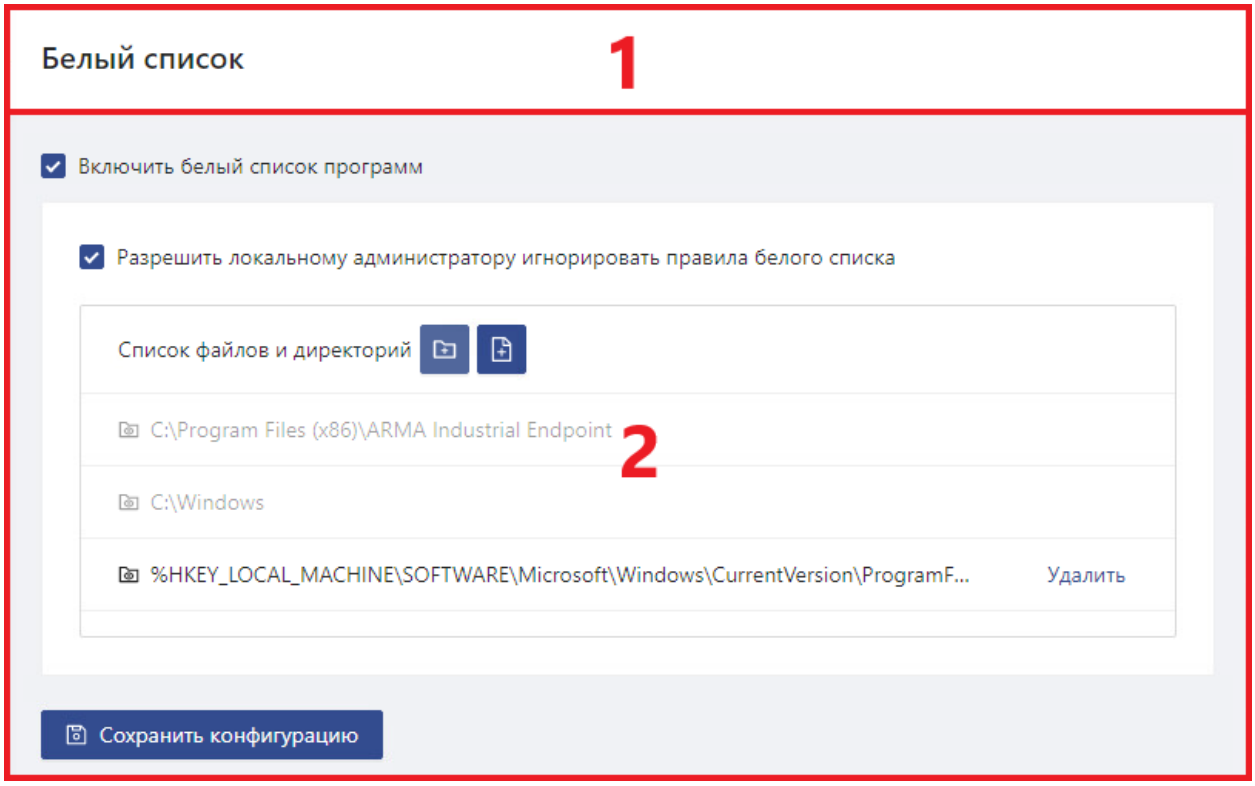

Рисунок – Форма раздела меню

Форма раздела меню содержит:

- название раздела (**1**);
- содержание раздела (**2**).

4 НАСТРОЙКА СИНХРОНИЗАЦИИ С ARMA MC

Существует возможность управления **ARMA IE** с помощью единого центра управления **ARMA MC**, для этого в **ARMA IE** предусмотрена функция **«Синхронизация»**.

Примечание:

Перед настройкой синхронизации **ARMA IE** с **ARMA MC** рекомендуется настройть Сетевой журнал (см. Настройка сетевого журнала).

Настройка синхронизации производится на каждом продукте по отдельности:

- в едином центре управления **ARMA MC**;
- в локальном графическом интерфейсе **ARMA IE**.

Для включения функции **«Синхронизация»** и настройки параметров синхронизации необходимо выполнить следующие действия:

1. Перейти в раздел меню **«Синхронизация»** (см. Рисунок – Синхронизация) и установить флажок для параметра **«Включить синхронизацию с ARMA Management Console»**.

   При установленном флажке для параметра **«Не пытаться восстановить соединение в случае ошибки»**, попытки синхронизации между **ARMA IE** и **ARMA MC** не будут осуществляться снова, в случае разрыва соединения.

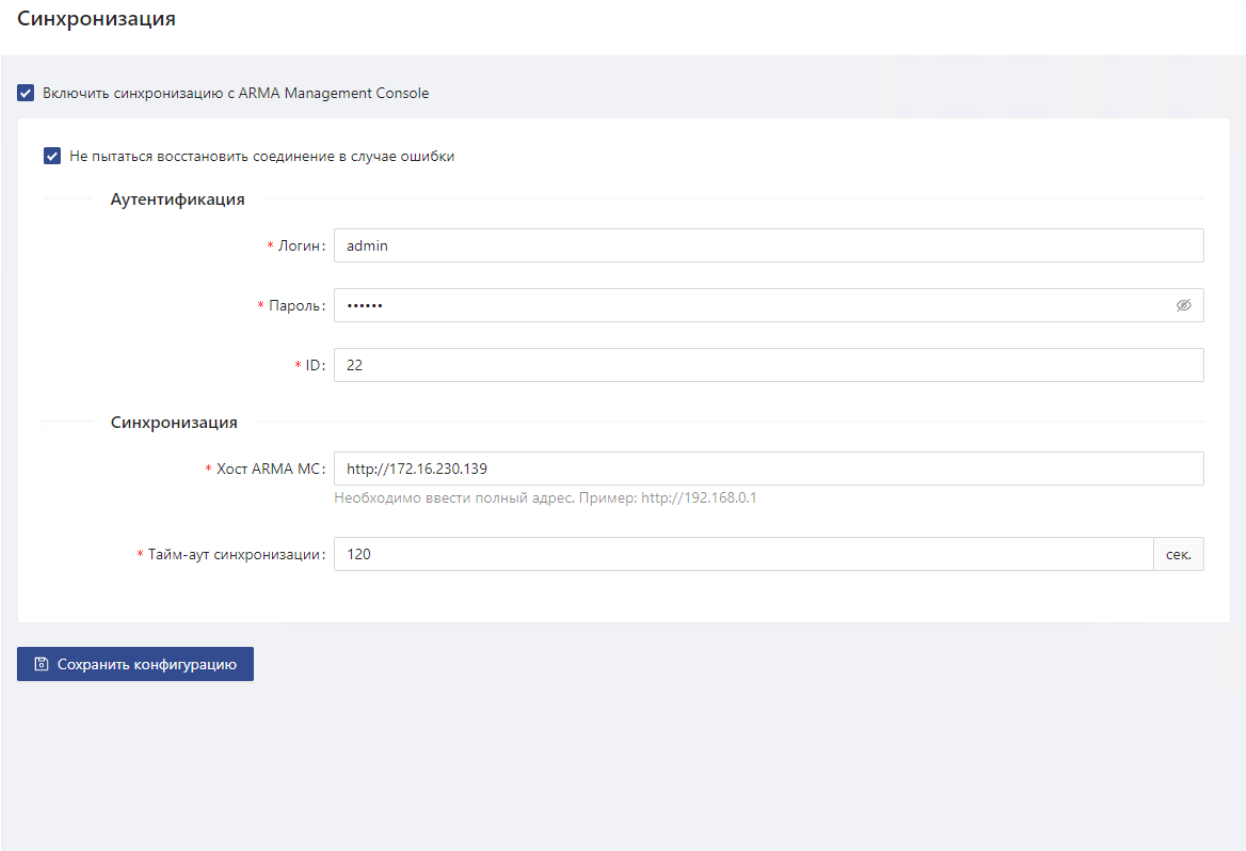

Рисунок – Синхронизация

2. В блоке настроек **«Аутентификация»** указать данные для параметров:
   - **«Логин»** – имя пользователя УЗ, созданной в **ARMA MC** для синхронизации с **ARMA IE**;
   - **«Пароль»** – пароль УЗ, созданной в **ARMA MC** для синхронизации с **ARMA IE**.
   - **«ID»** – значение ID, добавленного устройства **ARMA IE** из раздела **«Источники событий»** в **ARMA MC**.
3. В блоке настроек **«Синхронизация»** указать данные для параметров:
   - **«Хост ARMA MC»** – полный URL-адрес **ARMA MC**;
   - **«Тайм-аут синхронизации»** – время синхронизации в секундах, либо оставить значение по умолчанию «120».
4. Нажать **кнопку «Сохранить конфигурацию»**.

Примечание:

В случае ввода неверного пароля, при отсутствующем флажке для параметра **«Не пытаться восстановить соединение в случае ошибки»**, может произойти блокировка учетной записи пользователя **ARMA MC**, через которую происходит подключение **ARMA IE**, аналогичная

происходящей после ввода неверного пароля при авторизации в **ARMA MC**. Повторная авторизация, после вышеуказанной блокировки, возможна лишь по прошествии времени, согласно системным настройкам **ARMA MC**.

После включения функции **«Синхронизация»** перечисленные ниже функции:

- **«Белый список»** (см. Управление белым списком программ);
- **«Контроль устройств»** (см. Управление контролем устройств);
- **«Контроль целостности»** (см. Управление контролем целостности);
- **«Настройки»** (см. Дополнительные настройки);

будут частично доступны для управления через **ARMA MC** (см. Руководство пользователя **ARMA MC**) и недоступны через локальный графический интерфейс **ARMA IE**.

5 УПРАВЛЕНИЕ БЕЛЫМ СПИСКОМ ПРОГРАММ

Для ограничения перечня исполняемых программ в **ARMA IE** предусмотрена функция **«Белый список программ»**.

Управление функцией **«Белый список программ»** осуществляется одним из следующих способов:

- через единый центр управления **ARMA MC**;
- в локальном графическом интерфейсе **ARMA IE**.

Примечание:

Не гарантируется корректная работа **ARMA IE** в случае добавления в белый список исполняемых файлов с расширением, отличным от «EXE», а также каталогов, содержащих вышеуказанные файлы.

Для включения функции **«Белый список программ»** и добавления в белый список файла или каталога, содержащего исполняемые файлы, разрешенные к запуску, необходимо выполнить следующие действия:

1. Перейти в раздел меню **«Белый список»** (см. Рисунок – Белый список программ), установить флажок для параметра **«Включить белый список программ»** и нажать **кнопку «Сохранить конфигурацию»**.

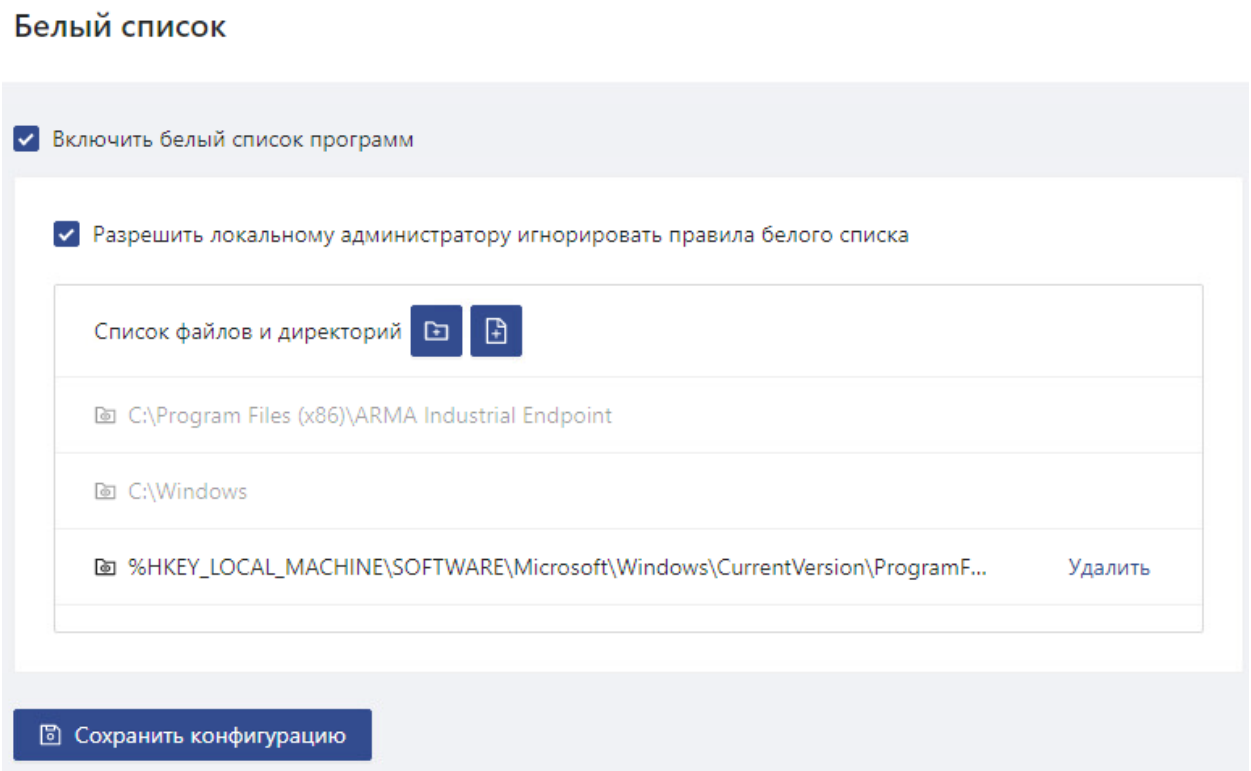

Рисунок – Белый список программ

2. Нажать **кнопку**:

- «  » для выбора в открывшейся форме проводника каталога, содержащего исполняемые файлы, разрешенные к запуску, и нажать **кнопку «Выбор папки»**. Исполняемые файлы во всех вложенных каталогах также будут разрешены к запуску;
- «  » для выбора в открывшейся форме проводника файла, разрешенного к запуску, и нажать **кнопку «Открыть»**.

3. Нажать **кнопку «Сохранить конфигурацию»**.

С целью исключения некорректной работы ОС или самоблокировки **ARMA IE**, в **«Белый список программ»** по умолчанию, без возможности удаления из списка, включены следующие каталоги, расположенные по пути:

C:\Program Files(x86)\ARMA Industrial Endpoint
C:\Windows

Каталог «%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%» включен в **«Белый список программ»** по умолчанию, с возможностью удаления из списка.

Примечание:

Пути расположения каталогов, включенных в **«Белый список программ»** по умолчанию, могут отличаться в случаях:

- установки ОС в другой корневой каталог;
- установки **ARMA IE** в каталог, отличный от предлагаемого по умолчанию.

Для УЗ, имеющей роль «Локальный администратор ОС», ограничения функции **«Белый список программ»** игнорируются в соответствии с параметром **«Разрешить локальному администратору игнорировать правила белого списка»**.

Примечание:

В случае, если каталог одновременно находится в списках функций **«Белый список программ»** и **«Контроль целостности»**, при любом изменении файлов каталога, происходит исключение его из списка функции **«Белый список программ»**.

Для исключения из белого списка файла или каталога, содержащего исполняемые файлы, необходимо выполнить следующие действия:

1. Перейти в раздел меню **«Белый список»**.
2. Нажать **кнопку «Удалить»** напротив файла или каталога, подлежащего исключению, и нажать **кнопку «Сохранить конфигурацию»**.

5.1 Проверка работы функций «Белый список программ»

Для проверки работы функций **«Белый список программ»** необходимо запустить любой исполняемый файл, не находящийся в указанных каталогах.

При попытке запуска исполняемого файла, не находящегося в указанных каталогах, появится информационное сообщение (см. Рисунок – Сообщение об ошибке).

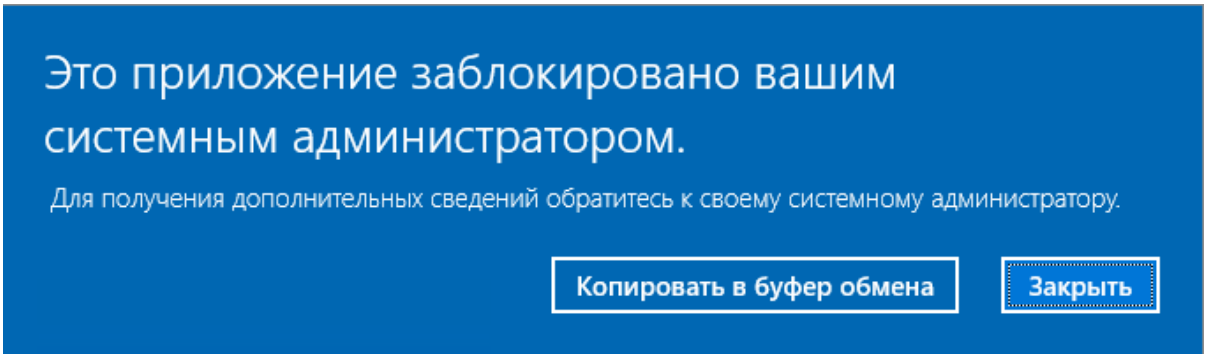

Рисунок – Сообщение об ошибке

6 УПРАВЛЕНИЕ КОНТРОЛЕМ ЦЕЛОСТНОСТИ

Для отслеживания неизменности файлов в **ARMA IE** предусмотрена функция **«Контроль целостности»**.

Управление функцией **«Контроль целостности»** осуществляется одним из следующих способов:

- через единый центр управления **ARMA MC**;
- в локальном графическом интерфейсе **ARMA IE**.

Для включения функции **«Контроль целостности»** и добавления каталога, подлежащего контролю целостности в перечень контролируемых каталогов, необходимо выполнить следующие действия:

1. Перейти в раздел меню **«Контроль целостности»** (см. Рисунок – Контроль целостности), установить флажок для параметра **«Включить контроль целостности»** и нажать **кнопку «Сохранить конфигурацию»**.

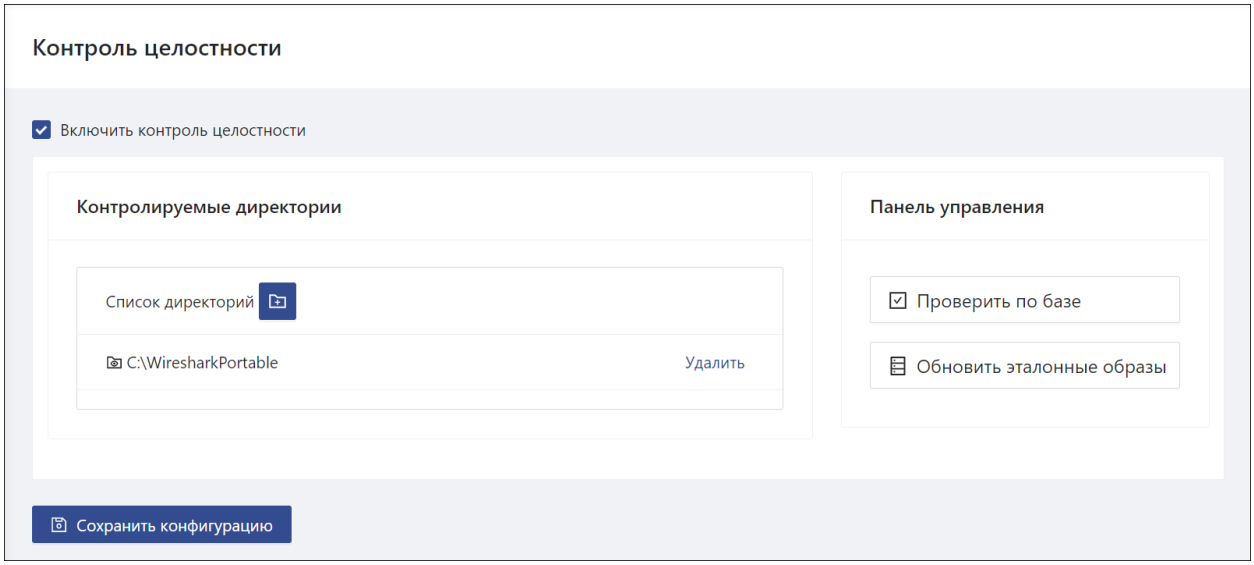

Рисунок – Контроль целостности

2. Нажать **кнопку** «  », в открывшейся форме проводника выбрать каталог, подлежащий контролю целостности, и нажать **кнопку «Выбор папки»**.
3. Нажать **кнопку «Сохранить конфигурацию»**.

При первоначальном добавлении каталогов в перечень контролируемых, необходимо запустить обновление эталонных образов нажатием **кнопки «Обновить эталонные образы»**. В дальнейшем, в случае любых изменений в контролируемых каталогах, необходимо обновлять эталонные образы во избежание блокировки белого списка.

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

Примечание:

При запуске процесса обновления эталонных образов или проверки по базе, возможна блокировка интерфейса **ARMA IE** вплоть до окончания запущенного процесса с выводом соответствующего оповещения (см. Рисунок – Уведомление о процессе обновления эталонных образов, Рисунок – Уведомление о процессе проверки по базе).

7 УПРАВЛЕНИЕ КОНТРОЛЕМ УСТРОЙСТВ

Для ограничения подключаемых USB-устройств и CD/DVD-носителей, в **ARMA IE** предусмотрена функция **«Контроль устройств»**.

Управление функцией **«Контроль устройств»** осуществляется одним из следующих способов:

- через единый центр управления **ARMA MC**;
- в локальном графическом интерфейсе **ARMA IE**.

Для включения функции **«Контроль устройств»** и указания типов контролируемых устройств необходимо выполнить следующие действия:

1. Перейти в раздел меню **«Контроль устройств»** (см. Рисунок – Контроль устройств) и установить флажок для параметра **«Включить управление устройствами»**.

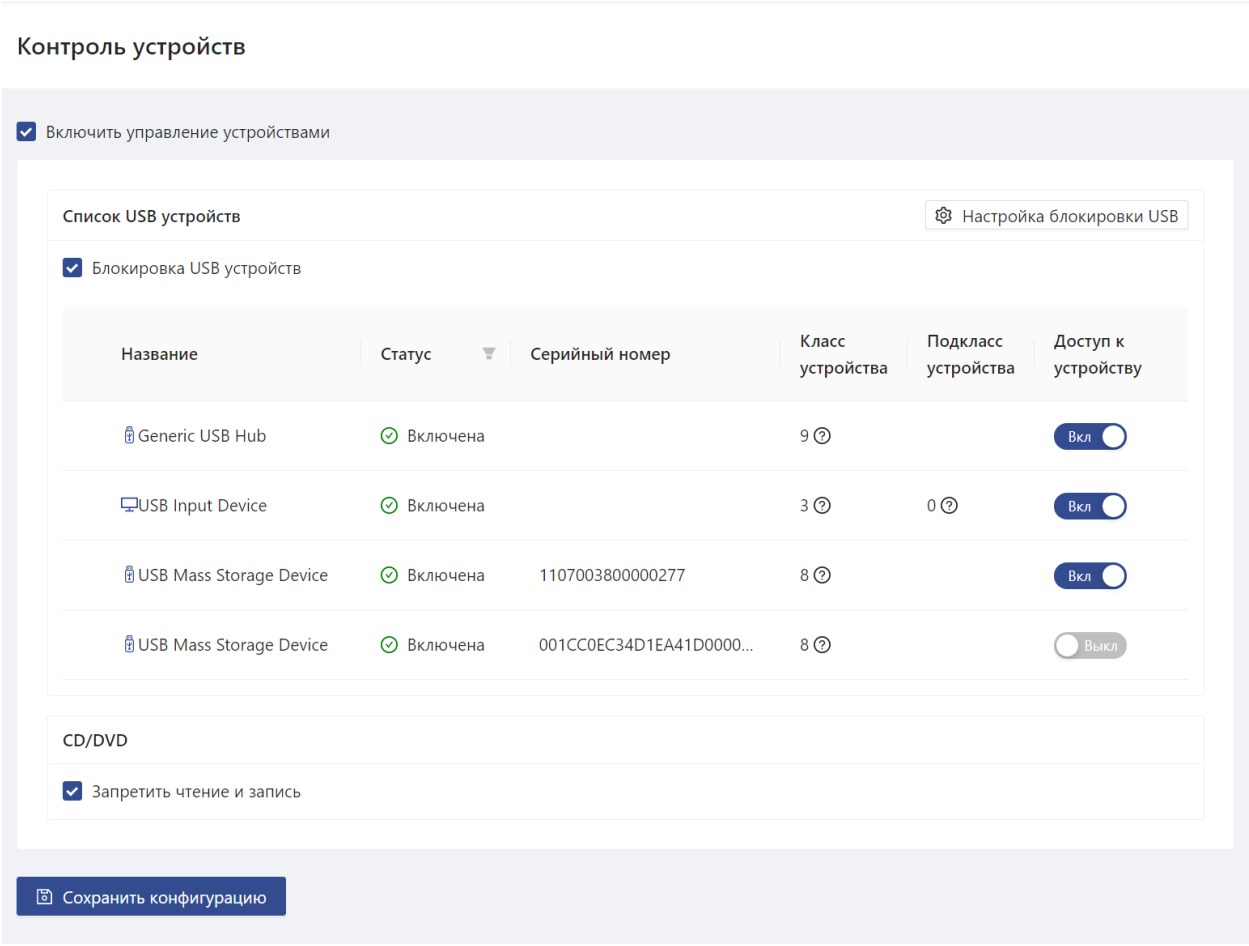

Рисунок – Контроль устройств

2. Установить флажки для выбранных типов контролируемых устройств и нажать **кнопку «Сохранить конфигурацию»**. Установленный флажок параметра **«Запретить чтение и запись»** автоматически блокирует операции чтения и записи для подключаемых CD/DVD-носителей.

В случае необходимости произвести перезагрузку компьютера для принятия изменений, будет выведено соответствующее уведомление (см. Рисунок – Предупреждение о перезагрузке компьютера).

7.1 Настройка блокировки USB-устройств

Настройка блокировки USB-устройств осуществляется в блоке настроек **«Список USB устройств»**.

Подключённые USB-устройства отображаются в виде таблицы.

Для управления доступом к выбранному USB-устройству необходимо установить переключатель в столбце **«Доступ к устройству»** в одно из положений:

- « 

» – для разрешения доступа;
- « 

» – для запрета доступа;

и нажать **кнопку «Сохранить конфигурацию»**.

Примечание:

Положение переключателя разрешает или запрещает доступ всему классу USB-устройств, а не конкретному устройству. Не распространяется на работу с USB-носителями.

В случае работы с USB-носителями, разрешает/запрещает действия с выбранным USB-носителем.

Назначенный режим доступа применяется после переподключения USB-устройства.

Классы USB-устройств, разрешенных к использованию, доступны в форме **«Разрешенные USB устройства»** (см. Рисунок – Разрешенные USB устройства) при нажатии **кнопки «Настройка блокировки USB»**.

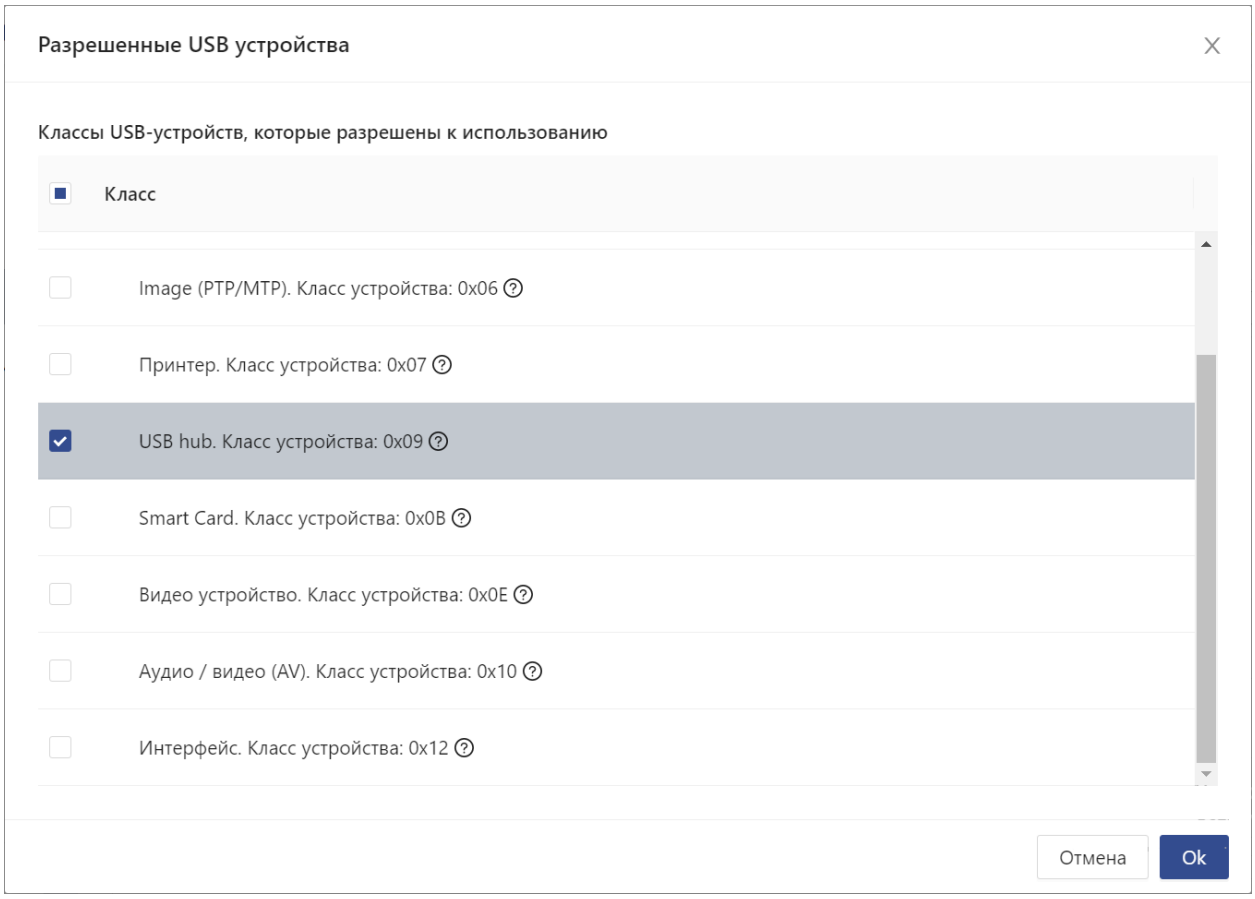

Рисунок – Разрешенные USB устройства

Для разрешения/запрета использования класса USB-устройств необходимо установить/снять флажок для соответствующего класса и нажать **кнопку «Ок»**, а затем **кнопку «Сохранить конфигурацию»**.

В случае необходимости произвести перезагрузку компьютера для принятия изменений, будет выведено соответствующее уведомление (см. Рисунок – Предупреждение о перезагрузке компьютера).

Примечание:

Не гарантируется возможность блокировки USB-носителей без серийного номера.

Блокировка USB сетевых и Wi-Fi адаптеров не поддерживается.

7.2 Проверка работы функции «Контроль устройств»

Заблокированные подключаемые съёмные USB-носители не отображаются в проводнике ОС.

Для проверки блокировки операции чтения для подключаемых CD/DVD-носителей необходимо выбрать подключённое устройство в проводнике ОС – при попытке выбора будет выведено сообщение об отсутствии доступа (см. Рисунок – Всплывающее окно «Расположение недоступно»).

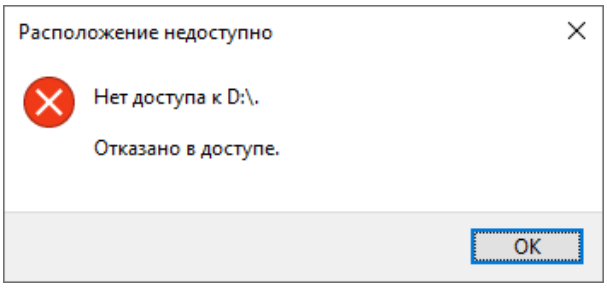

Рисунок – Всплывающее окно «Расположение недоступно»

7.3 Контроль устройств по признаку VID и PID

По признаку VID и PID осуществляется контроль устройств USB-накопителей посредством изменения конфигурационного файла **«config.json»**.

Конфигурационный файл **«config.json»** расположен в каталоге установки (см. Установка сервиса), по умолчанию – «C:\Program Files (x86)\ARMA Industrial Endpoint».

> **Примечание:**
>
> Для того чтобы узнать VID и PID подключенного USB-накопителя, необходимо открыть **«Диспетчер устройств ОС Windows»**, выбрать секцию **«Контроллеры USB»**, в выпадающем списке выбрать **«Запоминающее устройство USB»** и открыть его **«Свойства»**. В открывшемся окне выбрать вкладку **«Сведения»** и выбрать значение **«ИД оборудования»** в выпадающем списке **«Свойство»**.

Для включения USB-накопителя в список разрешенных к использованию USB-устройств по признаку VID и PID необходимо выполнить следующие действия:

1. Включить функцию **«Контроль устройств»** (см. Управление контролем устройств).
2. Открыть текстовым редактором конфигурационный файл **«config.json»**.
3. В секции **«usb_control»** ввести номер разрешенного класса USB-накопителя (например, класс 8 для запоминающего устройства) в параметр **«allowed_classes»** (см. Рисунок – Секция «usb_control»).

```
},
"usb_control": {
    "allowed_classes": [8],
    "enabled": false,
    "hid": {
```

Рисунок – Секция «usb_control»

4. В конце файла, перед последним знаком **«}»**, вставить секцию **«hardware»** (см. Рисунок – Секция «hardware»).

```
"hardware":{

}
```

```
    },
    "hardware":{

    }
}
```

Рисунок – Секция «hardware»

5. Добавить параметры разрешенного к использованию USB-накопителя в секцию **«hardware»** в следующем формате:

```
"allowed_vid" : ["VID"],
"allowed_pid" : ["PID"]
```

где «VID» и «PID» – значения VID и PID разрешенного к использованию USB-накопителя. В случае добавления двух и более USB-накопителей, значения добавляются через запятую в пределах квадратных скобок и обосабливаются кавычками (см. Рисунок – Пример указания значений VID и PID).

```
    },
    "hardware":{
    "allowed_vid":["2385", "2456"],
    "allowed_pid":["1666", "2345"]
    }
```

Рисунок – Пример указания значений VID и PID

Примечание:

VID и PID дополняют проверку USB-накопителей при их подключении, если доступ к этим устройствам был ранее разрешен в разделе **«Контроль устройств»**.

При подключении USB-накопителя, VID и PID которого не указаны в конфигурационном файле, устройство будет запрещено для использования с соответствующей записью в Журнале событий.

6. Сохранить конфигурационный файл **«config.json»**.
7. Перезапустить сервис **ARMA IE** (см. Перезагрузка сервиса ARMA IE).

Для проверки применения конфигурации необходимо проверить записи в реестре ОС Windows в разделе:

- «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ARMA_USB_Filter\USB\hardware».

В данном разделе должны находиться две папки «vid» и «pid» со значениями, введенными в конфигурационный файл.

8 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

В разделе меню **«Настройки»** (см. Рисунок – Настройки) существует возможность выполнять следующие действия:

- перезагружать **ARMA IE**;
- включать режим обучения;
- настраивать сетевой журнал;
- настраивать журналирование.

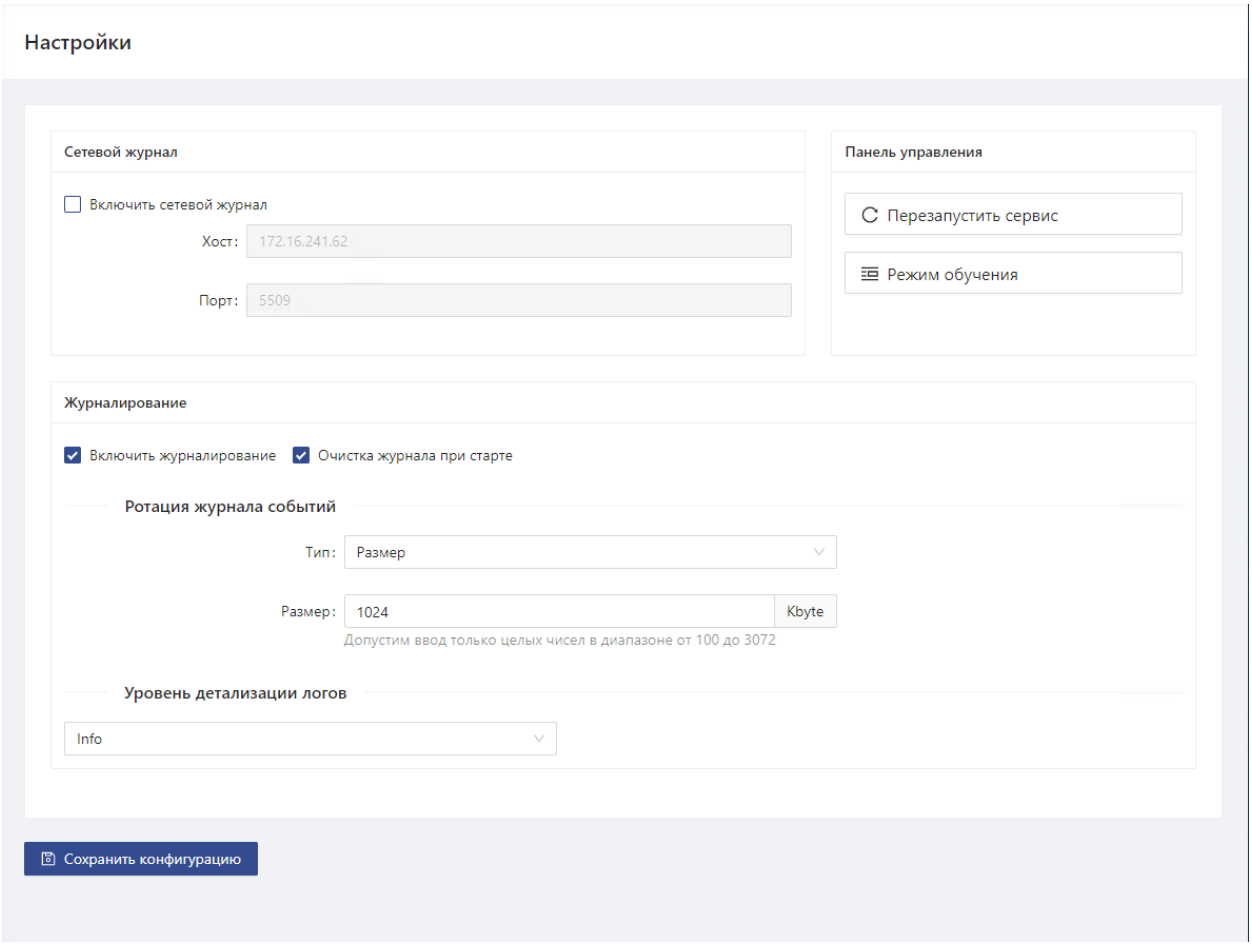

Рисунок – Настройки

8.1 Перезагрузка сервиса ARMA IE

Для перезагрузки сервиса **ARMA IE** необходимо нажать **кнопку «Перезапустить сервис»** в блоке настроек **«Панель управления»** (см. Рисунок – Блок настроек «Панель управления»).

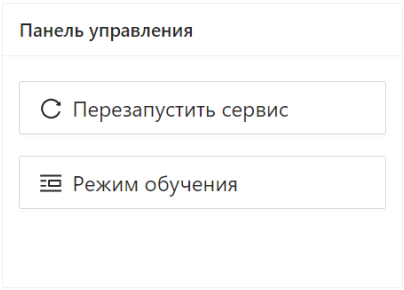

Рисунок – Блок настроек «Панель управления»

8.2 Режим обучения

Для сканирования всего запущенного в данный момент ПО и включения его в список функции **«Белый список программ»** (см. Управление белым списком программ) необходимо нажать **кнопку «Режим обучения»** в блоке настроек **«Панель управления»** (см. Рисунок – Блок настроек «Панель управления»).

После нажатия **кнопки «Режим обучения»** необходимо перейти в раздел меню **«Белый список»** и убедиться в наличии в списке каталогов, содержащих исполняемые файлы запущенного ПО.

8.3 Настройка сетевого журнала

В **ARMA IE** существует возможность экспорта событий по сети.

Для настройки экспорта событий по сети необходимо в блоке настроек **«Сетевой журнал»** (см. Рисунок – Блок настроек «Сетевой журнал») выполнить следующие действия:

1. Установить флажок для параметра **«Включить сетевой журнал»**;
2. Указать значения для параметров:
   - **«Хост»** – IP-адрес устройства, на которое будут отправляться события;
   - **«Порт»** – порт, по которому будут отправляться события, по умолчанию: «5500».
3. Нажать **кнопку «Сохранить конфигурацию»** в нижней части раздела.

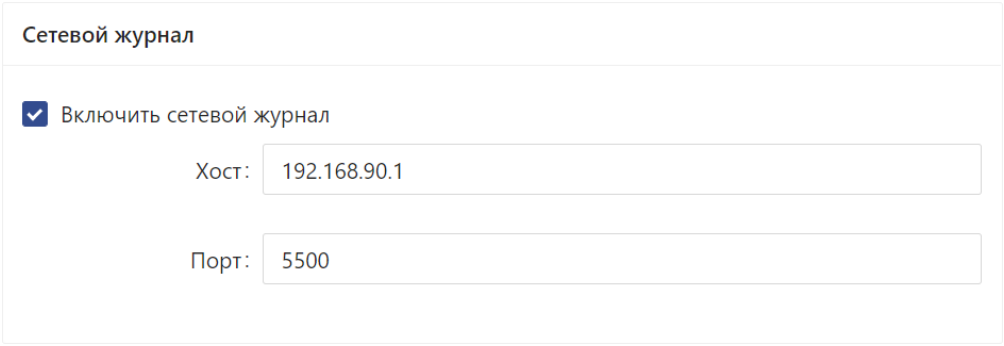

Рисунок – Блок настроек «Сетевой журнал».

8.4 Настройка журналирования

В **ARMA IE** доступны следующие параметры журналирования:

- включение журналирования событий;
- настройка уровня детализации событий;
- настройка ротации журнала событий;
- включение очистки журнала при запуске.

Настройка осуществляется в блоке настроек **«Журналирование»** (см. Рисунок – Блок настроек «Журналирование»).

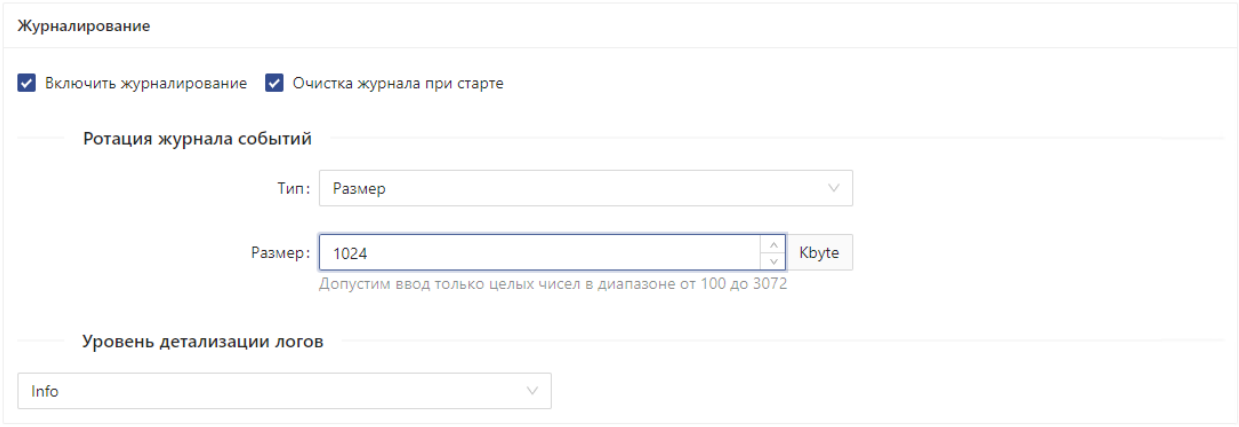

Рисунок – Блок настроек «Журналирование»

При включении журналирования записанные события отображаются в разделе меню **«Журнал»**.

Ротация журнала событий доступна по следующим типам:

- **«Размер»** – размер ротации указывается в поле параметра **«Размер»**;
- **«Время»** – период ротации задаётся с помощью выпадающего списка **«Период»** и указания значения в поле параметра **«Время»**.

Примечание:

Для стабильной работы приложения и экономии ресурсов рекомендуется настроить ротацию журнала событий либо по типу «Размер» со значением по умолчанию, либо по типу «Время» со значением «День».

В выпадающем списке **«Период»** доступны следующие значения:

- «день»;
- «неделя»;
- «месяц».

При выборе периода **«День»** типа ротации **«Время»**, ротация запускается в указанное время, однократно за сутки.

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.

Примечание:

При указании в поле параметра **«Время»** уже прошедшего времени возможны следующие варианты:

- ротации за текущий день ещё не было – ротация будет запущена немедленно;
- ротация за текущий день уже произведена ранее – ротация будет запущена в указанное время, с учетом выбранного значения в списке **«Период»**.

Примечание:

В случае изменения значения в поле параметра **«Время»**, а ротация за текущий день уже была произведена, очередная ротация будет запущена в указанное время следующих суток.

В выпадающем списке **«Уровень детализации логов»** доступны следующие варианты детализации записываемых событий:

- **«Info»** – записывает события информативного характера;
- **«Trace»** – записывает каждое действие **ARMA IE**;
- **«Debug»** – записывает события, считающиеся полезными во время отладки **ARMA IE**;
- **«Warning»** – записывает непредвиденные события, которые в дальнейшем могут нарушить работу одного из процессов **ARMA IE**;
- **«Error»** – записывает прикладные ошибки в работе функциональности **ARMA IE**;
- **«Fatal»** – записывает события, сообщающие о неработоспособности одной или нескольких ключевых бизнес-функций **ARMA IE**;
- **«Panic»** – записывает события об ошибке, прерывающей все сессии **ARMA IE**.

Ротированные записи событий сохраняются в каталог установки **ARMA IE** в формате **«JSON»** в следующем виде:

- «event_log_[Дата][Время]».

9 ПРОСМОТР ЖУРНАЛА СОБЫТИЙ

Для отображения зафиксированных событий безопасности в **ARMA IE** предусмотрена функция **«Журнал»** (см. Рисунок – Журнал).

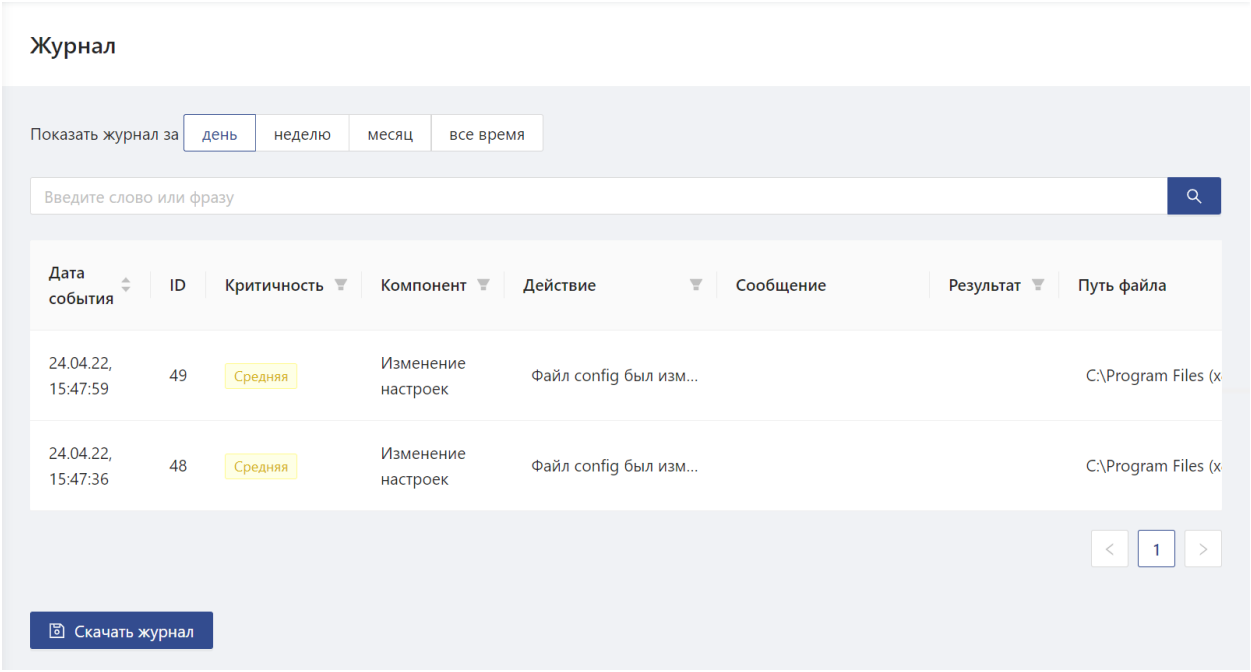

Рисунок – Журнал

События безопасности сортируются по следующим уровням критичности:

- « Высокая » – высокая;
- « Средняя » – средняя;
- « Низкая » – низкая.

Столбцы **«Дата события»**, **«Критичность»**, **«Компонент»**, **«Действие»** и **«Результат»** возможно настраивать нажатием **кнопки** « ».

События безопасности, отображаемые в журнале **ARMA IE**, представлены в таблице (см. Таблица «События безопасности, отображаемые в журнале ARMA IE»).

Таблица «События безопасности, отображаемые в журнале ARMA IE»

Компонент ARMA IE	Действие/результат
Белый список	Файл заблокирован белым списком
Контроль целостности	Файл/папка создана Файл/папка изменена Файл/папка удалена У файла/папки изменено название

Компонент ARMA IE	Действие/результат
Изменение настроек	Файл «config.json» был изменен **ARMA MC** Файл «config.json» был изменен в интерфейсе **ARMA IE**

Существует возможность экспортировать журнал событий нажатием **кнопки «Скачать журнал»**. Экспорт журнала осуществляется в формате **«CSV»** в следующем виде:

- «Industrial Endpoint journal at [Дата], [Время]».

10 ЗАПИСЬ СОБЫТИЙ В ФАЙЛ «ENDPOINT.LOG»

Все регистрируемые **ARMA IE** события сохраняются в файле **«endpoint.log»** и, в случае настроенной синхронизации, отправляются в **ARMA MC**.

События хранятся в виде строк следующего формата:

- «time=[Дата Время] level=[Уровень детализации логов] msg=[Сообщение]».

Примеры основных сообщений, хранимых в файле **«endpoint.log»** представлены в следущем списке:

1. **«Endpoint started»** – Запуск сервиса.
2. **«Restarting Endpoint»** – Перезапуск **ARMA IE**.
3. **«Can’t verify license: license wasn’t started»** – Невозможно проверить лицензию, дата старта лицензии не наступила.
4. **«Control server started on port 4509»** – Сервер управления запущен на порту 4509.
5. **«Config updated»** – Конфигурация обновлена.
6. **«filePath: C:\test.exe reason: Blocked by white list»** – Блокировка файла не добавленного (или заблокированного) в белый список.
7. **«type=USB status=DENIED pid:1666 vid:951 serial_number:E0D55EA574C61750C94C06DC»** – Блокировка устройств девайс контролем.
8. **«Integrity control started»** – Контроль целостности запущен.
9. **«Got event: FILE "Новый текстовый документ (2).txt" CREATE [C:\user\Новый текстовый документ (2).txt]»** - Добавлен новый текстовый документ с названием «Новый текстовый документ (2).txt». При создании файла указывается его первоначальное имя.
10. **«Got event: FILE "Новый текстовый документ (2).txt" RENAME [C:\use\test.txt]»** – Задано имя «test.txt» для созданного документа.
11. **«Got event: FILE "test.txt" WRITE [C:\user\test.txt]»** – Изменение файла «test.txt».
12. **«Got event: FILE "test.txt" REMOVE [C:\user\test.txt]»** – Удален текстовый документ с названием «test.txt».
13. **«Initializing update db»** – Обновление эталонных образов.
14. **«Initializing check from db»** – Инициализация проверки из БД.
15. **«Check done»** – Проверка выполнена.

16. **«msg="Start sync loop"» «func=ModeUpdateFromConsole»** – Запуск синхронизации с **ARMA MC**.
17. **«msg=Start func=LearnProcess»** – Старт тестового режима.
18. **«msg=Finish func=LearnProcess»** – Окончание тестового режима.
19. **«Select debug logging level»** – Указание выбранного уровня логов.
20. **«Syslog init finish. Connected to 192.168.0.68:1800»** – Завершение инициализации системного журнала. Подключено к 192.168.0.68:1800.

11 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

11.1 Уведомление об успешной активации лицензии

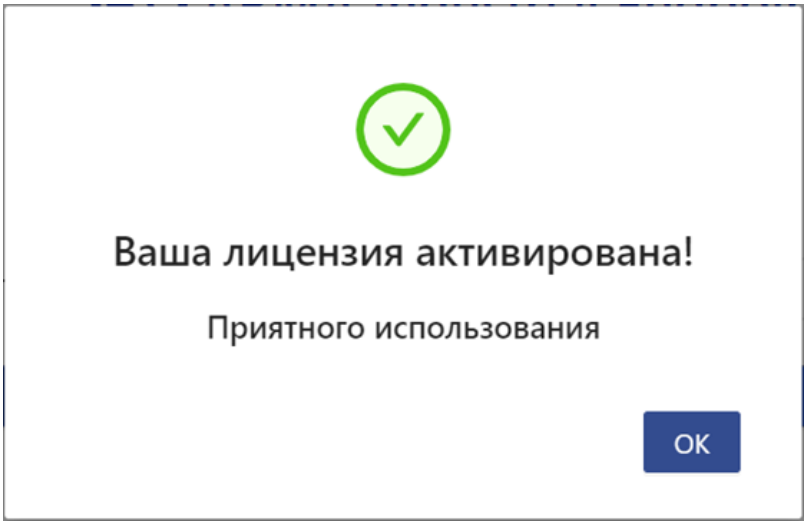

Рисунок – Уведомление об успешной активации лицензии

11.2 Предупреждение о необходимости перезагрузки компьютера

Рисунок – Предупреждение о перезагрузке компьютера

11.3 Уведомление о сохранении конфигурации

Рисунок – Уведомление о сохранении конфигурации

11.4 Уведомление о несохраненных изменениях

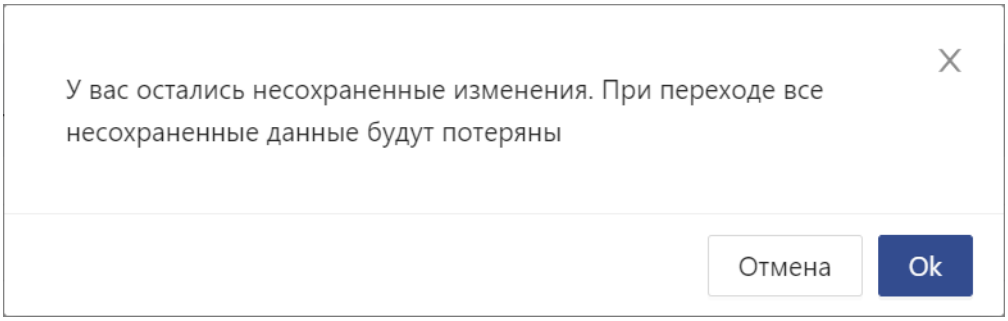

Рисунок – Уведомление о несохраненных изменениях

11.5 Уведомление о перезапуске сервиса

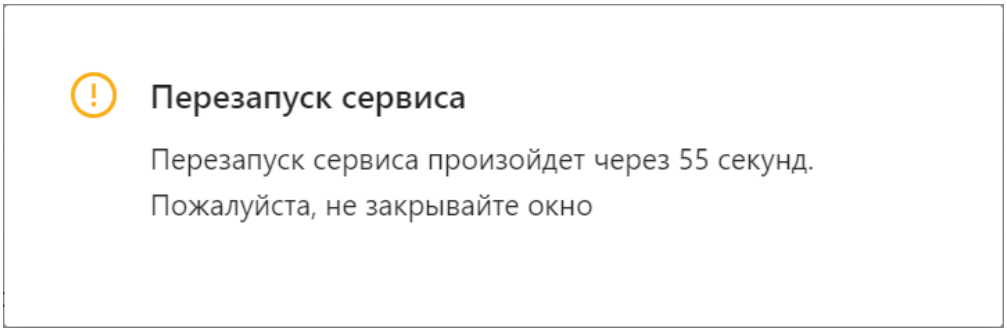

Рисунок – Уведомление о перезапуске сервиса

11.6 Уведомление о запуске проверки режима обучения

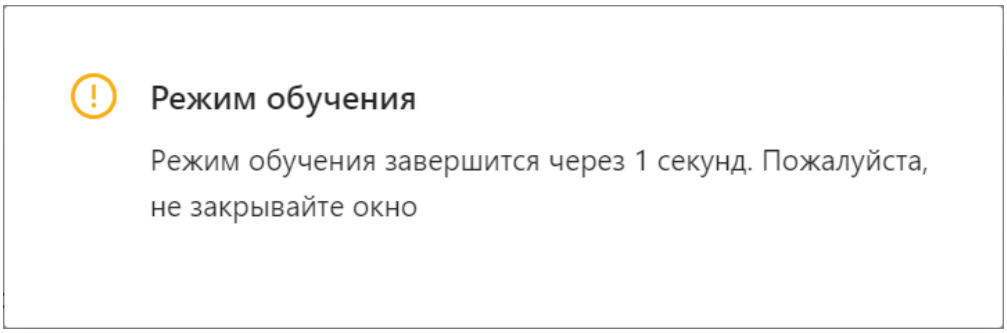

Рисунок – Уведомление о запуске проверки режима обучения

11.7 Уведомление о невозможности распознать файл лицензии

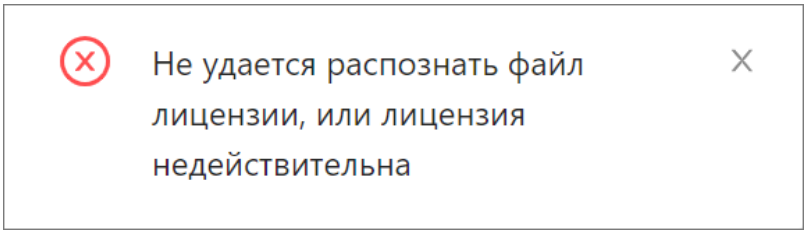

Рисунок – Уведомление о невозможности распознать файл лицензии

11.8 Уведомление о некорректно введенном формате серийного номера

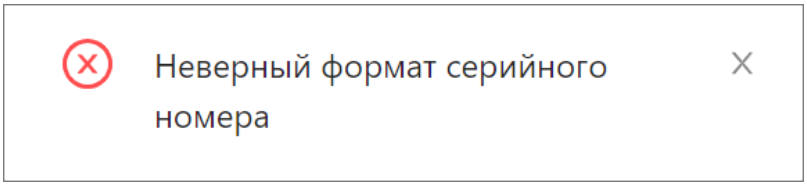

Рисунок – Неверный формат серийного номера

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

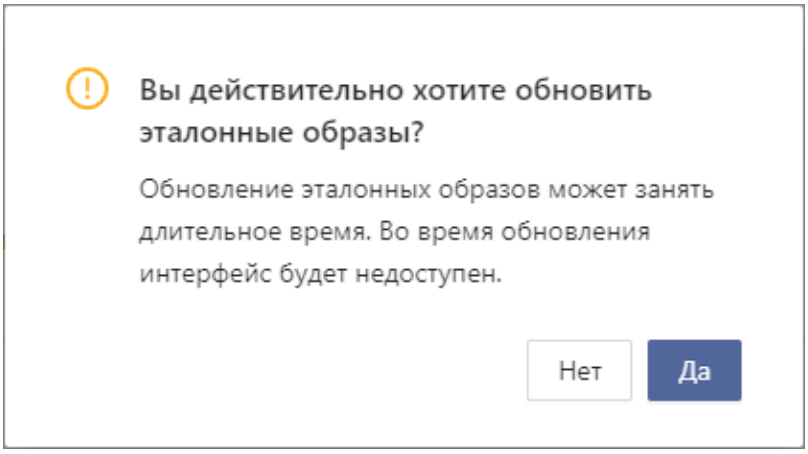

Рисунок – Запрос подтверждения запуска процесса обновления эталонных образов

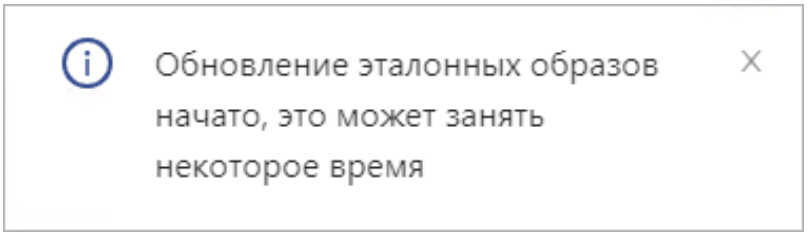

Рисунок – Уведомление о процессе обновления эталонных образов

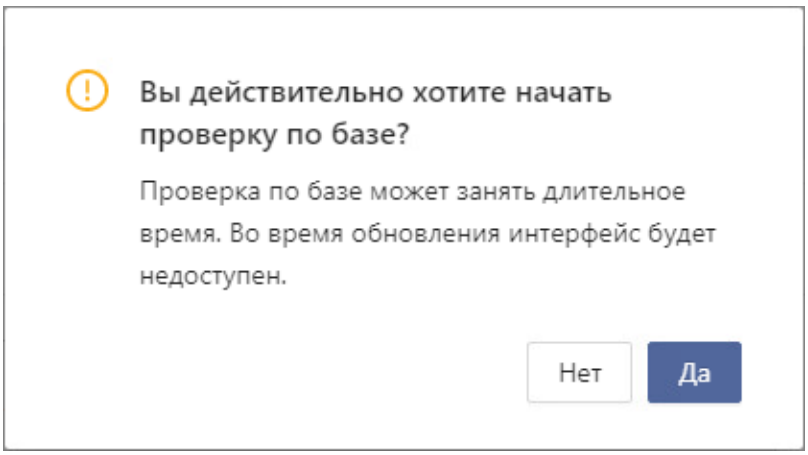

Рисунок – Запрос подтверждения запуска процесса проверки по базе

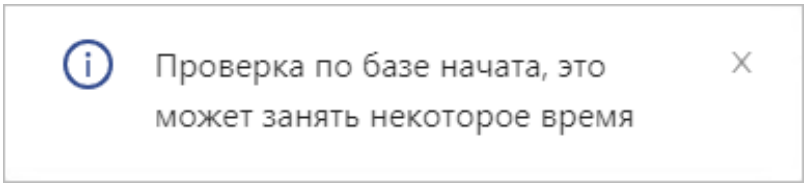

Рисунок – Уведомление о процессе проверки по базе

11.10 Уведомление при разрешении/запрещении локальному администратору игнорировать правила белого списка

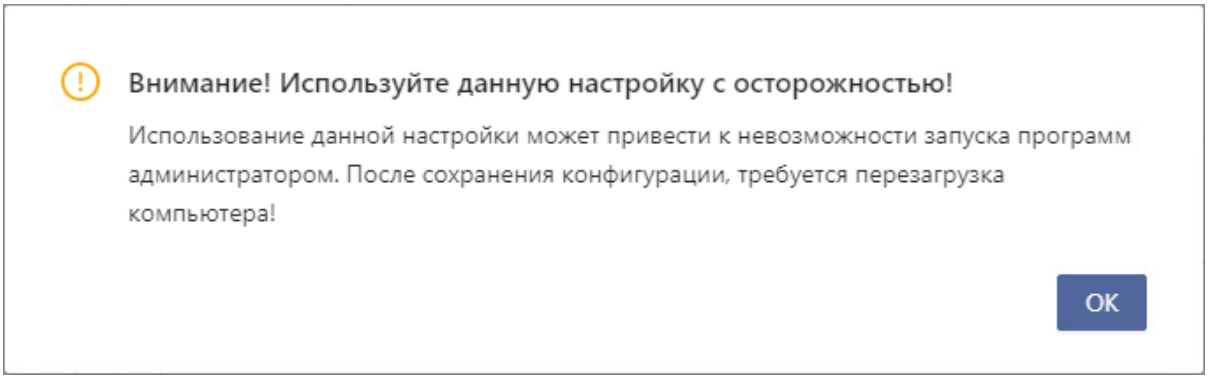

Рисунок – Уведомление при разрешении/запрещении локальному администратору игнорировать правила белого списка