

INFOWATCH ARMA INDUSTRIAL ENDPOINT



Руководство пользователя по эксплуатации

версия 1 ред. от 03.03.2025

Листов 33

СОДЕРЖАНИЕ

1	Об	щие настройки	5
	1.1	Журналирование	6
	1.2	Логирование	6
	1.3	Сетевой журнал	7
	1.4	Ротация журнала	7
2	Ко	нтроль целостности	9
	2.1	Настройка контроля целостности	10
3	Ко	нтроль устройств	12
	3.1	Настройка контроля устройств по типу устройства	15
	3.2	Настройка контроля устройств по конкретному устройству	16
4	Ко	нтроль приложений	19
	4.1	Добавление пути к файлу/директории	20
	4.2	Удаление пути к файлу/директории	21
	4.3	Режим обучения	22
	4.4	Контроль целостности белого списка	24
5	Co	бытия	27
	5.1	Формат вложенного сообщения «cef»	27
	5.1	I.1 Ключи блока « <extension>»</extension>	28
	5.2	Примеры «cef» сообщений	29
	5.2	2.1 Сообщения модуля «Контроль приложений»	29
	5.2	2.2 Сообщения модуля «Контроль целостности»	29
	5.2	2.3 Сообщения модуля «Контроль устройств»	
	5.2	2.4 Сообщение об изменении конфигурационного файла	31
6	Све	едения о лицензии и версии ПО	

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. <u>Таблица «Термины и сокращения»</u>).

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. <u>Таблица «Смежные документы»</u>).

Таблица «Смежные документы»

Сокращенное наименование	Полное наименование
Руководство администратора	Руководство администратора InfoWatch ARMA
ARMA IEL	Industrial Endpoint Linux
Руководство пользователя по	Руководство пользователя по эксплуатации
эксплуатации ARMA MC	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. <u>Рисунок –</u> <u>Общие настройки</u>).

	Администрирование / И	Сточники								Q @	8
+ Добавить 🗇	Удалить 🔘 Копировать	🕃 Скачать 🔅 Загрузит	ь ~ 10 Обновнть -	О Перезагрузить	🕤 🖞 Экспорт 🚺		EL Внешний	Наименование-1	Отменить	Сохранить	0
	Q Craryc: B	ыберите статус 🛛 👻	С: Выберите да	ry 🗉 No		0	Сбросить фильтры	Наименование"			
O ID	Наименование	Статус	Источник	ІР-адрес	Порт	Описание	Дата и 😑	Наименование-1			۲
0 24	123	Отключено	IEW	4,4.4.4	3432		13.12.2024 в	ІР-адрес*			
25	test	Отключено	EL	1.2.3.4	4321		16.12.2024 в	2.2.2.2			Θ
0 26	Наименование-1	Подилючено	(EL	2.2.2.2	7788		16.12.2024 в	Порт			
27	171-2	Подилючено	(EL)	2.3.4.5	5432		16.12.2024 в	7788	DP). Диапазон допустимых	значений от 1500 до	0 65535
								Onscanse Beachre teicr Beachre teicr Beachre teicr Macropolyse	ропа спости	Roman New Alexandria New Alexandria	0 pons bicra
								Версия ПО: 3.0.0 Лицензия: До 02.03.20	25		

Рисунок – Общие настройки

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

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

ARMA) INFOWAT	СН	ARMA			
≡ ©	ARMA MANAGEME CONSO Обзорная панель		Администрирование / Источники / Общие настройки Наименование_2 Общие настройки Наименование_2			Сохранить Сохранить
2	Карта сети Администрирование	~	Журналирование		Ротация	
ي ج ا	Журналы Настройки Лицензии	* *	Включить журналирование Логирование		Тип ротации* Время Период*	•
2	Пользователи	*	Включить логирование Детализация логов () (Info	~	 День Неделя Месяц Время* 00:00:00 	Ø
			 Очистка логов при запуске Сетевой журнал Включить сетевой журнал 		Время дня, когда запустится процесс ротации	
			п∽адрес			
			Протокол передачи данных (UDP). Диапазон допустимых значений от 1 до 65535			

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** <u>Расположение ключевых артефактов ARMA IEL</u>) 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** <u>Управление ARMA IEL с</u> 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. <u>Рисунок Настройка «Контроль целостности»</u>).

	мент DLE Администрирование /	Источники						Q 🕄 😫		
+ Добавить	ј Удалить Q Копировать	 Скачать 🗈 Загрузить 	 Обновить 	 Ø Перезагрузить ~ 	🗄 Экспорт			Наименование-1 Отменить Сохранить О		
Введите текст	Q Craryc:	Выберите статус	С: Выберите да	ту 🗐 По:		8	Сбросить фильтры	Наименование*		
	Наименование	Статус	Источник	ІР-адрес	Порт	Описание	Дата 😑	паименование-1		
O 1	source_1	Отключено	IEL	123.123.123.123	3333		15.01.2025	10.11.192.168		
0 6	SRC-487	Отключено	IEL	172.16.220.108	5506		16.01.2025	Порт*		
07	TECT	Отключено	IEL	33.22.1.2	5277		16.01.2025	(11192		
0 11	181	Отключено	IEL	1.2.3.4	4321		17.01.2025	Протокол передани данных (UDP). Дналазон допустимых значения от 1500 до 65535		
0 12	175	Отключено	IEL	2.3.4.5	5432		17.01.2025	KRIO4		
0 16	Наименование-1	Подключено	IEL	10.11.192.168	11192		20.01.2025	+dsj6elDVHsy8Tf4fOZObcn5FCTl39OCFw==		
								Описание		
								0		
								Общие Контроль Контроль		
								настройки целостности приложений устройств		

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. <u>Настройка контроля целостности</u>).

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.
- Выбрать в открывшемся окне проводника необходимую директорию или файл и нажать кнопку «Выбрать» (см. <u>Рисунок – Добавление пути к</u> <u>файлу/директории</u>).

=		E	Папки	Выбор папки/файла	
O	Обзорная панель		\Box (
	Карта сети		/.cache		
2	Администрирование	^	/bin	> 🔽 🥛 /lib/afick	
	Источники		/boot	> V hib/apt	
			/dev	/lib/aspell	
	Правила корреляции		/etc	V //ib/astra-satepolicy	
	Активы		/home		
	Организация				
	организации				
	Журналы	~	/lib64		
65	Настройки	~	/lost+found		
			/media		
	Системные настройки		/mnt		
	Экспорт		/opt		
	Обновление		/parsec	//ib/cypicedp/cypicases randoms	
	o on obstantia		/parsecfs		
(g)	Лицензии			> /ib/cups	
8	Пользователи	~		> /ib/dbus-1.0	
				> 🔽 🧴 /lib/dpkg	
			⊖ /run	> V hib/emacsen-common	
) /sbin	> 🔽 🦲 /lib/environment.d	
			Srv /srv	N D Antipa A	
			/sys		
			/tmp	Отменить Выбрать	
		ole 1	/usr		

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 USBустройств 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. <u>Рисунок –</u> <u>Настройка «Контроль устройств»</u>).

≡		Администрирование / 🕨	Источники							Q 0 (2
G	+ Добавить 🛈 Удал	ить 🔾 Копировать	🖹 Скачать 🖻 Заг	рузить 🗸 🐧	Обновить ~	💭 Перезагрузить 🗸	🗄 Экспорт			test_1 Отменить Сохранить С
8 8 8	Все NGFW IF Введите текст По: Выберите дату	Виберите статус • С: Виберите дату		8	8		бросить фильтры	Наименование* (test_1 ③) IP-адрас*		
8	םו	Наименов	Статус	Ист	Роль	ІР-адрес	Порт	Описание	Дата 😑	(1.1.1.1
0	0 1	test_3	Отключено	IEL		123.123.12	4444		27.02.2	Πορτ*
0	0 2	test_2	Отключено	IEL		123.123.12	5544		27.02.2	5678 Поллика переодни одному (LIDP). Висполон сопистикных значений от 1500 го 65535
	○ 3	test_1	Отключено	IEL		1.1.1.1	5678		28.02.2	
	4	test_4	Подключ	IEL		172.16.241	5656		28.02.2	U2FsdGVkX1/DAxjNV8+7CcNk3WeUyNICSUbKnYrFU4vRMFnea0m Q
	0 5	test_5	Подключ	N		172.16.230	5679		28.02.2	WeHlzooa/21364L+rJk3Z7H3cx94IqLWRIw==
										Onicanie Basario rosci Degeneration Schare escription escription Regioneration Regione

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. <u>Рисунок – Блок</u> «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).

Азмист MANAGEMENT Азминистрирование / Испочники / Контроль устройств Наименование_1										
Контроль устройств Наименование_1						Отменить	Сохранить			
 Включить контроль подключенных US Запретить доступ на чтение и запись 	В устройств CD/DVD									
Настройка разрешенных USB устр	ойств									
О Типы USB устройств										
Неопределенное USB устройство ()										
Устройство ввода информации 🚯										
Аудио/Видео (камера, наушники, в то	м числе составные устройства) 🕕									
🗌 Накопитель данных (flash-накопитель	и card reader) ()									
Устройство чтения Smart card ()										
USB-xaó 🕕										
Принтер 🕕										
Смартфон 🕕										
Bluetooth										
Подключенные устройства										
 Разрешить Запретить 							т Q			
Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние 🕕	8			
HD Camera Azurewave	Составное устройство	Запрещен	0001	13d3	5476	Подключено	\checkmark			
USB FLASH DRIVE	Накопитель данных (flash-на	Запрещен	1986113241B7	1005	b113	Отключено				
USB PnP Sound Device C-Media	Составное устройство	Запрещен	Не определено	0d8c	013a	Отключено	\checkmark			
						1	-Зиз3 < 1 > 📚			

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. <u>Рисунок – Блок «Подключенные устройства»</u>):

- «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.

яже CONSOLE Азменестрародание / Источники / Контроль устройств Наниенование_1		0 🤋 🙎									
Контроль устройств Наименование_1	Отменить	Сохранить									
Включить контроль падключенных USB устройств Запретить доступ на чтение и запись CD/DVD Настройка разрешенных USB устройств											
О Типы USB устройств											
— Неоградатенное USB устройство 🕜											
🔷 Устройство ввода информации 🕓											
О Аудию Видео (камера, наушники, в том числе составные устройства) 🛈											
○ Наколитель данных (Майн наколитель и саит reader) ○											
O Verpokerso vrewws Smart card 📀											
O USB-sa6 O											
О Принтер О											
Ο Δλαρτφοκι Ο											
O Bluetooth O											
Подключенные устройства											
Разрешить Запретить		or Q									
Устройство Тип устройства Статус Серийный номер VID PID	Состояние 🕕	8									
HD Camera Azurewawe Coctasilioo yctipolicities Sampnum 0001 13d3 5478	Подключено	\checkmark									
USB FLASH DRIVE Haikonstrone gammar Sampnum 198011324187 1005 b113	Отключено										
USB PhP Sound Device C-Media Coctaevoe yctpoiktreo Garpengen He onpegenevo OdBc 013a	Отключено	V									

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. <u>Рисунок – Составное</u> <u>устройство</u>).

Подключенные устройства							
🕑 Разрешить 🛞 Запретить							٩
Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние 🕕	•
HD Camera Azurewave	Составное устройство	Запрещен	0001	13d3	5476	Подключено	\sim
USB FLASH DRIVE	Накопитель данных (flash-на	Запрещен	1986113241B7	1005	b113	Отилючено	_
USB PnP Sound Device C-Media	Составное устройство	Запрещен	Не определено	0d8c	013a	Отключено	~
						1-3 #1 3 < 1	$\rightarrow 2$

Рисунок – Составное устройство



Подключенные устройства							
🕑 Разрешить 🛞 Запретить							٩
Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние 🕕	0
HD Camera Azurewave	Составное устройство	Запрещен	0001	13d3	5476	Подилючено	^
	Аудио/Видео (камера, наушники,	-					
· ·	Bluetooth	-				-	
USB FLASH DRIVE	Накопитель данных (flash-накопи	Запрещен	1986113241B7	1005	b113	Отключено	
USB PnP Sound Device C-Media	Составное устройство	Запрещен	Не определено	0d8c	013a	Отключено	~
						1-3 из 3 🧹 1) *0

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. <u>Рисунок – Контроль</u> <u>устройств по типу устройства</u>):

- 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.

ARMA MANAGEMENT Администрирован	ие / Источники / Контроль устройств На	именование_1				Q	9 🙎
Контроль устройств Наименование_1						Отменить	Сохранить
Включить контроль подключенных US	В устройств						
Запретить доступ на чтение и запись (CD/DVD						
Настройка разрешенных USB устр	ойств						
Типы USB устройств							
Неопределенное USB устройство ())						
Устройство ввода информации 🕕							
Аудио/Видео (камера, наушники, в то	м числе составные устройства) 🕕						
 Накопитель данных (flash-накопитель 	ы и card reader) 🕕						
Устройство чтения Smart card ①							
USB-xa6 🕕							
О Принтер ③							
О Смартфон 🛈							
Bluetooth							
Подключенные устройства							
 Разрешить (8) Запретить 							٩
Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние	0
HD Camera Azurewave	Составное устройство	Запрещен	0001	13d3	5476	Подключено	~
USB FLASH DRIVE	Накопитель данных (flash-на	Запрещен	1986113241B7	1005	b113	Отключено	
USB PnP Sound Device C-Media	Составное устройство	Запрощен	Не определено	0d8c	013a	Отключено	~
						1-3 на	3 < 1 > #

Рисунок – Контроль устройств по типу устройства

После сохранения внесённых изменений появится соответствующее уведомление (см. <u>Рисунок – Изменение статуса устройства</u>). 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.

	Подключенные устройства							
	 Разрешить Запретить 							٩
	Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние 🕕	•
	HD Camera Azurewave	Составное устройство	Запрещен	0001	13d3	5476	Подключено	\sim
	USB FLASH DRIVE	Накопитель данных (flash-накопи	Запрещен	1986113241B7	1005	b113	Отключено	
	USB PnP Sound Device C-Media	Составное устройство	Разрешен	Не определено	0d8c	013a	Отключено	~
_							1-3	на3 < 1 > ≵
\odot	Статус устройства изменен 🛛 🗙						01	2024 InfoWatch ARMA

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. <u>Рисунок – Контроль</u> <u>устройств по выбранному устройству</u>):

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



	ние / Источники / Контроль устройств Наимен	ювание_1				Q ()	2
Контроль устройств Наименование_1						Отменить Сох	ранить
Включить контроль подключенных US Запретить доступ на чтение и запись Настройка разрешенных USB устр	38 устройств CD/DVD ройств						
Типы USB устройств							
 Неопределенное USB устройство)						
🔘 Устройство ввода информации 🕕							
Аудио/Видео (камера, наушники, в то	м числе составные устройства) 🕕						
🥑 Накопитель данных (flash-накопитель	ь и card reader) 🕕						
Устройство чтения Smart card ()							
USB-xaó 🕕							
О Принтер 🕕							
🗌 Смартфон 🕔							
Bluetooth							
Подключенные устройства							
Разрешить Запретить							٩
😑 Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние 🕕	8
HD Camera Azurewave	Составное устройство	Запрещен	0001	13d3	5476	Подключено	~
USB FLASH DRIVE	Накопитель данных (flash-накопи	Запрещен	1986113241B7	1005	b113	Отключено	
USB PnP Sound Device C-Media	Составное устройство	Разрешен	Не определено	0d8c	013a	Отключено	\checkmark
						1-3 xm 3 🔍	1 > 🖈

Рисунок – Контроль устройств по выбранному устройству

3. Нажать кнопку «**Сохранить**».

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



Рисунок – Уведомление об успешном изменении статуса подключённого устройства

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

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



АРМАКТО МАЛАДЕМЕНТ Адаменистрирова	ние / Источники / Контроль устройств Наимен	ювание_1				Ô (3
Контроль устройств Наименование_1						Отменить	охранить
Включить контроль подключенных US Запретить доступ на чтение и запись Настройка разрешенных USB устр	38 устройств CD/DVD ройств						
Типы USB устройств							
 Неопределенное USB устройство 							
🔘 Устройство ввода информации 🕕							
Аудио/Видео (камера, наушники, в то	м числе составные устройства) 🕕						
🥑 Накопитель данных (flash-накопитель	ь и card reader) ()						
Устройство чтения Smart card ()							
USB-xa6 🕕							
🔿 Принтер 🕔							
🔘 Смартфон 🕕							
O Bluetooth							
Подключенные устройства							
Разрешить Sanpeтить							٩
😑 Устройство	Тип устройства	Статус	Серийный номер	VID	PID	Состояние 🕕	9
JD Camera Azurewave	Составное устройство	Разрешен	0001	13d3	5476	Подключено	~
JSB FLASH DRIVE	Накопитель данных (flash-накопи	Разрешен	198611324187	1005	b113	Отключено	
USB PnP Sound Device C-Media	Составное устройство	Разрешен	Не определено	0d8c	013a	Отключено	~
						1-3 из 3	< 1 > 📚

Рисунок – Блокировка устройства

3. Нажать кнопку «Сохранить».

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

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 <u>Контроль устройств</u>).

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»).

	Администрирование / Исто	чники						Q 0 🙎
+ Добавить	Удалить 🔾 Копировать 🕃	Скачать 🕃 Загрузиті	- ^с Обновить с	<i>©</i> Перезагрузить ∨	🗄 Экспорт			Наименование-1 Отменить Сохранить О
Введите текст	Q Статус: Выбе	рите статус 🗸	С: Выберите дату	Ino:			Сбросить фильтры	Наименование* (Наименование-1 ©)
O ID	Наименование	Статус	Источник	ІР-адрес	Порт	Описание	Дата 😕	IP-адрес*
01	source_1	Отключено	IEL	123.123.123.123	3333		15.01.2025	10.11.192.168
6	SRC-487	Отключено	IEL	172.16.220.108	5506		16.01.2025	Πορτ*
07	TECT	Отключено	IEL	33.22.1.2	5277		16.01.2025	11192
0 11	181	Отключено	IEL	1.2.3.4	4321		17.01.2025	протокон передачи данных (ООР), диалазон долустиках эначения от 1000 до 60000
0 12	175	Отключено	IEL	2.3.4.5	5432		17.01.2025	UMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
0 16	Наименование-1	Подключено	IEL	10.11.192.168	11192		20.01.2025	+dsj6elDVHsy8Tl4fOZObcn5FCTl39OCFw==
								Описание
								0
								© Общее кастройки кастройки состаности кастройки контропь контропь состаности контропь состаности контропь состаности контропь состаности контропь состаности контропь состаности состано состаности

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. <u>Контроль целостности</u> <u>белого списка</u>) 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. <u>Рисунок Настройка «Контроль приложений</u>»).
- 2. Установить флажок в чек-бокс параметра «Включить контроль приложений».
- 3. При необходимости снять флажок с чек-бокса параметра **«Разрешить пользователю гоот 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. <u>Рисунок Выбор файла/директории</u>).

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.

Папки	Выбор папки/файла
/ /.cache //bin //boot //dev	 Ibio Ibio
/etc /home /ib	> > > > > > > > > > > > > > > /lib/chromium > > /lib/compat-ld
 /lib64 /lost+found /media 	 У Ib/console-setup У Ib/console-setup Ib/console-setup Ib/console-setup Cимволическая ссылка Директория (раскрыто) Ib/consoleton (advance of the consoleton)
/mnt /opt /parsec	У /шб/стуртевир/акраз У /шб/стуртевир/акраз Директория У /шб/стуртевир/спиртевир/спир
/parsecfs /proc /root	 > /lib/cryptsetup/scripts > /lib/cups > /lib/dbus-1.0
/run /sbin /srv	 /lib/dpkg /lib/emacsen-common /lib/environment.d
/sys /tmp /usr	Отменить Выбрать

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. <u>Рисунок – Удаление</u> критических директорий).

АЛАКСЕ МАЛАСЕМЕНТ Администрарование / Источники / Контроль приложений Наименование-			Q 🕄 😫
Контроль приложений Наименование-1			Отменить Сохранить
Вилочить контроль приложений Разрешить пользователю гоот инкорнровать правила белого слижа Режим обучения Провежутся времени для режима обучения 00:05:00 0			
+ Добавить 🦿 Удалить 🕗 Разрешить 🛞 Вилючить 🛞 Выялючить			
Путь к файлу/папке	Удаление выбранного пути может нарушить работу	Контроль целостности файла/палки 🕥	6
🥑 /usr 🛈	операционной системы и IEL. Вы действительно хотите совершить действие?	Выялючено	
Iroot 🧿	Отменить Удалить		
🔿 /usr/bin/su		Выетночено	
/usr/bin/bash	Новый	Выятночено	
/usr/bin/kate	Новый	Выключено	

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).

Алико Манадемент Адинистрорование / Источники / Контроль приложений Наименование-	I.		Q 🛛 🖉
Контроль приложений Наименование-1			Отменить Сохранить
Вилочить контроль приложений Разрежить пользоватило гоот инсонтроваль правила белого слиска Реких обучения Промежуток времени для режима обучения 000500 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
никовани список + Добавить 🗘 Удалить ⊘ Разрешить 🛞 Вилючить 🛞 Вылючить			Веедите текст Q
О Путь к файлу/папке	Статус 🕠	Контроль целостности файла/палки 🕠	0
/root 📀	Разряшен	Выключено	
/lib/systemd/system ()	Разрешен	Выключено	

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).

🕷 INFOWATCH ARMA

АНАСТ МАНАСЕМЕНТ Азакнострирование / Источнии / Контроль приложений Наименования	e1		Q 0 🙎
Контроль приложений Наименование-1			Отменить Сохранить
Включить контроль приложений Разрешить пользователю гост инкорировать правила белого слнока Режим обучения Провимуток времени для режима обучения 00.05.00 О Продокительность рожена обучения. Декладок эканемий с 00.01.00 ло 23.55.50 Белый список			
+ Добавить 🖞 Удалить 🕝 Разрешить 💿 Включить 💿 Вкалючить			Введите текст Q
Путь к файлу/палке	Статус 🕔	Контроль целостности файла/палки 🕕	3
 Πуτь κ φαλληγίπαπα /root Ο 	Статус () (Разрешен	Контроль целостности файла/папки 🕥	0
 Νγτь κ φαληγίπατικε /root Ο Justribinisu 	Статус () (Разрицея) (Нозмай)	Контроль целостности файла/палки () (Виллочно) (Виллочно)	Θ
 Pyrs κ φάκιγ/name /root /usr/bin/su /usr/bin/sah 	Crarye () (Papuae Hossi Hossi	Контроль целостности файла/палки () Выточето Выпочето Вылючето	0
	Crarye () (Pappuon Honul Honul Honul	Контроль целостности файлаїлання () (Вылочено (Вылочено (Вылочено (Вылочено (Вылочено)	0
	Crarye () (Pospuso) (Honul (Honul) (Honul) (Honul)	Контроль целостности файлаїлания () Вылочено Вылочено Вылочено Вылочено Вылочено Вылочено	0
	Crarye () (Pospusor) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus)	Контроль целостности файла/палки () Вылочено Вылочено Вылочено Вылочено Вылочено Вылочено Вылочено Вылочено	0
	Cranye () (Pospuso) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus)	Контроль целостности файла/палки Вылочено Вылочено В	0
	Cranye () (Pospusor) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus) (Honus)	Контроль целостности файла/палки () Вилочено	0

Рисунок – Обучение завершено

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

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

Примечание:

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

()	Запущен режим обучения на 1 источнике: Наименование-1 . Настройка модуля временно недос	тупна					
Ξ	акий Манадемент CONSOLE	ave-1		Q (2		
0	Контроль приложений Наименование-1						
8 E 8	Велочить нонтроль пригожений Разрешить пользоватално тоот инкорнораать правила белого сликова Ремим обучения Променуток времени для ражима обучения ОООТО Прадоличтетичисть ремика обучения. Дналавон значений с 00.01.02 по 23.09 с5 Еслый список	00.00.59					
					٩		
	Путь к файлу/палке	Статус 🕢	Контроль целостности файла/папки 🕡		0		
	/root 🛈	Разрешен	Выключено				
	/lib/systemd/system ()	Разрошем	Выключено				

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. <u>Рисунок – Включение</u> КЦ).

Алико МАНАСЕМЕНТ Адаминстрирование / Источники / Контроль приложений Наи	менование-1		Q 0 😫
Контроль приложений Наименование-1			Отменить Сохранить
 Включить контроль приложений Разрешить пользователю гоо! игнорировать правила белого списка 			
Режим обучения			
Проиекуток времени для режима обучения 00:01:00 Прадплянатичность ремика обучения. Днападон эконений с 00:01:00 по 23:95:59 Белый список	ипь		
+ Добавить 🗇 Удалить 📀 Разрешить 💿 Включить 💿 Выключить			Введите текст Q
Путь к файлу/папке	Статус 🕕	Контроль целостности файла/палки 🔘	9
/mnt	Разрешен	Выключено	
/usr 🗿	Разрешен	Выключено	
/root 🧿	Разрешен	Выключено	
/lib/systemd/system ()	Разрешен	Выклочено	

Рисунок – Включение КЦ

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

Модуль Контроль целостности не активен	
Хотите его активировать?	
Отменить 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. <u>Рисунок – Статус КЦ</u>).

макадемент CONSOLE Администрорование / Источники / Контроль приложений Нанискование-1									
Контроль приложений Наименование-1			Отменить Сохранить						
Вилочить контроль приложений Разрешить лользователю гост инкорировать правила белого списка Режим обучения Промежуток времени для режима обучения 00.01.00 Прастиктельность режима обучения. Диалазон значений с 00.01.00 по 23.95.99 Белый список									
+ Добавить 🕆 Удалить 📀 Разрешить 💿 Включить 💿 Выключить			Введите текст Q						
О Путь к файлу/папке	Статус 🕟	Контроль целостности файла/папки 🕠	0						
⊖ /mnt	Разрошен	Вилючено							
🔿 /usr 🧿	Разрошен	Выключено							
🔿 /root 🧿	Разрешен	Выключено							
/lib/systemd/system ()	Разрошен	Выключено							

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»;

ARMA

- «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 «сеf» 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 «1111а», 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 «1111а», 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-controlconfig.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-e	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. <u>Рисунок – Сведения о лицензии и версии ПО</u>).

Примечание:

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

≡		Админист	рирование / Источн	ники									Q 💿 🙎
O	Обзорная панель	+ д	+ Добавить 🗇 Удалить 🖓 Копировать 🗈 Скачать 🕒 Загрузить 🗸							TEST1		Отменить	Сохранить
\square	Карта сети	00	🕤 Обновить 🗸 🎵 Перезагрузить 🗸 🏦 Экспорт							Порт*			
8	Администрирование ^	Bos	Bce NGFW IFW IEW IEL Внешний							43211			
	Источники			٩				осить фильтр	ы	Протокол передачи да	нных (UDP). Диапа:	зон допустимых значен	ий от 1500 до 65535
	Правила корреляции	Стату	с: Выберите ста	атус 🗸						Ключ 🕕			
	A	C :								U2FU2FVkX1+1X C9P1mwUs+JviF	(FHrb3/713gAv28 648QD28GLNNIr	QA8XqmJppdwV+sC xB9YnosaQ==	zUzLGm 🛛 🗘
	Организация	По:											
Ψ	Журналы 🗸	0	р н	. C	и	I	п	o	•				
\ (2)	Настройки 🗸	0.1	123			12	2222		3	Описание			
5	Лицензии		120			10	1001		0				
0		0 5	test	t <u> </u>	l	1.2	4321		3				
0	TIOIBSOBATEIN	0 6	Ha.	0)	L	10	12		3				
		0 8	Ha.		I	10	13		3				
		01	0 DE.	0	I	11	44		0		m	A	
		0 1	5 DC	0	I	17	11		0	(\$) (\$)			"
		0 1	8 Lo	0	I	2.2	8765		0	Общие настройки	Контроль целостности	Контроль приложений	Контроль устройств
		0 1	9 TE.	n	I	1.2	43		0				
										Берсия ПО: 3. Лицензия: До	0.0 07.03.2025		
							1-	8 из 8 < 1	-0-				

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. <u>Рисунок – Лицензия не активирована</u>).

≡		ENT LE	Администрирование	Э / Источники								Q ()	Q	
O	Обзорная панель		+ Добавить 🗇 Удалить 🖓 Копировать 🕃 Скачать 🔄 Загрузить 🗸							test	Отменить Сохранить) (
	Карта сети		🗇 Обновить	🕤 Обновить – 🖉 Перезагрузить – 🛧 Экспорт							test		\times	
8	Администрирование	^	Все NGFW IFW IEW IEL Внешний											
	Источники		Введите тек		٩			D Cóp	осить фильт	ры	1.2.3.4		×	
	Правила корреляции		Статус: Вы		×									
	Активы		С: Выберит								4321			
	Организация		По: Выбери								Протокол передачи данных (JDP). Диапазон допустимых значений от 1500 до 6	553	
Ũ	Журналы	~		н	c	И	I	п	o		Ключ 🤅			
\$	Настройки	~	0.1	123	0)	I	12	3333		3	U2FU2FVkX1+174NJiY xGN9UcxOnIn+tcC8UK	2NJjTCMstGSc+wa9Dk2h0O8f0A7/60FQDv zoBx9+RQCT6dKAw==	Q	
្វើ	Лицензии		0.5	test	0	- Lui	1.2	4321		3				
00	Пользователи	\sim	0.6	На	0		10	12		3				
			0.	Ha			10	12		2	Описание			
			0.40	DE	0		10	10		0	Введите текст			
			0 10	DE	0	· · ·	11	44		0				
			0 15	DC	0		17	11		0				
			0 18	Lo	0	l	2.2	8765		0				
			0 19	TE	П	I	1.2	43		0			_	
											 Версия ПО: 3.0.0 Лицензия: Не опреде 	лено		
								1	8из8 (1	> :8:				

Рисунок – Лицензия не активирована