



INFOWATCH ARMA

Система защиты информации АСУ ТП



Техническое описание линейки продуктов InfoWatch ARMA

версия 14 ред. от 21.06.2022

Листов 45

ОГЛАВЛЕНИЕ

Термины и сокращения	3
Аннотация.....	6
1 InfoWatch ARMA	7
2 InfoWatch ARMA Industrial Firewall	9
2.1 Технические требования	9
2.1.1 Требования к аппаратной платформе	9
2.1.2 Требования к виртуальной платформе	10
2.2 Функции	10
2.3 Поддерживаемые промышленные протоколы.....	15
2.3.1 Варианты использования функций ограничения	23
2.4 Варианты применения	23
2.4.1 На границе с корпоративным сегментом.....	23
2.4.2 Связь с технической поддержкой	24
2.4.3 Связь со смежными АСУ ТП	25
2.4.4 Мониторинг внутри АСУ ТП	26
2.5 Обнаруживаемые атаки	26
2.6 Описание аппаратных конфигураций	27
2.7 Лицензирование.....	30
3 InfoWatch ARMA Management Console	36
3.1 Технические требования	36
3.1.1 Требования к аппаратной платформе	36
3.1.2 Требования к виртуальной платформе	36
3.2 Функции	37
3.3 Варианты применения	40
3.4 Лицензирование.....	42
4 InfoWatch ARMA Industrial Endpoint	43
4.1 Технические требования	43
4.2 Функции	43
4.3 Варианты применения	45
4.4 Лицензирование.....	45

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Таблица 1
Термины и сокращения

Термины и сокращения	Значение
АСУ ТП	Автоматизированная система управления технологическим процессом
ИБ	Информационная безопасность
МЭ	Межсетевой экран
МЭК	Международная электротехническая комиссия
ОС	Операционная система
ПЛК	Программируемый логический контроллер
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
APCI	Advanced Configuration and Power Interface, усовершенствованный интерфейс управления
APDU	Application Protocol Data Unit, протокольный блок данных прикладного уровня
API	Application Programming Interface, программный интерфейс приложения
ARMA IE	ARMA Industrial Endpoint
ARMA IF	ARMA Industrial Firewall
ARMA MC	ARMA Management Console
CIP	Common Industrial Protocol, общий промышленный протокол
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
GOOSE	Generic Object-Oriented Substation Event, общее объектно-ориентированное событие на подстанции
FTP	File Transfer Protocol, протокол передачи файлов по сети

Термины и сокращения	Значение
HTTPS	HyperText Transfer Protocol Secure, расширенный протокол HTTP
ICAP	Internet Content Adaptation Protocol, протокол адаптации контента Интернета
IEC	International Electrotechnical Commission, Международная электротехническая комиссия
ID	Идентификатор
IOA	Information Object Address, адрес объекта информации
IP	Internet Protocol, межсетевой протокол
LDAP	Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам
MMS	Manufacturing Message Specification, протокол передачи данных по технологии «клиент-сервер»
NAT	Network Address Translation, преобразование сетевых адресов
NTP	Network Time Protocol, протокол сетевого времени
OPC	Open Platform Communications, семейство технологий управления объектов автоматизации
OSPF	Open Shortest Path First, протокол динамической маршрутизации
PAT	Port Address Translation, трансляция порт-адрес
RIP	Routing Information Protocol, протокол маршрутной информации
SCADA	Supervisory Control And Data Acquisition, диспетчерское управление и сбор данных
SMB	Server Message Block, сетевой протокол прикладного уровня для удалённого доступа к файлам
SNMP	Simple Network Management Protocol, простой протокол сетевого управления
SSH	Secure Shell, безопасная оболочка
TCP	Transmission Control Protocol, протокол управления передачей

Термины и сокращения	Значение
VLAN	Virtual Local Area Network, виртуальная локальная сеть
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети
WAN	Wide Area Network – глобальная вычислительная сеть

АННОТАЦИЯ

Настоящее техническое описание предназначено для ознакомления с системой защиты информации **InfoWatch ARMA** и описывает общую схему взаимодействия, технические требования, функции, варианты применения, а также обнаруживаемые атаки.

1 INFOWATCH ARMA

InfoWatch ARMA – это отечественная система (см. [Рисунок 1](#)) для защиты информации в автоматизированной системе управления технологическим процессом (АСУ ТП), выполняющая следующие функции:

- блокировка атак на сетевом уровне и уровне конечных станций;
- создание замкнутой безопасной среды;
- снижение ресурсов на мониторинг;
- защита от таргетированных (APT) атак;
- обеспечение выполнения приказов ФСТЭК России.

Все продукты интегрированы между собой и могут эксплуатироваться как по отдельности, так и в составе комплексной защиты InfoWatch ARMA.

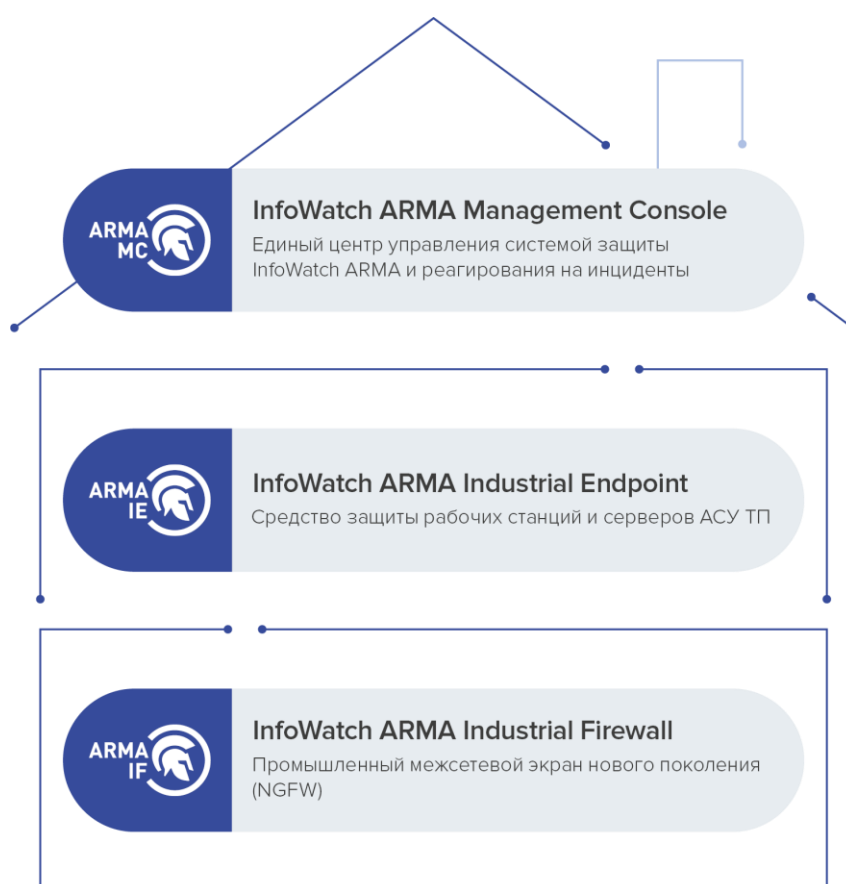


Рисунок 1 – Отечественная система защиты информации InfoWatch ARMA

1. InfoWatch ARMA Management Console.

Единый центр управления решениями InfoWatch ARMA и реагирования на инциденты.

2. InfoWatch ARMA Industrial Endpoint.

Решение по защите рабочих станций и серверов SCADA. Обеспечивает замкнутую защищенную среду за счет обеспечения контроля целостности, запуску ПО по белому списку, контролю подключения съемных носителей, антивирусной защите.

3. InfoWatch ARMA Industrial Firewall.

Промышленный межсетевой экран нового поколения с системой обнаружения вторжений (IDS/IPS) и VPN, обеспечивающее предотвращение угроз для критически важных инфраструктур и промышленных систем управления. Имеет возможность экспорта событий информационной безопасности (ИБ) в SIEM/SOC. Сертифицирован во ФСТЭК по ИТ.МЭ.Д4.ПЗ, ИТ.СОВ.С4.ПЗ, 4УД.

4. Центр экспертизы.

Команда экспертов InfoWatch более 10 лет реализовывала проекты на стороне заказчиков, вендоров и интеграторов и вложила свой опыт в разработку технологий защиты АСУ ТП.

На текущий момент времени реализованы следующие модули:

- InfoWatch ARMA Management Console;
- InfoWatch ARMA Industrial Endpoint;
- InfoWatch ARMA Industrial Firewall;

Общая схема применения InfoWatch ARMA представлена на рисунке (см. [Рисунок 2](#)).

Надежная производительность и мощное централизованное управление обеспечивают непревзойденную ценность в простом, универсальном решении.

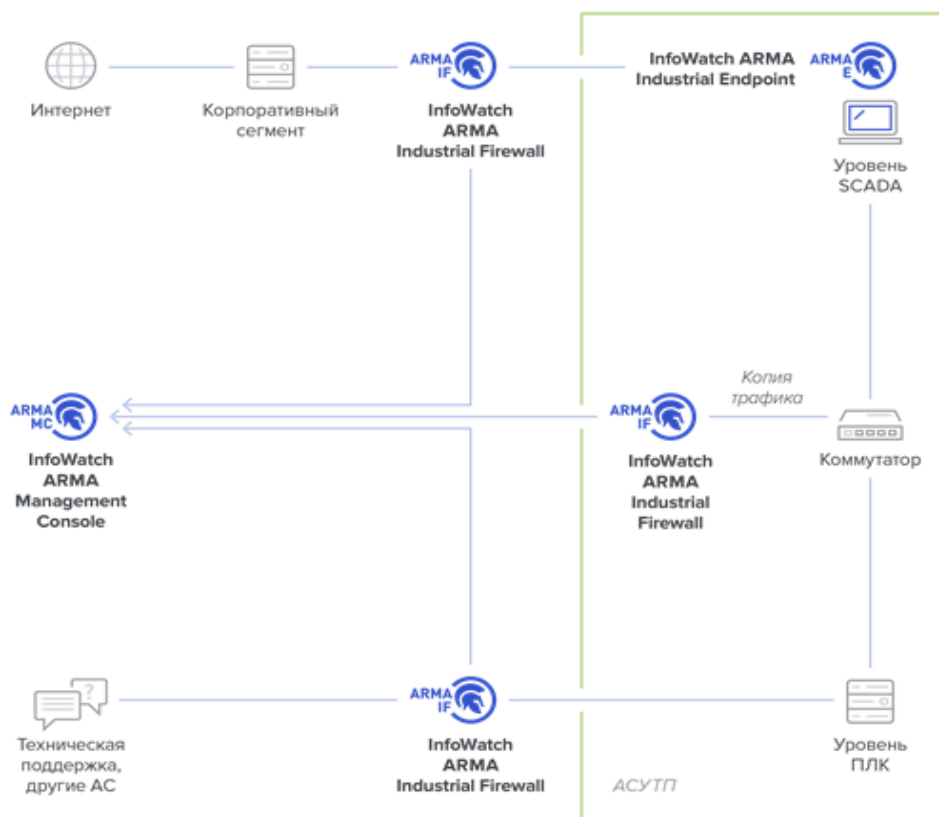


Рисунок 2 – Общая схема применения InfoWatch ARMA

2 INFOWATCH ARMA INDUSTRIAL FIREWALL

2.1 Технические требования

Установка **ARMA IF** производится на следующие типы платформ:

- аппаратная;
- виртуальная (гипервизор).

Установка на аппаратную платформу выполняется с использованием USB-накопителя, на который должен быть записан образ **ARMA IF** в формате «***.IMG**».

Установка на виртуальную платформу (гипервизор) производится с помощью образа в формате «***.ISO**».

2.1.1 Требования к аппаратной платформе

При установке **ARMA IF** на аппаратную платформу необходимо использовать микропроцессорную архитектуру **x86** или **x64**.

Для аппаратной платформы, на которую устанавливается **ARMA IF** достаточно руководствоваться минимальными требованиями к аппаратному обеспечению.

Для обеспечения корректного функционирования ПО и общей пропускной способности **ARMA IF** 150 Мбит/секунду при работе функций межсетевого экрана, системы предотвращения вторжений (COB) к оборудованию предъявляются минимальные требования, которые представлены в таблице (см. [Таблица 2](#)).

Таблица 2
Минимальные требования к оборудованию

Название оборудования	Требования
Процессор	2,0 ГГц, двухъядерный, x86 или x64
ОЗУ	8 ГБ
Интерфейсы, необходимые для установки программного обеспечения	Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры
Жесткий диск	120 ГБ, SSD
Сетевые интерфейсы	Не менее 2 x Ethernet 10/100/1000 Мбит/сек

Для корректного отображения веб-интерфейса к веб-браузерам предъявляются следующие требования:

- а. для ОС семейства Windows:
 - Chrome, Firefox;

- b. для ОС семейства Linux:
 - Chrome для Linux, Firefox для Linux.

2.1.2 Требования к виртуальной платформе

Виртуализация **ARMA IF** поддерживается для следующих виртуальных платформ (гипервизоров):

- HyperV Generation 1;
- VirtualBox версии 6.0.4 и выше;
- VMware ESXi версии 5.5 обновления 2 и выше.

ARMA IF может быть установлен на все среды виртуализации, которые поддерживают FreeBSD версии 11.1.

Для запуска **ARMA IF** предъявляются следующие минимальные требования к виртуальной среде:

- количество процессоров: 1;
- объем оперативной памяти: 4 ГБ;
- размер виртуального диска: 25 ГБ;
- количество сетевых интерфейсов: не менее 2.

В такой конфигурации производительность **ARMA IF** обеспечивает обработку трафика не более 30 Мбит/секунду при работе функций межсетевого экрана и системы предотвращения вторжений (COV). При необходимости хранения большого количества записей журналов, необходимо руководствоваться минимальными требованиями к аппаратной платформе в разделе 2.1.1.

Для корректного отображения веб-интерфейса к веб-браузерам предъявляются следующие требования:

- c. для ОС семейства Windows:
 - Chrome, Firefox;
- d. для ОС семейства Linux:
 - Chrome для Linux, Firefox для Linux.

2.2 Функции

Функции **ARMA IF** приведены в таблице (см. [Таблица 3](#)).

Таблица 3
Функции ARMA IF

№ п/п	Функционал	Комментарий
Межсетевого экран		
1.	Контроль доступа пользователей к сетевым ресурсам, указание срока действия учетной записи пользователя (Портал авторизации)	

№ п/п	Функционал	Комментарий
2.	Контроль доступа пользователей локальной сети к ресурсам Internet (URL-фильтрация)	
3.	Фильтрация сетевого трафика с учетом параметров пакета на сетевом и транспортном уровнях	
4.	Точная идентификация, классификация и предотвращение проникновения вредоносного трафика, включая червей, вирусов, сетевых атак и т.п.	
5.	Соккрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)	
6.	Возможность задания расписания срабатывания правил	
Система обнаружений вторжений		
7.	Обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровне	
8.	Обновление базы решающих правил	Локально, централизованно, по протоколам: FTP, SMB
9.	Возможность разработки пользовательских правил COB	Формат правил – Snort совместимый
10.	Возможность задания расписания срабатывания правил	
Сетевые функции		
11.	Возможность работы в режиме прозрачного моста	
12.	Поддержка статической маршрутизации	
13.	Поддержка протоколов динамической маршрутизации	Поддерживаемые протоколы маршрутизации: RIP, OSPF
14.	Прокси сервер	
15.	Поддержка VLAN IEEE 802.1q	
16.	DHCP сервер	
17.	Функции QoS (Traffic Shaping)	
18.	Возможность зеркалирования сетевого трафика на отдельный порт	
19.	Функционирование DNS клиента	
20.	Кэширующий DNS сервер	
21.	Поддержка протоколов туннелирования GIF, GRE	
22.	Поддержка IPv4, IPv6	

№ п/п	Функционал	Комментарий
23.	Поддержка объединения физических интерфейсов в логические	
24.	Просмотр таблицы активных соединений	
Функции сбора и анализа событий		
25.	Выбор совокупности регистрируемых событий для анализа по различным критериям	Выбор правил, по которым будут направляться предупреждения и регистрируемых событий на основе источника и других параметров
26.	Уведомления о событиях безопасности в интерфейсе	
27.	Мониторинг состояния по SNMP v.1, 2, 3	
28.	Экспорт событий по протоколу SYSLOG (интеграция с SIEM-системами), SYSLOG в формате CEF	
29.	Возможность сбора и экспорта дампов трафика	
30.	Интеграция по ICAP с внешними системами	
31.	Сбор и экспорт статистики NetFlow	
32.	Мониторинг загрузки и состояния сетевых интерфейсов, CPU, памяти и программных модулей	
33.	Инвентаризация сетевых ресурсов (в виде таблицы)	
Функции управления		
34.	Доступ к продукту и управление на ролевой основе, гибкая настройка прав доступа	
35.	Возможность аутентификации пользователей через Active Directory	
36.	Поддержка функций централизованного управления	С помощью интеграции с InfoWatch ARMA Management Console
37.	Возможность передачи событий в ARMA Management Console	
38.	Задание и синхронизации времени по протоколу NTP	
39.	Поддержка управления по SSH	
40.	Поддержка управления через консольный порт	

№ п/п	Функционал	Комментарий
41.	Возможность экспорта и импорта конфигурации	
42.	Возможность экспорта и импорта баз решающих правил	По протоколу FTP, SMB, локально
43.	Планировщик задач	На основе сервиса «cron»
44.	Возможность отключения/включения неиспользуемых сервисов	
45.	Журналы системных событий	
46.	Журналы событий безопасности	
47.	Журналы событий NAT	
48.	Журналы сервисных событий	
49.	Фильтрация по времени в каждом из журналов	
50.	Выгрузка журналов	
51.	Возможность удаленного/локального обновления	
52.	Возможность офлайн обновления: правил Suricate, сигнатур IPS, сигнатур анализа приложений и антивирусных баз	
53.	Возможность автоматической установки ARMA IF на оборудование при подключении к нему USB-носителя с программой установщиком	Не требует дополнительных действий со стороны пользователя
Функции отказоустойчивости, повышения надежности, резервирования		
54.	Поддержка отказоустойчивой конфигурации active-passive	
55.	Loop Protection. Технологии STP, RSTP	Доступен для режима сетевого моста
56.	Сохранение резервных копий конфигурации на выделенный FTP-сервер	
57.	Возможность настроить синхронизацию устройств при работе МЭ в режиме отказоустойчивого кластера	
58.	Возможность расширенного отката конфигураций	
59.	Возможность сброса настроек	
60.	Шифрование резервной копии конфигурации	
Защита доступа		

№ п/п	Функционал	Комментарий
61.	Обеспечение защищенного канала администрирования системы за счет управления по протоколам HTTPS, SSH	
62.	Конфигурация парольной политики	Задание «сложности» пароля
63.	Возможность аутентификации по различным базам: локальная база пользователей, каталог Active Directory (LDAP), RADIUS-сервер	
64.	Контроль целостности программного обеспечения устройства защиты	
65.	Контроль целостности конфигурационного файла	
66.	Блокировка пользователя при 5 попытках неудачного входа	
Антивирус		
67.	Потоковый антивирус в режиме прокси	
68.	Возможность конфигурации потокового антивируса, в том числе тайм аутов	
69.	Возможность просмотреть текущую версию антивируса и сигнатуры	
70.	Возможность загрузки новых сигнатур	
71.	Просмотр, скачивание и очистка журнала событий антивируса	
72.	Возможность обновления антивирусных баз	
C-ICAP		
73.	Включение/отключение сервисов C-ICAP	Производить антивирусную проверку данных, блокировать спам, запрещать доступ к персональным ресурсам
74.	Настройка работы сервисов C-ICAP	
75.	Осуществление сканирования на антивирусы с помощью сервисов протокола C-ICAP	Работает при включенном антивирусе
76.	Просмотр, скачивание и очистка журнала сервисов C-ICAP	
VPN		
77.	Возможность построения криптографического туннеля	VPN IPSEC, OpenVPN, OpenVPN-ГОСТ

№ п/п	Функционал	Комментарий
78.	Site-to-site VPN	

2.3 Поддерживаемые промышленные протоколы

ARMA IF выполняет анализ пакетов по различным полям и параметрам промышленных протоколов, портам, IP-адресам отправителя/получателя.

Поддерживаемые протоколы отражены в таблице (см. [Таблица 4](#)).

Таблица 4
Поддерживаемые протоколы

Возможность фильтрации	Обнаружение вторжений и мониторинг (без фильтрации)
Modbus TCP	Modbus TCP
IEC 60870-5-104	IEC 60870-5-104
S7 Communication	S7 Communication
OPC UA	OPC UA
OPC DA	OPC DA
Modbus TCP x90 func. code (UMAS)	Modbus TCP x90 func. code (UMAS)
IEC 61850-8-1 MMS	IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE	IEC 61850-8-1 GOOSE
KRUG	KRUG
	Profinet
	S7 Communication plus
	DNP3

Для протоколов, по которым возможна фильтрация, указана поддержка (см. [Таблица 5](#)).

Таблица 5
Поддерживаемые протоколы с указанием степени их разбора

Протокол	Стандарт	Степень разбора
Modbus TCP	MODBUS Application Protocol Specification V1.1b3	Для сообщений по протоколу Modbus TCP можно задать правило обнаружения на основе признака совпадения:

Протокол	Стандарт	Степень разбора
		• свойство функции (код или категория функции); • тип доступа к данным (тип доступа и основная модель данных); • диапазон функции (ввод кода функции, адреса и значения переменной вручную). При обнаружении по свойству функции возможно задать дополнительные опции: • используемую функцию, подфункцию; • Категории кодов функции. Категория кодов функции: • (назначенная (коды функций, которые определены в Modbus спецификации); • не назначенная, общедоступная (стандартные и организационные коды); • пользовательская (два диапазона кодов, для которых пользователь может назначить произвольную функцию); • зарезервированная (коды функций, которые не являются стандартными); • все категории. При классификации по доступу к данным возможно задать следующие дополнительные опции: • тип доступа к данным – записать или считать. Модель данных:

Протокол	Стандарт	Степень разбора
		• «Регистры флагов (Coils)» – битовые данные, доступ чтение/запись; • «Регистры хранения (Holding Registers)» – 16 битовые данные, доступ чтение/запись; • «Дискретные входы (Discrete Inputs)» – битовые данные, доступ чтение; • «Регистры ввода (Input Registers)» – 16 битовые данные, доступ чтение.
IEC 60870-5-104	ГОСТ Р МЭК 60870-5-104-2004	Сообщения по протоколу IEC 60870-5-104 могут быть определены по типу пакета: • полный – APDU; • для целей управления – только поля APCI. При классификации по типу пакета APCI возможен выбор формата пакета: • любой; • «U-format (unnumbered control functions)» – функции управления без нумерации; • «S-format (numbered supervisory functions)» – функции контроля с нумерацией. При классификации по типу пакета ASDU возможно задание: • диапазона разрешенных входящих пакетов (RX); • диапазона разрешенных исходящих пакетов (TX); • типа ASDU; • причины передачи (ASDU cause of transfer);

Протокол	Стандарт	Степень разбора
		• числового значения ASDU адреса; • адреса объекта информации в формате диапазона; • значения IOA.
S7 Communication	Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-300/400	Сообщения по протоколу S7Communication разделяются по функции: • CPUSERVICE; • SETUPCOMM; • READVAR; • WRITEVAR; • REQUESTDOWNLOAD; • DOWNLOADBLOCK; • DOWNLOADENDED; • STARTUPLOAD; • UPLOAD; • ENDUPLOAD; • PLCCONTROL; • PLCSTOP. При выборе в поле «Функция» функции «READVAR» необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных. При выборе в поле «Функция» функции «WRITEVAR» необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных, типа передаваемого значения, количество передаваемых данных, список значений данных. При выборе в поле «Функция» функции «REQUESTDOWNLOAD» появятся поле

Протокол	Стандарт	Степень разбора
		выбора типа блока, номера блока и целевой файловой системы. При выборе в поле «Функция» функции «DOWNLOADBLOCK» появятся поле выбора типа блока, номера блока и целевой файловой системы. При выборе в поле «Функция» функции «STARTUPLOAD» появятся поле выбора типа блока, номера блока и целевой файловой системы. При выборе в поле «Функция» функции «PLCCONTROL» появятся поле выбора функции управления ПЛК: • «INSE (Активация скаченного блока, параметром выступает имя блока)»; • «DELE (Удаление блока, параметром выступает имя блока)»; • «PPROGRAM (Запуск программы, параметром выступает имя программы)»; • «GARB (Сжатие памяти)»; • «MODU (Копирование RAM в ROM, параметр содержит идентификатор файловой системы A/E/P)»; • «OFF (Выключение ПЛК)»; • «ON (Включение ПЛК)».
OPC UA	IEC 62541	Сообщения по протоколу OPC UA разделяются по тип сообщения: • HELLO (маркер начала передачи данных между клиентом и сервером); • ACKNOWLEDGE (ответ на сообщение типа HELLO);

Протокол	Стандарт	Степень разбора
		• OPEN (открытие канала передачи данных с предложенным методом шифрования данных); • MESSAGE (передаваемое сообщение); • CLOSE (конец сессии). При выборе «OPEN» появятся поле выбора политика безопасности. При выборе «MESSAGE» в поле появятся поле выбора типа запроса. При выборе «BROWSE» в поле «Тип запроса» появятся поле ввода диапазон запроса. При выборе «READ» в поле «Тип запроса» появятся поле ввода диапазон запроса. При выборе «WRITE» в поле «Тип запроса» появятся поле ввода диапазон запроса. При выборе «CALL» в поле «Тип запроса» появятся поле ввода идентификатора узла, содержащий вызываемую процедуру и поле ввода идентификатора узла вызываемой процедуры.
OPC DA	OLE for Process Control Data Access Automation Interface Standard v.2.0	Сообщения по протоколу OPC DA разделяются по типу сообщения: • REQUEST; • PING; • RESPONSE; • FAULT; • WORKING; • NOCALL; • REJECT;

Протокол	Стандарт	Степень разбора
		• ACK; • CI_CANCEL; • FACK; • CANCEL_ACK; • BIND; • BIND_ACK; • BIND_NACK; • ALTER_CONTEXT; • ALTER_CONTEXT_RESP; • SHUTDOWN; • AUTH3; • CO_CANCEL; • ORPHANED. При выборе «REQUEST» в поле появятся поле ввода идентификатора вызываемого объекта и поле ввода номера вызываемой функции объекта.
UMAS	Основан на протоколе Xway Unite. Протокол Umas используется для настройки и мониторинга ПЛК Schneider-Electric.	Сообщения по протоколу UMAS разделяются по функциям: • инициализация UMAS сессии; • чтение информации о проекте; • чтение внутренней информации ПЛК; • назначение ПЛК владельца; • инициализация загрузки (копирование с инженерного ПК на ПЛК); • завершение загрузки (копирования с инженерного ПК на ПЛК);

Протокол	Стандарт	Степень разбора
		- инициализация скачивания (копирование с ПЛК на инженерный ПК); - конец скачивания (копирования с ПЛК на инженерный ПК); - включение ПЛК; - выключение ПЛК.
MMS	IEC 61850-8-1	Сообщения по протоколу MMS разделяются по типу сообщения. Для типа сообщения «CONFIRMED_REQUEST» возможен выбор типа служб. Для службы «READ» возможен ввод имени переменной и адреса переменной для функции чтения. Для службы «WRITE» возможен ввод имени переменной для функции записи.
GOOSE	IEC 61850-8-1	Сообщения по протоколу GOOSE разделяются по: - идентификатору приложения; - значению поля «dataset»; - значению поля «gocbref»; - значению поля «goid»; - значению поля «t».
KRUG	Круг ПК-контроллер	Сообщения по протоколу KRUG разделяются по: - значению поля «COMMAND»; - значению поля «CMD»; - значению поля «PORT»; - значению поля «ACCESS»; - значению поля «MODE»; - значению поля «ERRCODE»

2.3.1 Варианты использования функций ограничения

Возможны следующие варианты использования функций ограничения:

1. Контроль действий пользователя по сети (ограничение по управлению конкретными функциями).
2. Ограничение трафика между несколькими АСУ ТП (возможность работы по промышленным протоколам или ограничение такой работы).
3. Запрет заведомо недопустимых операций (обновление прошивки ПЛК).
4. Контроль значения переменных в АСУ ТП.

2.4 Варианты применения

ARMA IF может быть расположен на нескольких участках сети:

- на границе с корпоративным сегментом;
- защита канала технической поддержки;
- защита смежных АСУ ТП;
- мониторинг внутри АСУ ТП.

2.4.1 На границе с корпоративным сегментом

На границе с корпоративным сегментом возможен доступ злоумышленника к сегменту сети «Уровень SCADA» в соответствии со схемой (см. [Рисунок 3](#)).

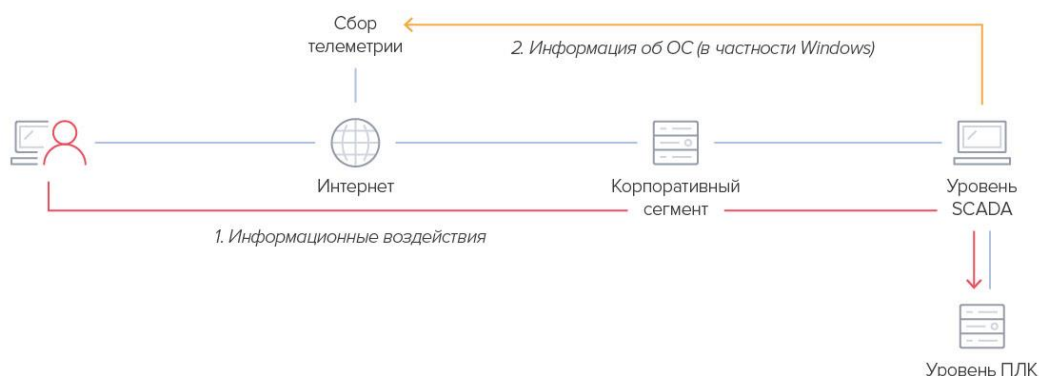


Рисунок 3 – Угрозы на границе с корпоративным сегментом

На схеме, представленной на рисунке (см. [Рисунок 4](#)), показан вариант применения **ARMA IF** на границе с корпоративным сегментом.

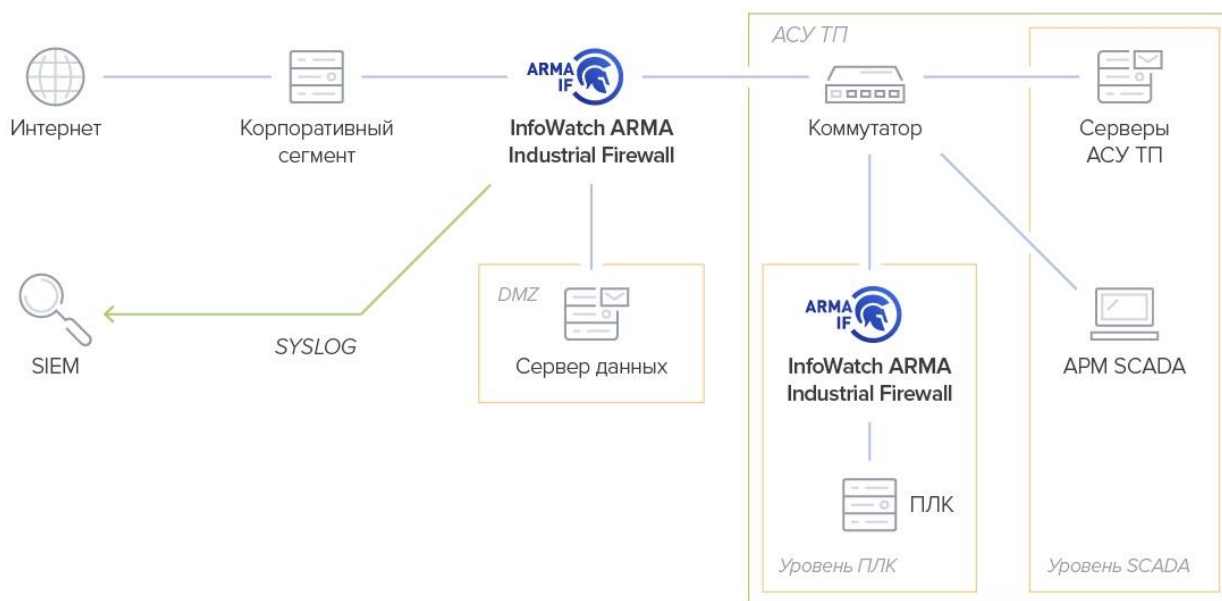


Рисунок 4 – Применение на границе с корпоративным сегментом

2.4.2 Связь с технической поддержкой

Через связь с технической поддержкой возможен доступ злоумышленника к сегменту сети «Уровень SCADA» в соответствии со схемой (см. Рисунок 5).

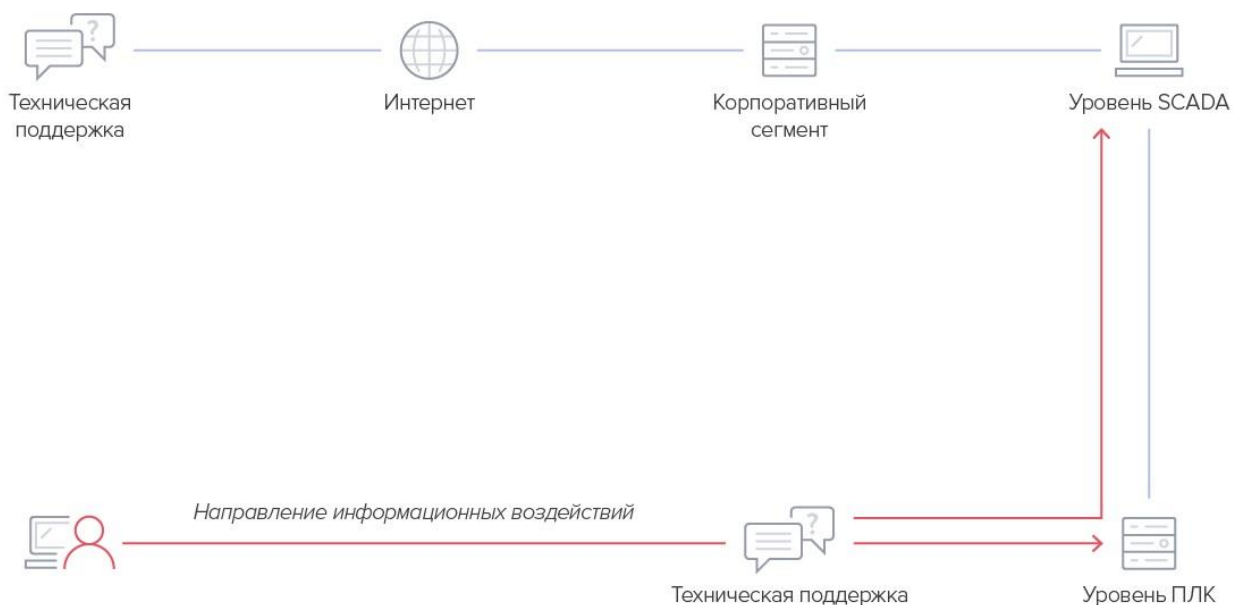


Рисунок 5 – Связь с технической поддержкой. Угрозы

На схеме, представленной на рисунке (см. Рисунок 6), показан вариант применения **ARMA IF** для обеспечения безопасной связи с технической поддержкой.

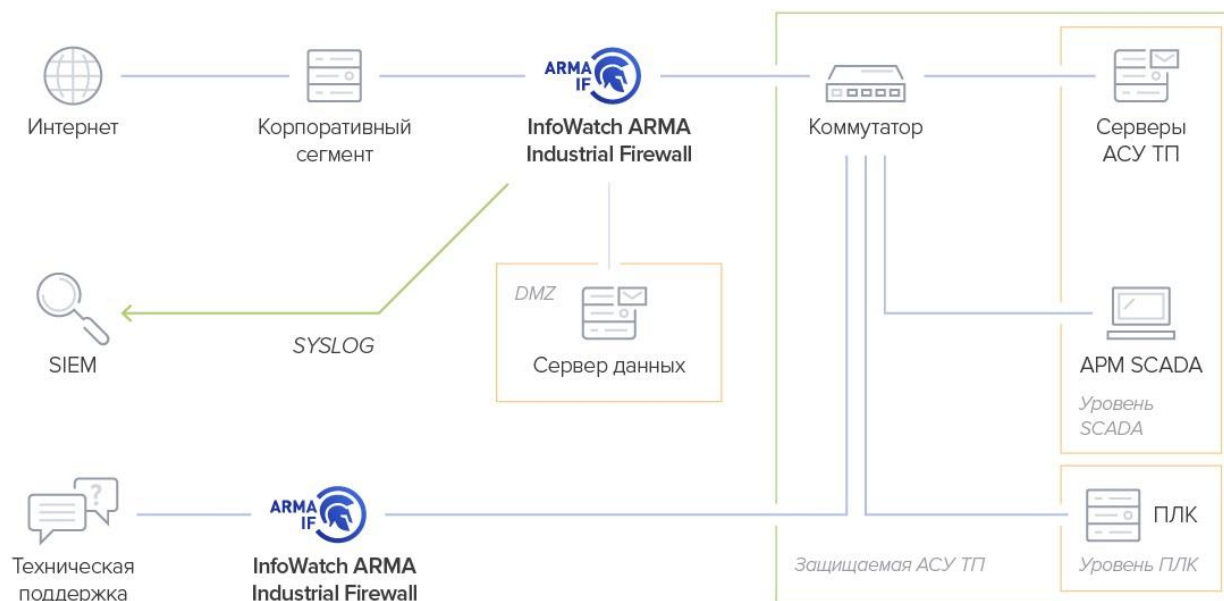


Рисунок 6 – Применение для обеспечения безопасной связи с технической поддержкой

2.4.3 Связь со смежными АСУ ТП

Через связь со смежными АСУ ТП возможен доступ злоумышленника к сегменту сети «Уровень SCADA» в соответствии со схемой (см. Рисунок 7).

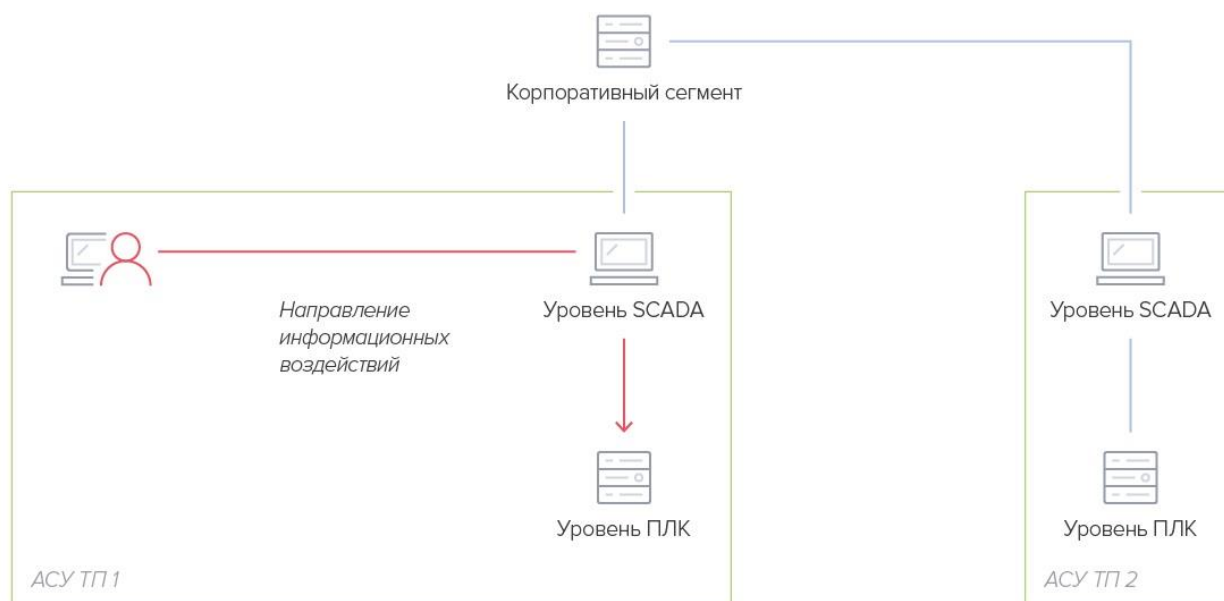


Рисунок 7 – Связь со смежными АСУ ТП. Угрозы

На схеме, представленной на рисунке (см. Рисунок 8), показан вариант применения **ARMA IF** для обеспечения безопасной связи со смежными АСУ ТП.

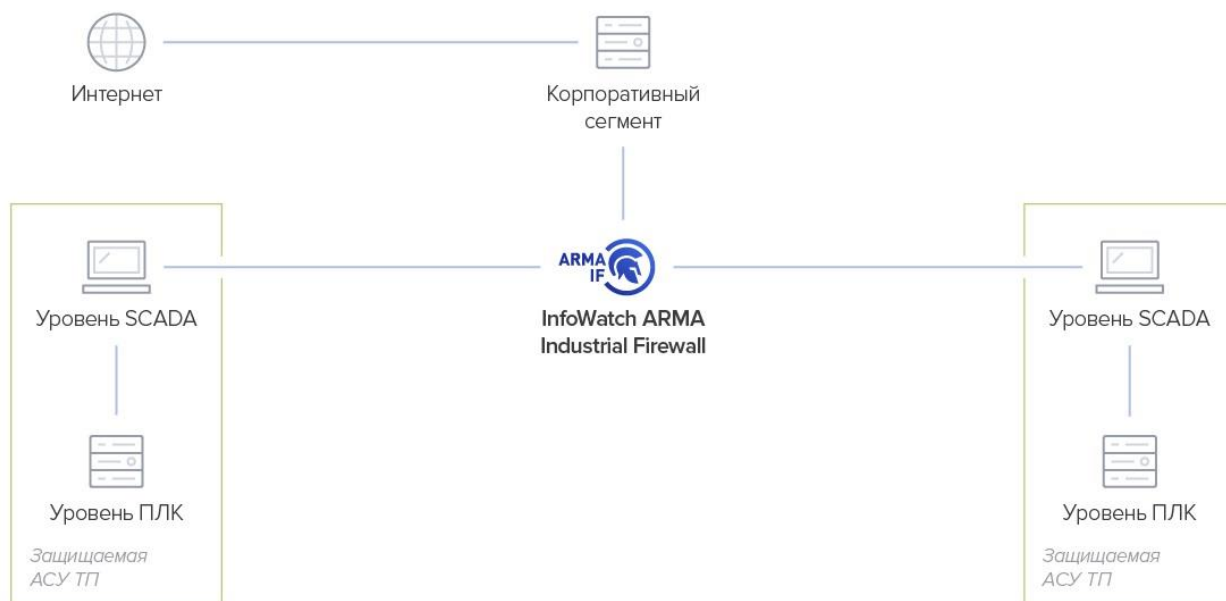


Рисунок 8 – Применение для обеспечения безопасной связи со смежными АСУ ТП

2.4.4 Мониторинг внутри АСУ ТП

На схеме, представленной на рисунке (см. Рисунок 9), показан вариант применения **ARMA IF** для осуществления мониторинга внутри АСУ ТП.

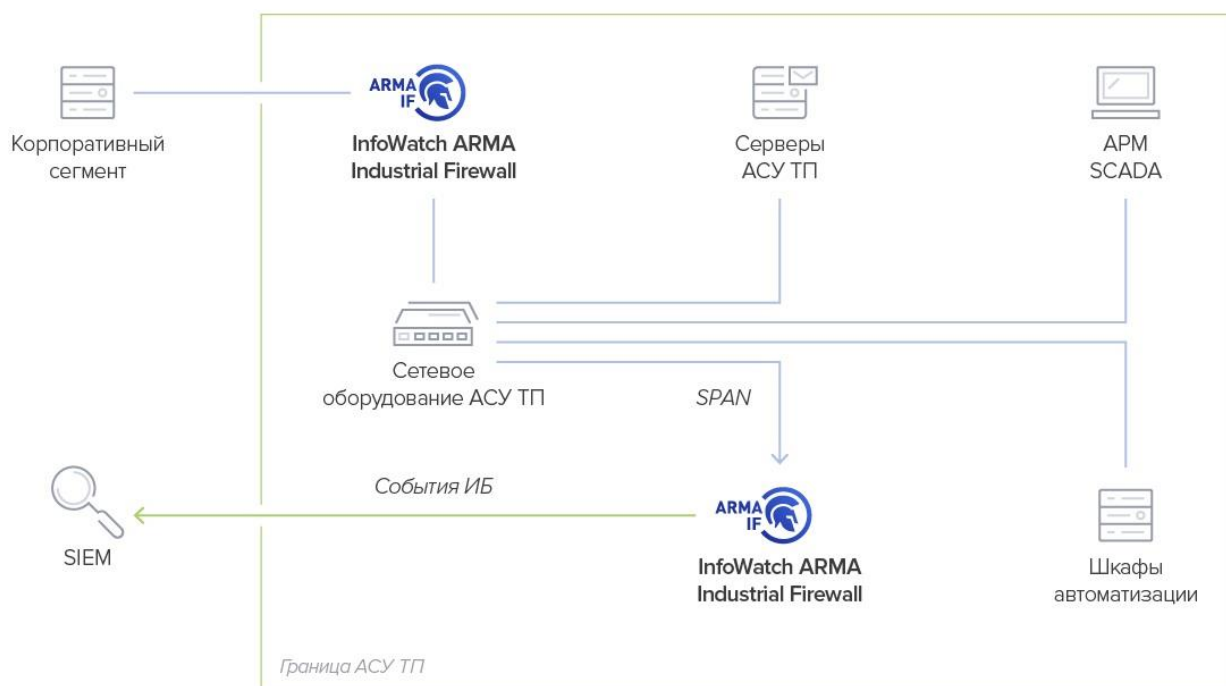


Рисунок 9 – Применение для мониторинга внутри АСУ ТП

2.5 Обнаруживаемые атаки

ARMA IF обнаруживает следующие атаки:

- сканирование сети;

- попытки эксплуатации уязвимостей ПО и программируемых логических контроллеров (ПЛК);
- использование запрещенных функций промышленных протоколов;
- появление запрещенных информационных потоков;
- подозрительные команды;
- действия вредоносного программного обеспечения;
- несанкционированная перепрошивка ПЛК;
- изменения установок ПЛК;
- подключение устройств в технологическую сеть;
- подмена сетевого адреса;
- несанкционированное подключение к АСУ ТП из внешней сети.

2.6 Описание аппаратных конфигураций

Возможны следующие варианты поставки **ARMA IF**:

1. Для поставки в стойку 19”:

- в серверном исполнении;
- в промышленном исполнении в соответствии требованиям ГОСТ Р МЭК 61850-3, ГОСТ Р 52931, ГОСТ IEC 60950-1.

2. Для крепления на DIN рейку:

- в промышленном исполнении.

В таблице ниже (см. [Таблица 6](#)) приведены основные технические характеристики различных аппаратных конфигураций **ARMA IF**.

Таблица 6
Аппаратные конфигурации ARMA IF

Параметр	ARMA IF-19RACK	ARMA IF-ELECTRO	ARMA IF-BOX	ARMA IF-DIN
Изображение				
Исполнение	1 Unit исполнение для монтажа в стойку. Серверное исполнение	1 Unit исполнение для монтажа в стойку. Промышленно е исполнение, без движущихся частей	Настольное исполнение, без движущихся частей	Промышленное исполнение, без движущихся частей

Параметр	ARMA IF-19RACK	ARMA IF-ELECTRO	ARMA IF-BOX	ARMA IF-DIN
Процессор	Intel Xeon E3-1220v6, 3 ГГц, 8 МБ кэш	Intel Core i7-7600U, 2.8 ГГц, 4МБ кэш	Intel Atom C3558, 2.2 ГГц, 8 МБ кэш	Intel Celeron N3350, промышленный, пассивное охлаждение
ОЗУ	От 16 Гб оперативной памяти	16 Гб оперативной памяти	16 Гб оперативной памяти	8 Гб оперативной памяти
Жесткий диск	От 240 Гб твердотельный накопитель	240 Гб твердотельный накопитель	256 Гб твердотельный накопитель	256 Гб твердотельный накопитель
Сетевые порты	Конфигурации: 1. Ethernet – 8 портов 1 Гб/с 2. Ethernet – 6 портов 1 Гб/с + 2 порта 10 Гб/с 3. Ethernet – 4 порта 1 Гб/с + 4 порта 10 Гб/с	Ethernet - 5 порта 1 Гб/с	Ethernet - 6 портов 1 Гб/с + 2 порта 10 Гб/с	Ethernet - 4 порта 1 Гб/с
Пассивное охлаждение	Нет	Да	Нет	Да
Степень защиты корпуса	-	IP-20	-	IP-30
Температура эксплуатации	0 ... 40 °C	-20°C...+70°C	0 ... 40 °C	-20 ... +70 °C
Влажность	5 ... 95 %	5 ... 95 % (без конденсата)	5 ... 95 % (без конденсата)	5 ... 95 % (без конденсата)
Вибрация	-	Воздействий стационарной синусоидальной вибрации: – с амплитудой перемещения 3 мм при частоте	-	2G, 10...150 Гц, амплитуда 0.35 мм

Параметр	ARMA IF-19RACK	ARMA IF-ELECTRO	ARMA IF-BOX	ARMA IF-DIN
		вибрации (0,5-9) Гц; – с амплитудой ускорения 10 м/с ² при частоте вибрации (9-200) Гц и 15 м/с ² при частоте - (200-500) Гц"		
Удар	-	Воздействий ударов длительностью 2-22 мс (половина синусоиды) с пиковым ускорением 100 м/с ²	-	25G, полусинусоида, продолжительность 11 мс
Дополнительно	Включен в реестр Минпромторг России (ТОРП)	Соответствует требованиям ГОСТ Р МЭК 61850-3, ГОСТ Р 52931, ГОСТ IEC 60950-1.	-	-
Питание	Питание - 2х450 Вт., с возможностью горячей замены	2х220 Вт.	Питание - 12...24 В, внешний блок питания	Питание - 12...24 В, внешний блок питания
Общая пропускная способность всего устройства с включенным модулем МЭ	6 Гб/с (оценка на основе характеристик оборудования)	4 Гб/с (оценка на основе характеристик оборудования)	2 Гб/с (оценка на основе характеристик оборудования)	1 Гб/с (оценка на основе характеристик оборудования)

Параметр	ARMA IF-19RACK	ARMA IF-ELECTRO	ARMA IF-BOX	ARMA IF-DIN
Общая пропускная способность всего устройства с включенными модулями МЭ и COB и DPI	750 Мб/с	500 Мб/с	180 Мб/с	80 Мб/с
Межсетевой экран, пакетов/с (оценочное значение)	2 700 000	1 800 000	330 000	120 000
Межсетевой экран, количество одновременных соединений (сессий)	9 200 000	2 000 000	700 000	250 000
Габаритные размеры (ШхГхВ)	444x615x44 (1U)	483x163x44 (1U)	197x231x44	155x110x79
Вес	11 кг.	4 кг	1.7 кг.	1.15 кг.

Гарантия на оборудование – 1 год.

2.7 Лицензирование

В **ARMA IF** предусмотрены следующие виды лицензии:

- Enterprise COB (система обнаружения вторжений);
- Enterprise МЭ (межсетевой экран (МЭ));
- Enterprise МЭ + COB (межсетевой экран «следующего поколения» (NGFW)).

Лицензия Enterprise COB можно расширить совместным или отдельным приобретением лицензий:

- Enterprise Промышленные протоколы;
- Enterprise OPCDA.

В таблице ниже (см. [Таблица 7](#)) перечислены функции **ARMA IF** для каждого вида лицензии.

Таблица 7
Функции ARMA IF для каждого вида лицензии

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
Межсетевой экран				
1.	Контроль доступа пользователей к сетевым ресурсам, указание срока действия учетной записи пользователя (Портал авторизации)	-	+	+
2.	Контроль доступа пользователей локальной сети к ресурсам Internet (URL-фильтрация)	-	+	+
3.	Фильтрация сетевого трафика с учетом параметров пакета на сетевом и транспортном уровнях	-	+	+
4.	Точная идентификация, классификация и предотвращение проникновения вредоносного трафика, включая червей, вирусов, сетевых атак и т.п.	-	+	+
5.	Соккрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)	-	+	+
6.	Возможность задания расписания срабатывания правил	-	+	+
Система обнаружений вторжений				
7.	Обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровне	+	-	+
8.	Обновление базы решающих правил	+	-	+
9.	Возможность разработки пользовательских правил СОВ	+	-	+
10.	Возможность задания расписания срабатывания правил	+	-	+
Сетевые функции				
11.	Возможность работы в режиме прозрачного моста	+	+	+
12.	Поддержка статической маршрутизации	-	+	+
13.	Поддержка протоколов динамической маршрутизации	-	+	+
14.	Прокси сервер	-	+	+

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
15.	Поддержка VLAN IEEE 802.1q	-	+	+
16.	DHCP сервер	-	+	+
17.	Функции QoS (Traffic Shaping)	-	+	+
18.	Возможность зеркалирования сетевого трафика на отдельный порт	-	+	+
19.	Функционирование DNS клиента	+	+	+
20.	Кэширующий DNS сервер	+	+	+
21.	Поддержка протоколов туннелирования GIF, GRE	+	+	+
22.	Поддержка IPv4, IPv6	+	+	+
23.	Поддержка объединения физических интерфейсов в логические	+	+	+
24.	Просмотр таблицы активных соединений	-	+	+
Функции сбора и анализа событий				
25.	Выбор совокупности регистрируемых событий для анализа по различным критериям	+	+	+
26.	Уведомления о событиях безопасности в интерфейсе	+	+	+
27.	Мониторинг состояния по SNMP v.1, 2, 3	+	+	+
28.	Экспорт событий по протоколу SYSLOG (интеграция с SIEM-системами), SYSLOG в формате CEF	+	+	+
29.	Возможность сбора и экспорта дампов трафика	+	+	+
30.	Интеграция по ICAP с внешними системами	-	+	+
31.	Сбор и экспорт статистики NetFlow	+	+	+
32.	Мониторинг загрузки и состояния сетевых интерфейсов, CPU, памяти и программных модулей	+	+	+
33.	Инвентаризация сетевых ресурсов (в виде таблицы)	+	+	+
Функции управления				
34.	Доступ к продукту и управление на ролевой основе, гибкая настройка прав доступа	+	+	+
35.	Возможность аутентификации пользователей через Active Directory	+	+	+
36.	Поддержка функций	+	+	+

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
	централизованного управления			
37.	Возможность передачи событий в InfoWatch ARMA Management Console	+	+	+
38.	Задание и синхронизации времени по протоколу NTP	+	+	+
39.	Поддержка управления по SSH	+	+	+
40.	Поддержка управления через консольный порт	+	+	+
41.	Возможность экспорта и импорта конфигурации	+	+	+
42.	Возможность экспорта и импорта баз решающих правил	+	-	+
43.	Планировщик задач	+	+	+
44.	Возможность отключения/включения неиспользуемых сервисов	+	+	+
45.	Журналы системных событий	+	+	+
46.	Журналы событий безопасности	+	+	+
47.	Журналы событий NAT	-	+	+
48.	Журналы сервисных событий	+	+	+
49.	Фильтрация по времени в каждом из журналов	+	+	+
50.	Выгрузка журналов	+	+	+
51.	Возможность удаленного/локального обновления	+	+	+
52.	Возможность офлайн обновления: правил Suricate, сигнатур IPS, сигнатур анализа приложений и антивирусных баз	+	+	+
53.	Возможность автоматической установки ARMA IF на оборудование при подключении к нему USB-носителя с программой установщиком	+	+	+
Функции отказоустойчивости, повышения надежности, резервирования				
54.	Поддержка отказоустойчивой конфигурации active-passive	-	+	+
55.	Loop Protection. Технологии STP, RSTP	-	+	+
56.	Сохранение резервных копий конфигурации на выделенный FTP-сервер	+	+	+
57.	Возможность настроить	-	+	+

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
	синхронизацию устройств при работе МЭ в режиме отказоустойчивого кластера			
58.	Возможность расширенного отката конфигураций	-	+	+
59.	Возможность сброса настроек	-	+	+
60.	Шифрование резервной копии конфигурации	-	+	+
Защита доступа				
61.	Обеспечение защищенного канала администрирования системы за счет управления по протоколам HTTPS, SSH	+	+	+
62.	Конфигурация парольной политики	+	+	+
63.	Возможность аутентификации по различным базам: локальная база пользователей, каталог Active Directory (LDAP), RADIUS-сервер	+	+	+
64.	Контроль целостности программного обеспечения устройства защиты	+	+	+
65.	Контроль целостности конфигурационного файла	+	+	+
66.	Блокировка пользователя при 5 попытках неудачного входа	+	+	+
Антивирус				
67.	Потоковый антивирус в режиме прокси	-	+	+
68.	Возможность конфигурации потокового антивируса, в том числе тайм аутов	-	+	+
69.	Возможность просмотреть текущую версию антивируса и сигнатуры	-	+	+
70.	Возможность загрузки новых сигнатур	-	+	+
71.	Просмотр, скачивание и очистка журнала событий антивируса	-	+	+
72.	Возможность обновления антивирусных баз	-	+	+
C-ICAP				
73.	Включение/отключение сервисов C-ICAP	-	+	+
74.	Настройка работы сервисов C-ICAP	-	+	+
75.	Осуществление сканирования на	-	+	+

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
	антивирусы с помощью сервисов протокола C-ICAP			
76.	Просмотр, скачивание и очистка журнала сервисов C-ICAP	-	+	+
VPN				
77.	Возможность построения криптографического тоннеля	-	+	+
78.	Site-to-site VPN (OpenVPN-ГОСТ)	-	+	+

3 INFOWATCH ARMA MANAGEMENT CONSOLE

3.1 Технические требования

Установка **ARMA MC** производится на следующие типы платформ:

- аппаратная;
- виртуальная (гипервизор).

Установка на аппаратную платформу выполняется с использованием USB-накопителя, на который должен быть записан образ **ARMA MC** в формате «*.ISO».

Установка на виртуальную платформу (гипервизор) производится с помощью образа в формате «*.ISO».

3.1.1 Требования к аппаратной платформе

При установке **ARMA MC** на аппаратную платформу необходимо использовать микропроцессорную архитектуру **x64** или **Байкал-М (ARMv8)**.

Для аппаратной платформы, на которую устанавливается **ARMA MC** достаточно руководствоваться минимальными требованиями к аппаратному обеспечению (см. Таблица 8).

Таблица 8
Минимальные требования к аппаратному обеспечению

Название оборудования	Требования
Процессор	2,0 ГГц, четырехъядерный, x64 или Байкал-М (ARMv8)
ОЗУ	16 ГБ
Интерфейсы, необходимые для установки программного обеспечения	Последовательная консоль или видео-выход (VGA или DVI) с USB (или PS/2) интерфейсами для подключения клавиатуры
Жесткий диск	512 ГБ, SSD
Сетевые интерфейсы	Не менее 1 x Ethernet 100/1000 Мбит/сек

3.1.2 Требования к виртуальной платформе

Виртуализация **ARMA MC** поддерживается для следующих виртуальных платформ (гипервизоров):

- HyperV Generation 1;
- VirtualBox версии 6.0.4 и выше;
- VMware ESXi версии 5.5 обновления 2 и выше.

Для запуска **ARMA MC** предъявляются следующие минимальные требования к виртуальной среде (см. [Таблица 9](#)).

Таблица 9
Минимальные требования к виртуальной среде

Название оборудования	Требования
Процессор	4 ядра
Объем оперативной памяти	16 ГБ
Размер виртуального диска	512 ГБ
Сетевые интерфейсы	Не менее 1

Для корректного отображения веб-интерфейса к веб-браузерам предъявляются следующие требования:

- а. для ОС семейства Windows:
 - Chrome, Firefox;
- б. для ОС семейства Linux:
 - Chrome для Linux, Firefox для Linux.

3.2 Функции

Функции **ARMA MC** приведены в таблице (см. [Таблица 10](#)).

Таблица 10
Функции ARMA MC

№ п/п	Функционал	Комментарий
Общие		
1.	Аутентификация и идентификация пользователей	
2.	Настройка политики аутентификации	(число попыток и время блокировки)
3.	Доступ к функционалу в соответствии с приобретённой лицензией	
4.	Доступ к функционалу в соответствии с ролевой политикой	
5.	Управление пользователями, включая разблокировку заблокированных пользователей	
6.	Поиск и фильтрация по всем журналам и списком консоли	
7.	Шифрование для подключения к web-интерфейсу	(TLS)
8.	Информация о работе системы на обзорной панели пользователя	
9.	Ротация журналов	

10.	Доступ ко всем скачанным из ARMA Management Console данным пользователя	
Подключение источников событий		
11.	Подключение источников событий	по IP и порту
Централизованное управление системами защиты		
12.	Защищенное централизованное управление продуктами InfoWatch ARMA	По API (HTTPS)
13.	Доступ к веб-интерфейсу InfoWatch ARMA Industrial Firewall	
14.	Импорт/экспорт конфигурации InfoWatch ARMA Industrial Firewall	Экспорт конфигурации на одно/несколько устройств
15.	Импорт/экспорт баз решающих правил InfoWatch ARMA Industrial Firewall	Экспорт баз решающих правил на одно/несколько устройств
Централизованное управление ARMA Industrial Endpoint		
16.	Подключение ARMA Industrial Endpoint	
17.	Индивидуальная настройка ARMA Industrial Endpoint по параметрам	Контроль целостности, запуск ПО белому списку, управление USB устройствами, антивирусная защита, настройка ротации журнала событий.
18.	Клонирование ARMA Industrial Endpoint	Включая все настройки
19.	Импорт/экспорт конфигурации InfoWatch ARMA Industrial Firewall	Экспорт конфигурации на одно/несколько устройств
Сбор и анализ данных аудита		
20.	Централизованный сбор событий с подключенных InfoWatch ARMA Industrial Firewall	
21.	Централизованный сбор инцидентов с подключенных InfoWatch ARMA Industrial Endpoint	
22.	Просмотр детальной информации по каждому событию	
23.	Корреляция событий	Возможность проверить наличие событий, соответствующих параметрам правила
		Корреляция в инциденты

		Добавление автоматизированного действия: - Создание и отправка правил на InfoWatch ARMA Industrial Firewall - Запуск Bash скрипта - Запуск исполняемого файла - HTTPS - Отправка по Syslog - Создание нового актива
		Добавление рекомендация для устранения инцидента
		Добавление последствий
24.	Пакеты встроенных правил корреляции	
25.	Возможность написания пользовательских правил корреляции	
26.	Загрузка обновлений правил корреляции	
27.	Предоставление детального отчета по каждому инциденту	
28.	Уведомление пользователя об инцидентах	
29.	Управление инцидентами	
30.	Отправка инцидентов в ГосСОПКА по решению пользователя	
31.	Взаимодействие с сотрудниками НКЦКИ в online режиме	
32.	Отправка инцидентов в другие системы	Syslog, OPC UA
Отображение активов сети		
33.	Список активов сети	
34.	Детальная информация о каждом активе, с возможностью дополнения	
35.	Отображение карты сети	Отображение другим цветом активы, которые имеют нерешенные инциденты;
		Отображение подробной информации об активе;
		Возможность задания связей между активами сети;

		Возможность перетаскивания активов по карте сети.
		Возможность добавлять фоновое изображение для фиксации активов на ней
		Возможность создания неограниченного числа карт сети
36.	Отображение карты сетевых взаимодействий	Отображение всех активов сети
		Отображение протоколов взаимодействия
		Отображение подробной информации об активе;
		Возможность фильтрации по: - времени - протоколу - по конкретным активам
37.	Возможность группировки активов сети на картах	

3.3 Варианты применения

На схеме показан вариант применения **ARMA MC** с другими продуктами **InfoWatch ARMA** (см. [Рисунок 10](#)).

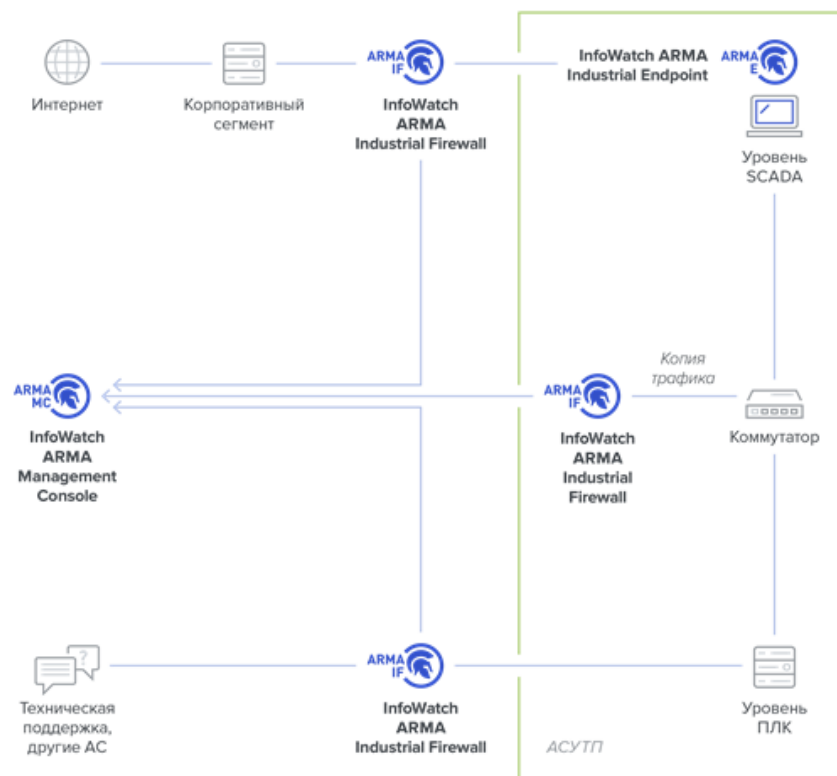


Рисунок 10 – Применение ARMA MC

Схема автоматической блокировки угрозы и ее источника с помощью **ARMA MC** (см. Рисунок 11).



Рисунок 11 – Блокировка угроз

3.4 Лицензирование

В **ARMA MC** предусмотрены следующие виды лицензии:

- Enterprise Сбор и агрегация событий безопасности;
- Enterprise Подключение источника событий;
- Enterprise Управление инцидентами.

4 INFOWATCH ARMA INDUSTRIAL ENDPOINT

4.1 Технические требования

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

Для аппаратной платформы, на которую устанавливается **ARMA IE**, достаточно руководствоваться минимальными требованиями к аппаратному обеспечению (см. Таблица 11, Таблица 12).

Таблица 11
Минимальные требования к аппаратному обеспечению

Название оборудования	Требования
Процессор	2 ГГц, одноплатный, x86 или x64
Жесткий диск	200 Мб свободной памяти на диске
ОЗУ	100 Мб свободной памяти
Операционная система	Windows 10/ Windows 10 LTSC/LTSB /Windows 7 (версии уточняются)
Зависимости	Программная платформа .NET Framework версия 3.5

Таблица 12
Минимальные требования к аппаратному обеспечению с лицензией ENTERPRISE
базовая + антивирусная защита

Название оборудования	Требования
Процессор	2 ГГц, одноплатный
Жесткий диск	6 Гб свободной памяти на диске
ОЗУ	3 Гб свободной памяти
Операционная система	Windows 10/ Windows 10 LTSC/LTSB /Windows 7 (версии уточняются)

4.2 Функции

Функции **ARMA IE** приведены в таблице (см. Таблица 12).

Таблица 12
Функции ARMA IE

№ п/п	Функционал	Комментарий
Общие		
1.	Доступ к функционалу в соответствии с приобретённой лицензией	
2.	Доступ к функционалу в соответствии с ролевой политикой	Только для Администратора
Контроль использования съемных носителей информации		
3.	Запрет чтение и запись USB	
4.	Запрет чтение и запись CD/DVD	
Управление запуском ПО (whitelisting)		
5.	Включение/отключение белого списка программ	
6.	Ограничение перечня исполняемых программ	
7.	Режим обучения для определения списка ПО, к которому пользователю необходим доступ	
Контроль целостности файлов и ПО рабочих станций и серверов АСУ ТП		
8.	Включение/отключение контроль целостности	
9.	Выбор контролируемых директорий	
10.	Проверка контрольных сумм файлов по базе	
11.	Обновление эталонных образов	
Антивирусная защита		
12.	Включение/отключение антивирус	
13.	Выбор контролируемых директорий	
14.	Выбор реакции на обнаруженные вредоносные программы	Удалить/информировать
15.	Обновление антивирусных баз	
16.	Запуск антивирусной проверки	Контролируемых директорий/всего хоста
17.	Просмотр очереди команд, стоящих в очереди на антивирусное сканирования	
18.	Возможность остановить запущенную проверку	
Журнал событий безопасности		
19.	Отображение списка событий безопасности в интерфейсе ARMA Industrial Endpoint	
20.	Поиск и фильтрация по журналу	
21.	Ротация журнала событий	По времени/по размеру
Синхронизация с ARMA Management Console		
22.	Отправка событий безопасности в ARMA Management Console	Syslog

23.	Управление настройками ARMA Industrial Endpoint из интерфейса ARMA Management Console
-----	---

4.3 Варианты применения

На схеме показан вариант применения **ARMA IE** с другими продуктами **InfoWatch ARMA** (см. [Рисунок 12](#)).

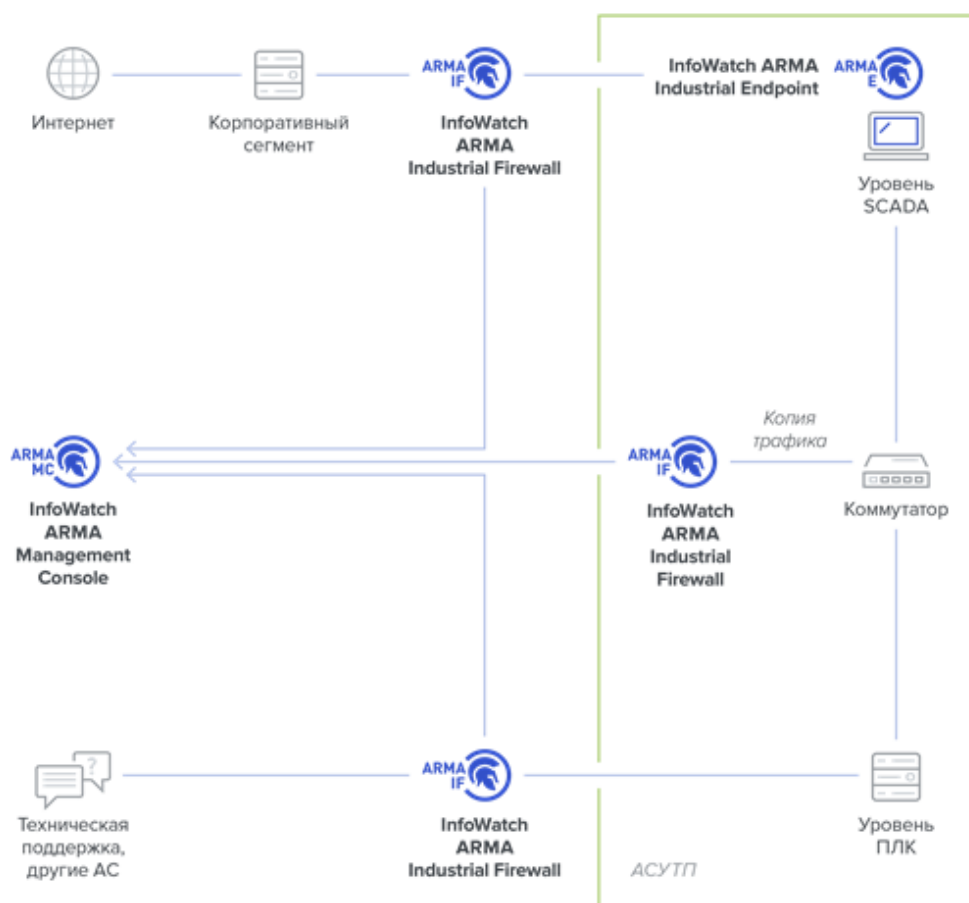


Рисунок 12 – Применение ARMA IE

4.4 Лицензирование

В **ARMA IE** предусмотрены следующие виды лицензии:

- Enterprise Базовая лицензия без антивирусной защиты;
- Enterprise Антивирусная защита.

Срок лицензии – 1 год.