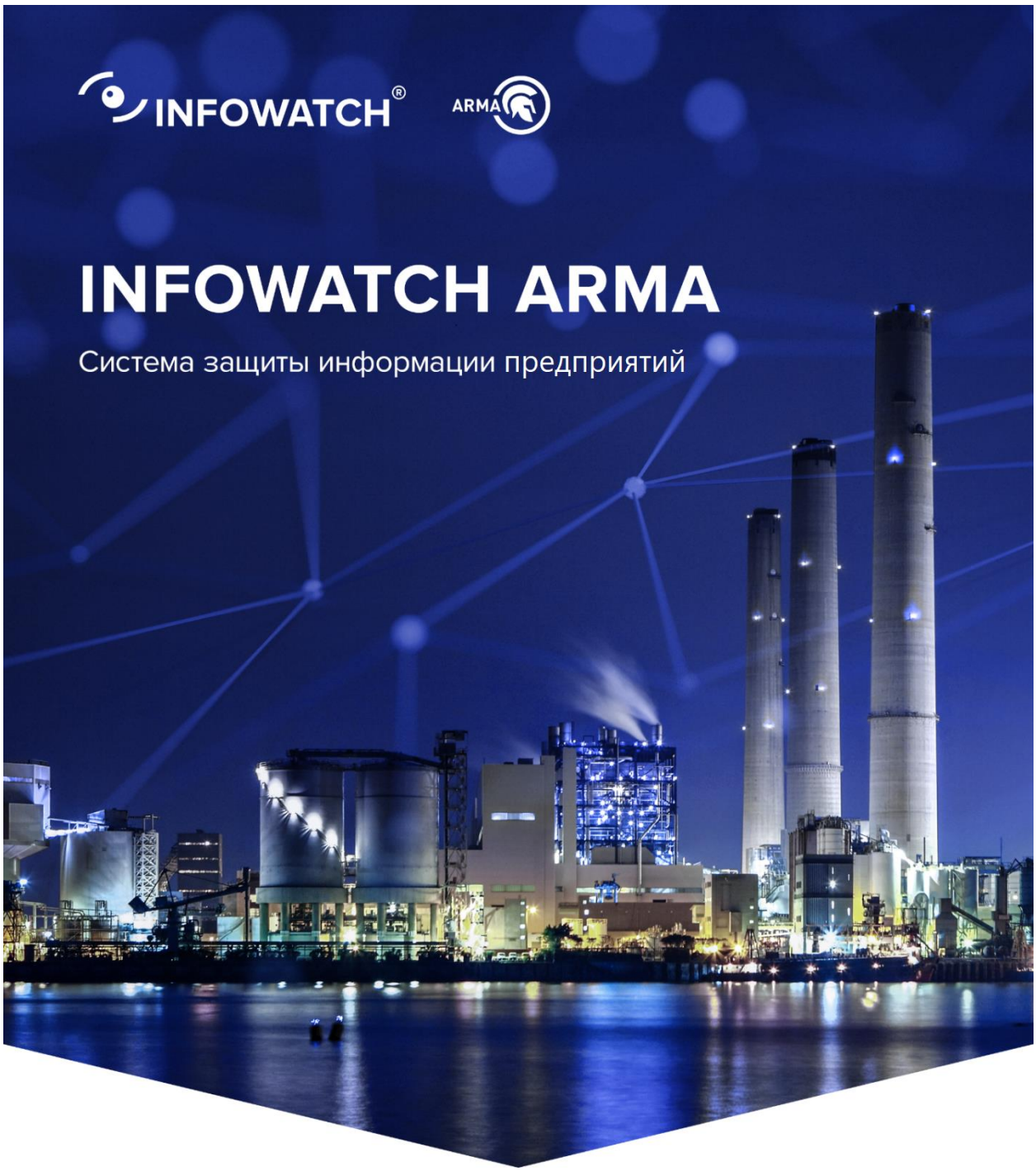


Техническое описание линейки продуктов InfoWatch ARMA

версия 17 ред. от 28.12.2022

Листов 39

ОГЛАВЛЕНИЕ

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
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
HTTPS	HyperText Transfer Protocol Secure, расширенный протокол HTTP

Термины и сокращения	Значение
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
S7 Communication	Протокол, предназначенный для обмена данными с контроллерами Siemens S7 и любым другим оборудованием, поддерживающим данный протокол
S7 Communication Plus	Протокол, предназначенный для обмена данными с оборудованием серий Siemens SIMATIC S7-1200 и S7-1500 и любым другим оборудованием, поддерживающим данный протокол
SCADA	Supervisory Control And Data Acquisition, диспетчерское управление и сбор данных
SMB	Server Message Block, сетевой протокол прикладного уровня для удалённого доступа к файлам

Термины и сокращения	Значение
SNMP	Simple Network Management Protocol, простой протокол сетевого управления
SSH	Secure Shell, безопасная оболочка
TCP	Transmission Control Protocol, протокол управления передачей
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 предприятий, в том числе в автоматизированных системах управления технологическим процессом (АСУ ТП). Система выполняет 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.

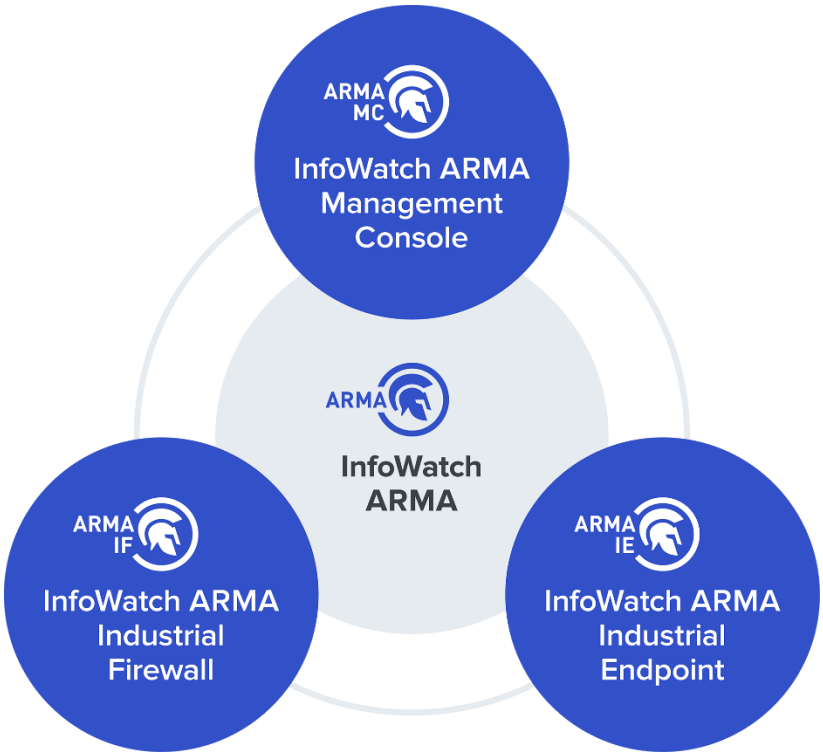


Рисунок 1 – Отечественная система защиты информации InfoWatch ARMA

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 ряда мер: контроль целостности, запуск ПО по белому списку, контроль подключения съемных носителей, антивирусная защита.

3. InfoWatch ARMA Industrial Firewall

Межсетевой экран нового поколения с системой обнаружения вторжений (IDS/IPS) и VPN, обеспечивающий предотвращение угроз для критически важных инфраструктур, в том числе 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.

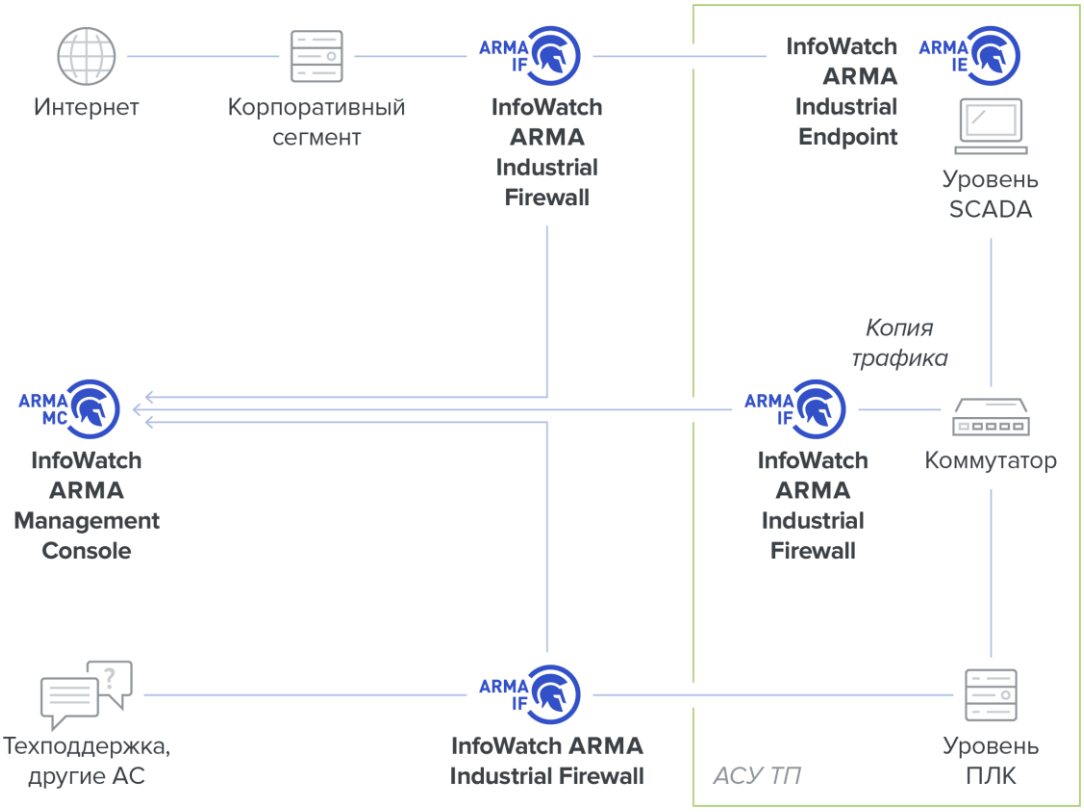


Рисунок 2 – Общая схема применения InfoWatch ARMA

2 INFOWATCH ARMA INDUSTRIAL FIREWALL

2.1 Технические требования

Установка **ARMA Industrial Firewall** производится на следующие типы платформ:

- аппаратная;
- виртуальная (гипервизор).

Установка на аппаратную платформу выполняется с использованием USB-накопителя, на который должен быть записан образ **ARMA** 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 Industrial Firewall** на аппаратную платформу необходимо использовать микропроцессорную архитектуру **x64**.

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

Для обеспечения корректного функционирования ПО и общей пропускной способности **ARMA Industrial Firewall** 150 Мбит/секунду при работе функций межсетевого экрана, системы предотвращения вторжений (СОВ) 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, x64
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	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:

a. для ОС семейства Windows:
   - Яндекс.Браузер, Chrome, Firefox;
b. для ОС семейства Linux /*nix:

- Яндекс.Браузер для Linux /*nix, Chrome для Linux /*nix, Firefox для Linux /*nix.

2.1.2 Требования к виртуальной платформе

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

- QEMU/KVM
- HyperV Generation 1
- VirtualBox версии 6.0.4 и выше
- VMware ESXi версии 5.5 обновления 2 и выше

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

- процессор: 8 ядер
- объем оперативной памяти: 16 ГБ
- размер виртуального диска: 25 ГБ
- количество сетевых интерфейсов: не менее 2

В такой конфигурации производительность **ARMA Industrial Firewall** обеспечивает обработку трафика до 100 Мбит/секунду при работе функций межсетевого экрана и системы предотвращения вторжений (СОВ). 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:
   - Яндекс.Браузер, Chrome, Firefox;
d. для ОС семейства Linux /*nix:
   - Яндекс.Браузер для Linux /*nix, Chrome для Linux /*nix, Firefox для Linux /*nix.

Примечание: Кластеризация ARMA Industrial Firewall не поддерживается на виртуальных машинах.

2.2 Функции

Функции **ARMA Industrial Firewall** приведены в таблице (см. Таблица 3).

Таблица 3
Функции ARMA Industrial Firewall

№	Функционал	МЭ	СОВ	МЭ + СОВ
Межсетевой экран				
1.	Контроль доступа пользователей к сетевым ресурсам, указание срока действия учетной	+	-	+

№	Функционал	МЭ	СОВ	МЭ + СОВ
	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, вирусы, сетевые атаки и т.п.	+	-	+
5.	Сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)	+	-	+
6.	Возможность задать расписание 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 задавать расписание срабатывания правил	-	+	+
Сетевые функции				
11.	Возможность работы в режиме прозрачного моста	+	+	+
12.	Поддержка статической маршрутизации	+	-	+
13.	Поддержка протоколов динамической маршрутизации: OSPF, RIP, BGP	+	-	+
14.	Прокси сервер	+	-	+
15.	Возможность настройки реверс-прокси (Nginx)	+	-	+
16.	Поддержка VLAN IEEE 802.1q	+	-	+

№	Функционал	МЭ	СОВ	МЭ + СОВ
17.	DHCP сервер	+	-	+
18.	Функции QoS (Traffic Shaping)	+	-	+
19.	Возможность зеркалирования сетевого трафика на отдельный порт	+	-	+
20.	Функционирование DNS клиента	+	+	+
21.	Кэширующий DNS сервер	+	+	+
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	+	+	+

№	Функционал	МЭ	СОВ	МЭ + СОВ
35.	Возможность аутентификации пользователей через Active Directory	+	+	+
36.	Возможность настройки двухфакторной авторизация пользователей (2FA)	+	+	+
37.	Поддержка функций централизованного управления	+	+	+
38.	Возможность передачи событий в InfoWatch ARMA Management Console	+	+	+
39.	Возможность задавать и синхронизировать временя по протоколу NTP	+	+	+
40.	Поддержка управления по SSH	+	+	+
41.	Поддержка управления через консольный порт	+	+	+
42.	Возможность экспорта и импорта конфигурации	+	+	+
43.	Возможность экспорта и импорта баз решающих правил	-	+	+
44.	Планировщик задач	+	+	+
45.	Возможность отключения/включения неиспользуемых сервисов	+	+	+
46.	Журналы системных событий	+	+	+
47.	Журналы событий безопасности	+	+	+
48.	Журналы событий NAT	+	-	+
49.	Журналы сервисных событий	+	+	+
50.	Фильтрация по времени в каждом из журналов	+	+	+
51.	Выгрузка журналов	+	+	+
52.	Возможность удаленного/локального обновления	+	+	+
53.	Возможность офлайн обновления: правил Suricate, сигнатур IPS, сигнатур анализа приложений и антивирусных баз	+	+	+

№	Функционал	МЭ	СОВ	МЭ + СОВ
54.	Возможность автоматической установки ARMA Industrial Firewall на оборудование при подключении к нему USB-носителя с программой установщиком	+	+	+
Функции отказоустойчивости, повышения надежности, резервирования				
55.	Поддержка отказоустойчивой конфигурации active-passive	+	-	+
56.	Loop Protection. Технологии STP, RSTP	+	-	+
57.	Сохранение резервных копий конфигурации на выделенный FTP-сервер	+	+	+
58.	Возможность настроить синхронизацию устройств при работе МЭ в режиме отказоустойчивого кластера	+	-	+
59.	Возможность расширенного отката конфигураций	+	-	+
60.	Возможность сброса настроек	+	-	+
61.	Шифрование резервной копии конфигурации	+	-	+
Защита доступа				
62.	Обеспечение защищенного канала администрирования системы за счет управления по протоколам HTTPS, SSH	+	+	+
63.	Конфигурация парольной политики	+	+	+
64.	Возможность аутентификации по различным базам: локальная база пользователей, каталог Active Directory (LDAP), RADIUS-сервер	+	+	+
65.	Контроль целостности программного обеспечения устройства защиты	+	+	+
66.	Контроль целостности конфигурационного файла	+	+	+
67.	Блокировка пользователя при 5 попытках неудачного входа	+	+	+
Антивирус				
68.	Потоковый антивирус в режиме прокси	+	-	+

№	Функционал	МЭ	СОВ	МЭ + СОВ
69.	Возможность конфигурации потокового антивируса, в том числе тайм аутов	+	-	+
70.	Возможность просмотреть текущую версию антивируса и сигнатуры	+	-	+
71.	Возможность загрузки новых сигнатур	+	-	+
72.	Просмотр, скачивание и очистка журнала событий антивируса	+	-	+
73.	Возможность обновления антивирусных баз	+	-	+
ICAP				
74.	Включение/отключение сервисов C-ICAP	+	-	+
75.	Настройка работы сервисов C-ICAP	+	-	+
76.	Осуществление сканирования на антивирусы с помощью сервисов протокола C-ICAP	+	-	+
77.	Просмотр, скачивание и очистка журнала сервисов C-ICAP	+	-	+
78.	Возможность интеграции с песочницами (SandBox)	+	-	+
VPN				
79.	Возможность построения криптографического тоннеля	+	-	+
80.	IPsec / OpenVPN / OpenVPN-ГОСТ	+	-	+

2.3 Поддерживаемые промышленные протоколы

ARMA Industrial Firewall 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
Modbus TCP x90 func. code (UMAS)	Modbus TCP x90 func. code (UMAS)
S7 Communication	S7 Communication
S7 Communication plus	S7 Communication plus
OPC DA	OPC DA
OPC UA	OPC UA
IEC 60870-5-104	IEC 60870-5-104
IEC 61850-8-1 MMS	IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE	IEC 61850-8-1 GOOSE
KRUG	KRUG
	Profinet

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: • 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);

Протокол	Стандарт	Степень разбора
		• 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: • «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;

Протокол	Стандарт	Степень разбора
		• причины передачи (ASDU cause of transfer)»; • 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 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

Протокол	Стандарт	Степень разбора
		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)».
S7 Communication plus	Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7- 1200 и S7-1500	Сообщения по протоколу S7Communication Plus разделяются по типу сообщения: • REQUEST; • RESPONSE; • NOTIFY; • RESPONSE2. По типу взаимодействия: • CONNECT; • DATA; • DATAFW1_5; • KEEPALIVE; • EXT_KEEPALIVE. По функции: • EXPLORE; • CREATEOBJECT; • DELETEOBJECT; • SETVARIABLE; • GETLINK; • SETMULTIVAR; • GETMULTIVAR;

Протокол	Стандарт	Степень разбора
		• BEGINSEQUENCE; • ENDSEQUENCE; • INVOKE; • GETVARSUBSTR. При выборе в поле **«Функция»** функции «EXPLORE» возможно выбрать диапазоны для параметров EXPLORE_AREA и EXPLORE_ATTR_ID. При выборе в поле **«Функция»** функции «CREATEOBJECT» возможно выбрать диапазон для параметра CREATEOBJECT_ATTR_ID. При выборе в поле **«Функция»** функции «DELETEOBJECT» возможно выбрать диапазоны для параметров DELETEOBJECT_OBJ_ID и DELETEOBJECT_ATTR_ID. При выборе в поле **«Функция»** функции «GETLINK» возможно выбрать диапазон для параметра GETLINK_ATTR_ID. При выборе в поле **«Функция»** функции «SETMULTIVAR» возможно выбрать диапазон для параметра SETMULTIVAR_ATTR_ID. При выборе в поле **«Функция»** функции «GETMULTIVAR» возможно выбрать диапазон для параметра GETMULTIVAR_ATTR_ID. При выборе в поле **«Функция»** функции «GETVARSUBSTR» возможно выбрать диапазон для параметра GETVARSUBSTR_ATTR_ID.
OPC UA	IEC 62541	Сообщения по протоколу OPC UA разделяются по типу сообщения: • HELLO (маркер начала передачи данных между клиентом и сервером); • ACKNOWLEDGE (ответ на сообщение типа HELLO); • 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.

Протокол	Стандарт	Степень разбора
		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; • 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.

Протокол	Стандарт	Степень разбора
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); • 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 «datset»; • 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»;

Протокол	Стандарт	Степень разбора
		• 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 Industrial Firewall 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 Industrial Firewall** на границе с корпоративным сегментом.

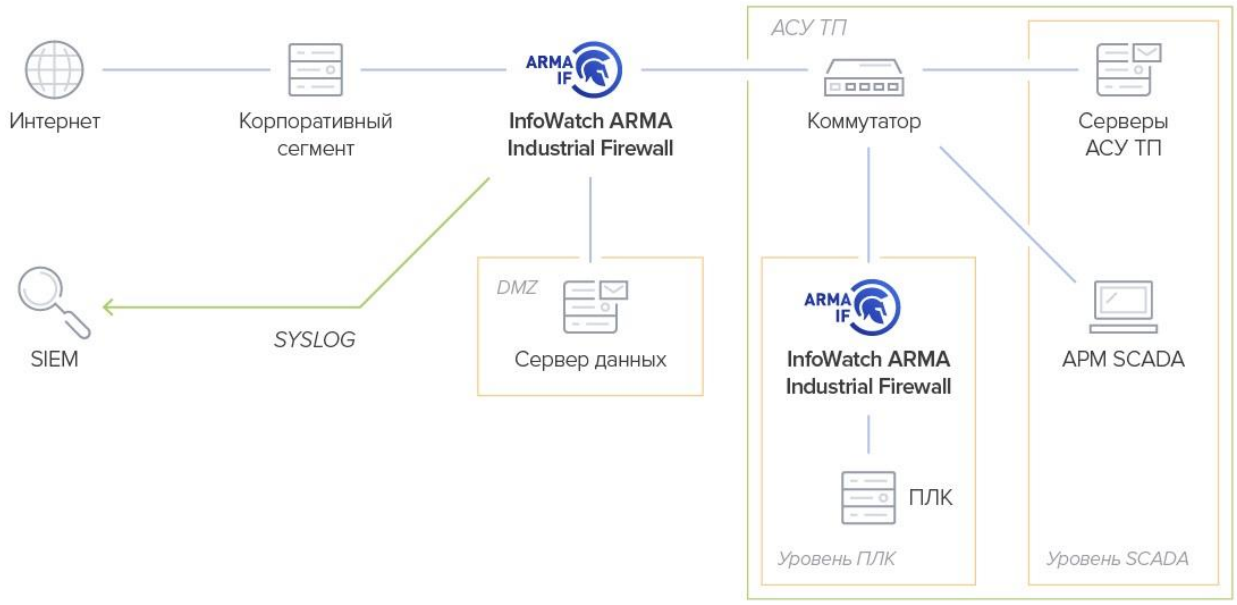


Рисунок 4 – Применение на границе с корпоративным сегментом

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).

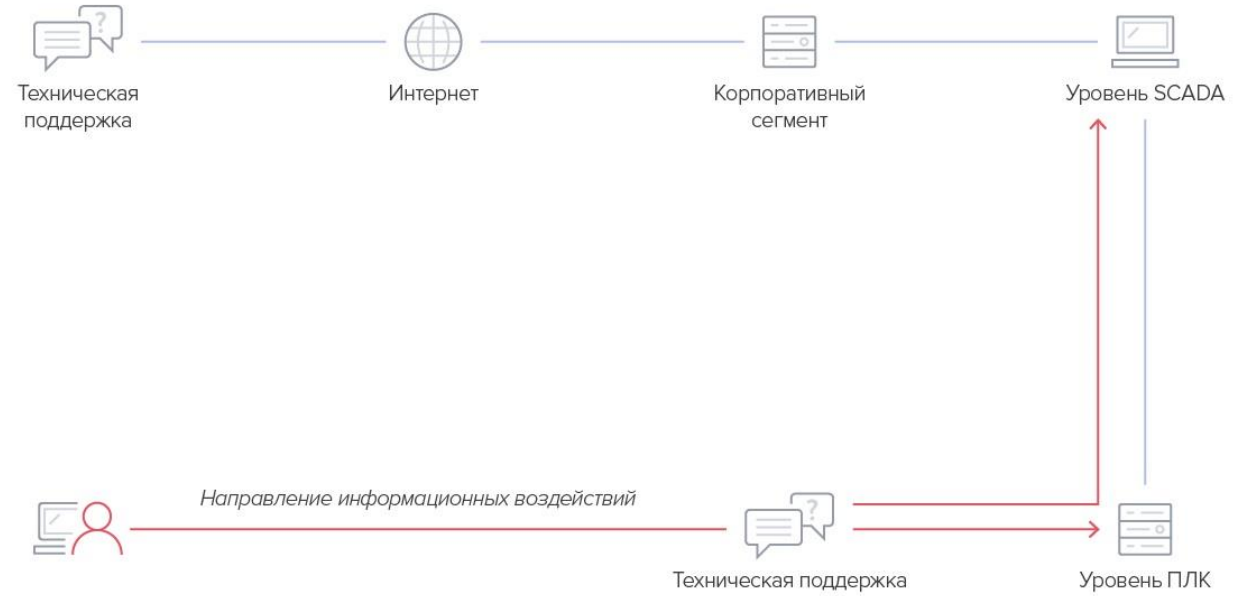


Рисунок 5 – Связь с технической поддержкой. Угрозы

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

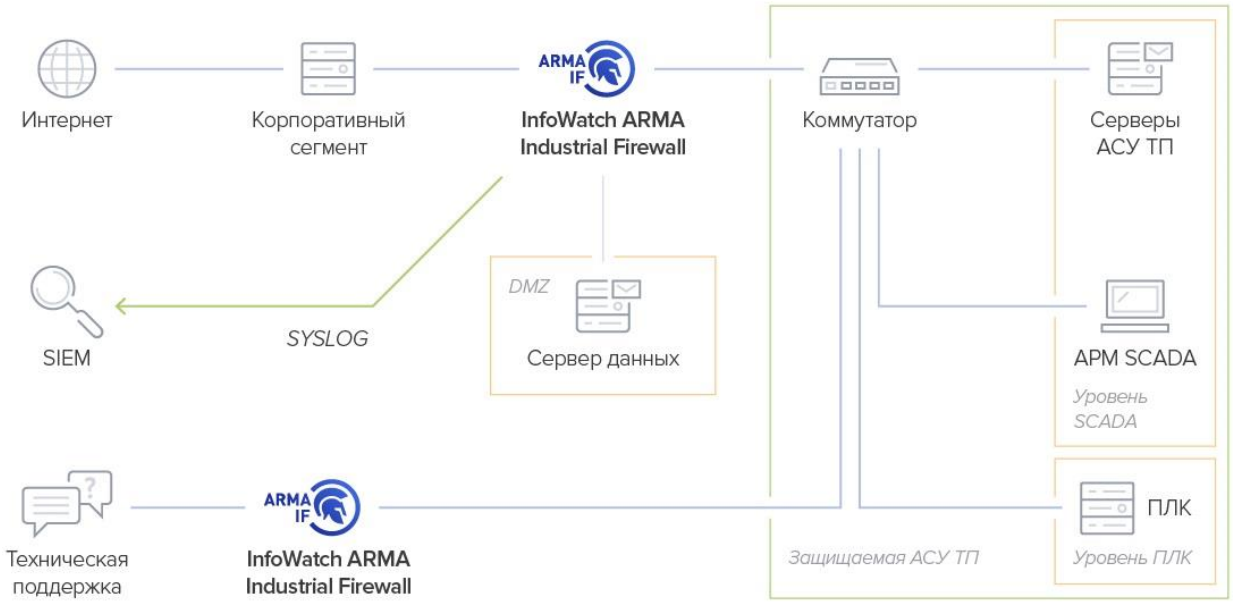


Рисунок 6 – Применение для обеспечения безопасной связи с технической поддержкой

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).

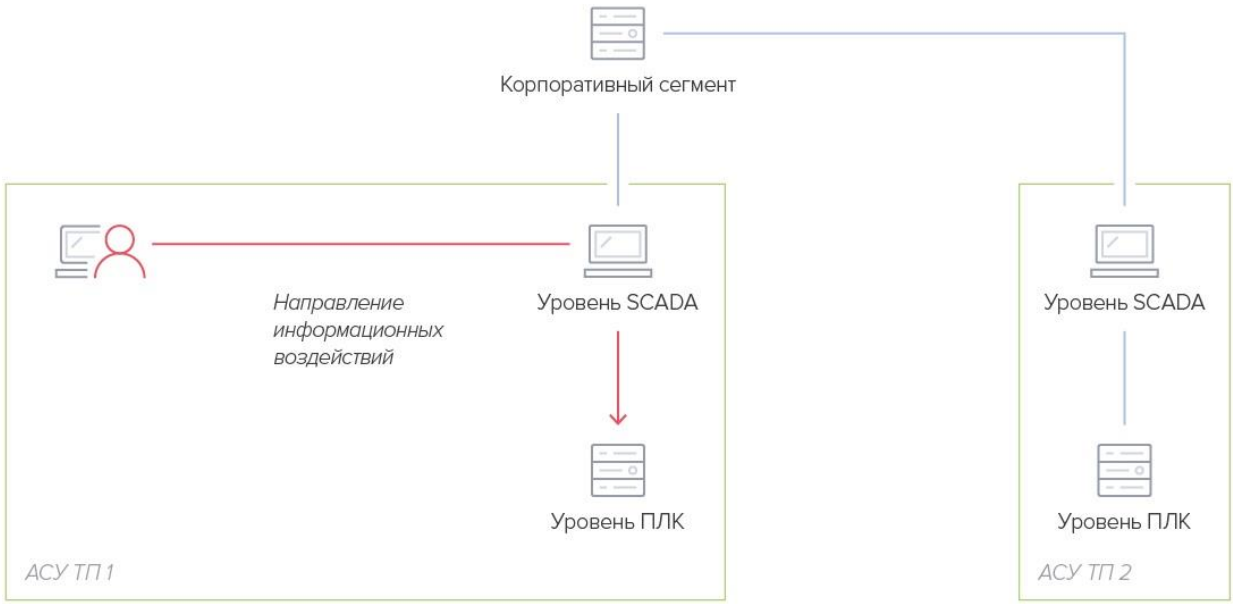


Рисунок 7 – Связь со смежными АСУ ТП. Угрозы

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

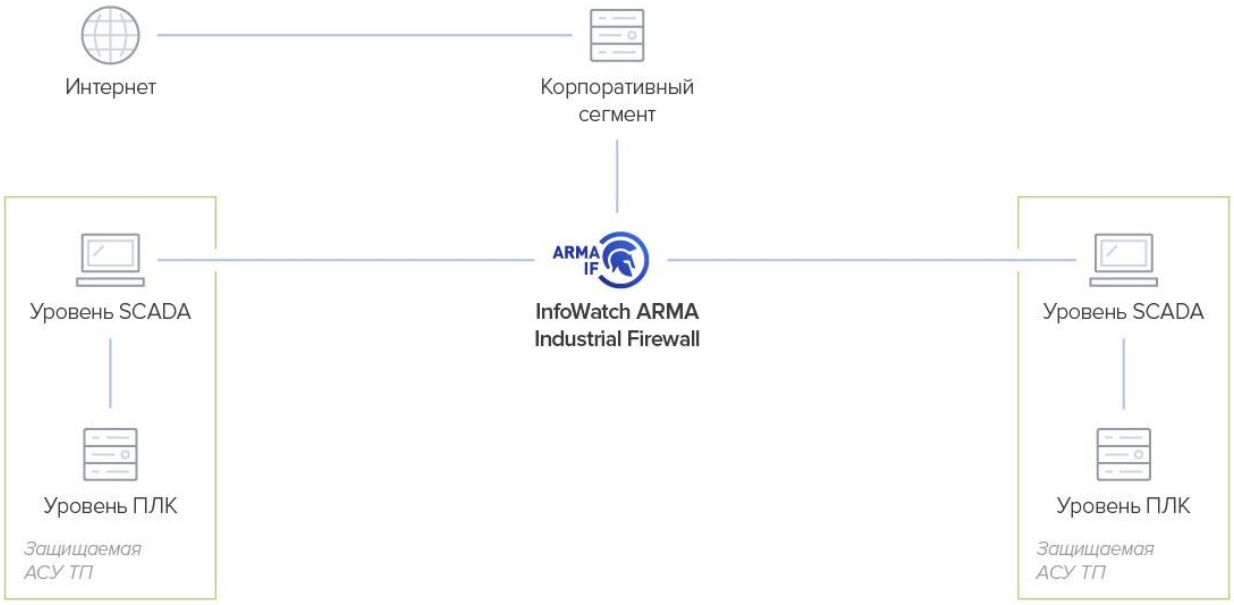


Рисунок 8 – Применение для обеспечения безопасной связи со смежными АСУ ТП

2.4.4 Мониторинг внутри АСУ ТП

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

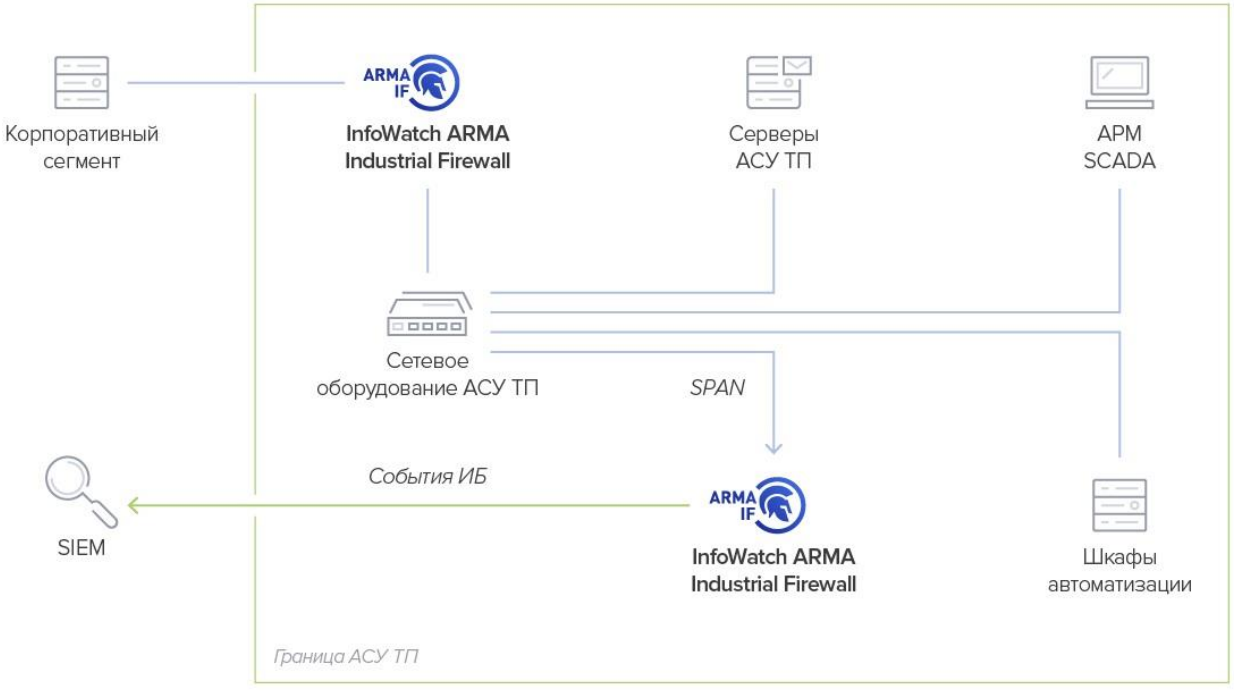


Рисунок 9 – Применение для мониторинга внутри АСУ ТП

2.5 Обнаруживаемые атаки

ARMA Industrial Firewall 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 Industrial Firewall**:
1. Для постановки в стойку 19”:

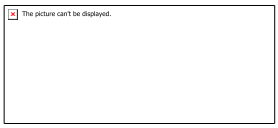
- в серверном исполнении;
- в промышленном исполнении в соответствии требованиям ГОСТ Р МЭК 61850-3, ГОСТ Р 52931, ГОСТ IEC 60950-1.

2. Для крепления на DIN рейку:

- в промышленном исполнении.

В таблице ниже (см. Таблица 6) приведены основные технические характеристики различных аппаратных конфигураций **ARMA Industrial Firewall**.

Таблица 6
Аппаратные конфигурации ARMA Industrial Firewall

Параметр	ARMA-BOX	ARMA-ELECTRO	ARMA-19RACK
Изображение			
Исполнение	Настольное промышленное исполнение, без движущихся частей	1U промышленное исполнение, без движущихся частей	1U исполнение для монтажа в стойку. Серверное исполнение
ОЗУ	32 Гб оперативной памяти	16 Гб оперативной памяти	от 32 Гб оперативной памяти

Параметр	ARMA-BOX	ARMA-ELECTRO	ARMA-19RACK
Жесткий диск	от 256 Гб твердотельный накопитель	от 240 Гб твердотельный накопитель	от 240 Гб твердотельный накопитель
Сетевые порты	Ethernet - 6 портов 1 Гб/с	Ethernet - 4 порта 1 Гб/с	Конфигурации: 1. Ethernet – 8 портов 1 Гб/с в конфигурациях ARMA-19RACK-8E / 8E-RM 2. Ethernet – 8 портов SFP+, 10 Гб/с (+ 4 шт. медных трансивера 10 Гб/с) в конфигурациях ARMA-19RACK-10G / 10G-RM
Пассивное охлаждение	Да	Да	Нет
Степень защиты корпуса	IP-40	IP-20	-
Температура эксплуатации	-40 … 60 °C (Без адаптера питания, с индустриальным SSD и памятью DDR)	-20°C…+70°C	0 … 40 °C
Влажность	10 … 90 % (без конденсата)	5 … 95 % (без конденсата)	10 … 95 % (без конденсата)
Вибрация	IEC 60068-2-64 (w/ SSD: 3Grms STD, random, 5 - 500 Hz, 1 hr/axis)	Воздействий стационарной синусоидальной вибрации: – с амплитудой перемещения 3 мм при частоте вибрации (0,5-9) Гц; – с амплитудой ускорения 10 м/с2 при частоте вибрации (9-200) Гц и 15 м/с2 при частоте - (200-500) Гц	-
Удар	IEC 60068-2-27 (w/ SSD: 50G, half-sine, 11 ms duration)	Воздействий ударов длительностью 2-22 мс (половина синусоиды) с	-

Параметр	ARMA-BOX	ARMA-ELECTRO	ARMA-19RACK
		пиковым ускорением 100 м/с2	
Питание	12...24 В, внешний блок питания	2x220 Вт.	2x650 Вт., с возможностью горячей замены
Общая пропускная способность всего устройства с включенным модулем МЭ (оценочное значение)	до 4 Гб/с	до 2 Гб/с	до 8 Гб/с в конфигурациях ARMA-19RACK-8E / 8E-RM до 60 Гб/с в конфигурациях ARMA-19RACK-10G / 10G-RM
Общая пропускная способность всего устройства с включенными модулями МЭ и СОВ и DPI (оценочное значение)	до 600 Мб/с	до 100 Мб/с	до 8 Гб/с в конфигурациях ARMA-19RACK-8E / 8E-RM до 25 Гб/с в конфигурациях ARMA-19RACK-10G / 10G-RM
Межсетевой экран, пакетов/с (оценочное значение)	до 1 400 000	до 600 000	до 2 700 000
Межсетевой экран, количество одновременных соединений (сессий) (оценочное значение)	до 3 100 000	до 1 500 000	До 9 200 000 в конфигурациях ARMA-19RACK-8E / 8E-RM До 18 000 000 в конфигурациях ARMA-19RACK-10G / 10G-RM
Габаритные размеры (ШхГхВ)	280x210x80,5	483x163x44 (1U)	444x615x44 (1U) в конфигурациях ARMA-19RACK-8E / 10G 482x762x43,4 (1U) в конфигурациях ARMA-19RACK-8E-RM / 10G-RM
Вес	5,6 кг.	4 кг.	11 кг.
Дополнительно	-	Соответствует требованиям ГОСТ Р МЭК 61850-3, ГОСТ Р	Включен в реестр Минпромторг РФ (Конфигурации ARMA-

Параметр	ARMA-BOX	ARMA-ELECTRO	ARMA-19RACK
		52931, ГОСТ IEC 60950-1.	19RACK-8E-RM / 10G-RM)

Гарантия на оборудование – 1 год.

Примечание: Все технические характеристики и фотографии аппаратных платформ могут быть изменены на усмотрение вендора без предварительного уведомления.

2.7 Лицензирование

В **ARMA Industrial Firewall** предусмотрены следующие виды лицензии:

- Enterprise МЭ (межсетевой экран (МЭ));
- Enterprise СОВ (система обнаружения вторжений);
- Enterprise МЭ + СОВ (межсетевой экран нового поколения (NGFW));
- Enterprise Промышленные протоколы.

ВАЖНО! Лицензия «Enterprise Промышленные протоколы» устанавливается только вместе с лицензией «Enterprise СОВ».

ВАЖНО! Функционал ГОСТ-VPN реализован в рамках лицензий «Enterprise МЭ» и «Enterprise МЭ + СОВ». Лицензия для использования "OpenVPN-ГОСТ" приобретается отдельно у вендора или дистрибьюторов.

Срок лицензии – Бессрочная.

В таблице (см. Таблица 3) перечислены функции **ARMA Industrial Firewall** для каждого вида лицензии.

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**.

Для аппаратной платформы, на которую устанавливается **ARMA MC** достаточно руководствоваться минимальными требованиями к аппаратному обеспечению (см. Таблица 7).

Таблица 7

Минимальные требования к аппаратному обеспечению

Название оборудования	Требования
Процессор	2,0 ГГц, четырехъядерный, x64
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 10/100/1000 Мбит/сек

3.1.2 Требования к виртуальной платформе

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

- 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 8).

Таблица 8

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:

a. для ОС семейства Windows:
   - Chrome, Firefox;
b. для ОС семейства Linux /*nix:
   - Chrome для Linux /*nix, Firefox для Linux /*nix.

3.2 Функции

Функции **ARMA MC** приведены в таблице (см. Таблица 9).

Таблица 9
Функции ARMA MC

№	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.	Управление пользователями, включая разблокировку заблокированных пользователей	
5.	Поиск и фильтрация по всем журналам	
6.	Шифрование для подключения к web-интерфейсу	(TLS)
7.	Ротация журналов	
8.	Доступ ко всем скачанным из ARMA Management Console данным пользователя	
Подключение источников событий		
9.	Подключение источников событий	по IP и порту
Централизованное управление системами защиты		
10.	Защищенное централизованное управление продуктами InfoWatch ARMA	По API (HTTPS)

11.	Управление InfoWatch ARMA Industrial Firewall через веб-интерфейс	
12.	Импорт/экспорт конфигурации InfoWatch ARMA Industrial Firewall	Экспорт конфигурации на одно/несколько устройств
13.	Импорт/экспорт баз решающих правил InfoWatch ARMA Industrial Firewall	Обновление базы правил СОВ
Централизованное управление ARMA Industrial Endpoint		
14.	Управление InfoWatch ARMA Industrial Endpoint через веб-интерфейс	
15.	Индивидуальная настройка ARMA Industrial Endpoint по параметрам	Контроль целостности, запуск ПО белому списку, управление USB устройствами, антивирусная защита, настройка ротации журнала событий.
16.	Клонирование ARMA Industrial Endpoint	Включая все настройки
17.	Обновление конфигурации с InfoWatch ARMA Industrial Endpoint	
18.	Возможность скачать конфигурацию InfoWatch ARMA Industrial Endpoint	
19.	Копирование конфигурации с InfoWatch ARMA Industrial Endpoint	
Сбор и анализ данных аудита		
20.	Централизованный сбор событий с подключенных InfoWatch ARMA Industrial Firewall	
21.	Централизованный сбор событий 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 Bush скрипта - Запуск исполняемого файла - HTTPS - Отправка по Syslog - Создание нового актива
		Добавление рекомендаций 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.	Управление инцидентами	
29.	Отправка инцидентов в ГосСОПКА по решению пользователя	
30.	Взаимодействие с сотрудниками НКЦКИ в online режиме	
Отображение активов сети		
31.	Список активов сети	
32.	Детальная информация о каждом активе, с возможностью дополнения	

3.3 Варианты применения

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

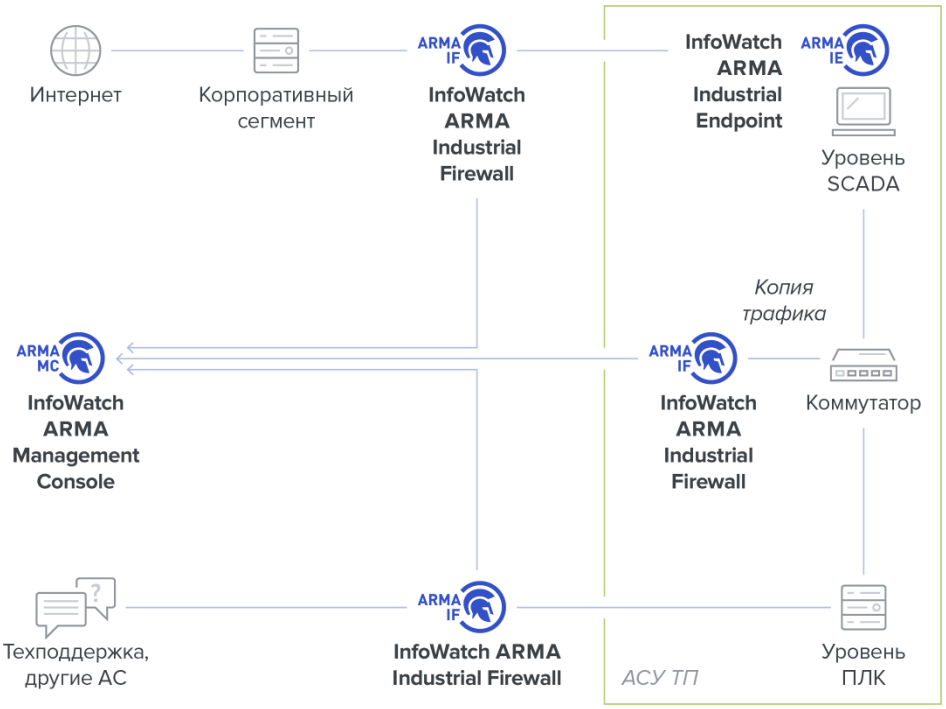


Рисунок 10 – Применение ARMA MC

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 Модуль централизованного управления (по количеству подключаемых источников событий);
- Enterprise Модуль сбора и анализа событий;
- Enterprise Модуль корреляции событий, управления и реакции на инциденты ИБ.

Срок лицензии – бессрочная.

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, одноядерный, x86 или x64
Жесткий диск	200 Мб свободной памяти на диске
ОЗУ	100 Мб свободной памяти
Операционная система	Windows 10/ Windows 10 LTSC/LTSB /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, одноядерный
Жесткий диск	6 ГБ свободной памяти на диске
ОЗУ	3 ГБ свободной памяти
Операционная система	Windows 10/ Windows 10 LTSC/LTSB /Windows 7

4.2 Функции

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

Таблица 12
Функции ARMA IE

№	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).

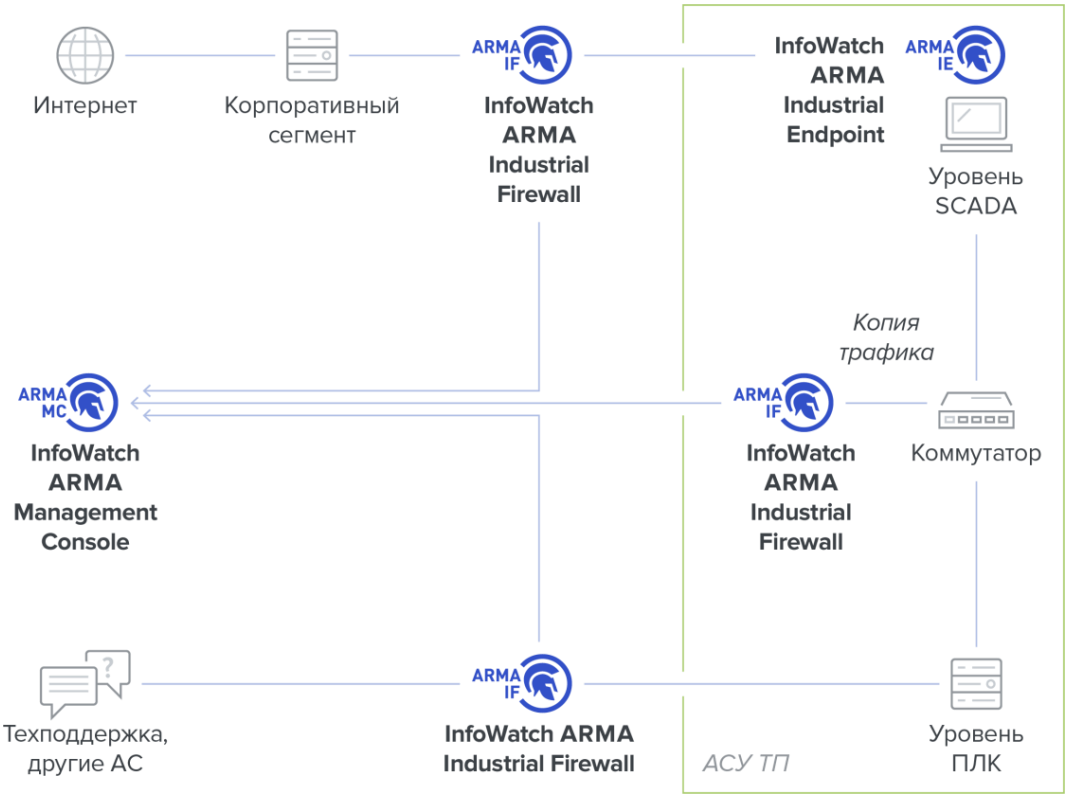


Рисунок 12 – Применение ARMA IE

4.4 Лицензирование

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

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

Срок лицензии – 1 год.