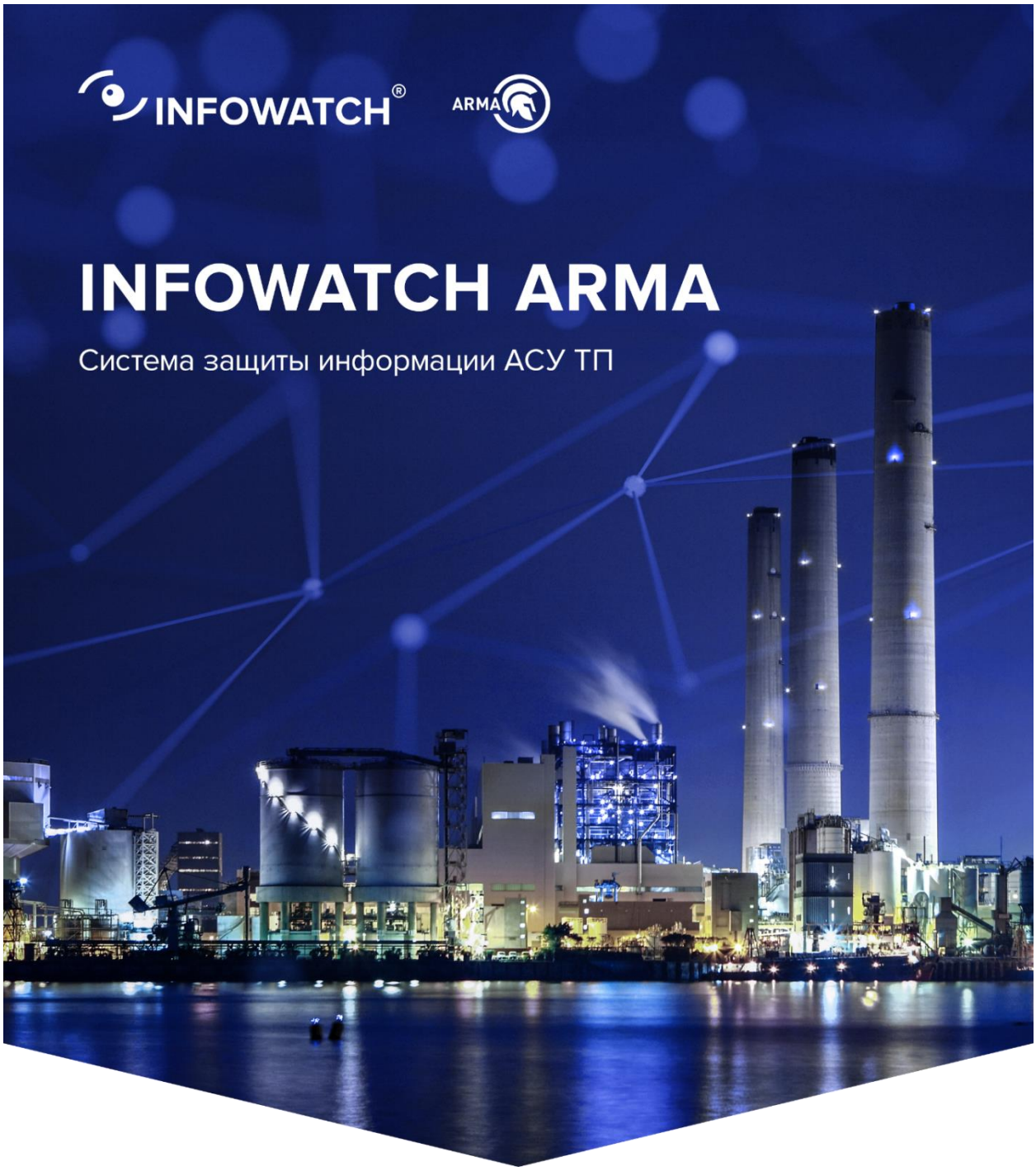

Техническое описание

версия 12 ред. от 25.01.2021

Листов 28

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АСУ	–	автоматизированная система управления
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	–	(англ. Advanced Configuration and Power Interface) – усовершенствованный интерфейс управления конфигурацией и питанием
APDU	–	(англ. Application Protocol Data Unit) – протокольный блок данных прикладного уровня
API	–	(англ. Application Programming Interface) – программный интерфейс приложения
CIP	–	(англ. Common Industrial Protocol) – общий промышленный протокол
DHCP	–	(англ. Dynamic Host Configuration Protocol) – протокол динамической настройки узла
GOOSE	–	(англ. Generic Object-Oriented Substation Event) – общее объектно-ориентированное событие на подстанции
FTP	–	(англ. File Transfer Protocol) – протокол передачи файлов по сети
HTTPS	–	(англ. HyperText Transfer Protocol Secure) – расширенный протокол HTTP
ICAP	–	(англ. Internet Content Adaptation Protocol) – протокол адаптации контента Интернета
IEC	–	англ. International Electrotechnical Commission) – Международная электротехническая комиссия
ID	–	идентификатор
IOA	–	(англ. Information Object Address) – адрес объекта информации
IP	–	(англ. Internet Protocol) – межсетевой протокол
LDAP	–	(англ. Lightweight Directory Access Protocol) – облегчённый протокол доступа к каталогам
MMS	–	(англ. Manufacturing Message Specification) – протокол передачи данных по технологии «клиент-сервер»
NAT	–	(англ. Network Address Translation) – преобразование сетевых адресов
NTP	–	(англ. Network Time Protocol) – протокол сетевого времени

OPC	–	(англ. Open Platform Communications) – семейство технологий управления объектов автоматизации
OSPF	–	(англ. Open Shortest Path First) – протокол динамической маршрутизации
PAT	–	(англ. Port Address Translation) – трансляция порт-адрес
RIP	–	(англд. Routing Information Protocol) – протокол маршрутной информации
SCADA	–	(англ. Supervisory Control And Data Acquisition) – диспетчерское управление и сбор данных
SMB	–	(англ. Server Message Block) – сетевой протокол прикладного уровня для удалённого доступа к файлам
SNMP	–	(англ. Simple Network Management Protocol) – простой протокол сетевого управления
SSH	–	(англ. Secure Shell) – безопасная оболочка
TCP	–	(англ. Transmission Control Protocol) – протокол управления передачей
VLAN	–	(англ. Virtual Local Area Network) – виртуальная локальная сеть

АННОТАЦИЯ

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

1 INFOWATCH ARMA

InfoWatch ARMA – это отечественная система (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.

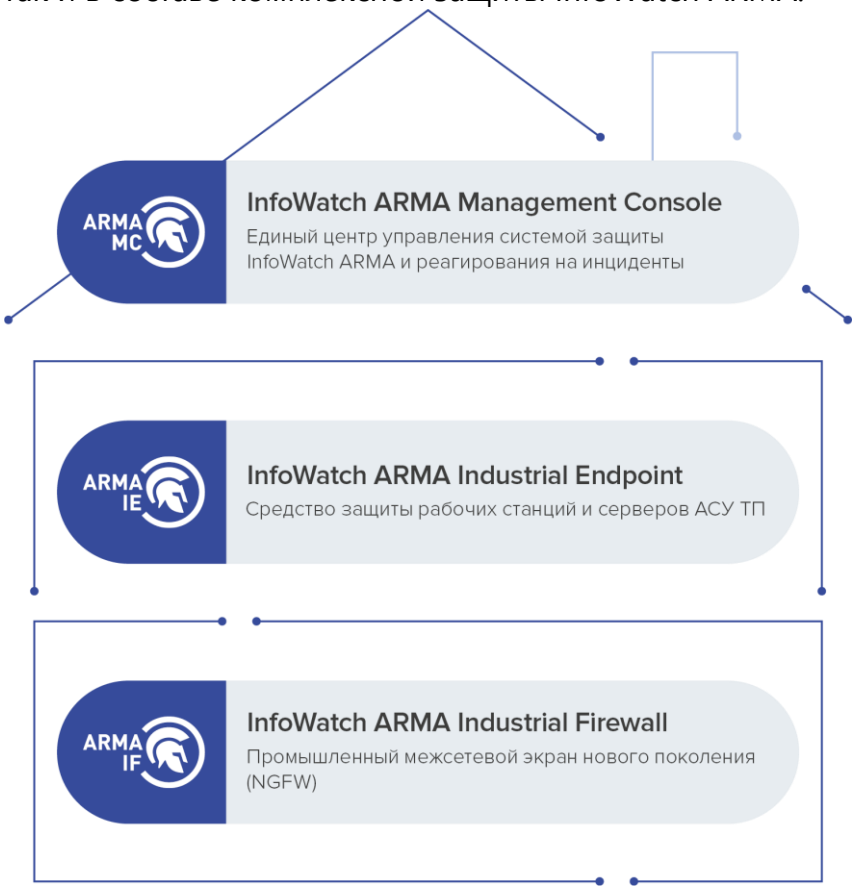

Рисунок 1 – Отечественная система защиты информации InfoWatch ARMA

1. InfoWatch ARMA Management Console.

Единый центр управления решениями InfoWatch ARMA и реагирования на инциденты.

2. InfoWatch ARMA Industrial Endpoint.

Осуществляет контроль целостности программного обеспечения (ПО) рабочих станций и серверов, запуска приложений и использования съемных носителей.

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. Проходит сертификацию 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;
– Центр экспертизы.

Общая схема применения InfoWatch ARMA представлена на рисунке 2. Надежная производительность и мощное централизованное управление обеспечивают непревзойденную ценность в простом, универсальном решении.

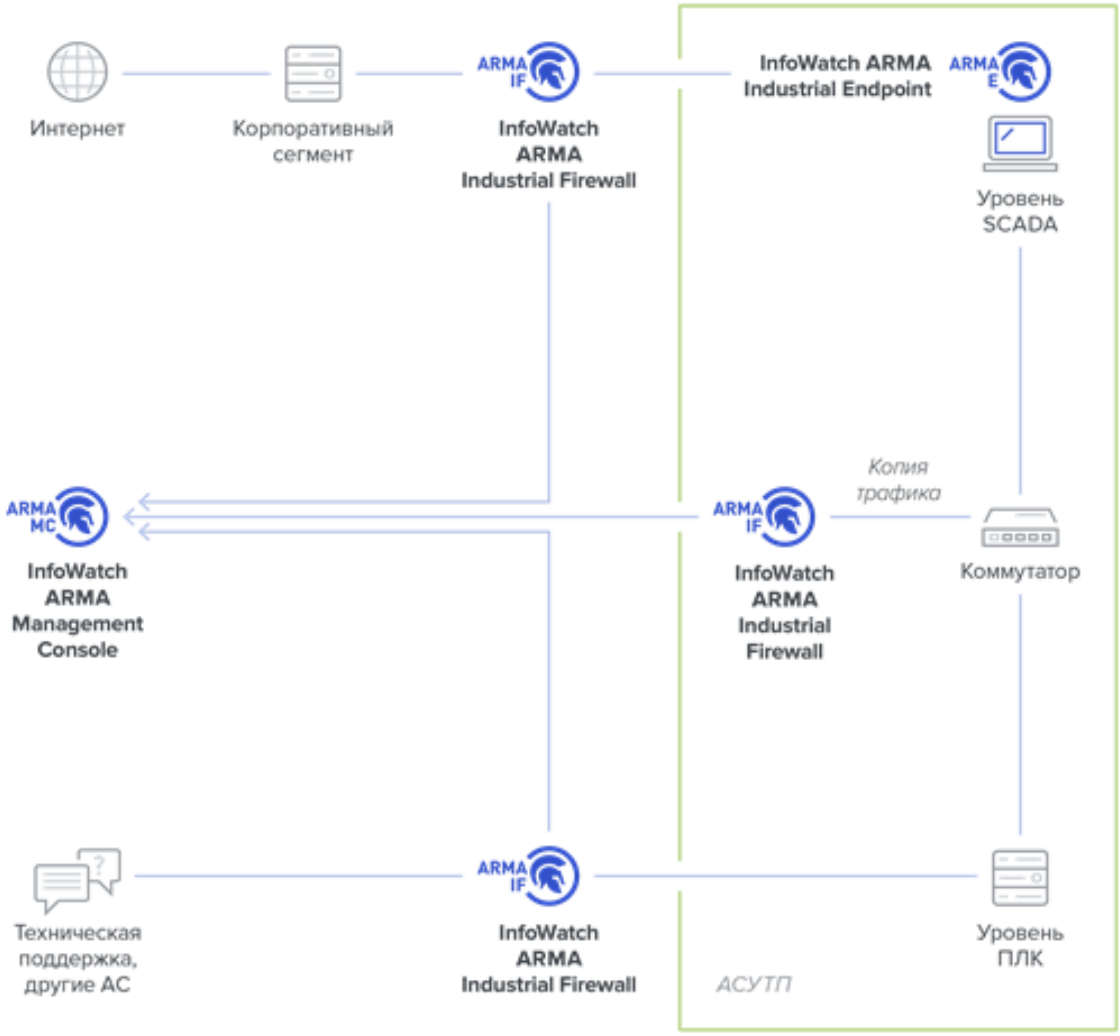

Рисунок 2 – Общая схема применения InfoWatch ARMA

2 INFOWATCH ARMA INDUSTRIAL FIREWALL

2.1 Функции

Функции InfoWatch ARMA Industrial Firewall приведены в таблице ниже.

Таблица 1 – Функции InfoWatch ARMA Industrial Firewall

№ п/п	Функционал	Комментарий
Межсетевой экран		
1.	Контроль доступа пользователей к сетевым ресурсам, указание срока действия учетной записи пользователя (Портал авторизации)	
2.	Фильтрация сетевого трафика с учетом параметров пакета на сетевом и транспортном уровнях	
3.	Точная идентификация, классификация и предотвращение проникновения вредоносного трафика, включая червей, вирусов, сетевых атак и т.п.	
4.	Сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)	
5.	Возможность задания расписания срабатывания правил	
Система обнаружений вторжений		
6.	Обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровне	
7.	Обновление базы решающих правил	Локально, централизованно, по протоколам: FTP, SMB
8.	Возможность разработки пользовательских правил СОВ	Формат правил – Snort совместимый
Сетевые функции		
9.	Возможность работы в режиме прозрачного моста	
10.	Поддержка статической маршрутизации	
11.	Поддержка протоколов динамической маршрутизации	Поддерживаемые протоколы маршрутизации: RIP, OSPF
12.	Прокси сервер	
13.	Поддержка VLAN IEEE 802.1q	
14.	DHCP сервер	
15.	Функции QoS (Traffic Shaping)	

№ п/п	Функционал	Комментарий
16.	Возможность зеркалирования сетевого трафика на отдельный порт	
17.	Поддержка IPv6	
18.	Поддержка объединения физических интерфейсов в логические	
19.	Просмотр таблицы активных соединений	
Функции сбора и анализа событий		
20.	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
21.	Мониторинг состояния по SNMP v.1, 2, 3	
22.	Экспорт событий по протоколу SYSLOG (интеграция с SIEM-системами), SYSLOG в формате CEF	
23.	Возможность сбора и экспорта дампов трафика	
24.	Интеграция по ICAP с внешними системами	
25.	Сбор и экспорт статистики NetFlow	
26.	Мониторинг загрузки и состояния сетевых интерфейсов, CPU,памяти и программных модулей	
Функции управления		
27.	Доступ к продукту и управление на ролевой основе, гибкая настройка прав доступа	
28.	Возможность аутентификации пользователей через Active Directory	
29.	Поддержка функций централизованного управления	
30.	Задание и синхронизации времени по протоколу NTP	
31.	Поддержка управления по SSH	
32.	Возможность экспорта и импорта конфигурации	
33.	Возможность экспорта и импорта баз решающих правил	Локально
34.	Планировщик задач	На основе сервиса «cron»
35.	Возможность отключения/включения неиспользуемых сервисов	

№ п/п	Функционал	Комментарий
36.	Журналы системных событий	
37.	Возможность удаленного/локального обновления	
Функции отказоустойчивости, повышения надежности, резервирования		
38.	Поддержка отказоустойчивой конфигурации active-passive	
39.	Loop Protection. Технологии STP, RSTP	Доступен для режима сетевого моста
40.	Сохранение резервных копий конфигурации на выделенный FTP-сервер	
Защита доступа		
41.	Обеспечение защищенного канала администрирования системы за счет управления по протоколам HTTPS, SSH	
42.	Конфигурация парольной политики	Задание «сложности» пароля
43.	Возможность аутентификации по различным базам: локальная база пользователей, каталог Active Directory (LDAP), RADIUS-сервер	
44.	Контроль целостности программного обеспечения устройства защиты	
VPN		
45.	Возможность построения криптографического тоннеля	VPN IPSEC, OpenVPN
46.	Site-to-site VPN	

2.2 Поддерживаемые промышленные протоколы

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

Поддерживаемые протоколы отражены в таблице 2.

Таблица 2 – Поддерживаемые протоколы

Возможность фильтрации	Обнаружение вторжений и мониторинг (без фильтрации)
Modbus TCP IEC 60870-5-104 S7 Communication OPC UA OPC DA	Modbus TCP IEC 60870-5-104 S7 Communication OPC UA OPC DA

Возможность фильтрации	**Обнаружение вторжений и мониторинг (без фильтрации)**
Modbus TCP x90 func. code (UMAS) IEC 61850-8-1 MMS IEC 61850-8-1 GOOSE	Modbus TCP x90 func. code (UMAS) IEC 61850-8-1 MMS IEC 61850-8-1 GOOSE ENIP/CIP Profibus S7 Communication plus DNP3

Для протоколов, по которым возможна фильтрация, указана поддержка (Таблица 3).

Таблица 3 – 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 возможно задать правило обнаружения на основе признака совпадения: – по функции; – по данным. При обнаружении по функции возможно задать дополнительные опции: – используемую функцию, подфункцию; – используемую категорию функции. При обнаружении по данным возможно задать дополнительные опции: – код функции в формате диапазона; – адрес изменяемых данных в формате диапазона; – значение данных в формате диапазона.
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, либо 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

Протокол	Стандарт	Степень разбора
		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)»; – 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.

Протокол	Стандарт	Степень разбора
		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 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); – 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.
UMAS	Основан на протоколе Xway Unite. Протокол Umas используется	Сообщения по протоколу UMAS разделяются по функциям: – инициализация UMAS сессии; – чтение информации о проекте;

Протокол	Стандарт	Степень разбора
	для настройки и мониторинга ПЛК Schneider-Electric.	– чтение внутренней информации PLC; – назначение PLC владельца; – инициализация загрузки (копирование с инженерного ПК на PLC); – завершение загрузки (копирования с инженерного ПК на PLC); – инициализация скачивания (копирование с PLC на инженерный ПК); – конец скачивания (копирования с PLC на инженерный ПК); – включение PLC; – выключение PLC.
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, по значению поля datset, по значению поля gocbref, по значению поля goid.

2.2.1 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.

2.3 Варианты применения

InfoWatch ARMA Industrial Firewall может быть расположен на нескольких участках сети:

- на границе с корпоративным сегментом;
- защита канала технической поддержки;
- защита смежных автоматизированных систем управления (АСУ);

– мониторинг внутри АСУ ТП.

2.3.1 На границе с корпоративным сегментом

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

Рисунок 3 – Угрозы на границе с корпоративным сегментом

На схеме, представленной на рисунке 4, показан вариант применения InfoWatch ARMA Industrial Firewall на границе с корпоративным сегментом.

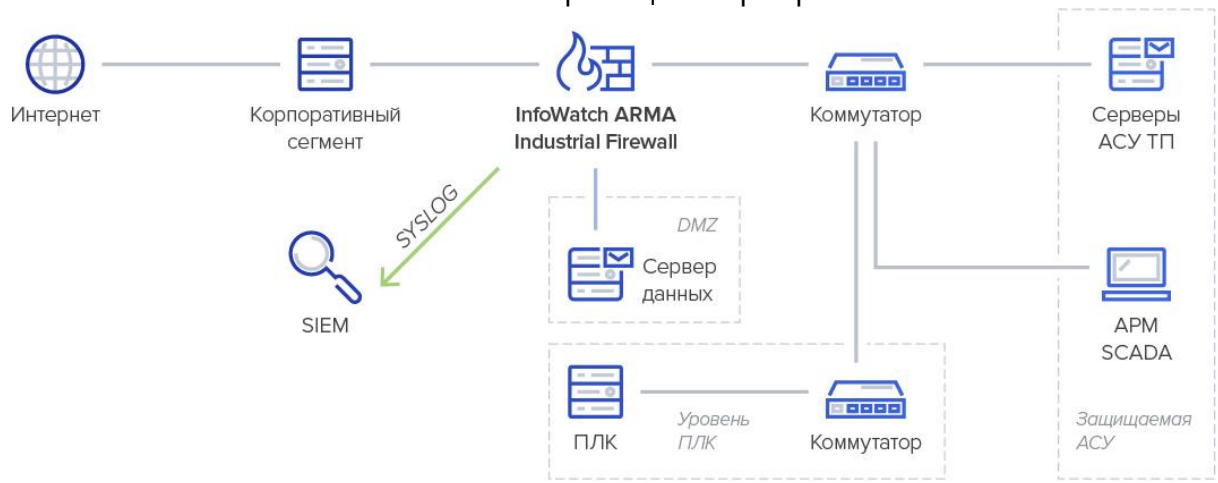

Рисунок 4 – Применение на границе с корпоративным сегментом

2.3.2 Связь с технической поддержкой

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

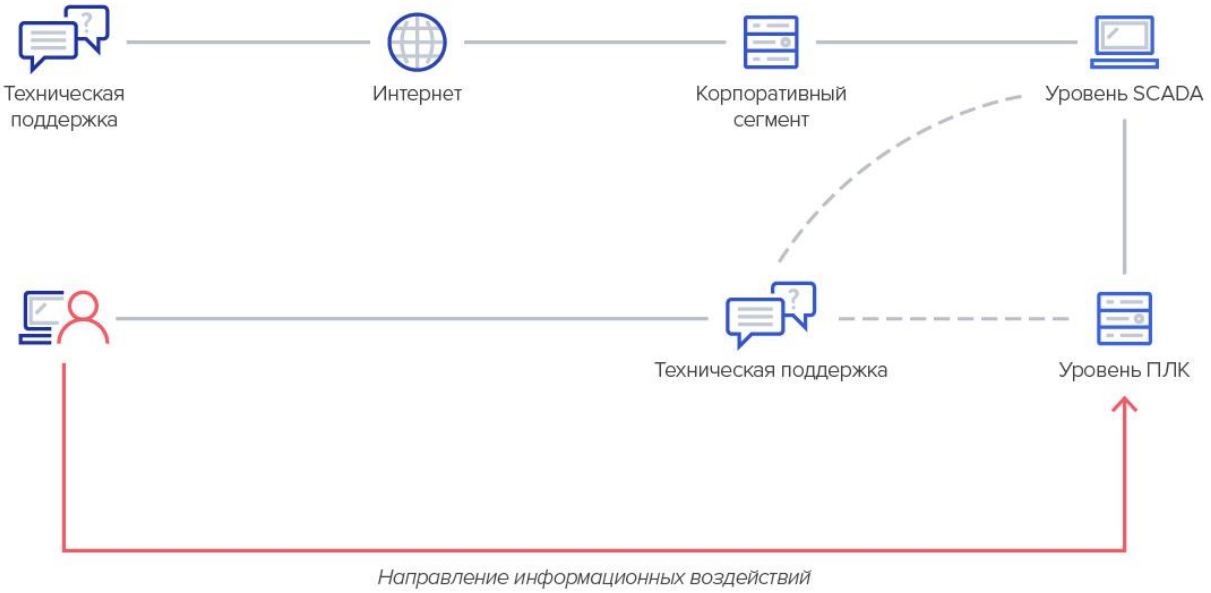

Рисунок 5 – Связь с технической поддержкой. Угрозы

На схеме, представленной на рисунке 6, показан вариант применения InfoWatch ARMA Industrial Firewall для обеспечения безопасной связи с технической поддержкой.

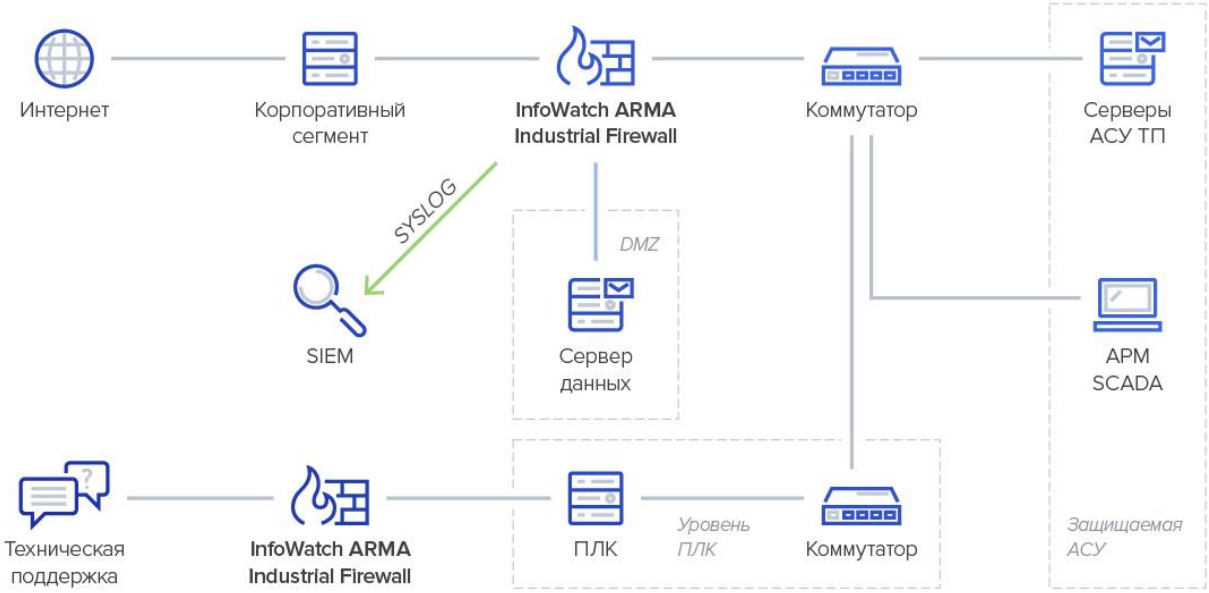

Рисунок 6 – Применение для обеспечения безопасной связи с технической поддержкой

2.3.3 Связь со смежными АСУ

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

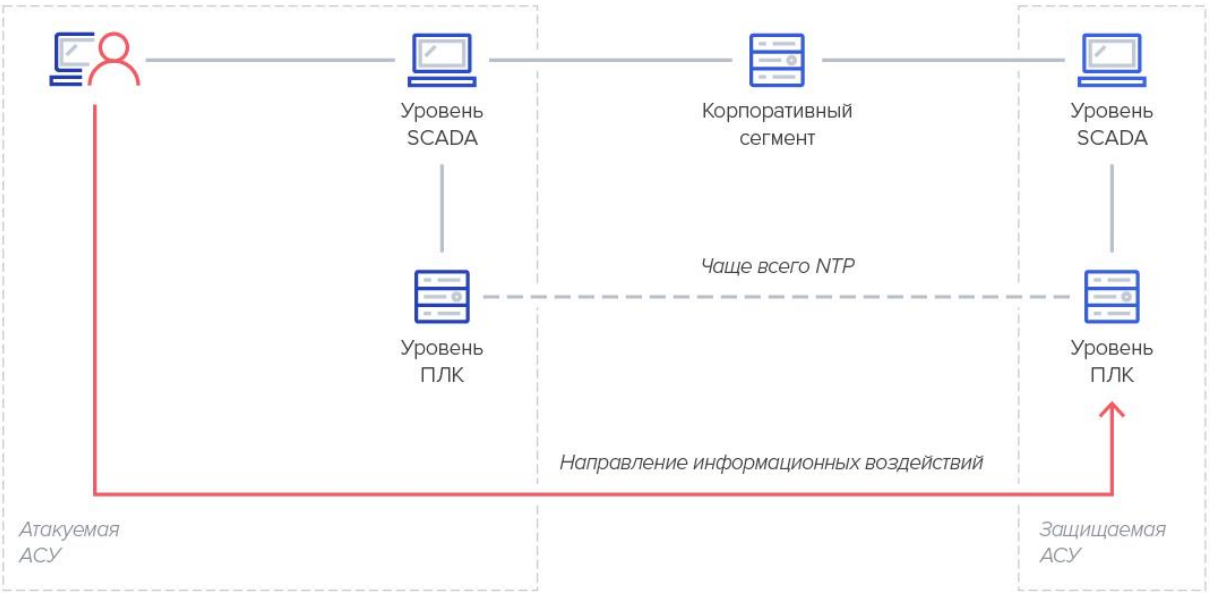

Рисунок 7 – Связь со смежными АСУ. Угрозы

На схеме, представленной на рисунке 8, показан вариант применения InfoWatch ARMA Industrial Firewall для обеспечения безопасной связи со смежными АСУ.

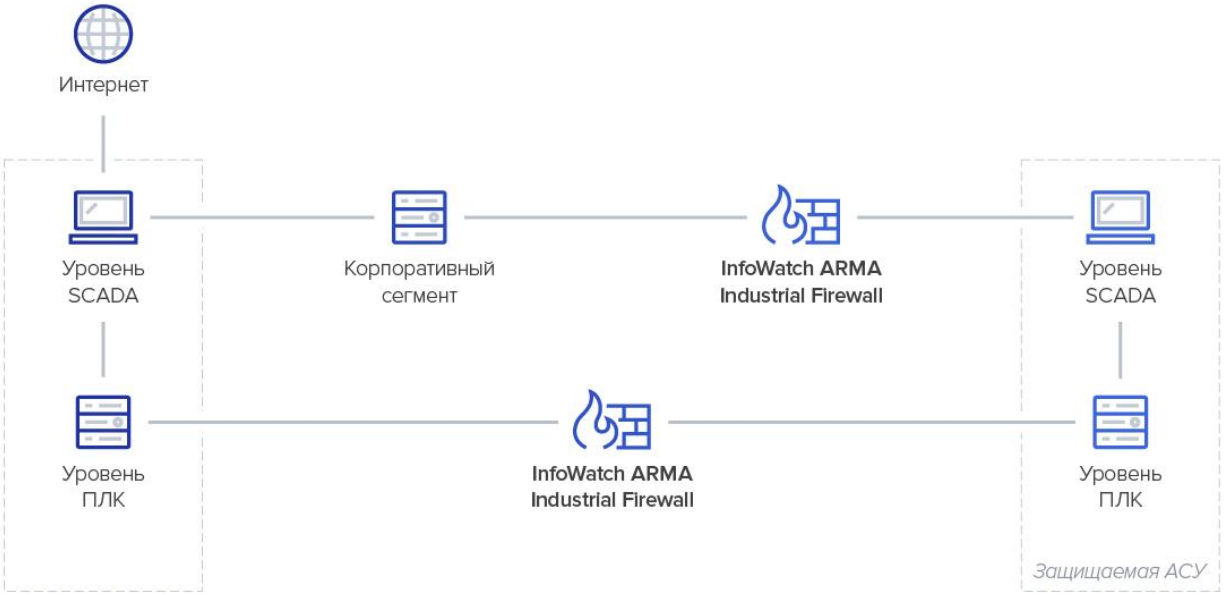

Рисунок 8 – Применение для обеспечения безопасной связи со смежными АСУ

2.3.4 Мониторинг внутри АСУ ТП

На схеме, представленной на рисунке 9, показан вариант применения InfoWatch ARMA Industrial Firewall для осуществления мониторинга внутри АСУ ТП.

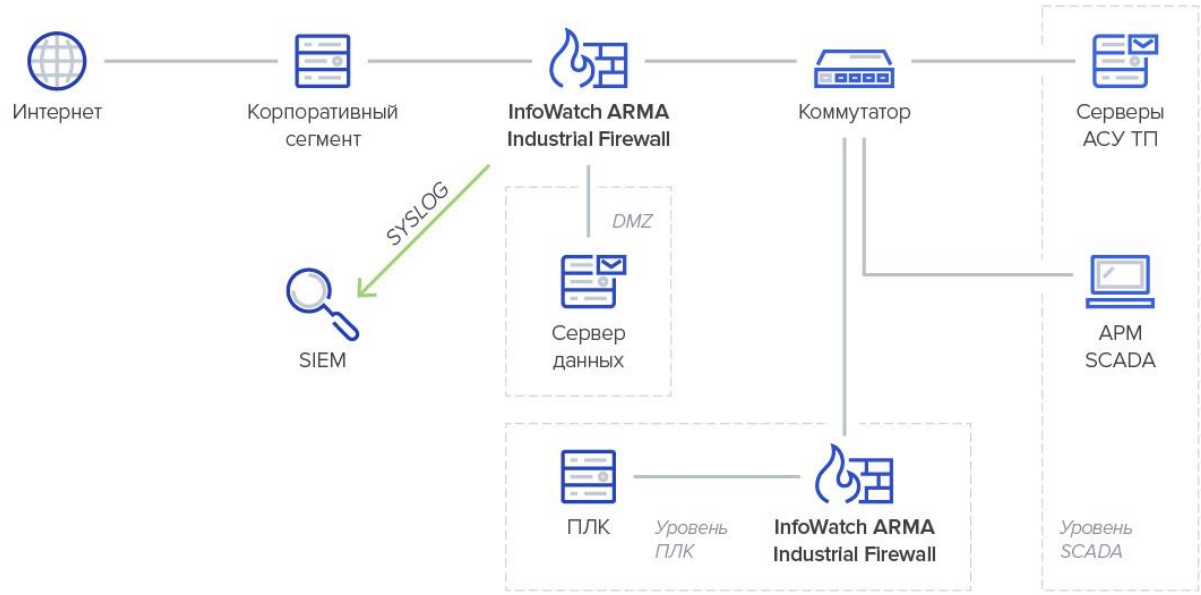

Рисунок 9 – Применение для мониторинга внутри АСУ ТП

2.4 Обнаруживаемые атаки

InfoWatch 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.

2.5 Описание аппаратных конфигураций

Возможны следующие варианты поставки InfoWatch ARMA Industrial Firewall:

1. Для поставки в стойку 19”:
   - в серверном исполнении;
   - в промышленном исполнении;
   - в серверном исполнении с bypass;
2. Для крепления на DIN рейку:
   - в промышленном исполнении.

В таблице 4 приведены основные технические характеристики различных аппаратных конфигураций InfoWatch ARMA Industrial Firewall.

Таблица 4 – Аппаратные конфигурации InfoWatch ARMA Industrial Firewall

Параметр	ARMAIF-19RACK	ARMAIF-BOX	ARMAIF-DIN	ARMAIF-RUGRACK
Изображение				
Исполнение	1 Unit исполнение для монтажа в стойку. Серверное исполнение	Промышленное исполнение, без движущихся частей	Промышленное исполнение, без движущихся частей	1 Unit исполнение для монтажа в стойку. Промышленное исполнение, без движущихся частей
Процессор	Intel Xeon E3-1220v6, 3 ГГц, 8 Мб кэш	Intel Core i5, пассивное охлаждение	Intel Celeron N3350, промышленный, пассивное охлаждение	Intel Core i7-7600U 2 x 2.8 GHz, 4MB cache
ОЗУ	16 Гб оперативной памяти	16 Гб оперативной памяти	8 Гб оперативной памяти	16 Гб оперативной памяти
Жесткий диск	240 Гб твердотельный накопитель	256 Гб твердотельный накопитель	256 Гб твердотельный накопитель	256 Гб твердотельный накопитель
Сетевые порты	Две конфигурации: 1. Ethernet - 4 порта 1 Гб/с (ARMAIF-19RACK-4E) 2. Ethernet - 8 портов 1 Гб/с (ARMAIF-19RACK-8E)	Ethernet - 6 портов 1 Гб/с	Ethernet - 4 порта 1 Гб/с	Ethernet - 4 порта 1 Гб/с
Пассивное охлаждение	Нет	Да	Да	Да
Питание	Питание - 2x450 Вт., с возможностью горячей замены	Питание - 2x24 В, встроенные блоки питания с резервированием (без возможности горячей замены)	Питание - 12...24 В, внешний блок питания	Питание - 2x450 Вт., с возможностью горячей замены

Параметр	ARMAIF-19RACK	ARMAIF-BOX	ARMAIF-DIN	ARMAIF-RUGRACK
Общая пропускная способность всего устройства с включенным модулем МЭ	6 Гб/с (оценка на основе характеристик оборудования)	2 Гб/с (оценка на основе характеристик оборудования)	1 Гб/с (оценка на основе характеристик оборудования)	4 Гб/с (оценка на основе характеристик оборудования)
Общая пропускная способность всего устройства с включенными модулями МЭ и СОВ и DPI	500 Мб/с	180 Мб/с	80 Мб/с	500 Мб/с
Межсетевой экран, пакетов/с (оценочное значение)	2 000 000	1 100 000	120 000	1 800 000
Межсетевой экран, количество одновременных соединений (сессий)	8 500 000	1 000 000	250 000	2 000 000
Габаритные размеры (ШхГхВ)	444x615x44 (1U)	192x230x127	155x110x79	1U
Вес	10.8 кг.	4.1 кг.	1.15 кг.	12 кг

Гарантия на оборудование – 1 год.

2.6 Лицензирование

В InfoWatch ARMA Industrial Firewall предусмотрены следующие виды лицензии:

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

В таблице 5 перечислены функции InfoWatch ARMA Industrial Firewall для каждого вида лицензии.

Таблица 5 – Функции InfoWatch ARMA Industrial Firewall 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.	Фильтрация сетевого трафика с учетом параметров пакета на сетевом и транспортном уровнях	-	+	+
3.	Точная идентификация, классификация и предотвращение проникновения вредоносного трафика, включая червей, вирусов, сетевых атак и т.п.	-	+	+
4.	Сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)	-	+	+
5.	Возможность задания расписания срабатывания правил	-	+	+
Система обнаружений вторжений				
6.	Обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровне	+	-	+
7.	Обновление базы решающих правил	+	-	+
8.	Возможность разработки пользовательских правил СОВ	+	-	+
Сетевые функции				
9.	Возможность работы в режиме прозрачного моста	+	+	+
10.	Поддержка статической маршрутизации	-	+	+
11.	Поддержка протоколов динамической маршрутизации	-	+	+
12.	Прокси сервер	-	+	+
13.	Поддержка VLAN IEEE 802.1q	-	+	+
14.	DHCP сервер	-	+	+
15.	Функции QoS (Traffic Shaping)	-	+	+
16.	Возможность зеркалирования сетевого трафика на отдельный порт	-	+	+
17.	Поддержка IPv6	+	+	+
18.	Поддержка объединения	+	+	+

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
	физических интерфейсов в логические			
19.	Просмотр таблицы активных соединений	-	+	+
Функции сбора и анализа событий				
20.	Выбор совокупности регистрируемых событий для анализа по различным критериям	+	+	+
21.	Мониторинг состояния по SNMP v.1, 2, 3	+	+	+
22.	Экспорт событий по протоколу SYSLOG (интеграция с SIEM-системами), SYSLOG в формате CEF	+	+	+
23.	Возможность сбора и экспорта дампов трафика	+	+	+
24.	Интеграция по ICAP с внешними системами	-	+	+
25.	Сбор и экспорт статистики NetFlow	+	+	+
26.	Мониторинг загрузки и состояния сетевых интерфейсов, CPU,памяти и программных модулей	+	+	+
Функции управления				
27.	Доступ к продукту и управление на ролевой основе, гибкая настройка прав доступа	+	+	+
28.	Возможность аутентификации пользователей через Active Directory	+	+	+
29.	Поддержка функций централизованного управления	+	+	+
30.	Задание и синхронизации времени по протоколу NTP	+	+	+
31.	Поддержка управления по SSH	+	+	+
32.	Возможность экспорта и импорта конфигурации	+	+	+
33.	Возможность экспорта и импорта баз решающих правил	+	-	+
34.	Планировщик задач	+	+	+
35.	Возможность отключения/включения неиспользуемых сервисов	+	+	+
36.	Журналы системных событий	+	+	+
37.	Возможность удаленного/локального обновления	+	+	+
Функции отказоустойчивости, повышения надежности, резервирования				
38.	Поддержка отказоустойчивой конфигурации active-passive	-	+	+

№ п/п	Функционал	СОВ	МЭ	МЭ + СОВ
39.	Loop Protection. Технологии STP, RSTP	-	+	+
40.	Сохранение резервных копий конфигурации на выделенный FTP-сервер	+	+	+
Защита доступа				
41.	Обеспечение защищенного канала администрирования системы за счет управления по протоколам HTTPS, SSH	+	+	+
42.	Конфигурация парольной политики	+	+	+
43.	Возможность аутентификации по различным базам: локальная база пользователей, каталог Active Directory (LDAP), RADIUS-сервер	+	+	+
44.	Контроль целостности программного обеспечения устройства защиты	+	+	+
VPN				
45.	Возможность построения криптографического тоннеля	-	+	+
46.	Site-to-site VPN	-	+	+

3 INFOWATCH ARMA MANAGEMENT CONSOLE

3.1 Функции

Все функции InfoWatch ARMA Management Console приведены в таблице 6.

Таблица 6 – Функции InfoWatch ARMA Management Console

№ п/п	Функционал	Комментарий
Централизованное управление системами защиты		
1.	Централизованное управление продуктами InfoWatch ARMA	По API (HTTPS)
2.	Доступ к веб-интерфейсу InfoWatch ARMA Industrial Firewall	
3.	Импорт/экспорт конфигурации InfoWatch ARMA Industrial Firewall	Экспорт конфигурации на одно/несколько устройств
4.	Импорт/экспорт баз решающих правил InfoWatch ARMA Industrial Firewall	Экспорт баз решающих правил на одно/несколько устройств
5.	Защищенное управление	
Сбор и анализ данных аудита		
6.	Централизованный сбор событий с подключенных InfoWatch ARMA Industrial Firewall	
7.	Централизованный сбор инцидентов с подключенных InfoWatch ARMA Industrial Firewall	
8.	Предоставление детального отчета по каждому инциденту	
9.	Управление инцидентами InfoWatch ARMA Industrial Firewall	
10.	Автоматическая группировка инцидентов InfoWatch ARMA Industrial Firewall	
Отображение устройств сети		
11.	Список устройств сети	
12.	Отображение карты сети	Отображение другим цветом устройств, которые имеют нерешенные инциденты; Отображение подробной информации об устройстве; Возможность задания связей между устройствами сети; Возможность перетаскивания устройств по карте сети.
13.	Возможность группировки	

№ п/п	Функционал	Комментарий
	устройств сети на карте сети	

3.2 Варианты применения

На схеме (Рисунок 10) показан вариант применения InfoWatch ARMA Management Console с другими продуктами InfoWatch ARMA.

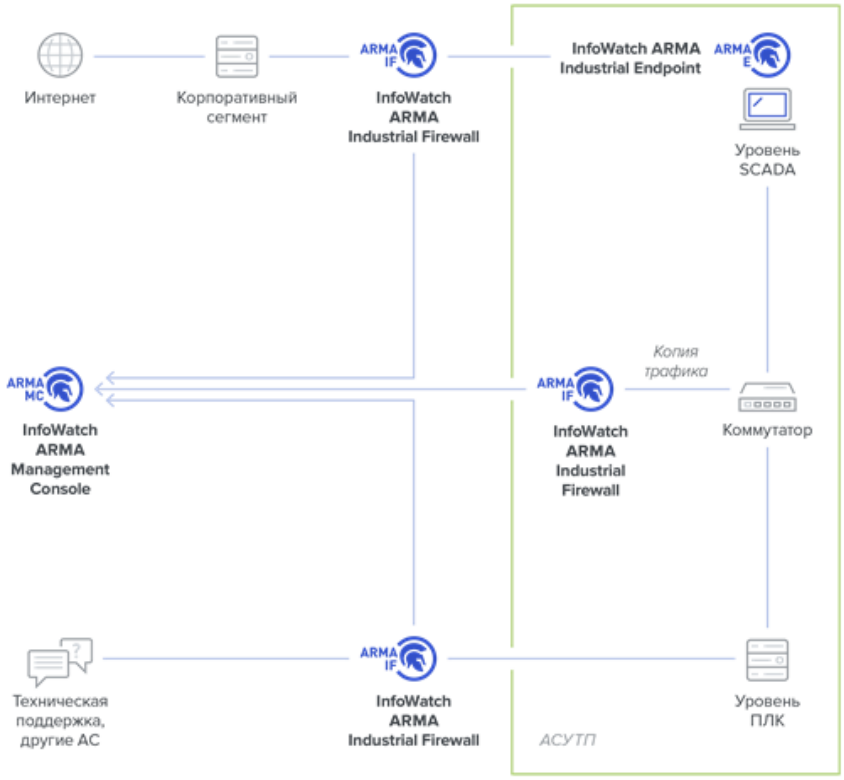

Рисунок 10 – Применение InfoWatch ARMA Management Console

На схеме (Рисунок 11) показан сбор событий с InfoWatch ARMA Industrial Firewall.

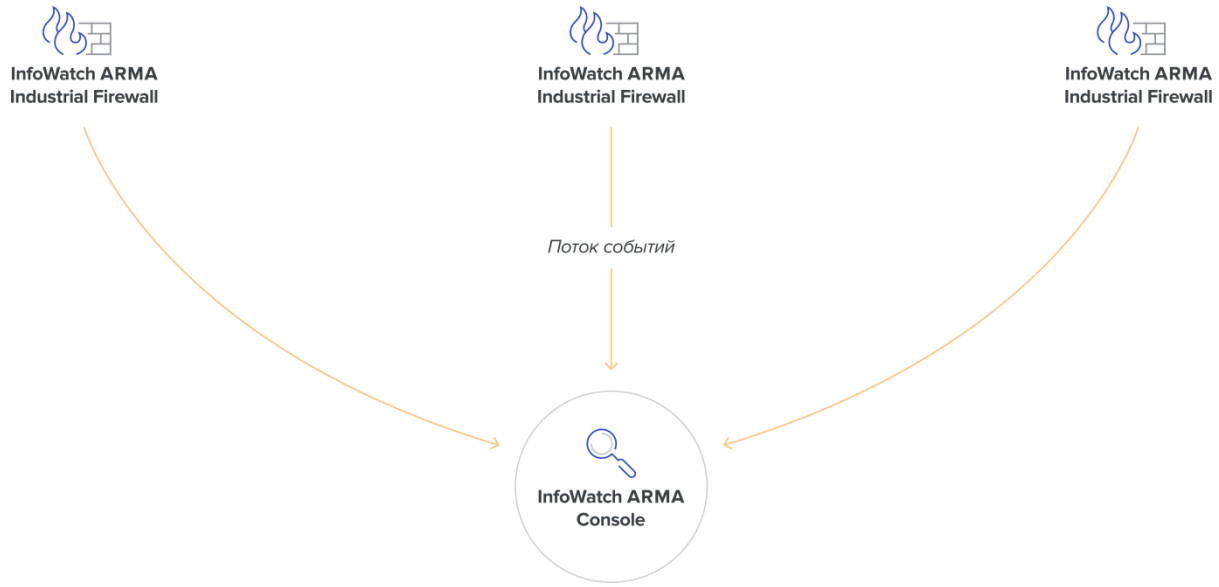

Рисунок 11 – Сбор событий с InfoWatch ARMA Industrial Firewall

4 INFOWATCH ARMA INDUSTRIAL ENDPOINT

4.1 Функции

InfoWatch ARMA Industrial Endpoint выполняет следующие функции:

- контроль использования съемных носителей информации;
- ограничение программной среды (whitelisting), управление запуском ПО;
- контроль целостности файлов и ПО рабочих станций и серверов АСУ ТП.

4.2 Варианты применения

На схеме (Рисунок 12) показан вариант применения InfoWatch ARMA Industrial Endpoint с другими продуктами InfoWatch ARMA.

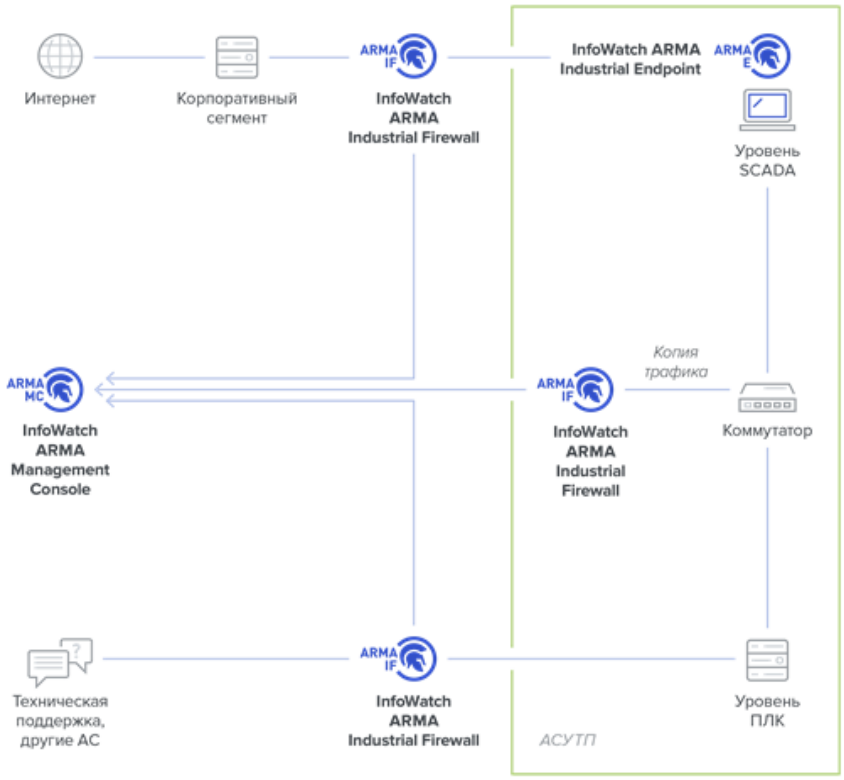

Рисунок 12 – Применение InfoWatch ARMA Industrial Endpoint