INFOWATCH®

ЗАЩИТА АСУ ТП ОТ КИБЕРАТАК

ARMA

INFOWATCH ARMA

arma.infowatch.ru

InfoWatch ARMA

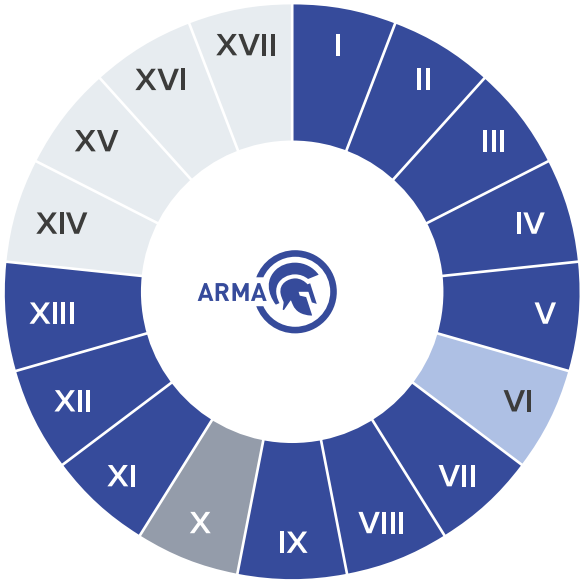
Отечественная система защиты информации в АСУ ТП на промышленных предприятиях

Развитие Индустрии 4.0 привело к слиянию двух «миров» — АСУ ТП и классического IT, ранее существовавших изолированно друг от друга. Традиционная модель угроз OT-сетей начала обрастать уязвимостями информационных систем со стороны IT. Этот процесс идёт в условиях, когда на предприятиях средства защиты устанавливаются точечно, слабо интегрированы между собой и не имеют единого центра управления. Результат — отсутствие у департаментов ИБ АСУ ТП возможностей оперативно реагировать на вторжения и кибератаки.

InfoWatch ARMA — отечественная система защиты информации в АСУ ТП на промышленных предприятиях

Позволяет построить эшелонированную защиту информации от современных киберугроз, исходящих как от внутренних, так и от внешних нарушителей.

Позволяет выполнить до 90% технических мер Приказа №239 ФСТЭК России от 25 декабря 2017



Римскими цифрами на диаграмме указаны группы мер Приказа №239 ФСТЭК России.

- Позволяет выполнить меры из группы
- Ожидается в Q2, 2022
- Выполняется мерами физической безопасности
- Выполняется организационными мерами

Состав системы защиты InfoWatch ARMA

Средство защиты рабочих станций и серверов АСУ ТП

InfoWatch ARMA Industrial Endpoint

Сертифицированный промышленный межсетевой экран нового поколения (NGFW)

InfoWatch ARMA Industrial Firewall

Все продукты интегрированы между собой

Единый центр управления системой защиты InfoWatch ARMA

InfoWatch ARMA Management Console

InfoWatch ARMA Industrial Firewall

Сертифицированный промышленный межсетевой экран нового поколения (NGFW)

InfoWatch ARMA Industrial Firewall позволяет своевременно обнаруживать и блокировать атаки на АСУ ТП, попытки эксплуатации уязвимостей, а также защищать от несанкционированных действий в промышленной сети.

Какие задачи решает

Защита информации в АСУ ТП от кибератак и несанкционированного доступа

Имеет возможность фильтрации сетевого трафика на прикладном уровне благодаря технологии глубокой инспекции промышленных протоколов (DPI). Содержит встроенную систему обнаружения и предотвращения вторжений, а также возможность организации безопасного удалённого подключения через VPN.

Соответствие требованиям регулятора

Позволяет реализовать меры защиты значимых объектов КИИ, согласно требованиям Приказа №239 ФСТЭК России. Имеет сертификат ФСТЭК России (№4429 со сроком действия до 27 июля 2026) по 4 уровню доверия. Является межсетевым экраном типа «Д» четвёртого класса защиты (ИТ.МЭ.Д4.ПЗ) и системой обнаружения вторжений уровня сети четвёртого класса защиты (ИТ.СОВ.С4.ПЗ). Включён в единый реестр российского ПО Минкомсвязи РФ.

Обеспечение непрерывной работы АСУ ТП в условиях совмещения IT и OT

Остановка работы средств защиты может привести к проникновению злоумышленников в промышленную сеть и, как следствие, — к нарушению технологического процесса. **InfoWatch ARMA Industrial Firewall** поддерживает режим отказоустойчивого кластера, благодаря которому повышает надёжность работы системы защиты информации в АСУ ТП.

Почему профессионалы доверяют защиту АСУ ТП InfoWatch ARMA Industrial Firewall?

Своевременное обнаружение и предотвращение вторжений в АСУ ТП зависит от способности средства защиты информации анализировать содержание пакетов промышленного трафика. **InfoWatch ARMA Industrial Firewall** глубоко инспектирует пакеты промышленных протоколов. Предоставляет полную информацию о событиях безопасности в промышленной сети и позволяет защищать АСУ ТП от кибератак.

Глубокая инспекция пакетов промышленного трафика

- **Высокая видимость промышленной сети**

  Определяет протоколы на основе содержания пакетов промышленного трафика. Разбор событий безопасности по промышленным протоколам позволяет детально зафиксировать действия пользователей и работу систем и своевременно отреагировать на киберугрозы.

- **Ограничение промышленного трафика на уровне отдельных промышленных протоколов**

  Позволяет задать правила взаимодействия в сети на уровне промышленных протоколов и отдельных команд. Это даёт возможность сократить информационные потоки только до регламентированных и уменьшить количество ложных срабатываний.

Позволяет работать с трафиком на уровне команд протоколов и настроить защиту под свои задачи. Вот некоторые сценарии, которые используют наши клиенты:

- **Контроль действий пользователей**

  Назначайте пользователям права, чтобы контролировать легитимность действий в сети. Например, ограничьте права оператора до функции чтения информации.

- **Контроль недопустимых операций с ПЛК**

  Установите запрет на изменения в системе, в частности, блокировку или оповещение при попытке загрузки программы управления или обновления операционной системы ПЛК.

Какие протоколы инспектирует InfoWatch ARMA Industrial Firewall

Глубина проработки и объём поддерживаемых функций и параметров приведён в техническом описании **InfoWatch ARMA Industrial Firewall.**

Позволяет фильтровать по полям до уровня команд и их значений	Обнаруживает вторжения и осуществляет мониторинг
S7 Communication	S7 Communication
	S7 Communication plus
Modbus TCP	Modbus TCP
Modbus TCP x90 func. code (UMAS)	Modbus TCP x90 func. code (UMAS)
OPC DA	OPC DA
OPC UA	OPC UA
IEC 61850-8-1 MMS	IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE	IEC 61850-8-1 GOOSE
IEC 60870-5-104	IEC 60870-5-104
	ENIP / CIP
	Profinet
	DNP3

Промышленная система обнаружения и предотвращения вторжений

Обнаруживает и блокирует компьютерные атаки на АСУ ТП и попытки эксплуатации уязвимостей ПЛК.

Почему наша система обнаружения и предотвращения вторжений эффективнее классических СОВ?

- **Содержит базу решающих правил обнаружения и предотвращения вторжений для АСУ ТП**

  Обнаруживает попытки эксплуатации как классических уязвимостей (операционных систем, баз данных, сканирования сети и др.), так и специфических уязвимостей АСУ ТП. Позволяет самостоятельно дополнять предустановленную базу СОВ собственными пользовательскими правилами для максимальной защиты конкретных АСУ ТП.

- **Использует глубокую инспекцию протоколов (DPI) для блокировки кибератак на АСУ ТП**

  Благодаря детальному разбору трафика до уровня команд и их значений можно настроить автоматическую блокировку вредоносных пакетов в трафике от источника угрозы.

Межсетевое экранирование для промышленных объектов

Контролирует доступ к сетевым ресурсам, защищает от несанкционированного действия в промышленной сети и регистрирует все информационные потоки.

Почему наш межсетевой экран повышает эффективность защиты АСУ ТП?

- **Предотвращает самые распространённые атаки на сервисные функции промышленного оборудования**

  Позволяет ограничить использование сервисных функций промышленного трафика: запретить несанкционированные действия с ПЛК: перепрошивку, изменение ПО, запись информации в ПЛК и др.

- **Использует глубокую инспекцию протоколов (DPI) для микросегментации сети АСУ ТП**

  Позволяет контролировать информационные потоки как между IT- и OT-сетями, так и между сегментами, например, внутри OT-сетей, а также гибко разграничивать права пользователей внутри OT-сегмента. Микросегментация позволяет предотвратить потенциальную атаку даже в случае появления недоверенных систем внутри АСУ ТП.

Безопасное удалённое подключение через VPN

Обеспечивает защиту информации при объединении в единую сеть филиалов предприятия, удалённом подключении к производственной площадке или при работе технической поддержки.

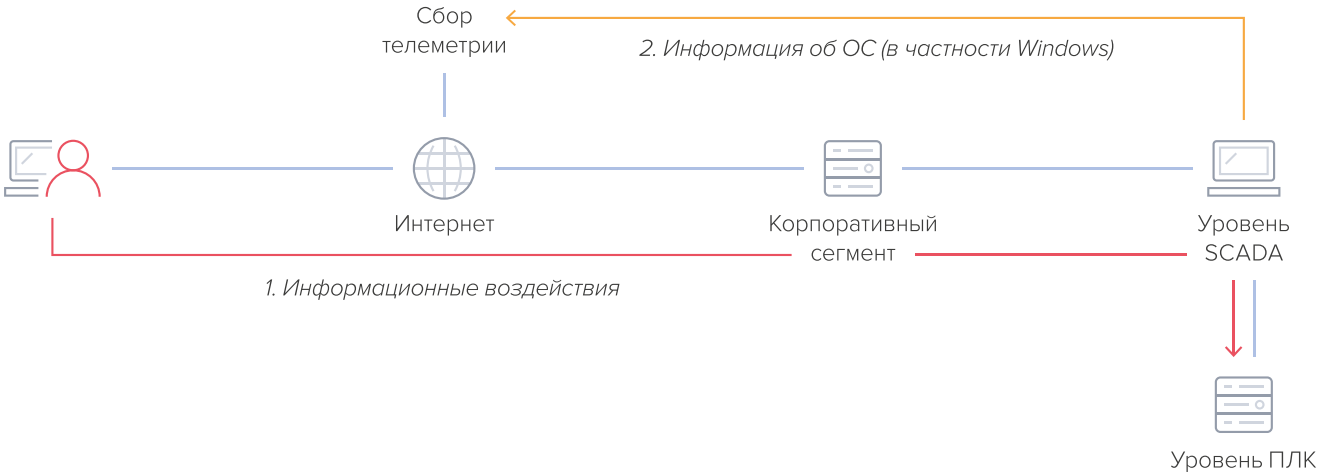
Примеры установки InfoWatch ARMA Industrial Firewall

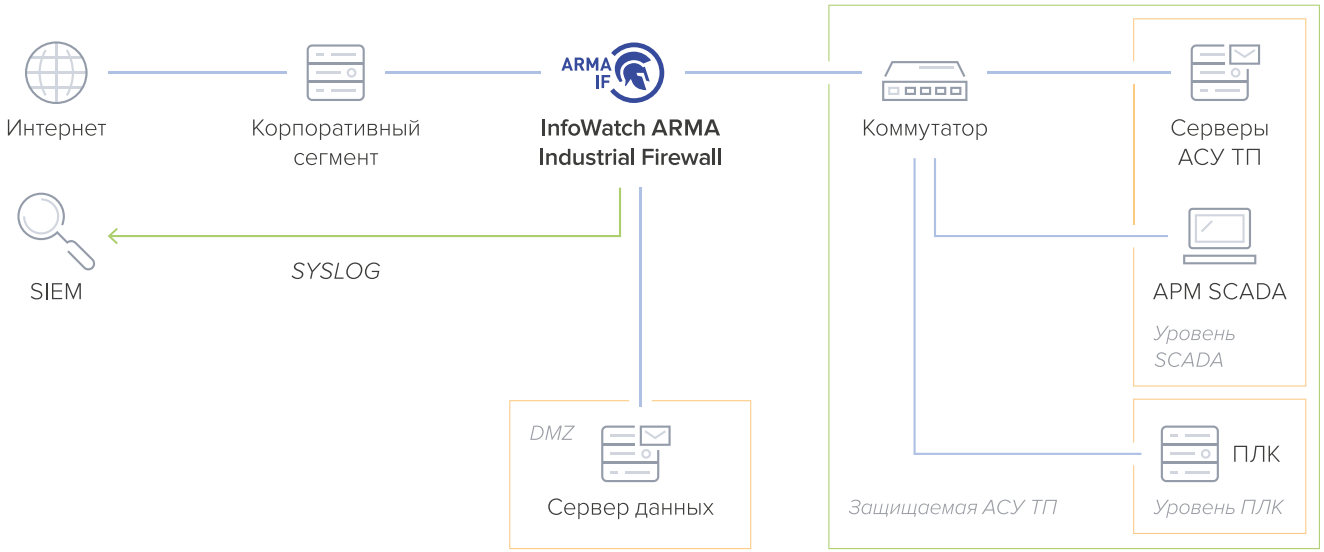
Шесть способов защиты от распространённых типов киберугроз.

Защищайте АСУ ТП на границе с корпоративным сегментом

- **Киберугрозы**

Рассмотрим пример: АСУ ТП не изолирована от корпоративной сети. Вторжение в промышленную сеть возможно через фишинг, заражённое ПО или в результате перехода на заражённый веб-сайт и далее в промышленную сеть.





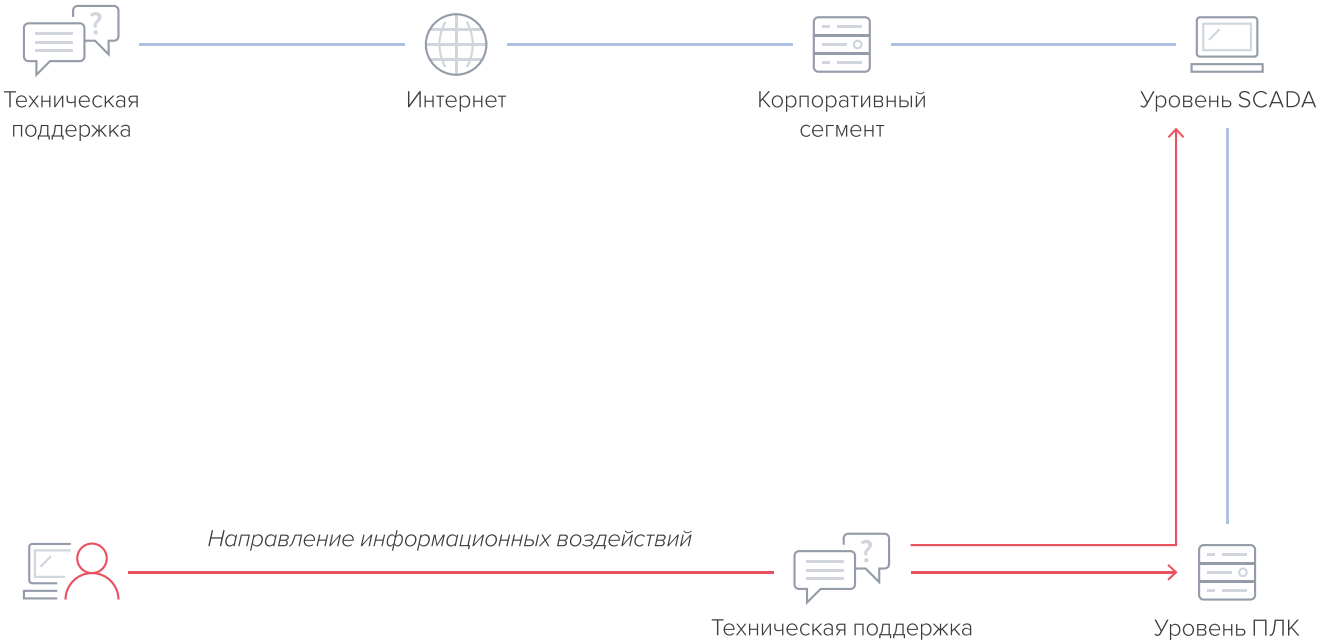
- **Сегментируйте сеть между корпоративным сегментом и АСУ ТП**

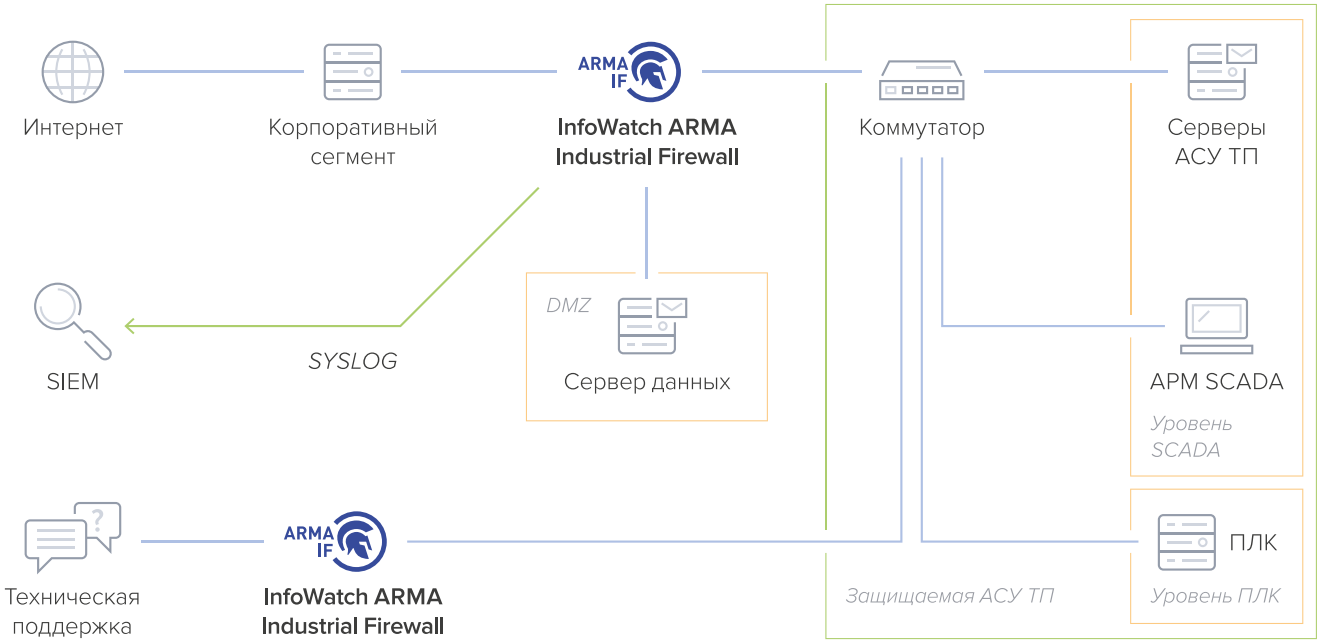
Аутентифицируйте пользователей, блокируйте атаки с помощью IPS, ограничивайте информационные потоки из корпоративной сети на уровень АСУ ТП.

Защищайте АСУ ТП на границе с каналом технической поддержки

Киберугрозы

Незащищённый канал технической поддержки может способствовать проникновению вредоносного ПО или предоставить киберпреступникам удалённый доступ к промышленной сети.





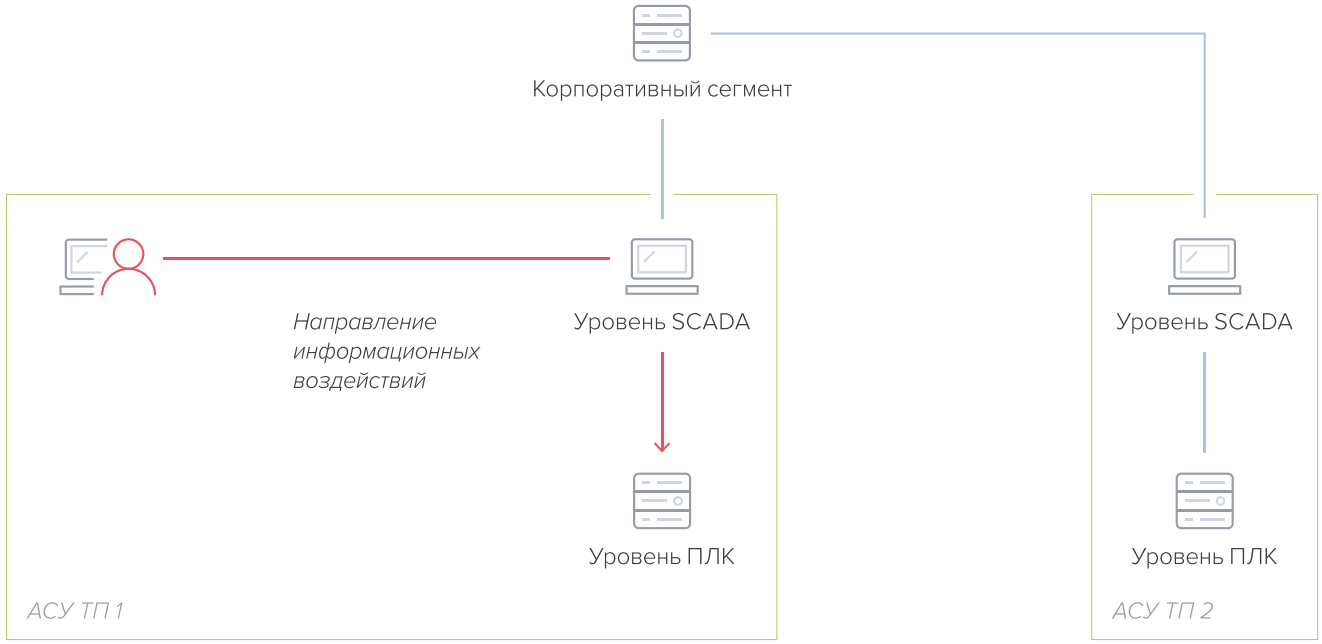
Сегментируйте сеть между технической поддержкой и АСУ ТП

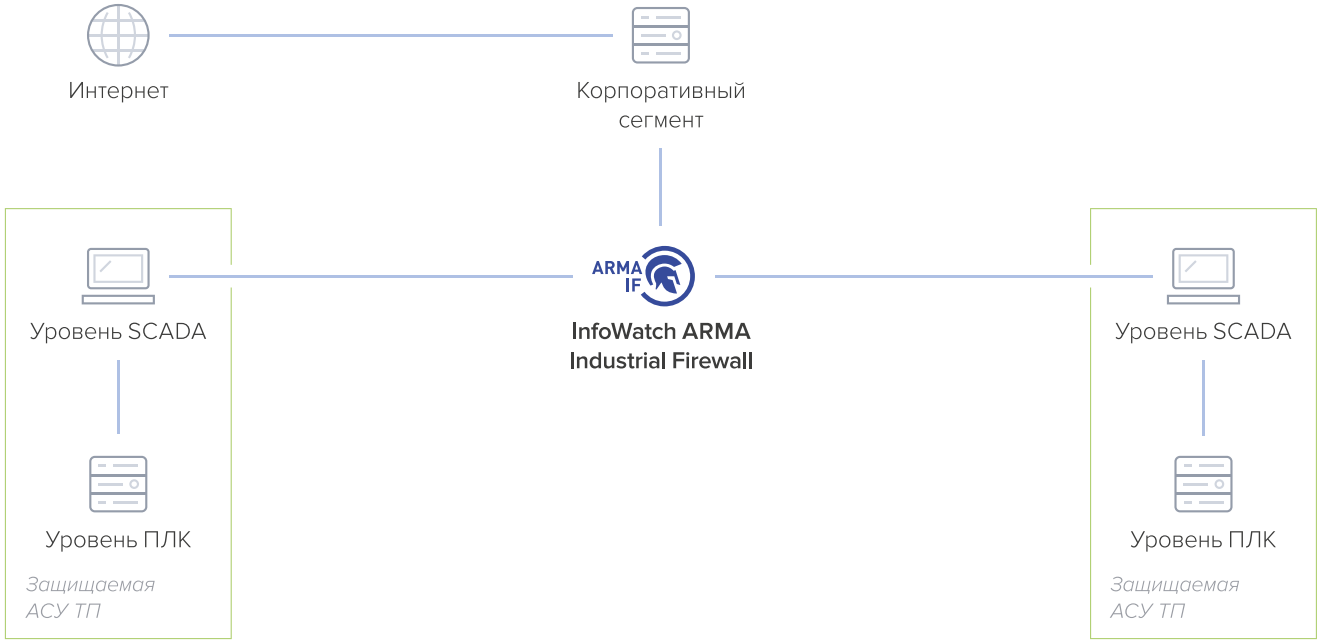
Блокируйте неразрешённые действия технической поддержки по установленным заранее правилам и правам для пользователей, журналируйте все происходящие действия, выявляйте атаки и распространение вредоносного ПО.

Защищайте взаимосвязанные АСУ ТП

Киберугрозы

Если киберпреступник атаковал одну АСУ через уязвимости ПЛК её уровня, он может получить доступ к смежной АСУ через корпоративный сегмент или смежный уровень ПЛК.





Сегментируйте сеть между смежными АСУ ТП

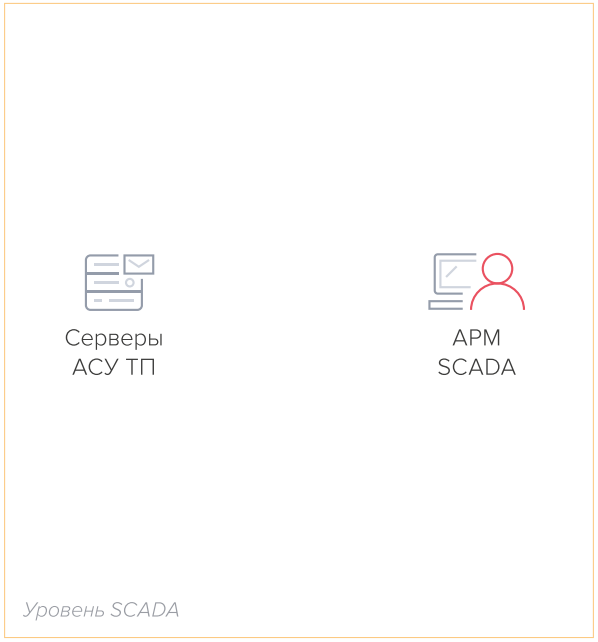
Установите правила и политики взаимодействия АСУ ТП, разного уровня защищённости, а также ограничьте трафик сети внутри обособленных или смежных АСУ ТП.

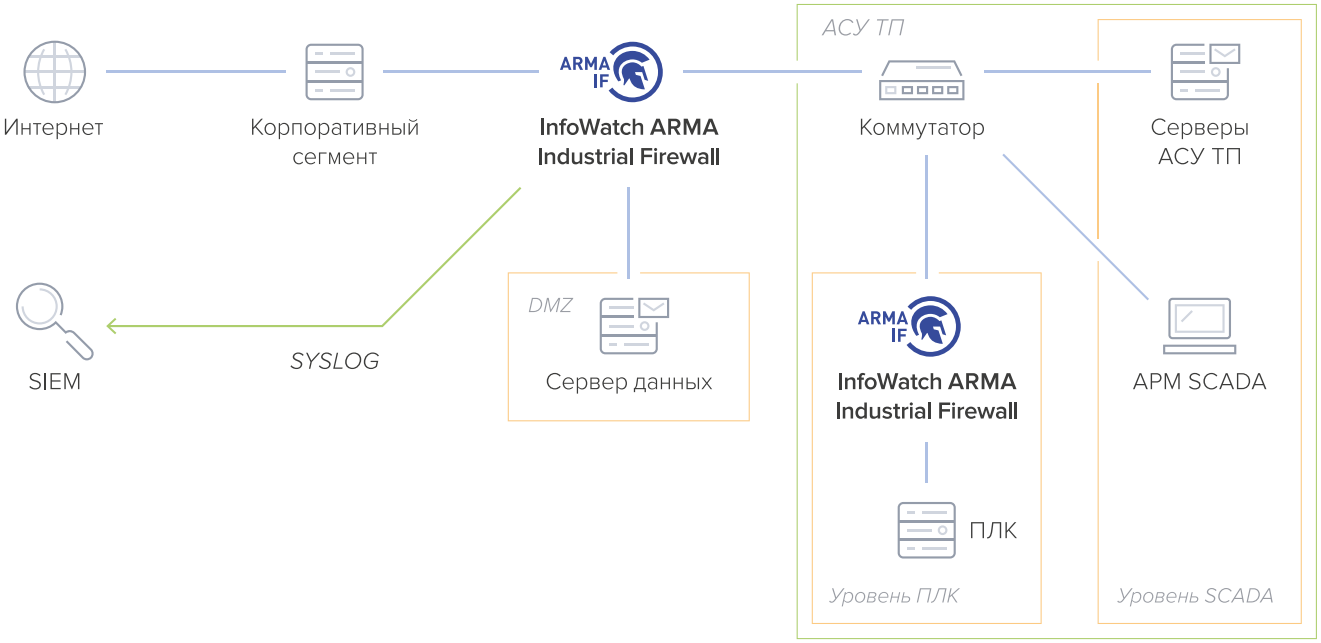
Это может быть особенно актуально, если одна из АСУ ТП подключена к внешней системе передачи данных.

Защищайте сеть между SCADA и ПЛК

Киберугрозы

Проникновение вредоносного ПО, несанкционированное подключение устройств и даже действия операторов могут нанести ущерб АСУ ТП внутри периметра.





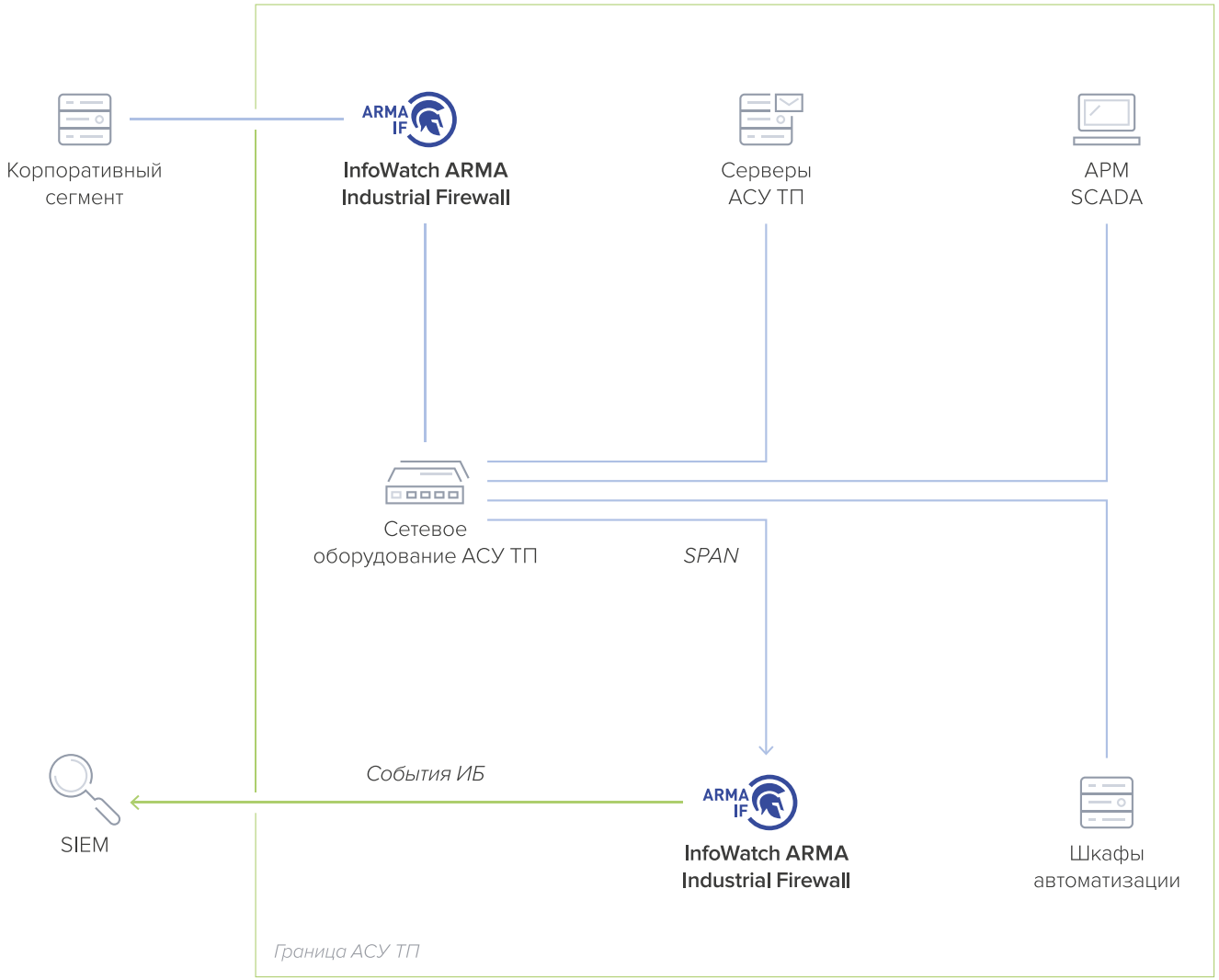
Сегментируйте сеть между SCADA и ПЛК

В АСУ ТП, где нет критически опасных процессов, например, на электросетях, установка межсетевого экрана между SCADA и ПЛК позволит построить дополнительный эшелон защиты, разделить права пользователей.

Дополнительные сценарии защиты

Получайте данные о всех событиях информационной безопасности внутри АСУ ТП

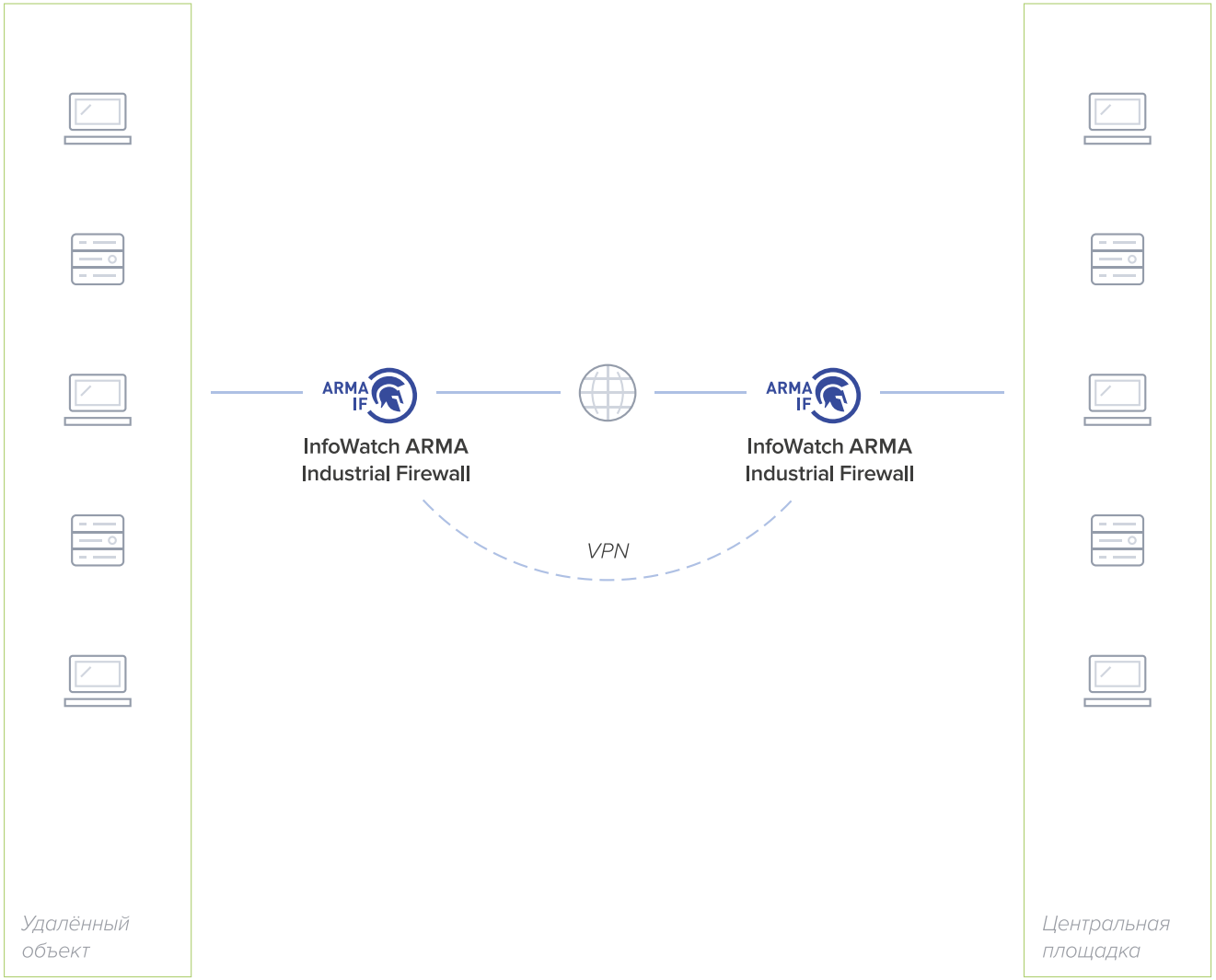
Если не требуется блокировать атаки, установите **InfoWatch ARMA Industrial Firewall** в режиме мониторинга сети и получайте информацию об аномалиях и событиях безопасности.



Дополнительные сценарии защиты

Защищайте удалённое подключение

InfoWatch ARMA Industrial Firewall обеспечивает безопасное удалённое подключение благодаря защите каналов администрирования и созданию паролей разного уровня сложностей, а также защищает периметр сети при объединении объектов в единую сеть (VPN).



Варианты установки и режимов работы

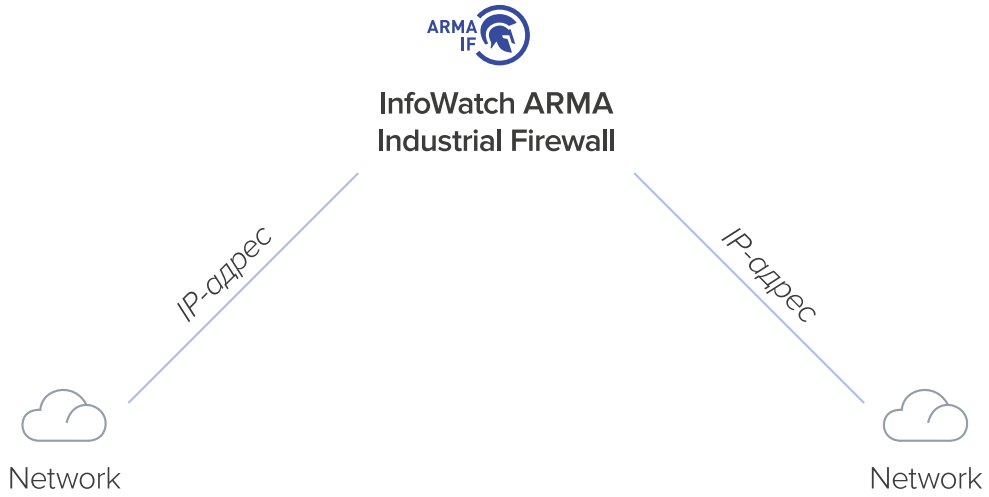
InfoWatch ARMA Industrial Firewall может устанавливаться в сеть в одном из двух типов режимов работы. Первый — в режиме маршрутизации, прозрачного моста, отказоустойчивого кластера или мониторинга. Второй — комбинированным способом.

Режим маршрутизации

Обнаружьте вторжения и заблокируйте атаки в сетях с разными адресами

В режиме маршрутизации **InfoWatch ARMA Industrial Firewall** функционирует как межсетевой экран с функциями обнаружения и предотвращения вторжений, обеспечивая защиту передачи информации на уровне L3.

Может использоваться при объединении подсетей, имеющих разное адресное пространство.



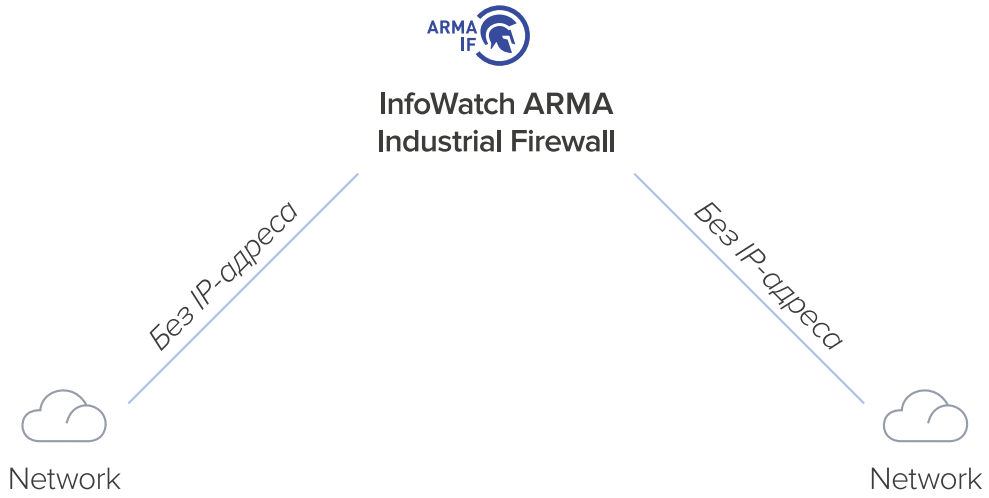
Режим прозрачного моста

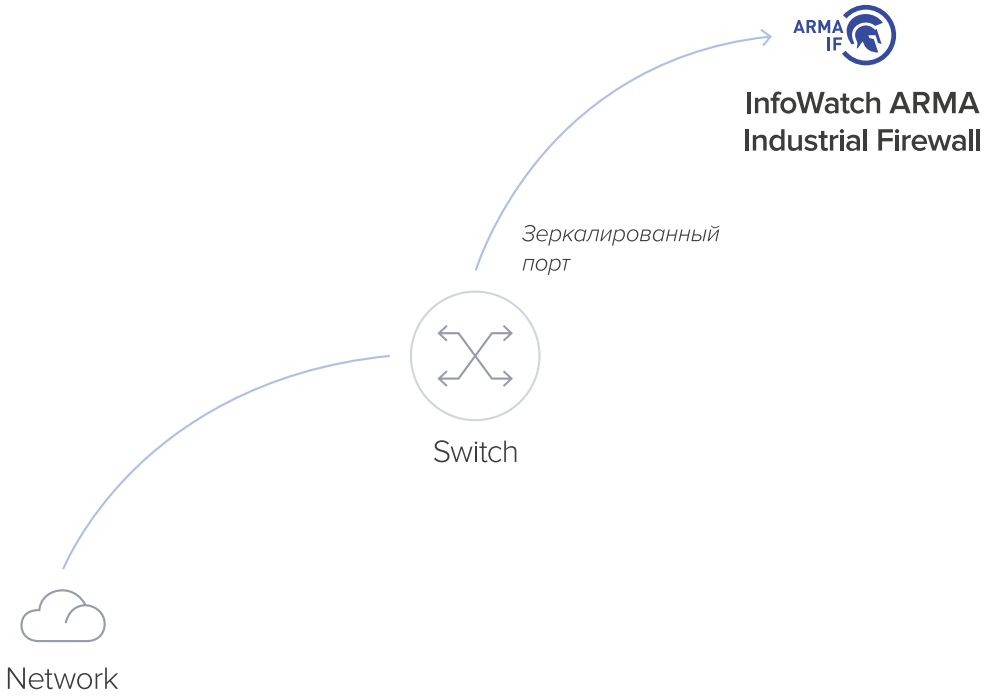
Обнаружьте вторжения и заблокируйте атаки в сетях с общим адресом

InfoWatch ARMA Industrial Firewall работает как система обнаружения и предотвращения вторжений в прозрачном режиме с возможностью блокировки вредоносных пакетов между сетями одного адресного пространства.

Интерфейсы при этом соединены в сетевой мост.

При обнаружении подозрительного либо вредоносного трафика информация о нём отправляется на веб-интерфейс для информирования пользователей, а при необходимости — блокируется.





Режим мониторинга с глубоким анализом пакетов трафика (DPI)

Обнаружьте вторжения в копии сетевого трафика с зеркалированного порта

В режиме sniffing mode (мониторинга) **InfoWatch ARMA Industrial Firewall** работает в качестве системы обнаружения вторжений, которая анализирует копии сетевого трафика, снятого с зеркалированного порта.

Проводит глубокий анализ пакетов (DPI) и, в случае необходимости, уведомляет специалиста ИБ АСУ ТП о событиях информационной безопасности.

Режим отказоустойчивого кластера в конфигурации active-passive

Обеспечьте непрерывность и надёжность работы АСУ ТП

В режиме отказоустойчивого кластера два **InfoWatch ARMA Industrial Firewall** объединяются в единый кластер в режиме active-passive.

Весь трафик в кластере обрабатывает ведущее устройство, а резервное — непрерывно синхронизирует с ним свою конфигурацию и берёт на себя функцию обработки трафика, в случае, если ведущее устройство выйдет из строя.

Варианты поставок и аппаратные конфигурации

Варианты поставок

InfoWatch ARMA Industrial Firewall поставляется в виде образа виртуальной машины или как программно-аппаратный комплекс.

Виртуальные машины

InfoWatch ARMA Industrial Firewall может работать со всеми популярными системами виртуализации:

- VMware
- ORACLE VirtualBox
- Microsoft Hyper-V

Программно-аппаратный комплекс

Серверное и промышленное исполнения предусмотрены без движущих частей:

- Серверы Intel x86 / x64
- Промышленные компьютеры

Аппаратные конфигурации

ПАК InfoWatch ARMA представлен как в серверном, так и в промышленном исполнениях без движущих частей для монтажа в стойку или на DIN-рейку.

Монтаж в 19-дюймовую стойку

ARMAIF-RUGRACK

ARMAIF-19RACK

Монтаж на DIN-рейку или в 19-дюймовую стойку

ARMAIF-DIN

ARMAIF-BOX

Лицензии и опции масштабирования

Приобретайте лицензию в зависимости от тех функций, которые нужны именно сейчас и не переплачивайте за то, чем не собираетесь пользоваться. Лицензию можно расширить в любой момент при необходимости.

Виды лицензий на ПО

1. Промышленный межсетевой экран нового поколения с VPN
2. Промышленная система обнаружения и предотвращения вторжений (IPS, IDS)
3. Промышленный межсетевой экран нового поколения с VPN
   - Глубокая инспекция промышленных протоколов (DPI)
4. Промышленный межсетевой экран нового поколения с VPN
   - Глубокая инспекция промышленных протоколов (DPI)
   - Промышленная система обнаружения и предотвращения вторжений (IPS, IDS)

С полной лицензией вы значительно расширите видимость промышленной сети, сможете работать с промышленными протоколами, пользоваться базой промышленных сигнатур и тонко настраивать политики безопасности.

Технические характеристики

Всё оборудование представлено в базовой комплектации

ARMAIF-RUGRACK

Преимущества

- Работает при температурах от −10 до +55°C
- Степень защиты корпуса — IP 20
- Монтаж в 19-дюймовую стойку

Исполнение	Промышленное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	До 6
Пассивное охлаждение	Да
Питание	24 В, 120 Вт, DC / DC, резервирование с поддержкой горячей замены
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 4
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 500
Межсетевой экран, пакетов / сек	До 1 800 000
Межсетевой экран, количество одновременных соединений (сессий)	До 2 000 000
Габаритные размеры (Ш × Г × В), мм	1U
Вес, кг	5

ARMAIF-19RACK

Преимущества

- При необходимости комплектуется платой bypass
- Монтаж в 19-дюймовую стойку

Исполнение	Серверное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	4 в конфигурации ARMAIF-19RACK-4E, 8 в конфигурации ARMAIF-19RACK-8E
Пассивное охлаждение	Нет
Питание	2 × 450 Вт, с возможностью горячей замены
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 6
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 500
Межсетевой экран, пакетов / сек	До 2 000 000
Межсетевой экран, количество одновременных соединений (сессий)	До 8 500 000
Работает при температурах	От 0 до +40°C
Работает при влажности	От 10 до 95% (без конденсата)
Габаритные размеры (Ш × Г × В), мм	444 × 615 × 44
Вес, кг	10,8

ARMAIF-DIN

Преимущества

- Степень защиты корпуса — IP 30
- Монтаж на DIN-рейку или настольное исполнение

Исполнение	Промышленное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	До 4
Пассивное охлаждение	Да
Питание	От 12 до 24 В, внешний блок питания
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 1
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 80
Межсетевой экран, пакетов / сек	До 120 000
Межсетевой экран, количество одновременных соединений (сессий)	До 250 000
Работает при температурах	От −20 до +70°C
Работает при влажности	От 5 до 95%
Работает при вибрации	2G, от 10 до 150 Гц, амплитуда — 0,35 мм
Работает при ударе	25G, полусинусоида, продолжительность — 11 мс
Габаритные размеры (Ш × Г × В), мм	155 × 110 × 79
Вес, кг	1,15

ARMAIF-BOX

Преимущества

- При возможности может комплектоваться платой bypass
- Монтаж на DIN-рейку или настольное исполнение

Исполнение	Промышленное, без движущихся частей
Сетевые порты Ethernet 1 Гб / сек, шт	До 6
Пассивное охлаждение	Да
Питание	2 × 24 В, встроенные блоки питания с резервированием (без возможности горячей замены)
Общая пропускная способность всего устройства с включённым модулем межсетевого экранирования, Гб / сек	До 2
Общая пропускная способность всего устройства с включёнными модулями межсетевого экранирования, системы обнаружения вторжений и глубокой инспекцией промышленных протоколов, Мб / сек	До 180
Межсетевой экран, пакетов / сек	До 1 100 000
Межсетевой экран, количество одновременных соединений (сессий)	До 1 000 000
Работает при температурах	От –10 до +40°C
Работает при влажности	От 5 до 95% (без конденсата)
Работает при вибрации	3G, от 5 до 500 Гц
Работает при ударе	20G, IEC-68-2-27, полусинусоида, продолжительность — 11 мс
Габаритные размеры (Ш × Г × В), мм	192 × 230 × 127
Вес, кг	4,1

InfoWatch ARMA Industrial Endpoint

Средство защиты информации рабочих станций и серверов АСУ ТП

InfoWatch ARMA Industrial Endpoint — программное обеспечение, которое защищает рабочие станции и серверы от киберугроз на уровне диспетчерского управления, позволяя запускать только разрешённые программы. Блокирует запуск недоверенных программ и контролирует целостность файлов рабочих станций и серверов АСУ ТП.

Какие задачи решает

Позволяет создать замкнутую программную среду

- **Контролирует целостность файлов**

  Непрерывно следит за неизменностью среды рабочих станций и серверов АСУ ТП — файлов, папок, каталогов.

- **Контролирует запуск приложений по «белому списку»**

  Разрешает доступ только к тем программам, которые необходимы специалистам для работы. Такой «белый список» доверенных программ может формироваться как вручную, так и автоматически, если включить режим обучения.

Контролирует подключение съёмных носителей

Представьте ситуацию. Оператор АСУ ТП, чтобы не скучать в ночную смену, принёс USB-модем и подключил его к рабочей станции в изолированном сегменте. Сам того не подозревая, он только что создал канал для доставки вредоносного ПО.

InfoWatch ARMA Industrial Endpoint позволяет разрешать или запрещать подключение съёмных носителей на уровне класса устройств — например, флеш-носителей, CD- / DVD-дисков, мультимедийных устройств и др.

В чём преимущества замкнутой программной среды InfoWatch ARMA Industrial Endpoint

- ## Непрерывность работы АСУ ТП

  Задача замкнутой программной среды — сохранить непрерывность работы промышленных систем. Вредоносное программное обеспечение не сможет повлиять на систему даже при загрузке на рабочую станцию. В отличие от защиты только с применением антивируса, неразрешённое ПО не запустится, а злоумышленник не сможет причинить вред, даже если его код ещё не попал в базы антивирусных сигнатур.

- ## Минимальная нагрузка на оборудование

  InfoWatch ARMA Industrial Endpoint не проводит постоянного сканирования, поэтому не создаёт дополнительной нагрузки на рабочие станции и серверы АСУ ТП.

- ## Автоматизация процессов защиты

  Самостоятельно составляет «белые списки» программ благодаря режиму обучения. Это позволяет снизить влияние человеческого фактора при обработке больших массивов данных.

InfoWatch ARMA Management Console

Единый центр управления системой защиты InfoWatch ARMA

InfoWatch ARMA Management Console позволяет централизованно обновлять продукты системы защиты **InfoWatch ARMA** и управлять их конфигурацией, а также оптимизировать работу с киберугрозами и значительно повысить скорость расследования инцидентов.

Какие задачи решает

Централизованное управление системой защиты InfoWatch ARMA

Позволяет централизованно управлять конфигурацией и обновлениями промышленного межсетевого экрана нового поколения (**InfoWatch ARMA Industrial Firewall**) и средства защиты рабочих станций и серверов АСУ ТП (**InfoWatch ARMA Industrial Endpoint**), а также загрузкой обновлений правил промышленной СОВ, запуском «белых списков» программ и съёмных носителей.

Управление инцидентами ИБ и их расследование

Расследовать инциденты быстрее и удобнее, когда они отображаются в едином веб-интерфейсе. **InfoWatch ARMA Management Console** собирает события информационной безопасности, которые поступили со средств защиты системы **InfoWatch ARMA** и коррелирует их в инцидент, показывает инциденты как взаимосвязанную цепочку событий и позволяет определить начало кибератаки. При необходимости передаёт их в SOC- и SIEM-системы и информирует штат ИБ.

Предотвращение ущерба на производстве

Позволяет в автоматизированном режиме настраивать и передавать рекомендации по решению инцидентов как сотрудникам внутри штата ИБ, так и диспетчерам АСУ ТП на производственной площадке. Прозрачное и чёткое кросс-функциональное взаимодействие в едином веб-интерфейсе позволяет быстрее локализовать кибератаку и снизить риск физического ущерба на производстве.

Полная картина информационной безопасности на производстве

Предоставляет централизованный и мгновенный доступ ко всем действиям пользователей, событиям и инцидентам ИБ в сети, а также продуктам системы защиты **InfoWatch ARMA** независимо от масштаба компании и парка оборудования.

Как помогает специалистам ИБ быстрее и эффективнее реагировать на кибератаки

Схема автоматической блокировки угрозы и её источника

- **Контролирует и анализирует события ИБ**

  Автоматическая карта информационных потоков даёт полную информацию о сетевом взаимодействии сетевых компонентов АСУ ТП, что позволяет своевременно выявлять нарушения в сегментации сети, наличие небезопасного трафика и уведомлять о неавторизованном доступе.

- **Автоматизирует процессы ИБ: от реагирования на инциденты до взаимодействия специалистов**

  Позволяет настроить автоматизированную реакцию на инцидент, например, блокировку атаки и её источника, и передачу персональных рекомендаций по решению инцидента в зависимости от его типа.

- **Снижает количество ложных срабатываний**

  Позволяет настраивать индивидуальные правила корреляции и реагирования на инциденты.
  Это сокращает количество ложных срабатываний и повышает скорость обнаружения киберугроз.

Попробуйте на вашем предприятии

Команда InfoWatch предусмотрела несколько вариантов тестирования InfoWatch ARMA. Начать можно с демонстрации работы, а дальше выбрать, нужно ли вам приглашать специалиста InfoWatch для проведения пилотного проекта или удастся самостоятельно развернуть решение на ваших мощностях. Что бы вы ни выбрали, мы вас поддержим.

sales@infowatch.ru

+7 495 22 900 22

INFOWATCH®

InfoWatch — ведущий российский разработчик решений для обеспечения информационной безопасности организаций. Мощная академическая база, лучшие инженеры, математики и лингвисты с 2003 года обеспечивают технологическое преимущество InfoWatch в области защиты предприятий от современных киберугроз, информационных и инсайдерских атак.

Признанный эксперт и лидер рынка России и СНГ в области защиты корпоративных данных InfoWatch успешно выполнил более 3000 проектов для коммерческих и государственных организаций в 20-ти странах мира.

Две трети из 50-ти крупнейших компаний России (в соответствии с рейтингом «Эксперта») доверили InfoWatch выполнение масштабных и, зачастую, нестандартных проектов, связанных с информационной безопасностью. Причина такого доверия — не только высокое качество и уникальность технологий, но и чувство уверенности, которое возникает от сотрудничества с InfoWatch благодаря сопровождению клиентов на всех этапах проектных работ.

Некоторые клиенты


Министерство обороны Российской Федерации


Федеральная таможенная служба


Фонд социального страхования


Федеральная налоговая служба

Объединённая двигательная корпорация

arma.infowatch.ru /InfoWatchOut /InfoWatch