INFOWATCH®

ARMA IF

Sk Участник

INFOWATCH ARMA INDUSTRIAL FIREWALL

промышленный межсетевой экран для защиты сетей АСУ ТП

InfoWatch ARMA Стена K1000

InfoWatch ARMA Стена K100

InfoWatch ARMA BOX-6E

InfoWatch ARMA BOX-4E

Эшелонированная защита с межсетевым экраном InfoWatch ARMA

InfoWatch ARMA Industrial Firewall является частью единой системы InfoWatch ARMA. Использование единой системы уменьшает поверхность для атаки злоумышленника и позволяет выполнить до 90% технических требований ФСТЭК России (Приказ № 239).

ARMA MC

события — **InfoWatch ARMA Management Console** — *события*

единый центр управления системой InfoWatch ARMA и инцидентами ИБ — осуществляет сбор событий со средств защиты ARMA, формирование инцидентов по преднастроенным правилам корреляции и настройку автоматического реагирования на них

ARMA IF

InfoWatch ARMA Industrial Firewall

межсетевой экран для предотвращения атак на промышленные сети

ARMA IE

InfoWatch ARMA Industrial Endpoint

промышленная защита рабочих станций и серверов

Сертификация ФСТЭК России

№4429 — действителен до 27 июля 2026

Межсетевой экран типа «Д» четвёртого класса защиты (ИТ.МЭ.Д4.ПЗ)

Система обнаружения вторжений уровня сети четвёртого класса защиты (ИТ.СОВ.С4.ПЗ)

Включён в единый реестр российского ПО Минкомсвязи РФ

Основные возможности для защиты промышленной сети с InfoWatch ARMA Industrial Firewall

Система обнаружения и предотвращения вторжений (СОВ), IPS / IDS

Собственная база сигнатур постоянно пополняется командой экспертов InfoWatch ARMA — это позволяет обнаруживать попытки эксплуатации как классических, так и специфических уязвимостей. Базу можно дополнять пользовательскими правилами для максимальной защиты компании.

- Modbus TCP
- Modbus TCP x90 func. code (UMAS)
- S7 Communication
- S7 Communication plus
- OPC DA
- OPC UA
- IEC 60870-5-104
- IEC 61850-8-1 MMS
- IEC 61850-8-1 GOOSE
- KRUG
- ADS TCP
- EtherCAT
- DNP3
- Fanuc Focas
- ENIP / CIP

Глубокий анализ промышленного трафика (DPI)

Качественное обнаружение и предотвращение вторжений в АСУ ТП невозможно без глубокого анализа промышленного трафика.

- Возможность сократить информационные потоки только до регламентированных и уменьшить количество ложных срабатываний
- Работа с трафиком на уровне команд протоколов и настройка защиты под свои задачи. Благодаря детальному разбору трафика до уровня команд и их значений можно настроить автоматическую блокировку вредоносных пакетов в трафике от источника угрозы
- Высокая видимость сети позволяет детально зафиксировать действия пользователей и работу систем и своевременно отреагировать на киберугрозы

Глубина проработки и объём поддерживаемых функций и параметров приведены в техническом описании InfoWatch ARMA Industrial Firewall: arma-firewall.infowatch.ru

Основные сценарии, которые используют наши клиенты

1 контроль

действий пользователей

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

2 контроль

недопустимых операций с ПЛК

Установите запрет на изменения в системе — блокировку или оповещение при попытке загрузки программы управления или обновления ОС ПЛК

Фильтрация протоколов RDP и Telnet

Обнаруживает любую попытку подключения по протоколам удалённого доступа Telnet и RDP и позволяет контролировать данное подключение — как со стороны технической поддержки, так и со стороны сотрудников (например, ИТ-специалиста).

Анализ трафика с помощью потокового антивируса

Сканирование данных в сети, обнаружение вредоносных объектов (вирусы, скрипты, трояны и другие угрозы), блокировка их на сетевом уровне. Антивирусные базы регулярно обновляются для обнаружения актуальных угроз.

Безопасное удалённое подключение по ГОСТ VPN

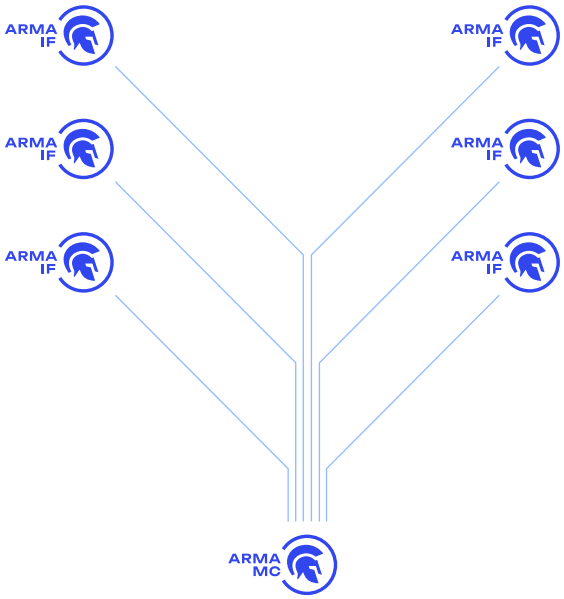
Безопасность передачи данных при объединении в единую сеть филиалов предприятия, удалённом подключении к производственной площадке и при работе технической поддержки.

Динамическая маршрутизация

Поддержка протоколов динамической маршрутизации трафика — OSPF, RIP и BGP. Поддержка протокола BFD позволяет быстро обнаруживать проблемы связности статических и динамических маршрутов и моментально восстанавливать соединение при разрыве.

Централизованное управление всеми межсетевыми экранами в сети с InfoWatch ARMA Management Console

Все межсетевые экраны InfoWatch ARMA Industrial Firewall подключаются к центру управления и автоматизации реагирования на инциденты InfoWatch ARMA Management Console. Для тех, у кого установлены десятки межсетевых экранов, централизованное администрирование позволяет экономить ресурсы специалистов ИБ благодаря нескольким возможностям:



Централизованный сбор событий

События передаются в единый интерфейс. Основываясь на преднастроенных правилах корреляции, из них автоматически генерируются инциденты

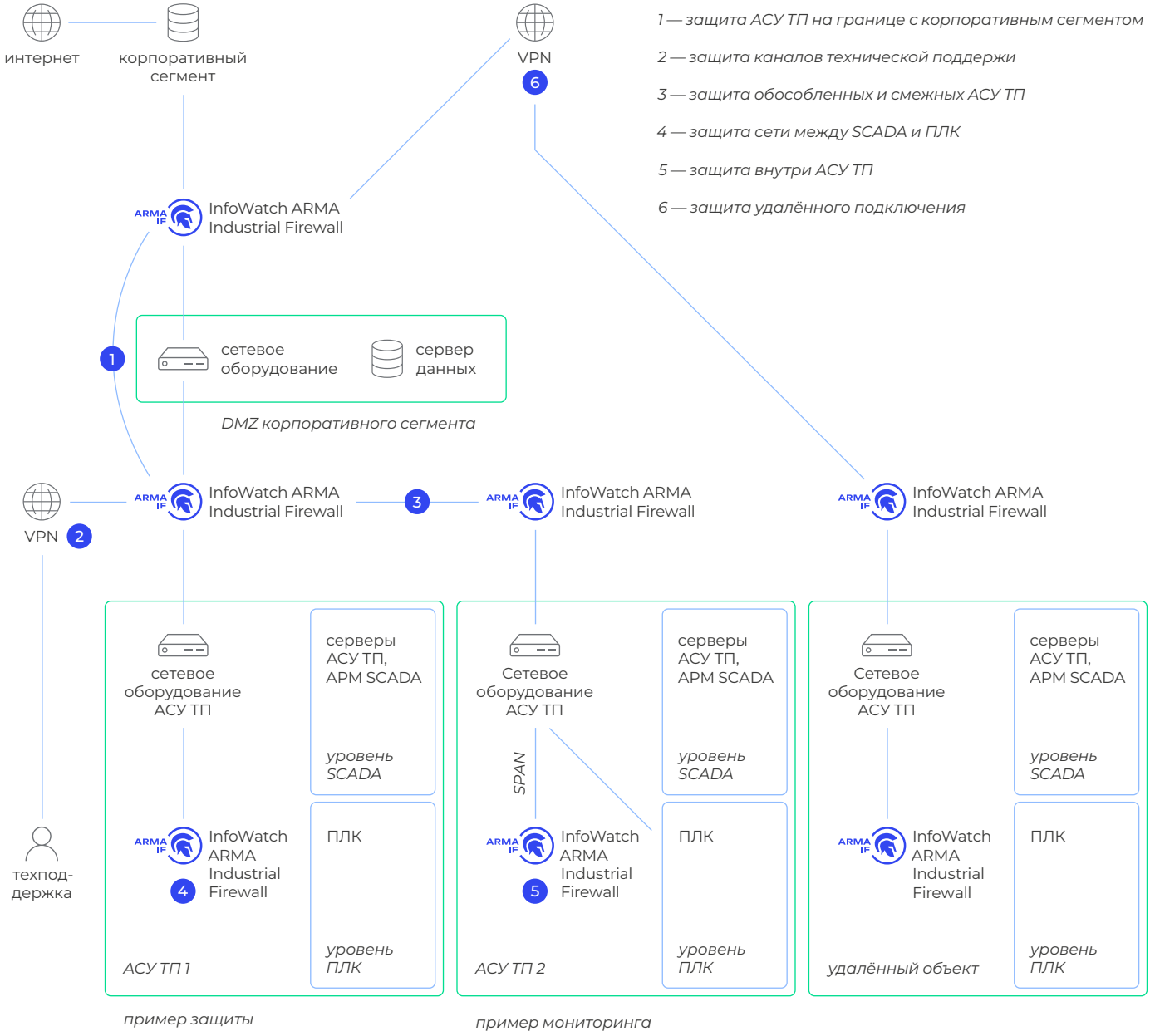
Автоматизация настройки политик

Достаточно настроить политики на одном межсетевом экране и тиражировать на прочие для экономии времени

Централизованное обновление правил СОВ

Регулярная процедура. Должна быть автоматизирована, чтобы не занимать время специалиста ИБ

Примеры установки InfoWatch ARMA Industrial Firewall



Технические функции

Межсетевой экран

- Фильтрация по адресам источника и назначения, протоколам, портам, операционной системе
- Каждое правило может задавать свои настройки ограничения одновременных соединений и определять свои настройки журналирования трафика
- Нормализация пакетов
- Возможность включения режима чистого маршрутизатора
- Маршрутизация мультикаст-трафика
- Сбор и отображение статистики для всех правил МЭ
- Отображение автоматических правил МЭ в веб-интерфейсе

Организация политик

- Поддержка псевдонимов (Alias) для IP-адресов, диапазонов портов, доменных имён (полностью определённое имя / FQDN)
- Возможность создания зон безопасности с помощью правил, ссылающихся на интерфейсные группы
- Категории правил
- Регулярное обновление базы GeoIP

Гибкий контроль таблицы состояний

- Настраиваемый размер таблицы состояний
- Каждое правило может задавать свои настройки: ограничение одновременных подключений от клиента, состояний для хоста, количества новых соединений в секунду, таймаут для состояний соединения, режим работы с соединениями
- Режимы работы с соединениями:
  - Keep (отслеживание состояния соединения)
  - Sloppy (менее строгий режим отслеживания)
  - Modulate (генерация Initial Sequence Number)

- Synproxy (режим защиты от атаки типа TCP YSN Flood)
- None (режим без отслеживания состояния соединения)

- Оптимизация работы с соединениями:
  - Normal (подходит для большинства сетей)
  - High latency (для спутниковых каналов связи)
  - Aggressive (истекают быстрее, тратится меньше памяти)
  - Conservative (истекают медленнее, тратится больше памяти)

Аутентификация

- Удалённые серверы LDAP и RADIUS
- Синхронизация пользователей с Active Directory
- Настройка прозрачной аутентификации (SSO)
- Локальный менеджер пользователей — ваучеры и карты

Авторизация

- Веб-интерфейс — локальный менеджер пользователей

Аккаунтинг

- Ваучеры и карты

Двухфакторная аутентификация

- Поддержка TOTP — одноразовых временных паролей
- Поддержка 2FA-аутентификации в Captive Portal, веб-прокси, VPN, веб-интерфейсе, SSH и консоли

Сертификаты

- Создание или импортирование удостоверяющего центра
- Создание или импортирование сертификатов

Поддержка 802.1Q VLAN

- Максимальное поддерживаемое число VLAN-сетей — 4096

Агрегирование каналов и переключение при сбое

- Переключение при сбое
- CARP
- Циклический алгоритм (Round Robin)
- Технология Ether Channel (FEC) от Cisco
- Протокол LACP из стандарта IEEE 802.3AD

Поддержка других типов интерфейсов

- Мостовые интерфейсы
- SPAN и RSPAN

Трансляция сетевых адресов (NAT)

- Перенаправление портов
- Поддержка NAT Reflection (обращение к серверам из внутренней сети по публичным IP-адресам)
- Логирование правил NAT
- Исходящий NAT

Шейпер трафика (Traffic Shaping)

- Ограничение пропускной способности
- Разделение пропускной способности
- Приоритезация трафика
- Критерии совпадения правил: протокол, адрес источника, адрес назначения, порт, направление

Dynamic DNS

- Выбор сервиса Dynamic DNS из списка
- Произвольно настраиваемый сервис

DNS-форвардер

- Переопределения для хостов и доменов

DNS-сервер

- Переопределения для хостов — ресурсных записей A и MX
- Списки доступа
- Поддержка DNSSEC

DNS-фильтрация

- Поддержка OpenDNS

DHCP-сервер

- Поддержка IPv4 и IPv6
- Поддержка режима ретрансляции
- Поддержка BOOTP-опций

MultiWAN

- Балансировка нагрузки
- Переключение на запасной канал при сбое основного канала
- Псевдонимы (Alias)

Network Time Server

- Поддержка источника Pulse Per Second
- Поддержка GPS-источника
- Задание и синхронизация времени по протоколу NTP

Обнаружение и предотвращение вторжений

- Работа в режиме Inline (устройство находится на пути трафика,)
- Предопределённые правила
- Блокировка сайтов по цифровым отпечаткам SSL-сертификатов
- Автообновление правил с помощью планировщика Cron
- Экспорт и импорт баз решающих правил локально и по протоколам FTP и SMB
- Фильтрация протоколов RDP и Telnet

Application Control (контроль приложений)

- Создание правил блокировки или разрешения для приложений

Layer 7 — фильтрация

- Системонезависимый API для userland-приложений, которые используют низкоуровневые механизмы захвата пакетов
- Блокировка трафика, распознанного с помощью DPI и запрещённого в настройках
- Правила для отчёта и блокировки приложений по отдельным подсетям — каждое может работать в режиме только отчёта или только блокировки

Captive Portal

- Сценарии использования:
  - Гостевая сеть
  - BYOD (мобильное рабочее место)
  - Wi-Fi-доступ в отелях и кемпингах
  - Управление шаблонами
  - Поддержка нескольких зон
- Аутентификаторы (все, поддерживаемые в системе)
- Менеджер ваучеров:
  - Поддержка нескольких баз данных ваучеров
  - Экспортирование ваучеров в формат CSV
  - Таймауты, распознавание зарегистрированных пользователей
- Управление пропускной способностью с помощью шейпера
- Обход портала по белым спискам IP- и MAC-адресов
- Отчёты в реальном времени — топ-лист по IP-адресам с наибольшим использованием пропускной способности канала, активные сессии, оставшееся время, интерфейс программирования REST

Виртуальные частные сети

- IPsec, OpenVPN и OpenVPN-ГОСТ — в режимах «сеть — сеть» и «узел — сеть» (подключение удалённых сотрудников)
- Экспорт конфигурации для лёгкой настройки клиента

- OpenVPN client export API для автоматизации процесса выдачи клиентских сертификатов для OpenVPN

Высокая доступность

- Переключение на запасной узел в кластере высокой доступности
- Loop Protection. Технологии STP и RSTP
- Синхронизация таблицы состояния соединений между узлами кластера
- Синхронизация настроек между узлами кластера

Кеширующий прокси

- Поддержка нескольких интерфейсов
- Режим прозрачного проксирования
- Создание списка разрешённых сайтов для варианта «запрещено всё» в режиме прозрачного проксирования
- Списки контроля доступа и чёрные списки ресурсов
- Кастомизация страниц уведомлений пользователей при блокировке доступа к веб-ресурсам
- Управление трафиком
- Поддержка скачиваемых чёрных списков
- ICAP (поддержка внешних антивирусов)
- Запись логов в БД, гибкая отчётность по доменам, URL, пользователям, IP-адресам и т. д.
- Логирование трафика OpenVPN с привязкой к пользователю
- Гибкая настройка правил пользователей и групп (приоритеты, чёрные и белые списки, правила ICAP, маршрутизация на разные интернет-каналы)
- Возможность формирования списка исключений для доступа к сайтам, имеющим собственные (самоподписанные) SSL-сертификаты. Список сайтов (доменов) устанавливается администратором вручную при настройке универсального шлюза безопасности
- Возможность принудительного ограничения пропускной способности прокси-сервера для отдельных пользователей

Настройка реверс-прокси (Nginx)

Антивирусная проверка

- Dr. Web Gateway Security Suite (приобретается отдельно). Работает со Squid через плагин C-ICAP
- Антивирусная проверка файлов, забираемых с прокси-сервера
- Гибкая настройка уровня детектирования
- Категоризация веб-ресурсов
- Регулярное обновление сигнатур
- История изменений настроек
- Поддержка интеграции с внешними антивирусами (ICAP)

Резервное копирование файлов

- Сохранение копий конфигурации на выделенный FTP-сервер

SNMP

- Мониторинг и ловушки

Диагностика

- Статус перезагрузки фильтров
- Информация по сетевому экрану
- Поддержка LLDP
- Топ по активным пользователям
- Таблицы сетевого экрана — псевдонимы (Alias) и Bogon-сети (немаршрутизируемые в интернете адреса)
- Текущие открытые сокеты
- Просмотр состояний всех соединений
- Сброс таблицы состояний
- Общие данные по состояниям соединений
- Технология Wake on LAN (пробуждение компьютера при получении пакета по сети)
- ARP-таблица (кэш протокола преобразования адресов)
- Просмотр данных в DNS
- NDP-таблица (кэш протокола обнаружения соседей)
- Утилита PING
- Захват пакетов
- Сканирование портов
- Трассировка маршрутов

Мониторинг

- Monit — проактивный мониторинг системы
- IPMITool — управление функциями аппаратной платформы

Усовершенствованная система отчётов

- Анализатор потоков Insight:
  - Полностью интегрирован в решение
  - Детальная агрегация данных
  - Графическая репрезентация данных
  - Поддержка поиска и кликабельность
  - Экспорт в формат CSV
- Здоровье системы:
  - Работа с собираемыми данными по циклическому алгоритму
  - Возможность выбора и масштабирования
  - Возможность экспорта
- Графики трафика (мониторинг трафика в реальном времени)
- Hardware widget — предоставление сведений об аппаратной платформе

Мониторинг сети

- NetFlow Exporter версий 5 и 9 (поставляет данные в Insight)

Интерфейс программирования REST

- Поддержка списков контроля доступа (ACL)
- API-правила
- Получение логов в форматах Syslog и CEF

InfoWatch ARMA Management Console

- Централизованная панель управления несколькими узлами на головном узле

Протоколы динамической маршрутизации

- RIPv.1, RIPv.2, OSPFv2 и OSPFv3, BGP
- Поддержка BFD для OSPF и BGP

Поддерживаемые промышленные протоколы

- Возможность фильтрации OPC UA, OPC DA, S7 Communication, S7 Communication plus, Modbus TCP, Modbus TCP x90 func. code (UMAS), IEC 60870-5-104, IEC 61850-8-1 MMS, IEC 61850-8-1 GOOSE, KRUG, ADS TCP, DNP3, Fanuc Focas, ENIP / CIP

Дополнительные возможности

- Интеграция с DLP InfoWatch Traffic Monitor
- Интеграция с песочницами по ICAP

Онлайн-документация

- В свободном доступе на русском языке, с поддержкой поиска

Сертифицированные аппаратные платформы

характеристики	InfoWatch ARMA Стена K100	InfoWatch ARMA Стена K1000
исполнение	настольное, с возможностью установки в 19”	19” 1U
процессор	CPU Intel Atom X6425E 2.00 GHz (4C / 4T)	Intel Xeon D-1537 (8C / 16T)
оперативная память	16 GB RAM DDR4	32 GB RAM DDR4
накопители SSD	256 GB M.2 SSD SATA	512 GB M.2 SSD SATA
сетевые порты	8 × RJ45 (1 Гб/с)	8 × RJ45 (1 Гб/с), 8 × SFP (1 Гб/с)
питание	внешний резервируемый блок	RPSU резервируемый 1+1 300 W
разъёмы	2 × USB, консольный порт RJ-45 (COM), HDMI	2 × USB, RJ-45 (COM), VGA
эксплуатация	от 10 до 35°C, влажность 20–80%	от 10 до 35°C, влажность 20–80%
дополнительно	крепление для стойки 19” в комплекте	
нагрузочные тесты	• режим UTM. 1000 правил МЭ, 10 000 правил IPS: EMIX-трафик = 296 Мбит/с	• режим МЭ. 1000 правил МЭ: EMIX-трафик = 840 Мбит/с • режим UTM. 1000 правил МЭ, 78 000 правил IPS: EMIX-трафик = 297 Мбит/с

характеристики	InfoWatch ARMA BOX-4E	InfoWatch ARMA BOX-6E
исполнение	промышленное, на DIN-рейку	настольное, промышленное, на DIN-рейку
процессор	Intel Atom E3930	Intel Core i7-8700
оперативная память	8 GB RAM DDR3L	32 GB RAM DDR4
накопители SSD	256 GB SSD SATA	2 × 256 GB SSD SATA
сетевые порты	4 × RJ45 (1 Гб/с)	6 × RJ45 (1 Гб/с, 4 × PoE)
питание	12В	24В (без адаптера), 90–264В, 120 W
разъёмы	2 × COM, 2 × USB, 1 × HDMI	2 × COM, 6 × USB, 1 × HDMI, 1 × DVI-I, 1 × DP
эксплуатация	-20 до 60°C, 10–95%, вибрация 2 м/с², 5–500 Гц	-40 до 60°C, 10–90%, вибрация 3 м/с², 5–500 Гц
дополнительно		2 слота Mini-PCIe, 1 × mSATA, 2 отсека 2,5” SATA
нагрузочные тесты	• режим МЭ. 1000 правил МЭ: EMIX-трафик = 903 Мбит/с • режим UTM. 20 правил МЭ и 192 правила IPS: EMIX-трафик = 84 Мбит/с	• режим МЭ. 1000 правил МЭ: EMIX-трафик = 910 Мбит/с • режим UTM. 500 правил МЭ, 70 000 правил IPS: EMIX-трафик = 230 Мбит/с

sales@infowatch.ru
+7 495 22 900 22