INFOWATCH® ARMA ARMA

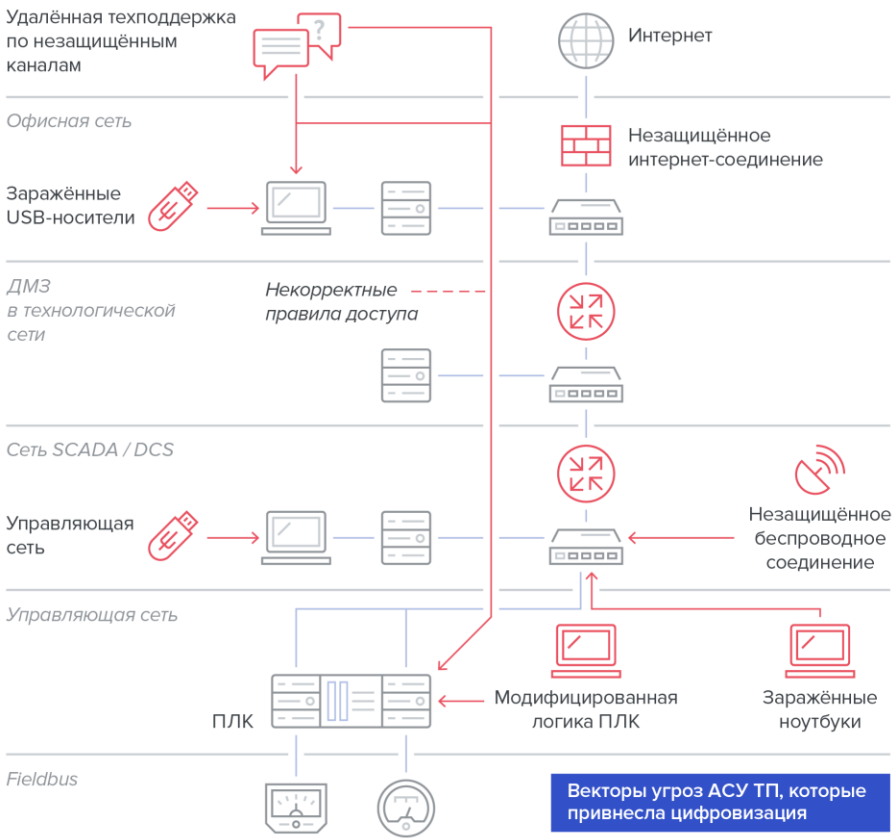
Эшелонированная защита АСУ ТП

Возможности и преимущества системы InfoWatch ARMA

Игорь Душа

Директор по развитию средств защиты АСУ ТП, InfoWatch ARMA

Обратная сторона цифровизации: повысился уровень угроз АСУ ТП



- **Смешение контуров IT- и OT-сетей, меняются модели угроз**
  - — **25% кибергруппировок** ищут способы обойти защитный компонент UAC в Windows
- **АСУ ТП недостаточно изолированы от корпоративного сегмента**
  - — **85% объектов КИИ** имеют связи с внешними сетями*
- **Уязвимости АСУ ТП могут эксплуатироваться удаленно**
  - — **70% уязвимостей АСУ ТП** могут эксплуатироваться удаленно**
  - — **53% уязвимостей АСУ ТП** опасные (Шкала CVSS-2020)

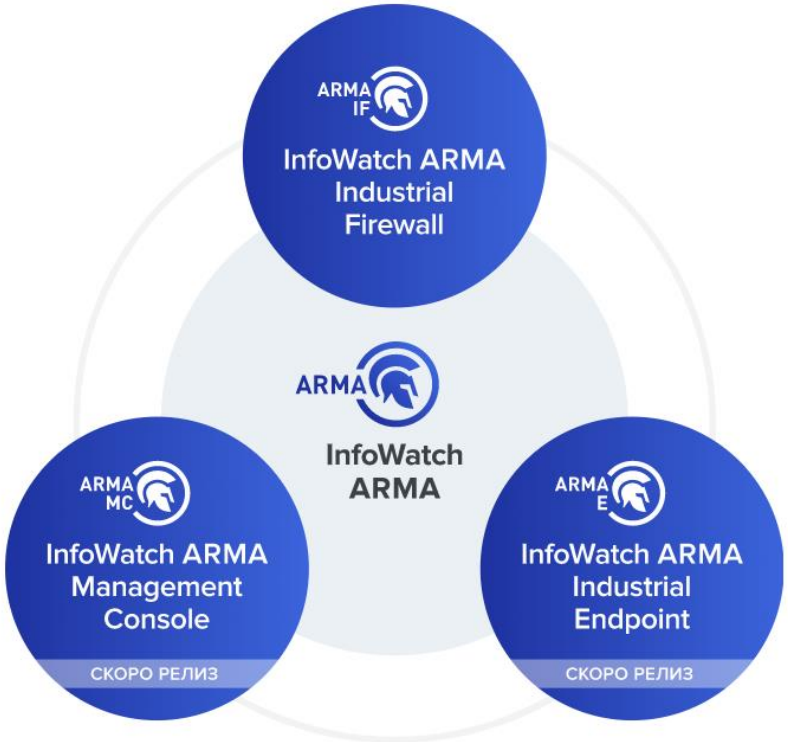
Данные исследований Аналитического Экспертного центра InfoWatch и Лаборатории Касперского, 2019–2010.
*Вопросы реализации ФЗ «О безопасности КИИ РФ». Выступление Алексея Кубарева, заместителя начальника управления ФСТЭК России.
**Анализ уязвимостей Claroty (1-е полугодие 2020)

Государство вводит требования к системам промышленной кибербезопасности

- **Закон о КИИ № 187 ФЗ**
  - — 12 субъектов КИИ обязаны выполнить требования законодательства
  - — Требования регулятора ФСТЭК России (Приказ № 239)
- **Категорирование завершено. Время строить систему безопасности и выбирать СЗИ**

InfoWatch ARMA

Комплексная система для обеспечения кибербезопасности АСУ ТП



Защищает КИИ от угроз, которые возникают при смешении IT- и OT-контуров и исходят **как от внутренних, так и от внешних** нарушителей

Все продукты интегрированы между собой

Комплексная система — выгоднее и легче внедрение

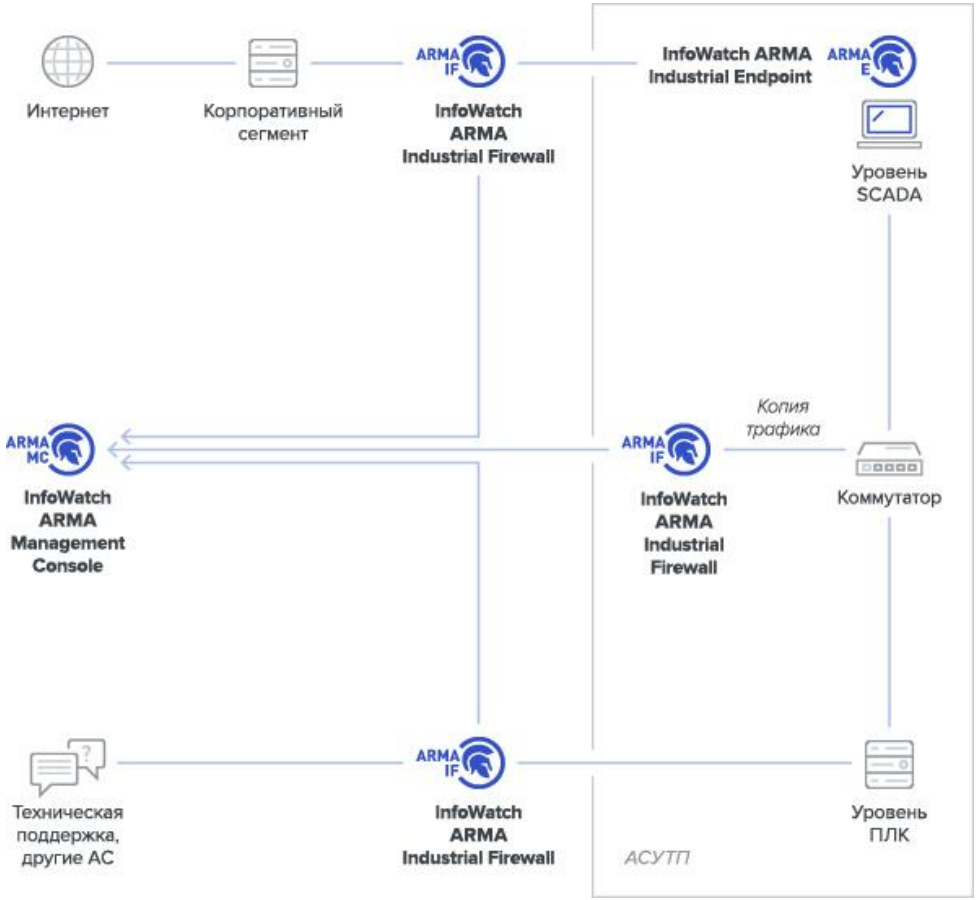
В комплексной системе **InfoWatch ARMA** все продукты интегрированы между собой.

Такой подход :

— **снижает время и затраты** на внедрение

— позволяет построить **эшелонированную защиту АСУ ТП**

— позволяет выполнить **до 90%** технических требований ФСТЭК России (Приказ №239).



INFOWATCH®

Отечественный промышленный межсетевой экран нового поколения

ARMA IF

InfoWatch ARMA Industrial Firewall

InfoWatch ARMA Industrial Firewall
Задачи, которые решает

1. Защита АСУ ТП от атак
2. Защита от несанкционированного доступа пользователей
3. Безопасное удалённое подключение через VPN

InfoWatch ARMA Industrial Firewall

Профессионалы доверяют защиту АСУ ТП нашему межсетевому экрану. Почему?

Глубокая инспекция промышленных протоколов

Обнаруживает вторжения по таким протоколам, как Modbus TCP, Modbus TCP x90 func. code (UMAS), OPC UA, OPC DA, IEC 60870 5 104, IEC 61850-8-1 MMS, IEC 61850-8-1 GOOSE, S7 Communication и другие

Встроенная система обнаружения вторжений (СОВ)

Содержит базу решающих правил СОВ для АСУ ТП, которая обновляется ежедневно!

Межсетевое экранирование для промышленных объектов

Позволяет блокировать неавторизованные действия и запрещать недопустимые операции с ПЛК: подключение к сети АСУ ТП, доступ к параметрам ПЛК или управление ПЛК по сети.

Безопасное удалённое подключение

Защищает от внутренних и внешних нарушителей. Обеспечивает безопасность информации при объединении в единую сеть филиалов предприятия, удаленном подключении к производственной площадке или при работе технической поддержки.

InfoWatch ARMA Industrial Firewall
Глубокая инспекция промышленных протоколов

Обнаружение вторжений и мониторинг (без фильтрации)	Глубокая фильтрации по полям протоколов
Modbus TCP Modbus TCP x90 func. code (UMAS) IEC 60870-5-104 IEC 61850-8-1 MMS IEC 61850-8-1 GOOSE OPC UA OPC DA ENIP / CIP S7 Communication S7 Communication plus Profibus DNP3	Modbus TCP Modbus TCP x90 func. code (UMAS) IEC 60870-5-104 IEC 61850-8-1 MMS IEC 61850-8-1 GOOSE OPC UA OPC DA S7 Communication

Значительно повышает видимость промышленной сети.

Кейс. Защита от несанкционированного действия
Фильтрация по команде протокола OPC DA

Заказчик	Крупное предприятие в нефтегазовой отрасли с большим количеством удалённых объектов
Задача	Разграничение доступа на прикладном уровне промышленных протоколов, **особенно** для протокола OPC DA, который не разбирается в достаточной для фильтрации степени никем из конкурентов
Решение	Установили стандартный модуль фильтрации промышленных протоколов и настроили в соответствии с политикой безопасности
Результат	Успешно прошли тестирование и настроили возможность разграничения доступа для инженеров разного уровня

InfoWatch ARMA Industrial Firewall
Встроенная система обнаружения вторжений

Обнаруживает и блокирует вредоносное ПО, компьютерные атаки и попытки эксплуатации уязвимостей ПЛК на сетевом и прикладном уровнях.

Почему наша СОВ обнаруживает больше типов атак и действует эффективнее, чем отечественные аналоги?

- **Содержит базу решающих правил СОВ для АСУ ТП, которая обновляется ежедневно!**

  Можно самостоятельно дополнять предустановленную базу СОВ собственными пользовательскими правилами для максимальной защиты конкретных АСУ ТП
- **Позволяет заблокировать угрозу и её источник в автоматическом режиме**
- **Позволяет защитить АСУ ТП на уровне отдельных команд благодаря функции фильтрация пакетов промышленных протоколов**

InfoWatch ARMA Industrial Firewall
Межсетевое экранирование для промышленных объектов

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

Почему наше межсетевое экранирование можно применять на промышленных объектах?

- Позволяет точно определить политики ИБ
- Проводит инспекцию пакетов промышленных протоколов и уменьшает количество ложных срабатываний
- Предотвращает самые распространённые атаки на сервисные функции промышленного оборудования

InfoWatch ARMA Industrial Firewall
Безопасное удалённое подключение

Обеспечивает безопасность информации при объединении в единую сеть филиалов предприятия, удаленном подключении к производственной площадке или при работе технической поддержки

Защита от внутренних и внешних нарушителей

- **Защищает доступ**

  Позволяет защитить каналы администрирования, создавать пароли разного уровня сложности, диагностировать целостность ПО.

- **Защищает удаленное подключение через VPN**

  Можно защитить периметр сети, объединить филиалы организации в виртуальную сеть (VPN) и организовать безопасное удаленное подключение.

InfoWatch ARMA Industrial Firewall
6 вариантов установки

1. Защита АСУ ТП на границе с корпоративным сегментом
2. Защита каналов технической поддержи
3. Защита обособленных и смежных АСУ ТП
4. Защита сети между SCADA и ПЛК
5. Защита внутри АСУ ТП
6. Защита удалённого подключения

6 вариантов защиты АСУ ТП межсетевым экранированием

Варианты поставок и конфигурации ПАК

InfoWatch ARMA Industrial Firewall
Варианты поставок

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

Программно-аппаратные комплексы (ПАК). Вариант InfoWatch ARMA.

Промышленные компьютеры

Серверы x86 / x64

Виртуальные машины

vmware

Microsoft Hyper-v

InfoWatch ARMA Industrial Firewall
Конфигурации ПАК

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

Монтаж в 19-дюймовую стойку		Монтаж на DIN-рейку или настольное исполнение	
ARMAIF-RUGRACK	ARMAIF-19RACK	ARMAIF-DIN	ARMAIF-BOX
			

Гарантия на оборудование — 1 год. Возможно расширение гарантии до пяти лет.

Гибкая система лицензирования

InfoWatch ARMA Industrial Firewall
Выгодное лицензирование

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

- **Межсетевой экран и VPN**
- **Система обнаружения вторжений**
- **Межсетевой экран нового поколения (NGFW)**

  Межсетевой экран с системой обнаружения вторжений и VPN

— Лицензия на ПО **бессрочная и без внутренних ограничений** (по числу ПЛК, пользователей и т. д.)

— Лицензируется **только ПО** (в том числе и Virtual Appliance)

— Лицензия при поставке в виде **ПАК привязана к оборудованию**

INFOWATCH®

Защита рабочих станций и серверов SCADA

ARMA E

InfoWatch ARMA Industrial Endpoint

Релиз — октябрь 2020

InfoWatch ARMA Industrial Endpoint

Релиз — октябрь 2020

Задачи, которые решает:

- **Контроль целостности ПО** рабочих станций и серверов АСУ ТП
- Контроль **подключения съёмных** носителей
- **Блокировка** любого недоверенного ПО

INFOWATCH®

Централизованное управление СЗИ и автоматическое реагирование на инциденты

ARMA MC

InfoWatch ARMA Management Console

Релиз — октябрь 2020

InfoWatch ARMA Management Console

Релиз — октябрь 2020

Задачи, которые решает:

- Централизованное управление продуктами **InfoWatch ARMA**
- **Управление инцидентами ИБ** и их расследование
- **Сбор событий ИБ** и предоставление инцидентов в SOC- и SIEM-системы
- Автоматическая блокировка угрозы **на всех СЗИ**
- Визуализация сети

INFOWATCH® ARMA ARMA

КЕЙСЫ

Как эффективно спроектировать защиту в соответствии с 187-ФЗ

Заказчик	Крупная компания-проектировщик, которая готовила проектную документацию для дочернего общества ФСК ЕЭС
Задача	Выполнить технические меры 187-ФЗ единым отечественным решением по защите информации
Решение	В дополнение к антивирусам и средствам резервного копирования был выбран межсетевой экран **InfoWatch ARMA** для закрытия большинства технических мер
Результат	**InfoWatch ARMA** позволила нивелировать большую часть угроз из модели, что позволило сократить затраты проектировщика

Защита от атак АСУ ТП

Заказчик	Крупная электрораспределительная компания, которая в входит в ПАО «Россети»
Задача	Провести аудит информационной безопасности АСУ ТП
Решение	Установили решение на порт зеркалирования, переправляли трафик на работающий одновременно с нами PT ISIM
Результат	Выявили ряд уязвимостей, вредоносного ПО и нерегламентированных информационных потоков, которые не были выявлены конкурентными решениями

Защита удалённого доступа

Заказчик	Подстанция, которая берёт попутный газ, сжигает, генерирует электричество и распределяет его
Проблема	Перебои в работе АСУТП. Разные агрегаты начали отключаться. На восстановление требовалось до 3 часов
Решение	Установка **InfoWatch ARMA.** Мониторинг и логирование всего происходящего по внешнему каналу связи, оставленному для технической поддержки
Результат	Организован защищённый удалённый доступ для технической поддержки

Группа компаний InfoWatch

INFOWATCH®

17 лет на рынке
информационной безопасности

Сертификация
на соответствие требованиям ФСБ, ФСТЭК и отраслевых стандартов

37 из 50-ти
крупнейших компаний России используют решения InfoWatch

Технологическое лидерство,
подтверждённое патентами

Представительства
в 15-ти регионах СНГ

2000 клиентов
из 20-ти отраслей в 20-ти странах

Клиенты

INFOWATCH®

НЕФТЕГАЗОВЫЙ СЕКТОР

Газпром ВНИИГАЗ

СлавНефть

Транснефть

ОАО «ВНИПИгаздобыча»

ЭНЕРГЕТИКА

e·on

ИНТЕР РАО
КАШИРСКАЯ ГРЭС

ТОПЛИВНАЯ КОМПАНИЯ РОСАТОМА
ТВЭЛ

ОДК

ПРОМЫШЛЕННОСТЬ

МИ МОСКОВСКИЙ ВЕРТОЛЕТНЫЙ ЗАВОД ИМ. М.Л. МИЛЯ

ОСК ОБЪЕДИНЕННАЯ СУДОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ

kira

ОБЪЕДИНЕННАЯ ПРОМЫШЛЕННАЯ КОРПОРАЦИЯ ОБОРОНПРОМ

ТЕЛЕКОММУНИКАЦИИ

МТС

БАНКИ

СБЕРБАНК
Всегда рядом

Райффайзен БАНК

БАНК Форштадт

Банк Кольцо Урала

СвязьБанк

HOME CREDIT BANK

СТРАХОВЫЕ КОМПАНИИ

СОГАЗ
СТРАХОВАЯ ГРУППА

ВСК СТРАХОВОЙ ДОМ

ГОСУДАРСТВЕННЫЙ СЕКТОР

Федеральная налоговая служба

Федеральная таможенная служба

Министерство обороны РФ

Фонд социального страхования

МЕДИЦИНА И ФАРМАЦЕВТИКА

STADA

НИАРМЕДИК

ТРАНСПОРТ И ЛОГИСТИКА

РОСЖЕЛДОР ПРОЕКТ

Газпром АВИА

SPSR express

ТОРГОВЛЯ

FIX price

МАГНИТ

О'КЕЙ

KUPIVIP.RU

INFOWATCH® ARMA ARMA

ХОТИТЕ ПРОВЕСТИ ПОЛНЫЙ ТЕСТ-ДРАЙВ INFOWATCH ARMA?

Оформите заявку на сайте
arma.infowatch.ru

/InfoWatchOut

/InfoWatch

/infowatchnews