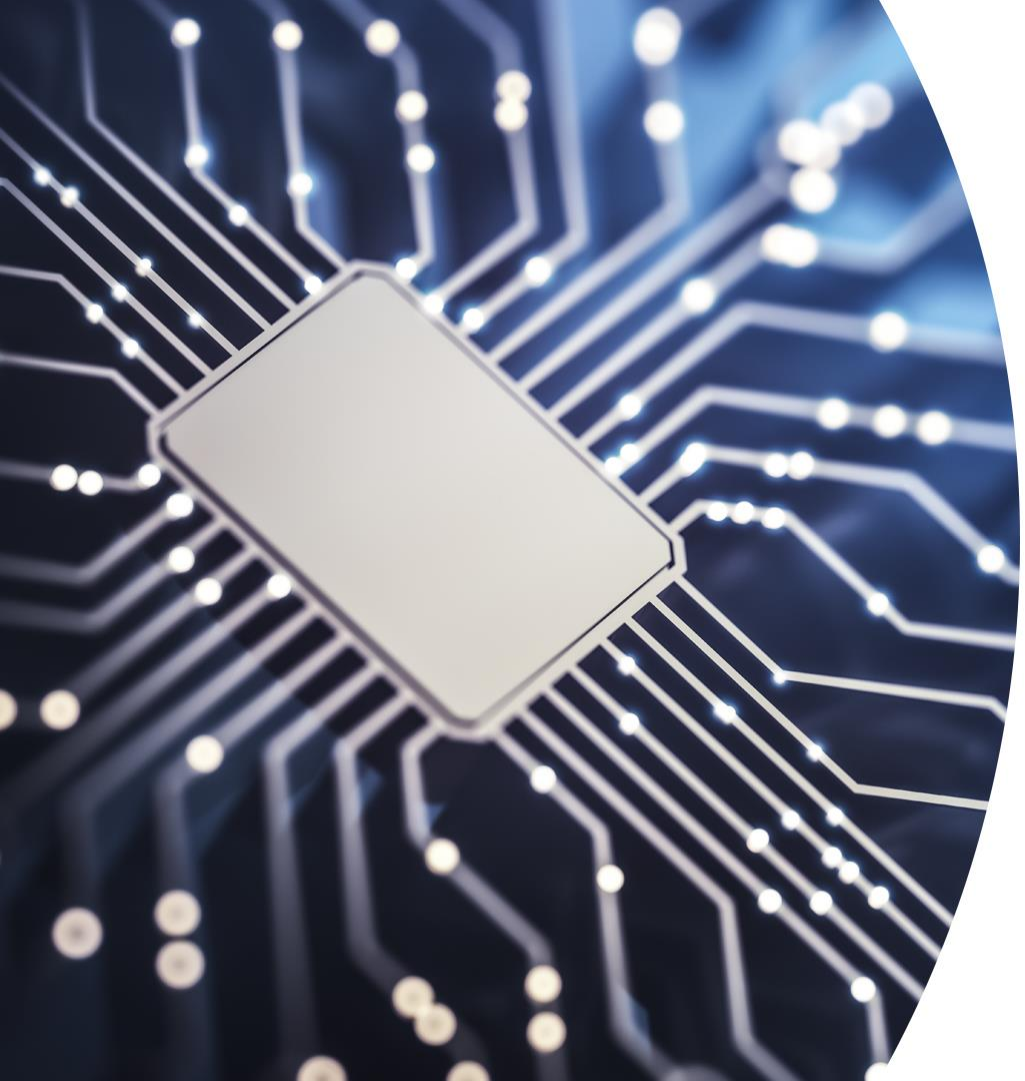
INFOWATCH® ARMA ARMA

Как защитить АСУ ТП от кибератак, обеспечить непрерывность промышленных процессов и выполнить 187-ФЗ

На примере системы InfoWatch ARMA

Игорь Душа

Технический директор InfoWatch ARMA



Крупные задачи ИБ АСУ ТП

- **Обеспечить защиту АСУ ТП** от компьютерных атак
- **Выполнить требования** регулятора
- **Автоматизировать работу** отдела ИБ и эффективно выполнить первые две задачи

ТОП-4 тех. задач ИБ АСУ ТП

1	Построение защиты от актуальных киберугроз
2	Управление активами и инвентаризация
3	Управление инцидентами и их расследование
4	Управление уязвимостями

*https://www.sans.org/u/1bRw

Построение защиты от актуальных киберугроз

1	**Построение защиты от актуальных киберугроз**	▶ Сетевая сегментация и управление доступом ▶ Защита рабочих станций и серверов ▶ Мониторинг и сбор событий ИБ
2	Управление активами и инвентаризация	
3	Управление инцидентами и их расследование	
4	Управление уязвимостями	

*https://www.sans.org/u/1bRw

arma-firewall.infowatch.ru

Промышленный межсетевой экран нового поколения

InfoWatch ARMA Industrial Firewall

Защита КИИ промышленных объектов от сетевых атак

- Проходит сертификацию: МЭ тип «Д», УД4; СОВ, УД4.
- Включён в единый реестр российского ПО Минкомсвязи РФ

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

→ Промышленная система обнаружения и предотвращения вторжений

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

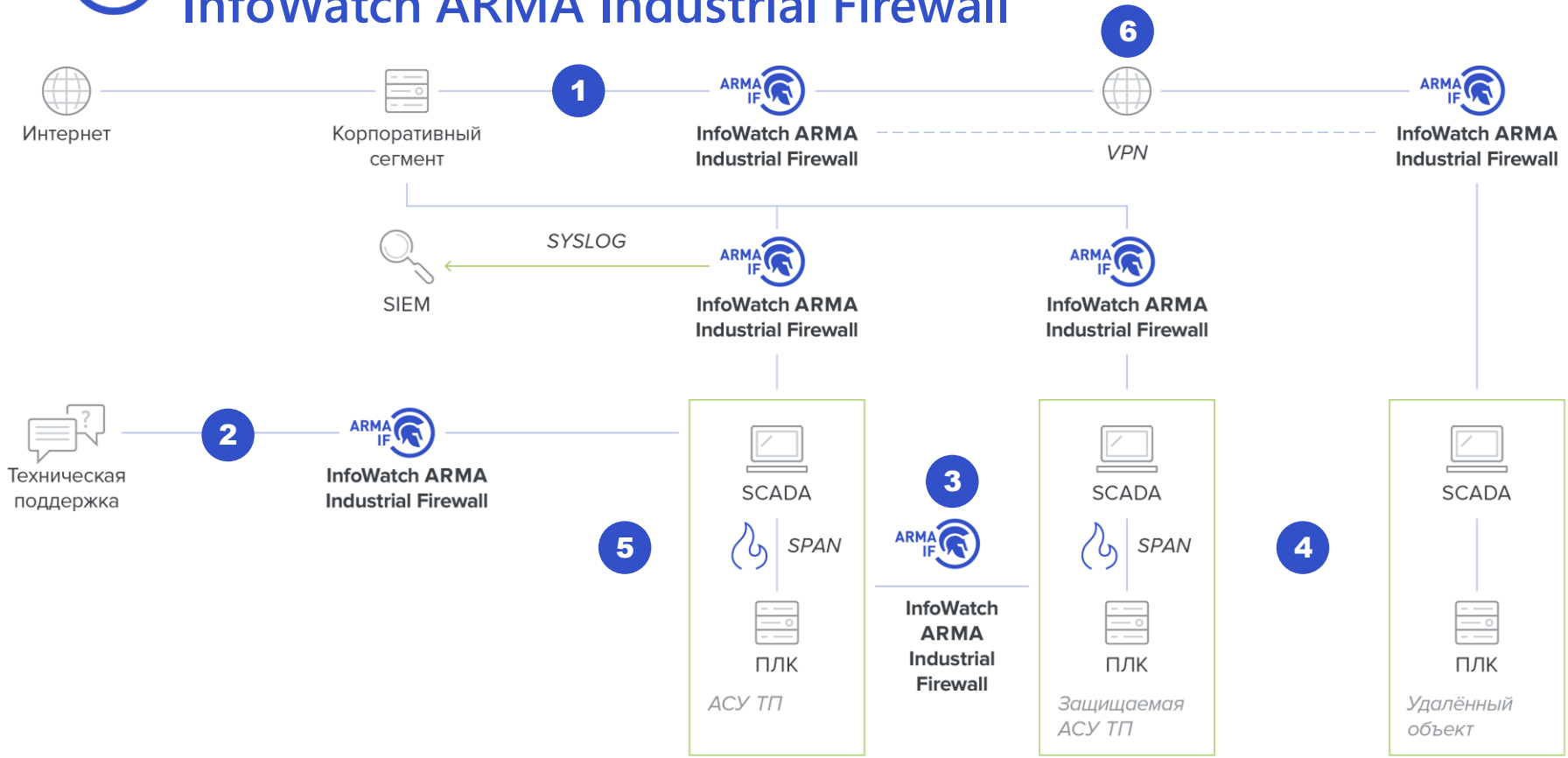
→ Межсетевое экранирование для промышленных объектов

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

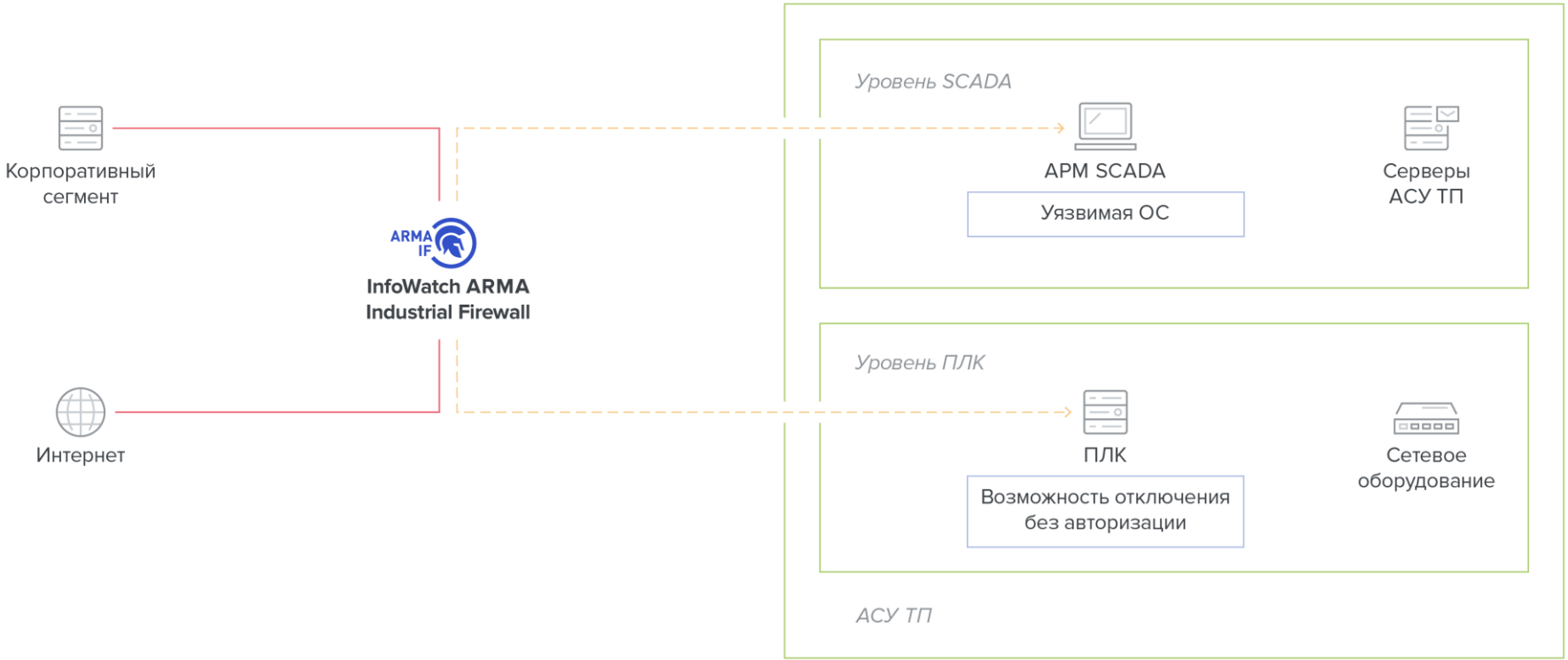
→ Безопасное удалённое подключение

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

Сегментация промышленной сети с InfoWatch ARMA Industrial Firewall



Эшелонированная защита
Виртуальный патчинг



Ограничения и ещё раз ограничения

Замкнутая среда в АСУ ТП — лучший вариант:

- Ограничение внешних информационных потоков и подключений к системе
- Ограничение программной среды
- Только разрешённые информационные потоки внутри системы

INFOWATCH®

Защита рабочих станций и серверов АСУ ТП

ARMA IE

InfoWatch ARMA Industrial Endpoint

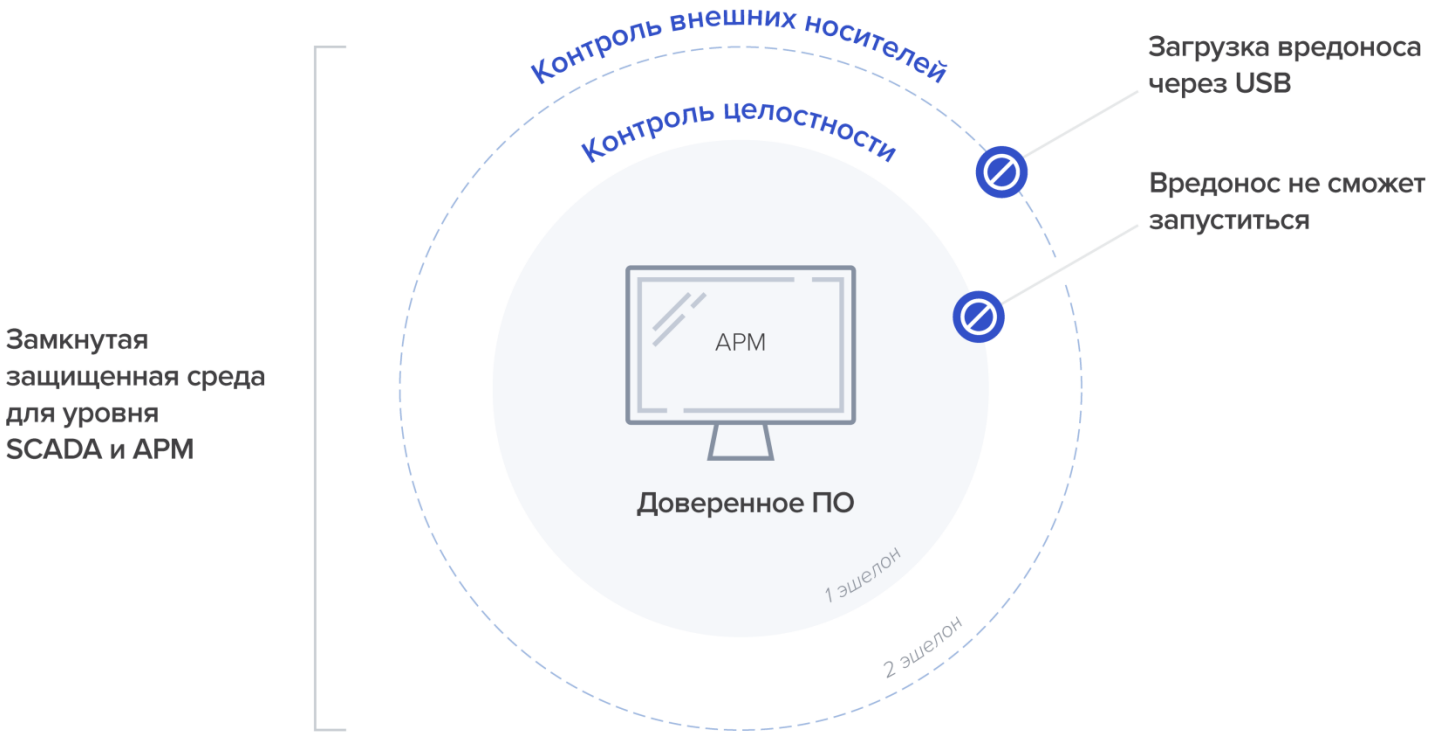
Создание замкнутой защищённой среды

arma-endpoint.infowatch.ru

Защита рабочих станций и серверов АСУ ТП

- **Контроль целостности файлов** рабочих станций и серверов АСУ ТП
- **Позволяет ограничивать** главный канал распространения угроз — **USB и другие съёмные носители**
- **Блокировка** недоверенного **ПО** на основе белых списков

Как InfoWatch ARMA Industrial Endpoint организует замкнутую защищенную среду



Мониторинг событий ИБ

- Контроль версий проектов ПЛК и SCADA
- Выявление фактов эксплуатации уязвимостей
- Перепрошивка ПЛК
- Информирование об опасных значениях технологического процесса и контроль параметров

InfoWatch ARMA Industrial Firewall
Встроенная система обнаружения вторжений (СОВ)

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

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

  Обнаруживает попытки эксплуатации классических уязвимостей и специфических уязвимостей АСУ ТП. Можно дополнять базу собственными пользовательскими правилами.

- **Работает как в режиме обнаружения, так и предотвращения вторжений**

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

InfoWatch ARMA Industrial Firewall
Глубокая инспекция промышленных протоколов с фильтрацией до уровня команд

Обнаружение вторжений и мониторинг (без фильтрации)	Глубокая фильтрация по полям протоколов
Modbus TCP	Modbus TCP
Modbus TCP x90 func. code (UMAS)	Modbus TCP x90 func. code (UMAS)
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
OPC UA	OPC UA
OPC DA	OPC DA
ENIP / CIP	S7 Communication
S7 Communication	
S7 Communication plus	
Profinet	
DNP3	

Инспекция пакетов трафика даёт высокую видимость промышленной сети, а повысить уровень защиты сети позволяет работа на уровне команд протоколов.

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

Сценарии защиты АСУ ТП посредством фильтрации протоколов

Глубокая инспекция пакетов промышленного трафика позволяет:

→ Повысить видимость промышленной сети

→ Ограничить промышленный трафик на уровне отдельных промышленных протоколов

Работа с трафиком на уровне команд протоколов

Сценарии, которые используют наши клиенты:

→ Контроль недопустимых операций в ОТ-сети

→ Контроль доступа к удалённой площадке и разграничение прав пользователей

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

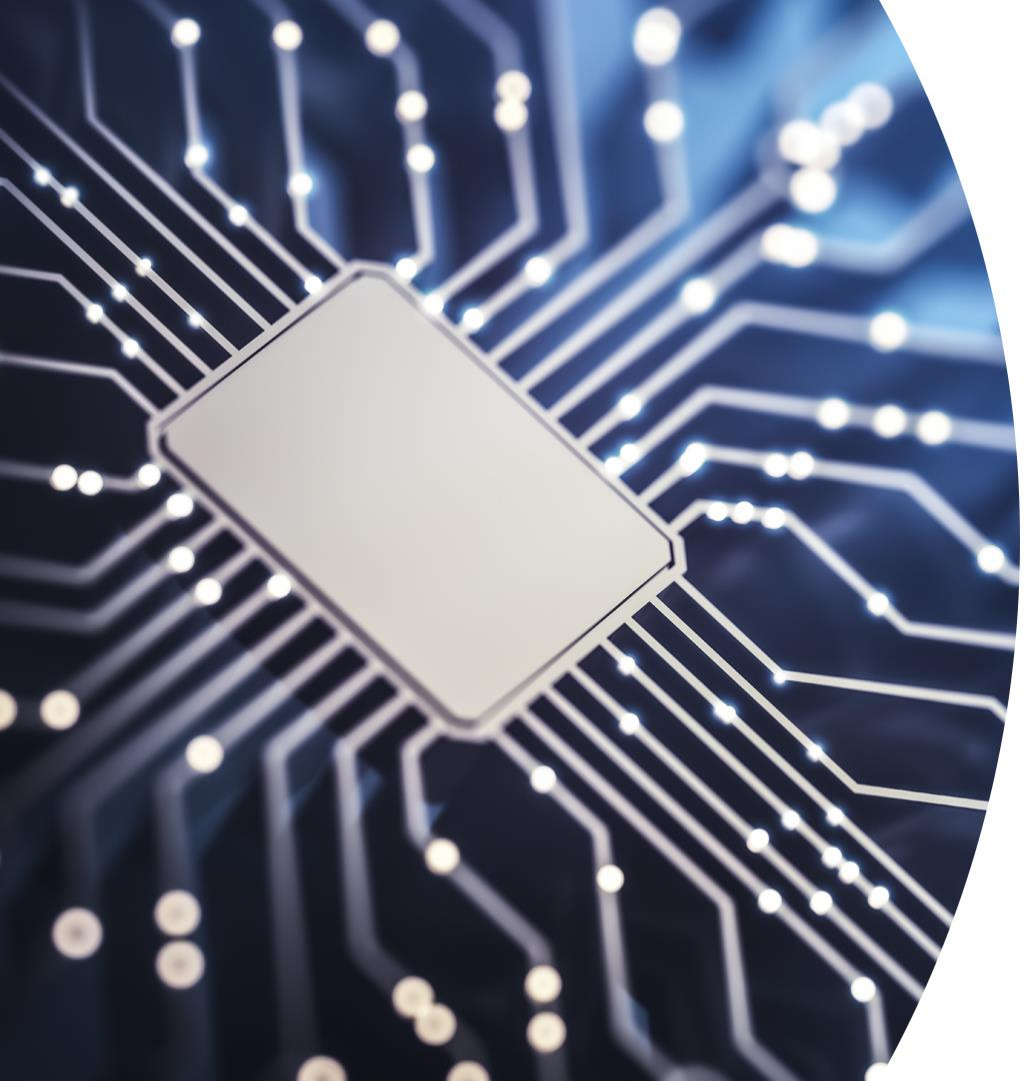
Заказчик	Крупное предприятие в нефтегазовой отрасли с большим количеством удалённых объектов
Задача	Разграничение доступа на прикладном уровне промышленных протоколов, **особенно** для протокола OPC DA, который не разбирается в достаточной для фильтрации степени никем из конкурентов
Решение	Установили 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

Управление активами и инвентаризация

1	Построение защиты от актуальных киберугроз	
2	**Управление активами и инвентаризация**	▶ Инвентаризация активов, ведение базы реальных устройств и информационных потоков между ними ▶ Учет uptime/downtime оборудования и серверов ▶ Аналитика подключений к оборудованию АСУ ТП
3	Управление инцидентами и их расследование	
4	Управление уязвимостями	

Управление инцидентами и их расследование

1	Построение защиты от актуальных киберугроз	
2	Управление активами и инвентаризация	
3	**Управление инцидентами и их расследование**	▶ Выявление инцидентов и ликвидация последствий ▶ Определение инцидентов из общего потока событий ИБ ▶ Сокращение ложных срабатываний
4	Управление уязвимостями	



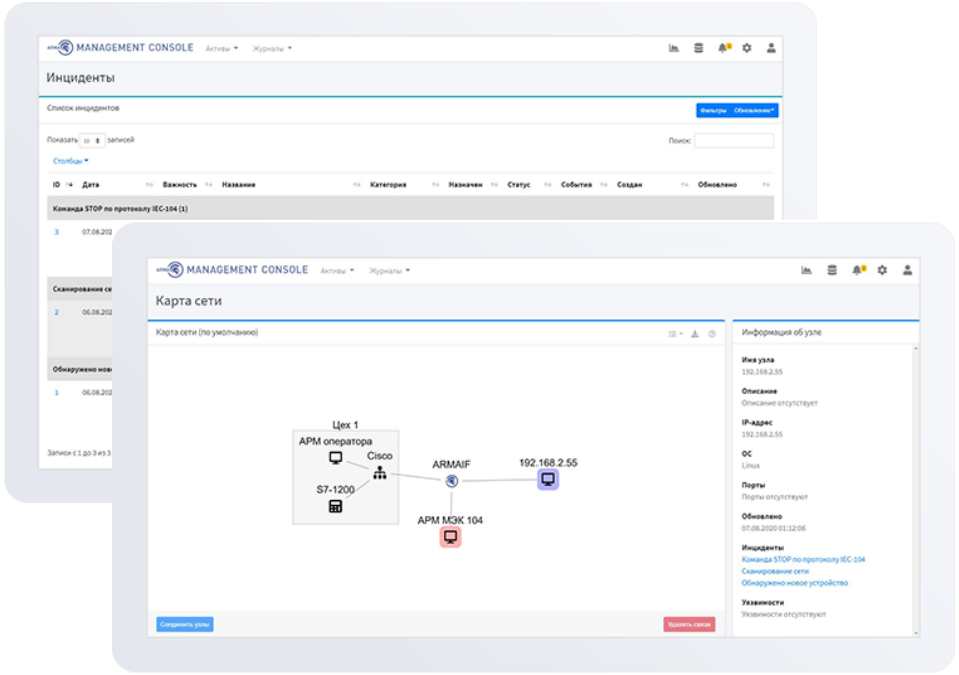
Единый центр управления системой защиты InfoWatch ARMA

InfoWatch ARMA Management Console

Централизованное обновление и управление конфигурациями

arma-console.infowatch.ru

Централизованное обновление и управление конфигурациями



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

Автоматизация реакции на инциденты

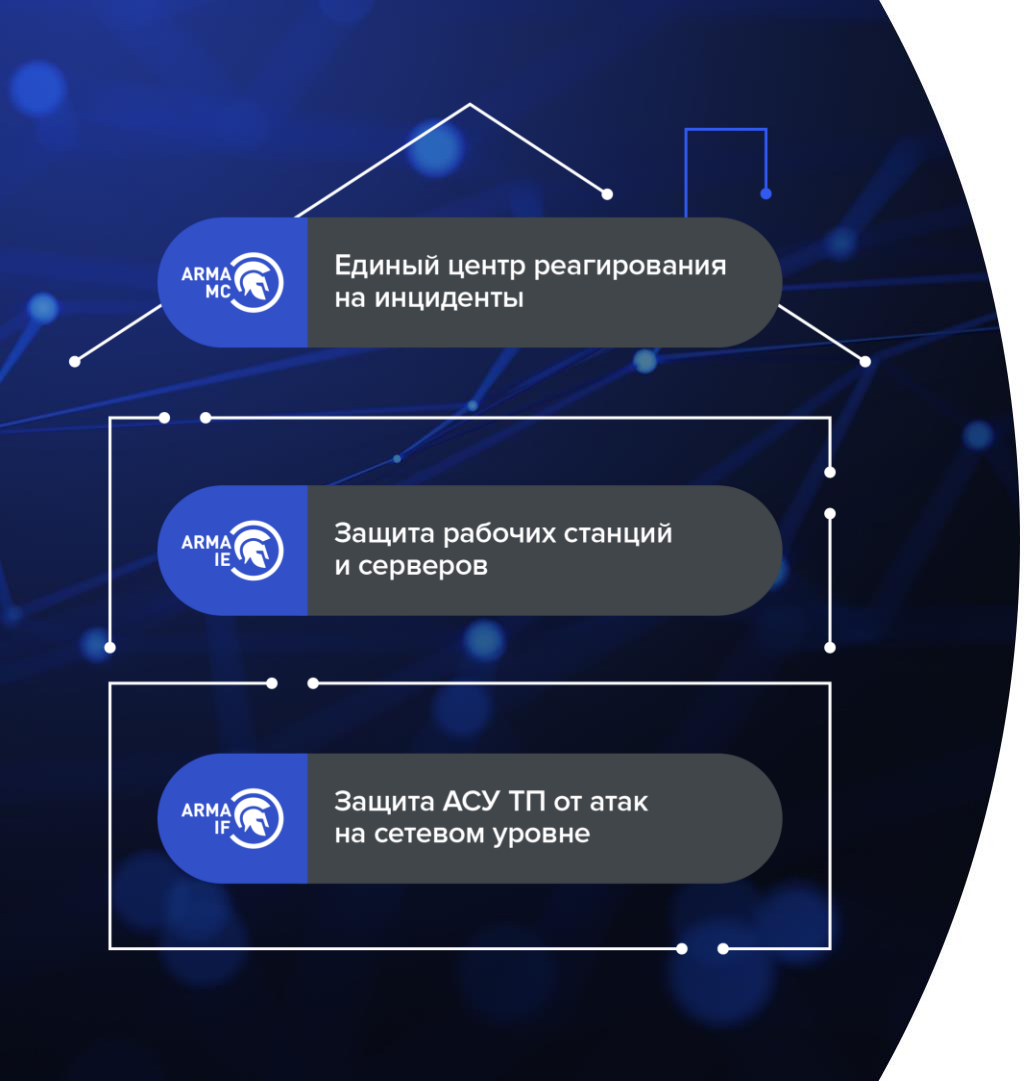
«Кадровый голод» требует автоматизации

→ К 2022 году $(ISC)^2$ прогнозирует* **1,8 миллиона незаполненных должностей OT security,** что дополняет нынешнюю нехватку кадров

→ **Адекватная реакция на недостаток квалифицированных кадров:**

- Настройка систем интеграторами, а не эксплуатантом
- Обучение уже нанятых сотрудников практическим навыкам
- Автоматизация реагирования на инциденты
- Использование внешних SOC

*https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

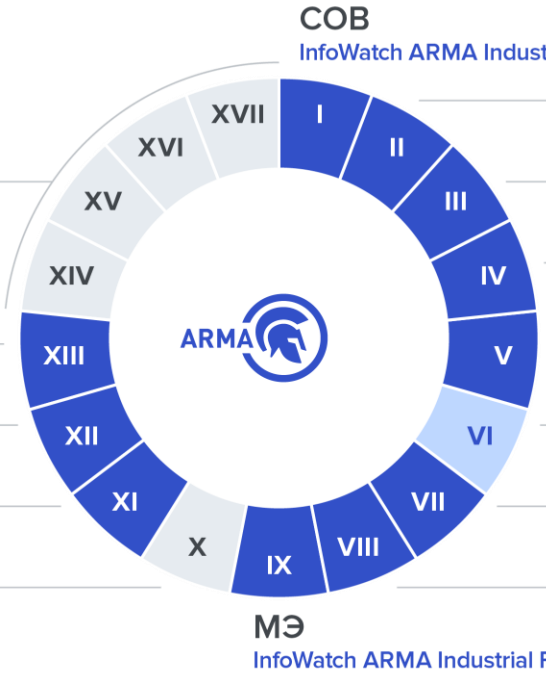


INFOWATCH®

InfoWatch ARMA — комплексная система для обеспечения кибербезопасности АСУ ТП

- Эшелонированная **защита с единым центром управления** системой защиты информации
- Выполнение до 90% **технических требований** приказа ФСТЭК России № 239
- **Снижение стоимости владения** и ресурсов на сопровождение системы

До 90% выполнения технических требований Приказа № 239 ФСТЭК России



СОВ
InfoWatch ARMA Industrial Firewall

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Endpoint
InfoWatch ARMA Industrial Endpoint

Endpoint
InfoWatch ARMA Industrial Endpoint

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Антивирусная защита
в разработке

СОВ
InfoWatch ARMA Industrial Firewall

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

МЭ
InfoWatch ARMA Industrial Firewall

Физическая безопасность

Endpoint, МЭ
InfoWatch ARMA Industrial Firewall / Industrial Endpoint

Средства управления инцидентами
InfoWatch ARMA Management Console

Endpoint
InfoWatch ARMA Industrial Endpoint

Организационные меры

Вышлем на почту карту соответствия InfoWatch ARMA группам мер ФСТЭК России

Запросите карту, оставив свой e-mail здесь

Возможность встроить в текущую инфраструктуру

INFOWATCH®

Интеграция и уведомление

Применение каждого средства защиты InfoWatch ARMA по отдельности

1. InfoWatch ARMA Industrial Firewall
2. InfoWatch ARMA Management Console
3. InfoWatch ARMA Industrial Endpoint

InfoWatch ARMA

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

Industrial Firewall	NGFW и VPN	IPS, IDS	Глубокая инспекция промышленных протоколов (DPI)	NGFW и VPN + DPI+ IPS, IDS
Industrial Endpoint	Количество защищаемых устройств			
Management Console	Количество подключаемых СЗИ			

— Лицензия на Industrial Firewall и Management Console **бессрочная**

— Поставка Industrial Firewall в виде лицензий или ПАК

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

INFOWATCH® ARMA ARMA

КАКИЕ ЗАДАЧИ СТОЯТ ПЕРЕД ВАМИ?

НАЙДЁМ РЕШЕНИЕ И ПРОВЕДЁМ ДЕМО

Исследование инцидентов
с АСУ ТП за 2020 г. от InfoWatch

Скачайте здесь

/InfoWatchOut /InfoWatch /infowatchnews

arma.infowatch.ru