INFOWATCH® ARMA ARMA

ЭШЕЛОНИРОВАННАЯ ЗАЩИТА АСУ ТП ОТ КИБЕРАТАК С СИСТЕМОЙ INFOWATCH ARMA

Николай Стаховский

Техническое сопровождение продаж,
InfoWatch ARMA

Современные вызовы кибербезопасности

INFOWATCH®

→ «Размытие» периметра — кибератаки гигантского размера

Гибридная архитектура: IT- и OT-сети управляются компонентами, которые взаимодействуют с физическими объектами (киберфизические системы)

→ Ограниченная видимость сети

Разновендорный парк без единого центра управления и расследования инцидентов: долгая реакция на инцидент, отсутствие полной картины происходящего в сети.
Как вы защитите то, что не видите?

→ Недостаток квалифицированных кадров

Кадровый «голод», «профессиональное выгорание» существующего штата ИБ: высокая нагрузка, рассогласованность действий служб ИТ и ИБ

→ Требования законодательства ужесточаются

«Кадровый голод» требует автоматизации

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

Реакция на недостаток квалифицированных кадров

→ Использование внешних SOC

→ Автоматизация реагирования на инциденты

→ Настройка систем интеграторами, а не эксплуатантом

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

3 тенденции ИБ АСУ ТП

→ **Киберпреступники могут получить неограниченный доступ** к любому устройству, работающему в сети, включая SCADA-приложения и другие критически важные компоненты АСУ ТП

Тенденция № 1. Эшелонированная защита АСУ ТП

Чем больше эшелонов защиты, тем меньше шансов у хакера совершить атаку

3 тенденции ИБ АСУ ТП

→ Сегодня **не только промышленные сети, но и рабочие станции АСУ ТП** уже имеют подключения к ИТ-сетям и доступ к цеху и ПЛК. Именно они часто становятся начальной точкой атаки

Тенденция № 2. Замкнутая программная среда

Ограничения и ещё раз ограничения:

→ Ограничение подключений к системе и информационных потоков извне

→ Ограничение программной среды

→ Только разрешённые информационные потоки внутри системы

3 тенденции ИБ АСУ ТП

- → Массовый переход на удалёнку спровоцировал киберпреступников **обратить внимание на сетевые ресурсы и активы компаний, которые «торчат наружу»**
- → Выиграли те компании, у которых уже были установлены **инструменты по повышению видимости событий в сети и учёту её активов,** а также более тщательного наблюдения за хостами

Тенденция № 3. Высокая видимость сети и централизованное управление системой защиты

Промышленный межсетевой экран нового поколения — уже не помеха работе АСУ ТП

INFOWATCH®

Уровни зрелости процесса

Зрелость: Низкая → Высокая

0

СЗИ отсутствуют

1

Внедрены базовые СЗИ

- Антивирус
- Шлюз на периметре

2

Внедряются специализированные средства ИБ АСУ ТП

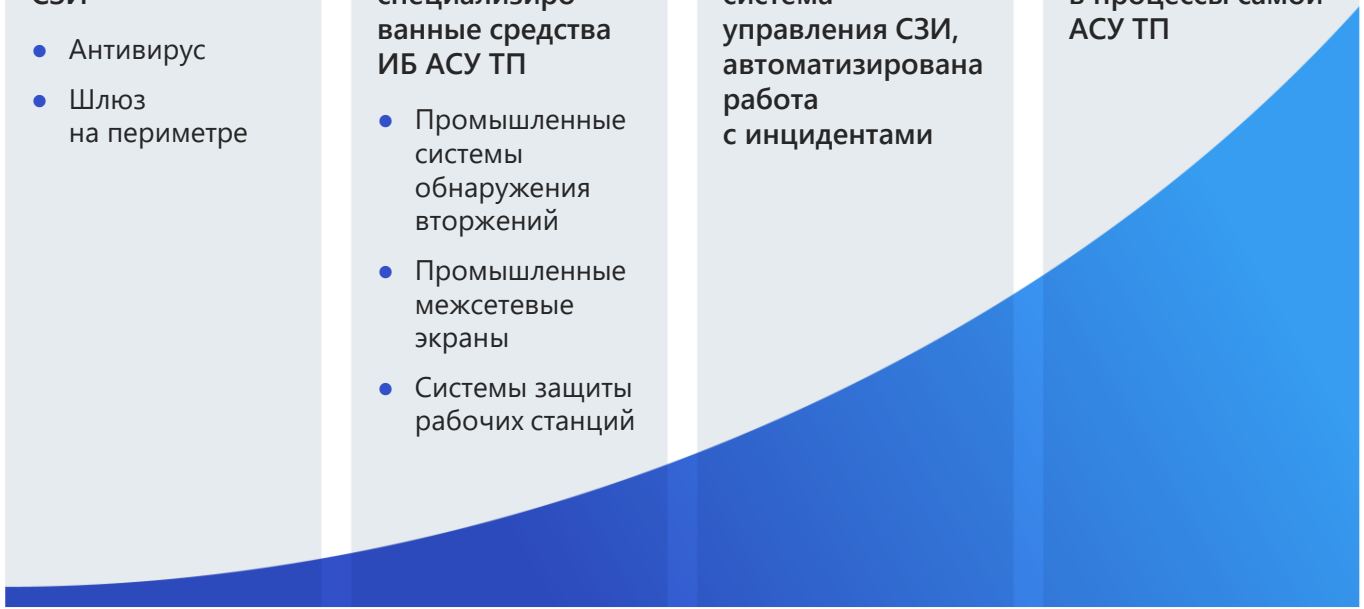
- Промышленные системы обнаружения вторжений
- Промышленные межсетевые экраны
- Системы защиты рабочих станций

3

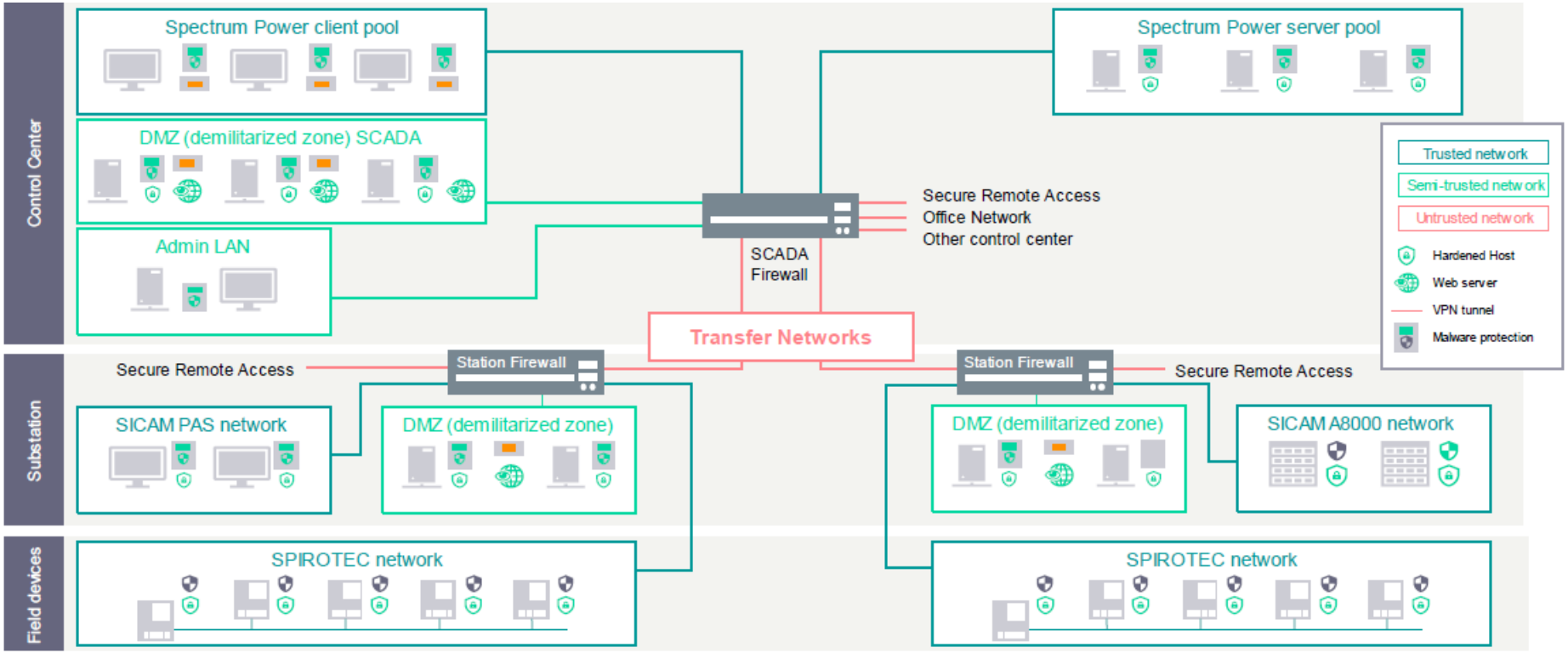
Сформирована система управления СЗИ, автоматизирована работа с инцидентами

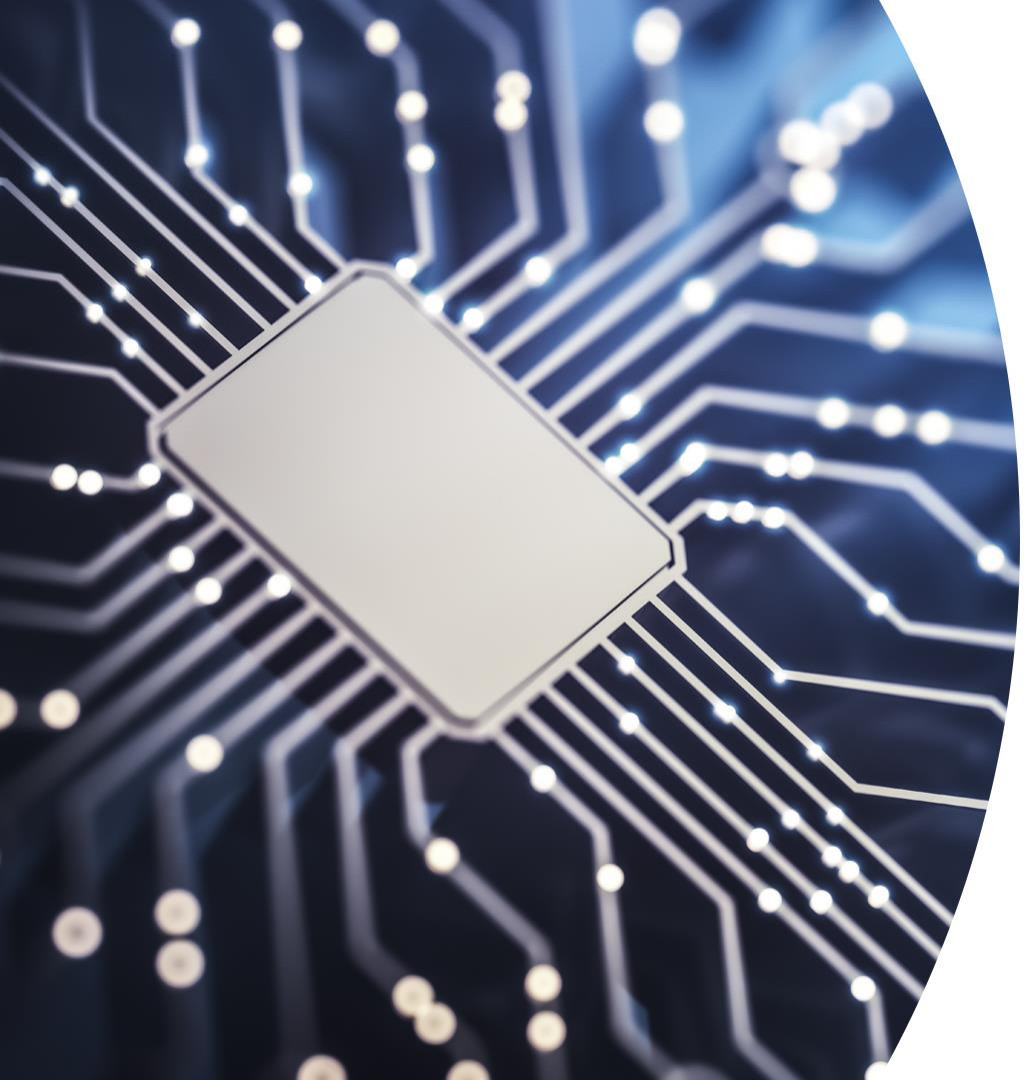
4

СЗИ встроены в процессы самой АСУ ТП



Пример сети Siemens





Задачи, стоящие перед специалистами ИБ АСУ ТП

1. Обеспечить кибербезопасность АСУ ТП
2. Выполнить требования регуляторов
3. Автоматизировать процессы отдела ИБ

INFOWATCH®

InfoWatch ARMA — комплексная система для обеспечения кибербезопасности АСУ ТП

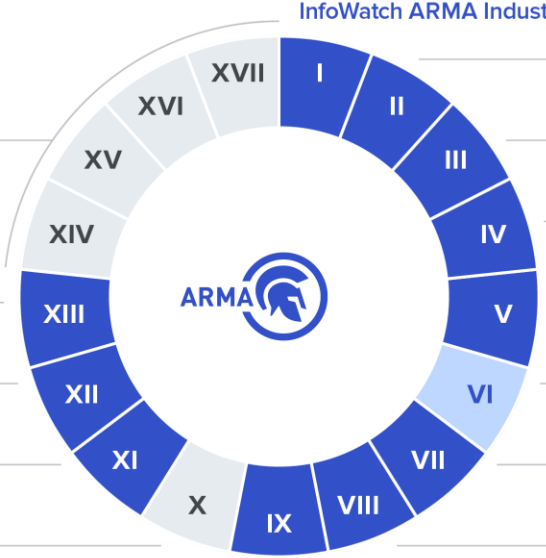
→ Эшелонированная **защита с единым центром управления** системой защиты информации

→ **Инструмент для выполнения до 90% технических требований** приказа ФСТЭК России № 239

→ **Автоматизация процессов отдела ИБ** по реагированию на инциденты

До 90% выполнения технических требований Приказа № 239 ФСТЭК России

INFOWATCH®



Организационные меры

Endpoint
InfoWatch ARMA Industrial Endpoint

Средства управления инцидентами
InfoWatch ARMA Management Console

Endpoint, МЭ
InfoWatch ARMA Industrial Firewall / Industrial Endpoint

Физическая безопасность

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
Q2 2022

СОВ
InfoWatch ARMA Industrial Firewall

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

МЭ
InfoWatch ARMA Industrial Firewall

Получите карту соответствия InfoWatch ARMA группам мер ФСТЭК России

Оставьте запрос на сайте
arma.infowatch.ru

InfoWatch ARMA Industrial Firewall

Защита КИИ промышленных объектов от сетевых атак

arma-firewall.infowatch.ru

Промышленный межсетевой экран нового поколения

- → **Сертификат ФСТЭК РОССИИ** МЭ тип «Д», УД4; СОВ, УД4
- → **Включён в единый реестр российского ПО** Минкомсвязи РФ
- → **Протоколы:** 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 и другие

InfoWatch ARMA Industrial Firewall

Профессионалы доверяют защиту АСУ ТП нашему межсетевому экрану. Почему?

1 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

2 Встроенная система обнаружения и предотвращения вторжений

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

3 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

4 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

Эшелонированная защита. Микросегментация

Зона IT

Уровни 4 и 5 — Корпоративная сеть

IT — OT сегментация

Зона OT

Уровень 3 — Компьютерная сеть (DMZ)

SCADA / DCS

Уровень 2 — Диспетчерского управления

HMI

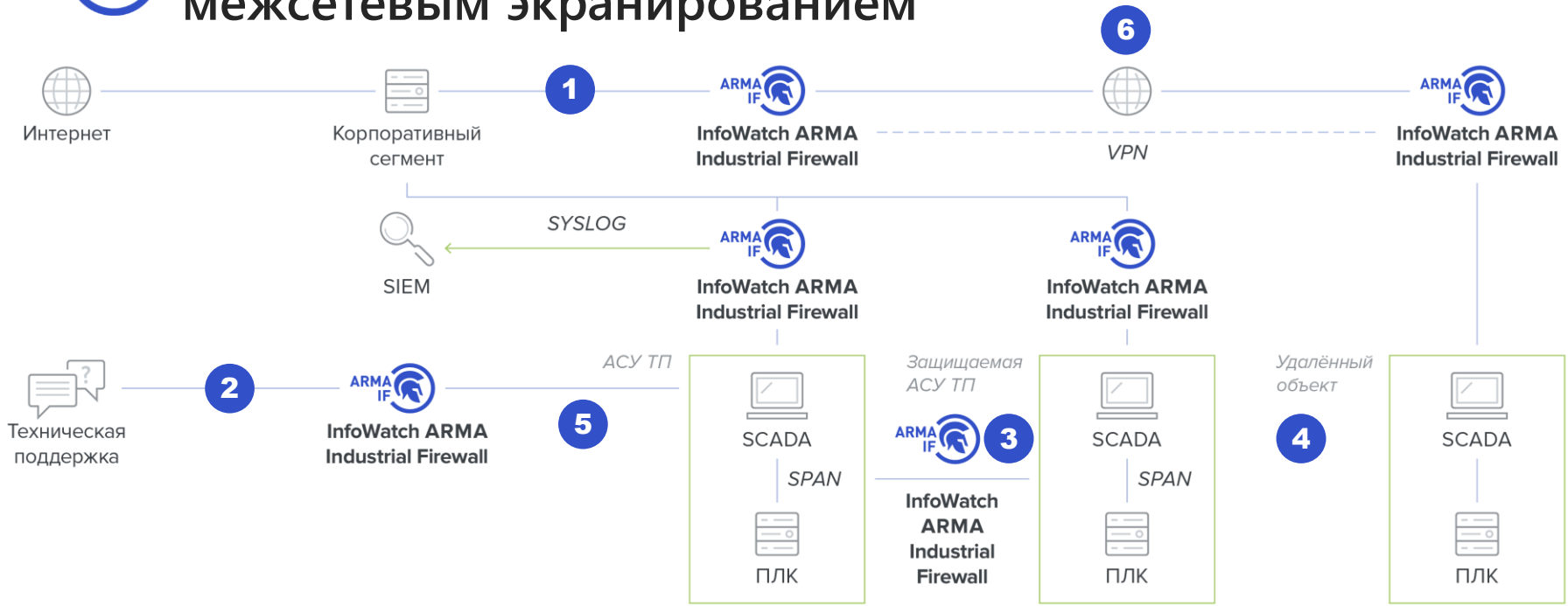
Микросегментация

Уровень 1 — Сетевых контроллеров и исполнительных устройств

PLCs / RTUs

Уровень 0 — Полевой

6 вариантов защиты АСУ ТП межсетевым экранированием



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

InfoWatch ARMA Industrial Endpoint

Создание замкнутой защищённой программной среды

arma-endpoint.infowatch.ru

Защита рабочих станций и серверов АСУ ТП

- → **Контроль целостности файлов** на рабочих станциях и серверах АСУ ТП
- → **Контроль USB** (флешек и других съёмных носителей)
- → **Блокировка недоверенного ПО** на основе белых списков
- → **Антивирусная защита** (Q2 2022)

Проходит сертификацию ФСТЭК России ИТ.САВЗ.Б4.ПЗ; ИТ.САВЗ.В4.ПЗ; ИТ.СКН.П4.ПЗ; УД4. **Включён в единый реестр российского ПО** Минкомсвязи РФ.

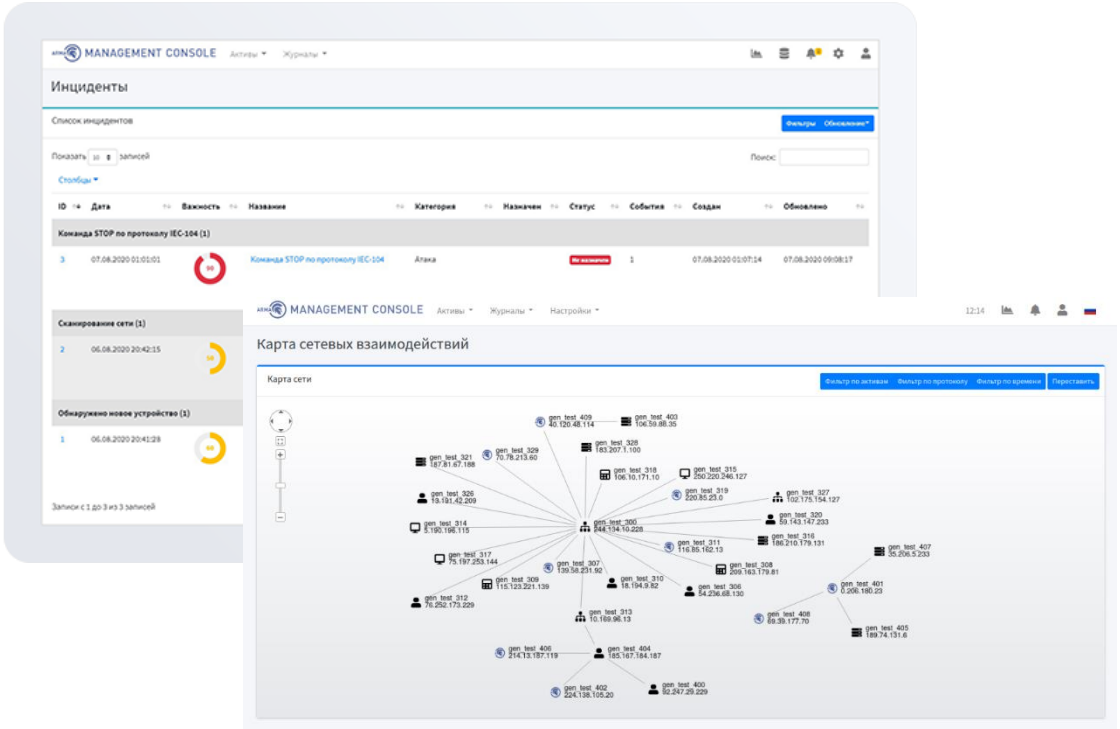
INFOWATCH®

Единый центр управления системой защиты InfoWatch ARMA

→ **Проходит сертификацию ФСТЭК России** ИТ.САВ3.А4.ПЗ; УД4

→ **Включён в единый реестр российского ПО** Минкомсвязи РФ

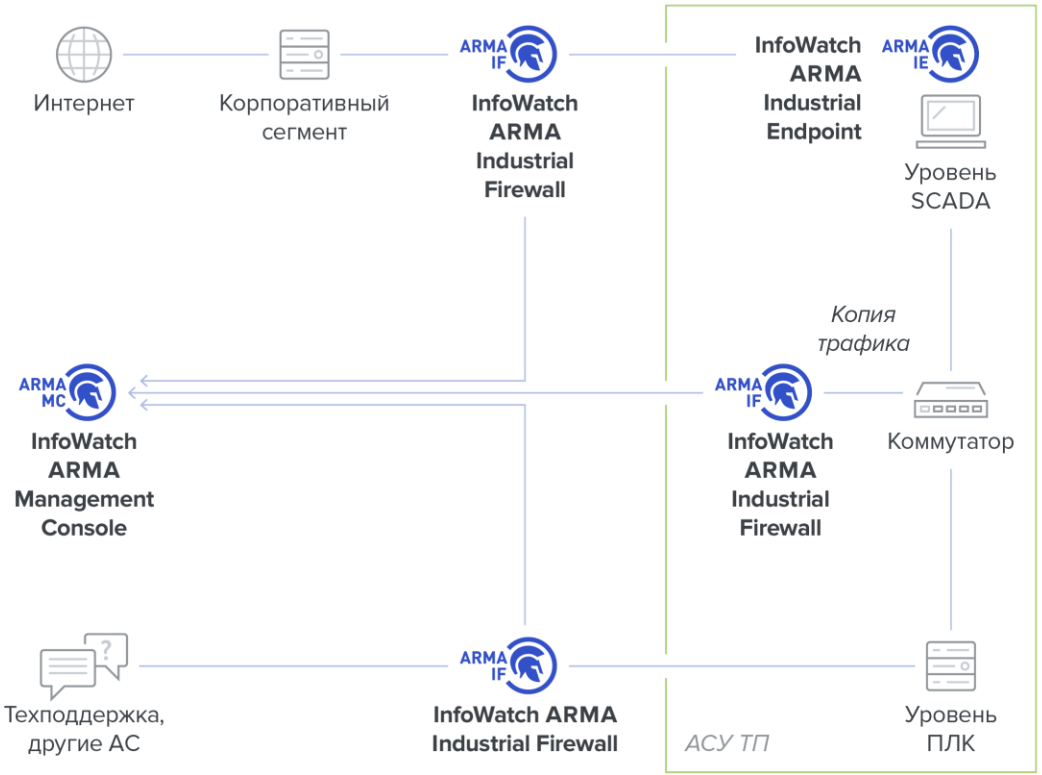
Расследование инцидентов в едином интерфейсе



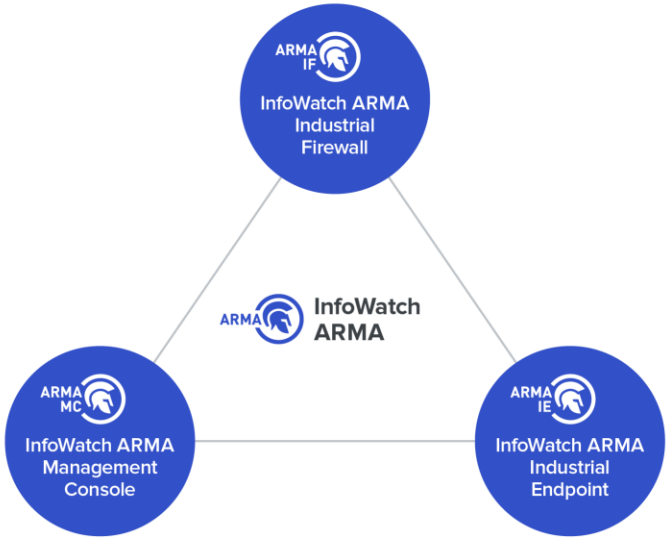
- → **Централизованное управление** продуктами InfoWatch ARMA
- → **Управление инцидентами ИБ** и их расследование
- → **Сбор событий ИБ** и предоставление инцидентов в SOC- и SIEM-системы
- → **Автоматическая реакция** на инциденты
- → **Визуализация сети**

Как автоматически блокируется угроза и её источник

Комплексная система — выгоднее и легче внедрение



Все продукты интегрированы между собой: могут эксплуатироваться как самостоятельные продукты, так и в комплексе.



InfoWatch ARMA 187

Закрытая демонстрация на стенде InfoWatch ARMA

Категорирование объектов КИИ в рамках 187-ФЗ

- → **Единое рабочее пространство** для учёта сведений об объектах КИИ
- → **Автоматизация процесса** категорирования объектов КИИ
- → **Формирование актов** категорирования для ФСТЭК России
- → **Контроль мероприятий** по соответствию требованиям регуляторов

INFOWATCH ARMA

ПРИХОДИТЕ НА СТЕНД INFOWATCH ARMA A50

НАЙДЁМ РЕШЕНИЕ И ПРОВЕДЁМ ДЕМО

Оставьте ваш контакт спикеру или оформите запрос по почте: sales@infowatch.ru

/InfoWatchOut /InfoWatch /InfoWatch