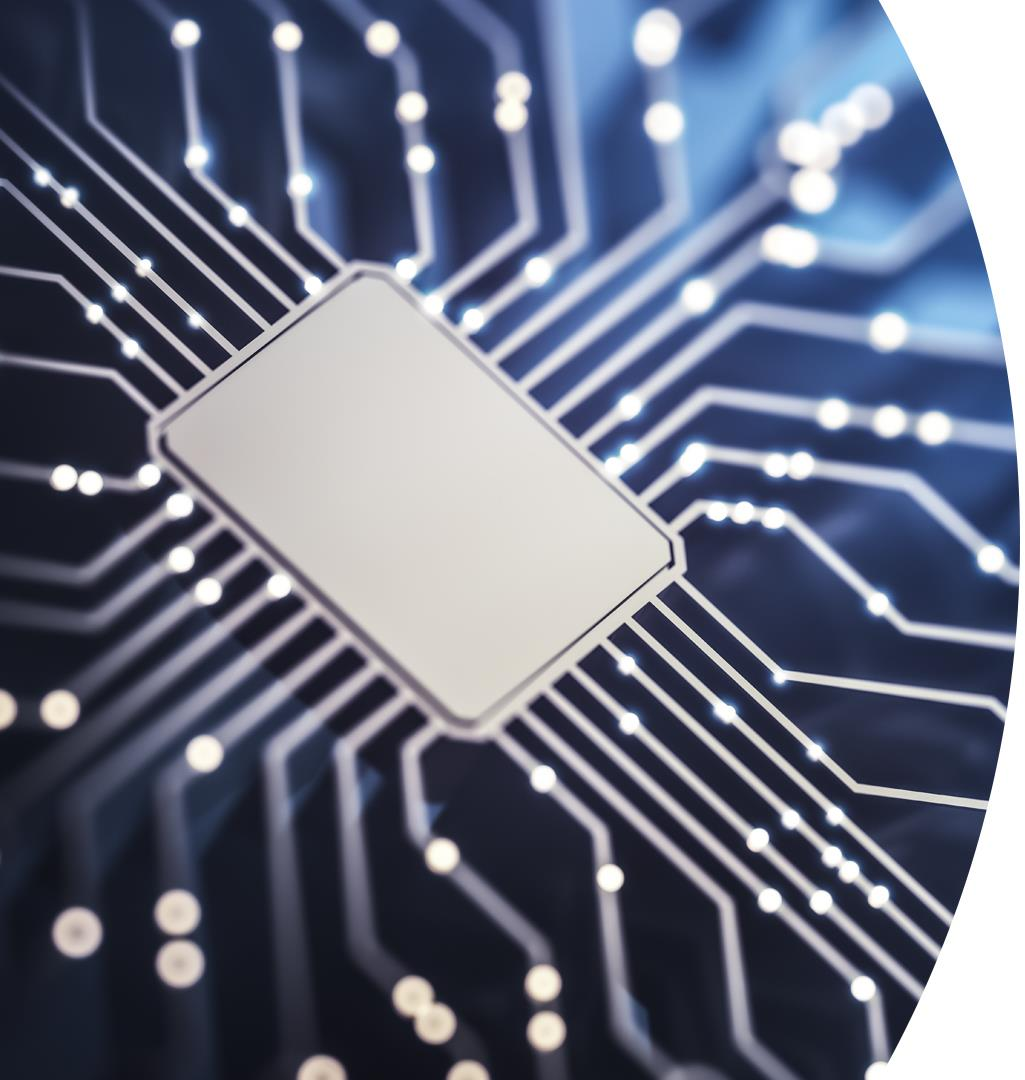
INFOWATCH® ARMA ARMA

КИБЕРБЕЗОПАСНОСТЬ АСУ ТП С СИСТЕМОЙ INFOWATCH ARMA

Создание эшелонированной защиты АСУ ТП от кибератак и выполнение 187-ФЗ

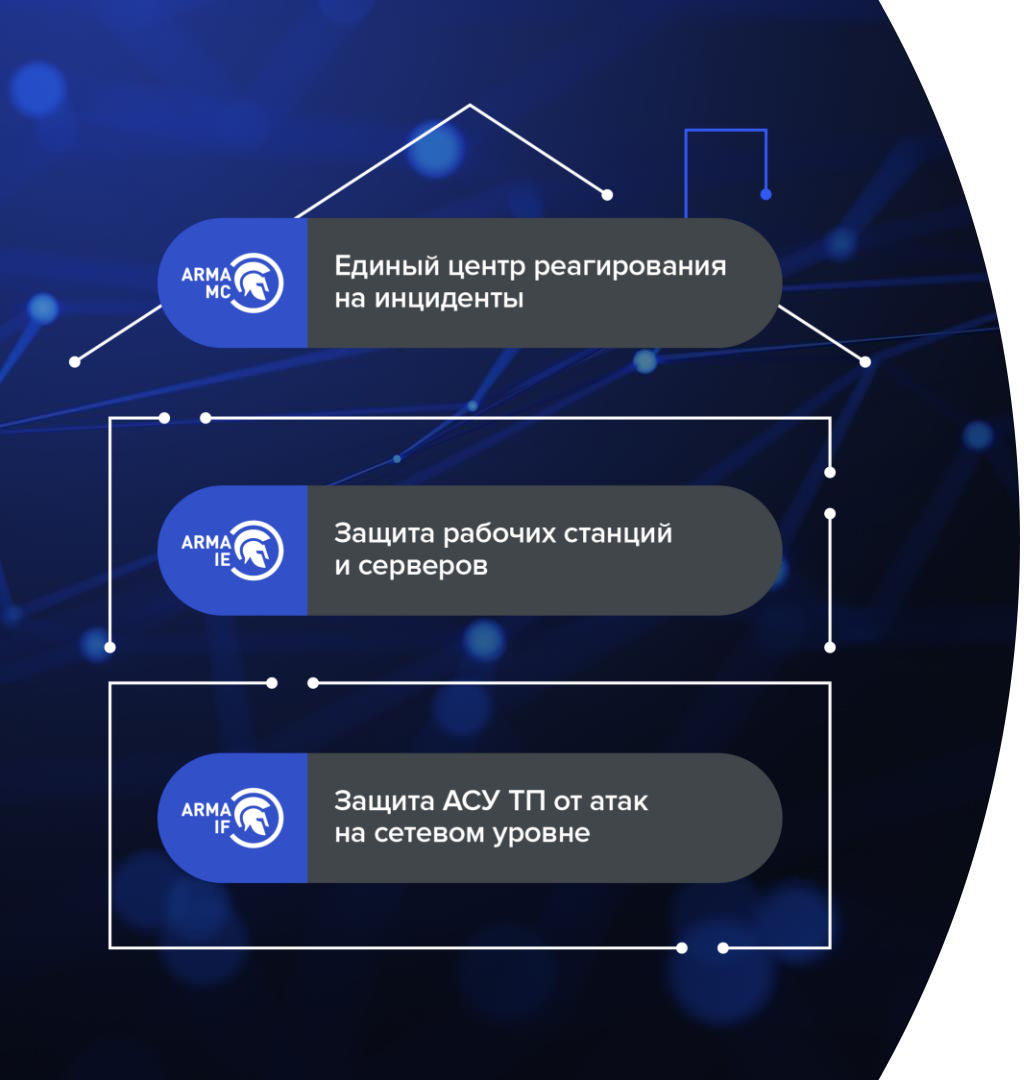
Игорь Душа

Технический директор InfoWatch ARMA



Задачи специалистов ИБ АСУ ТП

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



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

Зрелость систем ИБ АСУ ТП

INFOWATCH®

Уровни зрелости процесса

Зрелость: Низкая → Высокая

0
СЗИ отсутствуют

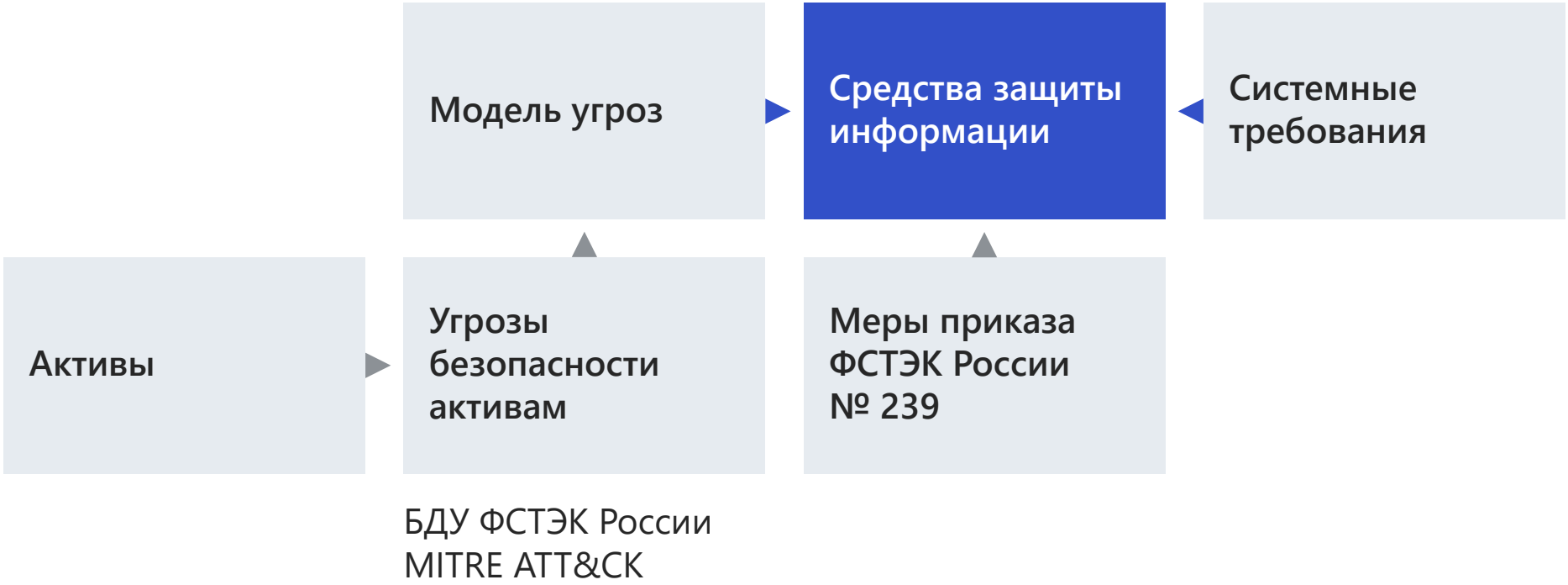
1
Внедрены базовые СЗИ
- Антивирус
- Шлюз на периметре

2
Внедряются спец. 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

Как выбирать средства защиты



Технические нюансы

1	Не потерять техническую поддержку вендора АСУ ТП
2	Ложные срабатывания и большой поток информации
3	Отсутствие ресурсов для управления средствами ИБ
4	Отсутствие выстроенных процессов ИБ
5	Долгая реакция на инциденты или её отсутствие
6	Отсутствие подробной информации для реакции на инциденты или их расследования
7	Разрозненность средств защиты

Что очевидно и на первый взгляд не видно

INFOWATCH®

1. **Много средств** защиты на малом сегменте АСУ ТП — **трудоёмко и затратно**
2. Постоянный мониторинг СЗИ требует много времени. **Времени — не хватает**
3. **Основная задача** — снизить возможность реализации атаки
4. **Атака реализовалась?** Срочно **локализовать** и предотвратить распространение!

Что же делать?

1	Для максимального препятствия атаке **нужно создать замкнутую защищённую среду** с точки зрения информационных потоков и политик ИБ
2	**Уменьшат ложные срабатывания специализированные (промышленные) средства защиты** информации, учитывающие специфику АСУ ТП
3	Средств защиты информации на промышленных объектах должно быть столько, чтобы **обеспечить выполнение Приказов** ФСТЭК России **и на их обслуживание хватило ресурсов штата** ИБ АСУ ТП
4	Система защиты информации **должна быть интегрирована, настраиваема** под предприятие и помогать выстраивать процесс ИБ и реагирования на инциденты (в том числе диспетчерского)

4 концепции ИБ АСУ ТП

→ Эшелонированная защита информации

Даст несколько попыток на то, чтобы прервать атаку, повысит вероятность обнаружения, позволит локализовать распространение инцидента.

→ Замкнутая защищённая среда

Меньше возможностей злоумышленника — сложнее проведение атаки.

→ Полная видимость происходящего

Важно: с возможностью организовать взаимодействие между службой ИБ АСУ ТП и диспетчерами и настройкой понятных инструкций в системе!

→ Автоматизация

Автоматизация работы с инцидентами, интеграция с АСУ

Эшелонированная защита
Микросегментация

Зона IT

Уровни 4 и 5	Корпоративная сеть	

IT — OT сегментация

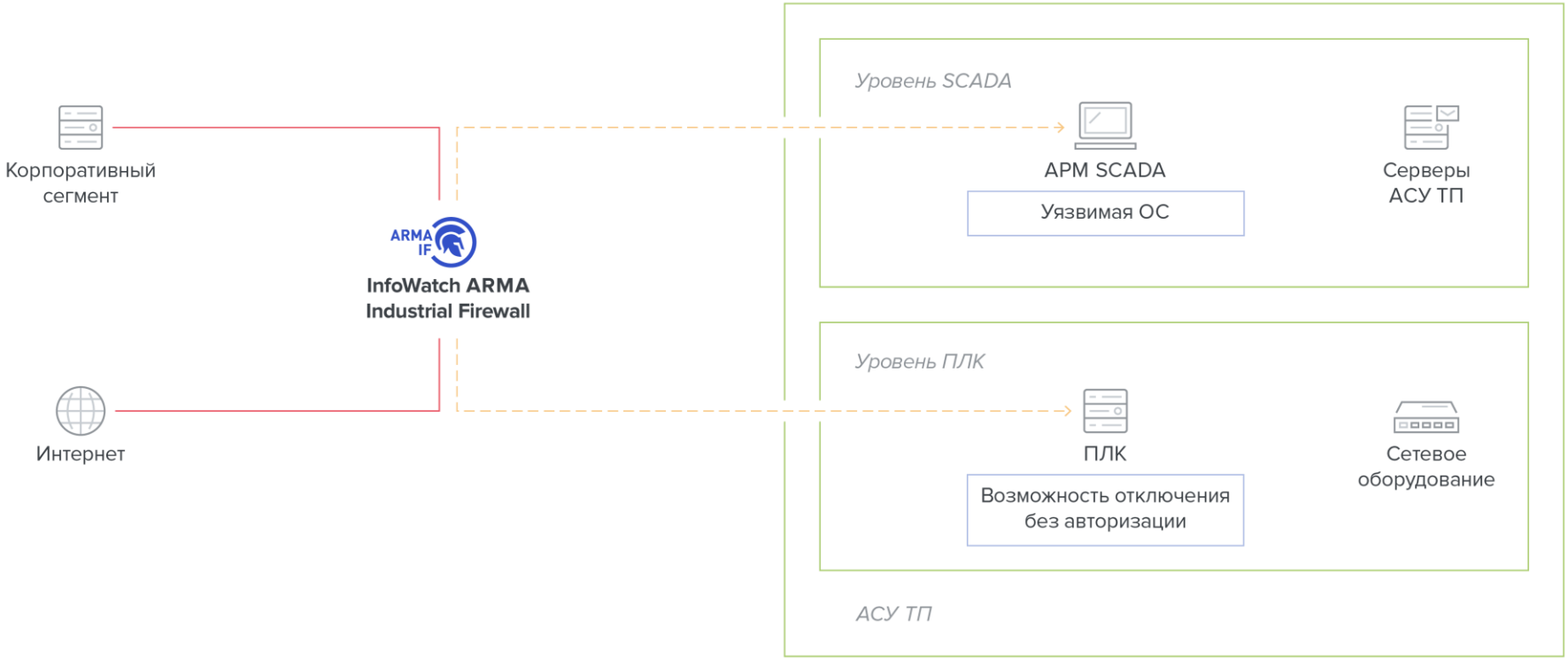
Зона OT

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	

Эшелонированная защита
Виртуальный патчинг



Замкнутая программная среда. Ограничения и ещё раз ограничения

Замкнутая среда в АСУ ТП — лучший вариант:

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

Почему важна «видимость событий»

Слабость периметра

100% всех киберпреступников получают доступ прямо из интернета.

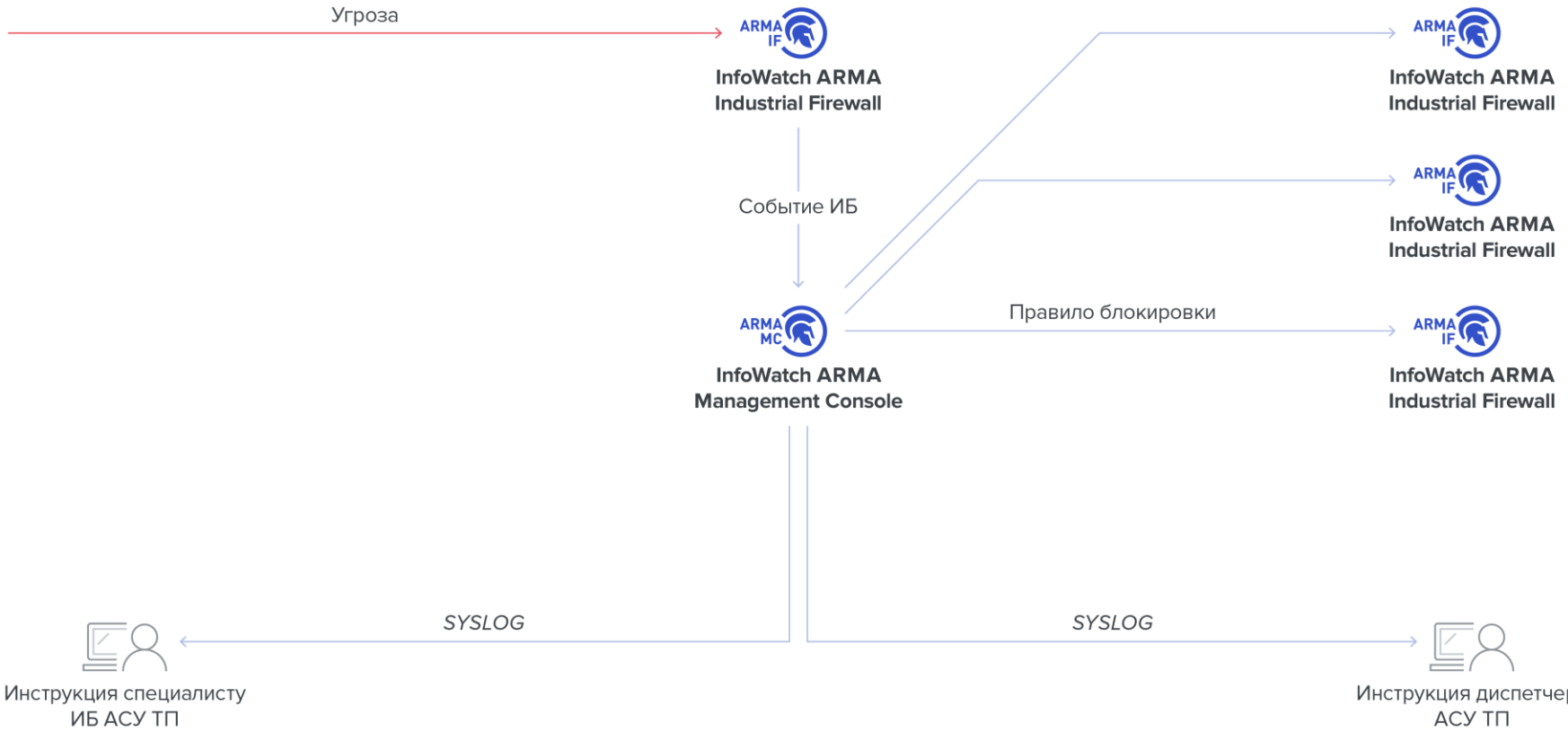
Ложные срабатывания

В 51% случаев выявленные диаграммы существующей архитектуры отсутствовали или представляли ложную информацию.

Слабая видимость сети

Снижение нагрузки на штат ИБ при реагировании на инциденты 0% — такой показатель можно обеспечить журналированием или пассивным мониторингом промышленных сетей. Каждое реагирование — это получение журналов вручную и распределённый анализ.

Автоматизация реакции на инциденты



Решение в объединении

XDR (eXtended Detection and Response) — платформа обнаружения и реагирования на угрозы с обширным покрытием:

Анализ на конечных устройствах

Сбор данных телеметрии, сведений о поведении пользователя и программ и др.

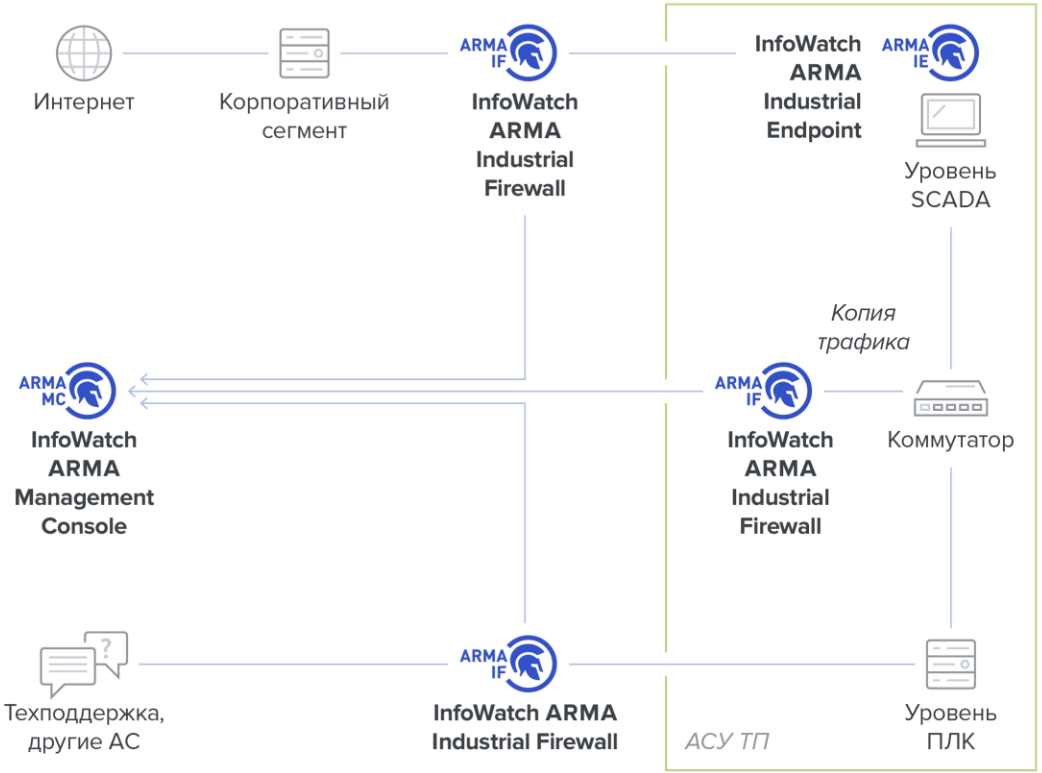
Анализ сетевого трафика

Всех устройств в сети, в т. ч. IoT / IIoT, встраиваемых устройств и т. д.

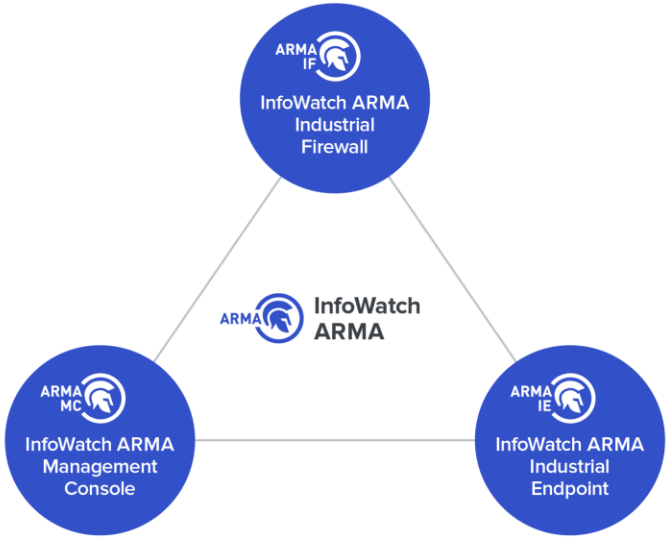
Централизованное управление событиями и инцидентами ИБ, формирование реакции

- Анализ событий ИБ в сети **как единое целое**
- **Несколько сообщений** об атаках **вместо тысяч** предупреждений
- Можно **отследить всю цепочку атаки:** от вредоносных действий до заражённых устройств

Комплексная система — выгоднее и легче внедрение



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



Возможность встроить в текущую инфраструктуру

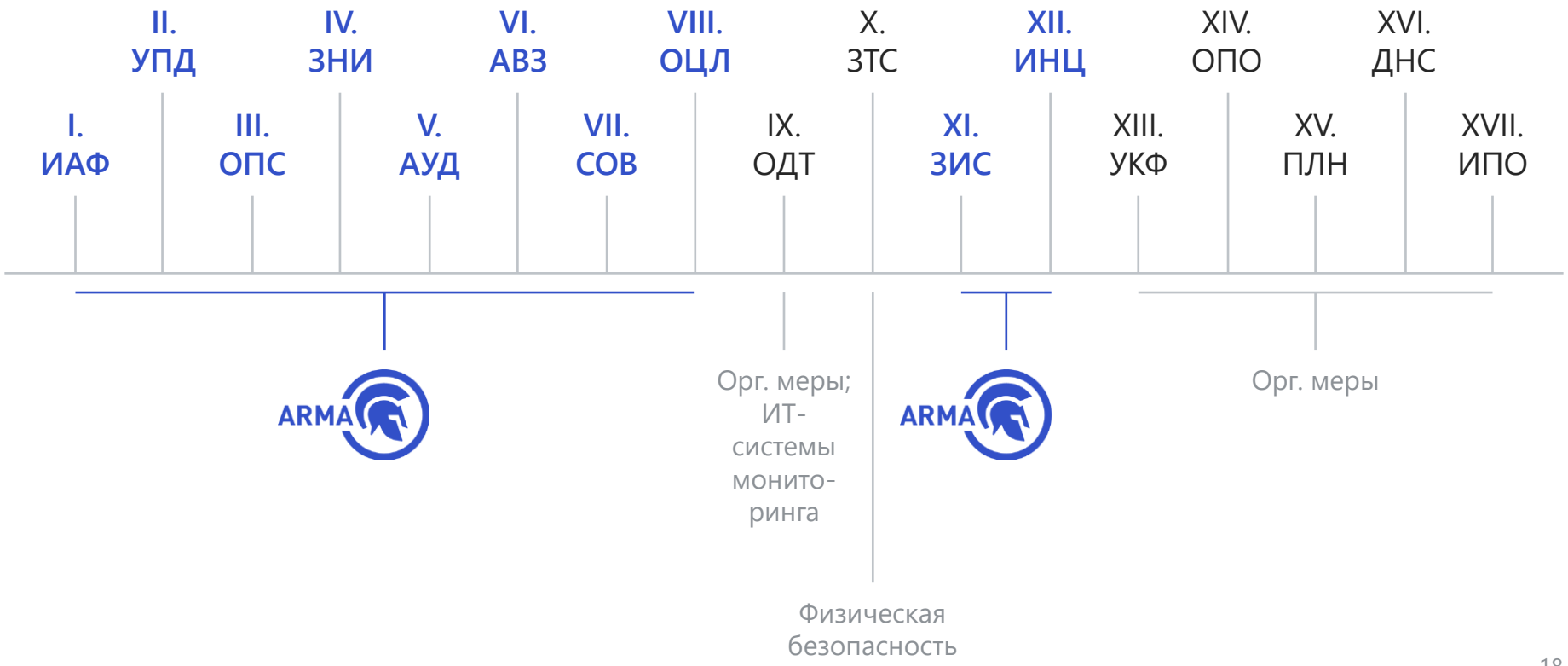
INFOWATCH®

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 для выполнения Приказа № 239 ФСТЭК России



arma-firewall.infowatch.ru

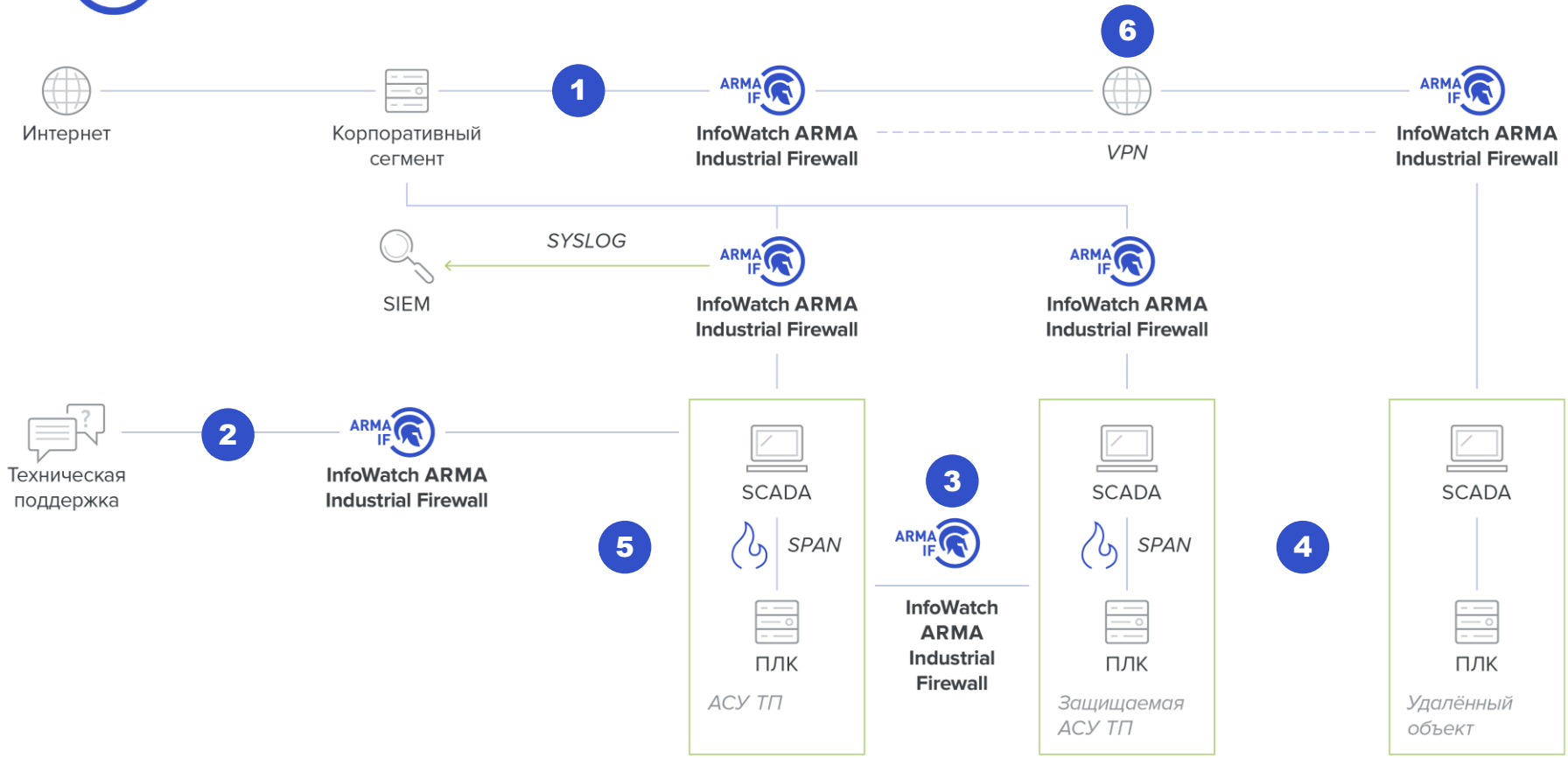
Промышленный межсетевой экран нового поколения

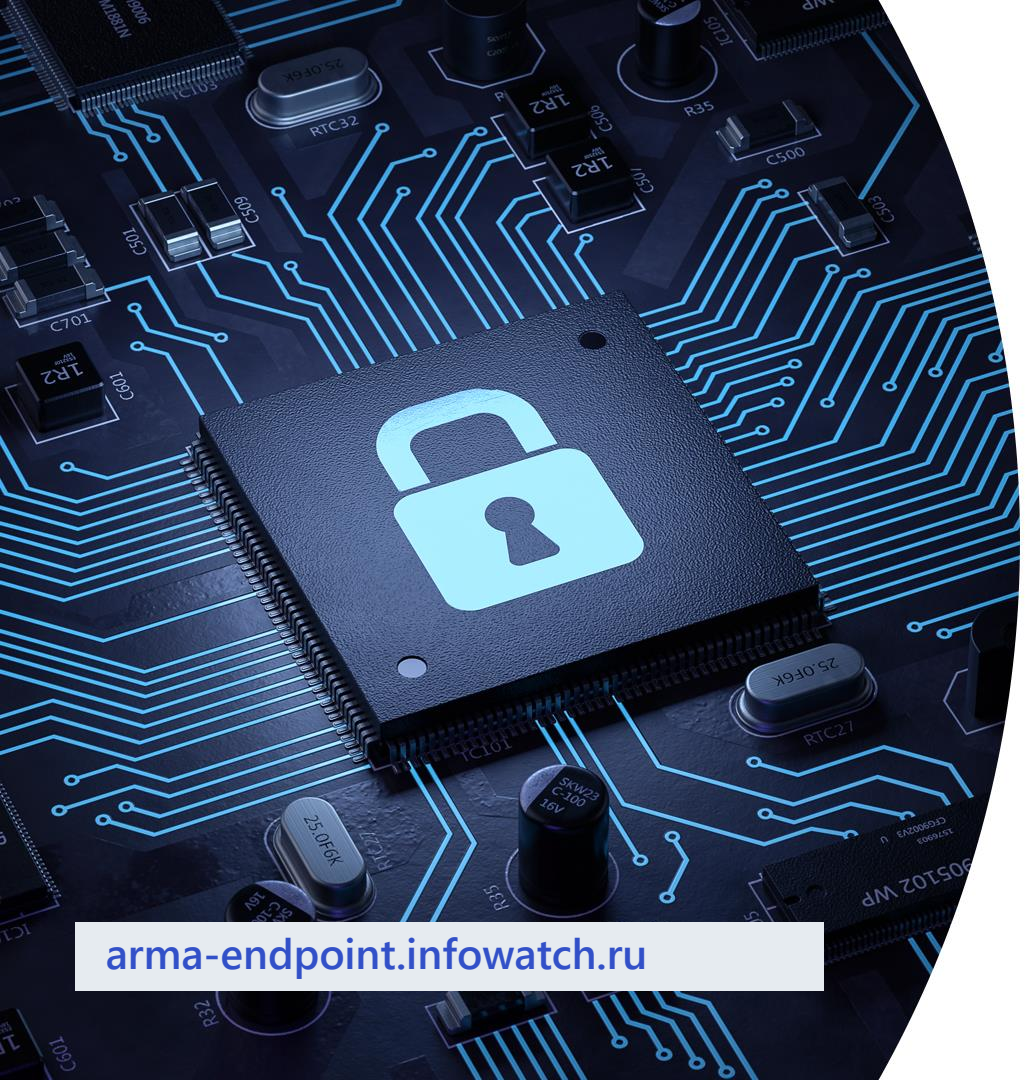
InfoWatch ARMA Industrial Firewall

Защита КИИ промышленных объектов от сетевых атак

- Проходит сертификацию по 4 классу защиты тип «Д»
- Включён в единый реестр российского ПО Минкомсвязи РФ

Сегментация промышленной сети





INFOWATCH®

Защита рабочих станций и серверов АСУ ТП

ARMA IE

InfoWatch ARMA Industrial Endpoint

Создание замкнутой защищённой среды

arma-endpoint.infowatch.ru

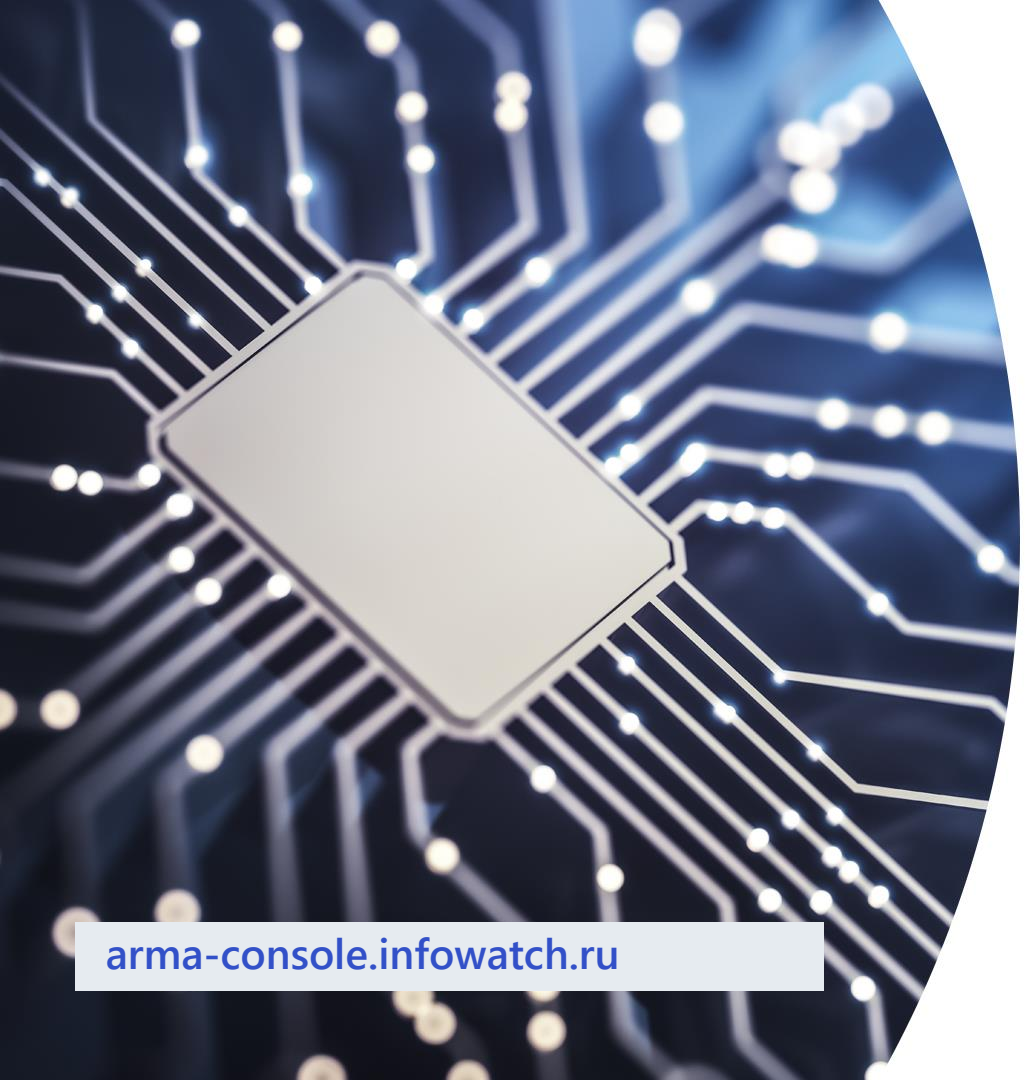
NEW Новый продукт

INFOWATCH®

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** любого недоверенного **ПО**

arma-endpoint.infowatch.ru



INFOWATCH®

Единый центр управления системой защиты InfoWatch ARMA

InfoWatch ARMA Management Console

Централизованное обновление и управление конфигурациями

arma-console.infowatch.ru

NEW Новый продукт

Единый центр управления системой защиты InfoWatch ARMA

- **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**

INFOWATCH® ARMA ARMA

КАКИЕ ЗАДАЧИ СТОЯТ ПЕРЕД ВАМИ?

НАЙДЁМ РЕШЕНИЕ И ПРОВЕДЁМ ДЕМО НА СТЕНДЕ INFOWATCH A23

/InfoWatchOut /InfoWatch /infowatchnews

arma.infowatch.ru