INFOWATCH® ARMA ARMA

ЭШЕЛОНИРОВАННАЯ ЗАЩИТА ИНФОРМАЦИИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ С СИСТЕМОЙ INFOWATCH ARMA

Игорь Душа

Директор по развитию продуктов для защиты информации в АСУ ТП, InfoWatch ARMA

I полугодие 2020: поток атак по всему миру

Январь 2020	**Атака на Picanol Group Бельгии, Румынии, Китае.** Нарушена работа заводов, ткацких станков, 2300 сотрудников — без работы
Февраль 2020	**Целевые атаки на промышленность Азербайджана.** Троянец удалённого доступа PoetRAT. Цель — SCADA-системы, связанные с ветряными турбинами
Апрель 2020	**Атака на португальскую энергетическую компанию EDP.** Кража конфиденциальной информации о счетах, договорах, транзакциях, клиентах, партнёрах. Шифровальщик Ragnar Locker. Выкуп: 1580 биткойнов ($10,9 млн)
Май 2020	**Атака на металлургический концерн BlueScope.** Пострадали производственные операции в Австралии
Июнь 2020	**Атака на бразильскую энергетическую компанию Light S.A.** Вирус Sodinikibi зашифровал системные файлы. За возврат данных — $7 млн в криптовалюте Monero, потом сумму удвоили

Причины и последствия сбоев на промышленных объектах

INFOWATCH®

Причины провалов работы ИС на производственных объектах и на объектах КИИ

Атаки внешних злоумышленников	Удалённый контроль со стороны производителя	Отказы ИТ-систем
ГЭС, ТЭЦ — остановка генерации энергии, жертвы, экономический ущерб. АСУ ТП в промышленности — аварии / катастрофы, ЧС. Системы связи, власть — потеря управления	Отключение оборудования «по щелчку» из-за несоблюдения условий эксплуатации, отказа в гарантийном обслуживании, санкций	Сбои в работе производственных систем, простои, убытки, аварии оборудования — вплоть до угрозы жизни (шахты, операционные)

Найдите себя. Что волнует сегодня

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)

«3 кита» ИБ промышленных объектов

Соответствие требованиям регуляторов

- **Выполнение требований** ФЗ-187 «О безопасности КИИ», Приказов ФСТЭК России № 239 и № 31. **InfoWatch ARMA позволяет выполнить до 90% техтребований**

Эшелонированная защита информации

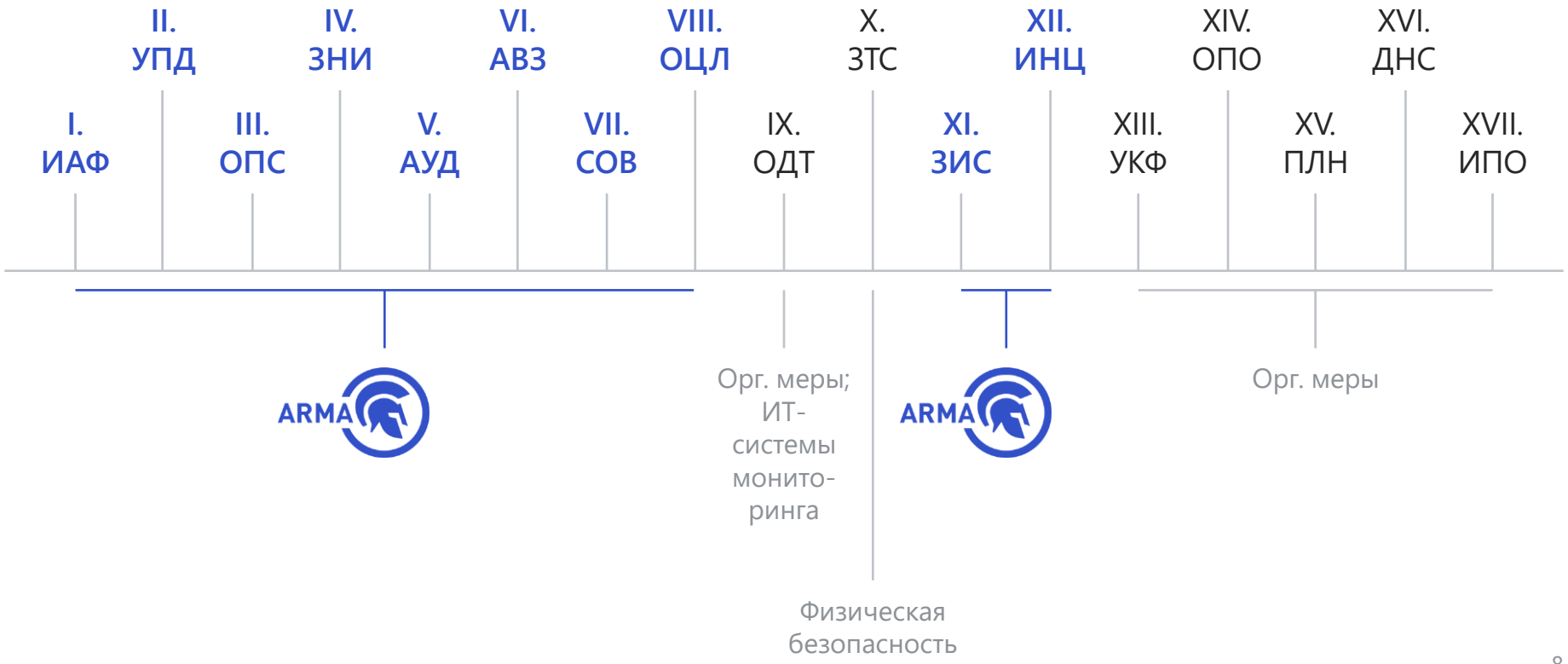
- **Важно: с уменьшением поверхности атаки** за счёт создания замкнутой среды и единым центром управления!

Промышленный межсетевой экран нового поколения + **Защита рабочих станций и серверов SCADA**

Полная видимость происходящего с автоматическим реагированием

- **Важно: с глубокой инспекцией промышленных протоколов** и настройкой автоматического реагирования на инцидент (по заранее согласованным правилам)!

Группы мер ФСТЭК России, которые позволяет закрыть InfoWatch ARMA



Эшелонированная защита

Эшелонированная защита (defense in depth) — наличие множественной защиты, в частности в виде уровней, с целью предотвращения или хотя бы сдерживания атаки.

Примечание. **Эшелонированная защита предполагает наличие уровней защиты и обнаружения угроз даже на обособленных системах и обладает следующими признаками:**

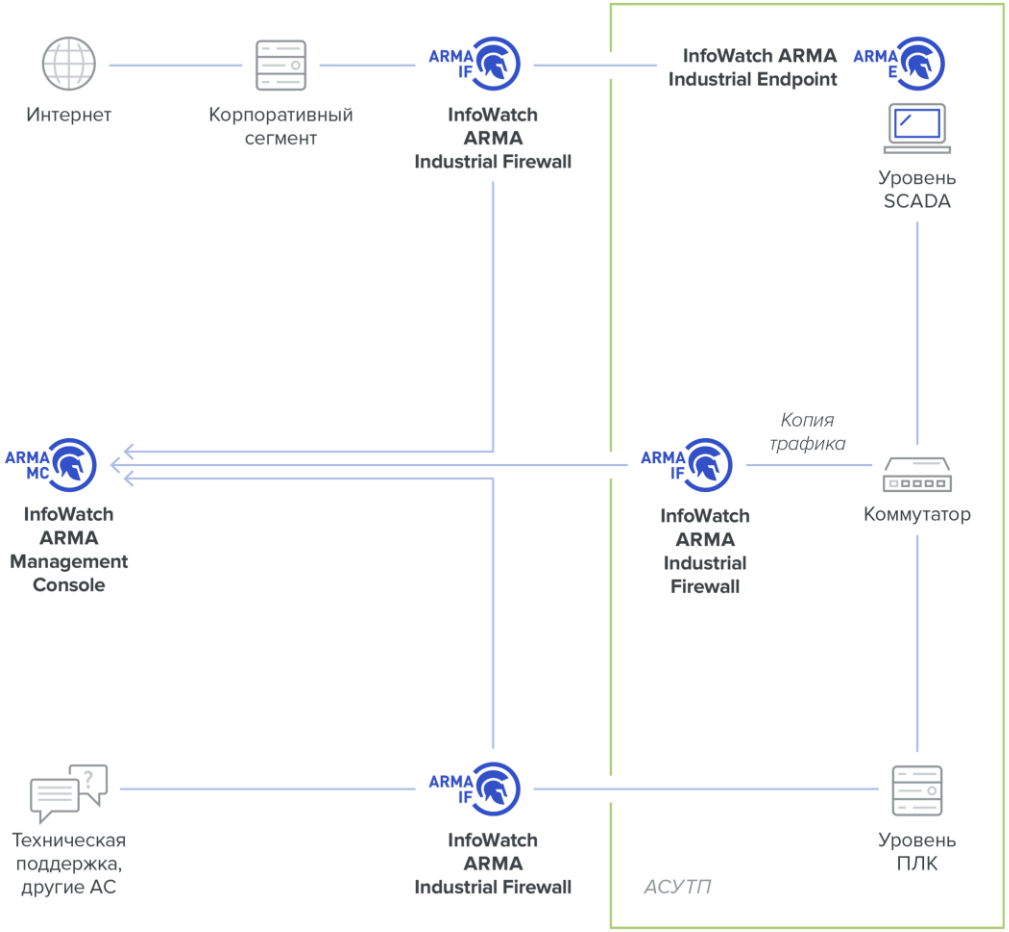
- Злоумышленники сталкиваются с проблемой незаметного прохождения или обхождения каждого уровня
- Дефект на одном уровне может быть ослаблен возможностями других уровней
- Безопасность системы сводится к набору уровней, которые определяют также общую безопасность сети

ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009

Эшелонированная защита

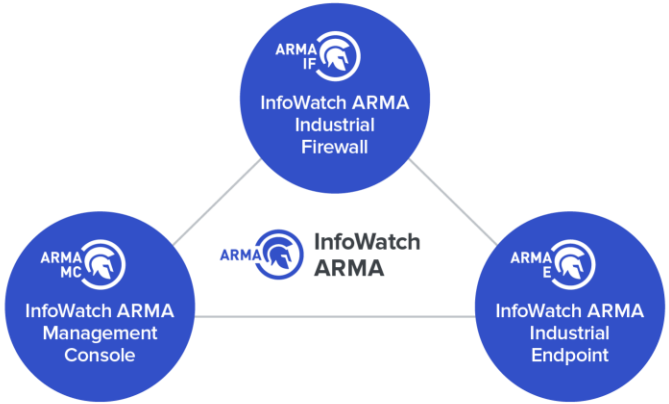
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+
ЗИС.3	**Эшелонированная защита** информационной (автоматизированной) системы	+	+	+
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+
ЗИС.5	Организация демилитаризованной зоны	+	+	+
ЗИС.6	Управление сетевыми потоками	+	+	+

Приказ ФСТЭК России №239 от 25 декабря 2017



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

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

InfoWatch ARMA Industrial Firewall
IT — OT сегментация и 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

InfoWatch ARMA Industrial Firewall

Профессионалы доверяют защиту АСУ ТП нашему межсетевому экрану. Почему?

1	Глубокая инспекция промышленных протоколов	2	Встроенная система обнаружения вторжений (СОВ)
3	Межсетевое экранирование для промышленных объектов	4	Безопасное удалённое подключение

InfoWatch ARMA Industrial Firewall
Глубокая инспекция промышленных протоколов до уровня команд и их значений

Значительно повышает видимость промышленной сети и позволяет создавать уникальные политики безопасности благодаря микросегментации.

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

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

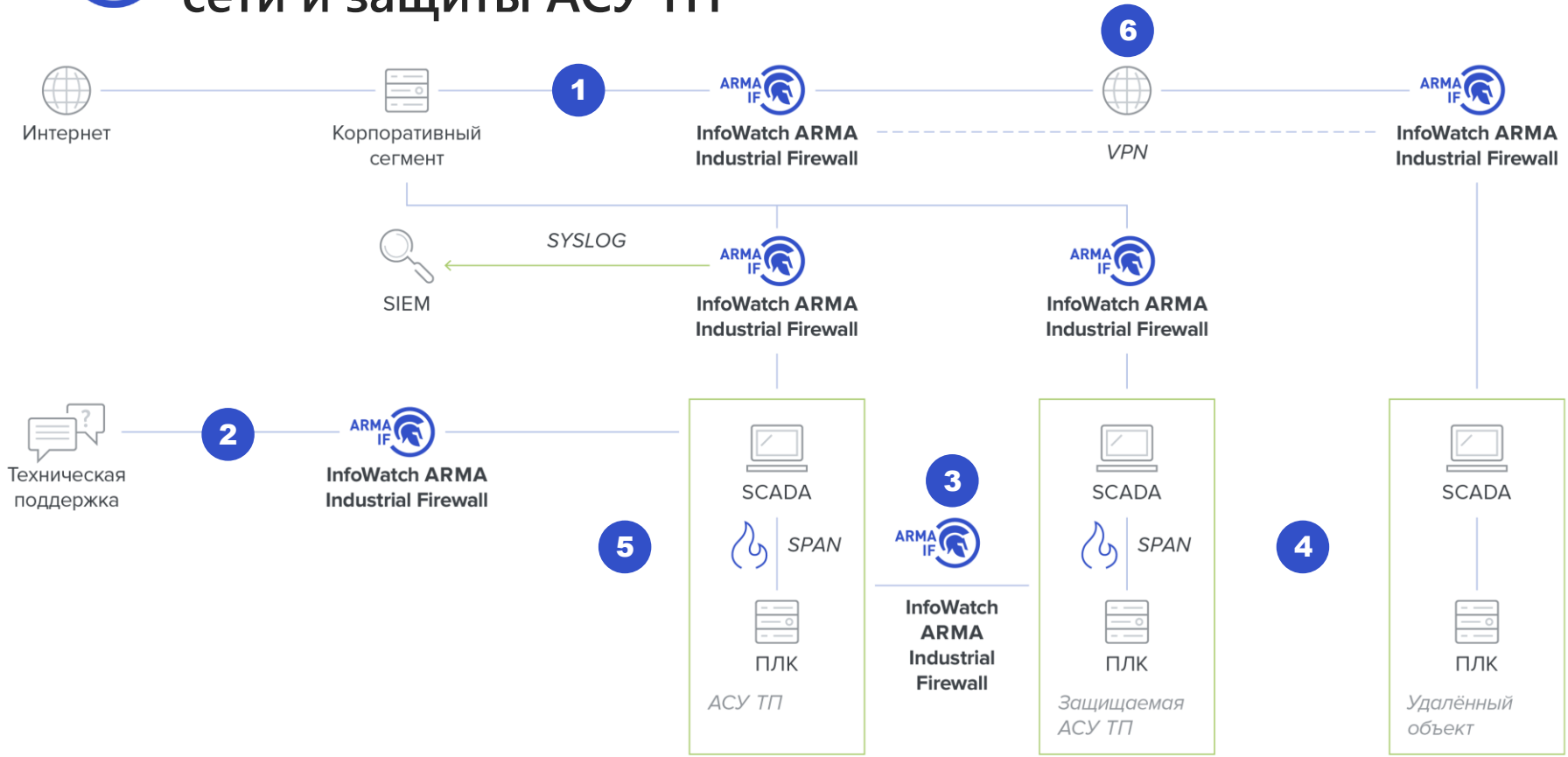
- **Содержит базу решающих правил СОВ для АСУ ТП, которая обновляется ежедневно!**

  Можно самостоятельно дополнять предустановленную базу СОВ собственными пользовательскими правилами для максимальной защиты конкретных АСУ ТП

- **Позволяет заблокировать угрозу и её источник в автоматическом режиме**

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

6 вариантов сегментации промышленной сети и защиты АСУ ТП



Защита рабочих станций и серверов АСУ ТП

InfoWatch ARMA Industrial Endpoint

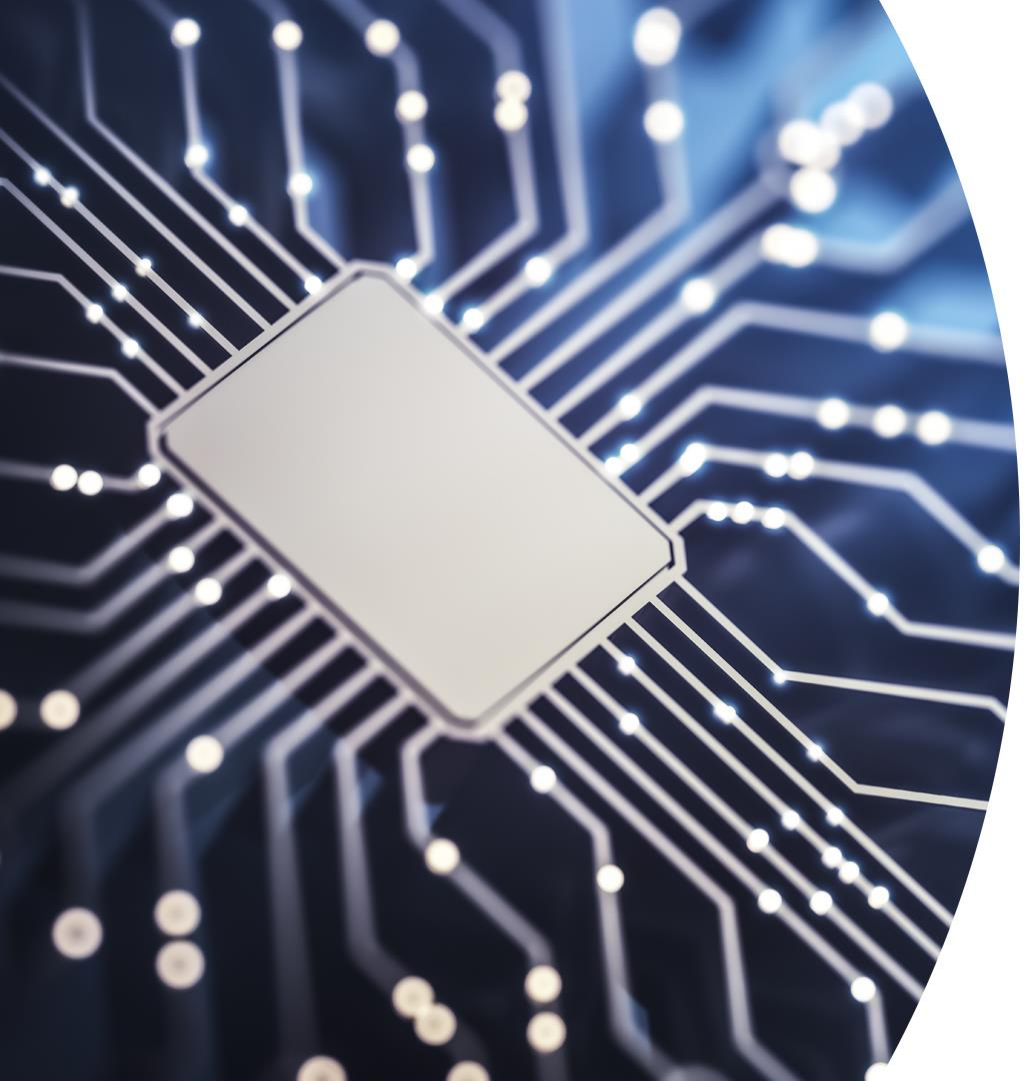
Создание замкнутой защищённой среды

NEW Новый продукт

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 **по белому списку**

arma-endpoint.infowatch.ru



Единый центр управления системой защиты InfoWatch ARMA

InfoWatch ARMA Management Console

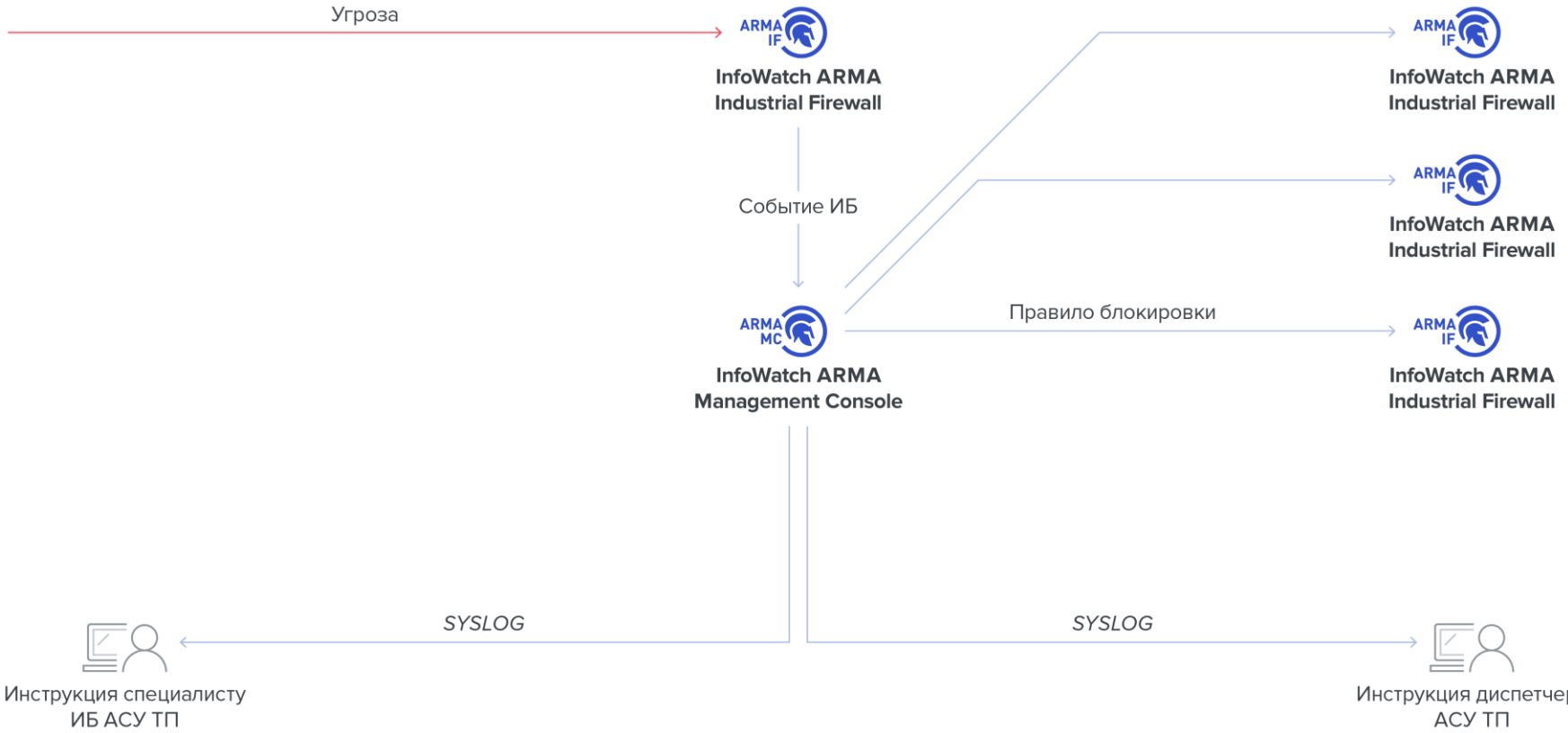
Централизованное обновление и управление конфигурациями

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**

Автоматизация реакции на инциденты



Преимущества
InfoWatch ARMA Management Console

1

Снижает нагрузку на штат ИБ АСУ ТП

Снижает количество ложных срабатываний, общую нагрузку на штат, позволяет автоматически заблокировать источник угрозы, информируя специалистов об инциденте

2

Позволяет настраивать индивидуальные сценария реагирования

С помощью конструктора правил реагирования. Персональные инструкции по решению и взаимодействию специалистов между собой можно создать для любого типа инцидентов

3

Позволяет автоматизировать работу с инцидентами

Можно настроить индивидуальную автоматическую реакцию на инцидент из системы InfoWatch ARMA

INFOWATCH® ARMA ARMA

Хотите провести полный тест-драйв InfoWatch ARMA?

Оформите заявку на сайте
arma.infowatch.ru

/InfoWatchOut /InfoWatch /infowatchnews