INFOWATCH® ARMA ARMA

Стратегия и тактика перехода на отечественные СЗИ

Стаховский Николай

Менеджер по техническому сопровождению продаж InfoWatch.

03.06.2022

Факторы, которые формируют стратегию ИБ АСУ ТП

→ **Критический уровень угрозы кибератак на РФ**

Официальное письмо НКЦКИ

→ **Уход иностранных вендоров**

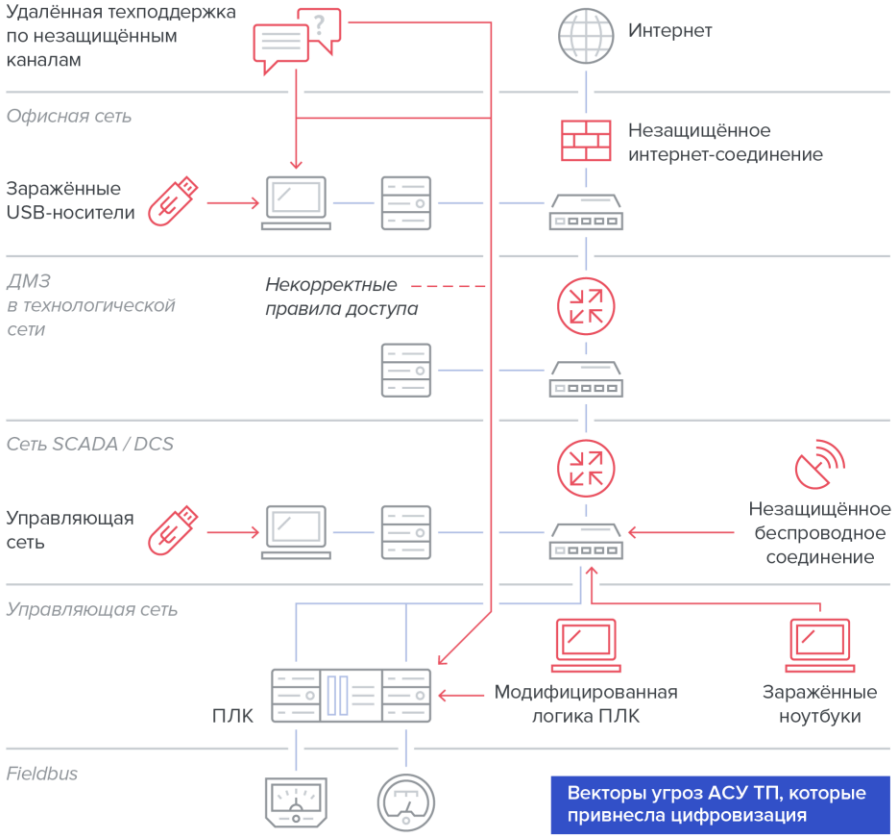
→ **Указ Президента о запрете зарубежного ПО в КИИ** (№166 от 30.03.2022)

Первый шаг. Принять неизбежность того, что отечественным СЗИ – быть.

Тактические задачи, которые стоят сейчас

1	**Замена иностранного оборудования и ПО. Обеспечение их независимой работы**
2	Обеспечение необходимого аппаратного обеспечения или виртуальных мощностей
3	Перенос политик безопасности для нового ПО
4	Выполнение первоочередных мер по защите информации

Формулируем требования исходя из инфраструктуры



→ **Векторы угроз не меняются** уже на протяжении нескольких лет

→ **Сейчас важно защищать,** а не наблюдать

- Мониторинг только дополнительно загружает специалистов
- Нужно максимально уменьшить поверхность атаки прямо сейчас

Первоочередные меры*. Общие

1	Исключение автоматического обновления посредством сети «Интернет»
2	Установка актуальных баз данных САВЗ и решающих правил СОВ у вендора СЗИ
3	Анализ и устранение уязвимостей узлов, являющихся точками проникновения (например, с помощью ScanOVAL)
4	Провести инвентаризацию сервисов и служб, отключить неиспользуемые

*На основе выступления представителя ФСТЭК России на конференции ИБ АСУ ТП КВО 2022

Меры для сетевые средства.

1	Настройка МЭ на блокировку «белым списком», блокировка входящего трафика с зарубежных IP-адресов, из Tor, отключение неиспользуемых портов
2	Ограничить количество подключений к информационной инфраструктуре с каждого отдельного IP адреса
3	Активировать дополнительные функции защиты (в т.ч. DPI и потоковый антивирус) на сетевых средствах защиты информации
4	Ограничить возможности удаленного управления прикладным и системным ПО через сети общего пользования

*На основе выступления представителя ФСТЭК России на конференции ИБ АСУ ТП КВО 2022

InfoWatch ARMA Industrial Firewall

Защита КИИ промышленных объектов от сетевых атак

arma-firewall.infowatch.ru

Промышленный межсетевой экран нового поколения

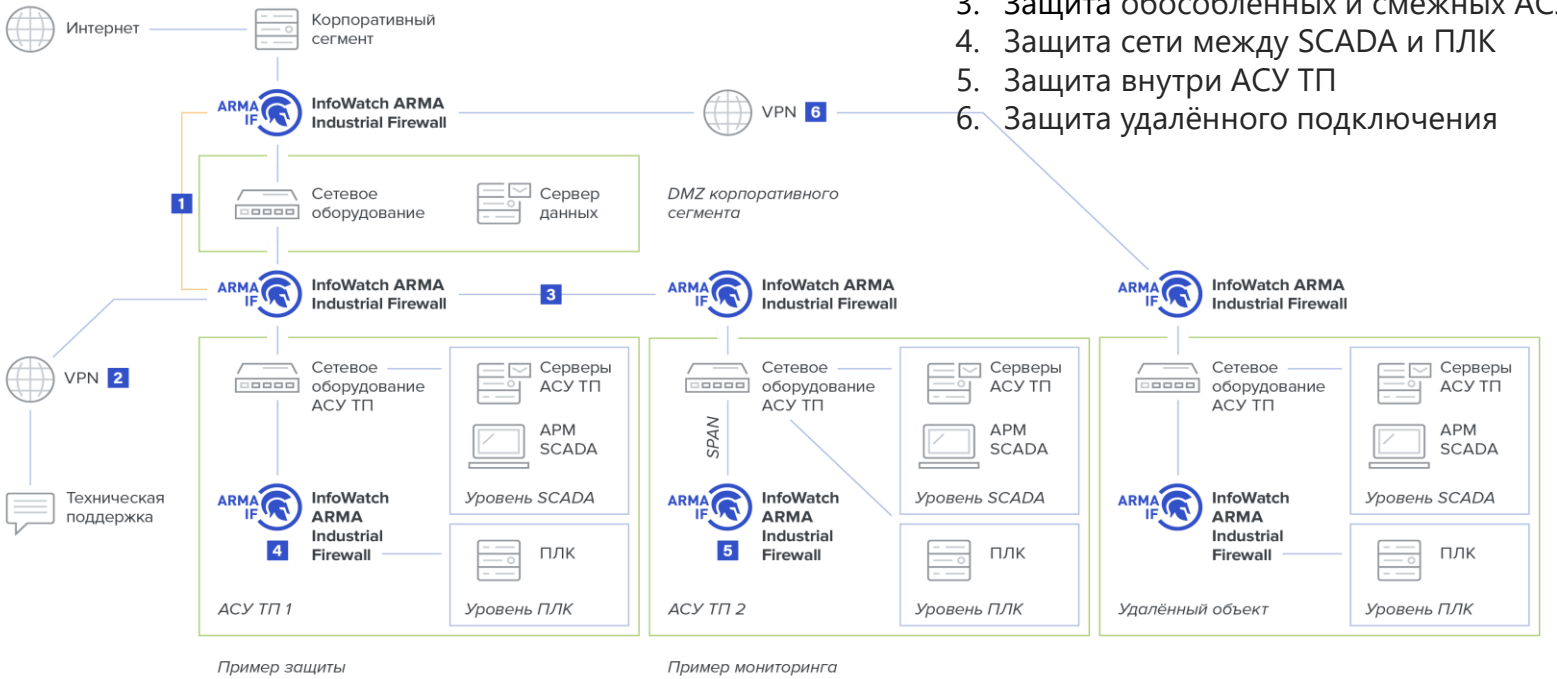
InfoWatch ARMA Industrial Firewall

Защита КИИ промышленных объектов от сетевых атак

- Имеет сертификат ФСТЭК России по 4 классу защиты, тип «Д»
- Включён в единый реестр российского ПО Минкомсвязи РФ

6 вариантов сегментации промышленной сети и защиты АСУ ТП

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



Меры для АРМ и серверов.

1	Исключить использование ПО, не требуемого для выполнения должностных обязанностей
2	Контроль/запрет подключения неучтенных съемных носителей и мобильных устройств
3	Исключить применение систем удаленного доступа, удалить их, если они используются в инфраструктуре
4	Ограничить использование личных СВТ, модемов, накопителей и обновить правила безопасного использования таких средств

*На основе выступления представителя ФСТЭК России на конференции ИБ АСУ ТП КВО 2022

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**

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.

Меры по мониторингу на инциденты

1	Организовать анализ критичных событий безопасности
2	Организовать мониторинг информационной безопасности объектов информационной инфраструктуры
3	Оперативно отправлять информацию об инцидентах в НКЦКИ и читать бюллетени безопасности

*На основе выступления представителя ФСТЭК России на конференции ИБ АСУ ТП КВО 2022

INFOWATCH®

Единый центр управления системой защиты InfoWatch ARMA

- → **Управление** продуктами InfoWatch ARMA в едином веб-интерфейсе
- → **Автоматизация процессов ИБ:** от реагирования на инциденты до взаимодействия специалистов
- → **Информирование ГосСОПКА об инцидентах** ИБ

Проходит сертификацию ФСТЭК России ИТ.САВЗ.А4.ПЗ; УД4. **Включён в единый реестр российского ПО** Минкомсвязи РФ

Взаимодействие с ГосСОПКА

- → **Информирование ГосСОПКА об инцидентах** информационной безопасности
- → **Оперативный двусторонний обмен** информацией об инцидентах и угрозах безопасности

INFOWATCH ARMA ARMA Участник

Срочные консультации по защите АСУ ТП бесплатно

Получите рекомендации от наших специалистов по настройке встроенных СЗИ с / без предоставления ПО InfoWatch ARMA (по необходимости)

Оформите заявку на сайте arma.infowatch.ru

/InfoWatchOut /InfoWatch