Особенности решений по защите АСУТП в 2024 году

Алексей Петухов
Руководитель отдела развития бизнеса InfoWatch ARMA

Цифровизация
Аналитика 2023

76% интегрируют информационные технологии (ИТ) и операционные технологии (ОТ) в единую сеть

При этом

Из 400 компаний по всему миру

97% опрошенных сообщили, что атаки на ИТ инфраструктуру предприятия также затронули и ОТ.

47% атак — вымогатели

Пример.
Атака на производство 28 апреля 2023

Сообщение для наших клиентов: инцидент с кибербезопасностью

28 апреля 2023 г.

В начале января 2023 года мы подверглись серьезной кибератаке на наш бизнес. Хотя атака была обнаружена относительно быстро, и нам удалось ограничить ущерб за счет быстрого разделения сети, атака привела к шифрованию ряда наших приложений и систем хранения данных, а также повреждению сетевых устройств.

После инцидента мы постепенно восстанавливали наши сети и системы, включая восстановление некоторых приложений и файловых систем, где их невозможно было восстановить. Мы привлекли ряд специализированных

Источник — Morgan Advanced Materials, 2023

ВИРУС-ВЫМОГАТЕЛЬ

Шифрование систем хранения данных с производственными документами, планами, а также SCADA

- Оценка прямых потерь — $14 млн
- Прогноз падения годовой прибыли — 10–15%

Необходимо создать и эксплуатировать систему ИБ, которая...

1. Построена на российских решениях
2. Выполняет требования регуляторов (ФСТЭК, ФСБ, Минцифры, Минпром)
3. Обеспечивает устойчивость производства к внешним воздействиям в сферах ИТ и АСУ

Построение системы ИБ АСУ ТП — 2024

Эффективное управление организационными мерами и процессами

ЛЮДИ

Эшелонированная защита предприятия

Системы обнаружения вторжений, песочницы, решения разных производителей для разных сегментов

Автоматизация управления и реагирования

Корреляция событий и формирование правил реагирования, обмен данными с ГосСОПКА

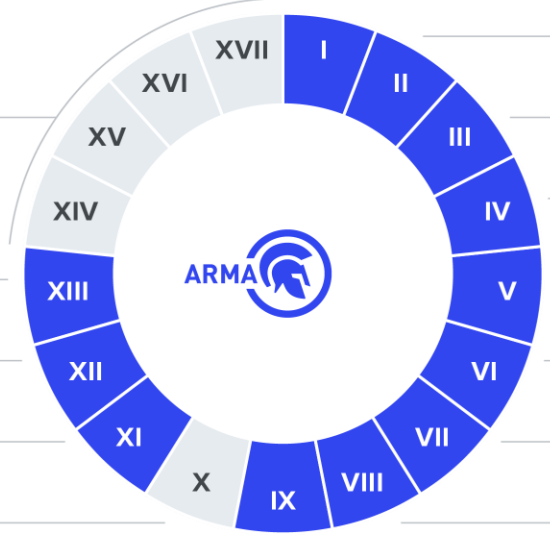
ТЕХНОЛОГИИ

Выполнение требований ФСТЭК и ФСБ России

Приказы ФСТЭК 17, 21, 31, 239, 235; требованиях ФСБ 368 и 282; ФЗ 187 и 152, ФЗ; указы президента РФ №250, 166 и т. д.

ПРОЦЕССЫ

Основные технические решения. Приказ ФСТЭК № 239, класс 3



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
Техническая мера ИБ

СОВ
InfoWatch ARMA Industrial Firewall

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

МЭ
InfoWatch ARMA Industrial Firewall

Физическая безопасность

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

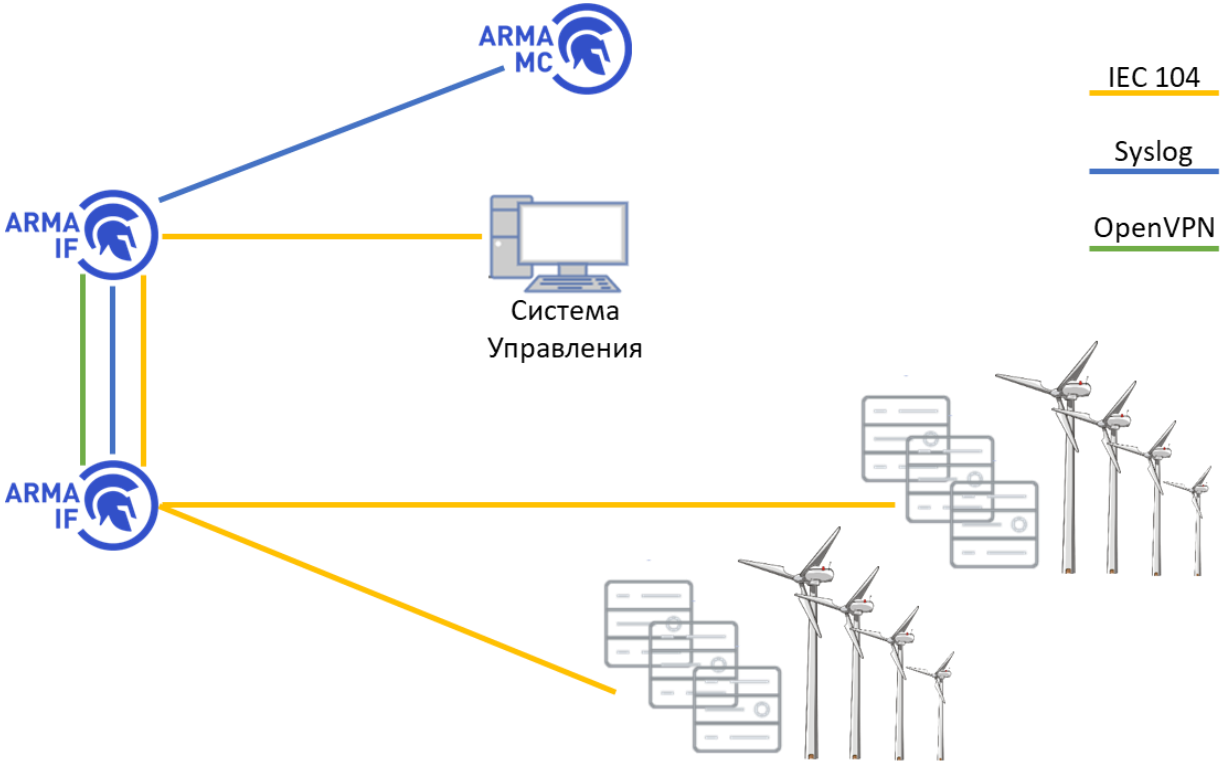
Средства управления инцидентами
InfoWatch ARMA Management Console

Организационные меры

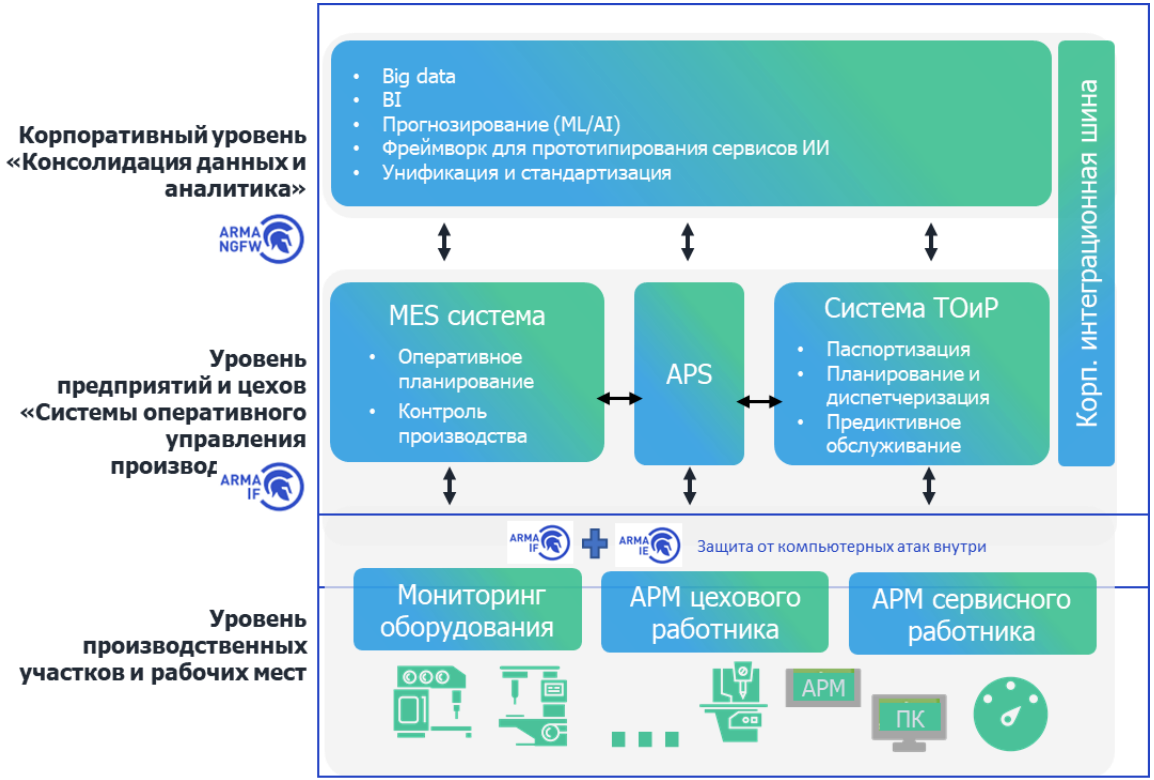
Получите карту соответствия InfoWatch ARMA группам мер ФСТЭК России

Оставьте запрос на сайте
arma.infowatch.ru

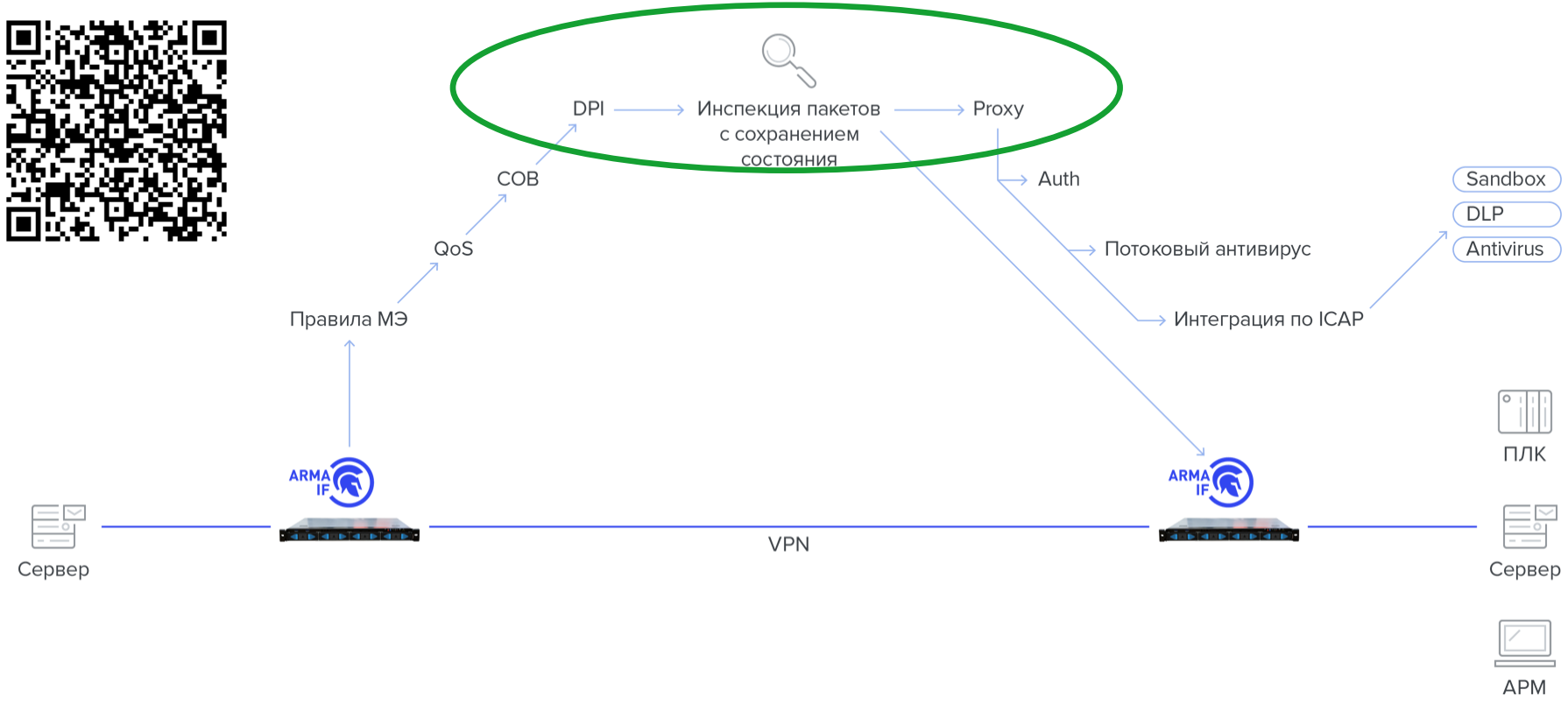
Пример реализации
Распределённый объект



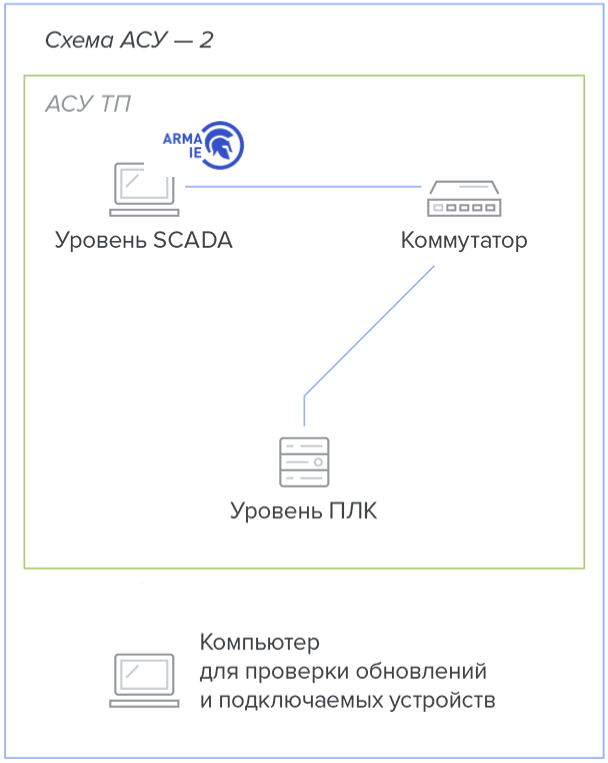
Пример реализации
Замкнутое предприятие



Ключевая особенность
Защита сети



Ключевая особенность
Защита рабочих станций и серверов



Организационные меры

— Доступ пользователей и авторизация

— Проверка съёмных носителей информации

— Проверка подключаемых устройств

СЗИ

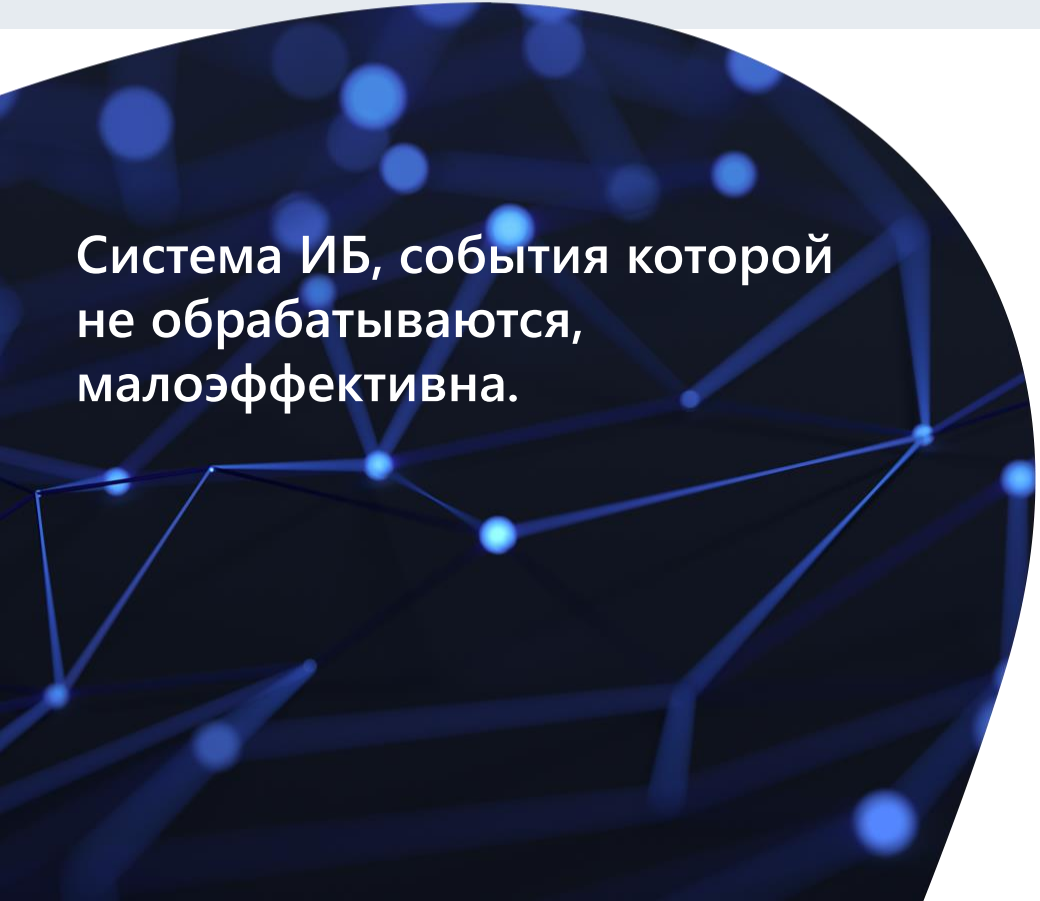
— Контроль подключаемых устройств

— Белые списки приложений

— Логирование действий и событий

\+ в рамках технологического обслуживания:
Антивирусная проверка, сканирование на уязвимости

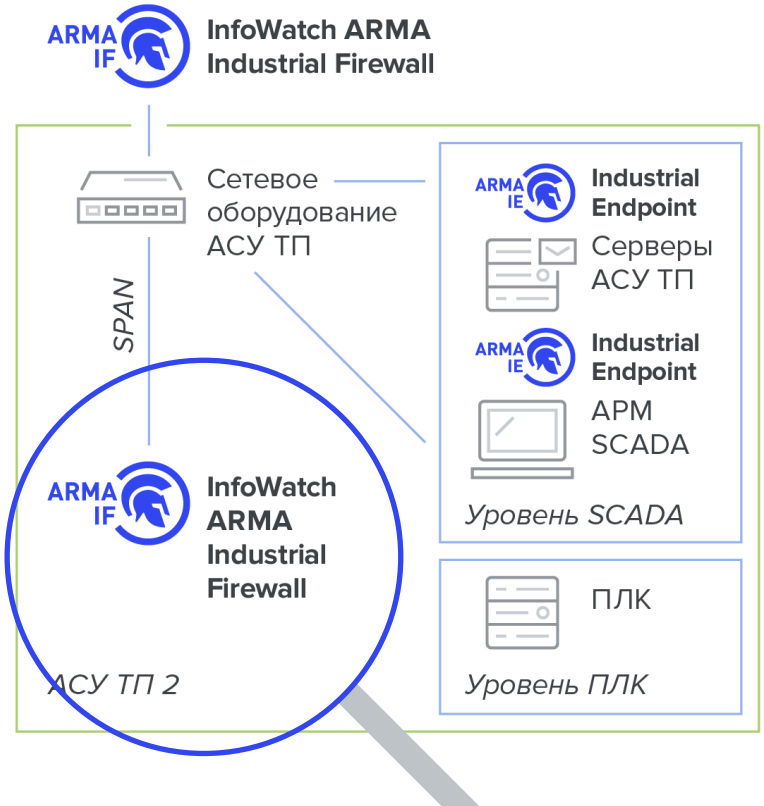
Автоматизация управления и реагирования



Система ИБ, события которой не обрабатываются, малоэффективна.

1. Интерактивное получение информации
2. Автоматическая или автоматизированная обработка информации
3. Автоматическое или автоматизированное реагирование
4. Оцифровка собираемой информации и принятых решений

Эшелонированная защита (ИБ) предприятия



1. **Максимальное сегментирование систем**
2. **Анализ трафика в защищённом периметре**
   СОВ, NTA и т. д.
3. **Углублённый анализ подключаемых устройств и передаваемых файлов**
   Сканеры уязвимостей, песочницы и т. д.
4. **Решения разных производителей для защиты разных сегментов**
   Разные МЭ и EP для производственной сети и бухгалтерии и т. д.

Управление системой ИБ

INFOWATCH® ARMA

Спасибо!

Задавайте ваши вопросы

infowatch.ru

/InfoWatchOut

/InfoWatch