INFOWATCH® ARMA ARMA

Эшелонированная защита АСУ ТП: практика INFOWATCH ARMA

Игорь Душа

Директор по развитию продуктов InfoWatch ARMA

Какие задачи стоят перед офицерами ИБ АСУ ТП

INFOWATCH®

Построить систему защиты, которая соответствует требованиям законодательства

— **151 конкретная мера** приказа ФСТЭК России от 25 декабря 2017 № 239

— **Требования продолжают ужесточаться**. (Пояснения к Приказу ФСТЭК 22 апреля 2019, в т. ч. использование сертифицированных маршрутизаторов)

Построить систему, которая обеспечивает реальную защиту АСУ ТП

— Каждая АСУ ТП уникальна. Требуется средство защиты информации, которое **учитывает специфику АСУ ТП**

— Корпоративные и технологические сети **не изолированы друг от друга.** Атаки на технологические сети идут через корпоративные ИТ-сети

— Учесть новые возникающие угрозы

InfoWatch ARMA — отечественная система для кибербезопасности АСУ ТП.

Промышленный межсетевой экран нового поколения (NGFW)

Единый центр управления инцидентами и решениями InfoWatch ARMA

Релиз — 4 кв. 2020

Система защиты АРМ и серверов

Релиз — 4 кв. 2020

Цель – дать возможность выполнить до 60% технических требований ФСТЭК России

Идентификация и аутентификация	**Управление доступом**	**Ограничение программной среды**
Обеспечение действий в нештатных ситуациях	**Аудит безопасности**	**Управление конфигурацией**
Защита информационной системы	**Реагирование на компьютерные инциденты**	**Предотвращение вторжений (компьютерных атак)**
Защита машинных носителей	**Обеспечение целостности**	Антивирусная защита
Информирование и обучение персонала	Обеспечение доступности	Защита технических средств и систем
Планирование мероприятий по обеспечению ИБ	Управление обновлениями ПО	

INFOWATCH® ARMA ARMA

INFOWATCH ARMA INDUSTRIAL FIREWALL

Централизованное управление инцидентами и решениями InfoWatch ARMA

Что защищает межсетевой экран InfoWatch ARMA

INFOWATCH®

- **Защита АСУ ТП от атак**

  Не только мониторинг, но и блокировка с поддержкой промышленных протоколов

- **Защита от несанкционированных действий пользователей**

  Разграничение прав доступа и анализ пакетов промышленных протоколов до отдельных функций

- **Защита удаленного доступа**

  Организация VPN, авторизация пользователей

Как защищает межсетевой экран InfoWatch ARMA

INFOWATCH®

1. Обнаруживает вторжения благодаря глубокому анализу пакетов промышленных протоколов
2. Содержит базу специализированных решающих правил кибербезопасности для АСУ ТП
3. Может использоваться как система мониторинга, так и как система блокировки атак
4. Позволяет контролировать действия пользователей благодаря гибкой настройка прав доступа
5. Обеспечивает непрерывную и отказоустойчивую работу АСУ ТП: конфигурация active-passive и аппаратный bypass
6. Учитывает все актуальные угрозы и при этом легко может быть обновлен, в отличие от АСУ ТП

Глубокий анализ промышленных протоколов. Зачем?

- **Контроль действий пользователя** (разрешение доступа на чтение, запись, ограничение по управлению конкретными функциями)
- **Ограничение трафика** между нескольким и АСУТП (возможность работы по промышленным протоколам или ограничение такой работы)
- **Запрет** заведомо **недопустимых операций** (обновление прошивки ПЛК)

Какие промышленные протоколы инспектирует для обнаружения вторжений

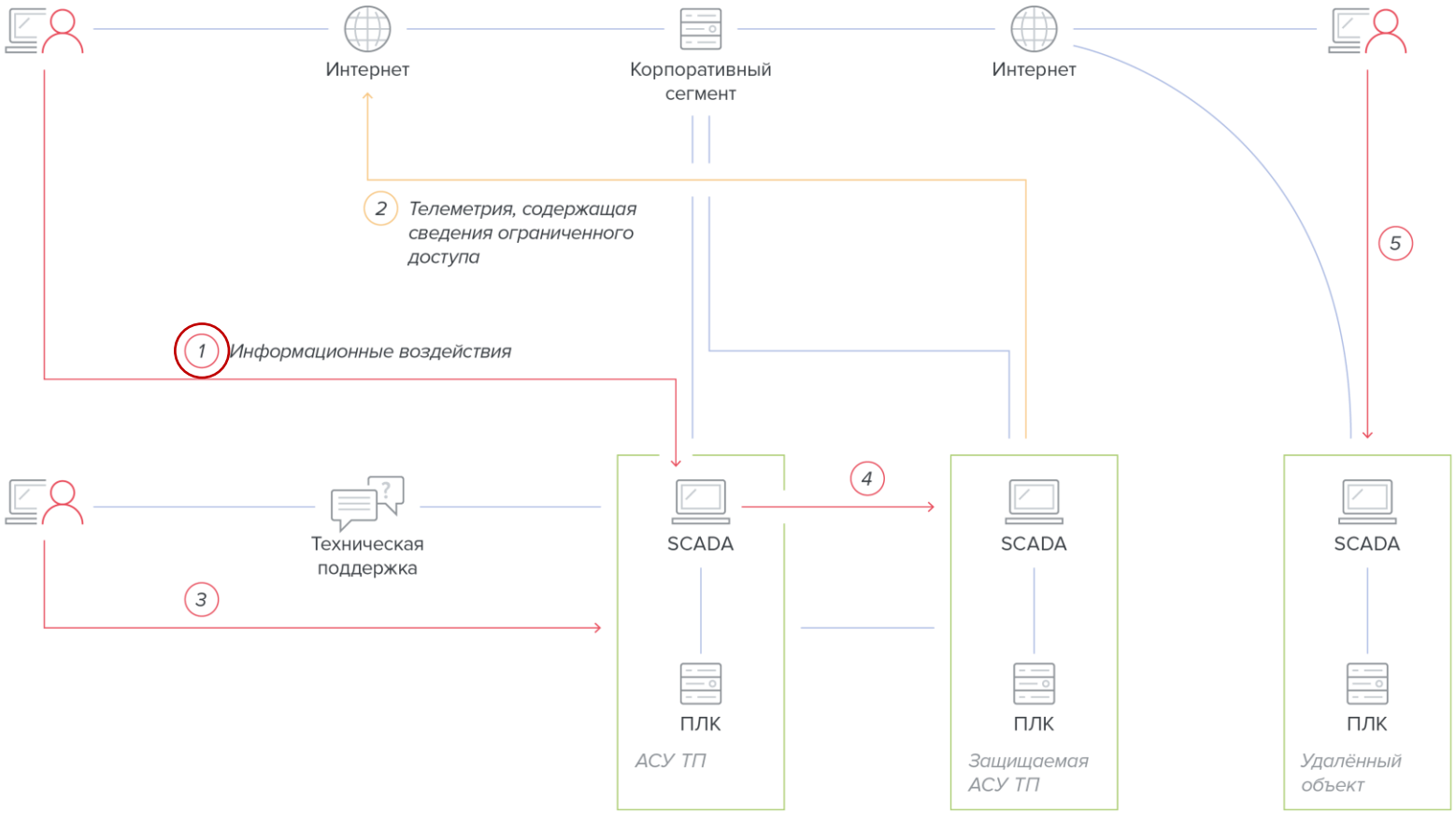
Обнаружение вторжений и мониторинг (без фильтрации)	Глубокая фильтрации по полям протоколов
Modbus TCP	Modbus TCP
Modbus TCP x90 func. code (UMAS)	Modbus TCP x90 func. code (UMAS)
IEC 60870-5-104	IEC 60870-5-104
IEC 61850-8-1 MMS	IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE	IEC 61850-8-1 GOOSE
OPC UA	OPC UA
OPC DA	OPC DA
ENIP / CIP	S7 Communication
S7 Communication	
S7 Communication plus	
Profibus	
DNP3	

Где должна быть обеспечена защита

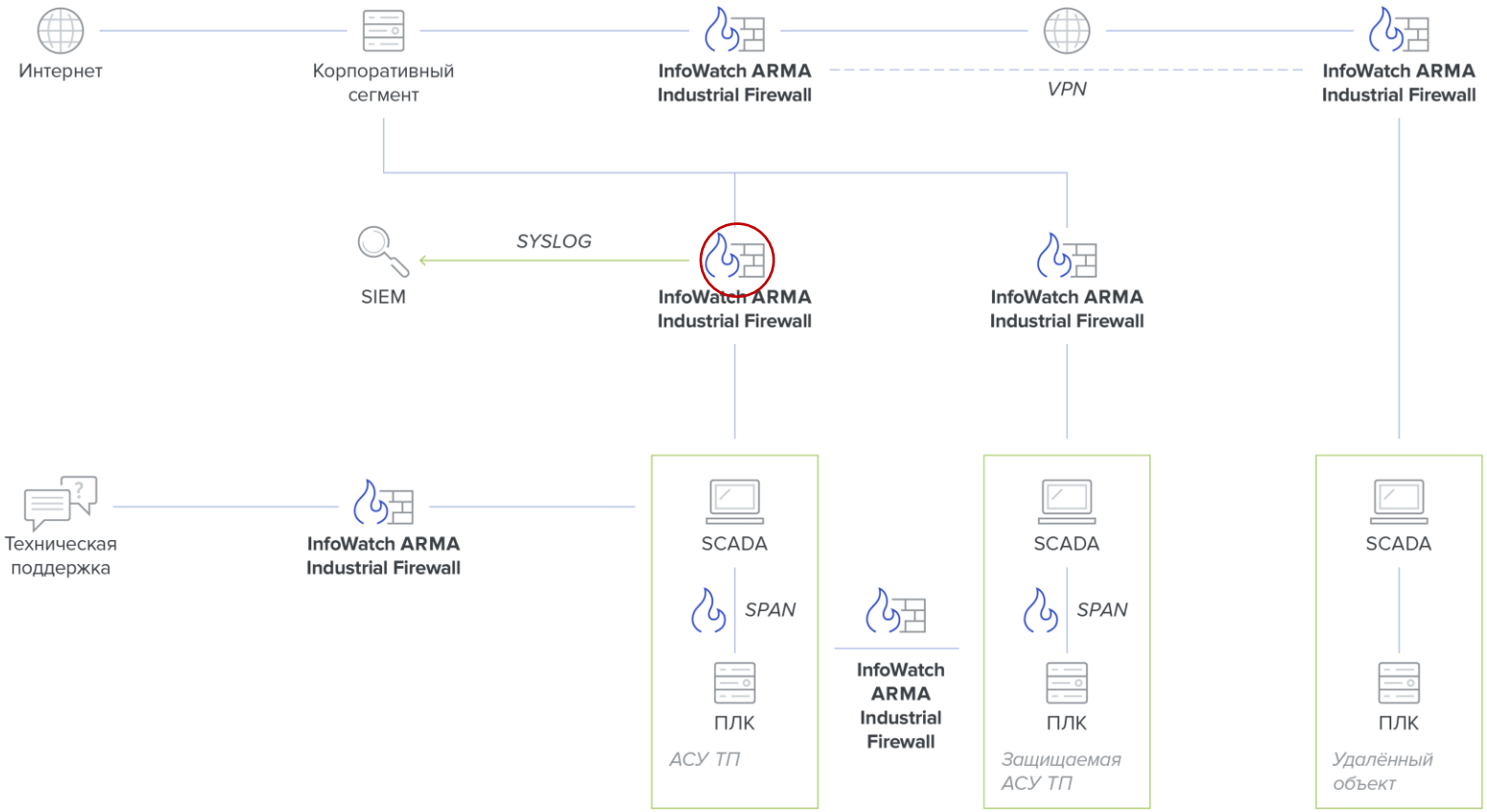
INFOWATCH®

1. АСУ ТП на границе с корпоративным сегментом
2. Каналы технической поддержи
3. Обособленные и смежные АСУ ТП
4. Сети между SCADA и ПЛК
5. Мониторинг внутри АСУ ТП
6. Удалённое подключение

6 векторов распространения сетевых угроз АСУ ТП



6 направлений защиты АСУ ТП по сети



Варианты поставок

Программно-аппаратные комплексы (ПАК). Вариант InfoWatch ARMA.

Промышленные компьютеры

Серверы x86 / x64

Виртуальные машины

vmware

Microsoft Hyper-v

Аппаратные конфигурации InfoWatch ARMA

Оборудование **InfoWatch ARMA** представлено как в промышленном, так и серверном исполнениях без движущих частей для монтажа в стойку или на DIN-рейку.

Монтаж в 19-дюймовую стойку

ARMAIF-RUGRACK

ARMAIF-19RACK

Монтаж на DIN-рейку или 19-дюймовую стойку

ARMAIF-DIN

ARMAIF-BOX

Гарантия на оборудование — 1 год. Возможно расширение гарантии до пяти лет.

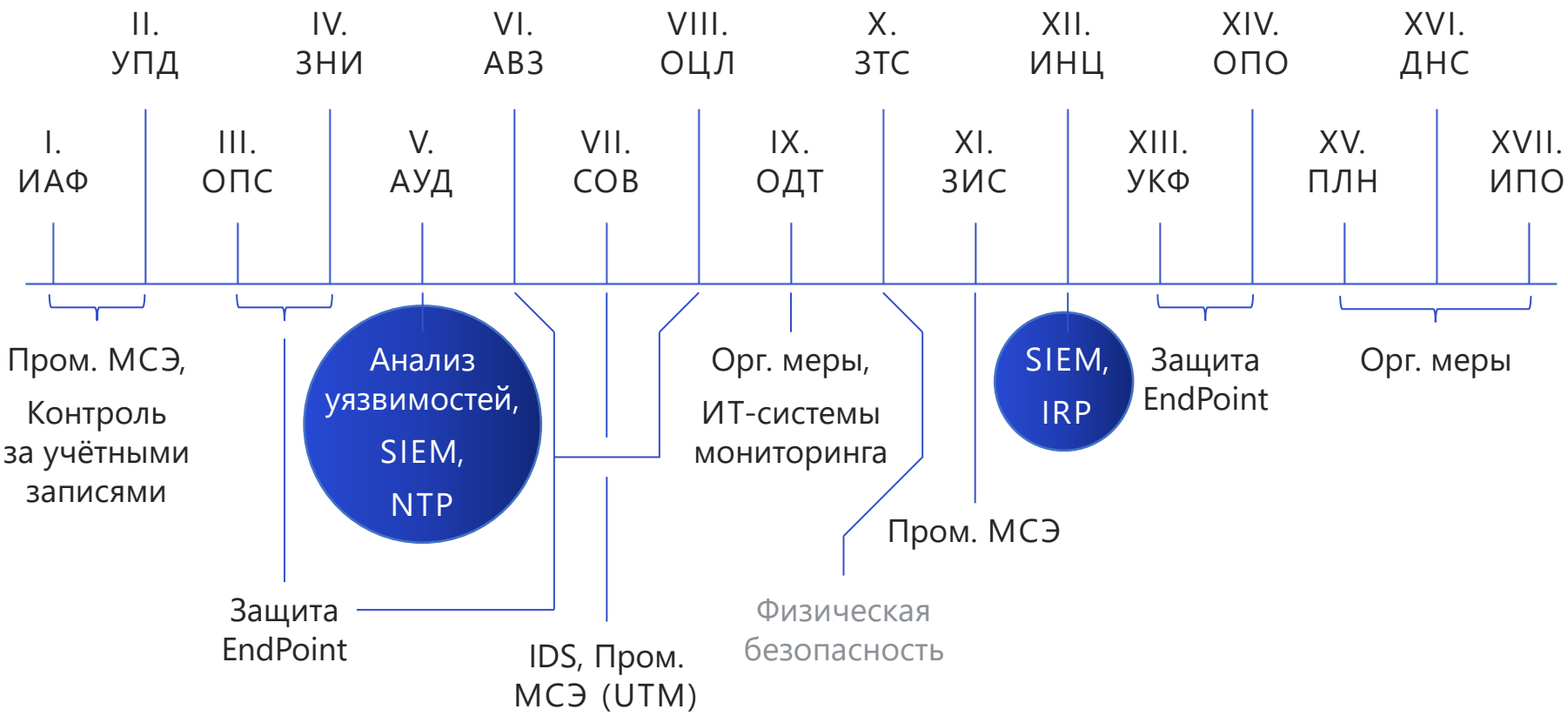
INFOWATCH® ARMA ARMA

INFOWATCH ARMA MANAGEMENT CONSOLE

Централизованное управление инцидентами и решениями InfoWatch ARMA

Релиз — 4 кв. 2020

Приоритетная задача — исполнение 187-ФЗ



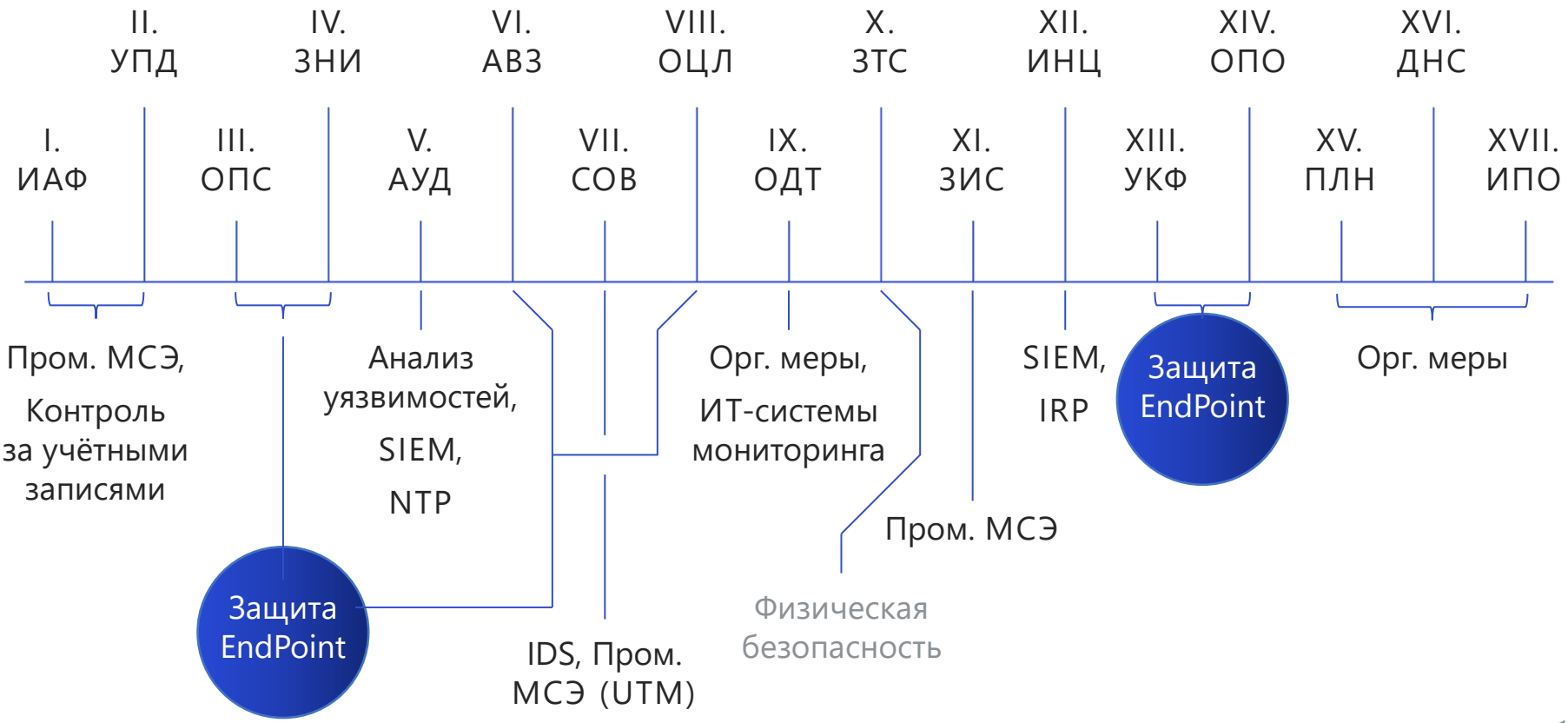
INFOWATCH® ARMA ARMA

INFOWATCH ARMA ENDPOINT

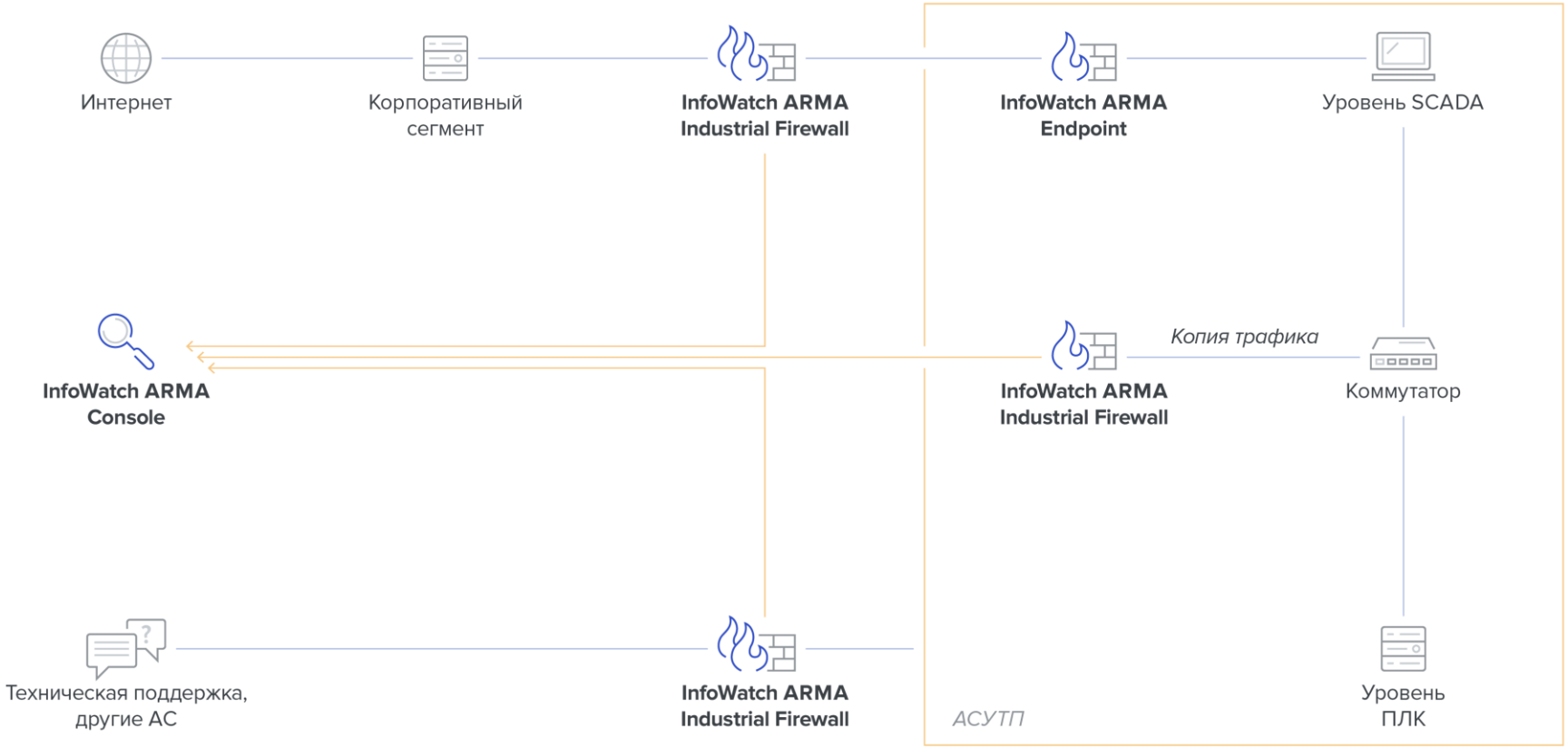
Организация замкнутой защищенной среды

Релиз — 4 кв. 2020

Приоритетная задача — исполнение 187-ФЗ



Общая схема — способ установки



Как эффективно спроектировать защиту в соответствии с 187-ФЗ

Заказчик

Крупная компания-проектировщик, которая готовила проектную документацию для дочернего общества ФСК ЕЭС

Задача

Выполнить технические меры 187-ФЗ единым отечественным решением по защите информации

Решение

В дополнение к антивирусам и средствам резервного копирования был выбран межсетевой экран InfoWatch ARMA для закрытия большинства технических мер.

Результат

InfoWatch ARMA позволила нивелировать бо́льшую часть угроз из модели, что позволило сократить затраты проектировщика.

Кейс: защита от атак АСУ ТП

Заказчик

Крупная электрораспределительная компания, которая в входит в ПАО «Россети»

Задача

Провести аудит информационной безопасности АСУ ТП

Решение

Установили решение на порт зеркалирования, переправляли трафик на работающий одновременно с нами PT ISIM

Результат

Выявили ряд уязвимостей, вредоносного ПО и нерегламентированных информационных потоков благодаря базе данных промышленных сигнатур

INFOWATCH®

ARMA ARMA

ДЕМО-ВЕРСИЯ С ТЕХНИЧЕСКОЙ ПОДДЕРЖКОЙ

Бесплатно 14 дней

Подать заявку

arma.infowatch.ru

/InfoWatchOut /InfoWatch