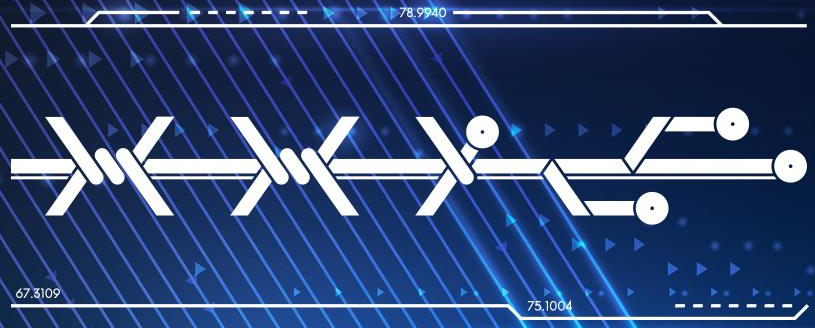
INFOWATCH®

ARMA ARMA



Кибербезопасность IIoT: теория и практика

Москва, 2020

Нестабильность? Это уже было!

50% Рост числа выявленных уязвимостей SCADA систем в первом полугодии 2018*

48% Промышленных предприятий России было атаковано киберпреступниками**

* По сравнению с аналогичным периодом предыдущего года, исследование TrendMicro

** По данным аналитиков Лаборатории Касперского

Атака на энергетическую систему Венесуэлы

ЧТО ПРОИЗОШЛО

Хакеры **атаковали** АСУ ГЭС «Эль-Гури» и **прервали процесс восстановления** системы

Организованы **физические нападения** (поджоги и подрывы ЭС)

РЕЗУЛЬТАТ АТАКИ

Произошло **полное отключение энергии** в 18 из 23 штатов Венесуэлы, **отключение главного аэропорта страны**, отказ резервных генераторов в аэропорту

Дискредитация действующей власти Венесуэлы

Ситуация с энергоснабжением была **использована оппозицией**

Объявлено **чрезвычайное положение**

Риски атак на АСУ растут

Атаки на киберфизические системы — новый вид военных действий

- Хакеры отключили все компьютеры (АСУТП остановили) НПЗ «Башнефти» с помощью вредоносa Petya. 2017.
- Пассажир за 20 минут взломал Wi-Fi «Сапсана» и получил доступ к информации ограниченного доступа. 2019.

74%

организаций, где функционируют АСУТП, сталкивались с инцидентами, связанными с проникновением злоумышленников в систему

При чем здесь IoT?

IIoT (промышленный интернет вещей)- многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.

- Один из стандартов безопасности ISO/TR 22100-4:2018 «Безопасность производственного оборудования — Связь с ISO 12100 — Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов информационной безопасности (кибербезопасности)»

IIoT распространяется широкими шагами

IIoT постепенно внедряется в разных отраслях:

- ✓ Умные здания
- ✓ Системы автоматизации производства
- ✓ Автомобильные системы
- ✓ Электрические подстанции
- ✓ MES и ICS-системы управления

IIoT сразу (модель Greenfield)

IT
Information technology

Сервисы

Пользователи

Стек протоколов: IP

IoT
Internet-of-Things

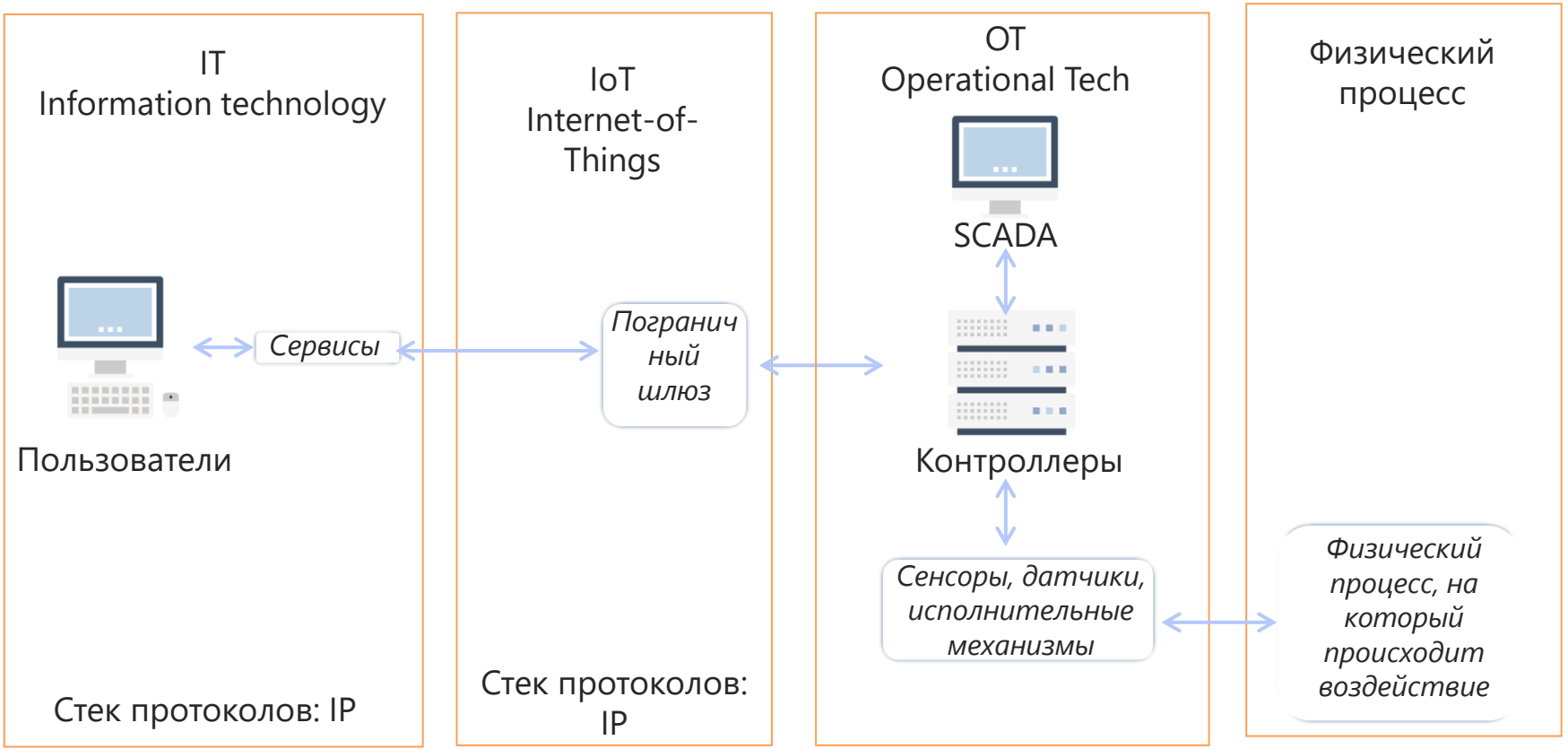
Сенсоры, датчики, исполнительные механизмы

Стек протоколов: IP

Физический процесс

Физический процесс, на который происходит воздействие

IIoT потом (модель Brownfield)



Основные проблемы безопасности IIoT

- Сложность обновления ПО
- Сложность определения зловредного внедрения в работу
- Отсутствие человеческого управления (в стандартном понимании)
- Большой масштаб (большое количество устройств и поверхности атаки)
- Небезопасные протоколы (например, Modbus, DNP3, PROFINET)
- Удаленное управление

Рекомендации ФСТЭК России по обеспечению дистанционной работы

На основе письма ФСТЭК России от 20 марта 2020 г. N 240/84/389:

- Минимизация прав и привилегий
- Идентификация удаленных СВТ
- Организация защищенного доступа с удаленного СВТ
- Применение на удаленных СВТ средств антивирусной защиты информации
- Исключение возможности установки работником программного обеспечения на удаленное СВТ
- Обеспечение мониторинга безопасности
- И другие (всего 14 пунктов)

В период нестабильности злоумышленники становятся активнее

- Количество заражений вредоносным софтом увеличилось на 38%
- 4 тысячи новых сайтов по теме COVID. Из них 8% – мошеннические
- $1 млн – ущерб Великобритании от мошеннических схем по теме COVID
- 441 сообщение о продаже тестов на COVID-19 и вакцин (которых пока в мире не существует)

Эта волна «догонит» все сферы жизни.

В промышленной отрасли атаки на фоне пандемии могут приводить к разрушительным последствиям.

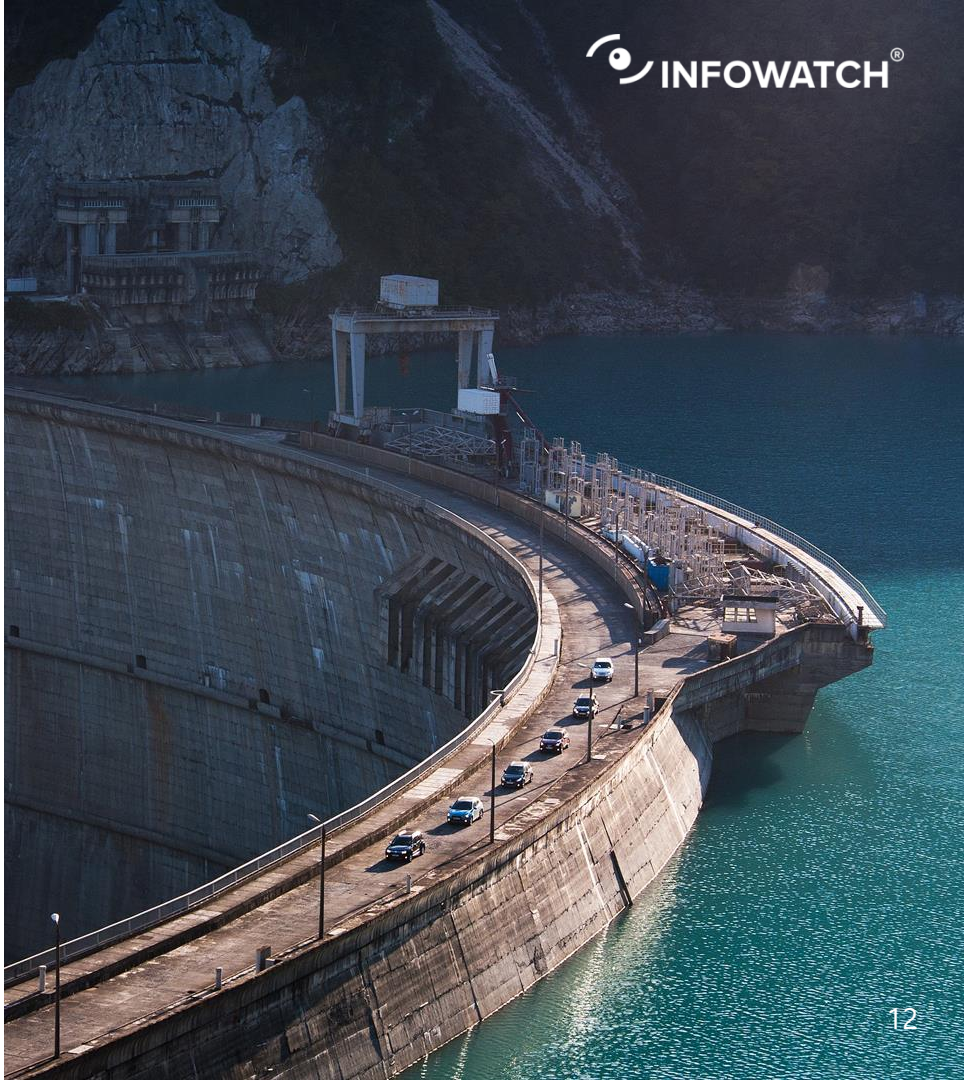
Требования регулятора

151 конкретная мера

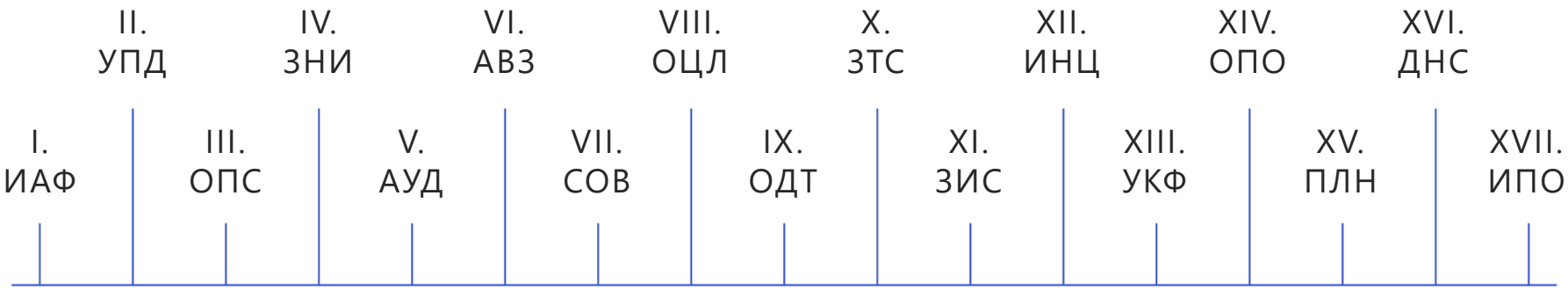
Все объекты КИИ должны быть приведены в соответствие требованиям регулятора:

- Приказ ФСТЭК РФ от 25.12.17 № 239
- Пояснения к Приказу ФСТЭК 22.04.19, в т. ч. использование сертифицированных маршрутизаторов

2022 год покажет...



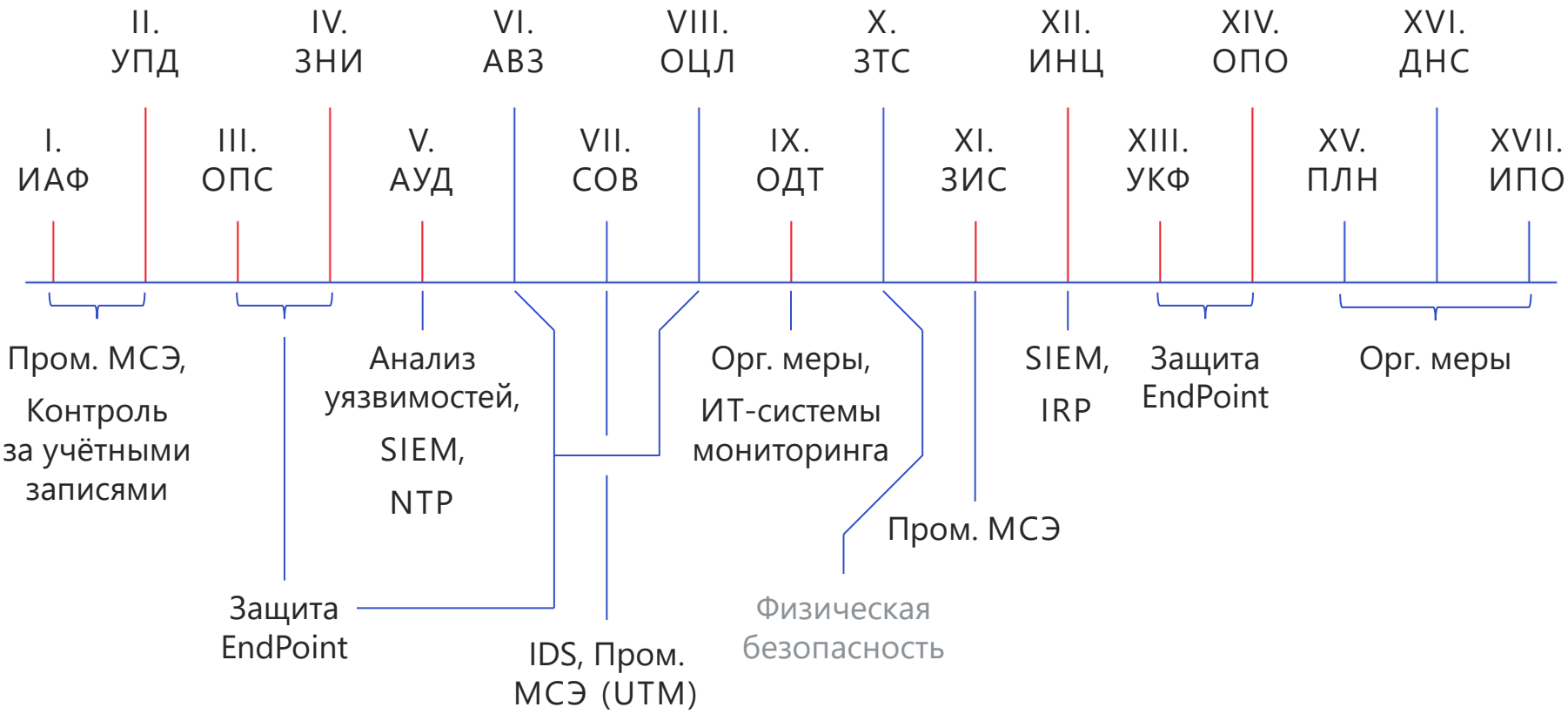
Требования регуляторов



~30% мер относятся к организационным

~70% мер требуют внедрения технологий защиты информации

Соответствие мер и классов решений



Как выбирать СЗИ

Технические средства на основе стендартов

Меры не соотносятся напрямую со средствами защиты, но в общем случае можно составить список СЗИ

- ✓ Системы идентификации, аутентификации (IdM)
- ✓ Средства доверенной загрузки
- ✓ Средства ограничения программной среды (Endpoint)
- ✓ Средства контроля подключения машинных носителей информации (Endpoint)
- ✓ Средства анализа защищенности
- ✓ Антивирусные средства
- ✓ Средства криптографической защиты
- ✓ Системы обнаружения вторжений
- ✓ Средства контроля целостности
- ✓ Системы управления инцидентами (IRP) и / или SIEM
- ✓ Средства резервирования, резервного копирования и т. д.
- ✓ Межсетевые экраны

Как выбирать средства защиты

Использование БДУ ФСТЭК России

На первый взгляд, 29 угроз из БДУ подходят для применения в АСУТП.
Но нет уверенности, что это все актуальные угрозы.
И что список не придётся дополнять.

- Угроза внедрения кода или данных
- Угроза воздействия на программы с высокими привилегиями
- Угроза восстановления и / или повторного использования аутентификационной информации
- Угроза изменения компонентов информационной (автоматизированной) системы
- Угроза загрузки нештатной операционной системы
- Угроза искажения вводимой и выводимой на периферийные устройства информации
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- Угроза использования слабостей протоколов сетевого/локального обмена данными
- Угроза несанкционированного доступа к аутентификационной информации
- Угроза несанкционированного доступа к виртуальным каналам передачи
- Угроза обнаружения хостов
- Угроза определения типов объектов защиты
- Угроза определения топологии вычислительной сети
- Угроза отключения контрольных датчиков
- Угроза передачи запрещённых команд на оборудование с числовым программным управлением
- Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
- Угроза перехвата вводимой и выводимой на периферийные устройства информации
- Угроза подмены содержимого сетевых ресурсов
- Угроза подмены субъекта сетевого доступа
- Угроза получения предварительной информации об объекте защиты
- Угроза преодоления физической защиты
- Угроза приведения системы в состояние «отказ в обслуживании»
- Угроза «фишинга»
- Угроза перехвата управления автоматизированной системой управления технологическими процессами
- Угроза подмены программного обеспечения
- Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты (антивирус)
- Угроза утечки информации с неподключенных к сети Интернет компьютеров
- Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров
- Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации

Всегда есть чем дополнить

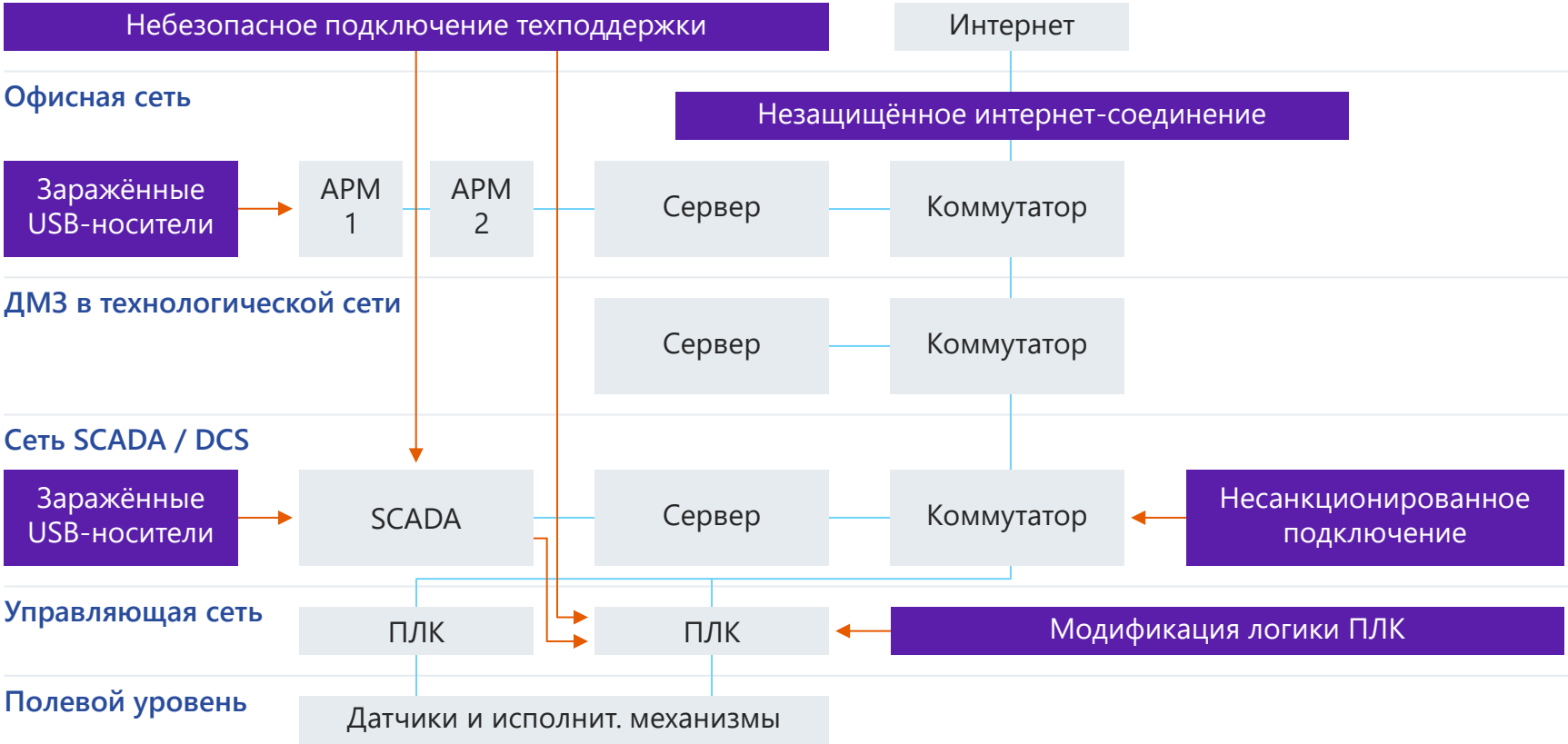
Если уйти от абстракций угроз и **перейти к атомарным действиям атакующего,** то список резко увеличивается:

- ✓ Перехват управления PLC с помощью MiTM
- ✓ Сканирование сети (в разных формах)
- ✓ Чтение проекта с ПЛК (с помощью **документированной** функции промышленного протокола)
- ✓ Чтение проекта с ПЛК (с помощью **недокументированной** функции промышленного протокола)
- ✓ Несанкционированная запись данных в ПЛК
- ✓ Установка вредоносного ПО

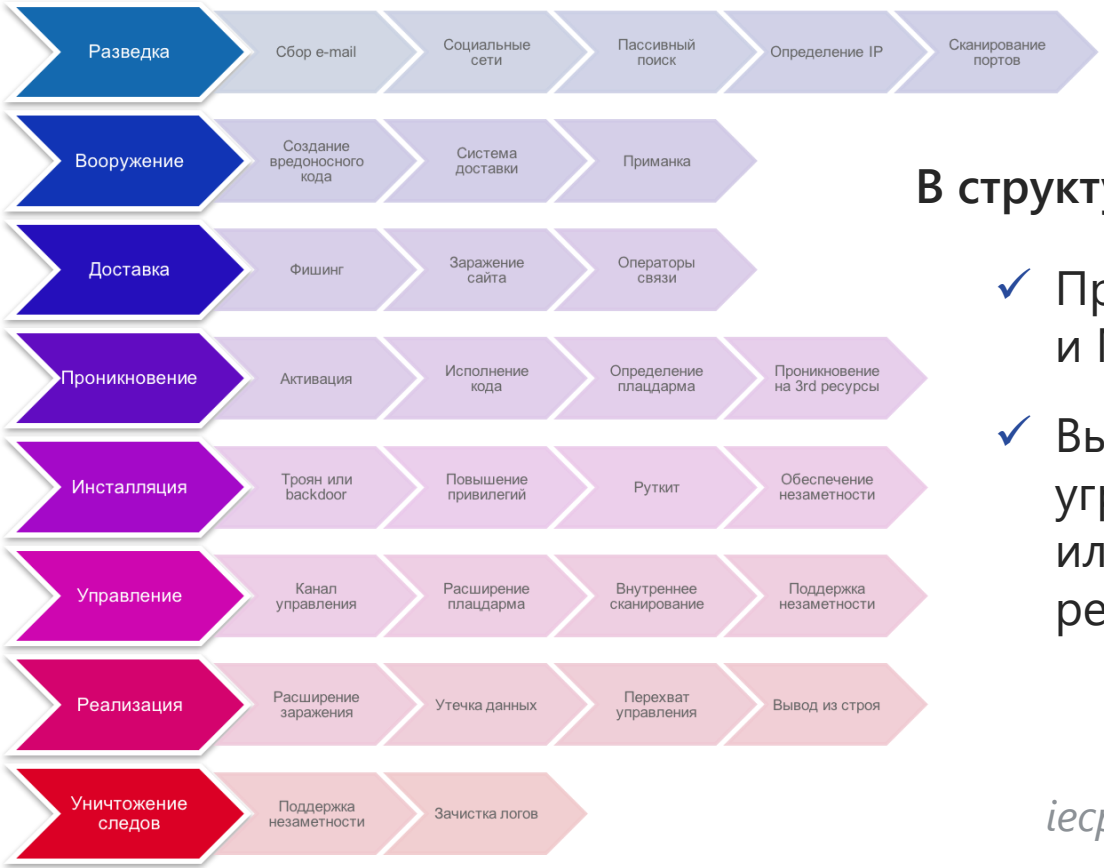
Как быть уверенным в неструктурированном перечне?..

На основе данных с S4x19 и учений SUTD

Добавим немного векторов



Как выбирать средства защиты



В структурировании угроз помогут:

- ✓ Применение Kill Chain и MITRE ATT&CK
- ✓ Выявление векторов развития угроз (через какой механизм или канал возможно реализовать угрозу)

iecp.ru/news/item/407302-Kill-Chain

Сопоставление Kill Chain и мер защиты

Стадии	МСЭ	СОВ/СПВ	Антивирус	Sandbox	ОПС (Endpoint)	СКЦ (Endpoint)	Контроль носителей (Endpoint)
Сканирование	+	+					
Фишинг	+		+	+	+		
Повышение привилегий			+				
Доставка ВПО	+	+		+			+
Установка ВПО			+		+	+	
Управление	+	+	+	+			

Как выбирать средства защиты

Красиво,
но непонятно
как выполнить

Модель угроз

Средства защиты информации

Системные требования

Активы

Угрозы безопасности активам

Меры приказа ФСТЭК России № 239

БДУ
ФСТЭК России
MITRE ATT&CK

Системные требования

Сами угрозы позволяют выбрать средства защиты. Это необходимый, но недостаточный параметр, ведь не менее важна возможность применения в АСУТП.

Проблемы применения средств защиты:

- Необходимость подтверждения возможности работы СЗИ в контуре АСУ с вендорами АСУ (особенно сложно с антивирусами и системами предотвращения вторжений из-за сигнатурного движка)
- Средства активного сканирования могут нарушить работу системы
- Обновление сигнатур + мониторинг за СОВ требует людские ресурсы, которых чаще всего нет на производстве

Иными словами применение СОВ, антивирусов, САЗ затруднены.

InfoWatch ARMA — линейка продуктов для защиты информации в АСУТП

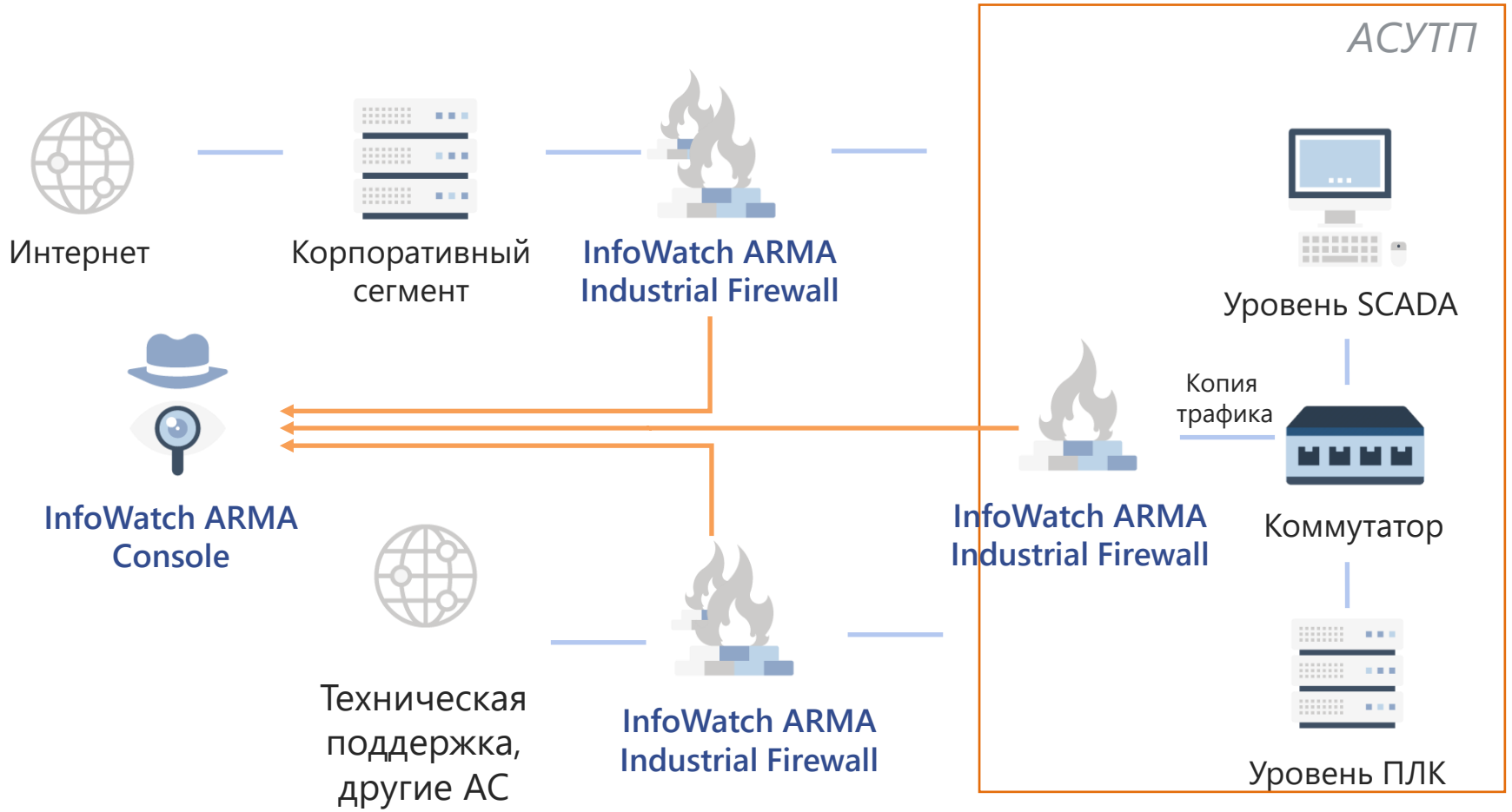
InfoWatch ARMA Industrial Firewall

Промышленный межсетевой экран с функцией обнаружения и предотвращения вторжений

InfoWatch ARMA Management Console

Консоль централизованного управления с возможностью управления инцидентами

Общая схема применения



Промышленный межсетевой экран. Тип «Д»
Система обнаружения вторжений

Решаемые задачи:

Защита удаленного доступа

Организация VPN, авторизация пользователей

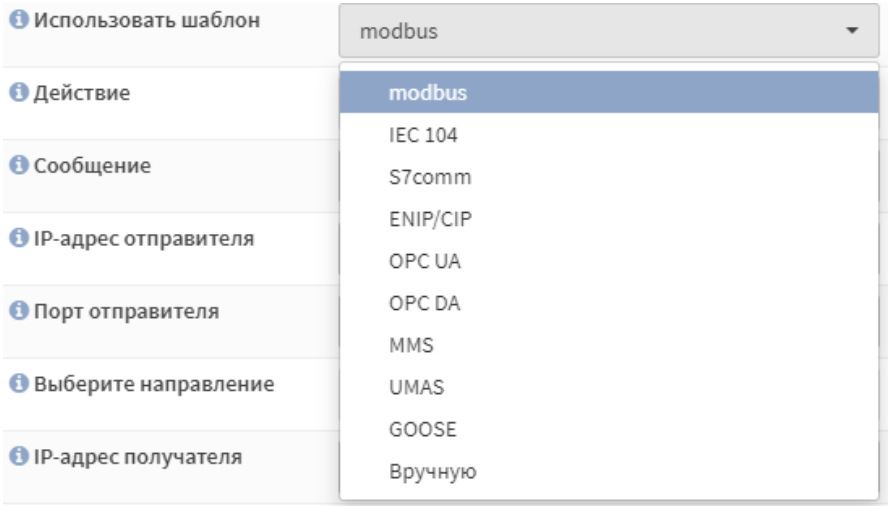
Межсетевое экранирование

С применением глубокой инспекции промышленных протоколов

Обнаружение и предотвращение вторжений

С учетом промышленной специфики

Чем отличается промышленный межсетевой экран от обычного?

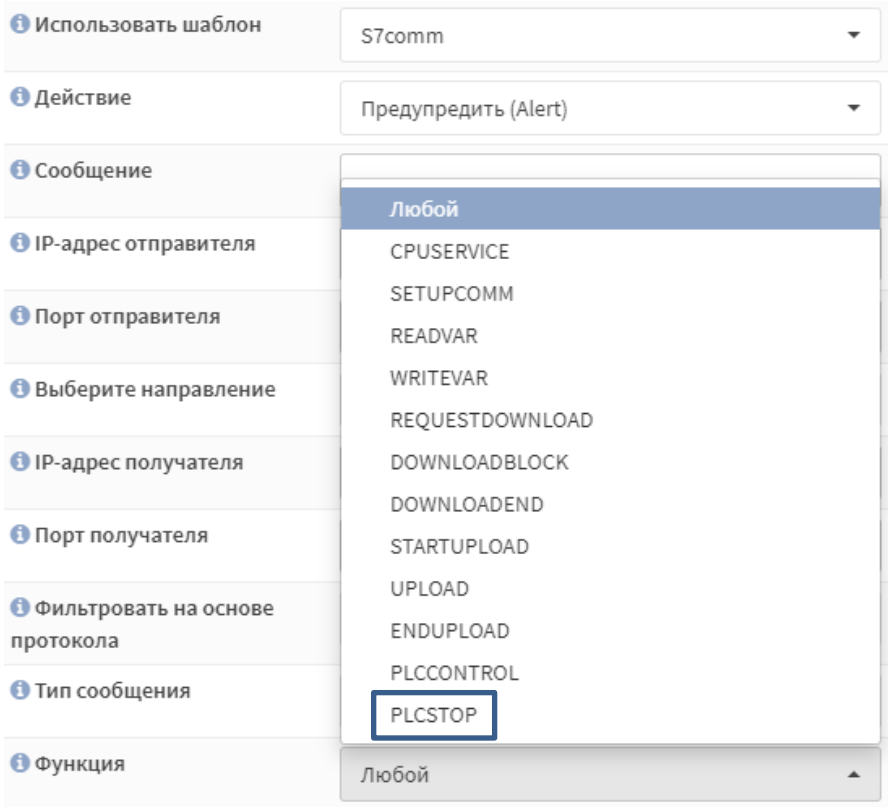


- Возможность фильтрации сетевого трафика на основе различных полей и параметров промышленных протоколов

— IEC 60870-5-104
— Modbus TCP (в том числе x90 UMAS)
— OPC UA

— IEC 61850 (MMS, GOOSE)
— S7 Communication
— OPC DA

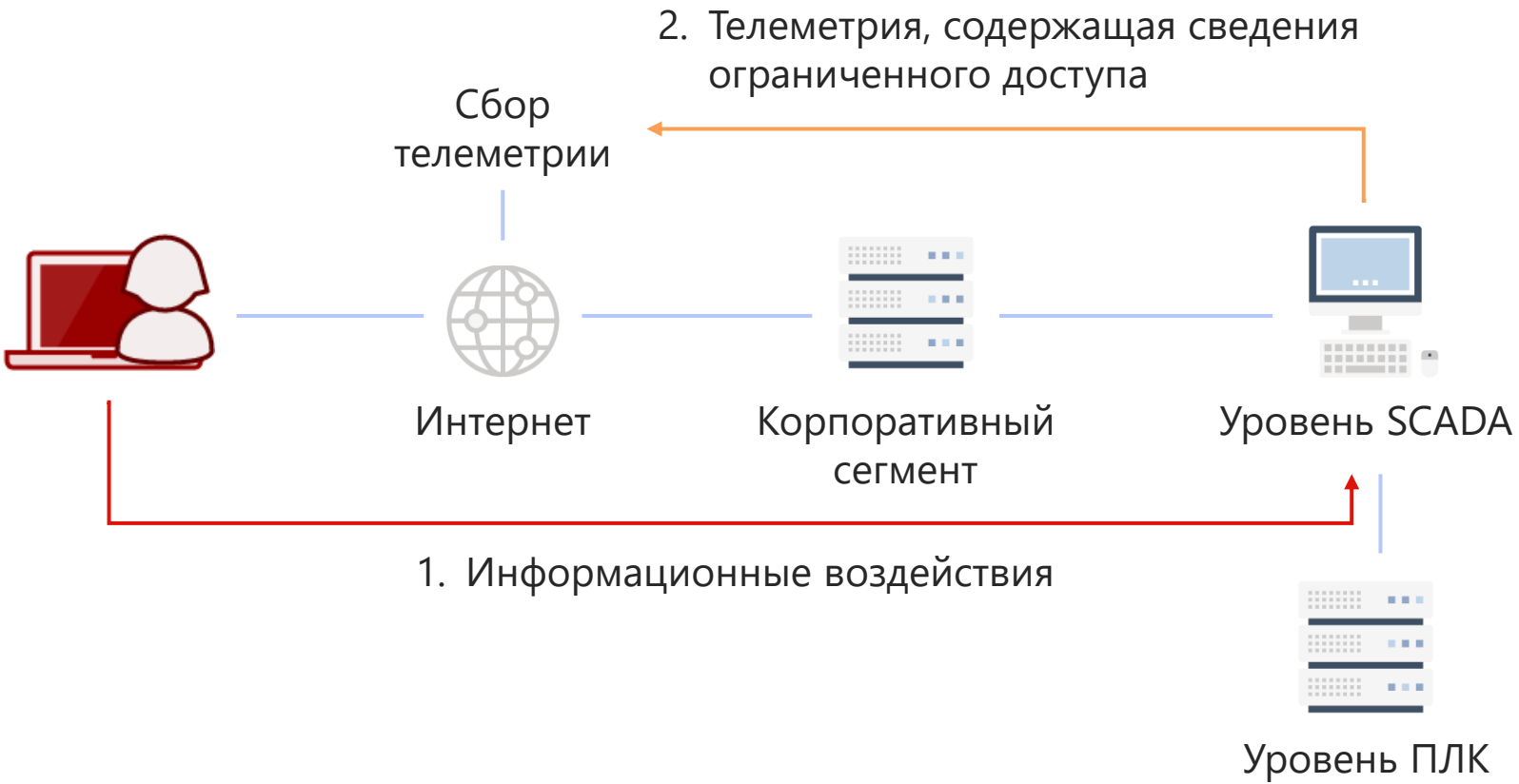
Разбор протоколов по функциям



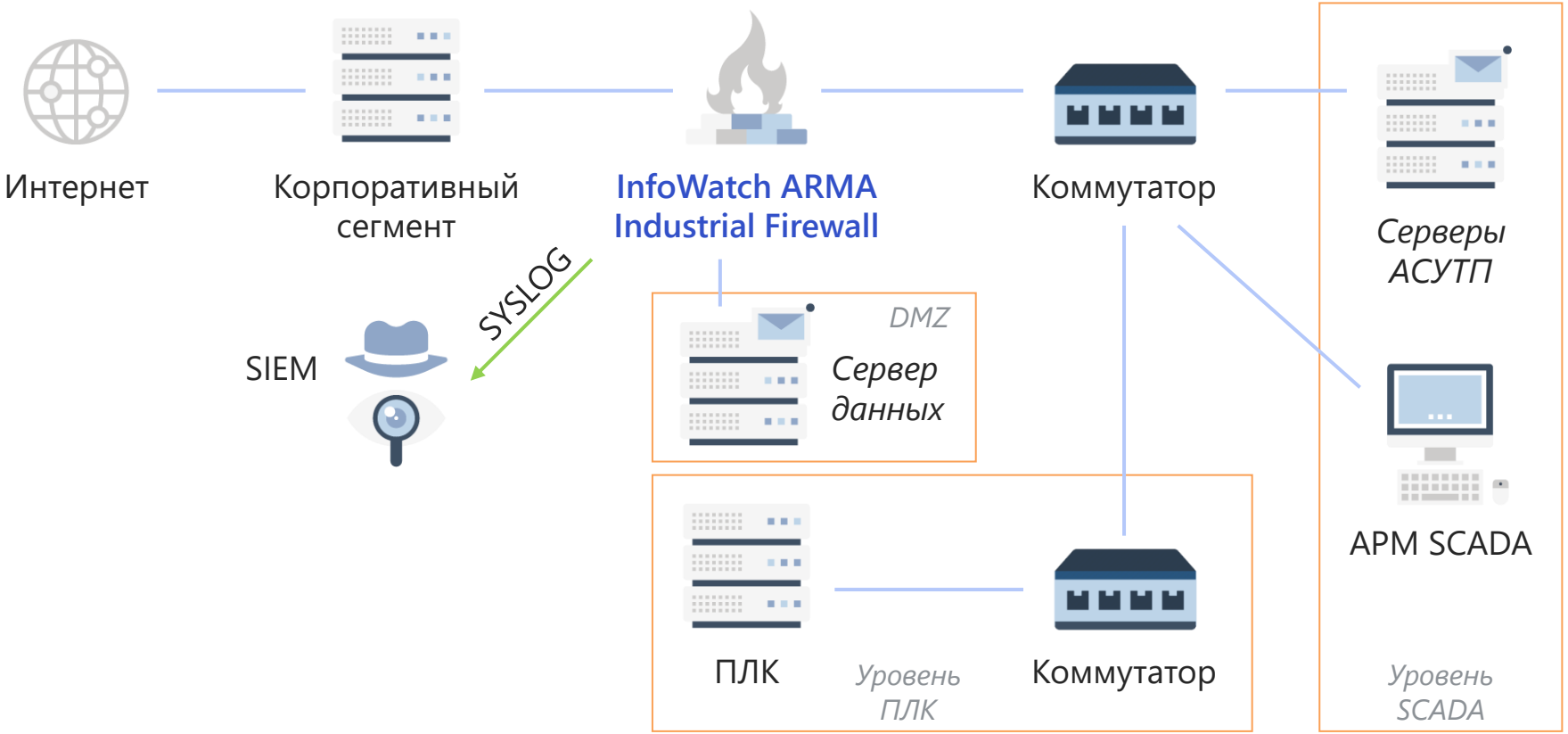
- **Анализ пакетов** по протоколам, портам, IP-адресам отправителя / получателя
- **Разбор протоколов** до уровня конкретных функций (например, обновление прошивки ПЛК)
- **Задать правила** блокирования / разрешения выполнения функции, например, выключение ПЛК

Варианты применения

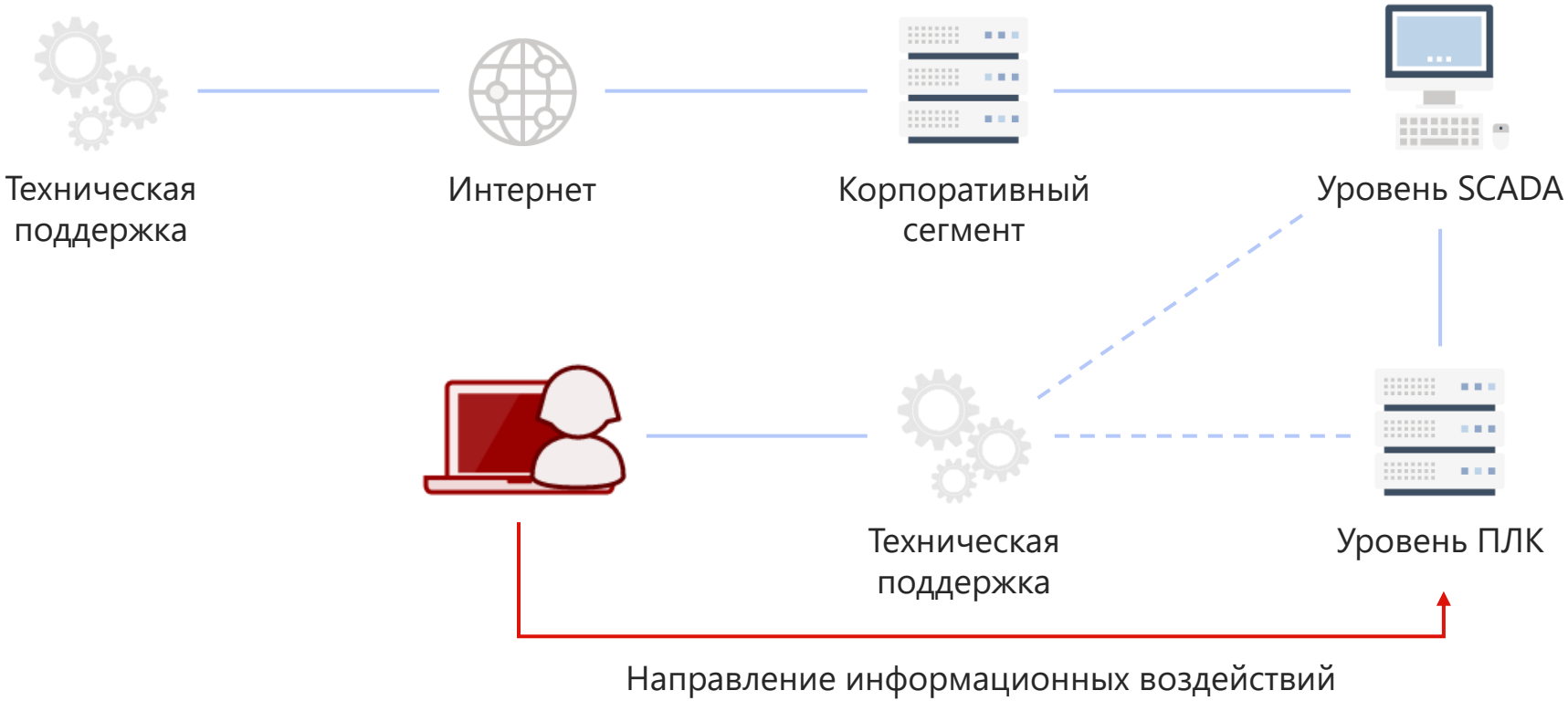
Граница с корпоративным сегментом. Угрозы



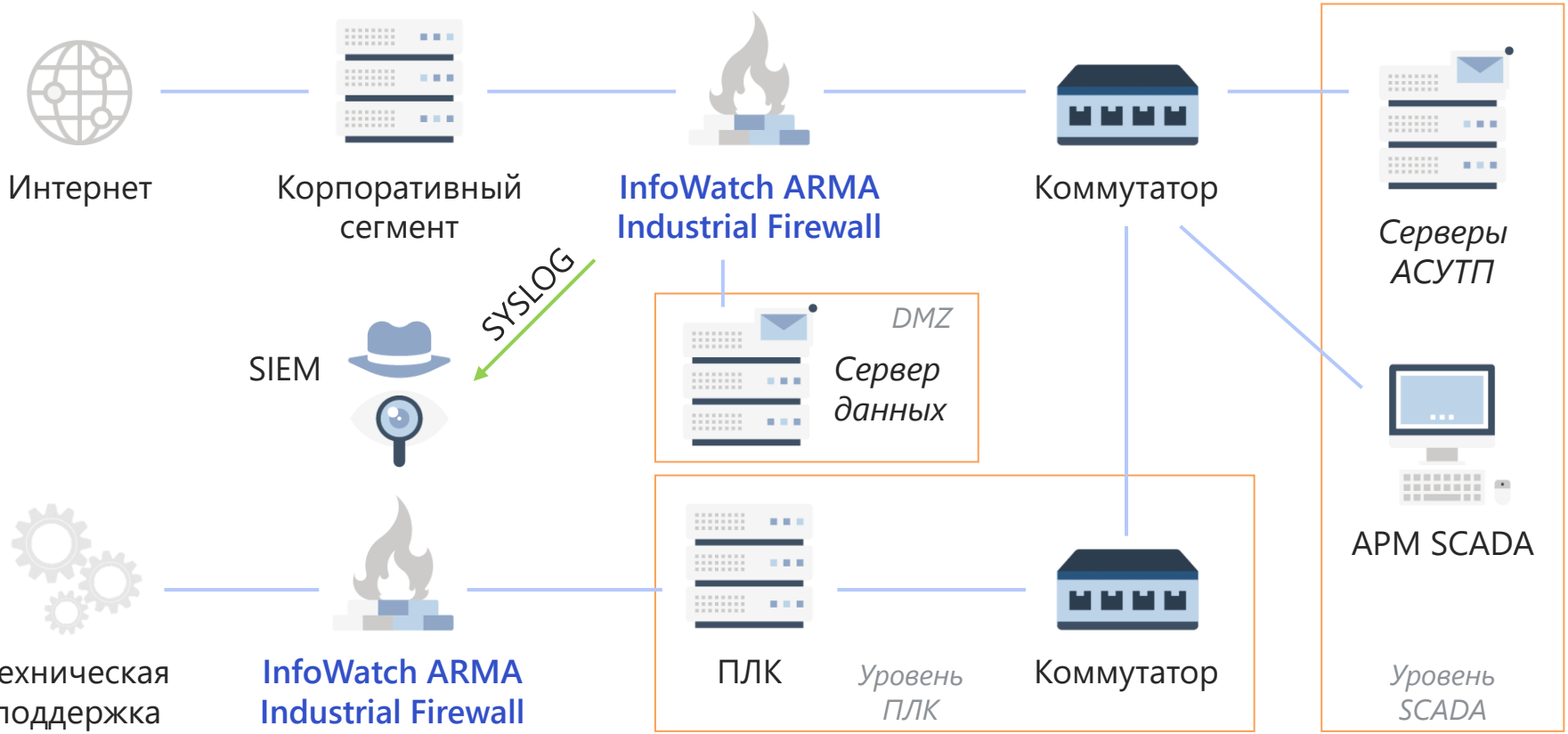
Граница с корпоративным сегментом. Защита



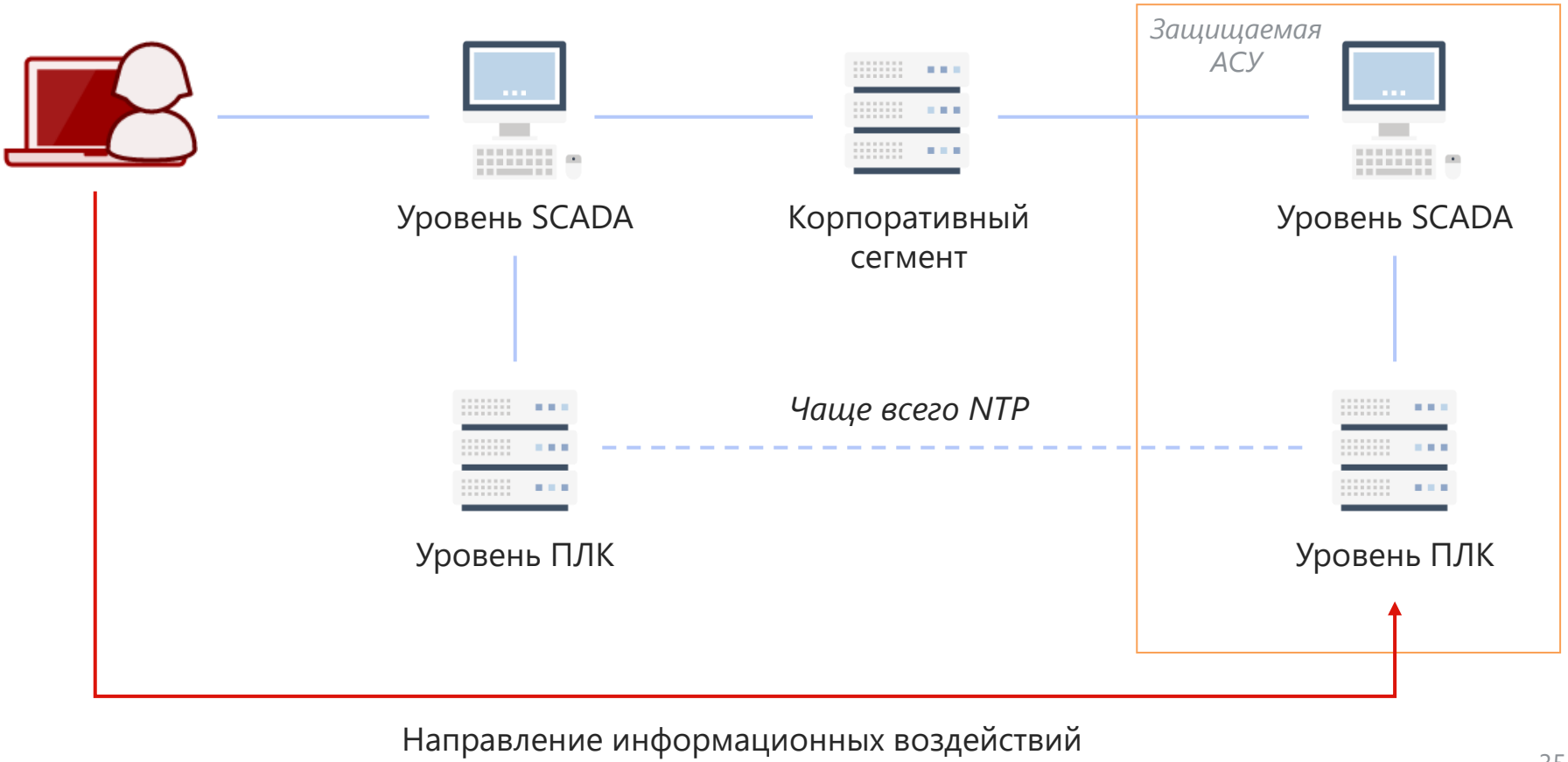
Связь с технической поддержкой. Угрозы



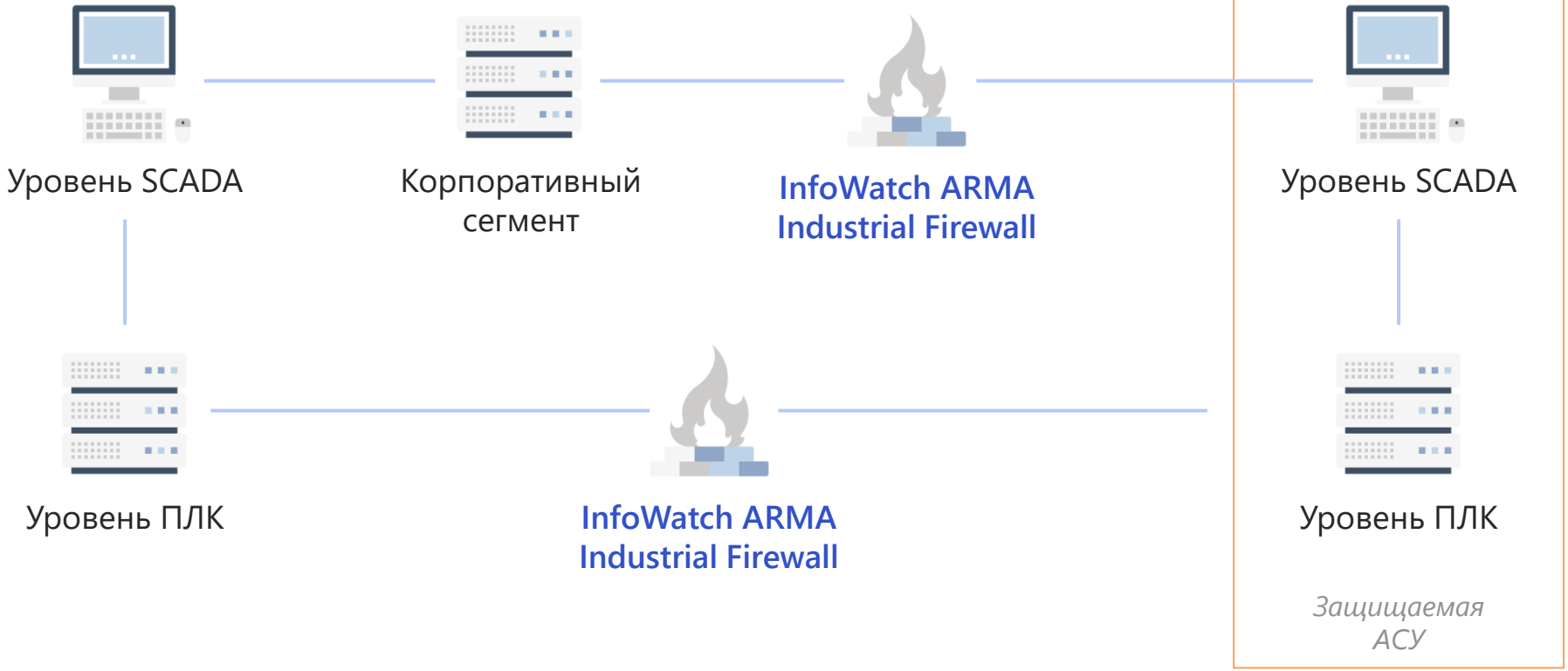
Связь с технической поддержкой. Защита



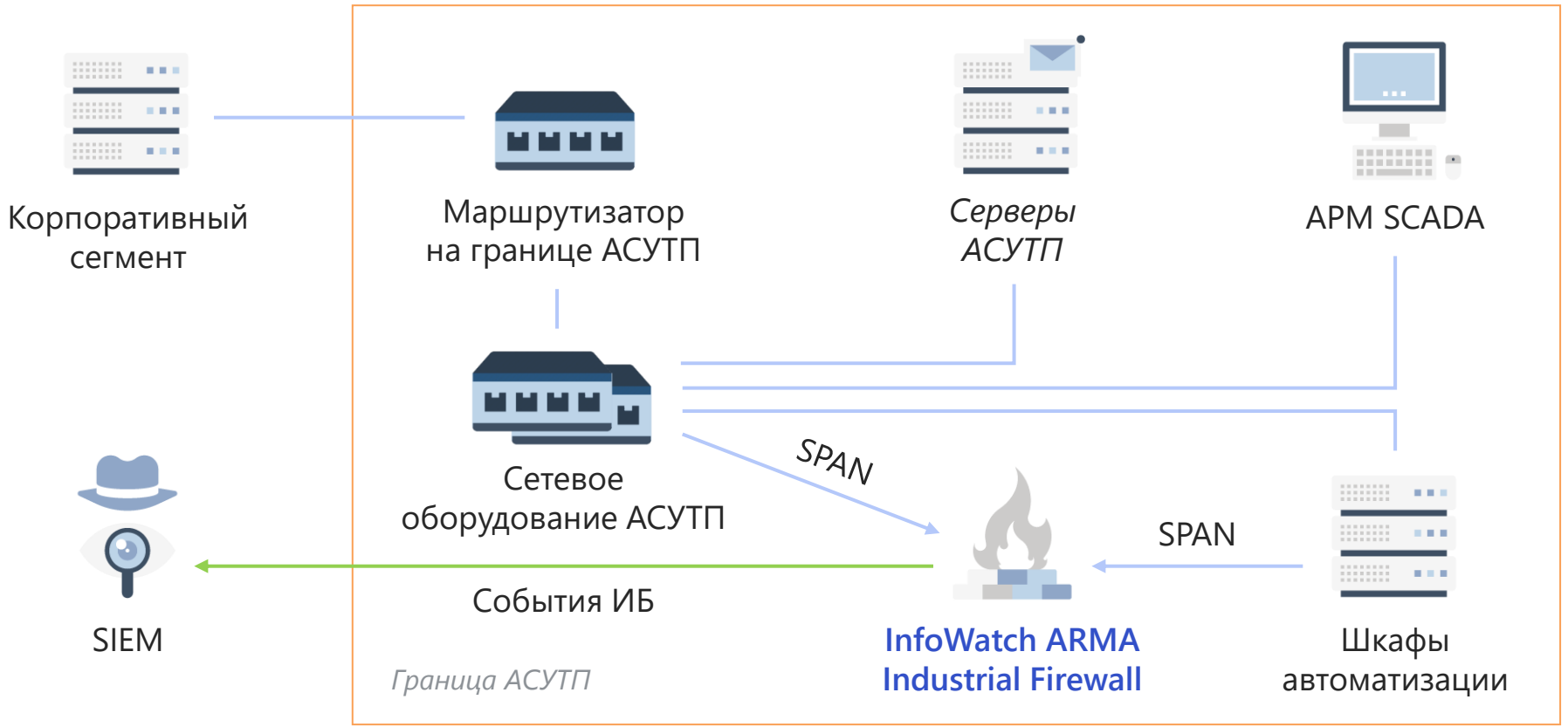
Связь со смежными АСУ. Угрозы



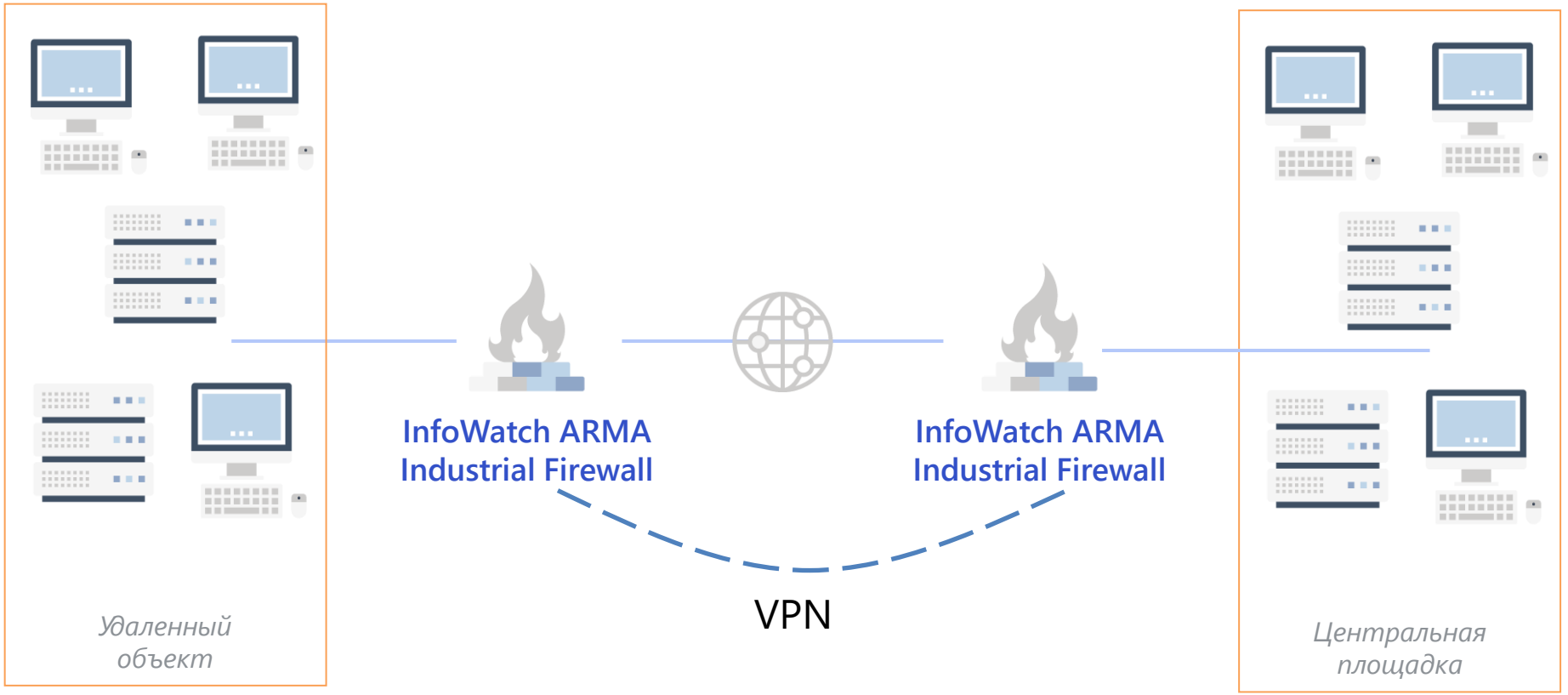
Отделение от смежных АСУ



Мониторинг трафика



Доступ к удаленному объекту по VPN



INFOWATCH®

ARMA ARMA

Получите карту реализации мер ФСТЭК России и продуктов InfoWatch

anna@team.infowatch.com

/InfoWatch

/InfoWatchOut

arma.infowatch.ru