INFOWATCH® ARMA ARMA

Главные риски кибербезопасности в 2022 и варианты реагирования на них

Игорь Душа

заместитель генерального директора
InfoWatch ARMA

Igor.Dusha@infowatch.com

Кибератаки на российские объекты КИИ: прямая угроза национальной безопасности

New York Times заявило со ссылкой на правительство США: **«Американские спецслужбы усилили попытки внедрить вредоносное программное обеспечение в российские энергосистемы».** Внедрение вредоносных программ в российские системы КИИ рассматривается как механизм «сдерживания» России.

Внедрение вредоносного ПО в российские объекты КИИ — механизм «сдерживания» России. В оборонном бюджете США-2020 инвестиции в кибербезопасность — $9,6 млрд, в т. ч. $3,7 млрд — на наступательные и оборонительные кибероперации (Interfax, 12.03.2019).

Актуальная повестка ИБ в России

→ **Уровень угроз признан критическим**

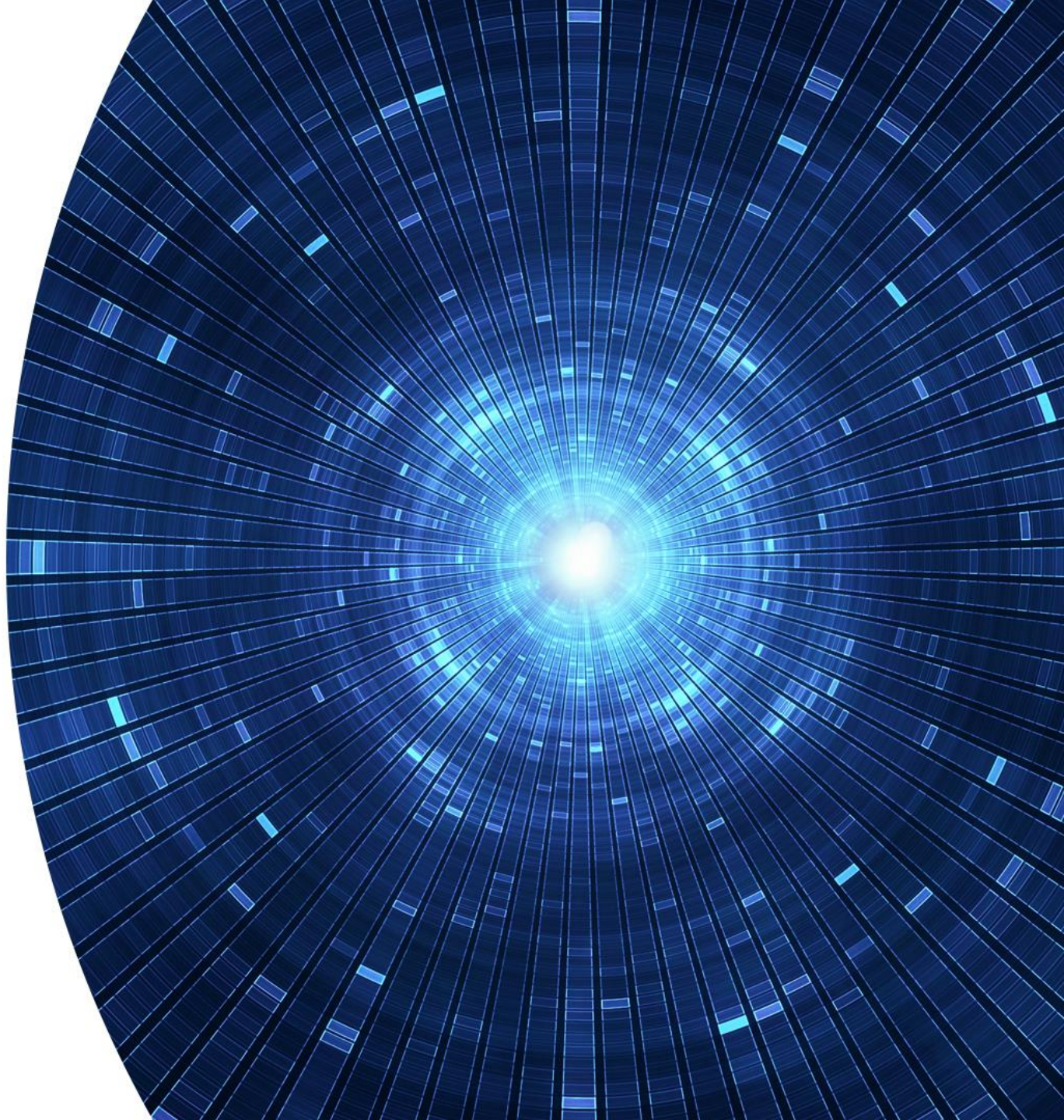
Письмо НЦКИ от 24 февраля 2022

→ **Указ Президента РФ от 1.05.22 № 250 «О дополнительных мерах по обеспечению ИБ»**

- Ускоренное импортозамещение

- Персональная ответственность руководителя за состояние ИБ

Что делать?



Современные вызовы кибербезопасности

→ «Размытие» периметра — кибератаки гигантского размера

Гибридная архитектура: IT- и OT-сети управляются компонентами, которые взаимодействуют с физическими объектами (киберфизические системы)

→ Ограниченная видимость сети

Разновендорный парк без единого центра управления и расследования инцидентов: долгая реакция на инцидент, отсутствие полной картины происходящего в сети. Как вы защитите то, что не видите?

→ Недостаток квалифицированных кадров

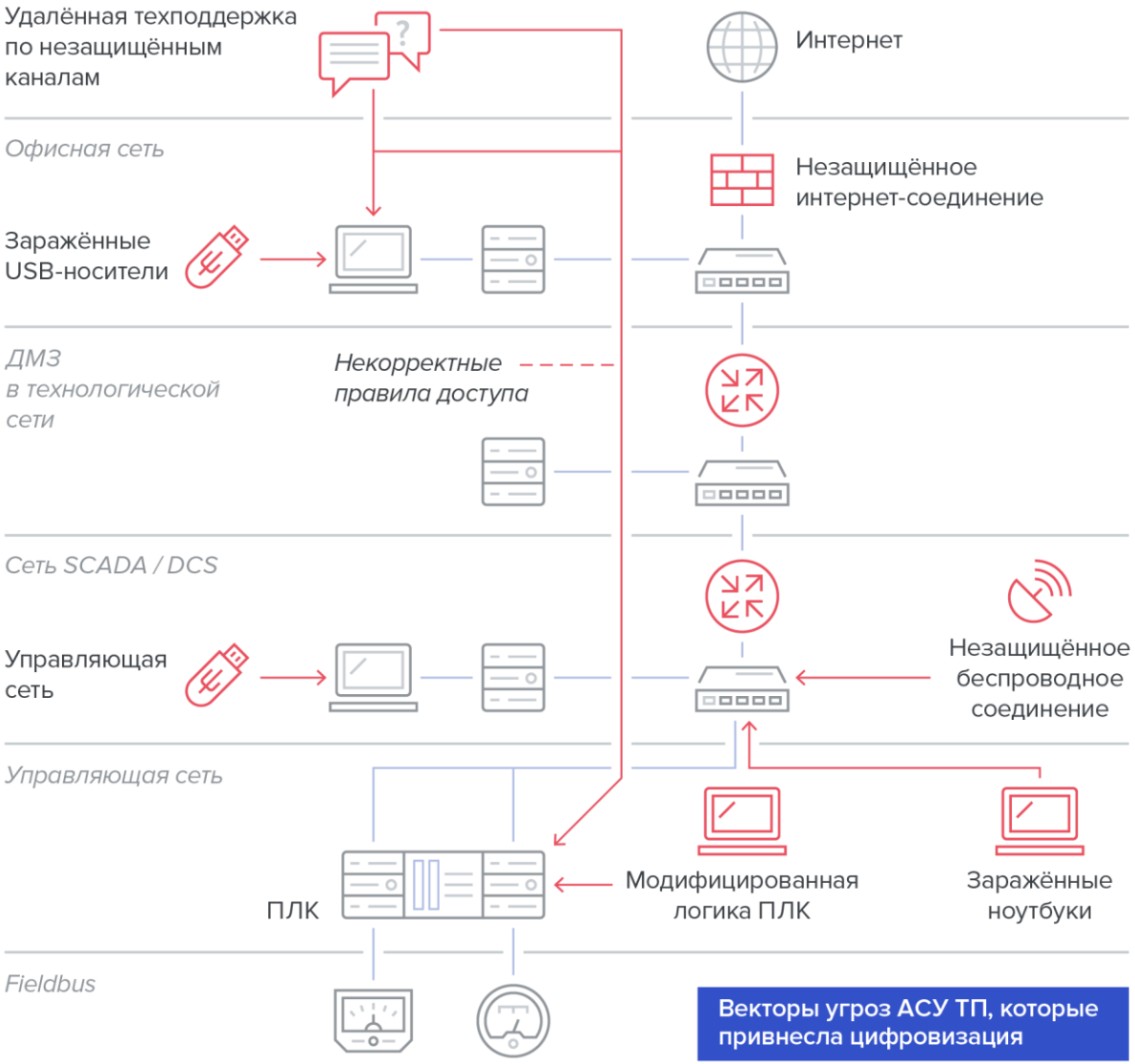
Кадровый «голод», «профессиональное выгорание» существующего штата ИБ: высокая нагрузка, рассогласованность действий служб ИТ и ИБ

→ Требования законодательства ужесточаются

Рост киберугроз с развитием цифровизации: тенденции 2022

- 100% рост атак типа supply chain. Пример: ПО SolarWinds. Гигантская площадь атак становится еще шире.
- Рост 30% атак с целью контроля инфраструктуры[1] и геополитического влияния. Рост интернационального кибершпионажа и APT-группировок.
- Рост атак на промышленные объекты
- Рост активности хактивистов/хакпионеров. Угроза высокой степени реализации, наравне с активностью киберпреступников[2]. Дело РЖД.

Защита — приоритетное требование времени



→ **Уровень угроз критический**

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

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

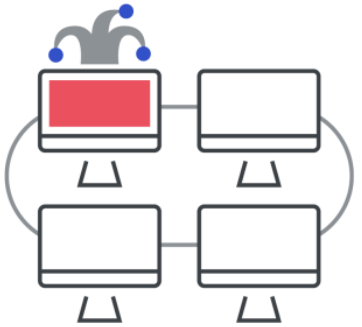
- Мониторинг дополнительно загружает специалистов
- Нужно максимально уменьшить поверхность атаки прямо сейчас

Основные векторы атаки

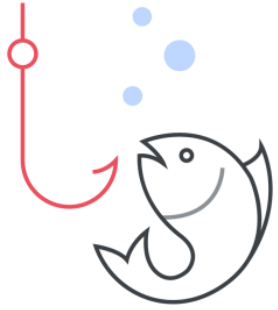
Подключение переносного носителя информации

Непроверенное оборудование и ПО

Атака инсайдера



Доступ к сети через стороннее ПО



Использование удалённого доступа и беспроводной связи

Рост рисков с развитием цифровизации

→ 449 уязвимостей в АСУ ТП (II пол. 2020)

→ Более 70% — критические (CVSS)

Отчёт Claroty

→ 49% — рост уязвимостей в АСУ ТП

→ 22% — скачок атак на промышленность (II кв. к I кв. 2020)

→ 25% всех атак в мире — на производство (1–8.2020)

Отчёт IBM

72% можно использовать удалённо

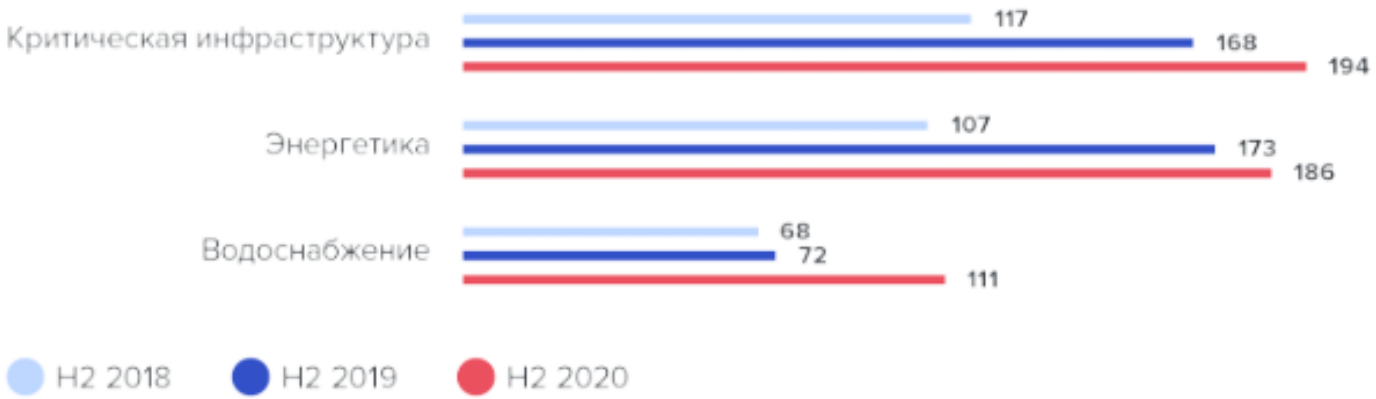
47% затрагивают уровни 1 и 2 модели Purdue (PLC, SCADA, DMZ)

76% не требуют аутентификации для эксплуатации

Аналитика: рост рисков — рост атак

- → **449 новых уязвимостей АСУ ТП найдено во II полугодии 2020** (по сравнению с 365 в I пол. 2020)
- → **Более 70% — критические** (по CVSS)
- → **На 25% выросло число уязвимостей АСУ ТП** (к 2019)
- → **72% можно использовать удалённо**
- → **47% затрагивают уровни 1 и 2 модели Purdue** (PLC, SCADA)
- → **76% не требуют аутентификации** для эксплуатации

Топ отраслей с обнаруженными уязвимости АСУ ТП



- → **EDP, Португалия**

  Вирус-вымогатель RagnarLocker
  Требование выкупа: $10,9 млн

- → **Light S. A., Бразилия**

  Вирус-вымогатель Sodinokibi
  Требование выкупа: $14 млн

- → **Enel Group, Италия**

  Вирус-вымогатель NetWalker
  Требование выкупа: $14 млн

- → **Более ранние известные атаки**
  - **Йоханнесбург:** отключение энергосистем
  - **Украина:** 300 тысяч человек без электричества
  - **Венесуэла:** блэкаут в 18 из 23 штатов

Почему и как удаётся реализовать кибератаки

Социальная инженерия, фишинговые письма

Персонал стал чаще пользоваться USB, личными устройствами при подключении к АРМ и т. п.

→ Использование USB в промышленности — рост на 30% в 2020. 51% вредоносного ПО на USB позволял проникать в сеть

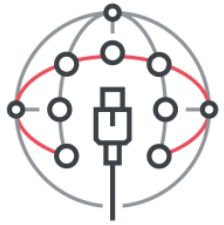
Продажа доступа в скомпрометированные сети компаний в даркнете

→ Рост в 4 раза в 2020

Незащищённый канал технической поддержки

Небольшие компании, подрядчики: слабое звено в цепочке поставок

→ Рост атак на цепочку поставок через подрядчиков — +100% в 2020



Низкая видимость сети и событий ИБ из-за усложнения инфраструктуры и отсутствия единого центра управления процессами ИБ

Как злоумышленники осуществляют атаку

→ **Подготовка**

Целенаправленное или случайное заражение файлов и оборудования работников предприятия (начиная, в том числе, с личных).

→ **Проникновение**

Эскалация заражения / компрометации / НСД внутрь корпоративного, затем технологического периметра (иногда сразу внутрь технологического). Проникновение может не замечаться годами — злоумышленники заметают следы.

→ **Последствия**

Чаще всего — шантаж, требование выкупа. Время от времени — акты киберагрессии (политически мотивированные): вывод из строя оборудования, отключение / разрушение объекта.

«Кадровый голод» требует автоматизации

К 2022 году (ISC)² прогнозировал* 1,8 миллиона незаполненных должностей OT security, что дополняет нынешнюю нехватку кадров

Реакция на недостаток квалифицированных кадров

→ Использование внешних SOC

→ Автоматизация реагирования на инциденты

→ Настройка систем интеграторами, а не эксплуатантом

https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

Внутренний нарушитель

Системный администратор

→ Инженер

→ Дежурный

→ Администратор

Пользователь ОКИИ

→ Оператор

Не является пользователем ОКИИ

→ Обслуживающий персонал

→ Работники субъекта КИИ

→ Перепрошивка аппаратных средств ОКИИ

→ Программно-аппаратные закладки

→ Вредоносные действия с АРМ пользователей ОКИИ и в ЛВС субъекта КИИ

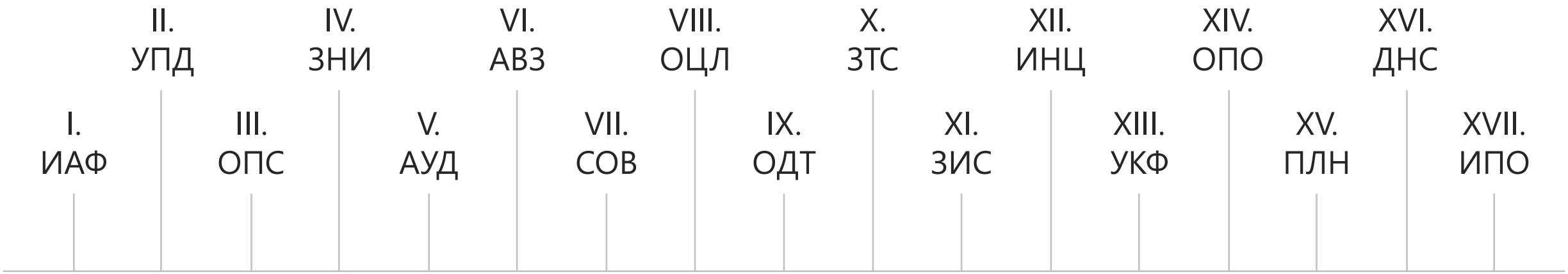
→ Атаки на системное и прикладное ПО

Внешний нарушитель

- → Специальные службы иностранных государств
- → Террористические и экстремистские группировки
- → Преступные группы (криминальные структуры)
- → Отдельные физические лица (хакеры)
- → Конкурирующие организации
- → Физические лица — бывшие работники субъекта КИИ, которые ранее являлись пользователями ОКИИ
- → Посторонние лица, пытающиеся получить доступ к информации в инициативном порядке
- → Конкурирующие организации
- → Разработчики ПО и ТС

→ Программно-аппаратные закладки	→ Удалённый доступ для получения информации ОКИИ
→ Вредоносное воздействие на ОКИИ	→ Атаки на системное и прикладное ПО

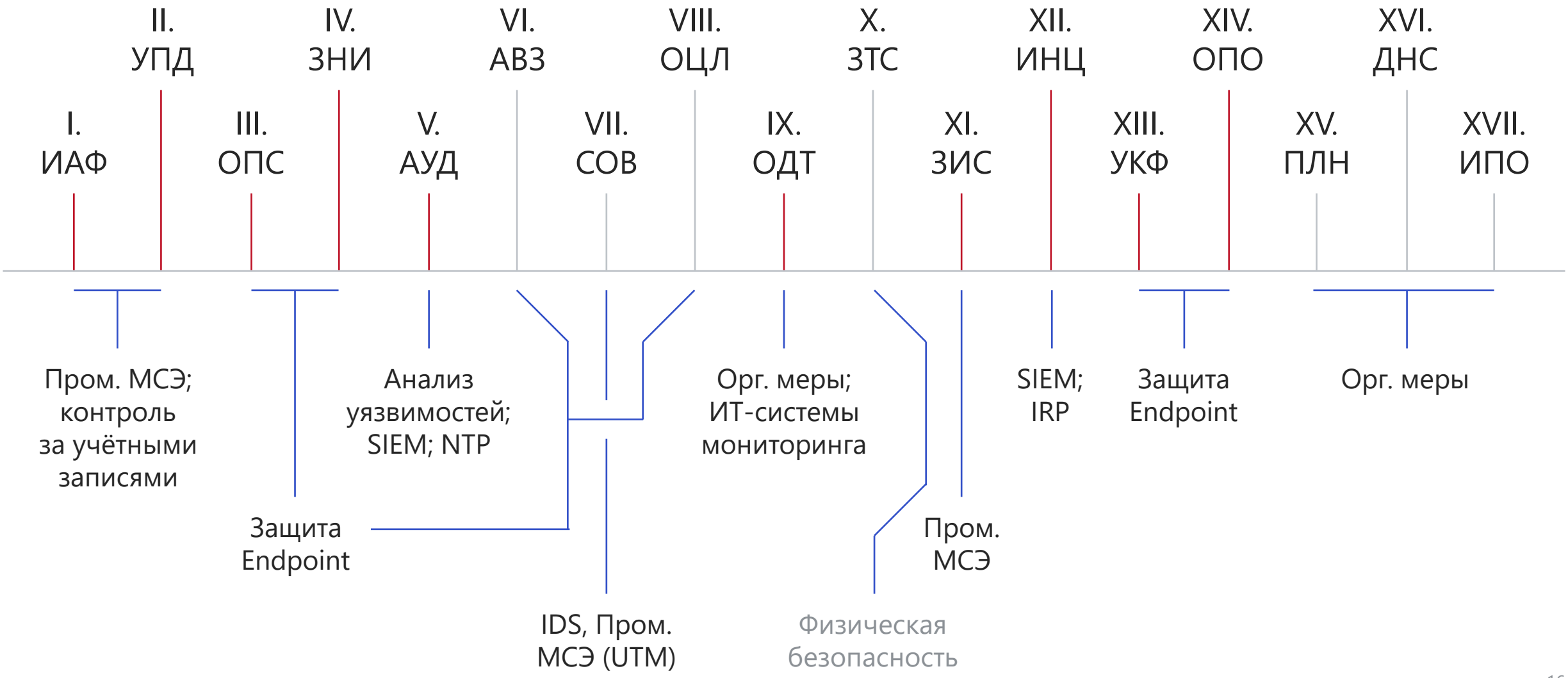
Анализ: меры обеспечения безопасности информации согласно 239 Приказу ФСТЭК России



~30% мер относятся к организационным

~70% мер требуют внедрения технологий защиты информации

Соответствие мер и классов решений



Как выбирать средства защиты

INFOWATCH® ARMA ARMA

СПАСИБО!

Игорь Душа

Заместитель генерального директора, InfoWatch ARMA

Igor.Dusha@infowatch.com

/InfoWatchOut /InfoWatch