КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Как выбрать СЗИ для исполнения приказа ФСТЭК России № 239 на АСУ ТП

Игорь Душа

Директор по развитию продуктов,
Защита АСУ ТП, InfoWatch

Ужесточение требований регулятора

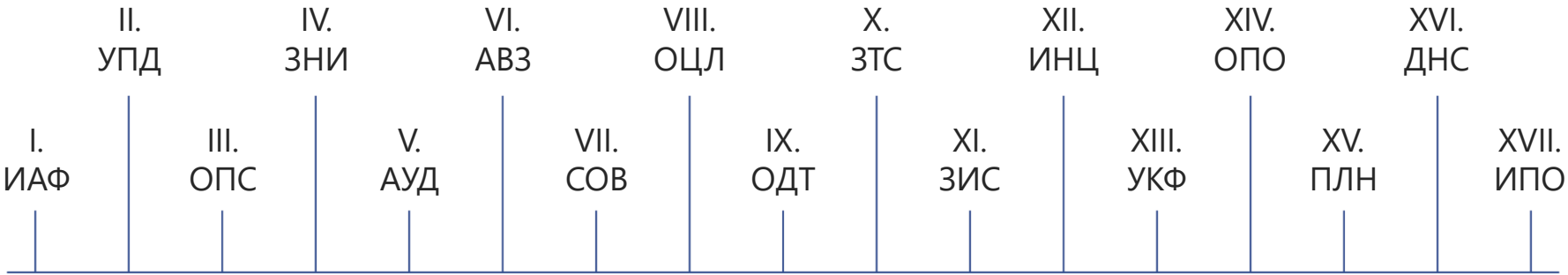
135 КОНКРЕТНЫХ МЕР

Все объекты КИИ должны быть приведены в соответствие требованиям регулятора:

Приказ ФСТЭК РФ от 25.12.17 № 239

2022 ГОД ПОКАЖЕТ...

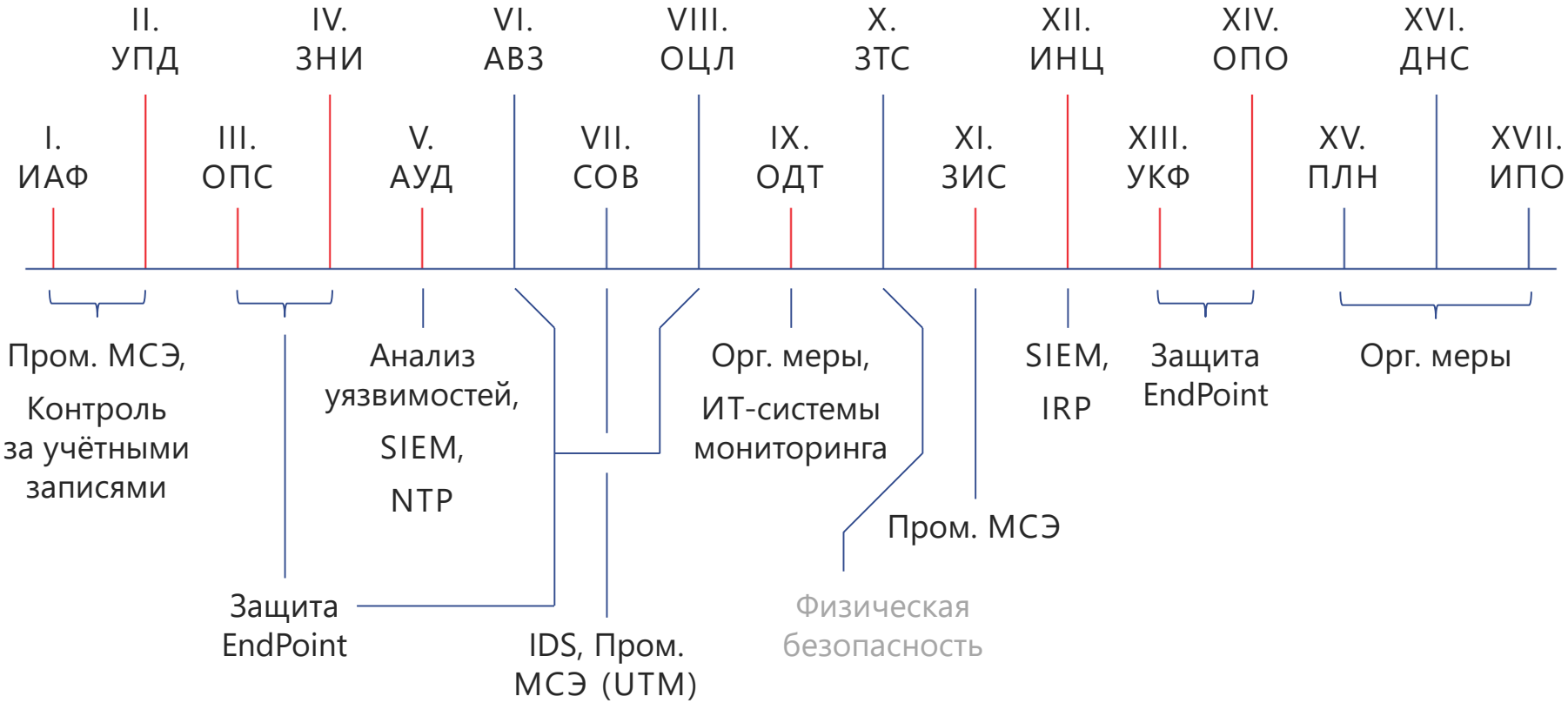
Анализ: меры обеспечения безопасности информации согласно 239 Приказу ФСТЭК



~30% мер относятся к организационным

~70% мер требуют внедрения технологий защиты информации

Соответствие мер и классов решений



Многообразие классов решений для защиты информации

Пример использования СЗИ

Состав СЗИ и их расположения зависит от модели угроз и адаптированного набора мер

Построение «гарантированной» защиты?

МИФ

- «Тотальная защита»

РЕАЛЬНОСТЬ

- Фокус: управление рисками на основе модели угроз.
- Бизнес оперирует новыми видами операционных рисков — киберриски.
- Рост зрелости в сегменте кибербезопасность АСУТП

ИАФ

Обозначение меры	Наименование меры	Возможные механизмы реализации
ИАФ.2	Идентификация и аутентификация устройств	Идентификация по IP, MAC адресам, IDM, МЭ
УПД.2	Реализация модели управления доступом	Ограничение на МЭ, СЗИ НСД, средства ОС
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	МЭ СОВ / СПВ
ЗИС.5	Организация демилитаризованной зоны	МЭ

Практические рекомендации

Промышленный МСЭ с функцией обнаружения вторжений (IDS/IPS) и маршрутизации.

1

Работает как в режиме мониторинга, так и БЛОКИРОВКИ атак на SCADA и ПЛК

2

Поддерживает промышленные протоколы:

- OPC UA
- OPC Classic
- МЭК-60870-5-104
- Modbus TCP

3

Обеспечивает отказоустойчивость: кластер Active / Passive, режим Bypass, агрегация каналов

4

Проходит сертификацию во ФСТЭК РФ по ИТ.МЭ.Д4.ПЗ и ИТ.СОВ.С4.ПЗ

Практические рекомендации

Промышленный МСЭ с функцией обнаружения вторжений (IDS/IPS) и маршрутизации.

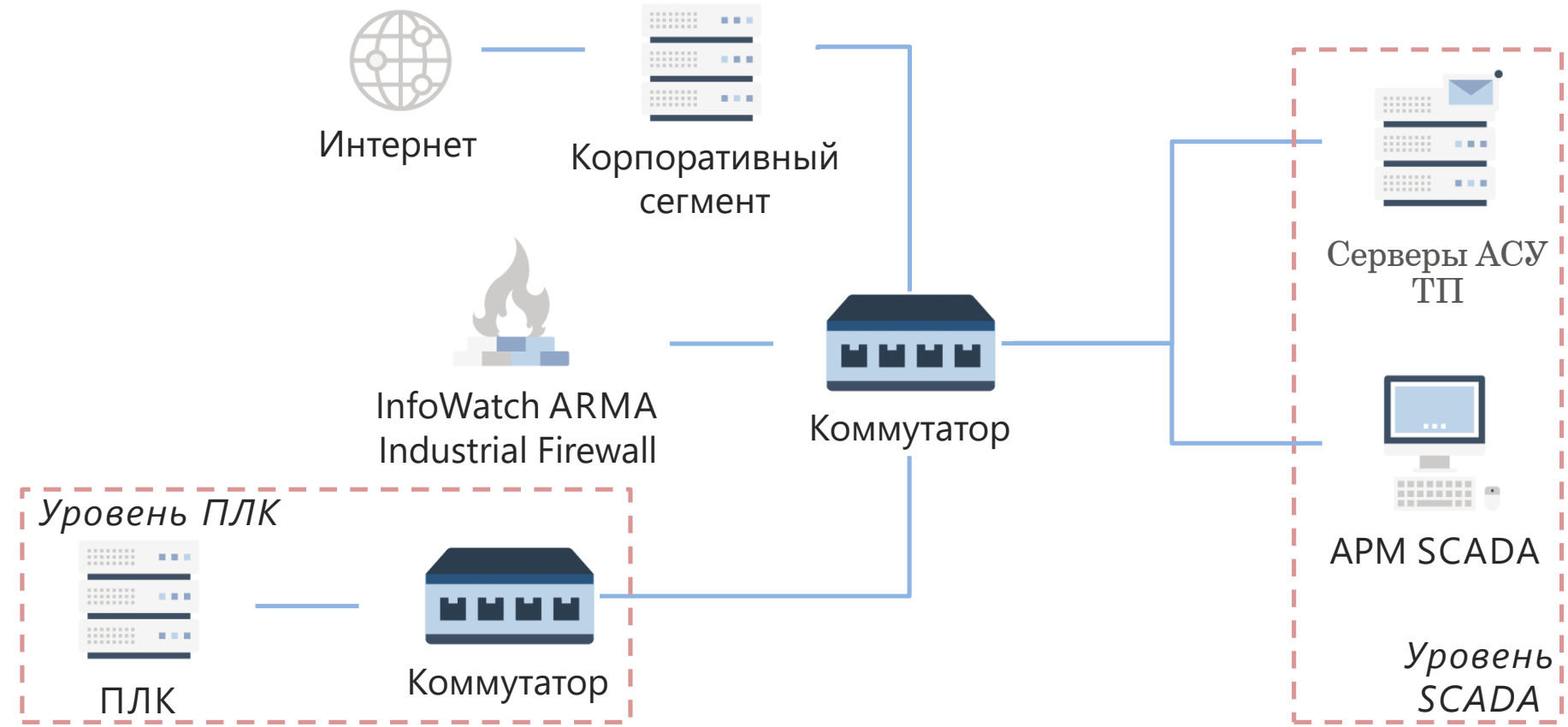
5 Работа на уровнях L2/L3

6 Статическая и динамическая маршрутизация трафика

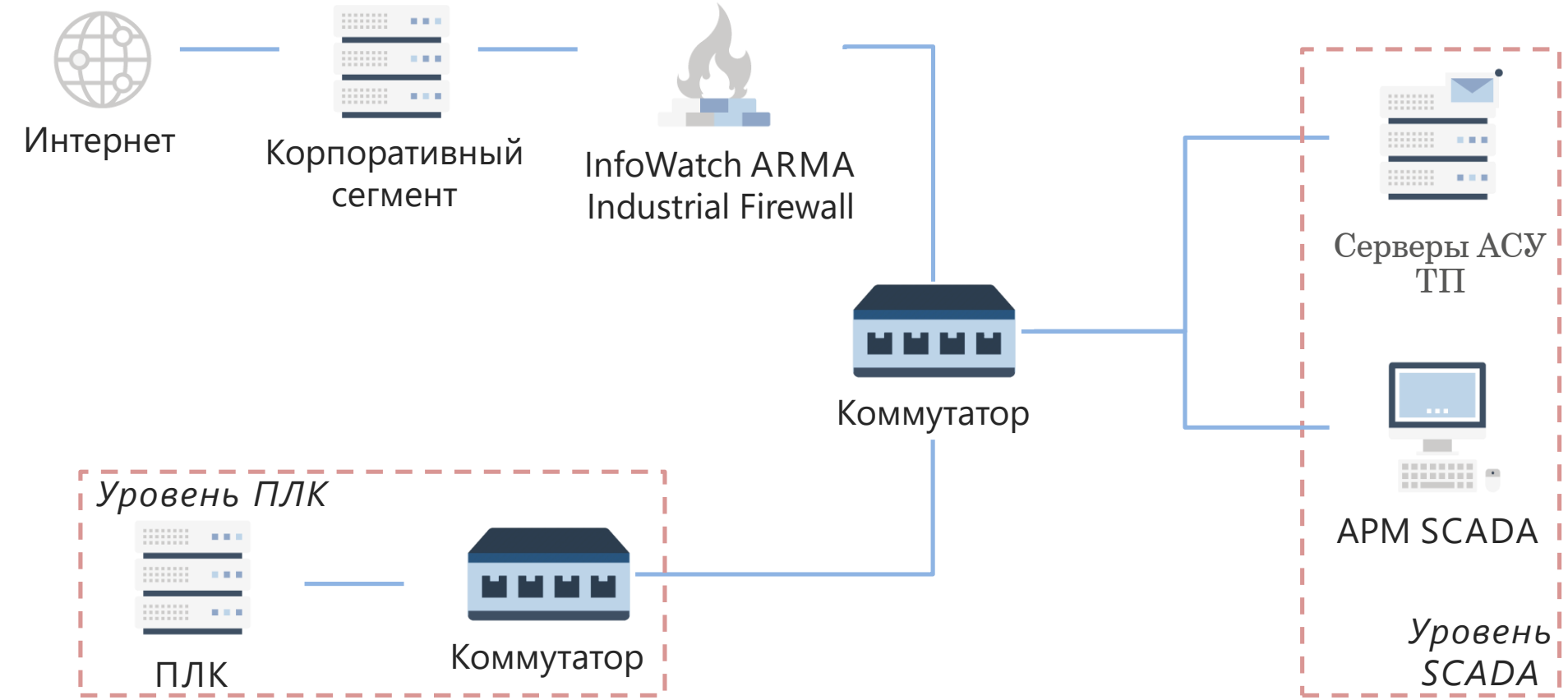
7 Поддержка Network Address Translation (NAT) и Proxy

8 Передача событий ИБ в SOC и SIEM системы

SPAN


Интернет
Корпоративный сегмент
Серверы АСУ ТП
InfoWatch ARMA Industrial Firewall
Коммутатор
АРМ SCADA
Уровень ПЛК
ПЛК
Коммутатор
Уровень SCADA

IN-Line и далее маршрутизация



Режим блокировки

Зачем

- Число уязвимостей растет ежегодно, а количество людей в отделе ИБ - нет
- Отсутствие понимания, что делать с результатами мониторинга
- Проще поставить систему, которая ограничит лишние действия и защитит

Сценарии заказчика

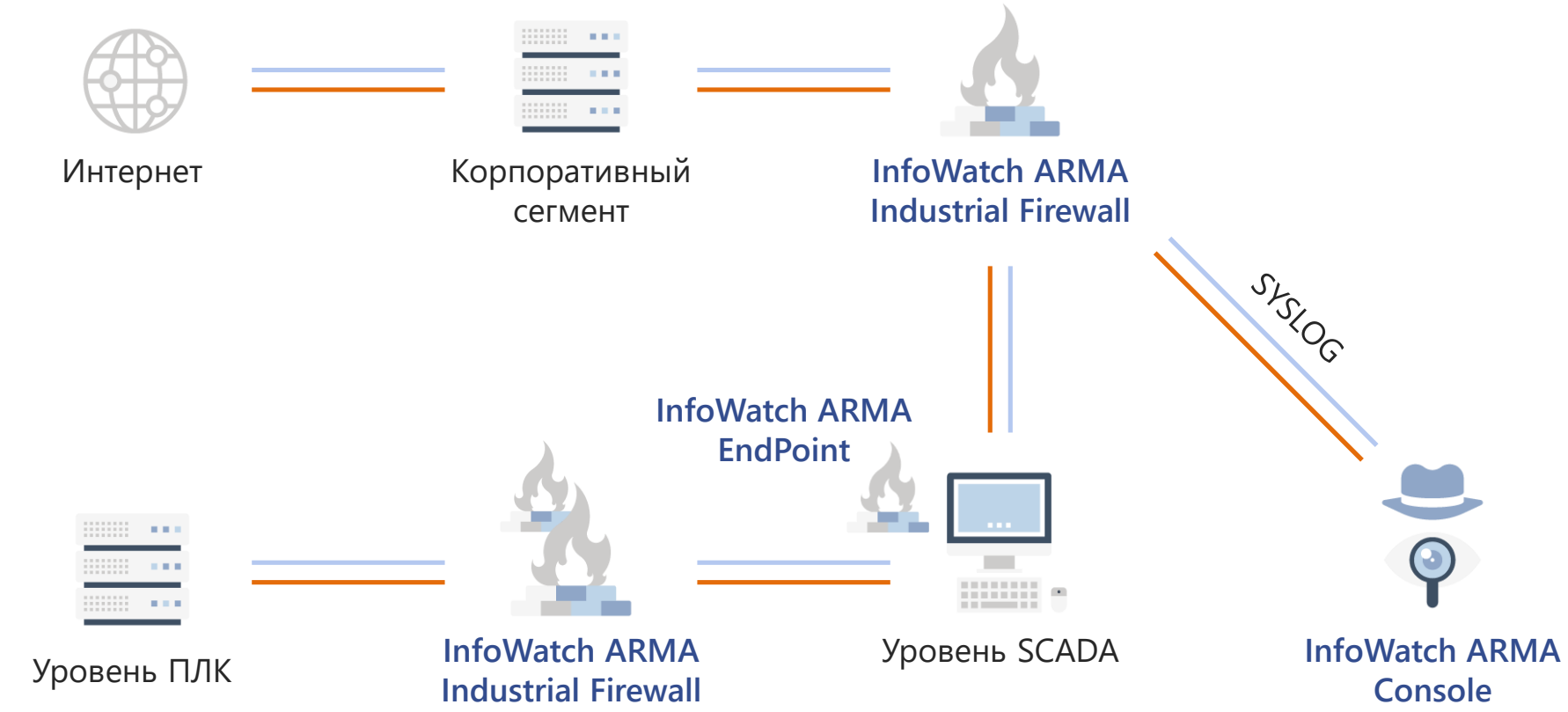
1. Разрешить прохождение только определенного типа трафика
2. Разграничить права по доступу к оборудованию

Ограничения и еще раз ограничения

Замкнутая среда в АСУ ТП — лучший вариант:

- Ограничение программной среды
- Только разрешенные информационные потоки
- Ограничение подключения к системе

Схема внедрения



#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

ИГОРЬ ДУША

Директор по развитию продуктов, Защита АСУ ТП, InfoWatch

Igor.Dusha@infowatch.com | info@infowatch.ru


КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ