КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Управление рисками

26.05.2022

Николай Казанцев

Коротко обо мне

Образование

Специалитет и аспирантура на кафедре комплексного обеспечения информационной безопасности
ГУМ РФ им. Адм. Макарова.

Опыт работы

В ИБ с 2010, работал в Лаборатории противодействия промышленному шпионажу, Администрации Санкт-Петербурга, сейчас – начальник отдела ИБ в фарм-компании ПОЛИСАН.

Полученные сертификаты

EC Council CEH, Comptia Security+, Медаль ФСТЭК за заслуги в области защиты информации

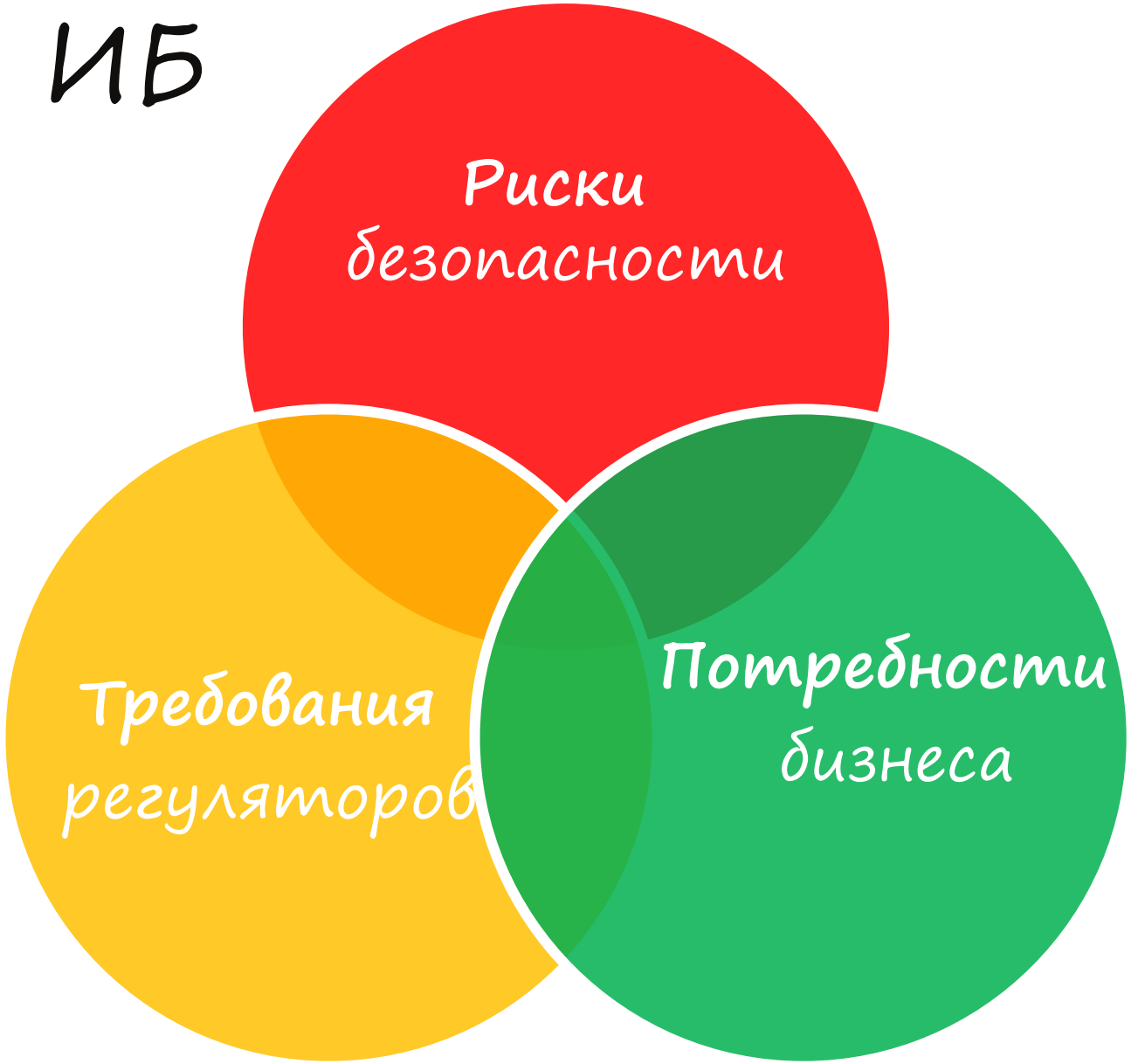
Блог spbsecurity.blogspot.com
Основатель securitm.ru

Только **15%** служб информационной безопасности сегодня ведут формализованный и повторяемый процесс управления рисками

* Результаты опроса > 50 служб безопасности

Зачем нужна ИБ ?

Зачем ИБ


Риски безопасности
Требования регуляторов
Потребности бизнеса

Что такое риск ИБ ?

Сочетание вероятности нанесения ущерба и тяжести этого ущерба

ГОСТ Р 51898-2002

Вероятность причинения ущерба сети электросвязи или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в сети электросвязи.

ГОСТ Р 52448-2005

Сочетание вероятности события и его последствий

ГОСТ Р 51901.1-2002

Влияние неопределенности на цели

ISO/IEC 27000:2018

Риск ~ ущерб

Методика оценки угроз ФСТЭК от 05.02.2021

Потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации.

ГОСТ ИСО/МЭК 27000-2012

Вероятность того, что угрозы будут реализовываться с использованием уязвимостей информационных активов или групп информационных активов и, тем самым, наносить ущерб организации

ISO/IEC 27000:2018

Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов. Определяется как сочетание вероятности события и его последствий.

ГОСТ Р ИСО/МЭК 13335-1-2006

УГРОЗЫ

- Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (*ГОСТ Р 50.1.056-2005)*
- Потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации (*ГОСТ Р ИСО/МЭК 27002-2012)*
- Потенциальный источник опасности, вреда и т.д. (*ГОСТ Р 58771-2019)*

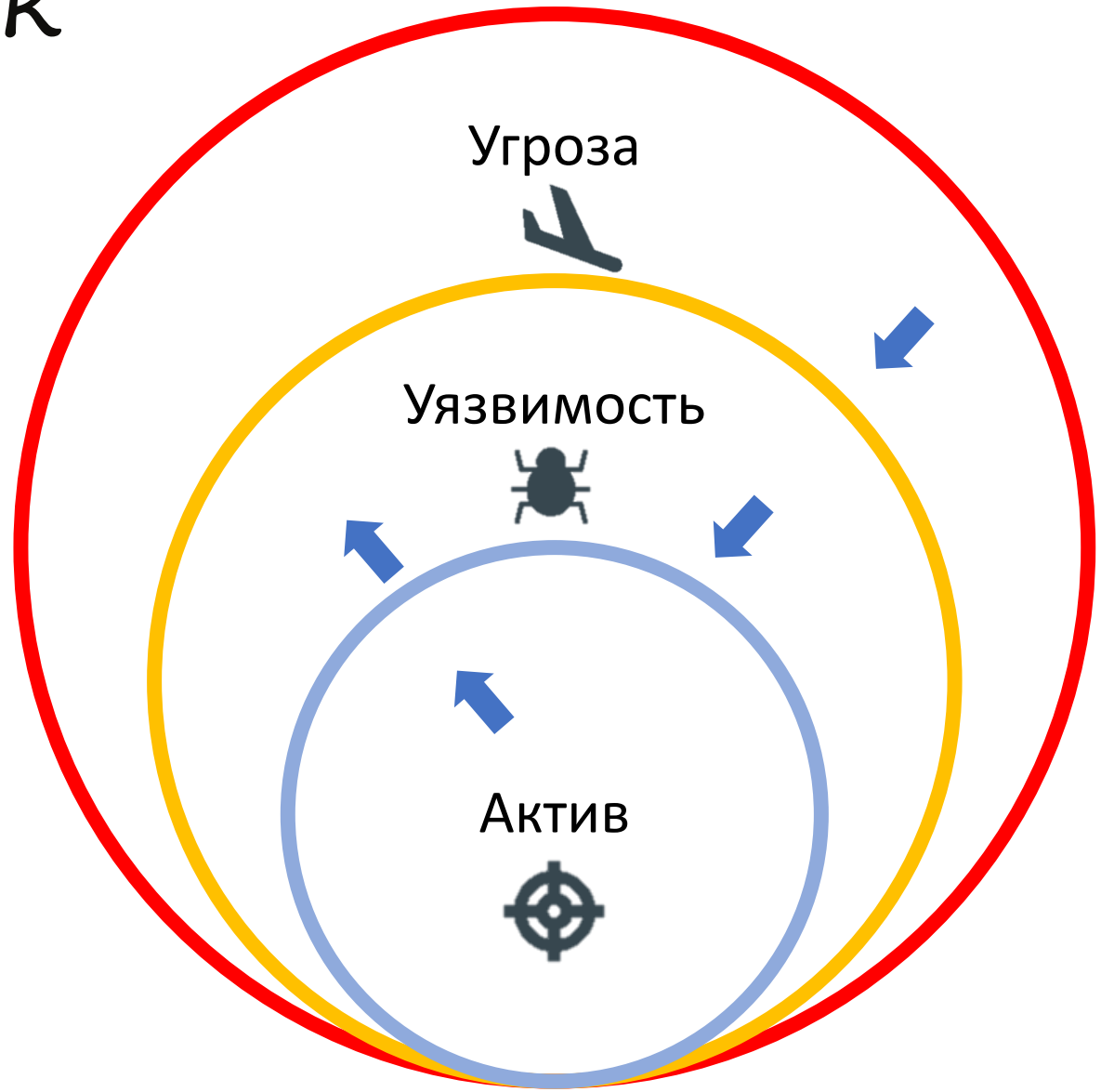
= Что то плохое

= Свойство актива

УЯЗВИМОСТИ

- Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами (*ГОСТ Р ИСО/МЭК 27002-2012*)
- Свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации (*Р 50.1.056-2005, ГОСТ Р 50922-2006*)
- Недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации (*МУ ФСТЭК*)

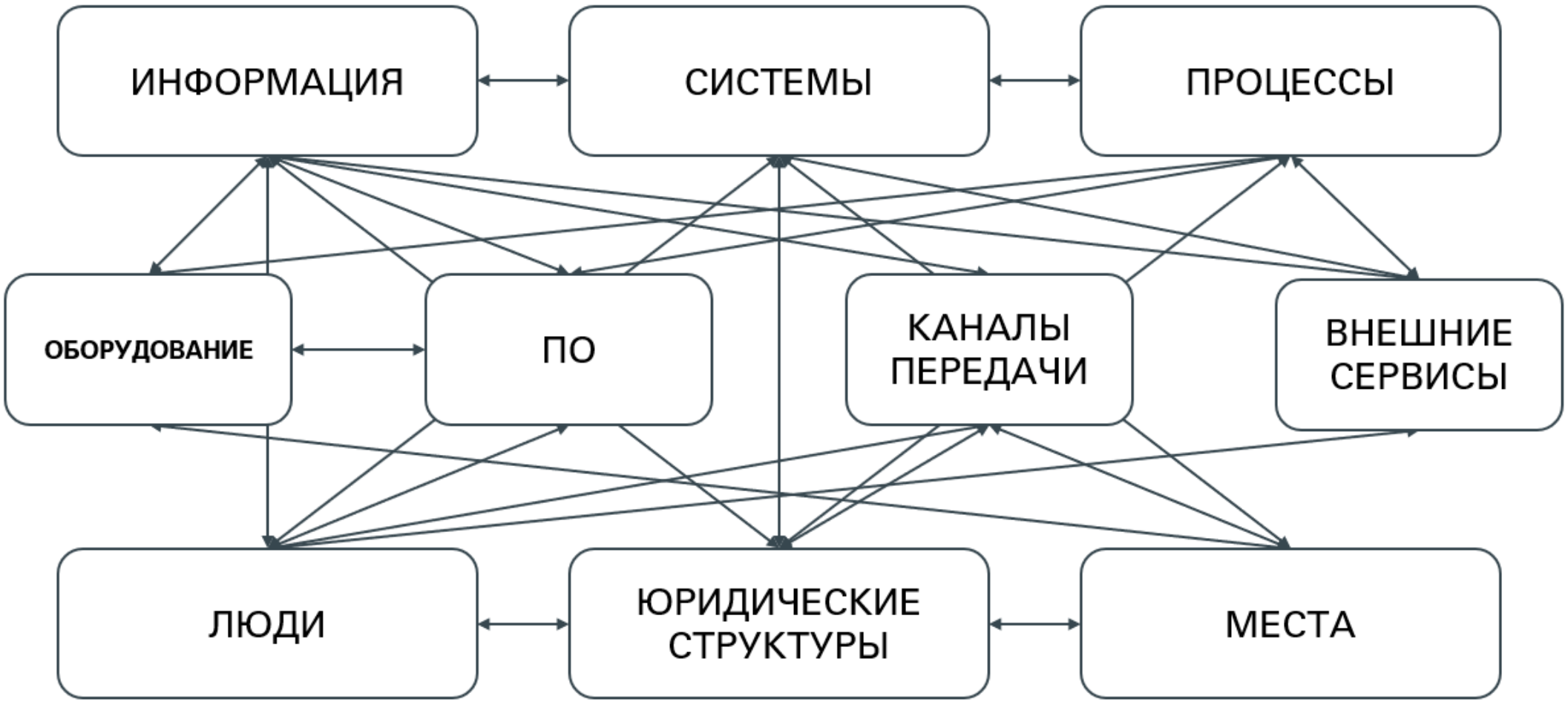
Риск



Возможность реализации **угрозы** через использование **уязвимости** в группе **активов**

Какие активы вы контролируете?

Типы активов



ТИПЫ АКТИВОВ КЛАССИФИКАЦИЯ

- Физические серверы
- Вычислительные комплексы (Blade системы)
- Компьютеры
- Системы хранения данных
- Электронные носители информации
  - Встроенные носители информации
    - НЖМД
    - SSD
    - NVMe
  - Съемные носители информации
    - USB-токены
    - USB flash drive
    - Съемный HDD
- Сетевое оборудование
  - Коммутаторы
  - Маршрутизаторы
  - Беспроводные точки доступа
- IP телефоны
- Мобильные устройства
- Средство антивирусной защиты
- Веб-сайты

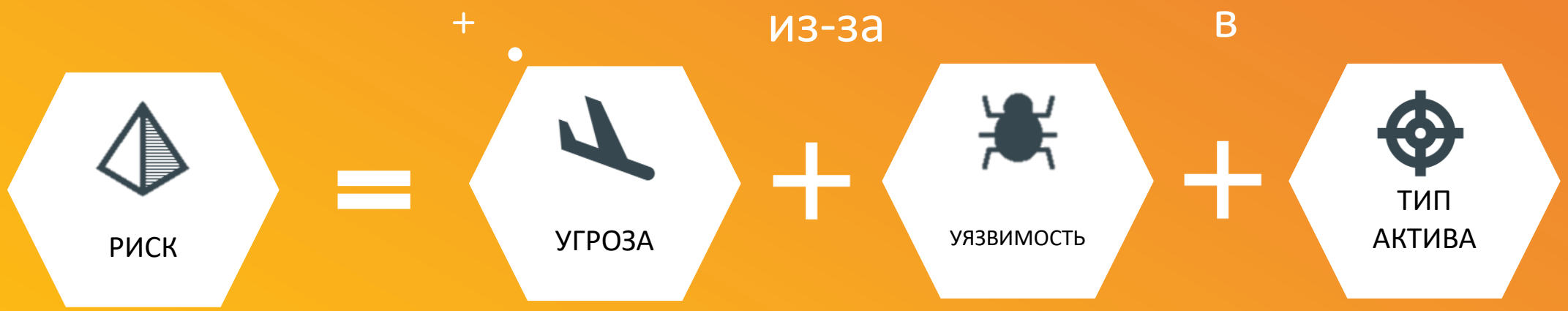
Внешние сервисы

- Облачный сервис
  - SaaS
    - Облачное хранилище
    - Microsoft Office 365
  - IaaS
    - Microsoft Azure
  - PaaS
    - Amazon Web Services
    - Google Cloud Platform
- Интернет-провайдер

Процессы

- Операционный бизнес-процесс
- Управляющий бизнес-процесс
- Поддерживающий бизнес-процесс

Риск это

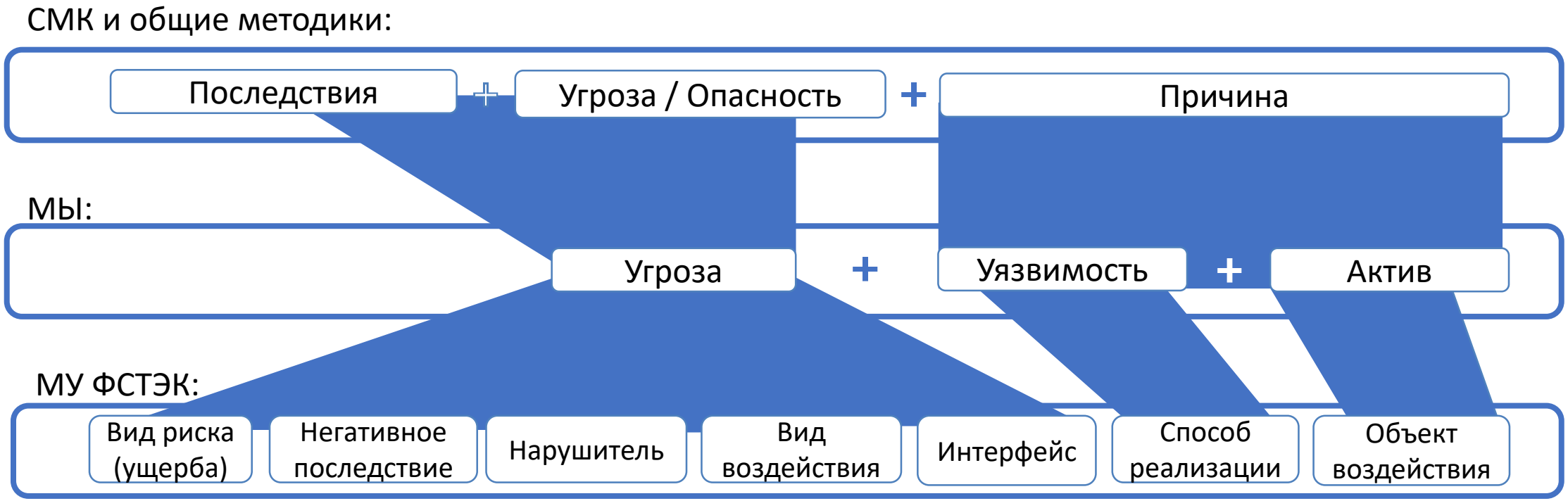


Примеры

Риск **неработоспособности серверного оборудования** из-за **нарушения температурного режима** в **серверном помещении**

Неработоспособность серверного оборудования	Нарушение температурного режима	Серверное помещение
Перехват данных, передаваемых по локальной сети	Возможность проведения атаки DNS cache poisoning	DNS сервер
Нарушение установленных политик информационной безопасности	Отсутствие ознакомления с политиками информационной безопасности	Работник
Перехват управления социальными сетями	Возможность подбора пароля путем перебора	Представительство в социальных сетях

Как бывает


СМК и общие методики:
Последствия
+
Угроза / Опасность
+
Причина
МЫ:
Угроза
+
Уязвимость
+
Актив
МУ ФСТЭК:
Вид риска (ущерба)
Негативное последствие
Нарушитель
Вид воздействия
Интерфейс
Способ реализации
Объект воздействия

Риск, угроза или уязвимость?

Возможность отзыва
лицензий
производителем ПО

Риск, угроза или уязвимость?

Кража оборудования

Риск, угроза или уязвимость?

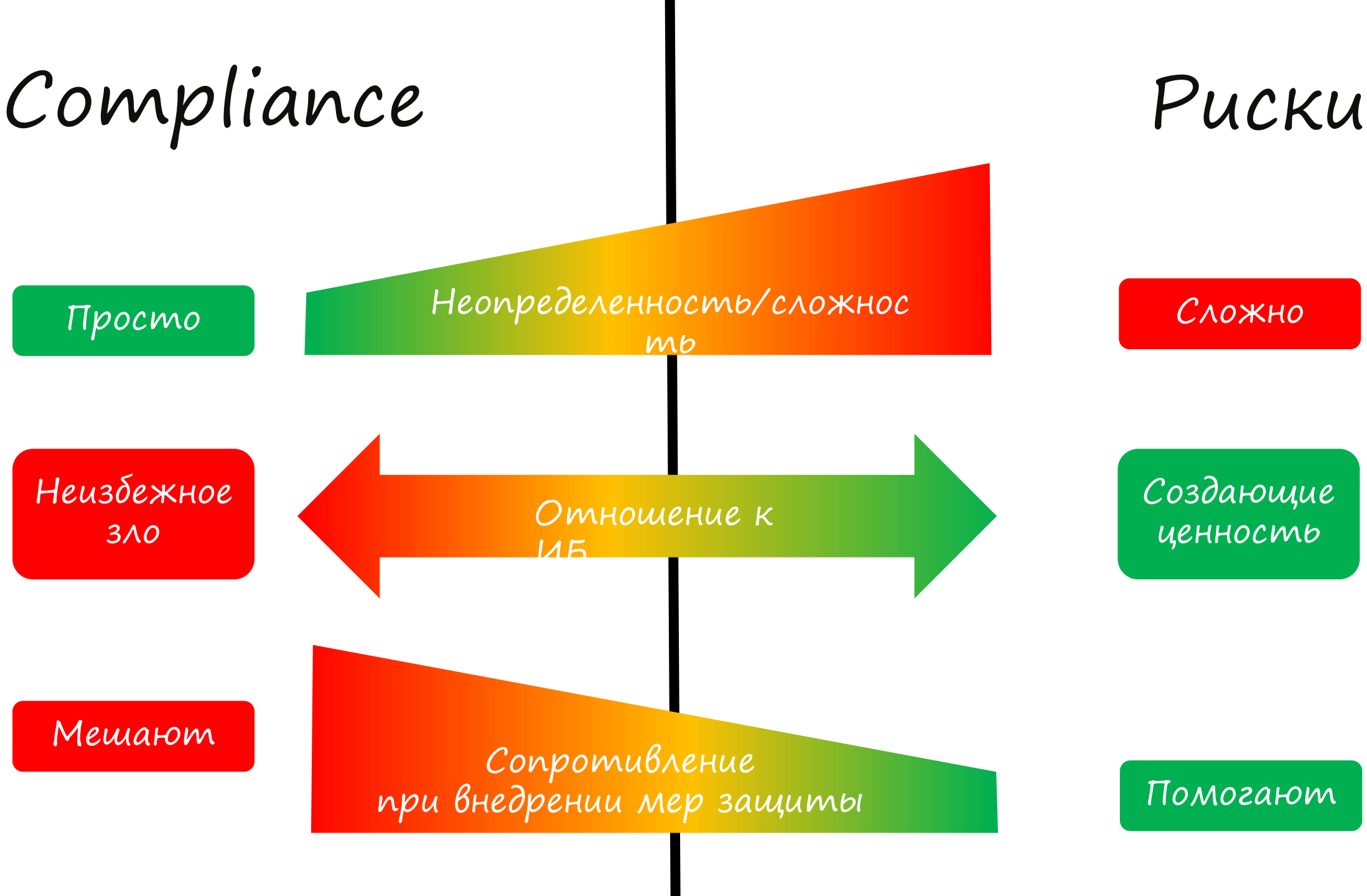
Потеря смарт-карты
(ключа доступа)

Риск, угроза или уязвимость?

Горизонтальное перемещение злоумышленника по локальной сети из-за использования WMI в ОС Windows

Зачем управлять рисками ИБ ?


Где
копать?


Compliance
Риски
Просто
Неопределенность/сложность
Сложно
Неизбежное зло
Отношение к ИБ
Создающие ценность
Мешают
Сопротивление при внедрении мер защиты
Помогают

Немного теории

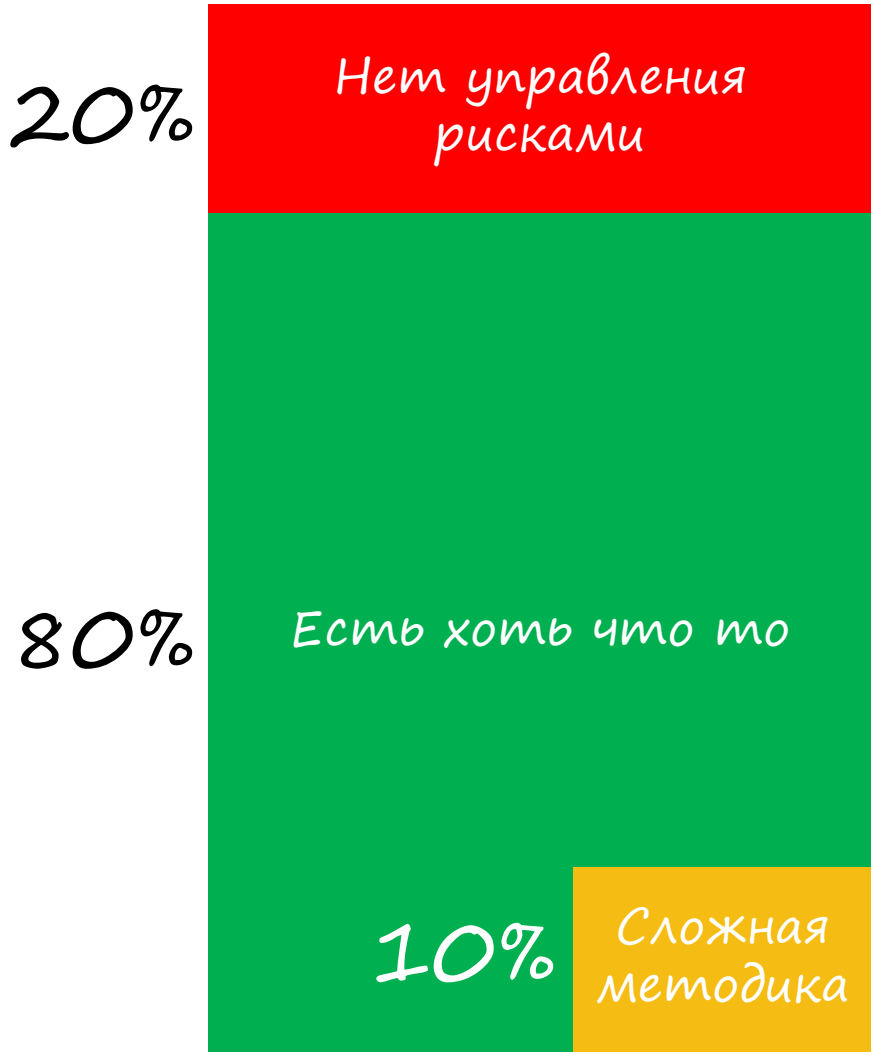
ПРОБЛЕМЫ УПРАВЛЕНИЯ РИСКАМИ

- **Нет методологии/инструмента**
  Непонятно как управлять рисками
- **Нет данных**
  Долго и сложно сформировать полный реестр рисков компании
- **Нет понимания**
  Риски ИБ это птичий язык для бизнеса
- **Много рутины**
  Мотивации и сил не хватает на регулярный пересмотр и контроль

Методики

Стандарты и регуляторика
ISO/IEC 27005, ISO/IEC 31000, NIST SP 800-*, Методика МУ ФСТЭК 2021, РС БР ИББС-2.2-2009, Положение 716-П Банка России

Методики
FRAP, OCTAVE, FAIR, CRAMM, RiskWatch, Дельфи, FMEA, FMECA, HAZOP, FTA, ETA … > **1000**



Инструменты

Excel / Access

Free ISO27k Toolkit ,
Risk Assessment Template,
...

Eng SaaS

VComply,
CyberComply,
Eramba, vsRisk,
ISMS.online

Ru SaaS/ПО

SECURITM.ru

Ru Enterprise ПО

R Vision, Security Vision,
E-Plat4m

Критерии выбора

- Простота
- Интеграция в процессы ИБ
- Локализация (регуляторика РФ)
- Стоимость

ПРОБЛЕМЫ УПРАВЛЕНИЯ РИСКАМИ

- **Нет методологии/инструмента**
  Непонятно как управлять рисками
- **Нет данных**
  Долго и сложно сформировать полный реестр рисков компании
- **Нет понимания**
  Риски ИБ это птичий язык для бизнеса
- **Много рутины**
  Мотивации и сил не хватает на регулярный пересмотр и контроль

Специфичные для компании риски

20%

Каталоги угроз

80%

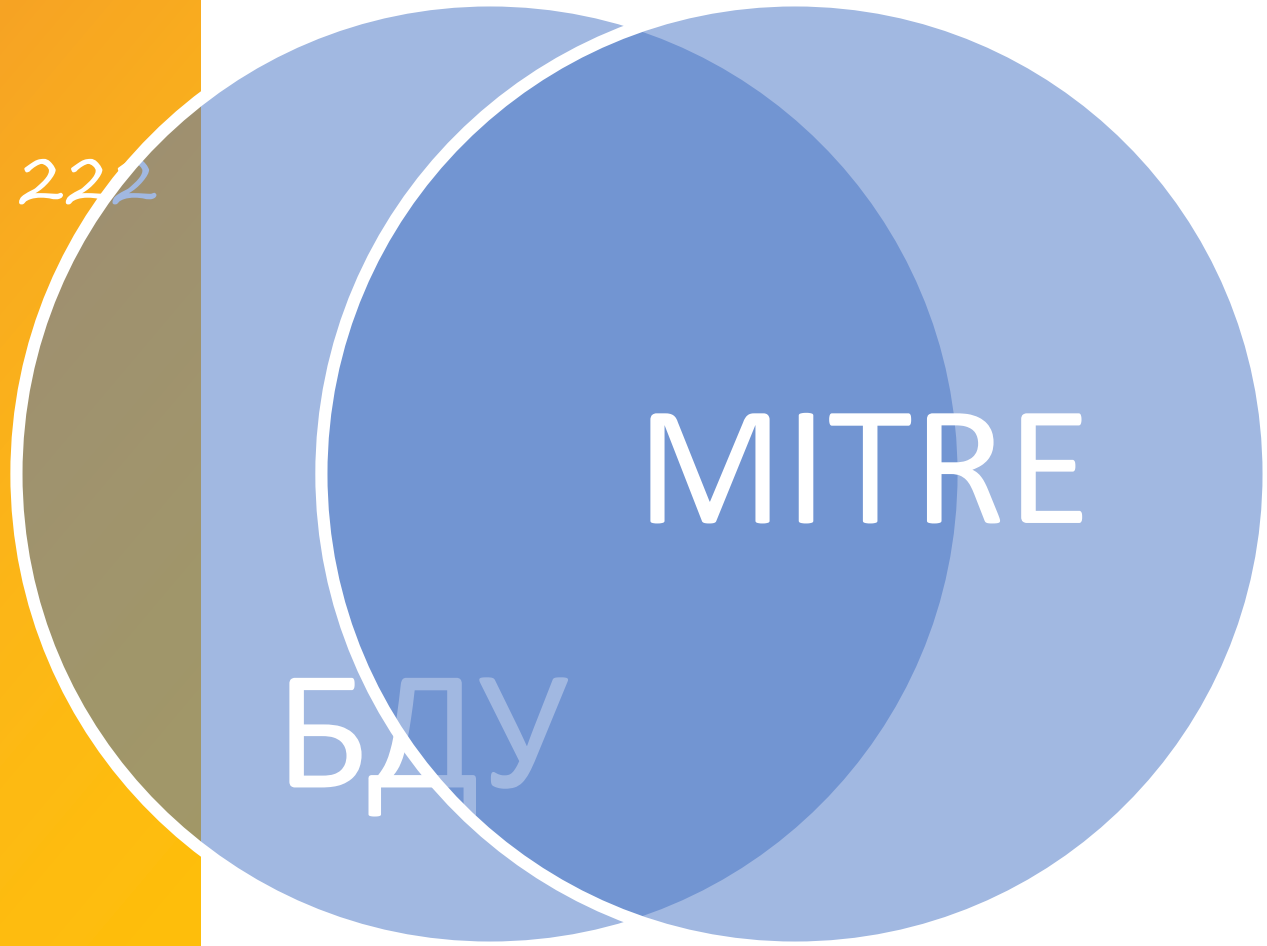
Каталоги и базы знаний – основа для реестров рисков, но:

- Каталогов **много**
- Каталоги **разные**
- Как использовать в работе?

ПОХОЖИЕ ОБЪЕКТЫ

БДУ ФСТЭК 222
MITRE ATT&CK 567

- 40 - 43% объектов уникальны
- 57-60% пересечений



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб

Вид

УБИ.099: Угроза обнаружения хостов

Вид

УБИ.104: Угроза определения топологии вычислительной сети

Вид

Раскрытие информации об ИТ инфраструктуре

Возможность сканирования IP адресов

Локальная сеть

информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика).

Раскрытие информации об ИТ инфраструктуре

Возможность сканирования IP адресов

Публичный IP-адрес

Объект воздействия	Сетевой узел, сетевое программное обеспечение, сетевой трафик
Последствия реализации угрозы	Нарушение конфиденциальности

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques

Home > Techniques > Enterprise > Network Service Scanning

Network Service Scanning

Home > Techniques > Enterprise > Gather Victim Network Information > Network Topology

Gather Victim Network Information: Network Topology

Home > Techniques > Enterprise > Active Scanning

Active Scanning

Sub-techniques (2)

ID	
T1595.001	
T1595.002	

ID: T1595

Раскрытие информации об ИТ инфраструктуре

Возможность сканирования IP адресов

Локальная сеть

Раскрытие информации об ИТ инфраструктуре

Возможность сканирования IP адресов

Публичный IP-адрес

Version: 1.0

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary prob
interaction.

Adversaries may p
performed in vario
opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

Угрозы | Уязвимости | Документы | Термины

Поиск

Главная / Раздел угроз

В настоящее время

Замечания и предло

ктронной почты.

УБИ.8 Угроза нарушения нкционирования отоспособности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

1

УБИ.11 Угроза несанкционированного массового сбора информации

3

- СП.8.1 Обнаружение открытых портов
- СП.8.2 Обнаружение сетевых служб
- СП.8.3 Обнаружение устройств
- СП.8.4 Идентификация программного обеспечения и его версий с целью поиска уязвимостей
- СП.8.5 Идентификация пользователей
- СП.8.6 Обнаружение доступных общих сетевых каталогов
- СП.8.7 Обнаружение

2

П.1 Эксплуатация уязвимостей 2

СП.2 Испол нед конф

2 Использование недостатков конфигурации 11

СП.3.2 Эк недост децентрали неконтро подключения к

СП.4 Внедрение вредоносного программного обеспечения 12

СП.5 Внедрение программных и атных закладок 8

СП.8 Сканирование сетевой инфраструктуры 8

СП.9 Изучение информации о системе 8

Использование недостатков архитектуры 12

СП.4 Внедрение вредоносного 12

СП.13 Реализация социальной инженерии 8

СП.18 Использование 2

УБИ.1 Угроза утечки информации

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

роза ния ования обности)

УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации

СП.1 Эксплуатация уязвимостей 2

СП.2 Использование недостатков конфигурации 11

СП.3 Использование недостатков архитектуры 2

СП.2.2 Использование недостатков, связанных с управлением учетными данными

СП.3.2 Эксплуатация недостатков, децентрализованного и неконтролируемого подключения к сети Интернет

СП.4 Внедрение вредоносного программного обеспечения 12

пример

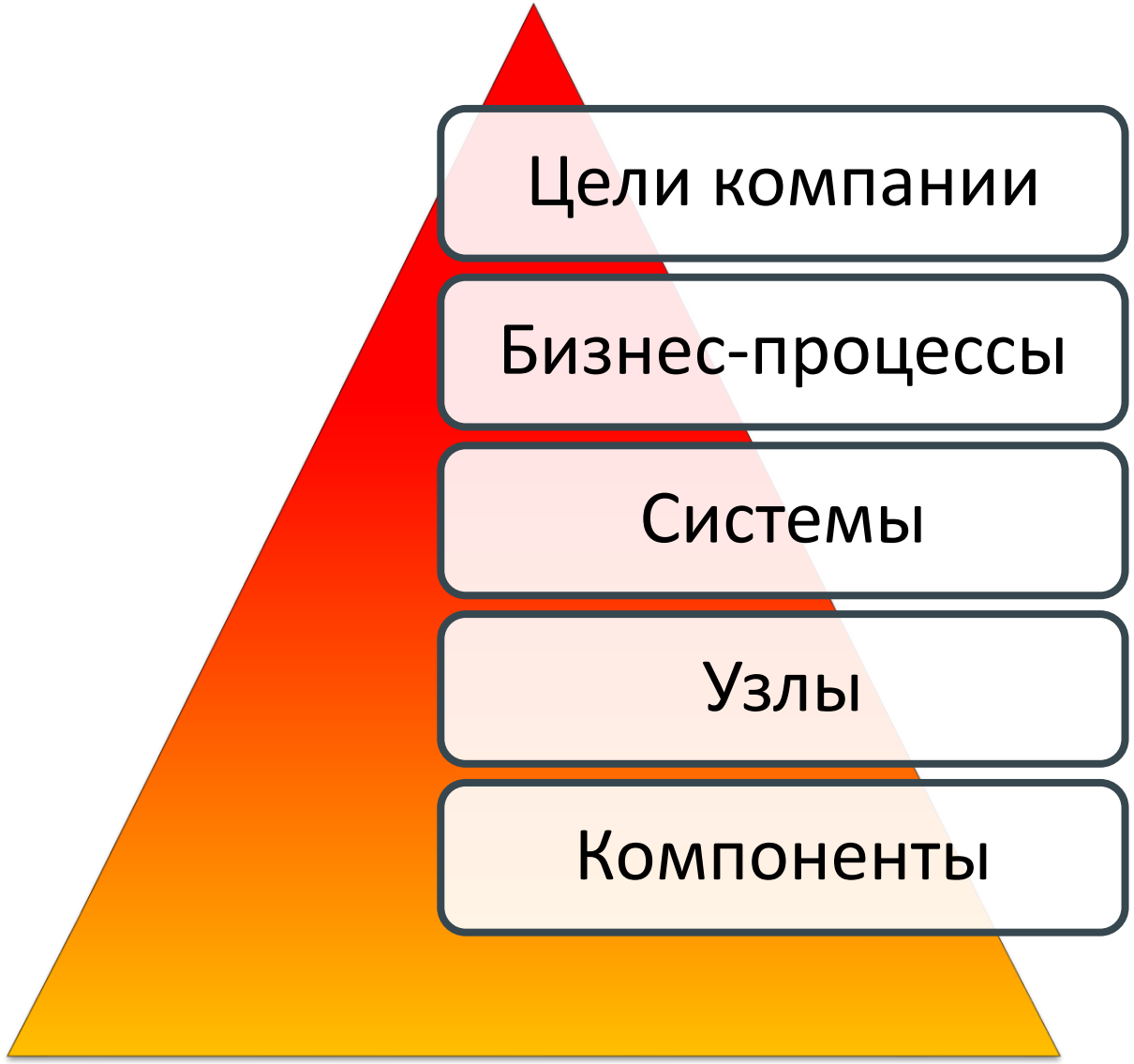
УБИ.2.1.1 Угроза несанкционированного доступа к автоматизированному рабочему месту за счет эксплуатации уязвимостей

ПРОБЛЕМЫ УПРАВЛЕНИЯ РИСКАМИ

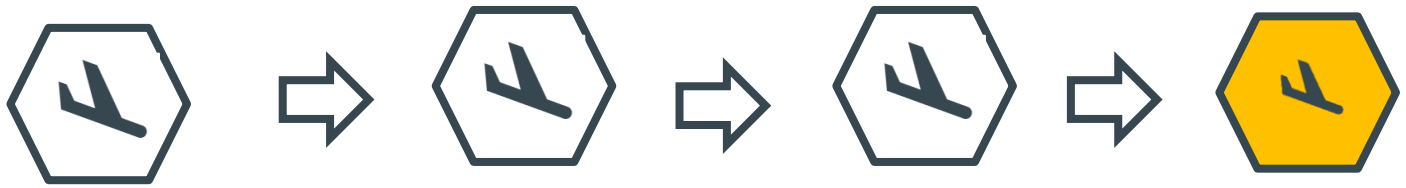
- Нет методологии/инструмента
  Непонятно как управлять рисками
- Нет данных
  Долго и сложно сформировать полный реестр рисков компании
- **Нет понимания**
  Риски ИБ это птичий язык для бизнеса
- Много рутины
  Мотивации и сил не хватает на регулярный пересмотр и контроль


Деньги
Деньги
Деньги
CVE
Lateral
Movement
SQL injection
Exploit
DDOS
Spoofing
!!!!!

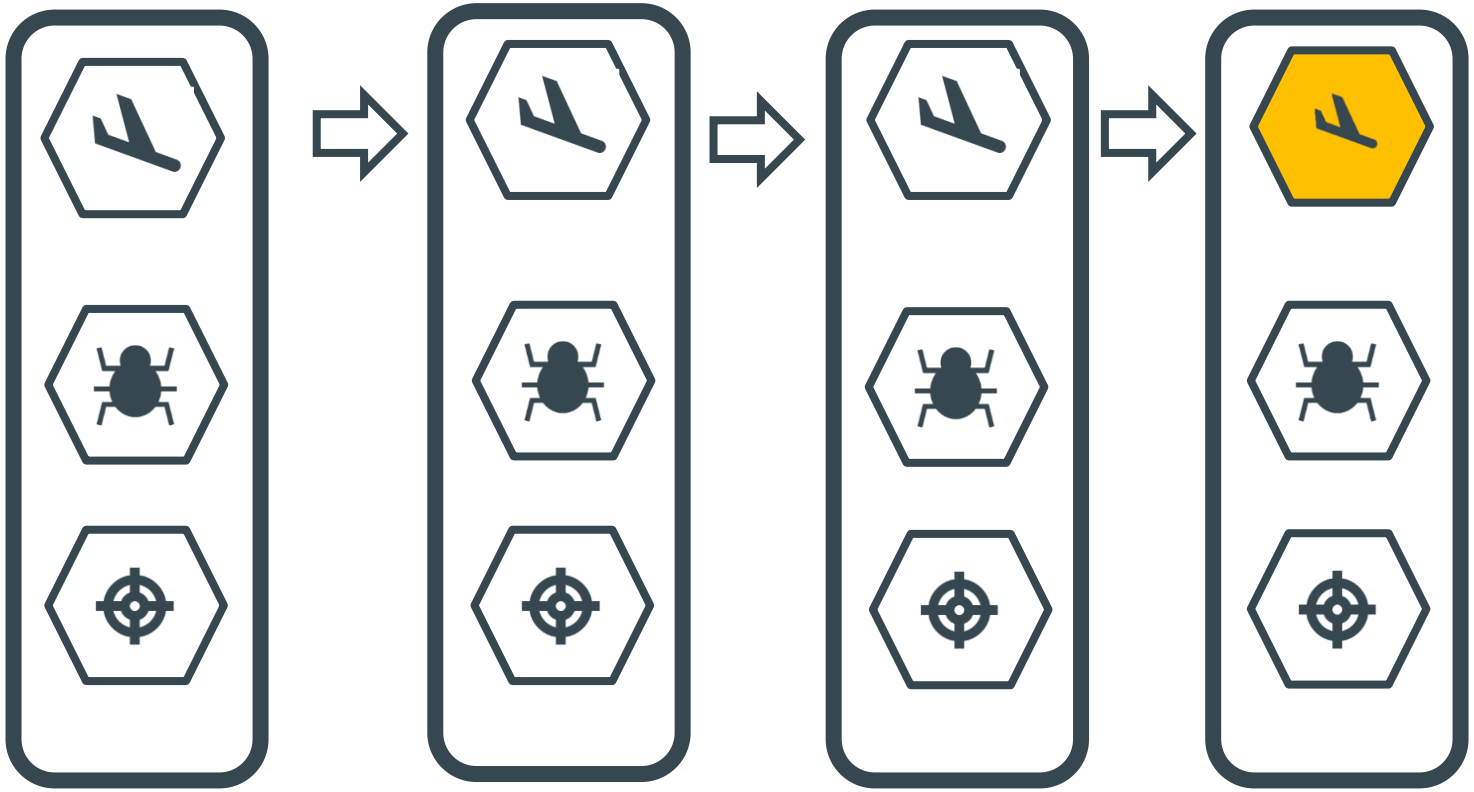
Уровни



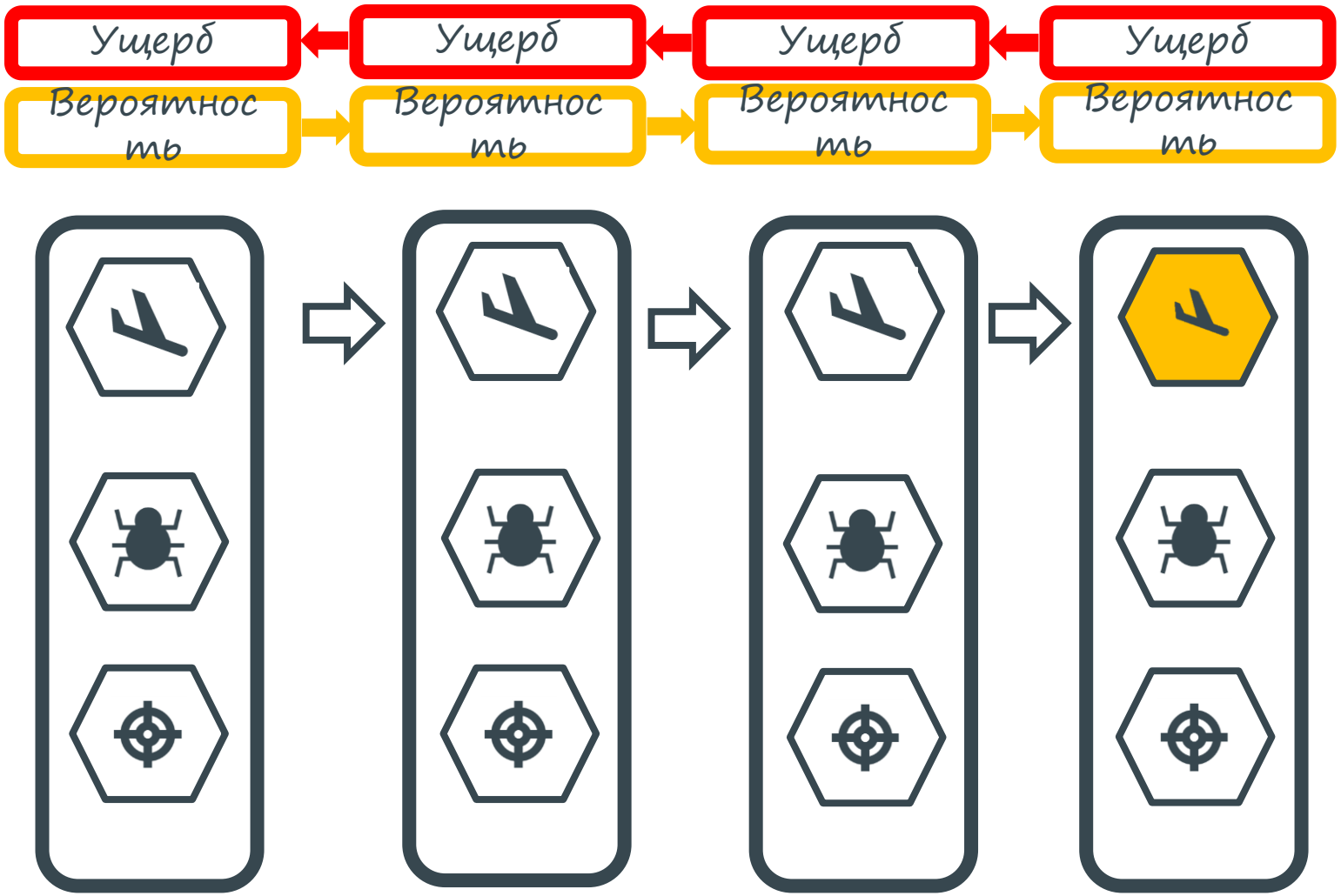
Цепочка угроз



Цепочка угроз



Цепочка угроз



Оценка риска

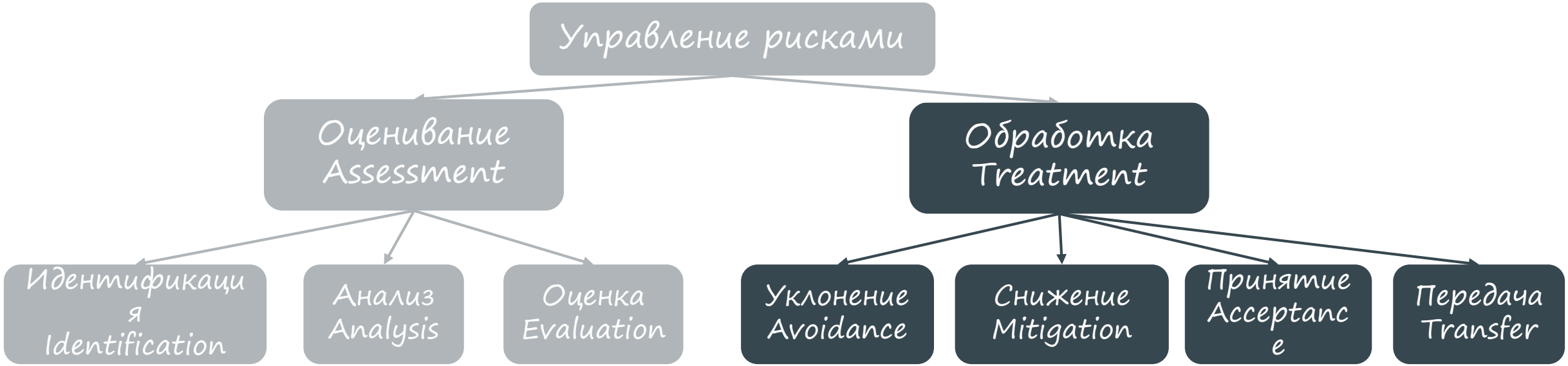
Базовая оценка
на уровне отдельных
угрозы, уязвимости,

›

Переоценка
на уровне рисков
на уровне

›

Дополнение
Через цепочки угроз
Через связь активов


Управление рисками
Оценивание
Assessment
Обработка
Treatment
Идентификация
Identification
Анализ
Analysis
Оценка
Evaluation
Уклонение
Avoidance
Снижение
Mitigation
Принятие
Acceptance
Передача
Transfer

Защитные меры = все что угодно

ЗАДАЧА ИБ

СНИЖАТЬ РИСКИ
информационной безопасности

ИСПОЛНЯТЬ ТРЕБОВАНИЯ
регуляторов и стандартов

ЗАКРЫВАТЬ ПОТРЕБНОСТИ
заинтересованных сторон

Защитные меры

Карточка

- Название/Описание/Инструкции
- Ответственный
- Инструменты
- Периодичность
- Классификация
- Способ реализации
- Влияние на риски
- Влияние на требования
- Статус

Периодичность
- Разово
- Постоянно
- По событию
- Периодически

Способ реализации
- Автоматически
- Вручную

Классификация
- Организационная
- Техническая
- Физическая
- Превентивная
- Детективная
- Корректирующая
- Восстанавливающая
- Удерживающая
- Компенсирующая

СТАТУС
Не определен > Потребность > Проект > Внедрение > Реализовано > Поломка > Отменено

Защитные меры

Пример

Использование на части серверов и ПК альтернативного средства антивирусной защиты

Тип

Техническая
Превентивная
Компенсирующая

Реализация

Автоматически

Периодичность

Постоянно

Ответственный

Администратор АВЗ

Инструменты

АВЗ Kaspersky

Риски	Требования
4	7

Проведение рассылки по информационной безопасности

Тип

Организационная
Удерживающая

Реализация

Вручную

Периодичность

Ежемесячно

Ответственный

Отдел ИБ

Инструменты

-

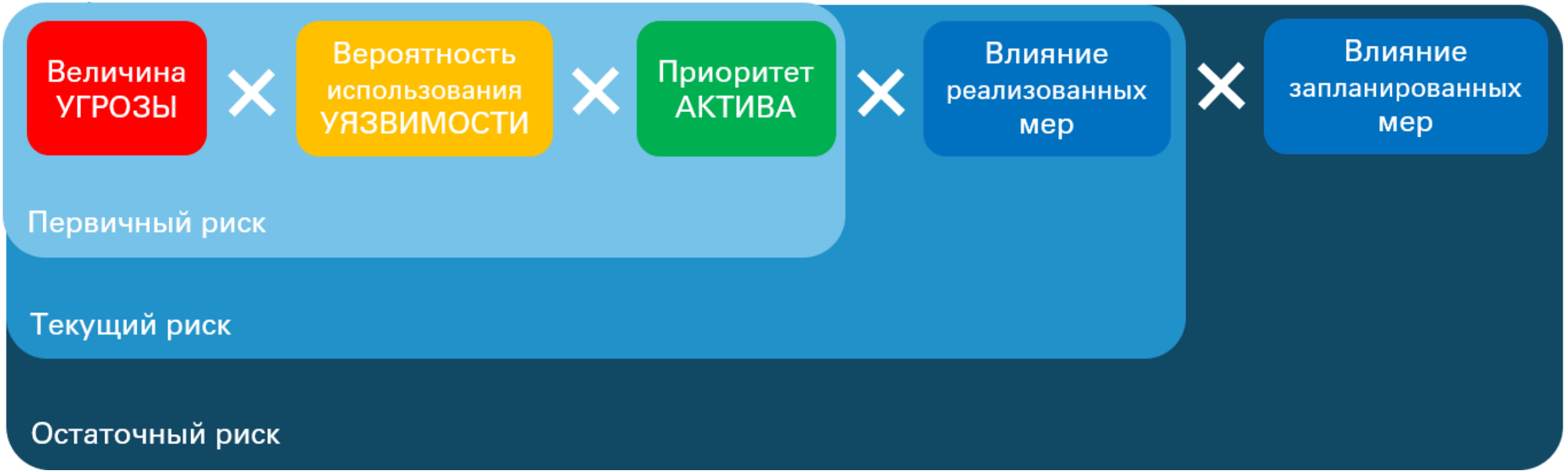
Риски	Требования
8	3

Что не является защитной мерой?

Защитные меры

Влияние на риск

Снижение величины угрозы и/или вероятности: низкое, среднее, высокое, полно



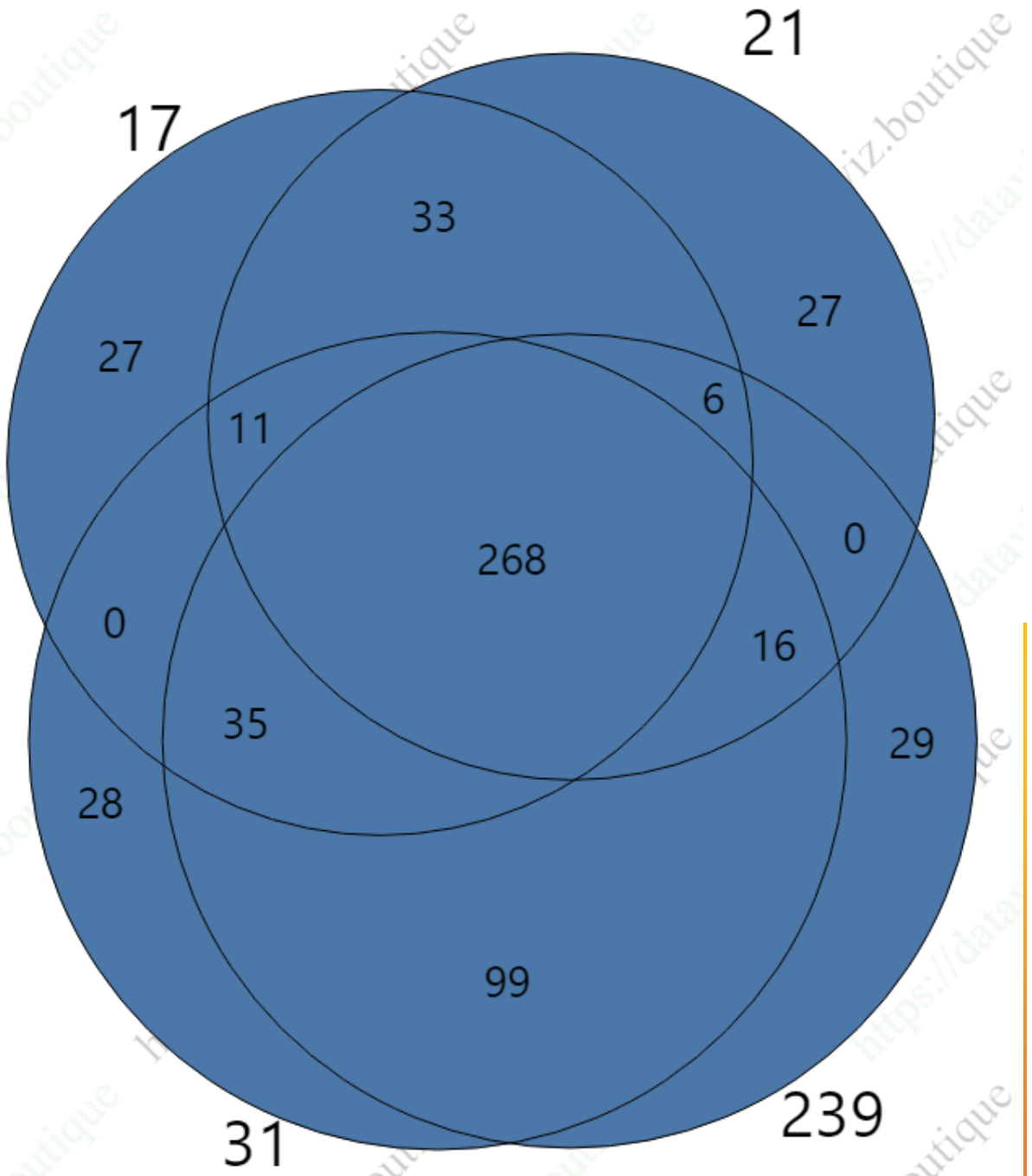
Немного про Compliance

- **Требований много**
  и документы дублируют друг друга, приходится делать одинаковую работу для разных документов
- **Нет конкретики**
  как исполнять требования ?
- **Нет смысла**
  Не понятны причины, лежащие в основе многих требований
- **Много рутины**
  Контролировать и подтверждать соответствие требуется регулярно

ПРИКАЗЫ ФСТЭК

№21	107
№17	113
№31	149
№239	145

- 20%-25% требований **уникальны**
- 75-80% требований **повторяются** хотя бы раз
- 46% - 62% **одинаковы** во всех приказах

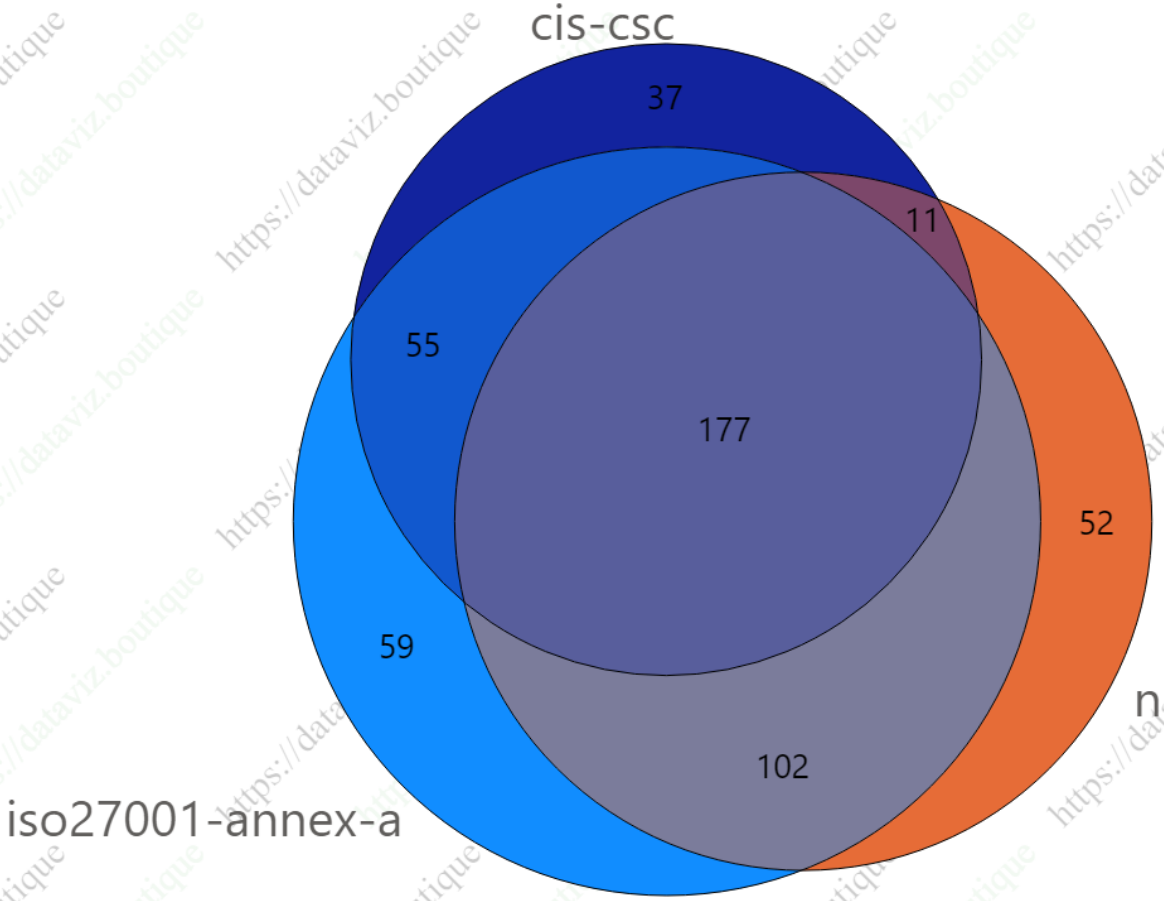


МЕЖДУНАРОДНЫЕ СТАНДАРТЫ

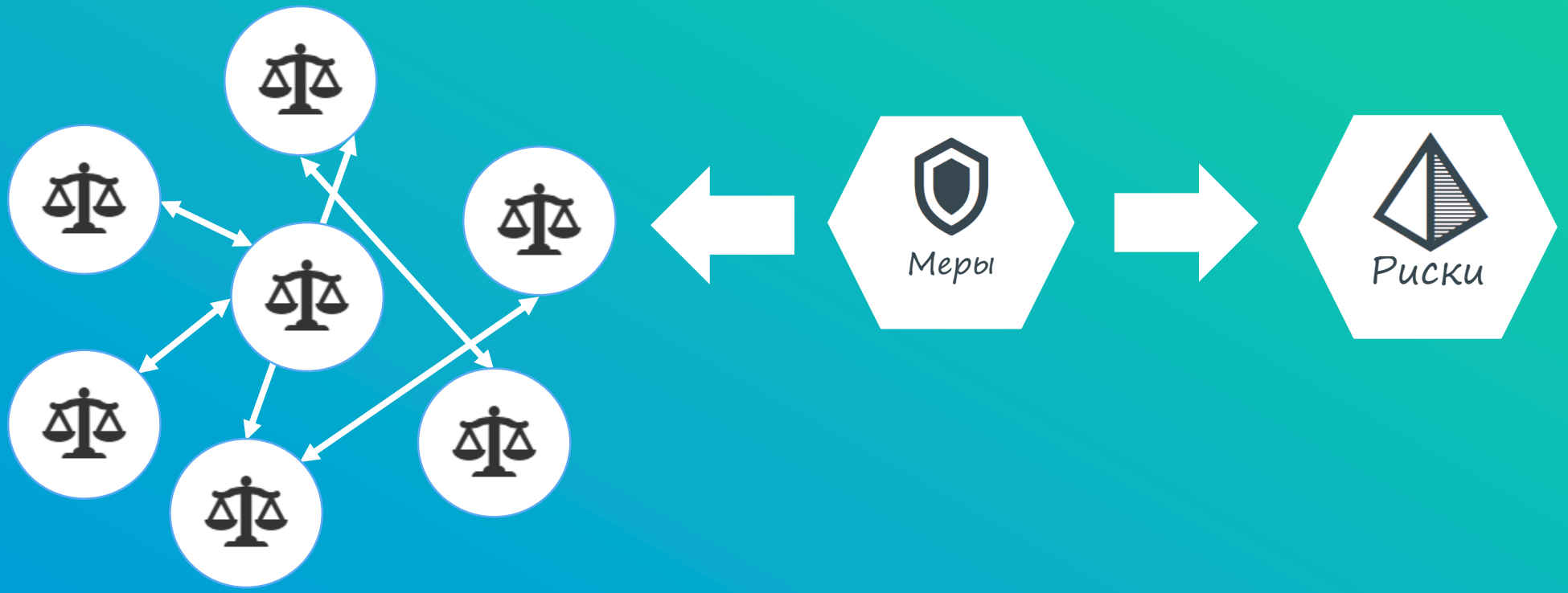
ISO 27001 107
NIST Cybersecurity Framework 108
The 20 CIS Controls Resources 149

24%-55% требований **уникальны**

39% - 62% **одинаковы** во всех приказах



Ценность требований через риски



Пример

- *Приказ ФСТЭК России № 239 от 25.12.2017* УПД.1
- *Приказ ФСТЭК России № 17 от 11.02.2013* УПД.1 АНЗ.5
- *Приказ ФСТЭК России № 31 от 14.03.2014* УПД.1 ИАФ.3
- *Приказ ФСТЭК России № 21 от 18.02.2013* АНЗ.5 УПД.1
- *ГОСТ Р № 57580.1-2017 от 01.01.2018* УЗП.3 УЗП.4
- *Framework The 20 CIS Controls & Resources* CSC 16.8 CSC 16.9 CSC 16.7
- *Framework NIST Cybersecurity Framework* PR.AC-1

Отключение неиспользуемых учетных записей в домене Active Directory

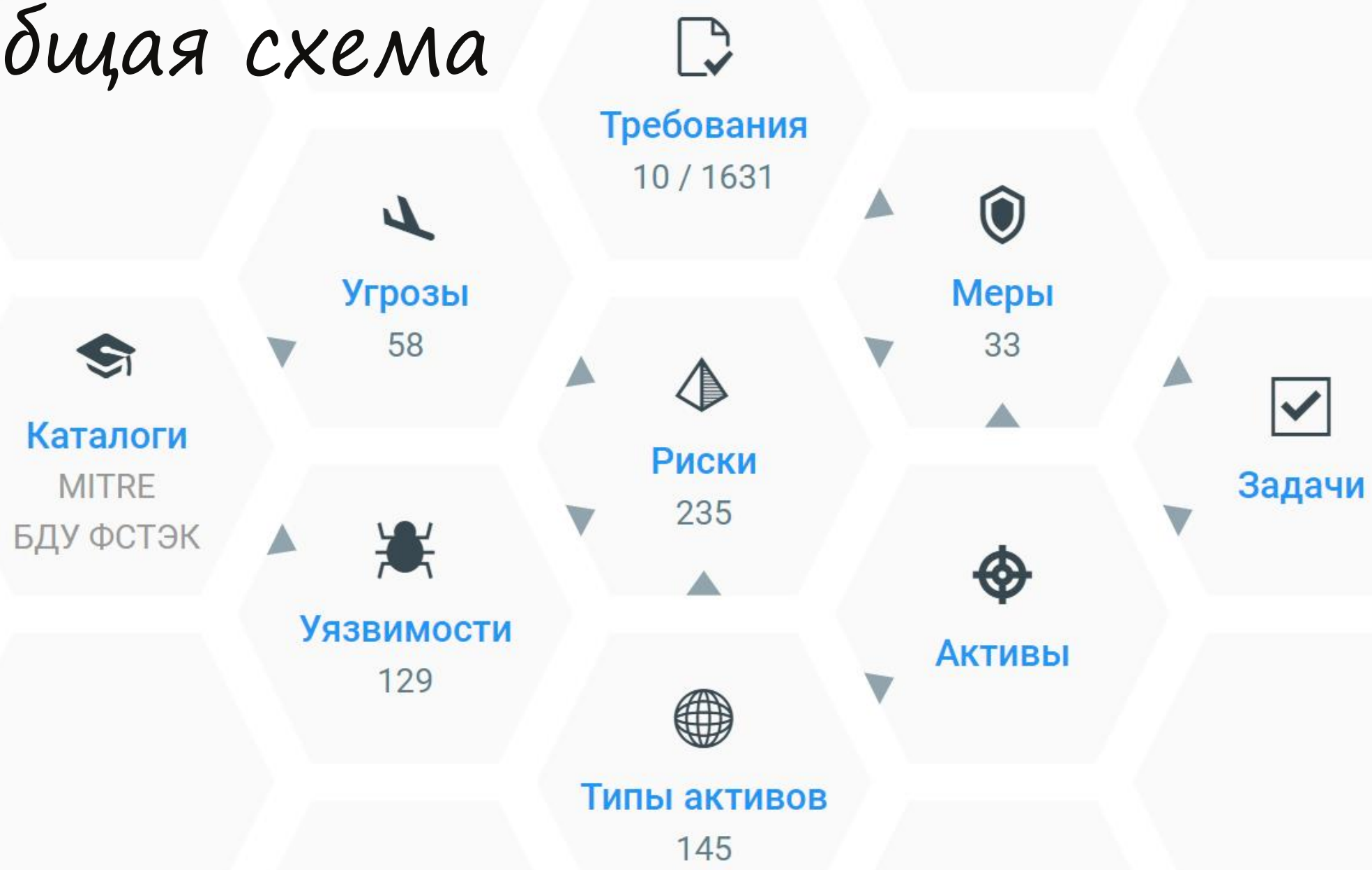
Тип
Техническая
Корректирующая
Компенсирующая
Реализация
Автоматически
Периодичность
По событию
Ответственный
Отдел ИБ
Инструменты
Скрипт

Несанкционированный доступ к информационным системам со стороны бывших работников и контрагентов

Наличие не используемых (устаревших) учетных записей

Доменные службы Active Directory

Общая схема


Требования
10 / 1631
Угрозы
58
Меры
33
Каталоги
MITRE
БДУ ФСТЭК
Риски
235
Задачи
Уязвимости
129
Активы
Типы активов
145

ПРОФИТЫ ОТ РИСК - ОРИЕНТИРОВАННОЙ ИБ

1. Понять **что** надо делать в первую очередь
2. Объяснить **зачем** мы это делаем
3. Найти общий язык с **бизнесом**
4. Распределить **ответственность**
5. Оптимизировать и обосновать **затраты**
6. Крепче спать по ночам)

РЕКОМЕНДАЦИИ

- Использовать **инструменты** для автоматизации
- Использовать готовые **каталоги** БДУ, MITRE
- Учитывать **меры**
- **Связывать** риски
  - друг с другом,
  - с мерами
  - с операционными процессами

Спасибо за Внимание

E-mail

nic-kazantsev@ya.ru

spbsecurity.blogspot.com

Telegram

@NicKazantsev

securitm.ru