КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

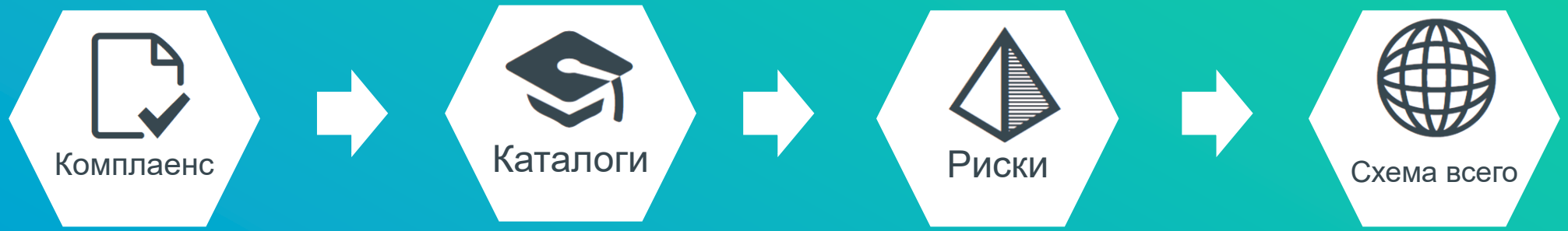
КОД ИБ ИТОГИ 02 ДЕКАБРЯ 2021

КАК МЫ СВЯЗАЛИ РИСКИ, КОМПЛАЕНС, КАТАЛОГИ УГРОЗ И ЧТО ИЗ ЭТОГО ВЫШЛО

НИКОЛАЙ КАЗАНЦЕВ, НТФФ ПОЛИСАН

Санкт-Петербург

О ЧЕМ БУДЕМ ГОВОРИТЬ ?



СИНХРОНИЗАЦИЯ

Цель ИБ:

1. Снижение рисков безопасности
2. Исполнение требований регуляторов
3. Исполнение потребностей бизнеса

Все что делает ИБ это

- Планирование
- Внедрение
- Сопровождение

} защитных мер

ПРОБЛЕМЫ УПРАВЛЕНИЯ СООТВЕТСТВИЕМ (COMPLIANCE)

- Требований много

  + документы дублируют друг друга

- Нет конкретики

  Не понятно **как** конкретно

  исполнять требования

- Нет смысла

  Не понятны причины,

  зачем исполнять требования

- Много рутины

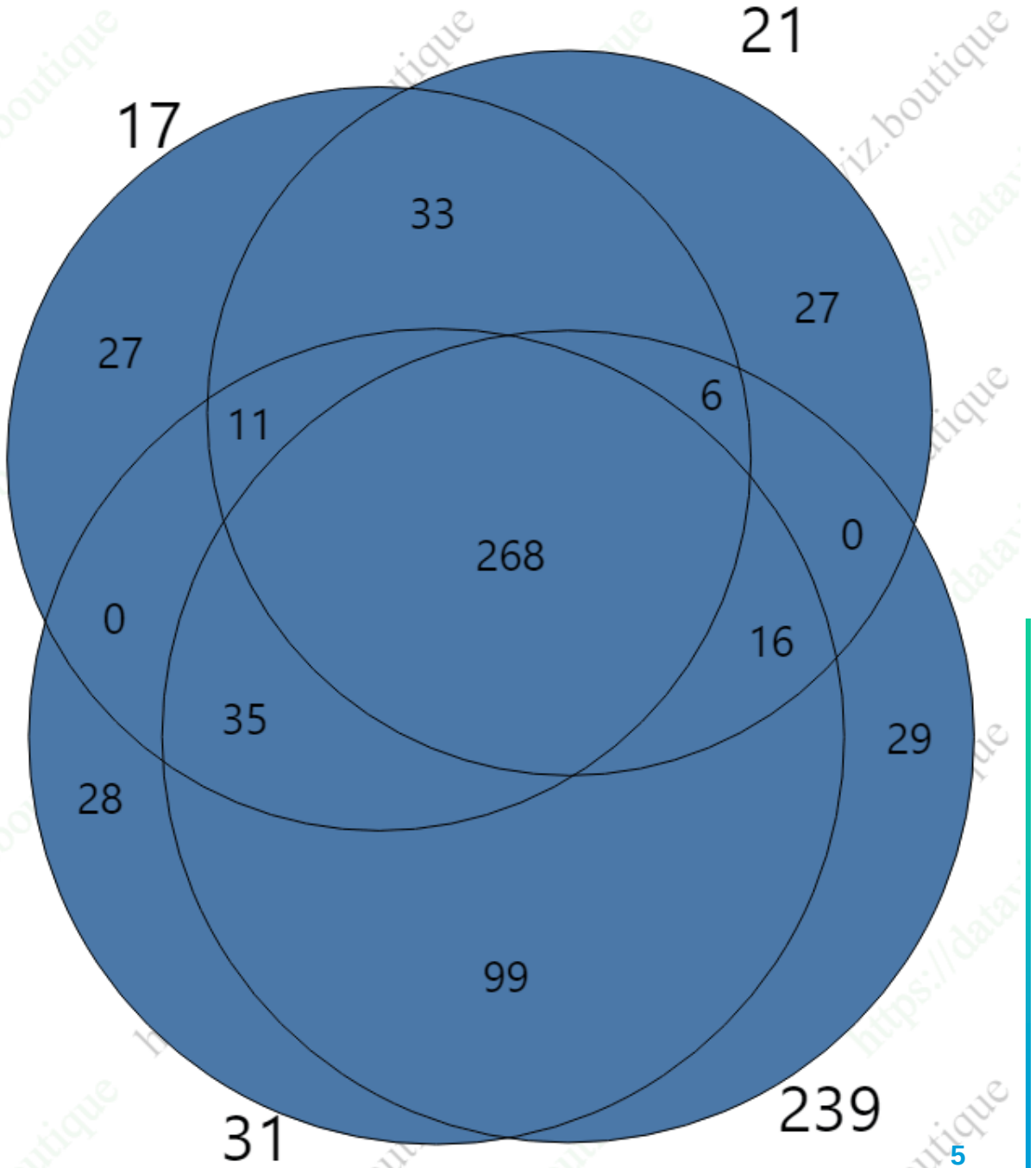
  Контролировать соответствие

  нужно ~~постоянно~~ 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

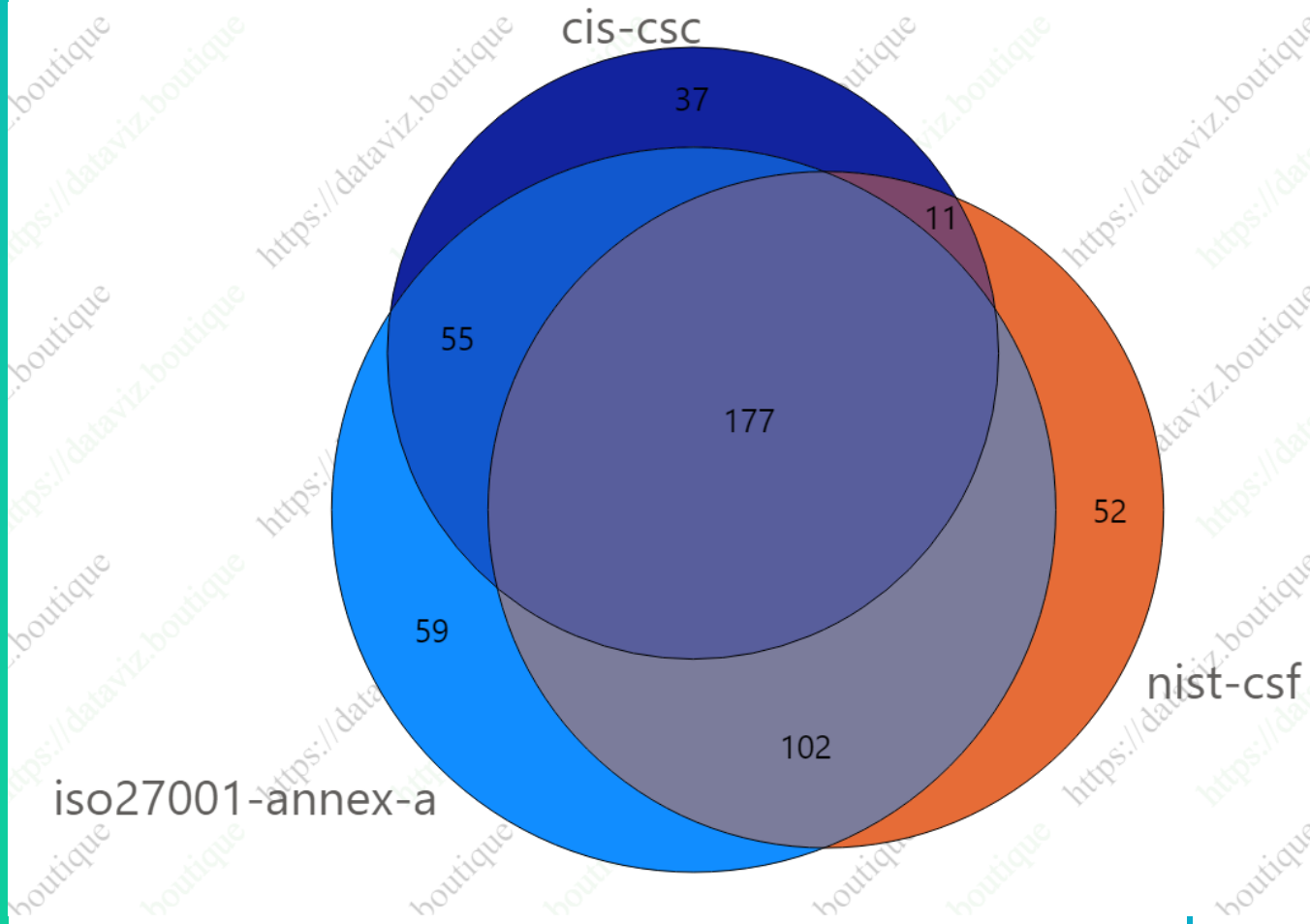


МЕЖДУНАРОДНЫЕ СТАНДАРТЫ

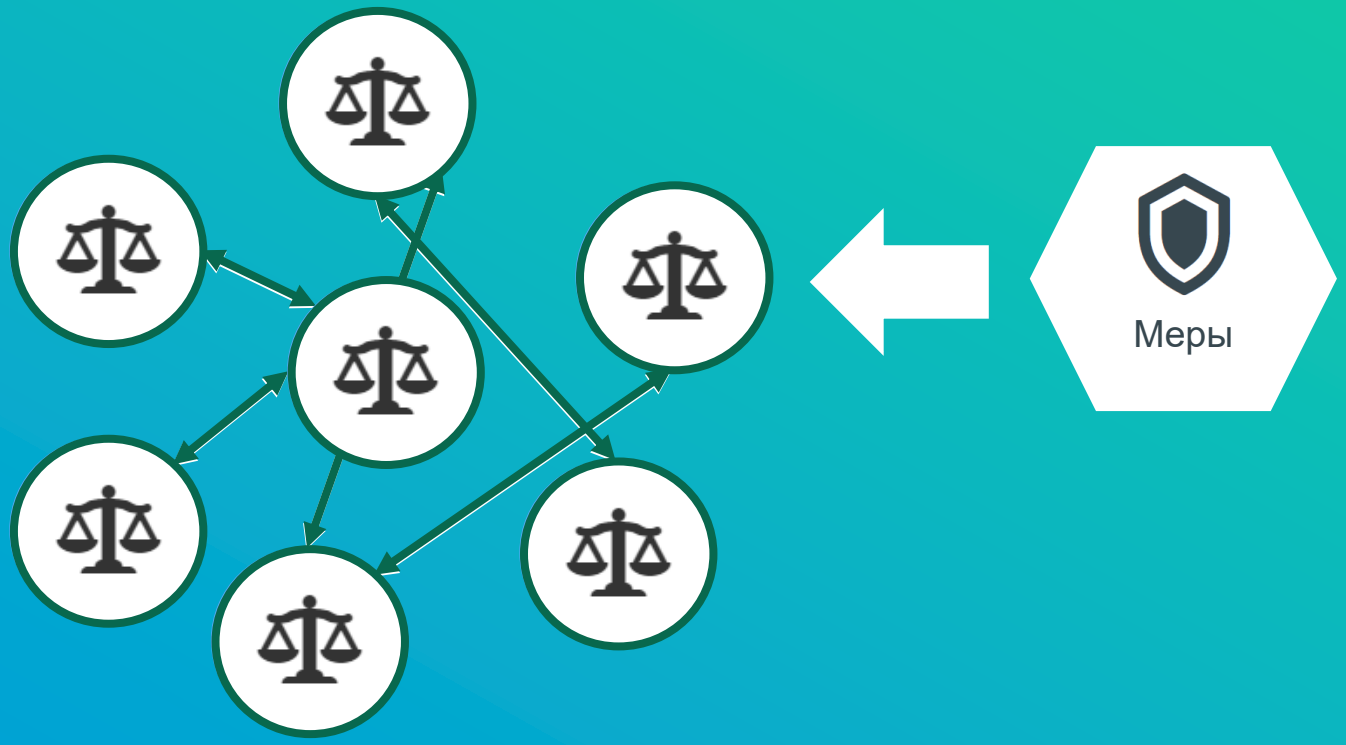
ISO 27001	**107**
NIST Cybersecurity Framework	**108**
The 20 CIS Controls Resources	**149**

24%-55% требований **уникальны**

39% - 62% одинаковы во всех приказах



1 МЕРА ЗАКРЫВАЕТ МНОГО ТРЕБОВАНИЙ



1 МЕРА ЗАКРЫВАЕТ МНОГО ТРЕБОВАНИЙ

- 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

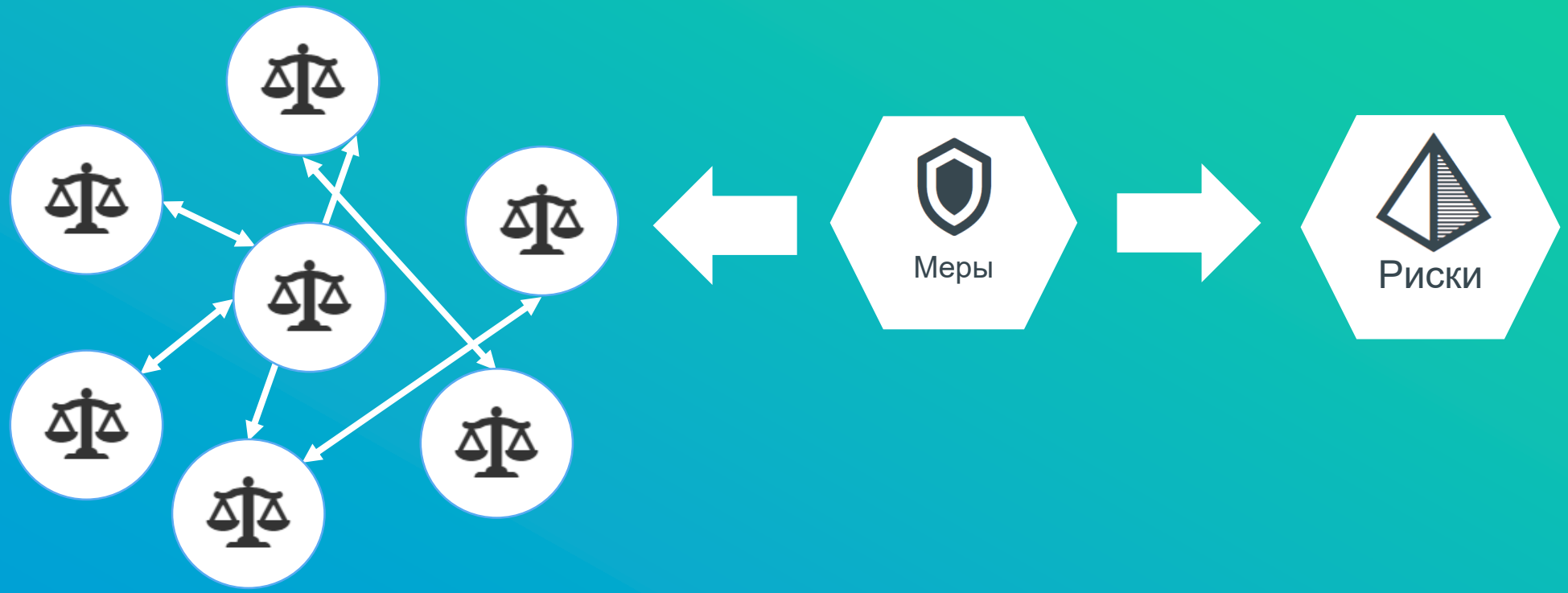
Отдел ИБ

Инструменты

Скрипт


Где копать?

ЦЕННОСТЬ ТРЕБОВАНИЙ ЧЕРЕЗ РИСКИ БЕЗОПАСНОСТИ



1 МЕРА И ЗАКРЫВАЕТ ТРЕБОВАНИЯ И СНИЖАЕТ РИСКИ

- 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

ПРОБЛЕМЫ
С КАТАЛОГАМИ УГРОЗ

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

OWASP

CAPEC

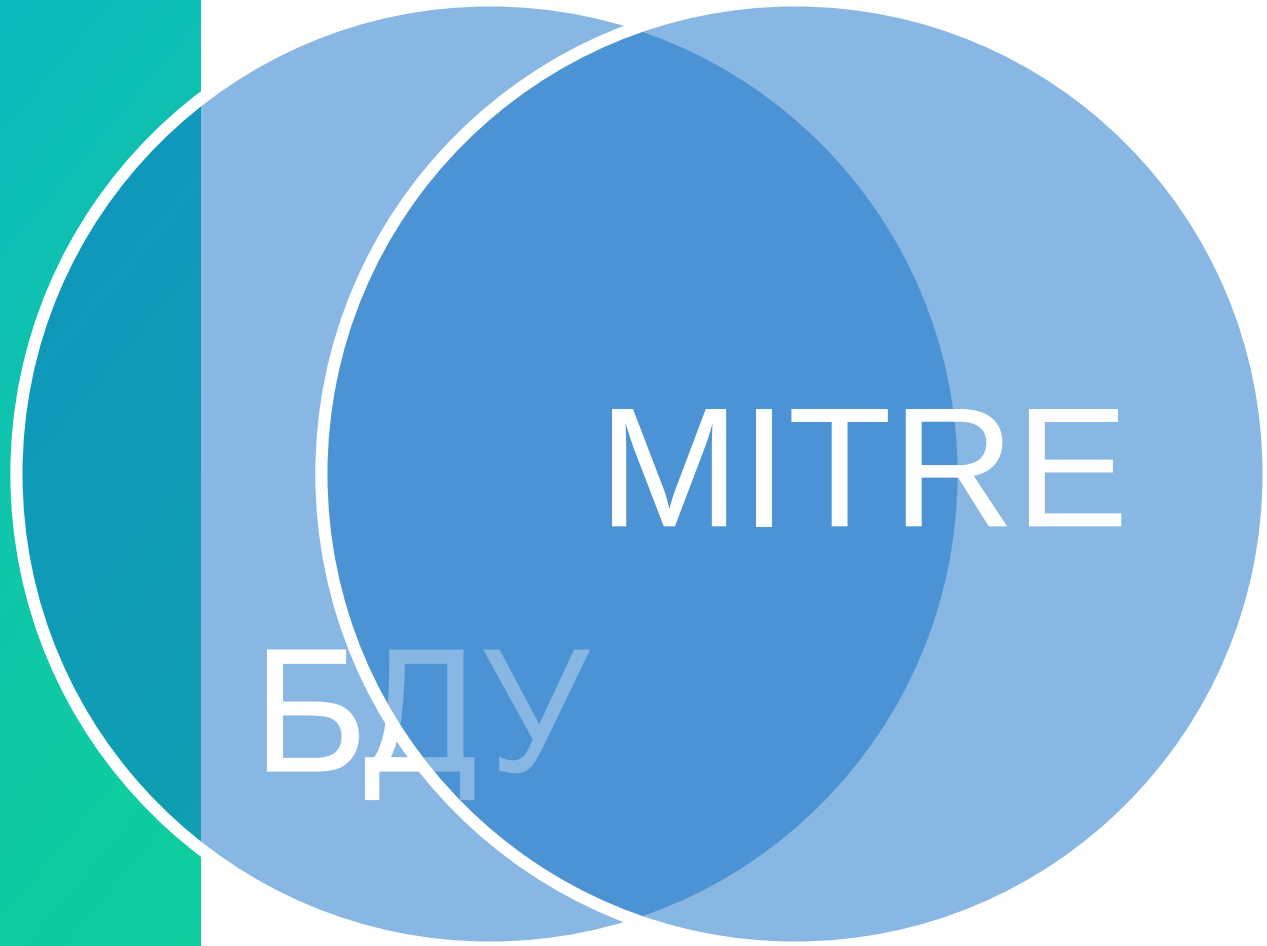
MITRE | ATT&CK

CWE

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

Version: 1.0

Раскрытие информации об ИТ инфраструктуре

Возможность сканирования IP адресов

Публичный IP-адрес

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).

КАТАЛОГИ УГРОЗ

БДУ ФСТЭК:

- **УБИ.098** Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
- **УБИ.099** Угроза обнаружения хостов
- **УБИ.104** Угроза определения топологии вычислительной сети

Техники ATT@CK:

- **T1046** Network Service Scanning
- **T1590.004** Gather Victim Network Information: Network Topology
- **T1595** Active Scanning
- **T1595.001** Active Scanning: Scanning IP Blocks
- **T1595.002** Active Scanning: Vulnerability Scanning

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

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

* Результаты опроса служб безопасности

КАТАЛОГИ УГРОЗ – ОСНОВА ДЛЯ РЕЕСТРА РИСКОВ

Специфичные для компании риски

20%

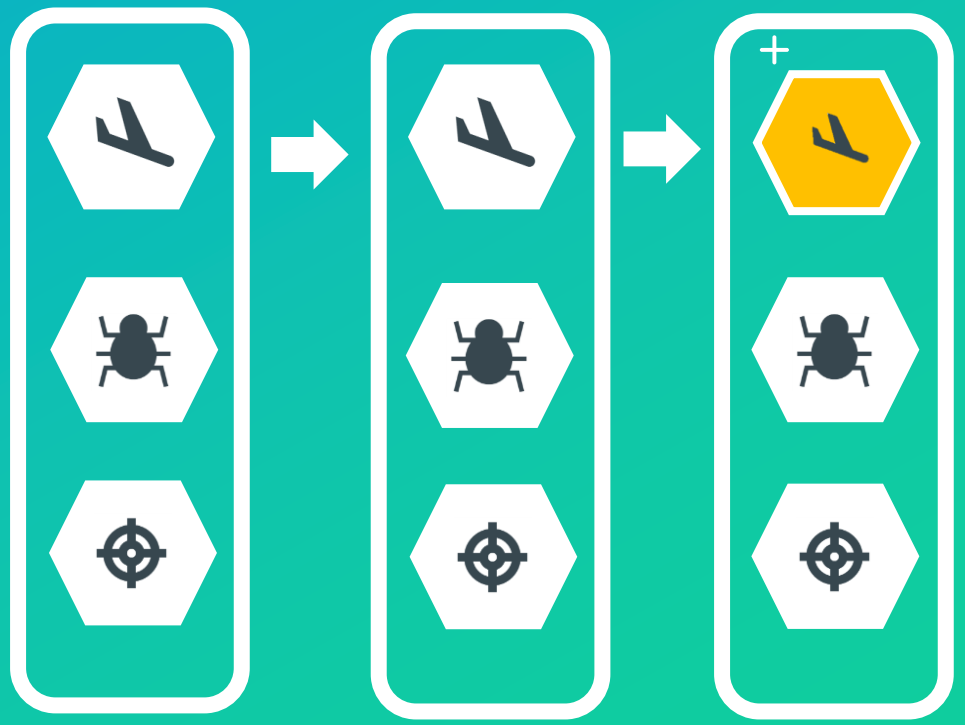
Каталоги угроз

80%

Риски

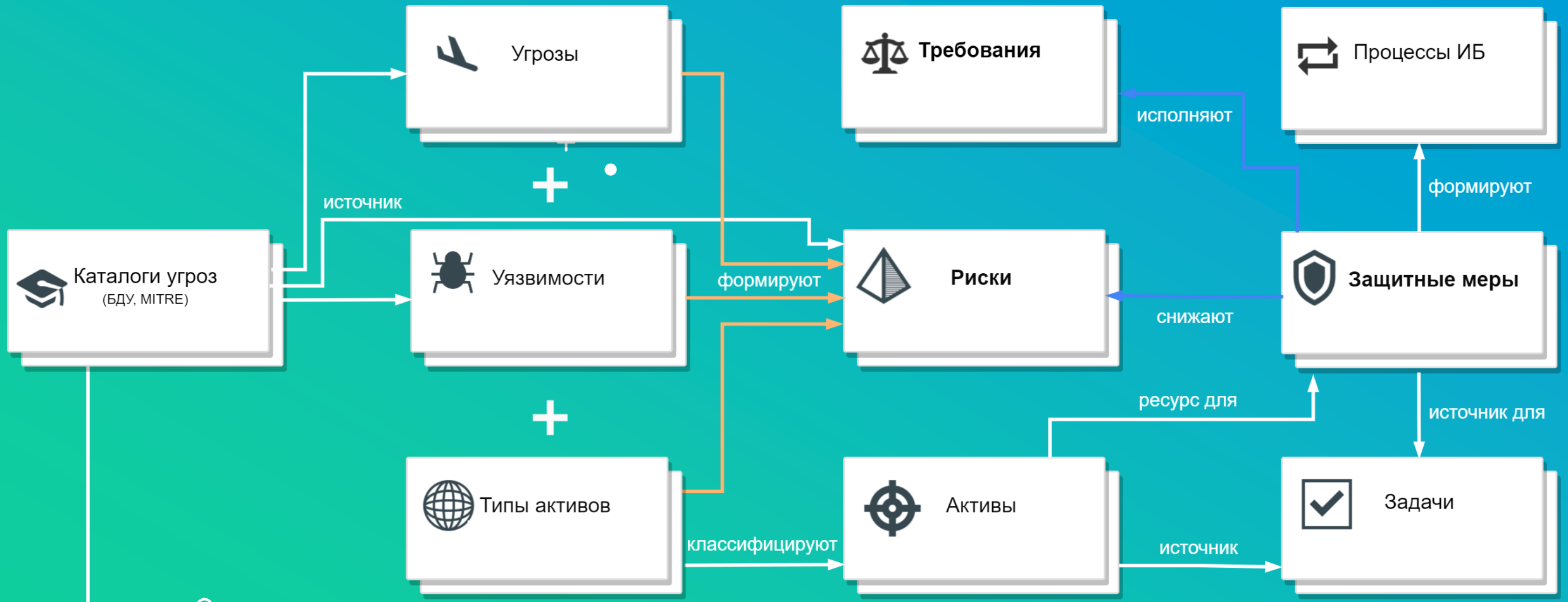
Меры

ИЕРАРХИЯ/ЦЕПОЧКИ/СЦЕНАРИИ УГРОЗ/РИСКОВ




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

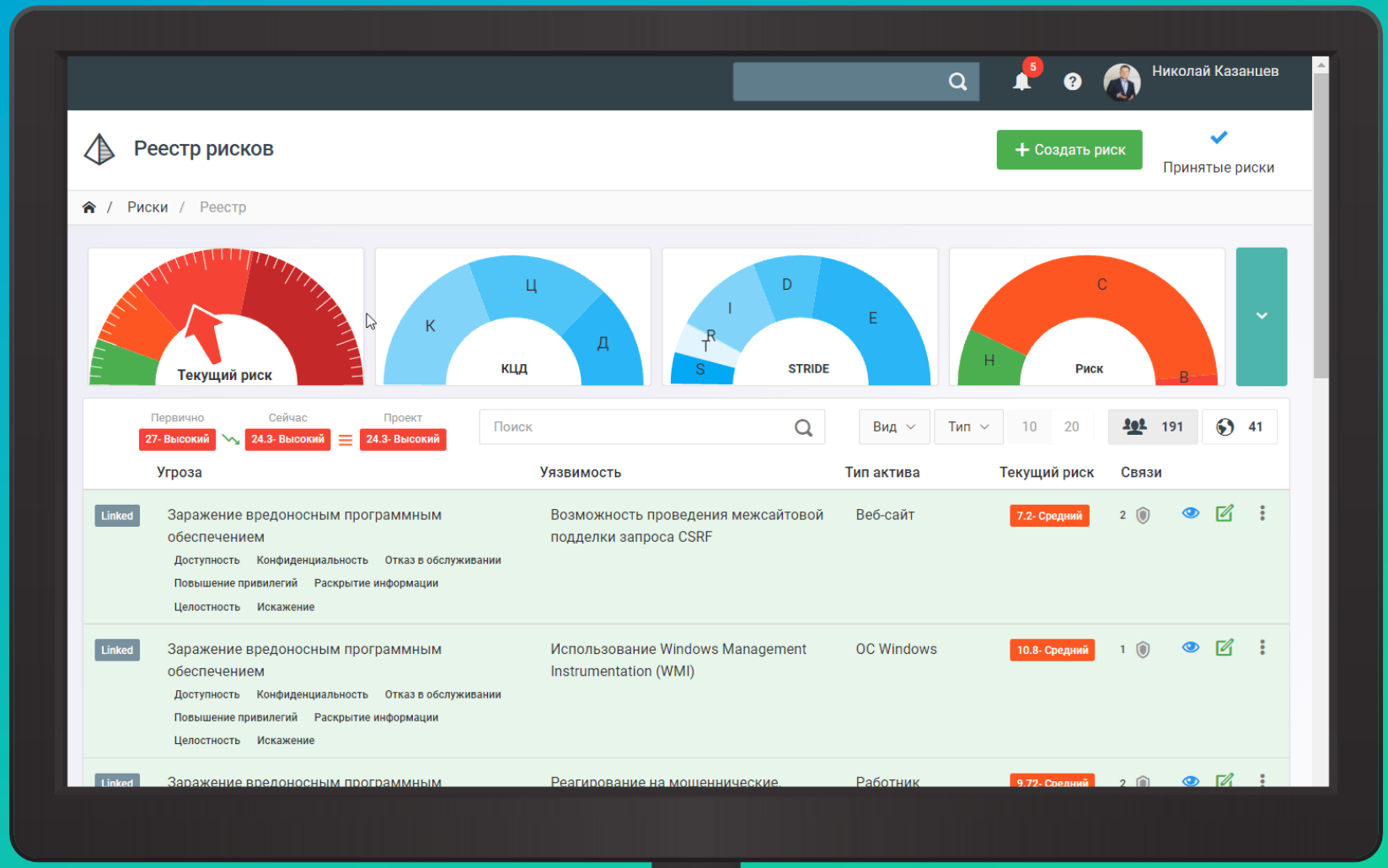
СХЕМА ВСЕГО


Угрозы
Требования
Процессы ИБ
исполняют
формируют
источник
Каталоги угроз
(БДУ, MITRE)
Уязвимости
формируют
Риски
снижают
Защитные меры
ресурс для
источник для
Типы активов
классифицируют
Активы
источник
Задачи

	Проблема	Решение	Результат
Комплаенс	Много документов Нет конкретики Нет смысла Много рутины	Связываем требования друг с другом Формируем проекты конкретных защитных мер Связываем требования с рисками через защитные меры Управляем защитными мерами, а не требованиями	Не тратим время на дубли Не гадаем как исполнить требование Видим причины и устанавливаем приоритеты Не возвращаемся к контролю соответствия повторно
Каталоги	Много каталогов Разный формат Не понятен приоритет	Работаем с рисками, а не каталогами Связываем каталоги с нашими рисками	Не тратим время на похожие угрозы/техники Обогащаем риски знаниями из каталогов Понимаем приоритеты
Риски	Нет данных Нет понимания у руководства Много рутины	80% реестра рисков создаем из каталогов Строим цепочку (иерархию), доходя до бизнес-рисков Управляем защитными мерами, а не рисками	Экономим время на наполнении реестра рисков Говорим с бизнесом на одном языке Экономим время на оценку и контроль

БЕЗОПАСНОСТЬ – ДЕЛО ОБЩЕЕ

service.securitm.ru



СПАСИБО ЗА ВНИМАНИЕ

- **Николай Казанцев**

t.me/NicKazantsev

spbsecurity.blogspot.com