Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Управление рисками информационной безопасности

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

1. Риск
Уязвимость
Угроза

Угроза (threat)

- **Угроза** – это действие или событие, способное нарушить безопасность информационных систем.

- **Угроза** потенциальная причина инцидента, который может нанести ущерб системе или организации [ГОСТ Р ИСО/МЭК 13335-1-2006];

- **Угроза** – набор обстоятельств и действий, которые потенциально могут привести к нарушению безопасности системы

- **Угроза ИБ** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ГОСТ Р 50922-2006];

Уязвимость (брешь) (vulnerability)

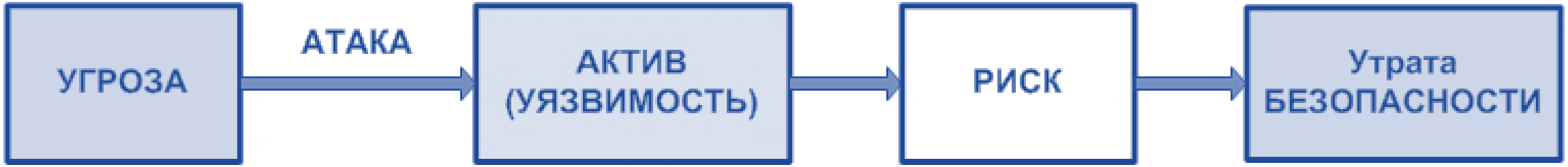
- **Уязвимость** – слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами [ГОСТ Р ИСО/МЭК 13335-1-2006];
- **Уязвимость** – это слабое звено информационной системы, которое, став известным злоумышленнику, может позволить ему нарушить ее безопасность.
- **Уязвимость – это потенциальный путь для выполнения атаки.**

- Уязвимости системы могут быть скрытыми, то есть еще не обнаруженными, известными, но только теоретически, или же общеизвестными и активно используемыми злоумышленниками.

- **Актив** – все, что имеет ценность для организации [ГОСТ Р ИСО/МЭК 13335-1-2006];

Риск

- **Если уязвимость соответствует угрозе, то существует риск**
  (ИСО 2382-8:1998)



- **Риск – это сочетание угрозы и уязвимости.**
- **Угрозы без уязвимости не являются риском** так же, как и уязвимости без угроз. В реальном мире ни одно из этих условий не существует.
- **Атака (attack)** – это реализованная угроза
- Следовательно, **оценка риска** – это определение вероятности того, что непредвиденное событие произойдет.

Риск. Еще определения

- **Риск** – это возможность опасности, неудачи или действие наудачу в надежде на счастливый исход.
- **Риск** – это вероятность причинения вреда с учетом его тяжести.
- **Риск** – опасность возникновения непредвиденных потерь ожидаемой прибыли, дохода или имущества, денежных средств в связи со случайным изменением условий экономической деятельности, неблагоприятными обстоятельствами.
- **Термин «риск» используют** только тогда, когда существует возможность негативных последствий, само же понятие риска ИБ является комбинированным, сочетающим в себе ряд других ключевых терминов – активы, уязвимости, угрозы, ущерб.

Риск. Определения в стандартах

- **Согласно ГОСТ Р 51897–2002** «Менеджмент риска. Термины и определения» **риск** представляет собой сочетание вероятности события и его последствий.
- **В ГОСТ Р 51898–2002** «Аспекты безопасности. Правила включения в стандарты»: **риск** – это сочетание вероятности нанесения ущерба и тяжести этого ущерба.
- **В стандарте США NIST 800–30 риск** является функций вероятности использования данным источником угроз ИБ отдельной потенциальной уязвимости и результата воздействия этого неблагоприятного события на организацию.
- **Стандарт ГОСТ Р ИСО/МЭК 27005–2010** определяет **риск ИБ** как потенциальную возможность использования уязвимостей актива или группы активов конкретной угрозой ИБ для причинения ущерба организации.
- **Стандарт ISO/IEC 27005:2011** определяет **риск ИБ** как влияние неопределенности на цели.
- **В СТО БР ИББС 1.0–2010 риск нарушения ИБ** – риск, связанный с угрозой ИБ. Под риском понимается мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

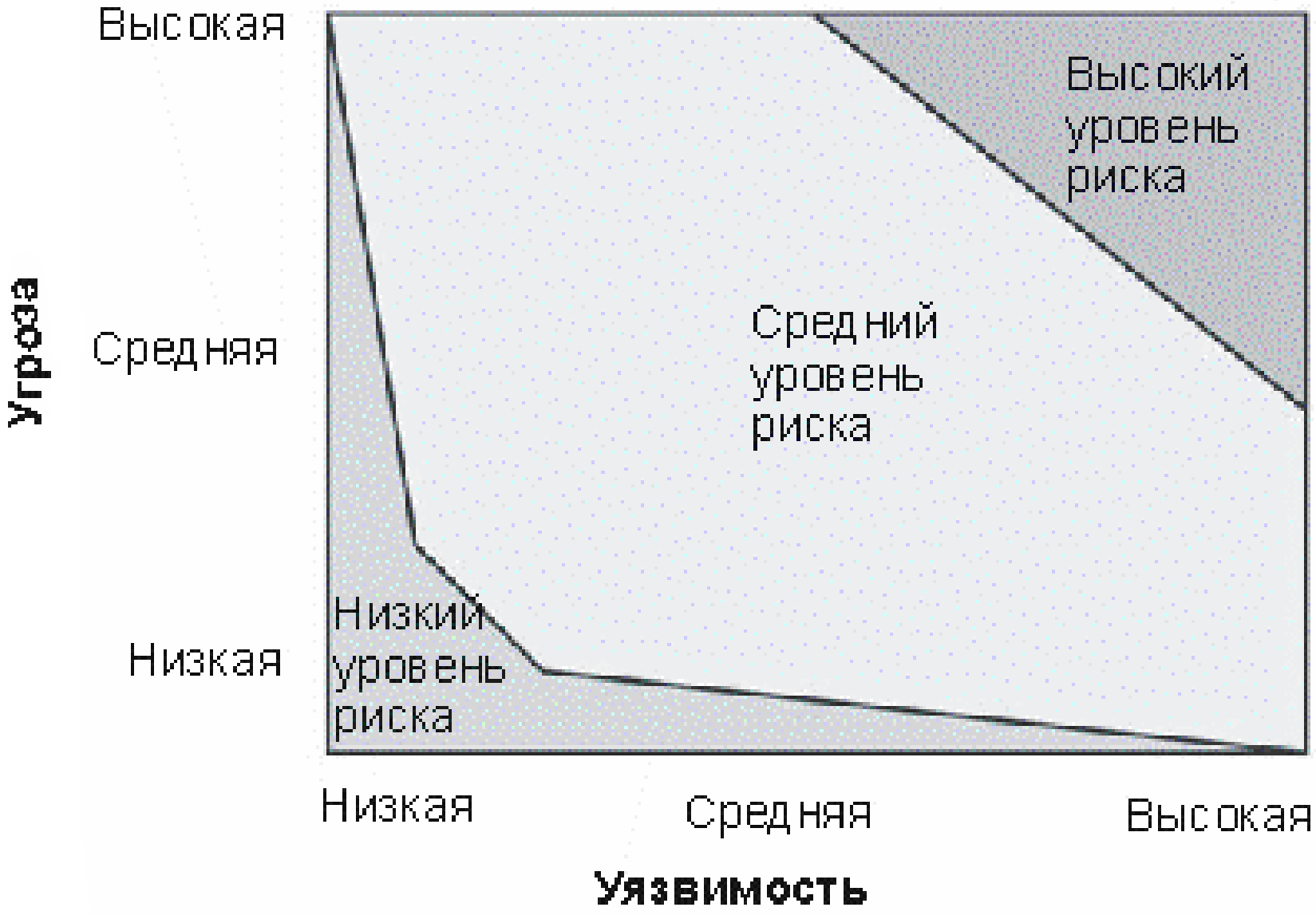
Риск информационной безопасности

- **Риск ИБ** – риск нарушения состояния защищенности информации.
- **Риск нарушения ИБ (риск ИБ)** – потенциальная возможность использования уязвимостей активов организации угрозами ИБ для причинения ущерба организации, измеряемая с учетом вероятности реализации угроз ИБ и величины ущерба от реализации угроз ИБ.

- Таким образом, в представленном определении **риск ИБ** есть функция как минимум двух переменных: величины потенциального (негативного) воздействия – ущерба для бизнеса организации и вероятности реализации угрозы ИБ.
- Риски ИБ всегда должны рассматриваться в контексте бизнеса организации.

Зона риска

Соотношение между уязвимостью и угрозой



3 уровня риска

- **Риск качественно определяется тремя уровнями.**
- **Низкий**. **Существует маленькая вероятность проявления угрозы**. По возможности нужно предпринять действия по устранению уязвимого места, но их стоимость должна быть сопоставлена с малым ущербом от риска.
- **Средний**. **Уязвимость является значительным уровнем риска для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации**. Существует реальная возможность осуществления такого события. Действия по устранению уязвимости целесообразны.
- **Высокий**. **Уязвимость представляет собой реальную угрозу для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации**. Действия по устранению этой уязвимости должны быть предприняты незамедлительно.

2. Управление рисками

Управление рисками

- **Управление информационной безопасностью является дочерним процессом более широкого процесса управления рисками**: если компания после анализа и оценки всех своих бизнес-рисков делает вывод об актуальности рисков ИБ, то в игру вступает уже непосредственно защита информации как способ минимизации некоторых рисков.

- **Управление рисками или риск-менеджмент (англ. risk management)** – особый вид деятельности (процесс) по принятию и выполнению управленческих решений, направленных на снижение вероятности возникновения неблагоприятного результата и минимизацию возможных потерь, вызванных его реализацией.

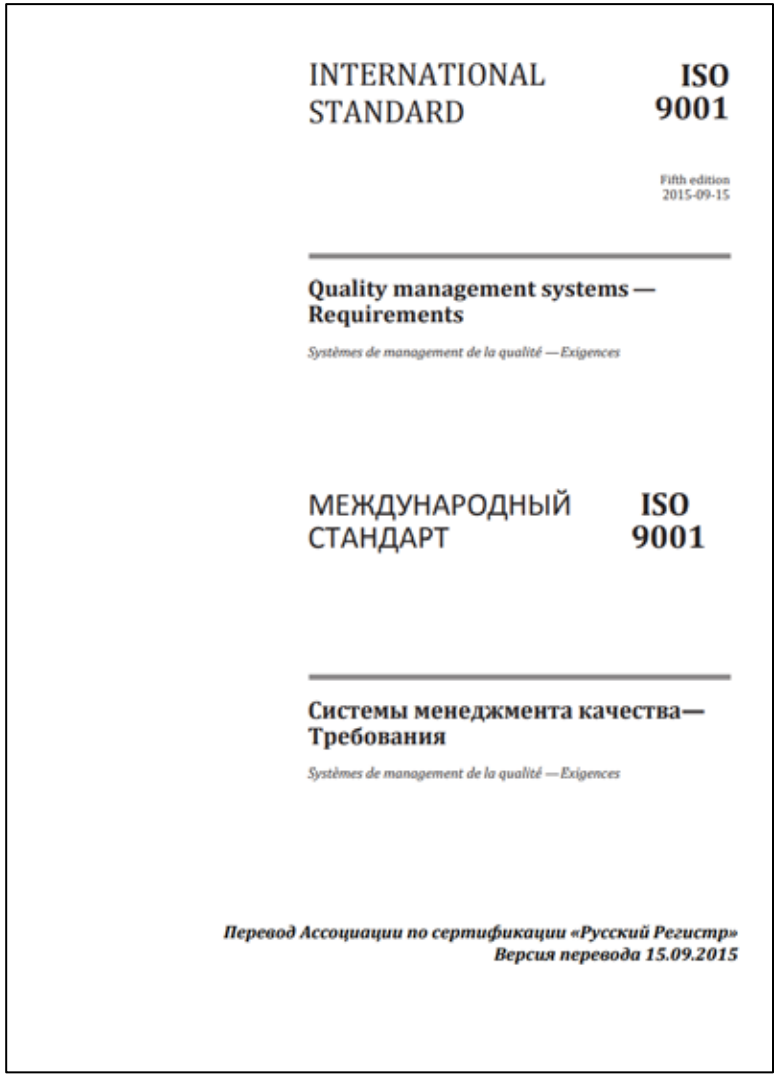
Управление рисками

- **В классическом управлении рисками принято выделять пять ключевых этапов:**
  - **1) выявление риска и оценка вероятности его реализации** и масштаба последствий, определение максимально-возможного убытка;
  - **2) выбор методов и инструментов управления выявленным риском** (это ключевой этап);
  - **3) разработка риск-стратегии с целью снижения вероятности реализации риска** и минимизации возможных негативных последствий;
  - **4) реализация риск-стратегии;**
  - **5) оценка достигнутых результатов и корректировка риск-стратегии.**

Управление рисками

- **В стандарте ISO 9001:2015 «Системы менеджмента качества. Требования»** четко **прописаны требования по управлению рисками**, а этим стандартом руководствуются большинство организаций в своей работе.

ISO 9001-2015 **Системы менеджмента качества. Требования**



INTERNATIONAL STANDARD **ISO 9001**

Fifth edition
2015-09-15

Quality management systems — Requirements

Systèmes de management de la qualité — Exigences

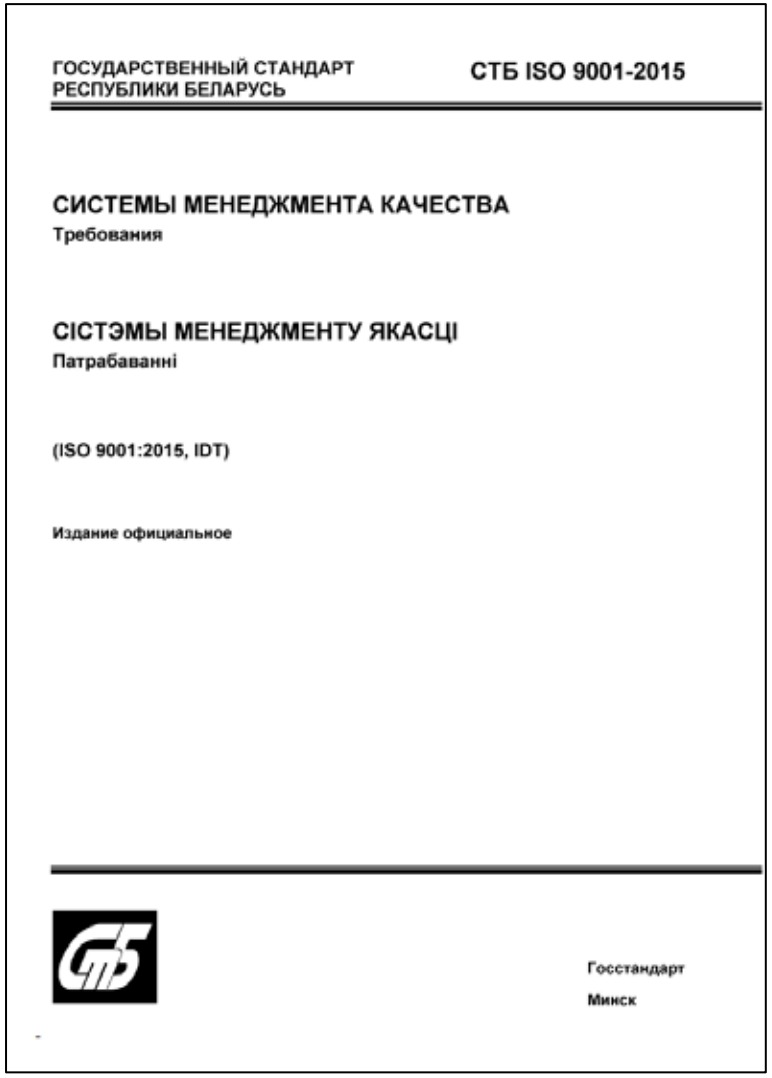
МЕЖДУНАРОДНЫЙ СТАНДАРТ **ISO 9001**

Системы менеджмента качества— Требования

Systèmes de management de la qualité — Exigences

Перевод Ассоциации по сертификации «Русский Регистр»
Версия перевода 15.09.2015

https://iso-group.ru/unik/ISO-9001-2015.pdf
https://bsuedu.ru/upload/iblock/32a/ISO%209001%202015.pdf



ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ **СТБ ISO 9001-2015**

СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА
Требования

СІСТЭМЫ МЕНЕДЖМЕНТУ ЯКАСЦІ
Патрабаванні

(ISO 9001:2015, IDT)

Издание официальное

Госстандарт
Минск

https://mshp.gov.by/uploads/Files/ochrtrud/recomdacii/stb9001.pdf

Управление рисками (ISO 9001:2015)

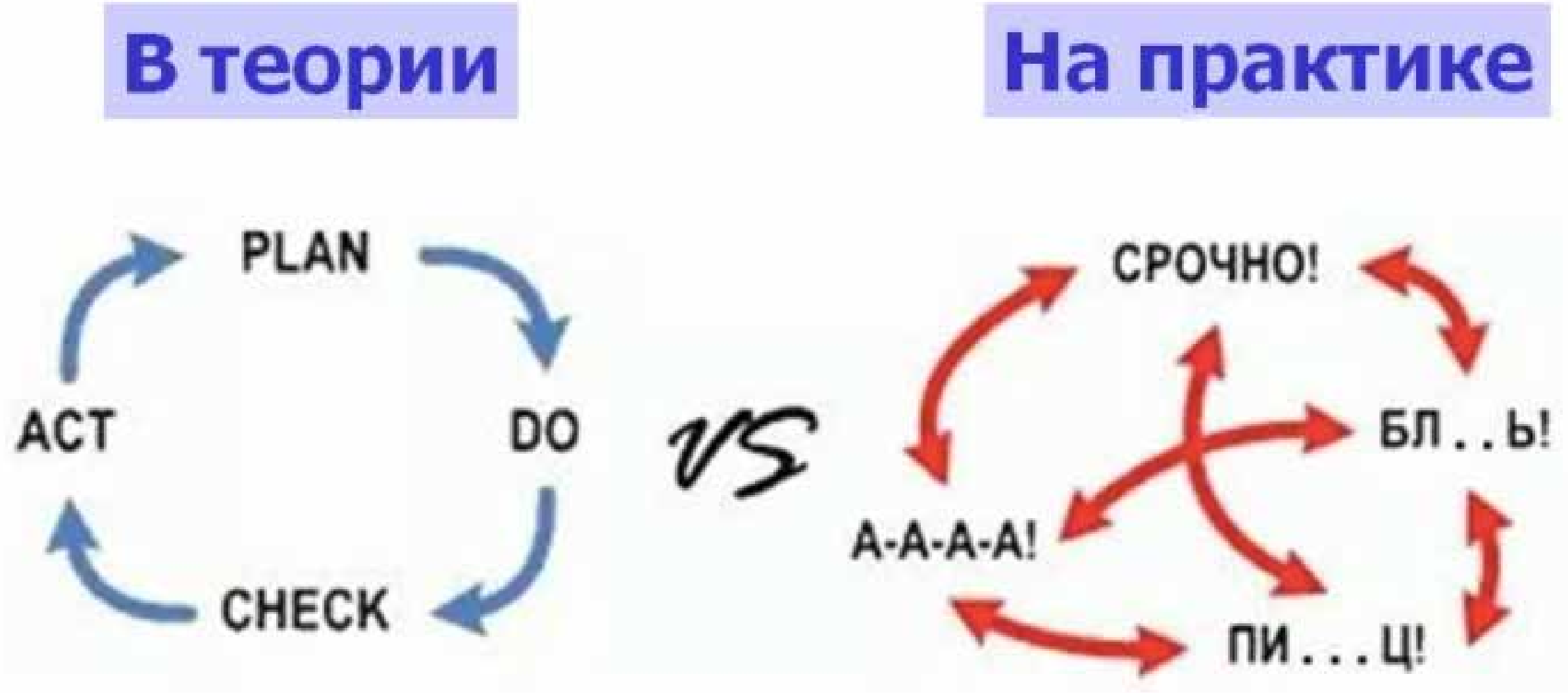
- Требования по управлению рисками в соответствии с ISO 9001:2015 используют процессный подход, включающий в себя цикл PDCA (Plan – Do – Check – Act) и **риск-ориентированное мышление**.

- **PDCA (Plan-Do-Check-Act)** – это интерактивный, четырехступенчатый подход к постоянному улучшению продукта, услуг, а также для использования в решении проблем.

Цикл Деминга / PDCA cycle

- **Планирование.** Сначала анализ процесса: разберитесь, в чём проблема, почему что-то не получается. Для этого надо привлечь всю команду, чтобы увидеть картину с разных сторон и понять, что и как можно улучшить. Потом план: установить сроки и согласовать с командой, что и когда нужно делать.
- **Действие.** Работать согласно новому плану и не нарушать его условий.
- **Проверка.** Посмотреть на результат и понять, всё ли получилось так, как было задумано. Доволен ли заказчик, всё ли работает. А ещё проанализировать, как шёл сам процесс, чтобы в следующем цикле поменять что-то к лучшему.
- **Корректировка.** Использовать план или менять: если всё получилось, то применить новые наработки, сделать процесс стабильным и пытаться улучшить ещё. Если нет, то вернуться к первому пункту и повторить всё сначала, но уже с работой над ошибками.

Цикл Деминга / PDCA cycle



Риск ориентированный подход

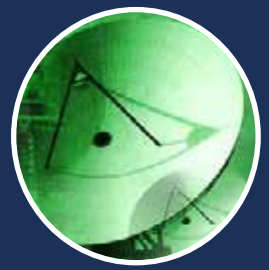
ISO 9001:2015 не требует проведения полной, официальной оценки рисков или ведения реестра рисков.

ISO 31000 «Менеджмент рисков - Принципы и руководства» является полезным документом, но **не является обязательным**.

ISO 31000 **Управление рисками**

Системы экологичес-кого менеджмента

(ISO 14001)



Системы менеджмента информаци-онной безопасности

(ISO 27001)

Системы менеджмента охраны здоровья и обеспечения безопасности труда

(OHSAS 18001)

Системы менеджмента безопасности продуктов питания

(ISO 22000)

Менеджмент ИТ-услуг

(ISO 20000)

Социальная ответствен-ность

(ISO 26000)

ISO 9001 Системы менеджмента качества

Управление рисками

- **Управление рисками позволяет** эффективно и рационально выстраивать процессы ИБ и распределять ресурсы для защиты активов компании, а **оценка рисков позволяет** применять целесообразные меры по их минимизации: для защиты от существенных и актуальных угроз логично будет применять более дорогостоящие решения, чем для противодействия незначительным или труднореализуемым угрозам.
- Кроме этого, выстроенный процесс управления рисками ИБ позволит разработать и в случае необходимости применить чёткие планы обеспечения непрерывности деятельности и восстановления работоспособности (Business Continuity & Disaster Recovery): глубокая проработка различных рисков поможет заранее учесть, например, внезапно возникшую потребность в удаленном доступе для большого количества сотрудников, как это может произойти в случае эпидемий, чрезвычайных ситуаций или коллапса транспортной системы

Этапы внедрения системы управления рисками

Общая концепция управления рисками ИБ

- Под **риском информационной безопасности**, или киберриском, понимают потенциальную возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

- Под **величиной риска** условно понимают произведение вероятности негативного события и размера ущерба. В свою очередь под вероятностью события понимается произведение вероятности угрозы и опасности уязвимости, выраженные в качественной или количественной форме.

Управление рисками ИБ

- **Управление рисками ИБ, включает в себя:**

1. идентификацию, анализ, оценку, отслеживание и устранение рисков;
2. превентивную разработку программы мероприятий по ликвидации последствий кризисных ситуаций;
3. разработку механизмов выживания; создание системы страхования;
4. прогнозирование развития организации с учетом возможного изменения конъюнктуры и другие мероприятия.

Управление рисками ИБ

- Применительно к области ИБ **определения управления рисками ИБ** (англ. information security risk management или IS risk management) в разных стандартах достаточно близки по смыслу и хорошо дополняют друг друга:
  - согласованные виды деятельности по руководству и управлению организацией в отношении рисков ИБ;
  - скоординированные непрерывные действия по управлению и контролю рисков ИБ в организации;
  - скоординированные действия по руководству и управлению организацией в отношении рисков ИБ, обычно включающие в себя оценку, обработку, принятие и коммуникацию риска ИБ;
  - процесс выявления, контроля и минимизации или устранения рисков ИБ, оказывающих влияние на ИС, в рамках допустимых затрат;
  - полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы ИТ;
  - непрерывный процесс, устанавливающий контекст управления рисками ИБ, оценку и обработку рисков ИБ на основе плана обработки рисков для реализации рекомендаций и принятых решений.

Управление рисками ИБ

- **Управление рисками ИБ определим как** скоординированную непрерывную деятельность по руководству и управлению организацией в отношении рисков ИБ на основе политики управления рисками ИБ и плана обработки рисков ИБ, обычно включающую в себя установление контекста управления рисками ИБ, оценку, обработку, принятие, мониторинг, пересмотр и коммуникацию рисков ИБ.

Задачи управления рисками ИБ

- 1) планирование управления рисками ИБ;
- 2) выявление, идентификация и документирование рисков ИБ;
- 3) детальная оценка рисков ИБ и их приоритетности с целью выявления их потенциального влияния на бизнес;
- 4) планирование ответных действий для каждого риска ИБ (обработка рисков ИБ);
- 5) мониторинг рисков ИБ, по результатам которого возможно изменение приоритетов и планов обработки ранее выявленных рисков ИБ;
- 6) мониторинг всех работ по управлению рисками ИБ в организации с целью внесения необходимых корректив в этот процесс.

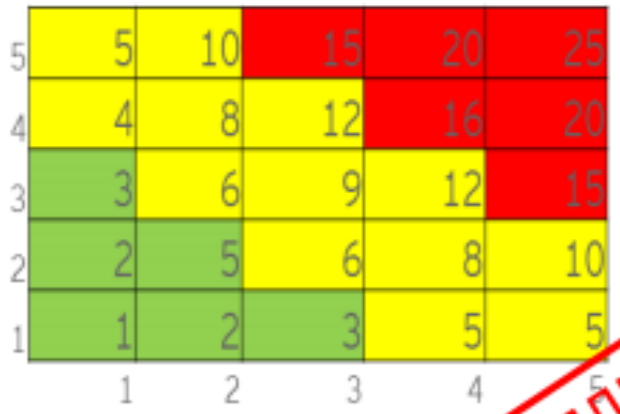
Общая концепция управления рисками ИБ

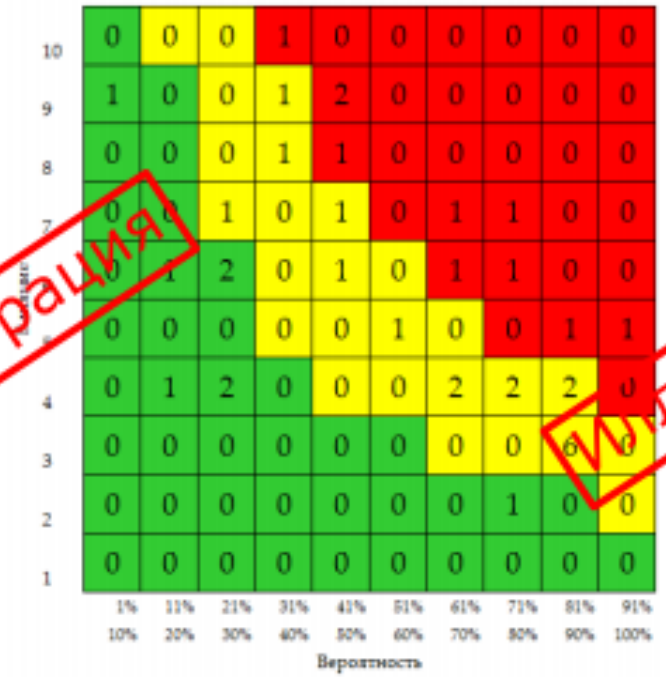
- Условно можно выразить это логической формулой:

ВеличинаРиска = ВероятностьСобытия * РазмерУщерба, где

ВероятностьСобытия = ВероятностьУгрозы * ВеличинаУязвимости

Примеры матрицы рисков информационной безопасности



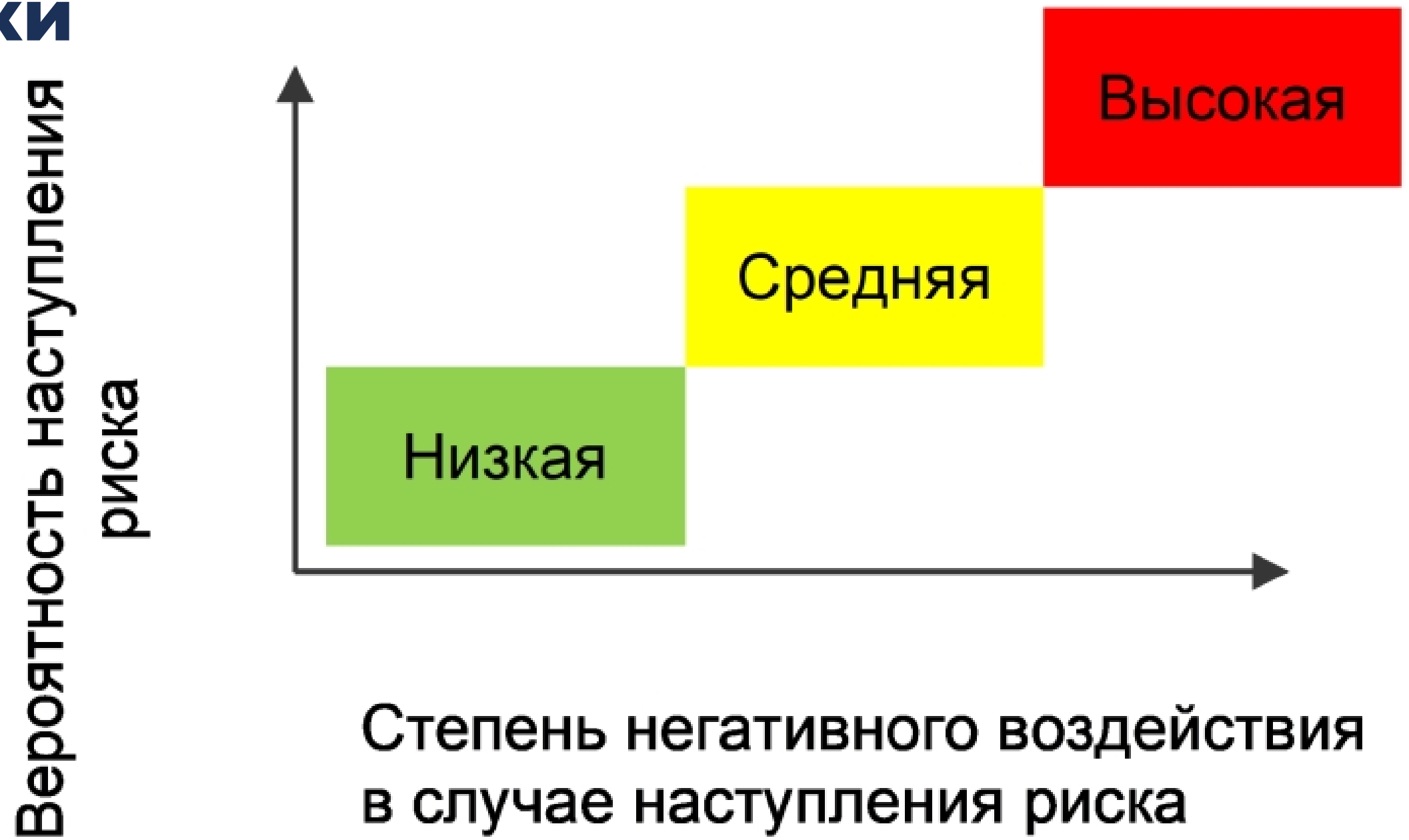


Вероятность причинения вреда	Тяжесть последствий при причинении вреда				
	ОВТ	ВТ	СТ	НТ	НЗТ
Высокая вероятность (ВВ)	СЗ	СЗ	СЗ	С	С
Средняя вероятность (СВ)	СЗ	СЗ	С	С	Н
Низкая вероятность (НВ)	СЗ	С	С	Н	Н
Малая вероятность (МВ)	С	С	Н	Н	Н

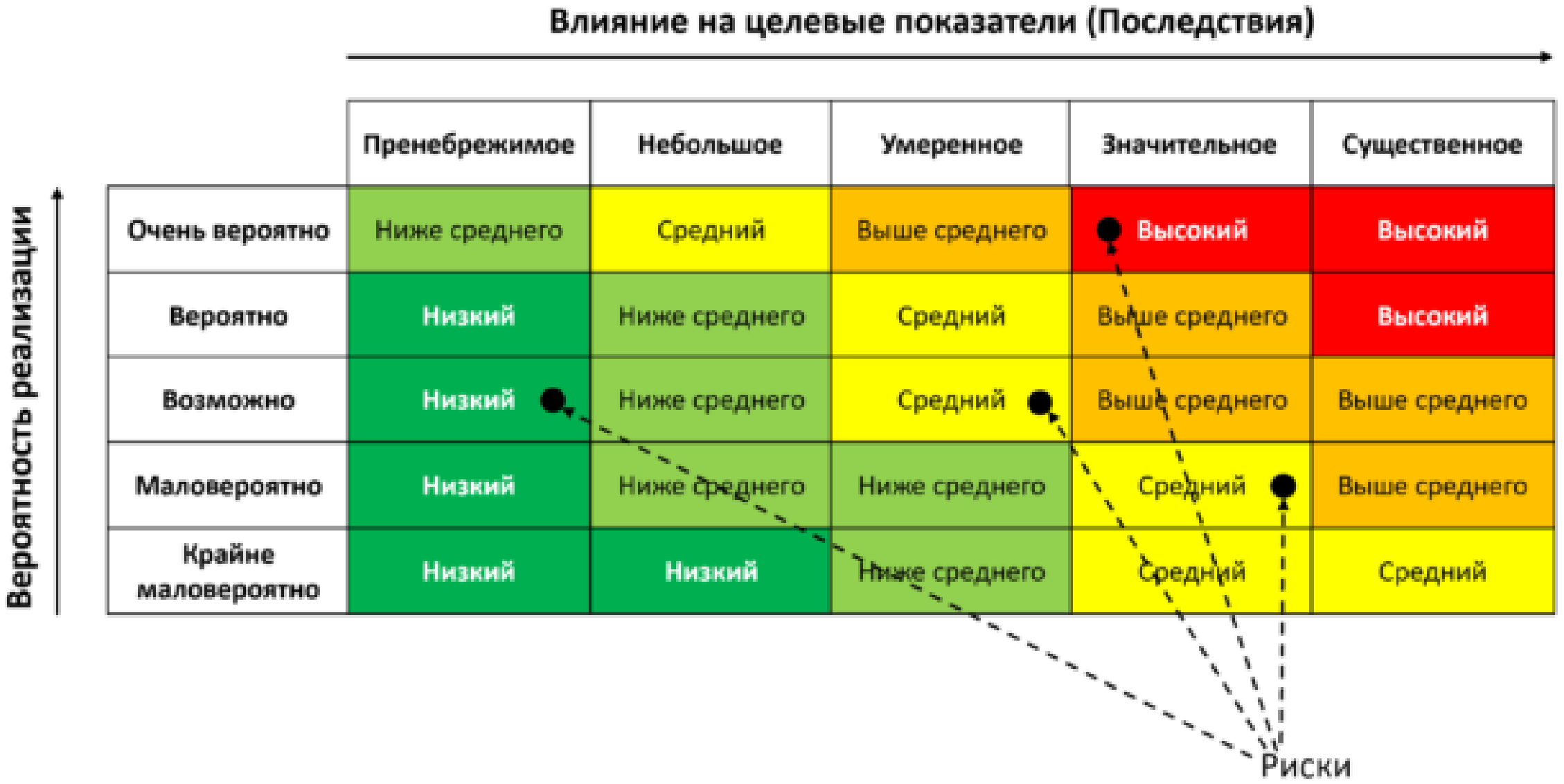
Иллюстрация

Иллюстрация

Риски


Высокая
Средняя
Низкая
Вероятность наступления риска
Степень негативного воздействия в случае наступления риска

Карта рисков



Матрица «вероятность - последствия»

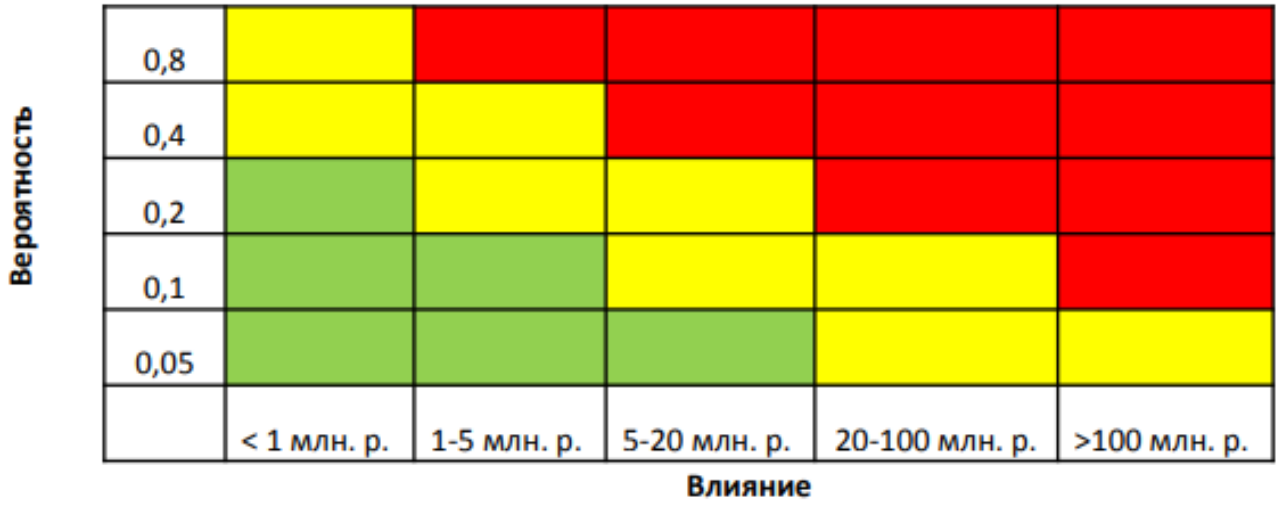
Качественные оценки

Балльные оценки

Вероятность						
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Влияние

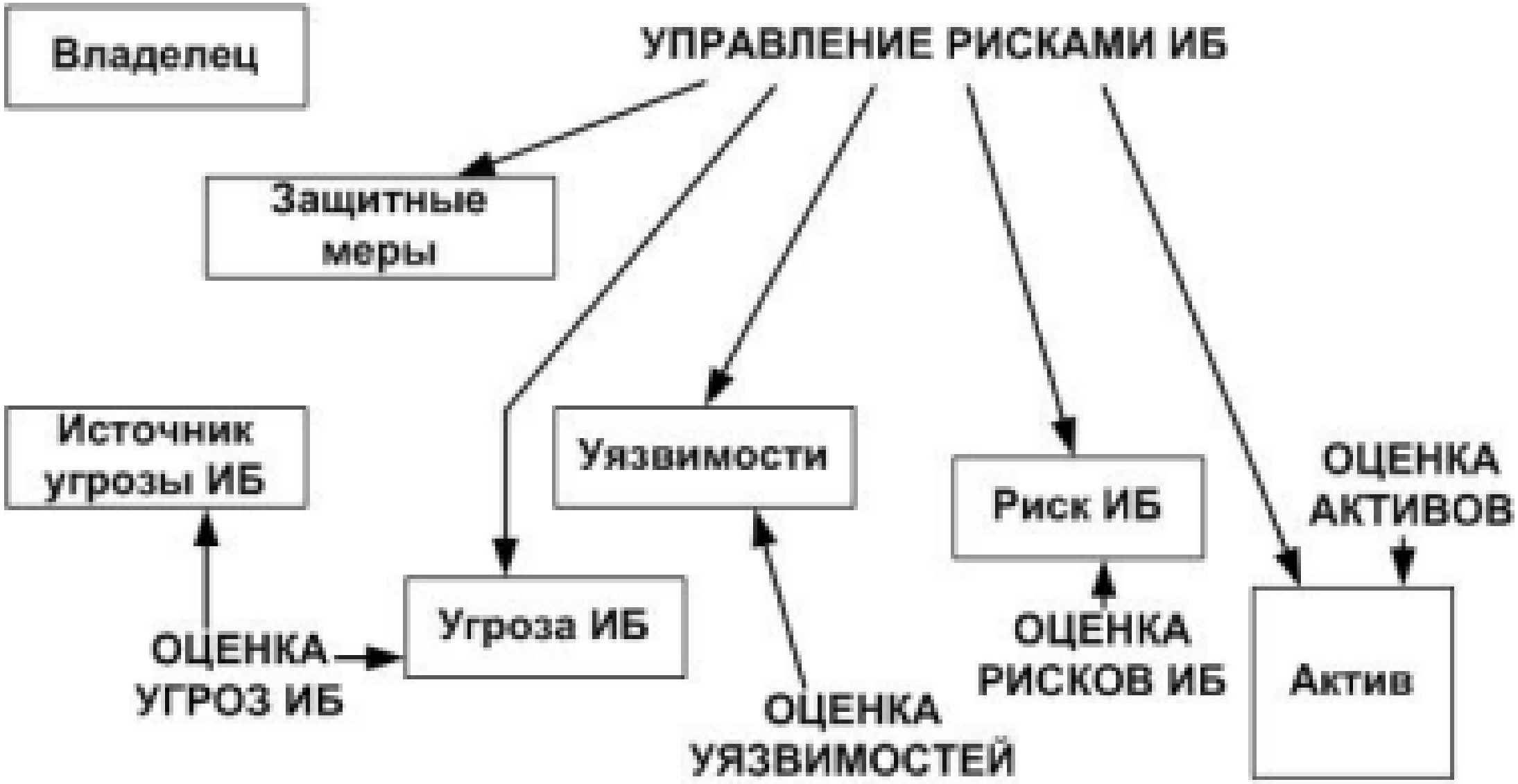
Количественные оценки



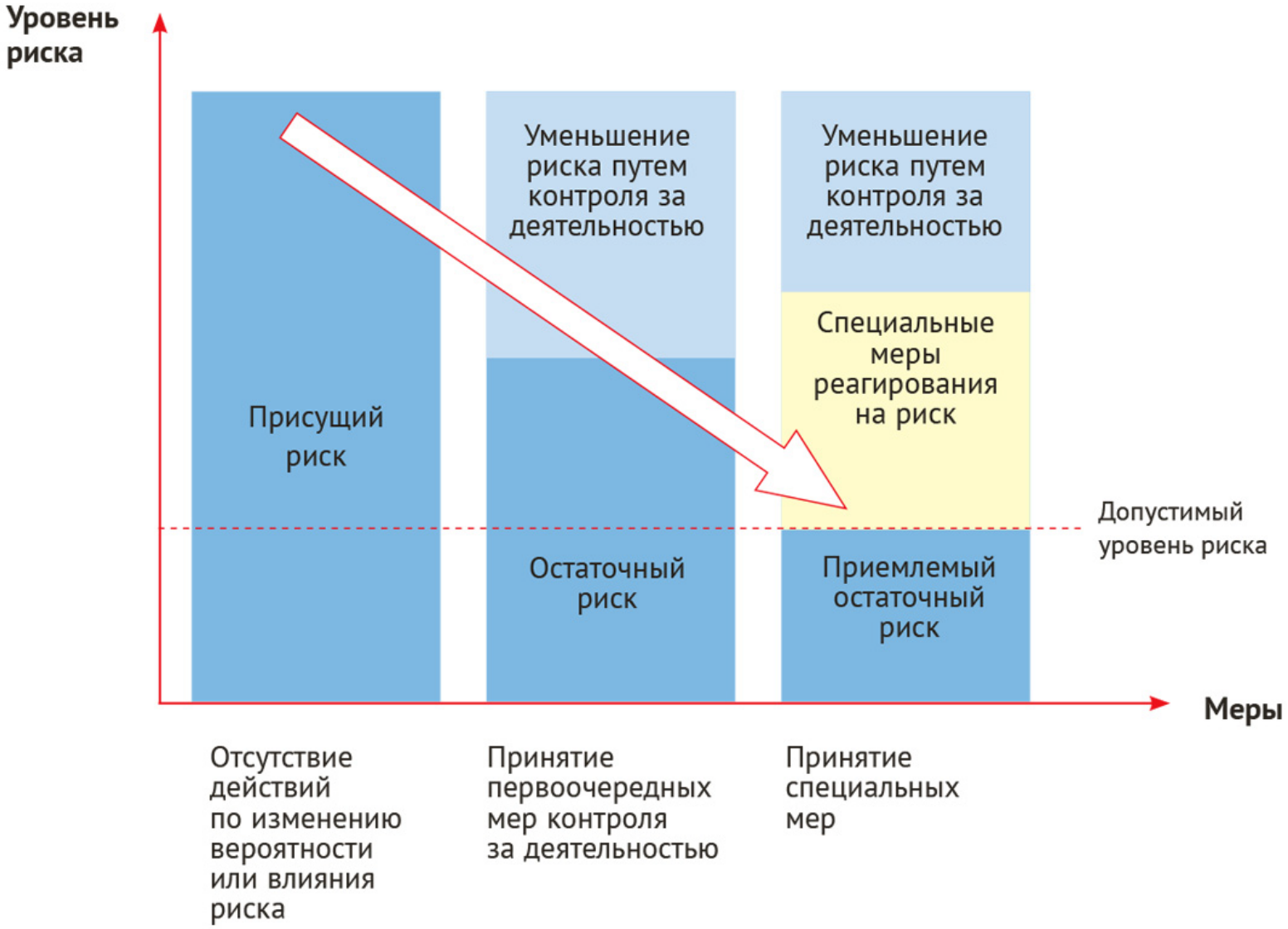
Измерение рисков/угроз ИБ

	Почти нереально	Маловероятно	Возможно	Вероятно	Очень вероятно
Катастрофически	6	7	8	9	10
Значительно	5	6	7	8	9
Умеренно	4	5	6	7	8
Незначительно	3	4	5	6	7
Несущественно	2	3	4	5	6
	Принять (уровень = 2,3)	Мониторить (уровень = 4,5)	Управлять (уровень = 6)	Избежать / разрулить (уровень = 7)	Немедленно избежать / разрулить (уровень = 8, 9, 10)

Управление рисками



Общая логика Снижения Уровня риска до приемлемого уровня



3. Классификация рисков

Классификация рисков

- Существуют **также условные классификации рисков**:
  - **по источнику риска** (например, атаки хакеров или инсайдеров, финансовые ошибки, воздействие государственных регуляторов, юридические претензии контрагентов, негативное информационное воздействие конкурентов);
  - **по цели** (информационные активы, физические активы, репутация, бизнес-процессы);
  - **по продолжительности влияния** (операционные, тактические, стратегические).

Цели анализа рисков

- **Цели анализа рисков ИБ** таковы:
  1. **Идентифицировать** активы и оценить их ценность.
  2. **Идентифицировать** угрозы активам и уязвимости в системе защиты.
  3. **Просчитать** вероятность реализации угроз и их влияние на бизнес (англ. business impact).
  4. **Соблюсти** баланс между стоимостью возможных негативных последствий и стоимостью мер защиты, дать рекомендации руководству компании по обработке выявленных рисков.

Цели анализа рисков

- **Этапы с 1-го по 3-й являются оценкой риска (англ. risk assessment)** и представляют собой сбор имеющейся информации. **Этап 4** представляет из себя уже непосредственно **анализ рисков (англ. risk analysis)**, т.е. изучение собранных данных и выдачу результатов/указаний для дальнейших действий. При этом важно понимать собственный уровень уверенности в корректности проведенной оценки.
- **На этапе 4** также предлагаются методы обработки для каждого из актуальных рисков:
  - **передача** (например, путем страхования),
  - **избегание** (например, отказ от внедрения той или иной технологии или сервиса),
  - **принятие** (сознательная готовность понести ущерб в случае реализации риска),
  - **минимизация** (применение мер для снижения вероятности негативного события, приводящего к реализации риска).
- После завершения всех этапов анализа рисков следует выбрать приемлемый для компании **уровень рисков (англ. acceptable risk level)**, установить **минимально возможный уровень безопасности (англ. baselines of performance)**, затем внедрить контрмеры и в дальнейшем оценивать их с точки зрения достижимости установленного минимально возможного уровня безопасности.

Ущерб от реализации атаки

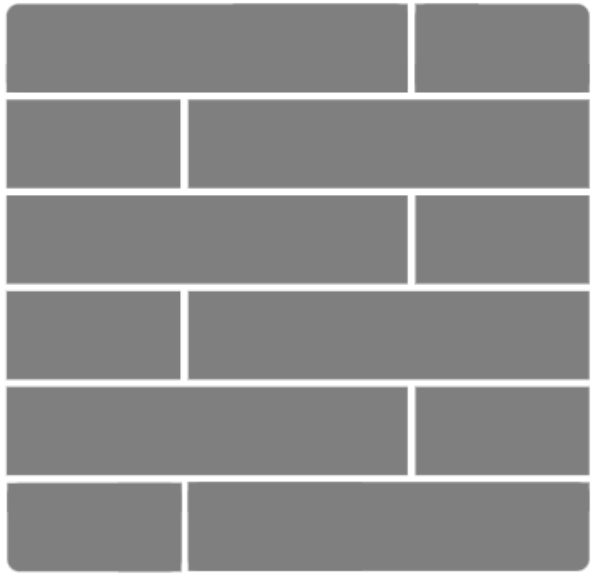
- **Ущерб от реализации атаки может быть прямым или непрямым.**

- **Прямой ущерб** — это непосредственные очевидные и легко прогнозируемые потери компании, такие как утеря прав интеллектуальной собственности, разглашение секретов производства, снижение стоимости активов или их частичное или полное разрушение, судебные издержки и выплата штрафов и компенсаций и т.д.

- **Непрямой ущерб** может означать качественные или косвенные потери.
- Качественными потерями могут являться приостановка или снижение эффективности деятельности компании, потеря клиентов, снижение качества производимых товаров или оказываемых услуг. Косвенные потери — это, например, недополученная прибыль, потеря деловой репутации, дополнительно понесенные расходы.
- Кроме этого, в зарубежной литературе встречаются также такие понятия, как **тотальный риск** (англ. total risk), который присутствует, если вообще никаких мер защиты не внедряется, а также **остаточный риск** (англ. residual risk), который присутствует, если угрозы реализовались, несмотря на внедренные меры защиты.

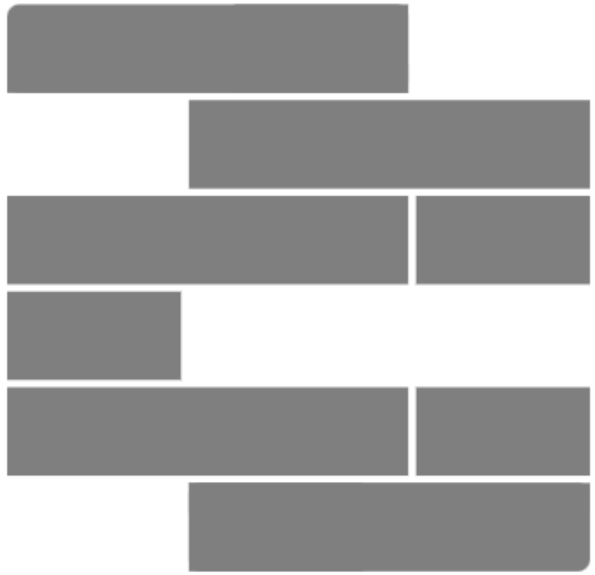
Оценка эффективности решений по устранению рисков

Выполняет все свои функции



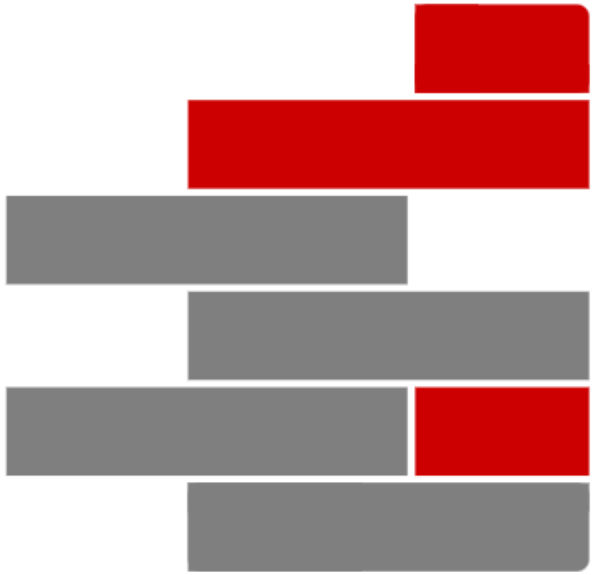
Допустимый ущерб

Выполняет свои функции частично



Значительный ущерб

Не выполняет свои функции



Недопустимый ущерб

4. Методологии риск-менеджмента


acceptable risk level
CYBER RISK
ARO
baselines of performance
NIST SP 800-37
AssetValue*EF.
Facilitated Risk Analysis Process
NIST Risk Management Framework
iso 27005
total risk
EF
ISO/IEC 27005:2018
NIST SP 800-30
CRAMM
risk governance
OCTAVE
NZS 4360
FRAP
SLE
security risk management
RISK ANALYSIS
Failure Modes and Effect Analysis
iso 31000
RISK GOVERNANCE
RISK ASSESSMENT
RESIDUAL RISK
Managing Information Security Risk
FMEA
residual risk
ASSETVALUESECURITY VISION
ALE
iso 31000
risk-based security
FAULT TREE ANALYSIS
Guide for Conducting Risk Assessments
cybersecurity framework
NIST 800
NIST SP 800-39
International Organization for Standardization

Методологии риск-менеджмента

Методологии риск-менеджмента

- РБ – Методика по **СТБ 34.101.70-2016**
- РФ – Методика по **ГОСТ Р ИСО/МЭК 27005**
- **Стандарты Международной организации по стандартизации ISO** (International Organization for Standardization)
- Фреймворк «**NIST Risk Management Framework**»
- Методология **FRAP** (Facilitated Risk Analysis Process)
- Методология **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- Стандарт **AS/NZS 4360**
- Методология **FMEA** (Failure Modes and Effect Analysis)
- Методология **CRAMM** (Central Computing and Telecommunications Agency Risk Analysis and Management Method)
- Методология **FAIR** (Factor Analysis of Information Risk)
- Концепция **COSO ERM** (Enterprise Risk Management)

Методологии риск-менеджмента

- **Фреймворк «NIST Risk Management Framework»** на базе американских правительственных документов NIST (National Institute of Standards and Technology, Национального института стандартов и технологий США) включает в себя набор взаимосвязанных т.н. «специальных публикаций» (Special Publication (SP):
  - **NIST SP 800-39** «Managing Information Security Risk»
  - **NIST SP 800-37** «Risk Management Framework for Information Systems and Organizations»
  - **NIST SP 800-30** «Guide for Conducting Risk Assessments»
  - **NIST SP 800-137** «Information Security Continuous Monitoring»

Методологии риск-менеджмента

- **Стандарты Международной организации по стандартизации ISO** (International Organization for Standardization):
  - **ISO/IEC 27005:2018** Information technology — Security techniques — Information security risk management
  - **ISO/IEC 27102:2019** Information security management — Guidelines for cyber-insurance
  - **ISO/IEC 31000:2018** Risk management — Guidelines

Методологии риск-менеджмента

- **Методология FRAP (Facilitated Risk Analysis Process)** является относительно упрощенным способом оценки рисков, с фокусом только на самых критичных активах. Качественный анализ проводится с помощью экспертной оценки.

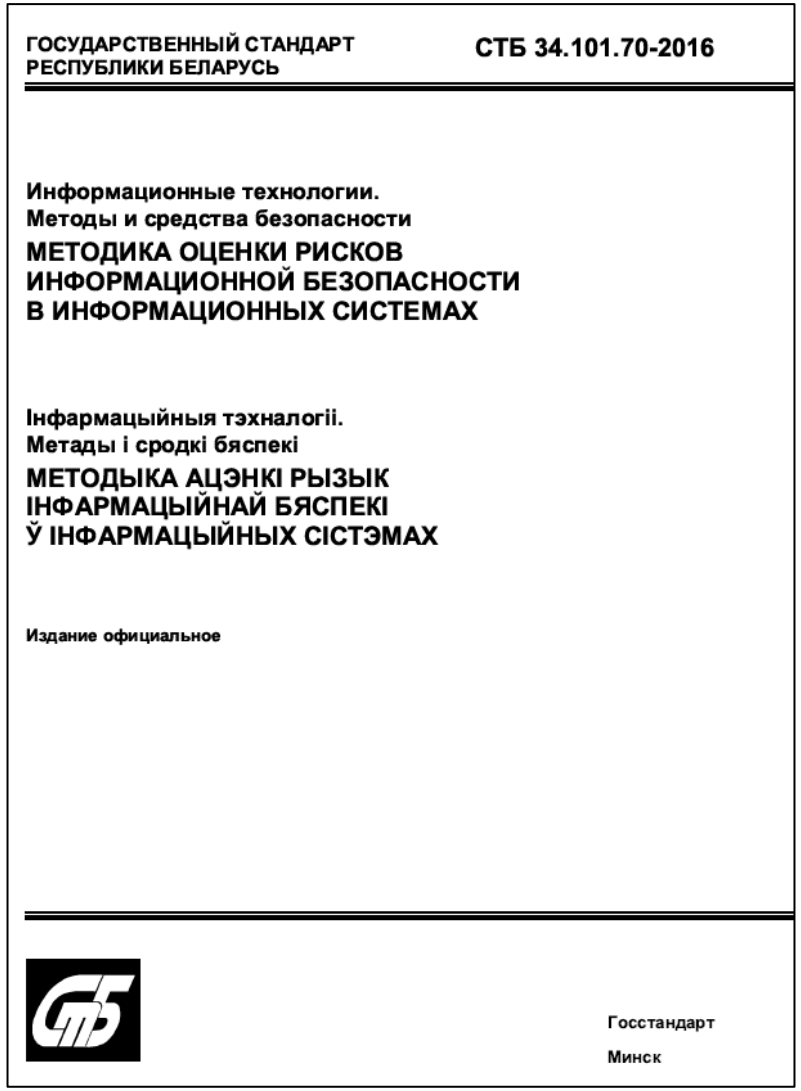
- **Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)** разработана в Институте программной инженерии при Университете Карнеги—Меллона. Она сфокусирована на самостоятельной работе членов бизнес-подразделений. Она используется для масштабной оценки всех информационных систем и бизнес-процессов компании.

Методологии риск-менеджмента

- **Стандарт AS/NZS 4360** является австралийским и новозеландским стандартом с фокусом не только на ИТ-системах, но и на бизнес-здоровье компании, т.е. предлагает более глобальный подход к управлению рисками. Отметим, что данный стандарт в настоящий момент заменен на стандарт AS/NZS ISO 31000-2009.
- **Методология FMEA (Failure Modes and Effect Analysis)** предлагает проведение оценки системы с точки зрения её слабых мест для поиска ненадежных элементов.
- **Методология CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method)** разработана Central Computer and Telecommunications Agency (Великобритания), предлагает использование автоматизированных средств для управления рисками.

5. Методика оценки рисков информационной безопасности в информационных системах по СТБ 34.101.70-2016

СТБ 34.101.70-2016



ГОСУДАРСТВЕННЫЙ СТАНДАРТ
РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ 34.101.70-2016

Информационные технологии.
Методы и средства безопасности
МЕТОДИКА ОЦЕНКИ РИСКОВ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Інфармацыйныя тэхналогіі.
Метады і сродкі бяспекі
МЕТОДЫКА АЦЭНКІ РЫЗЫК
ІНФАРМАЦЫЙНАЙ БЯСПЕКІ
Ў ІНФАРМАЦЫЙНЫХ СІСТЭМАХ

Издание официальное

Госстандарт
Минск

СТБ 34.101.70-2016. Информационные технологии. Методы и средства безопасности. **Методика оценки рисков информационной безопасности в информационных системах**. - Введ. 01.04.2017. - Минск : Госстандарт : БелГИСС, 2016. - 35 с.

СТБ 34.101.70-2016 Методика оценки рисков информационной безопасности в информационных системах

- **Область применения**
- Настоящий стандарт устанавливает требования по выполнению процедуры оценки рисков информационной безопасности (ИБ) в информационных системах (ИС).
- **Настоящий стандарт содержит:**
  - описание процесса оценки рисков ИБ в ИС;
  - рекомендации по выбору методов оценки рисков ИБ;
  - пример оценки рисков ИБ в ИС
- Стандарт может применяться организациями - владельцами ИС, органами, осуществляющими контроль за нарушением ИБ в ИС.

СТБ 34.101.70-2016 Методика оценки рисков информационной безопасности в информационных системах

- **Общие положения**
- Оценка рисков определяет ценность информационных активов, идентифицирует применимые угрозы и уязвимости, которые существуют (или могут существовать), идентифицирует существующие средства управления и их влияние на идентифицированные риски, определяет потенциальные последствия и, наконец, приоритизирует риски и ранжирует их согласно критериям оценивания рисков, заданным при установлении контекста.
- **На основе задач и целей оценки рисков различают следующие подходы к оценке рисков:**
  - **высокоуровневая оценка ИБ, являющейся общей для всех ИС;**
  - **детальная оценка, учитывающая особенности эксплуатации конкретных типов ИС.**
- Основное различие между ними состоит в степени глубины проводимого анализа. Поскольку обычно проведение детального анализа рисков для всех ИС сопряжено со слишком большими затратами, тогда как поверхностное рассмотрение проблем, связанных с рисками, не дает нужного эффекта, необходимо найти баланс между рассматриваемыми подходами.

СТБ 34.101.70-2016 Методика оценки рисков информационной безопасности в информационных системах

- **При высокоуровневой оценке рисков ИБ** эксперт (группа экспертов) использует справочные материалы (каталоги) о базовых наборах требований ИБ, из которых можно подобрать наиболее актуальные угрозы для рассматриваемой ИС.
- Существует ряд преимуществ использования этого варианта подхода, в том числе:
  - возможность обойтись минимальным количеством ресурсов при проведении оценки рисков;
  - ресурсы и денежные средства могут быть применены там, где они наиболее полезны, и ИС, наиболее нуждающиеся в защите, будут рассмотрены первыми.
- В то же время этот вариант подхода имеет следующий недостаток: **высокоуровневый анализ рисков является менее точным**, поэтому некоторые риски могут быть не идентифицированы, что может привести к нарушению ИБ ИС.
- Если цели актива крайне важны для ведения бизнеса организации или если активы имеют высокий уровень риска, то для конкретного актива ИС (или его части) должна быть проведена детальная оценка рисков ИБ.

СТБ 34.101.70-2016 Методика оценки рисков информационной безопасности в информационных системах

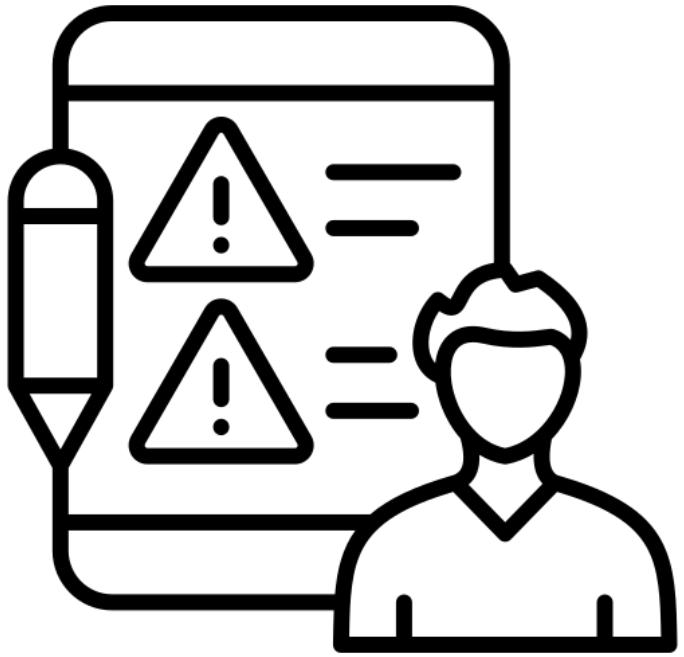
- **Здесь применяется следующее общее правило:** если отсутствие ИБ может привести к существенным неблагоприятным последствиям для организации, ее бизнес-процессов или ее активов, то необходима оценка рисков на более детальном уровне для идентификации потенциальных рисков.
- **Детальный процесс оценки рисков ИБ включает в себя** тщательную идентификацию и определение ценности активов, оценку угроз этим активам и оценку уязвимостей. Результаты этих мероприятий потом используются для оценки рисков, а затем - для идентификации оправданных средств управления безопасности.
- Детальная последовательность действий обычно требует значительного времени, усилий и компетентности и поэтому может быть наиболее пригодной для ИС с высоким уровнем риска.

СТБ 34.101.70-2016 Методика оценки рисков информационной безопасности в информационных системах

- **5 Процесс оценки рисков информационной безопасности в информационных системах**
- 5.1 Идентификация активов
- 5.2 Идентификация угроз
- 5.3 Идентификация уязвимостей
- 5.4 Идентификация мер защиты
- 5.5 Оценка вероятности реализации угроз
- 5.6 Оценка возможных последствий
- 5.7 Оценка рисков
- 5.8 Документирование результатов

СТБ 34.101.70-2016 Методика оценки рисков информационной безопасности в информационных системах

- **6 Выбор метода оценки рисков**
- 6.1 Общие положения по выбору метода оценки рисков
- 6.2 Метод идентификации активов и сбора информации об информационной системе
- 6.3 Метод идентификации угроз
- 6.4 Метод идентификации уязвимостей
- 6.5 Анализ мер защиты
- 6.6 Методы оценки вероятности реализации угроз
- 6.7 Метод оценки влияния угроз
- 6.8 Метод оценки рисков информационной безопасности



6. Фреймворк «NIST Risk Management Framework»

NIST Risk Management Framework

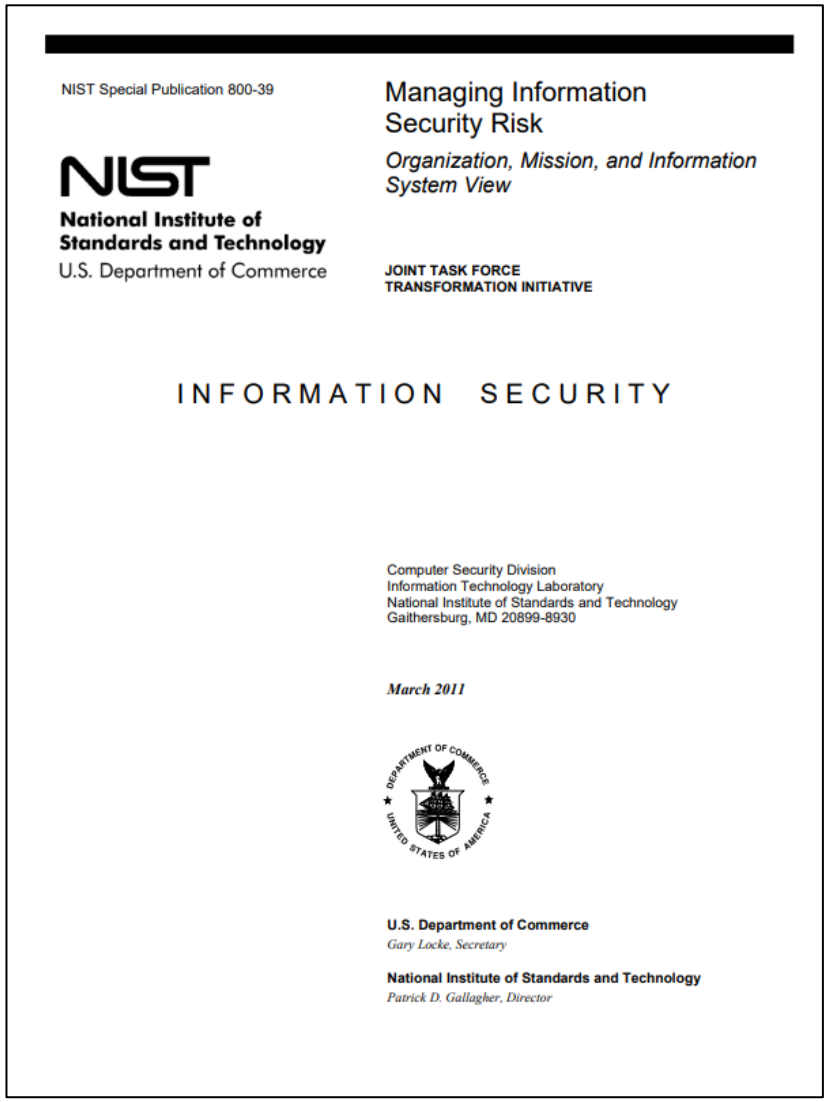
- **Фреймворк «NIST Risk Management Framework»** на базе американских правительственных документов NIST (National Institute of Standards and Technology, Национального института стандартов и технологий США) включает в себя набор взаимосвязанных т.н. «специальных публикаций» (англ. Special Publication (SP), будем для простоты восприятия называть их стандартами):

  1. **Стандарт NIST SP 800-39 «Managing Information Security Risk»** («Управление рисками информационной безопасности»)
  2. **Стандарт NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations»** («Фреймворк управления рисками для информационных систем и организаций»)
  3. **Стандарт NIST SP 800-30 «Guide for Conducting Risk Assessments»** («Руководство по проведению оценки рисков»)
  4. **Стандарт NIST SP 800-137 «Information Security Continuous Monitoring»** («Непрерывный мониторинг информационной безопасности»)

Стандарты NIST SP 800

- **1. Стандарт NIST SP 800-39 «Managing Information Security Risk» («Управление рисками информационной безопасности»)** предлагает трехуровневый подход к управлению рисками: организация, бизнес-процессы, информационные системы. Данный стандарт описывает методологию процесса управления рисками: определение, оценка, реагирование и мониторинг рисков.
- **2. Стандарт NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations»** («Фреймворк управления рисками для информационных систем и организаций») предлагает для обеспечения безопасности и конфиденциальности использовать подход управления жизненным циклом систем.
- **3. Стандарт NIST SP 800-30 «Guide for Conducting Risk Assessments» («Руководство по проведению оценки рисков»)** сфокусирован на ИТ, ИБ и операционных рисках. Он описывает подход к процессам подготовки и проведения оценки рисков, коммуницирования результатов оценки, а также дальнейшей поддержки процесса оценки.
- **4. Стандарт NIST SP 800-137 «Information Security Continuous Monitoring»** («Непрерывный мониторинг информационной безопасности») описывает подход к процессу мониторинга информационных систем и ИТ-сред в целях контроля примененных мер обработки рисков ИБ и необходимости их пересмотра.

NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View



NIST Special Publication 800-39

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Managing Information Security Risk

Organization, Mission, and Information System View

JOINT TASK FORCE TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2011

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

- **NIST SP 800-39** Managing Information Security Risk: Organization, Mission, and Information System View
- (**Управление риском информационной безопасности: Уровень организации, миссии, информационной системы**)
- https://csrc.nist.gov/publications/detail/sp/800-39/final
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST SP 800-39

- Документ **NIST SP 800-39 «Managing Information Security Risk: Organization, Mission, and Information System View» («Управление риском информационной безопасности: Уровень организации, миссии, информационной системы»)** предлагает вендоро-независимый, структурированный, но гибкий подход к управлению рисками ИБ в контексте операционной деятельности компании, активов, физических лиц и контрагентов.
- При этом риск-менеджмент должен быть целостным процессом, затрагивающим всю организацию, в которой практикуется риск-ориентированное принятие решений на всех уровнях.
- Управление риском определяется в данном документе как всеобъемлющий процесс, включающий в себя этапы определения (frame), оценки (assess), обработки (respond) и мониторинга (monitor) рисков. Рассмотрим эти этапы подробнее.

NIST SP 800-39

- **1. На этапе определения рисков** организации следует выявить:
- **предположения о рисках**, т.е. идентифицировать актуальные угрозы, уязвимости, последствия, вероятность возникновения рисков;
- **ограничения рисков**, т.е. возможности осуществления оценки, реагирования и мониторинга;
- **риск-толерантность**, т.е. терпимость к рискам — приемлемые типы и уровни рисков, а также допустимый уровень неопределенности в вопросах управления рисками;
- **приоритеты и возможные компромиссы**, т.е. нужно приоритизировать бизнес-процессы, изучить компромиссы, на которые может пойти организация при обработке рисков, а также временные ограничения и факторы неопределенности, сопровождающие этот процесс.

NIST SP 800-39

- **2. На этапе оценки рисков** организации следует выявить:
- **угрозы ИБ**, т.е. конкретные действия, лиц или сущности, которые могут являться угрозами для самой организации или могут быть направлены на другие организации;
- **внутренние и внешние уязвимости**, включая организационные уязвимости в бизнес-процессах управления компанией, архитектуре ИТ-систем и т.д.;
- **ущерб** организации с учетом возможностей эксплуатации уязвимостей угрозами;
- **вероятность возникновения ущерба**.

- В итоге организация получает детерминанты риска, т.е. уровень ущерба и вероятность возникновения ущерба для каждого риска.

NIST SP 800-39

- Для обеспечения процесса оценки рисков организация предварительно определяет:
  - инструменты, техники и методологии, используемые для оценки риска;
  - допущения относительно оценки рисков;
  - ограничения, которые могут повлиять на оценки рисков;
  - роли и ответственность;
  - способы сбора, обработки и передачи информации об оценке рисков в пределах организации;
  - способы проведения оценки рисков в организации;
  - частоту проведения оценки рисков;
  - способы получения информации об угрозах (источники и методы).

NIST SP 800-39

- **3. На этапе реагирования на риск** организация выполняет следующие работы:
  - разработку возможных планов реагирования на риск;
  - оценку возможных планов реагирования на риск;
  - определение планов реагирования на риск, допустимых с точки зрения риск-толерантности организации;
  - реализацию принятых планов реагирования на риск.

- Для обеспечения возможности реагирования на риски организация определяет типы возможной обработки рисков (принятие, избегание, минимизация, разделение или передача риска), а также инструменты, технологии и методологии для разработки планов реагирования, способы оценки планов реагирования и методы оповещения о предпринятых мерах реагирования в рамках организации и/или внешних контрагентов.

NIST SP 800-39

- **4. На этапе мониторинга рисков** решаются следующие задачи:
  - проверка реализации принятых планов реагирования на риск и выполнения нормативных требований ИБ;
  - определение текущей эффективности мер реагирования на риски;
  - определение значимых для риск-менеджмента изменений в ИТ-системах и средах, включая ландшафт угроз, уязвимости, бизнес-функции и процессы, архитектуру ИТ-инфраструктуры, взаимоотношения с поставщиками, риск-толерантность организации и т.д.

- Организации описывают методы оценки нормативного соответствия и эффективности мер реагирования на риски, а также то, как контролируются изменения, способные повлиять на эффективность реагирования на риски.

NIST SP 800-39

- **Управление рисками ведется на уровнях**
  - организации,
  - бизнес-процессов
  - и информационных систем,
- при этом следует обеспечивать взаимосвязь и обмен информацией между данными уровнями в целях непрерывного повышения эффективности осуществляемых действий и коммуникации рисков всем стейкхолдерам.

NIST SP 800-39

- **На верхнем уровне (уровне организации)** осуществляется принятие решений по определению рисков, что напрямую влияет на процессы, ведущиеся на нижележащих уровнях (бизнес-процессов и информационных систем), а также на финансирование этих процессов.
- **На уровне организации** осуществляются выработка и внедрение функций управления, согласующихся с бизнес-целями организации и с нормативными требованиями: создание функции риск-менеджмента, назначение ответственных, внедрение стратегии управления рисками и определение риск-толерантности, разработка и реализация инвестиционных стратегий в ИТ и ИБ.

NIST SP 800-39

- **На уровне бизнес-процессов** осуществляются определение и создание риск-ориентированных бизнес-процессов и организационной архитектуры, которая должна быть основана на сегментации, резервировании ресурсов и отсутствии единых точек отказа. Кроме того, на данном уровне осуществляется разработка архитектуры ИБ, которая обеспечит эффективное выполнение требований ИБ и внедрение всех необходимых мер и средств защиты.
- **На уровне информационных систем** следует обеспечить выполнение решений, принятых на более высоких уровнях, а именно обеспечить управление рисками ИБ на всех этапах жизненного цикла систем: инициализации, разработки или приобретения, внедрения, использования и вывода из эксплуатации. В документе подчеркивается важность стойкости (resilience) ИТ-систем, которая является показателем жизнеспособности бизнес-функций компании.

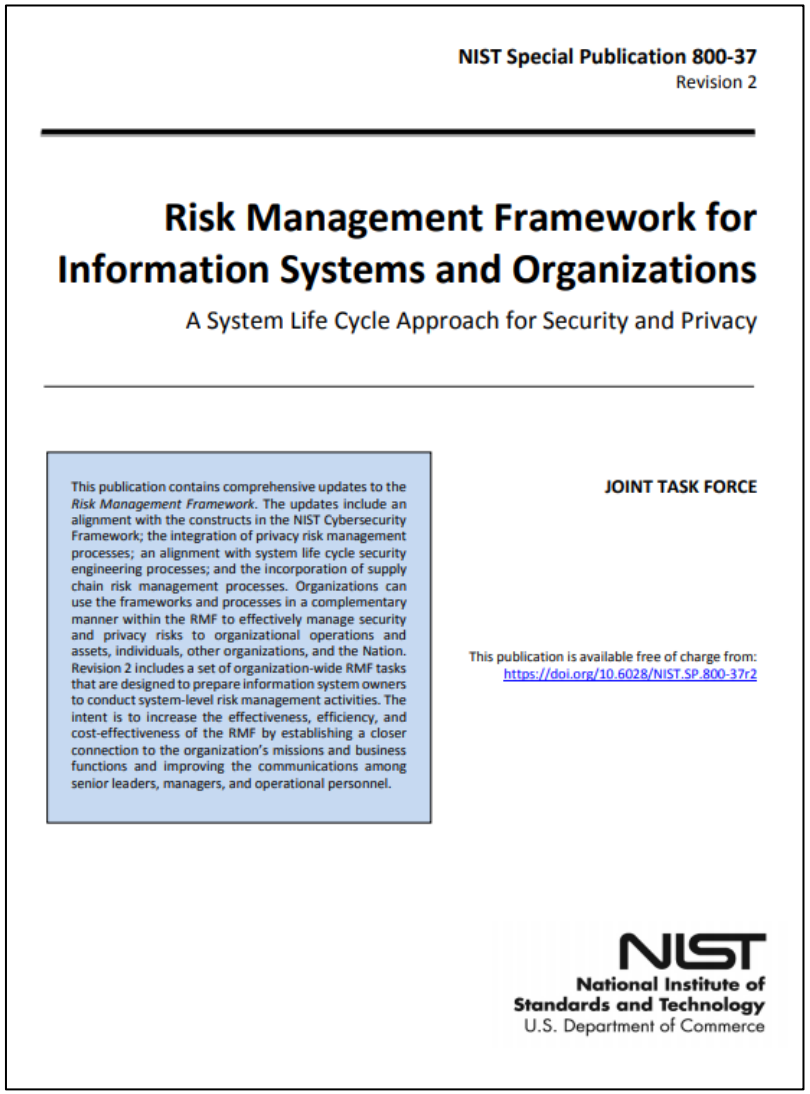
NIST SP 800-39

- В приложении «H» к рассматриваемому в документу приводится описание каждого из способов обработки рисков, перечисленных в этапе реагирования на риск. Так, указано, что в организации должна существовать как общая стратегия выбора конкретного способа обработки риска в той или иной ситуации, так и отдельные стратегии для каждого из способов обработки рисков.
- Указаны основные принципы выбора того или иного **подхода к обработке рисков**:
  - принятие (acceptance) риска
  - избегание (avoidance) риска
  - разделение (share) и передача (transfer) рисков
  - минимизация (или смягчение) (mitigation) рисков

NIST SP 800-39

- **В документе также уделено большое внимание организационной культуре** и доверию поставщикам/контрагентам как факторам успешного управления рисками. В частности, говорится, что организационная культура и топ-менеджеры компании напрямую влияют на выбираемые решения по обработке рисков, поэтому общая стратегия риск-менеджмента должна учитывать риск-аппетит компании и отражать реально практикующиеся способы управления рисками. Модели построения доверия с контрагентами и поставщиками описаны в приложении «G»: перечислены модели, базирующиеся на проверках контрагентов (например, путем проведения аудитов), на исторически сложившемся доверии (когда за многолетнюю историю взаимоотношений контрагент не допускал нарушений), на доверии третьей стороне (которая проводит независимую оценку контрагентов), на мандатном доверии (в случае, когда регуляторными нормами устанавливаются требования о доверии такому поставщику), а также гибридная модель.

NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy



NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- **NIST SP 800-37** «Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy» («**Фреймворк управления рисками для информационных систем и организаций: жизненный цикл систем для обеспечения безопасности и конфиденциальности**»).
- https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST SP 800-37

- Актуальный документ **NIST SP 800-37** имеет редакцию №2 и был обновлен в декабре 2018 с тем, чтобы учесть современный ландшафт угроз и акцентировать внимание на важности управления рисками на уровне руководителей компаний, подчеркнуть связь между фреймворком управления рисками (Risk Management Framework, RMF) и фреймворком кибербезопасности (Cybersecurity Framework, CSF), указать на важность интеграции процессов управления конфиденциальностью (англ. privacy) и управления рисками цепочек поставок (англ. supply chain risk management, SCRM), а также логически увязать список предлагаемых мер защиты (контролей, англ. controls) с документом NIST SP 800-53.
- Кроме этого, выполнение положений NIST SP 800-37 можно использовать при необходимости провести взаимную оценку процедур риск-менеджмента компаний в случаях, когда этим компаниям требуется обмениваться данными или ресурсами.
- По аналогии с NIST SP 800-39, рассматривается управление рисками на уровнях организации, миссии, информационных систем.

NIST SP 800-37

- В NIST SP 800-37 указано, что **Risk Management Framework** в целом указывает на важность разработки и внедрения возможностей по обеспечению безопасности и конфиденциальности в ИТ-системах **на протяжении всего жизненного цикла** (англ. system development life cycle, SDLC), непрерывной поддержки ситуационной осведомленности о состоянии защиты ИТ-систем с применением процессов непрерывного мониторинга (continuous monitoring, CM) и предоставления информации руководству для принятия взвешенных риск-ориентированных решений.
- В RMF выделены **следующие типы рисков**: программный риск, риск несоответствия законодательству, финансовый риск, юридический риск, бизнес-риск, политический риск, риск безопасности и конфиденциальности (включая риск цепочки поставок), проектный риск, репутационный риск, риск безопасности жизнедеятельности, риск стратегического планирования.

NIST SP 800-37

- Кроме этого, **Risk Management Framework**:
  - предоставляет повторяемый процесс для риск-ориентированной защиты информации и информационных систем;
  - подчеркивает важность подготовительных мероприятий для управления безопасностью и конфиденциальностью;
  - обеспечивает категоризацию информации и информационных систем, а также выбора, внедрения, оценки и мониторинга средств защиты;
  - предлагает использовать средства автоматизации для управления рисками и мерами защиты в режиме, близком к реальному времени, а также актуальные временные метрики для предоставления информации руководству для принятия решений;
  - связывает процессы риск-менеджмента на различных уровнях и указывает на важность выбора ответственных за приятие защитных мер.

NIST SP 800-37

- В документе указаны **7 этапов** применения RMF:
  1. **подготовка**, т.е. определение целей и их приоритизация с точки зрения организации и ИТ-систем;
  2. **категоризация** систем и информации на основе анализа возможного негативного влияния в результате потери информации (кроме негативного влияния, NIST SP 800-30 также указывает еще 3 фактора риска, учитываемых при проведении оценки риска: угрозы, уязвимости, вероятность события);
  3. **выбор** базового набора мер защиты и их уточнение (адаптация) для снижения риска до приемлемого уровня на основе оценки риска;
  4. **внедрение** мер защиты и описание того, как именно применяются меры защиты;
  5. **оценка** внедренных мер защиты для определения корректности их применения, работоспособности и продуцирования ими результатов, удовлетворяющих требованиям безопасности и конфиденциальности;
  6. **авторизация** систем или мер защиты на основе заключения о приемлемости рисков;
  7. **непрерывный мониторинг** систем и примененных мер защиты для оценки эффективности примененных мер, документирования изменений, проведения оценки рисков и анализа негативного влияния, создания отчетности по состоянию безопасности и конфиденциальности.

NIST SP 800-37

- Далее в публикации NIST SP 800-37 перечисляются задачи, которые следует выполнить на каждом из этапов применения RMF.
- Для каждой из задач указывается название задачи (контроля), перечисляются входные и выходные (результирующие) данные процесса с привязкой к категориям соответствующих контролей CSF, приводится список ответственных и вспомогательных ролей, дополнительное описание задачи, а также при необходимости даются ссылки на связанные документы NIST.

NIST SP 800-37

- Перечислим далее задачи для каждого из этапов применения RMF.
  - Задачи этапа «Подготовка»
  - Задачи этапа «Подготовка» на уровне ИТ-систем
  - Задачи этапа «Категоризация»
  - Задачи этапа «Выбор набора мер защиты»
  - Задачи этапа «Внедрение мер защиты»
  - Задачи этапа «Оценка внедренных мер защиты»
  - Задачи этапа «Авторизация»
  - Задачи этапа «Непрерывный мониторинг»

NIST SP 800-37

- **Задачи этапа «Подготовка»** на уровне организации включают в себя:
  - определение ролей для управления рисками;
  - создание стратегии управления рисками, с учетом риск-толерантности организации;
  - проведение оценки рисков;
  - выбор целевых значений мер защиты и/или профилей из документа Cybersecurity Framework;
  - определение для ИТ-систем общих мер защиты, которые могут быть унаследованы с более высоких уровней (например, с уровня организации или бизнес-процессов) приоритизацию ИТ-систем;
  - разработку и внедрение стратегии непрерывного мониторинга эффективности мер защиты.

NIST SP 800-37

- Задачи этапа **«Подготовка» на уровне ИТ-систем** включают в себя:
  - определение бизнес-функций и процессов, которые поддерживает каждая ИТ-система;
  - идентификацию лиц (стейкхолдеров), заинтересованных в создании, внедрении, оценке, функционировании, поддержке, выводе из эксплуатации систем;
  - определение активов, требующих защиты;
  - определение границы авторизации для системы;
  - выявление типов информации, обрабатываемых/передаваемых/хранимых в системе;
  - идентификацию и анализ жизненного цикла всех типов информации, обрабатываемых/передаваемых/хранимых в системе;
  - проведение оценки рисков на уровне ИТ-систем и обновление списка результатов оценки;
  - определение требований по безопасности и конфиденциальности для систем и сред функционирования;
  - определение местоположения систем в общей архитектуре компании;
  - распределение точек применения требований по безопасности и конфиденциальности для систем и сред функционирования;
  - формальную регистрацию ИТ-систем в соответствующих департаментах и документах.

NIST SP 800-37

- Задачи этапа **«Категоризация»** включают в себя:
  - документирование характеристик системы;
  - категоризацию системы и документирование результатов категоризации по требованиям безопасности;
  - пересмотр и согласование результатов и решений по категоризации по требованиям безопасности.

NIST SP 800-37

- Задачи этапа **«Выбор набора мер защиты»** включают в себя:
  - выбор мер защиты для системы и среды её функционирования;
  - уточнение (адаптация) выбранных мер защиты для системы и среды её функционирования;
  - распределение точек применения мер обеспечения безопасности и конфиденциальности к системе и среде её функционирования;
  - документирование запланированных мер обеспечения безопасности и конфиденциальности системы и среды её функционирования в соответствующих планах;
  - создание и внедрение стратегии мониторинга эффективности применяемых мер защиты, которая логически связана с общей организационной стратегией мониторинга и дополняет ее;
  - пересмотр и согласование планов обеспечения безопасности и конфиденциальности системы и среды её функционирования.

NIST SP 800-37

- Задачи этапа **«Внедрение мер защиты»** включают в себя:
  - внедрение мер защиты в соответствии с планами обеспечения безопасности и конфиденциальности;
  - документирование изменений в запланированные меры защиты постфактум, на основании реального результата внедрения.

NIST SP 800-37

- Задачи этапа **«Оценка внедренных мер защиты»** включают в себя:
  - выбор оценщика или команды по оценке, соответствующих типу проводимой оценки;
  - разработку, пересмотр и согласование планов по оценке внедренных мер защиты;
  - проведение оценки мер защиты в соответствии с процедурами оценки, описанными в планах оценки;
  - подготовку отчетов по оценке, содержащих найденные недочеты и рекомендации по их устранению;
  - выполнение корректирующих действий с мерами защиты и переоценку откорректированных мер;
  - подготовку плана действий на основании найденных недочетов и рекомендации из отчетов по оценке.

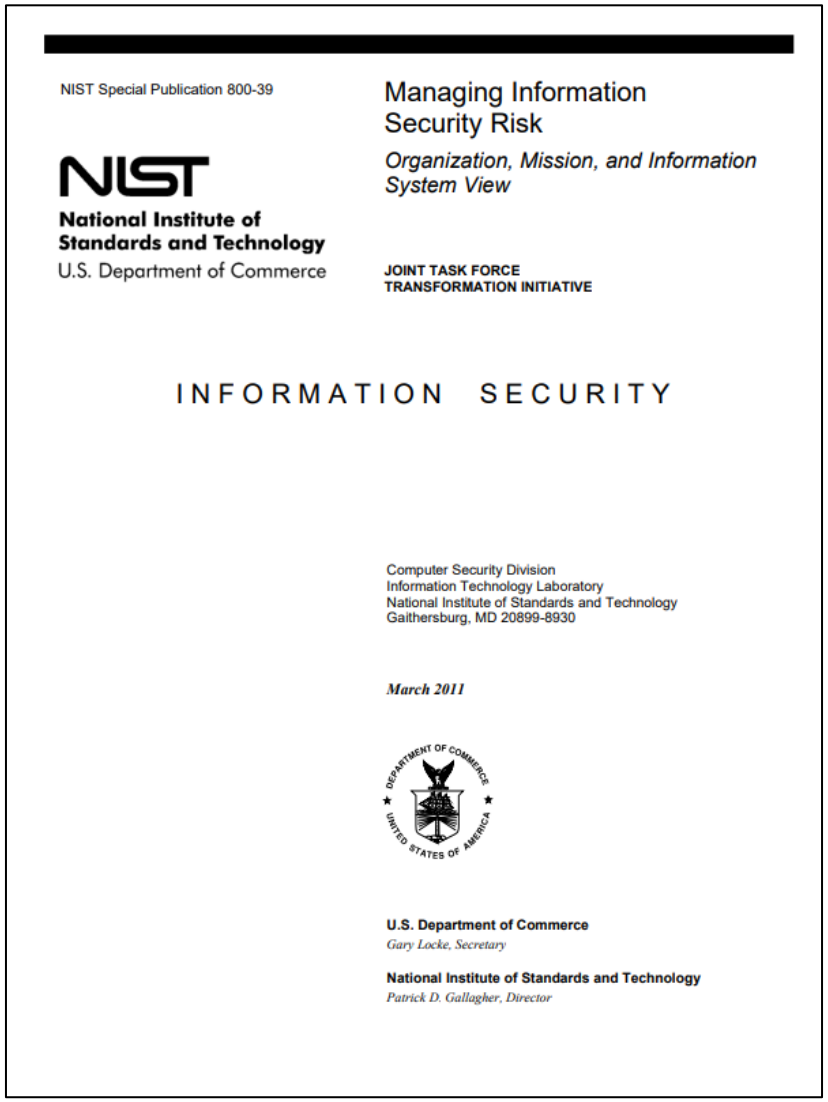
NIST SP 800-37

- Задачи этапа **«Авторизация»** включают в себя:
  - сбор авторизационного пакета документов и отправку его ответственному лицу на авторизацию;
  - анализ и определение риска использования системы или применения мер защиты;
  - определение и внедрение предпочтительного плана действий при реагировании на выявленный риск;
  - определение приемлемости риска использования системы или применения мер защиты;
  - сообщение о результатах авторизации и о любом недостатке мер защиты, представляющем значительный риск для безопасности или конфиденциальности.

NIST SP 800-37

- Задачи этапа **«Непрерывный мониторинг»** включают в себя:
  - мониторинг информационной системы и среды её функционирования на наличие изменений, которые влияют на состояние безопасности и конфиденциальности системы;
  - оценку мер защиты в соответствии со стратегией непрерывного мониторинга;
  - реагирование на риск на основе результатов непрерывного мониторинга, оценок риска, плана действий;
  - обновление планов, отчетов по оценке, планов действий на основании результатов непрерывного мониторинга;
  - сообщение о состоянии безопасности и конфиденциальности системы соответствующему должностному лицу в соответствии со стратегией непрерывного мониторинга;
  - пересмотр состояния безопасности и конфиденциальности системы для определения приемлемости риска;
  - разработку стратегии вывода системы из эксплуатации и выполнение соответствующих действий при окончании срока её службы.

NIST SP 800-30 Guide for Conducting Risk Assessments



NIST Special Publication 800-39

Managing Information Security Risk

Organization, Mission, and Information System View

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

JOINT TASK FORCE TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2011

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

- **NIST SP 800-30** «Guide for Conducting Risk Assessments» (**Руководство по проведению оценок риска**)
- https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST SP 800-30

- **NIST SP 800-30 «Guide for Conducting Risk Assessments» («Руководство по проведению оценок риска»)** посвящена процедуре проведения оценки риска, которая является фундаментальным компонентом процесса управления риском в организации в соответствии с NIST SP 800-39, наряду с определением, обработкой и мониторингом рисков. Процедуры оценки рисков используются для идентификации, оценки и приоритизации рисков, порождаемых использованием информационных систем, для операционной деятельности организации, её активов и работников.
- **Целями оценки рисков** являются информирование лиц, принимающих решения, и поддержка процесса реагирования на риск путем идентификации:
  - актуальных угроз как самой организации, так и опосредованно другим организациям;
  - внутренних и внешних уязвимостей;
  - потенциального ущерба организации с учетом возможностей эксплуатации уязвимостей угрозами;
  - вероятности возникновения этого ущерба.

NIST SP 800-30

- **Конечным результатом** является вычисление детерминанты (значения) риска, т.е. функции от размера ущерба и вероятности возникновения ущерба.
- Оценку риска можно проводить на всех трех уровнях управления рисками (уровни организации, миссии, информационных систем), по аналогии с подходом, применяемым в NIST SP 800-39 и NIST SP 800-37.
- Подчеркивается, что **оценка рисков** — это непрерывный процесс, затрагивающий все уровни управления рисками в организации, а также требующий включения в жизненный цикл разработки систем (англ. system development life cycle, SDLC) и проводимый с частотой, адекватной целям и объему оценки.

NIST SP 800-30

- **Процесс оценки рисков** включает в себя:
  - подготовку к оценке рисков;
  - проведение оценки рисков;
  - коммуницирование результатов оценки и передачу информации внутри организации;
  - поддержание достигнутых результатов.
- В документе говорится о важности составления методологии оценки риска, которая разрабатывается организацией на этапе определения рисков. Указано, что организация может выбрать одну или несколько методологий оценки риска, в зависимости от имеющихся ресурсов, фазы SDLC, сложности и зрелости бизнес-процессов, критичности/важности обрабатываемой информации. При этом созданием корректной методологии организация повышает качество и воспроизводимость реализуемых оценок риска.

NIST SP 800-30

- **Методология оценки риска** обычно включает в себя:
  - **описание процесса** оценки риска;
  - **модель рисков**, описывающая оцениваемые факторы риска и взаимосвязи между ними;
  - **способ оценки рисков** (например, качественный или количественный), описывающий значения, которые могут принимать факторы риска, и то, как комбинации этих факторов могут быть обработаны;
  - **способ анализа** (например, угрозо-центричный, ориентированный на активы или уязвимости), описывающий, как идентифицируются и анализируются комбинации факторов риска.

NIST SP 800-30

- **Модель рисков** описывает оцениваемые факторы риска и взаимосвязи между ними. **Факторы риска** — это характеристики, используемые в моделях риска в качестве входных данных для определения уровней рисков при проведении оценки рисков. Кроме этого, факторы риска используются при коммуницировании рисков для выделения тех факторов, которые ощутимо влияют на уровни рисков в определенных ситуациях и контекстах.
- **Типовые факторы риска включают в себя**:
  - угрозы;
  - уязвимости;
  - негативное влияние;
  - вероятность;
  - предварительные условия.
- При этом некоторые факторы риска могут быть декомпозированы до более детальных характеристик, например, угрозы можно декомпозировать до **источников угроз** (англ. threat sources) и **событий угроз** (англ. threat events).

NIST SP 800-30

- **Угроза** — это любое обстоятельство или событие, имеющее потенциал негативного влияния на бизнес-процессы или активы, сотрудников, другие организации путем осуществления несанкционированного доступа, разрушения, разглашения или модификации информации и/или отказа в обслуживании. **События угроз порождаются источниками угроз.**

- **Источником угроз может быть** намеренное действие, направленное на эксплуатацию уязвимости, или ненамеренное действие, в результате которого уязвимость была проэксплуатирована случайно.
- В целом, **типы источников угроз включают в себя**:
  - враждебные кибератаки или физические атаки;
  - человеческие ошибки;
  - структурные ошибки в активах, подконтрольных организации;
  - природные или техногенные аварии или катастрофы.

NIST SP 800-30

- **Детальность определения событий угроз зависит от глубины построения модели рисков.**
- В случае детального рассмотрения модели рисков можно строить сценарии угроз, которые являются набором из нескольких событий угроз, приводящих к негативным эффектам, атрибутированных к определенному источнику угроз (или нескольким источникам) и упорядоченных по времени; при этом рассматривается потенциальная вероятность последовательной эксплуатации нескольких уязвимостей, приводящей к успешной реализации атаки.
- События угроз в кибер- или физических атаках характеризуются набором тактик, техник и процедур (англ. tactics, techniques, and procedures, TTPs).

NIST SP 800-30

- Рассматриваемый документ также говорит о таком понятии, как **«смещение угрозы»** (англ. threat shifting), под которым понимается изменение атакующими своих TTPs в зависимости от мер защиты, предпринятых компанией и выявленных атакующими. Смещение угрозы может быть осуществлено во временном домене (например, попытки атаковать в другое время или растянуть атаку во времени), в целевом домене (например, выбор менее защищенной цели), ресурсном домене (например, использование атакующими дополнительных ресурсов для взлома цели), домене планирования или метода атаки (например, использование другого хакерского инструментария или попытки атаковать иными методами). Кроме этого, подчеркивается, что атакующие зачастую предпочитают путь наименьшего сопротивления для достижения своих целей, т.е. выбирают самое слабое звено в цепи защиты.

NIST SP 800-30

- **Уязвимость** — это слабость в информационной системе, процедурах обеспечения безопасности, внутренних способах защиты или в особенностях конкретной реализации/внедрения той или иной технологии или системы.

- Уязвимость характеризуется своей опасностью в контексте расчётной важности её исправления; при этом опасность может быть определена в зависимости от ожидаемого негативного эффекта от эксплуатации этой уязвимости.
- Большинство уязвимостей в информационных системах организации возникают или из-за не примененных (случайно или нарочно) мер ИБ, или примененных неверно. Важно также помнить и об эволюции угроз и самих защищаемых систем — и в тех, и в других со временем происходят изменения, которые следует учитывать при проведении переоценки рисков. Кроме уязвимостей технического характера в ИТ-системах, следует учитывать и ошибки в управлении организацией и в архитектуре систем.

NIST SP 800-30

- **Предварительное условие** (англ. predisposing condition) **в контексте оценки рисков** — это условие, существующее в бизнес-процессе, архитектуре или ИТ-системе, влияющее (снижающее или увеличивающее) на вероятность причинения ущерба угрозой. Логическими синонимами будут термины «подверженность» (англ. susceptibility) или «открытость» (англ. exposure) риску, означающие, что уязвимость может быть проэксплуатирована угрозой для нанесения ущерба.

- Например, SQL-сервер потенциально подвержен уязвимости SQL-инъекции. Кроме технических предварительных условий, следует учитывать и организационные: так, местоположение офиса в низине увеличивает риск подтопления, а отсутствие коммуникации между сотрудниками при разработке ИТ-системы увеличивает риск её взлома в дальнейшем.

NIST SP 800-30

- **Вероятность возникновения** (англ. likelihood of occurrence) **угрозы** — фактор риска, рассчитываемый на основе анализа вероятности того, что определенная уязвимость (или группа уязвимостей) может быть проэксплуатирована определенной угрозой, с учетом вероятности того, что угроза в итоге причинит реальный ущерб.
- **Для намеренных угроз оценка вероятности возникновения** обычно оценивается на основании намерений, возможностей и целей злоумышленника.
- **Для ненамеренных угроз оценка вероятности возникновения**, как правило, зависит от эмпирических и исторических данных.
- При этом вероятность возникновения оценивается на определенную временную перспективу — например, на следующий год или на отчетный период. В случае, если угроза практически стопроцентно будет инициирована или реализована в течение определенного временного периода, при оценке рисков следует учесть ожидаемую частоту её реализации. При оценке вероятности возникновения угрозы следует учитывать состояние управления и бизнес-процессов организации, предварительные условия, наличие и эффективность имеющихся мер защиты.

NIST SP 800-30

- Вероятность негативного влияния означает возможность того, что при реализации угрозы будет нанесен какой-либо ущерб, вне зависимости от его величины.
- При определении общей вероятности возникновения событий угроз можно использовать следующие **три этапа**:
  - Оценка вероятности того, что событие угрозы будет кем-либо инициировано (в случае намеренной угрозы) или случится само (в случае ненамеренной).
  - Оценка вероятности того, что возникшая угроза приведет к ущербу или нанесет вред организации, активам, сотрудникам.
  - Общая вероятность рассчитывается как комбинация первых двух полученных оценок.
- Кроме этого подхода, в документе дается рекомендация не искать абсолютно все взаимосвязанные угрозы и уязвимости, а сконцентрироваться на тех из них, которые действительно могут быть использованы в атаках, а также на бизнес-процессах и функциях с недостаточными мерами защиты.

NIST SP 800-30

- **Уровень негативного влияния** (англ. **impact**) **события угрозы** — это величина ущерба, который ожидается от несанкционированного разглашения, доступа, изменения, утери информации или недоступности информационных систем.
- **Организации явным образом определяют:**
  - **Процесс**, используемый для определения негативного влияния.
  - **Предположения**, используемые для определения негативного влияния.
  - **Источники и методы** получения информации о негативном влиянии.
  - **Логическое обоснование**, использованное для определения негативного влияния.
- Кроме этого, при расчете негативного влияния организации должны учитывать ценность активов и информации: можно использовать принятую в компании систему категорирования информации по уровням значимости или **результаты оценок негативного влияния на конфиденциальность** (англ. Privacy Impact Assessments).

NIST SP 800-30

- При оценке рисков важным фактором является **степень неточности** (англ. uncertainty), которая возникает из-за следующих, в общем-то, естественных ограничений, таких как невозможность с точностью спрогнозировать будущие события; недостаточные имеющиеся сведения об угрозах; неизвестные уязвимости; нераспознанные взаимозависимости.

- С учетом вышесказанного, **модель риска** можно описать как следующую логическую структуру:
- **источник угрозы** (с определенными характеристиками) с определенной долей вероятности инициирует **событие угрозы**, которое **эксплуатирует уязвимость** (имеющую определенную долю опасности, с учетом предварительных условий и успешного обхода защитных мер), вследствие чего создается **негативное влияние** (с определенной величиной риска как функции от размера ущерба и вероятности возникновения ущерба), которое порождает риск.

NIST SP 800-30

- Документ дает также рекомендации по использованию процесса **агрегирования рисков** (англ. risk aggregation) в целях объединения нескольких разобщенных или низкоуровневых рисков в один более общий: например, риски отдельных ИТ-систем могут быть агрегированы в общий риск для всей поддерживаемой ими бизнес-системы. При таком объединении следует учитывать то, что некоторые риски могут реализовываться одновременно или чаще, чем это прогнозировалось. Также следует учитывать взаимосвязи между разобщенными рисками и либо объединять их, либо, наоборот, разъединять.

NIST SP 800-30

- В NIST SP 800-30 также описаны **основные способы оценки рисков**: количественный (англ. quantitative), качественный (англ. qualitative) и полуколичественный (англ. semi-quantitative).
- **Количественный анализ** оперирует конкретными цифрами (стоимостью, временем простоя, затратами и т.д.) и лучше всего подходит для проведения анализа выгод и затрат (англ. Cost–benefit analysis), однако является достаточно ресурсоёмким.
- **Качественный анализ** применяет описательные характеристики (например, высокий, средний, низкий), что может привести к некорректным выводам ввиду малого количества возможных оценок и субъективности их выставления.
- **Полуколичественный способ** является промежуточным вариантом, предлагающим использовать больший диапазон возможных оценок (например, по шкале от 1 до 10) для более точной оценки и анализа результатов сравнения.
- Применение конкретного способа оценки рисков зависит как от сферы деятельности организации (например, в банковской сфере может применяться более строгий количественный анализ), так и от стадии жизненного цикла системы (например, на начальных этапах цикла может проводиться только качественная оценка рисков, а на более зрелых — уже количественная).

NIST SP 800-30

- В документе также описаны **три основных способа анализа факторов рисков**: угрозо-центричный (англ. threat-oriented), ориентированный на активы (англ. asset/impact-oriented) или уязвимости (англ. vulnerability-oriented).
- **Угрозо-центричный способ сфокусирован** на создании сценариев угроз и начинается с определения источников угроз и событий угроз; далее, уязвимости идентифицируются в контексте угроз, а негативное влияние связывается с намерениями злоумышленника.
- Способ, **ориентированный на активы**, подразумевает выявление событий угроз и источников угроз, способных оказать негативное влияние на активы; во главу угла ставится потенциальный ущерб активам.
- Применение способа, **ориентированного на уязвимости**, начинается с анализа набора предварительных условий и недостатков/слабостей, которые могут быть проэксплуатированы; далее определяются возможные события угроз и последствия эксплуатации ими найденных уязвимостей. Документ содержит рекомендации по комбинированию описанных способов анализа для получения более объективной картины угроз при оценке рисков.

NIST SP 800-30

- По NIST SP 800-30 **процесс оценки рисков** разбивается на 4 шага:
  - подготовка к оценке рисков;
  - проведение оценки рисков;
  - коммуницирование результатов оценки и передача информации внутри организации;
  - поддержание достигнутых результатов.

NIST SP 800-30

- По NIST SP 800-30 **процесс оценки рисков** разбивается на 4 шага:
- **1. Подготовка к оценке рисков.**
- В рамках подготовки к оценке рисков выполняются следующие задачи:
- 1.1. Идентификация цели оценки рисков: какая информация ожидается в результате оценки, какие решения будут продиктованы результатом оценки.
- 1.2. Идентификация области (англ. scope) оценки рисков в контексте применимости к конкретной организации, временного промежутка, сведений об архитектуре и используемых технологиях
- 1.3. Идентификация специфичных предположений и ограничений, с учетом которых проводится оценка рисков. В рамках этой задачи определяются предположения и ограничения в таких элементах, как источники угроз, события угроз, уязвимости, предварительные условия, вероятность возникновения, негативное влияние, риск-толерантность и уровень неточности, а также выбранный способ анализа.
- 1.4. Идентификация источников предварительной информации, источников угроз и уязвимостей, а также информации о негативном влиянии, которая будет использоваться в оценке рисков. В этом процессе источники информации могут быть как внутренними (такими, как отчеты по инцидентам и аудитам, журналы безопасности и результаты мониторинга), так и внешними (например, отчеты CERTов, результаты исследований и прочая релевантная общедоступная информация).
- 1.5. Идентификация модели рисков, способа оценки рисков и подхода к анализу, которые будут использоваться в оценке рисков.

NIST SP 800-30

- По NIST SP 800-30 **процесс оценки рисков** разбивается на 4 шага:
- **2. Проведение оценки рисков.**
- В рамках оценки рисков выполняются следующие **задачи**:
  - **2.1. Идентификация и характеризация актуальных источников угроз**, включая возможности, намерения и цели намеренных угроз, а также возможные эффекты от ненамеренных угроз.
  - **2.2. Идентификация потенциальных событий угроз**, релевантности этих событий, а также источников угроз, которые могут инициировать события угроз.
  - **2.3. Идентификация уязвимостей и предварительных условий**, которые влияют на вероятность того, что актуальные события угроз приведут к негативному влиянию. Ее целью является определение того, насколько рассматриваемые бизнес-процессы и информационные системы уязвимы перед идентифицированными ранее источниками угроз и насколько идентифицированные события угроз действительно могут быть инициированы этими источниками угроз.
  - **2.4. Определение вероятности** того, что актуальные события угроз приведут к негативному влиянию, с учетом характеристик источников угроз, уязвимостей и предварительных условий, а также подверженности организации этим угрозам, принимая во внимание внедренные меры защиты.
  - **2.5. Определение негативного влияния**, порожденного источниками угроз, с учетом характеристик источников угроз, уязвимостей и предварительных условий, а также подверженности организации этим угрозам, принимая во внимание внедренные меры защиты.
  - **2.6. Определение риска** от реализации актуальных событий угроз, принимая во внимание уровень негативного влияния от этих событий и вероятность наступления этих событий. В Приложении «I» к данному стандарту приведена таблица I-2 для расчета уровня риска в зависимости от уровней вероятности и негативного влияния.

NIST SP 800-30

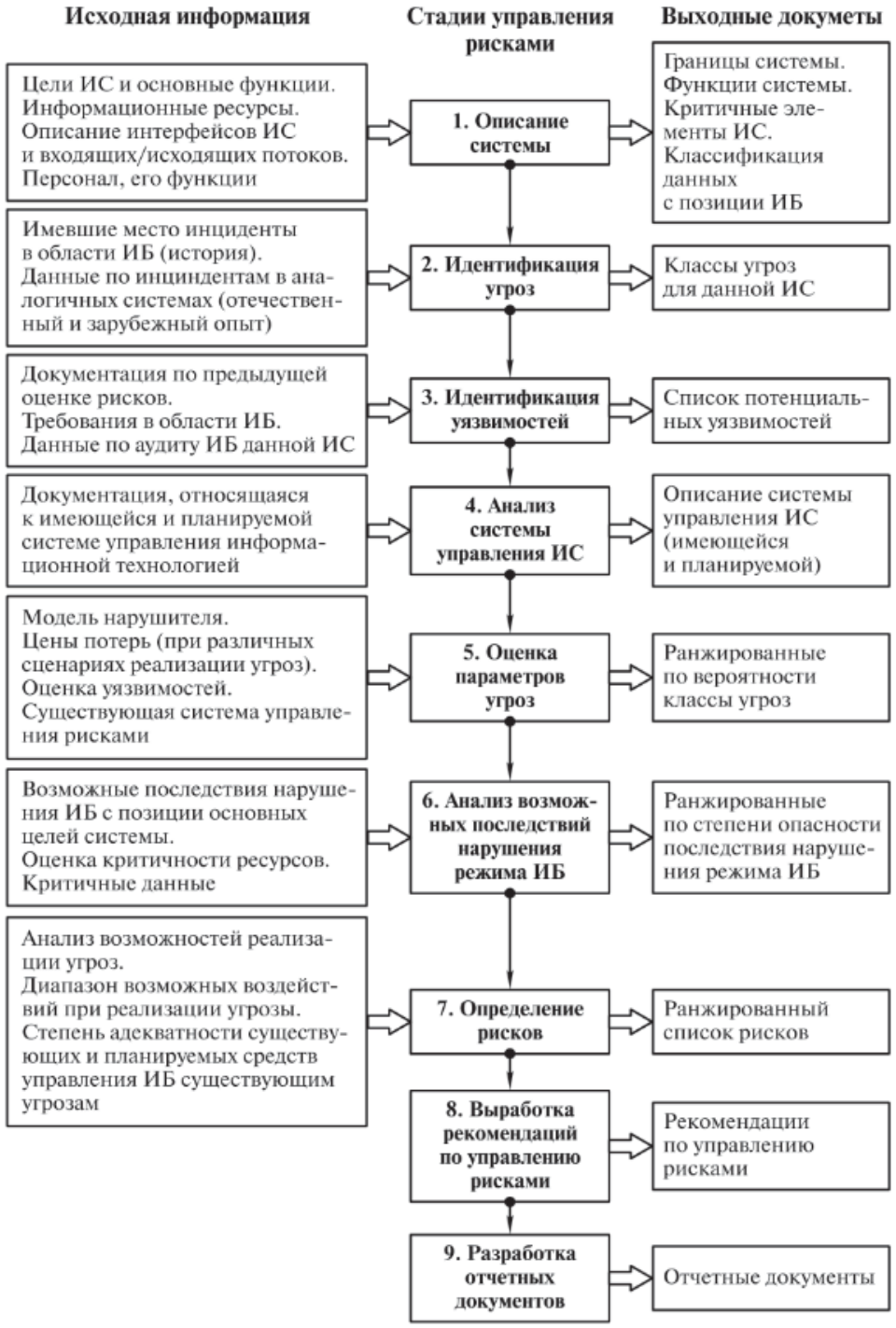
- По NIST SP 800-30 **процесс оценки рисков** разбивается на 4 шага:
- **3. Коммуницирование результатов оценки рисков и передача информации.**
- В рамках коммуницирования результатов оценки рисков и передачи информации выполняются следующие задачи:
  - 3.1. Коммуницирование результатов оценки рисков лицам, принимающим решения, для реагирования на риски.
  - 3.2. Передача заинтересованным лицам информации, касающейся рисков, выявленных в результате оценки.

NIST SP 800-30

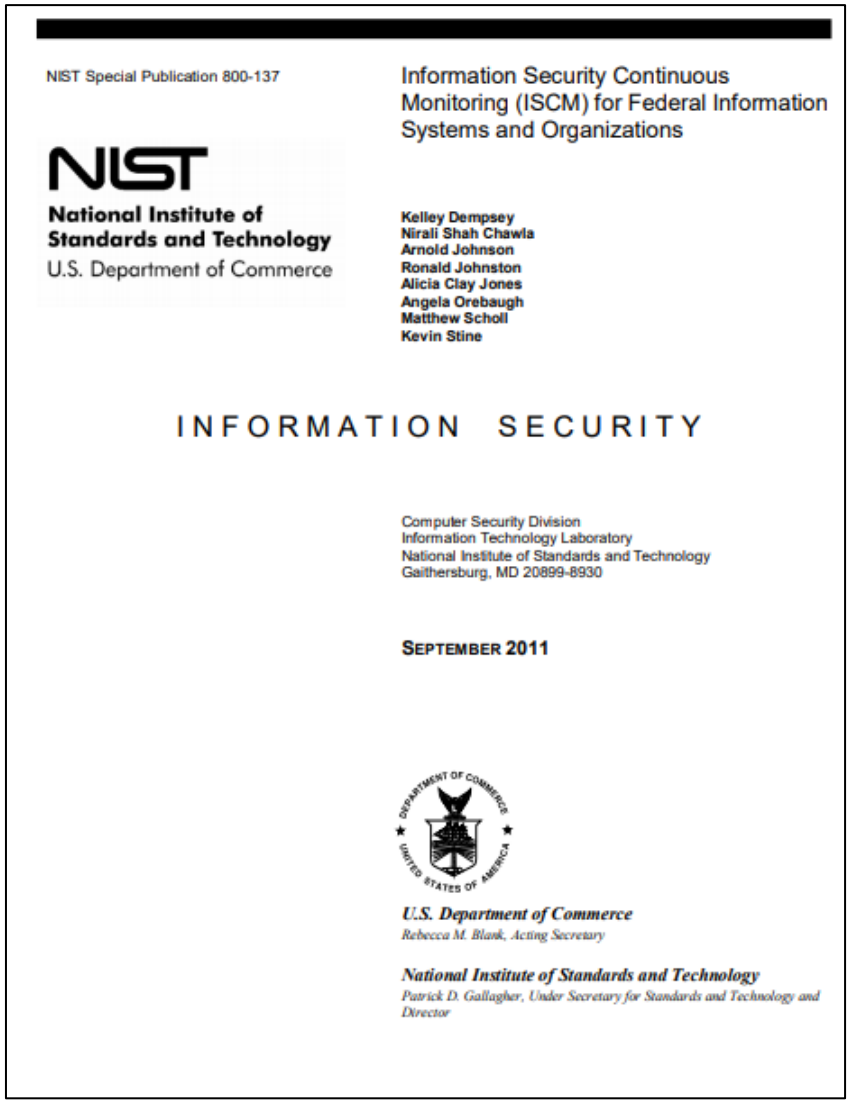
- По NIST SP 800-30 **процесс оценки рисков** разбивается на 4 шага:
- **4. Поддержание достигнутых результатов.**
- В рамках поддержания достигнутых результатов выполняются следующие **задачи**:
  - **4.1. Проведение непрерывного мониторинга факторов риска**, которые влияют на риски в операционной деятельности организации, на её активы, сотрудников, другие организации. Данной задаче посвящен стандарт NIST SP 800-137.
  - **4.2. Актуализация оценки рисков** с использованием результатов процесса непрерывного мониторинга факторов риска.
- Как видим, документ NIST SP 800-30 предлагает достаточно детальный подход к моделированию угроз и расчету рисков. Ценными являются также приложения к данному стандарту, содержащие примеры расчетов по каждой из подзадач оценки рисков, а также перечни возможных источников угроз, событий угроз, уязвимостей и предварительных условий.

NIST SP 800-30

Процесс управления рисками NIST SP 800-30



NIST SP 800-137 Information Security Continuous Monitoring for Federal information Systems and Organizations



NIST Special Publication 800-137

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

SEPTEMBER 2011

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

- **NIST SP 800-137** «Information Security Continuous Monitoring for Federal information Systems and Organizations» (**Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций**).
- https://csrc.nist.gov/publications/detail/sp/800-137/final
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

NIST SP 800-137

- **Задачей** построения стратегии непрерывного мониторинга информационной безопасности является оценка эффективности мер защиты и статуса безопасности систем с целью реагирования на постоянно меняющиеся вызовы и задачи в сфере информационной безопасности.
- Система непрерывного мониторинга ИБ помогает предоставлять ситуационную осведомленность о состоянии безопасности информационных систем компании на основании информации, собранной из различных ресурсов (таких как активы, процессы, технологии, сотрудники), а также об имеющихся возможностях по реагированию на изменения ситуации. Данная система является одной из тактик в общей стратегии управления рисками.

NIST SP 800-137

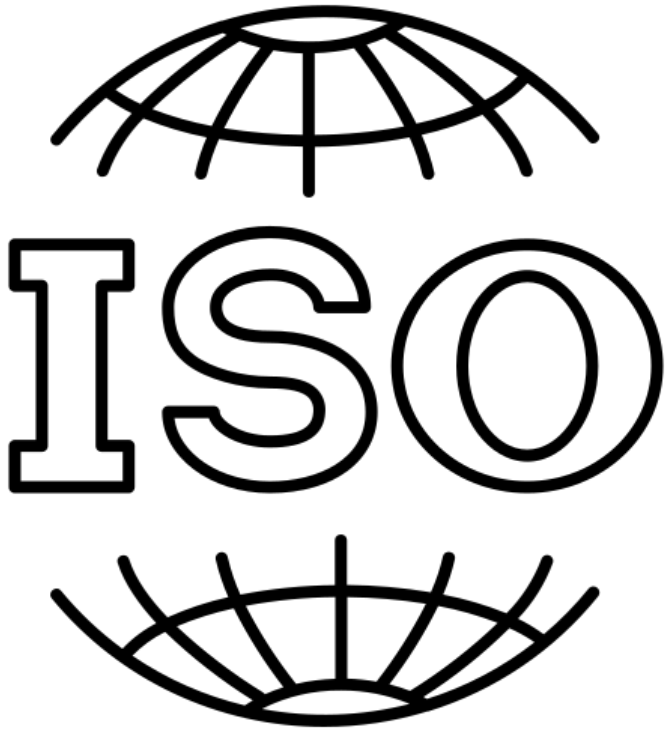
- Как и прочие документы серии SP, в данном документе приведен рекомендуемый **процессный подход к выстраиванию системы мониторинга ИБ**, состоящий из:
  - **определения стратегии непрерывного мониторинга ИБ** (включает в себя выстраивание стратегии на уровне организации, бизнес-процессов и информационных систем; назначение ролей и ответственных; выбор тестового набора систем для сбора данных);
  - **разработки программы непрерывного мониторинга ИБ** (включает в себя определение метрик для оценки и контроля; выбор частоты проведения мониторинга и оценки; разработку архитектуры системы мониторинга);
  - **внедрения программы непрерывного мониторинга ИБ**;
  - **анализа найденных недочетов и отчета о них** (включает в себя анализ данных; отчетность по оценке мер защиты; отчетность по мониторингу статуса защиты);
  - **реагирования на выявленные недочеты**;
  - **пересмотра и обновления стратегии и программы непрерывного мониторинга ИБ**.

NIST SP 800-137

- В документе также даются следующие рекомендации по **выбору инструментов обеспечения непрерывного мониторинга ИБ**:
  - поддержка ими большого количества источников данных;
  - использование открытых и общедоступных спецификаций (например, SCAP — Security Content Automation Protocol);
  - интеграция с другим ПО, таким как системы Help Desk, системы управления инвентаризацией и конфигурациями, системами реагирования на инциденты;
  - поддержка процесса анализа соответствия применимым законодательным нормам;
  - гибкий процесс создания отчетов, возможность «проваливаться» (англ. drill-down) в глубину рассматриваемых данных;
  - поддержка систем Security Information and Event Management (SIEM) и систем визуализации данных.

NIST SP 800-39, NIST SP 800-37 и NIST SP 800-30

- **NIST SP 800-39, NIST SP 800-37 и NIST SP 800-30 предлагают логически связанный системный подход к оценке и обработке рисков, а NIST SP 800-53, NIST SP 800-53A и NIST SP 800-137 предлагают конкретные меры по минимизации рисков ИБ.**
- Однако следует иметь ввиду, что данные документы по своей сути носят лишь рекомендательный характер и не являются стандартами (например, в отличие от документов NIST FIPS), а также то, что изначально они разрабатывались для компаний и организаций из США. Это накладывает определенные ограничения на их использование: так, организации не могут получить международную сертификацию по выполнению положений данных документов, а применение всего набора связанных фреймворков NIST может оказаться чрезмерно трудозатратным и нецелесообразным.
- Зачастую компании выбирают путь сертификации по требованиям Международной Организации по Стандартизации (англ. International Organization for Standardization, ISO), получая, например, статус ”ISO 27001 Certified”, признаваемый во всем мире. В серию стандартов ISO 27000 входят документы, посвященные информационной безопасности и управлению рисками. Рассмотрим основной документ данной серии по управлению рисками ИБ: стандарт ISO/IEC 27005:2018.



7. Стандарты Международной организации по стандартизации ISO (International Organization for Standardization)

Стандарты ISO

- **Серия стандартов ISO/IEC 27000** представляет собой семейство стандартов, описывающих лучшие практики и требования для систем менеджмента информационной безопасности (ISMS), направленные на обеспечение конфиденциальности, целостности и доступности информации.

- **Серия стандартов ISO/IEC 31000** представляет собой руководящие принципы и рекомендации для управления рисками, предоставляющие систематический подход к идентификации, анализу и реагированию на риски в различных сферах организационной деятельности.

Серия стандартов ISO/IEC 27000

- **ISO/IEC 27002:2022**«Information security, cybersecurity and privacy protection — Information security controls» (рус. **Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью**)

- **ISO/IEC 27005:2018** «Information technology — Security techniques — Information security risk management» («**Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности**»)

- **ISO/IEC 27102:2019** «Information security management — Guidelines for cyber-insurance» («**Управление информационной безопасностью. Руководство по киберстрахованию**»)

Серия стандартов ISO/IEC 31000

- **ISO 31000:2018** «Risk management — Guidelines» (**Менеджмент риска. Принципы и руководство**) стандарт описывает общие рекомендации, применимые к любым организациям и любым типам рисков. Он не предназначен для целей сертификации, а скорее предоставляет руководство для внутреннего или внешнего аудита риск-менеджмента.

- **ISO/IEC 31010:2019** «Risk management — Risk assessment techniques» («**Менеджмент риска - Методы оценки риска**») стандарт предназначен для поддержки процесса управления рисками, описанного в ISO 31000, и помогает организациям понимать сложность рисков, с которыми они сталкиваются, и способы их измерения и оценки.

ISO/IEC 27002
до 2007 ISO/IEC 17799 **до 2000** - BS 7799-1:1999

- **ISO/IEC 17799** — стандарт информационной безопасности, опубликованный в 2005 году организациями ISO и IEC. Он озаглавлен **Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности** (англ. Information technology - Security techniques - Code of practice for information security management).
- **Стандарт является переработкой версии, опубликованной в 2000 году, которая являлась полной копией Британского стандарта BS 7799-1:1999.**
- **Стандарт ISO/IEC 17799 был пересмотрен в июне 2005 года, а в июле 2007 года его номер был изменен на ISO/IEC 27002, когда он был включен в растущее семейство стандартов ISO/IEC 27000.**

Стандарт ISO/IEC 27005:2018

- Стандарт ISO/IEC 27005:2018 «Information technology — Security techniques — Information security risk management» («**Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности**») входит в серию стандартов ISO 27000 и является логически взаимосвязанным с другими стандартами по ИБ из этой серии. Данный стандарт отличается фокусом на ИБ при рассмотрении процессов управления рисками.

ISO/IEC 27005:2018

- **Стандарт ISO/IEC 27005:2018 «Information technology — Security techniques — Information security risk management»** («Информационные технологии – Техники обеспечения безопасности – Управление рисками информационной безопасности») является уже третьей ревизией: первая версия стандарта была опубликована в 2005 году, а вторая — в 2011.
- **Документ вводит несколько риск-специфичных терминов.**
- Так, **средством защиты** (англ. control) называется мера, изменяющая риск.
- В понятие **контекстов** (англ. context) входят внешний контекст, означающий внешнюю среду функционирования компании (например, политическую, экономическую, культурную среду, а также взаимоотношения с внешними стейкхолдерами), и внутренний контекст, означающий внутреннюю среду функционирования компании (внутренние процессы, политики, стандарты, системы, цели и культуру организации, взаимоотношения с внутренними стейкхолдерами, а также договорные обязательства).

ISO/IEC 27005:2018

- **Риск — это результат неточности (англ. uncertainty) при достижении целей;** при этом неточность означает состояние недостатка информации, относящейся к некому событию, его последствиям или вероятности его наступления.

- Под **уровнем риска** (англ. level of risk) понимается величина риска, выраженная в произведении последствий значимых событий и вероятности возникновения этих событий.
- **Остаточный риск** (англ. residual risk) — риск, оставшийся после проведения процедуры обработки рисков.
- Под **оценкой риска** (англ. risk assessment) понимают общий процесс идентификации (т.е. поиска, определения и описания риска), анализа (т.е. понимания природы риска и определения его уровня) и оценки опасности (т.е. сравнения результатов анализа риска с риск-критериями для определения допустимости его величины) рисков.

ISO/IEC 27005:2018

- **Обработка рисков** — это процесс модификации рисков, который может включать в себя:
  - **избегание** риска путем отказа от действий, которые могут привести к рискам;
  - **принятие** или увеличение риска в целях достижения бизнес-целей;
  - **устранение** источников риска;
  - **изменение** вероятности реализации риска;
  - **изменение** ожидаемых последствий от реализации риска;
  - **перенос** (разделение) риска;
  - **сохранение** риска.

ISO/IEC 27005:2018

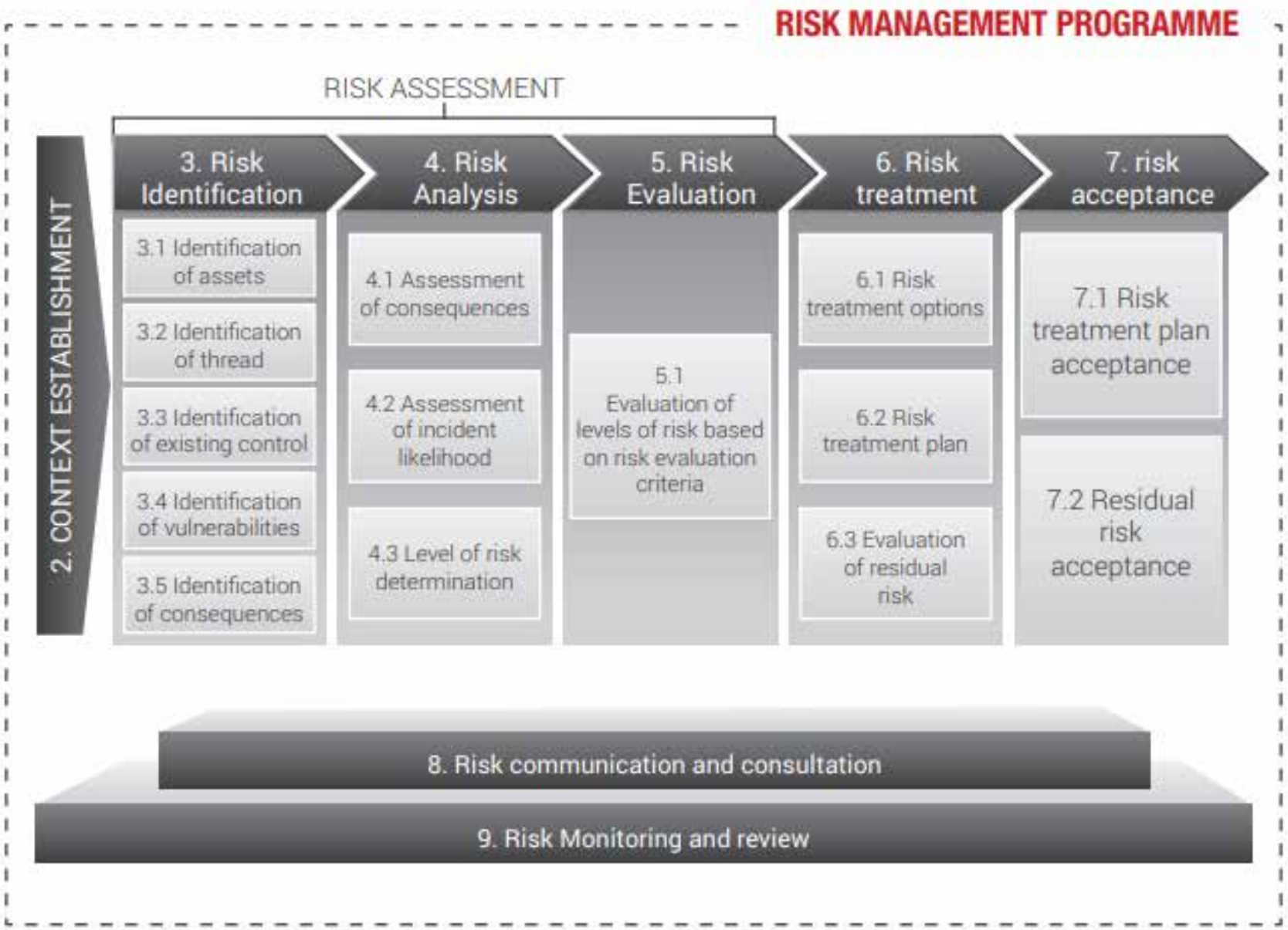
- **Процесс управления рисками** ИБ с точки зрения авторов стандарта ISO/IEC 27005:2018 **должен характеризоваться следующими особенностями**:
  1. Оценка рисков ведется с учетом последствий рисков для бизнеса и вероятности возникновения рисков. Осуществляются идентификация рисков, их анализ и сравнение (с учетом выбранного уровня риск-толерантности).
  2. Вероятность и последствия рисков доводятся до заинтересованных сторон и принимаются ими.
  3. Устанавливается приоритет обработки рисков и конкретных действий по снижению рисков.
  4. В процесс принятия решений по управлению рисками вовлекаются стейкхолдеры, которые затем также информируются о статусе управления рисками.
  5. Оценивается эффективность проведенной обработки рисков.
  6. Контролируются и регулярно пересматриваются риски и сам процесс управления ими.
  7. На основе получаемой новой информации процесс управления рисками непрерывно улучшается.
  8. Проводится обучение сотрудников и руководителей относительно рисков и предпринимаемых действий для их снижения.

ISO/IEC 27005:2018

- Сам **процесс управления рисками состоит из следующих шагов** (процессов), которые соответствуют принятому в стандарте ISO 27001 подходу **PDCA (Plan — Do — Check — Act):**
  1. Определение контекста.
  2. Оценка рисков.
  3. Разработка плана обработки рисков.
  4. Принятие рисков.
  5. Внедрение разработанного плана обработки рисков.
  6. Непрерывный мониторинг и пересмотр рисков.
  7. Поддержка и улучшение процесса управления рисками ИБ.

- Рассмотрим далее каждый из этих шагов подробнее.

ISO/IEC 27005



ISO/IEC 27005:2018

- **1. Определение контекста**
- **Входными данными** при определении контекста являются все релевантные риск-менеджменту сведения о компании. В рамках данного процесса выбирается подход к управлению рисками, который должен включать в себя критерии оценки рисков, критерии оценки негативного влияния (англ. impact), критерии принятия рисков. Кроме этого, следует оценить и выделить необходимые для осуществления данного процесса ресурсы.

- **Критерии оценки рисков должны** быть выработаны для оценки рисков ИБ в компании и должны учитывать стоимость информационных активов, требования к их конфиденциальности, целостности, доступности, роль информационных бизнес-процессов, требования законодательства и договорных обязательств, ожидания стейкхолдеров, возможные негативные последствия для гудвилла и репутации компании.

ISO/IEC 27005:2018

- **1. Определение контекста**
- **Критерии оценки негативного влияния** должны учитывать уровень ущерба или затрат компании на восстановление после реализованного риска ИБ с учетом уровня значимости ИТ актива, нарушения информационной безопасности (т.е. потери активом свойств конфиденциальности, целостности, доступности), вынужденный простой бизнес-процессов, экономические потери, нарушение планов и дедлайнов, ущерб репутации, нарушение требований законодательства и договорных обязательств.
- **Критерии принятия рисков** можно выразить как отношение ожидаемой бизнес-выгоды к ожидаемому риску. При этом для разных классов рисков можно применять различные критерии: например, риски несоответствия законодательству могут не быть приняты в принципе, а высокие финансовые риски могут быть приняты, если они являются частью договорных обязательств. Кроме этого, следует учитывать и прогнозируемый временной период актуальности риска (долгосрочные и краткосрочные риски). Критерии принятия рисков необходимо разрабатывать, учитывая желаемый (целевой) уровень риска с возможностью принятия топ-менеджментом рисков выше этого уровня в определенных обстоятельствах, а также возможность принятия рисков при условии последующей обработки рисков в течение оговоренного временного периода.

ISO/IEC 27005:2018

- **1. Определение контекста**
- Кроме вышеперечисленных критериев, в рамках процесса определения контекста следует учесть **границы и объем** (англ. scope) процесса управления рисками ИБ:
  - нужно принять во внимание бизнес-цели,
  - бизнес-процессы,
  - планы и политики компании,
  - структуру и функции организации,
  - применимые законодательные и иные требования,
  - информационные активы,
  - ожидания стейкхолдеров, взаимодействие с контрагентами.
- Рассматривать процесс управления рисками можно в рамках конкретной ИТ-системы, инфраструктуры, бизнес-процесса или в рамках определенной части всей компании.

ISO/IEC 27005:2018

- **2. Оценка рисков**

- **В рамках проведения процесса оценки рисков** компания должна оценить стоимость информационных активов, идентифицировать актуальные угрозы и уязвимости, получить информацию о текущих средствах защиты и их эффективности, определить потенциальные последствия реализации рисков. В результате оценки рисков компания должна получить количественную или качественную оценку рисков, а также приоритизацию этих рисков с учетом критериев оценки опасности рисков и целей компании.
- Сам **процесс оценки рисков состоит** из действий по **идентификации** (англ. identification) рисков, **анализа** (англ. analysis) рисков, **оценки** опасности (англ. evaluation) рисков.

ISO/IEC 27005:2018

- **2. Оценка рисков**
- **2.1. Идентификация рисков**
- **Целью идентификации рисков** является определение того, что может случиться и привести к потенциальному ущербу, а также получить понимание того, как, где и почему этот ущерб может произойти. При этом следует учитывать риски вне зависимости от того, находится ли источник этих рисков под контролем организации или нет. **В рамках данного процесса следует провести:**
  - **идентификацию (инвентаризацию) активов**, получив в итоге список ИТ-активов и бизнес-процессов;
  - **идентификацию угроз**, при этом следует учитывать преднамеренные и случайные угрозы, внешние и внутренние источники угроз, а информацию о возможных угрозах можно получать как у внутренних источников в организации (юристы, HR, IT и т.д.), так и у внешних (страховые компании, внешние консультанты, статистическая информация и т.д.);
  - **идентификацию имеющихся и запланированных к внедрению мер защиты** для исключения их дублирования;
  - **идентификацию уязвимостей**, которые могут быть проэксплуатированы актуальными угрозами и нанести ущерб активам; при этом следует учитывать уязвимости не только в программном или аппаратном обеспечении, но и в структуре организации, её бизнес-процессах, персонале, физической инфраструктуре, отношениях с контрагентами;
  - **идентификацию последствий реализации угроз** нарушения конфиденциальности, целостности, доступности ИТ-активов.

ISO/IEC 27005:2018

- **2. Оценка рисков**
- **2.2. Анализ рисков**
- Анализ рисков может быть проведен с различной глубиной, в зависимости от критичности активов, количества известных уязвимостей, а также с учетом ранее произошедших инцидентов. Методология анализа рисков может быть как качественной, так и количественной: как правило, вначале применяют качественный анализ для выделения высокоприоритетных рисков, а затем уже для выявленных рисков применяют количественный анализ, который является более трудоемким и дает более точные результаты.
- При использовании качественного анализа специалисты оперируют шкалой описательной оценки опасности (например, низкая, средняя, высокая) потенциальных последствий неких событий и вероятности наступления этих последствий.
- При использовании методов количественного анализа уже применяются численные величины, с учетом исторических данных об уже произошедших инцидентах. Следует при этом иметь ввиду, что в случае отсутствия надежных, проверяемых фактов количественная оценка рисков может дать лишь иллюзию точности.

ISO/IEC 27005:2018

- **2. Оценка рисков**
- **2.2. Анализ рисков**
- При непосредственно самом процессе анализа рисков сначала проводится оценка потенциальных последствий инцидентов ИБ: оценивается уровень их негативного влияния на компанию с учетом последствий от нарушений свойств конфиденциальности, целостности, доступности информационных активов. Проводятся проверка и аудит имеющихся активов с целью их классификации в зависимости от критичности, также оценивается (желательно в денежных величинах) потенциальное негативное влияние нарушения свойств ИБ этих активов на бизнес. Оценка стоимости активов проводится в рамках анализа негативного влияния на бизнес (англ. Business Impact Analysis) и может быть рассчитана исходя из стоимости замены или восстановления активов/информации, а также последствий утери или компрометации активов/информации: рассматриваются финансовые, юридические, репутационные аспекты. Следует также учитывать, что угрозы могут затронуть один или несколько взаимосвязанных активов либо затронуть активы лишь частично.

ISO/IEC 27005:2018

- **2. Оценка рисков**
- **2.2. Анализ рисков**
- Далее проводится оценка вероятности возникновения инцидента, т.е. всех потенциальных сценариев реализации угроз. Следует учесть частоту реализации угрозы и легкость эксплуатации уязвимостей, руководствуясь статистической информацией об аналогичных угрозах, а также данными о мотивации и возможностях преднамеренных источников угроз (построение модели нарушителя), привлекательности активов для атакующих, имеющихся уязвимостях, примененных мерах защиты, а в случае рассмотрения непреднамеренных угроз — учитывать местоположение, погодные условия, особенности оборудования, человеческие ошибки и т.д. В зависимости от требуемой точности оценки активы можно группировать или разделять с точки зрения применимых к ним сценариев атак.
- Наконец, проводится определение уровня рисков для всех сценариев из разработанного списка сценариев атак. Величина ожидаемого риска является произведением вероятности сценария инцидента и его последствий.

ISO/IEC 27005:2018

- **2. Оценка рисков**
- **2.3. Оценка опасности рисков**
- В рамках процесса оценки опасности рисков проводится сравнение полученных на предыдущем этапе уровней рисков с критериями сравнения рисков и критериями принятия рисков, полученными на этапе определения контекста. При принятии решений следует учитывать последствия реализации угроз, вероятность возникновения негативных последствий, уровень собственной уверенности в корректности проведенной идентификации и анализа рисков. Следует учесть свойства ИБ активов (например, если потеря конфиденциальности нерелевантна для организации, то все риски, нарушающие данное свойство, можно отбросить), а также важность бизнес-процессов, обслуживаемых определенным активом (например, риски, затрагивающие малозначимый бизнес-процесс, могут быть признаны низкоприоритетными).

ISO/IEC 27005:2018

- **3. Обработка рисков ИБ**
- К началу осуществления данного подпроцесса у нас уже имеется список приоритизированных рисков в соответствии с критериями оценки опасности рисков, связанных со сценариями инцидентов, которые могут привести к реализации этих рисков. В результате прохождения этапа обработки рисков мы должны выбрать меры защиты, предназначенные для модификации (англ. modification), сохранения (англ. retention), избегания (англ. avoidance) или передачи (англ. sharing) рисков, а также обработать остаточные риски и сформировать план обработки рисков.
- Указанные опции обработки рисков (модификацию, сохранение, избегание или передачу) следует выбирать в зависимости от результатов процесса оценки рисков, ожидаемой оценки стоимости внедрения мер защиты и ожидаемых преимуществ каждой опции, при этом их можно комбинировать (например, модифицировать вероятность риска и передавать остаточный риск). Предпочтение следует отдавать легкореализуемым и низкобюджетным мерам, которые при этом дают большой эффект снижения рисков и закрывают большее количество угроз, а в случае необходимости применения дорогостоящих решений следует давать экономическое обоснование их применению. В целом, следует стремиться максимально снизить негативные последствия, а также учитывать редкие, но разрушительные риски.

ISO/IEC 27005:2018

- **3. Обработка рисков ИБ**
- В итоге ответственными лицами должен быть сформирован план обработки рисков, который чётко определяет приоритет и временной интервал, в соответствии с которыми следует реализовать способ обработки каждого риска. Приоритеты могут быть расставлены по результатам ранжирования рисков и анализа затрат и выгод (англ. cost-benefit analysis). В случае, если в организации уже были внедрены какие-либо меры защиты, будет разумно проанализировать их актуальность и стоимость владения, при этом следует учитывать взаимосвязи между мерами защиты и угрозами, для защиты от которых данные меры применялись.

- В окончании составления плана обработки рисков следует определить остаточные риски. Для этого могут потребоваться обновление или повторное проведение оценки рисков с учетом ожидаемых эффектов от предлагаемых способов обработки рисков.

- Далее рассмотрим подробнее возможные опции обработки рисков.

ISO/IEC 27005:2018

- **3. Обработка рисков ИБ**
- **3.1. Модификация рисков**
- Модификация рисков подразумевает такое управление рисками путём применения или изменения мер защиты, которое приводит к оценке остаточного риска как приемлемого. При использовании опции модификации рисков выбираются оправданные и релевантные меры защиты, которые соответствуют требованиям, определенным на этапах оценки и обработки рисков. Следует учитывать разнообразные ограничения, такие как стоимость владения средствами защиты (с учетом внедрения, администрирования и влияния на инфраструктуру), временные и финансовые рамки, потребность в обслуживающем эти средства защиты персонале, требования по интеграции с текущими и новыми мерами защиты. Также нужно сравнивать стоимость указанных затрат со стоимостью защищаемого актива.К мерам защиты можно отнести: коррекцию, устранение, предотвращение, минимизацию негативного влияния, предупреждение потенциальных нарушителей, детектирование, восстановление, мониторинг и обеспечение осведомленности сотрудников.
- Результатом шага «Модификация рисков» должен стать список возможных мер защиты с их стоимостью, предлагаемыми преимуществами и приоритетом внедрения.

ISO/IEC 27005:2018

- **3. Обработка рисков ИБ**
- **3.2. Сохранение риска**
- Сохранение риска означает, что по результатам оценки опасности риска принято решение, что дальнейшие действия по его обработке не требуются, т.е. оценочный уровень ожидаемого риска соответствует критерию принятия риска. Отметим, что эта опция существенно отличается от порочной практики игнорирования риска, при которой уже идентифицированный и оцененный риск никак не обрабатывается, т.е. решение о его принятии официально не принимается, оставляя риск в «подвешенном» состоянии.

ISO/IEC 27005:2018

- **3. Обработка рисков ИБ**
- **3.3. Избегание риска**
- При выборе данной опции принимается решение не вести определенную деятельность или изменить условия её ведения так, чтобы избежать риска, ассоциированного с данной деятельностью. Это решение может быть принято в случае высоких рисков или превышения стоимости внедрения мер защиты над ожидаемыми преимуществами. Например, компания может отказаться от предоставления пользователям определенных онлайн-услуг, касающихся персональных данных, исходя из результатов анализа возможных рисков утечки такой информации и стоимости внедрения адекватных мер защиты.

ISO/IEC 27005:2018

- **3. Обработка рисков ИБ**
- **3.4. Передача риска**
- Риск можно передать той организации, которая сможет управлять им наиболее эффективно. Таким образом, на основании оценки рисков принимается решение о передаче определенных рисков другому лицу, например, путем страхования киберрисков (услуга, набирающая популярность в России, однако до сих пор в разы отстающая от объема этого рынка, например, в США) или путем передачи обязанности по мониторингу и реагированию на инциденты ИБ провайдеру услуг MSSP (Managed Security Service Provider) или MDR (Managed Detection and Response), т.е. в коммерческий SOC. При выборе опции передачи риска следует учесть, что и сама передача риска может являться риском, а также то, что можно переложить на другую компанию ответственность за управление риском, но нельзя переложить на нее ответственность за негативные последствия возможного инцидента.

ISO/IEC 27005:2018

- **4. Принятие риска**

- Входными данными этого этапа будут разработанные на предыдущем шаге планы обработки рисков и оценка остаточных рисков. Планы обработки рисков должны описывать то, как оцененные риски будут обработаны для достижения критериев принятия рисков. Ответственные лица анализируют и согласовывают предложенные планы обработки рисков и финальные остаточные риски, а также указывают все условия, при которых данное согласование выносится. В упрощенной модели проводится банальное сравнение величины остаточного риска с ранее определенным приемлемым уровнем. Однако следует учитывать, что в некоторых случаях может потребоваться пересмотр критериев принятия рисков, которые не учитывают новые обстоятельства или условия. В таком случае ответственные лица могут быть вынуждены принять такие риски, указав обоснование и комментарий к решению о невыполнении критериев принятия рисков в конкретном случае.

- В итоге, формируется список принимаемых рисков с обоснованием к тем, которые не соответствуют ранее определенным критериям принятия рисков.

ISO/IEC 27005:2018

- **5. Внедрение разработанного плана обработки рисков. Коммуницирование рисков ИБ**

- На данном этапе осуществляется непосредственное претворение в жизнь разработанного плана обработки рисков: в соответствии с принятыми решениями закупаются и настраиваются средства защиты и оборудование, заключаются договоры кибер-страхования и реагирования на инциденты, ведется юридическая работа с контрагентами. Параллельно до руководства и стейкхолдеров доводится информация о выявленных рисках ИБ и принимаемых мерах по их обработке в целях достижения всеобщего понимания проводимой деятельности.
- Разрабатываются планы коммуникации рисков ИБ для ведения скоординированной деятельности в обычных и экстренных ситуациях (например, на случай крупного инцидента ИБ).

ISO/IEC 27005:2018

- **6. Непрерывный мониторинг и пересмотр рисков**

- Следует учитывать, что риски могут незаметно меняться со временем: изменяются активы и их ценность, появляются новые угрозы и уязвимости, изменяются вероятность реализации угроз и уровень их негативного влияния. Следовательно, необходимо вести непрерывный мониторинг происходящих изменений, в том числе с привлечением внешних контрагентов, специализирующихся на анализе актуальных угроз ИБ. Требуется проводить регулярный пересмотр как рисков ИБ, так и применяемых способов их обработки на предмет актуальности и адекватности потенциально изменившейся ситуации. Особое внимание следует уделять данному процессу в моменты существенных изменений в работе компании и осуществляющихся бизнес-процессов (например, при слияниях/поглощениях, запусках новых сервисов, изменении структуры владения компанией и т.д.).

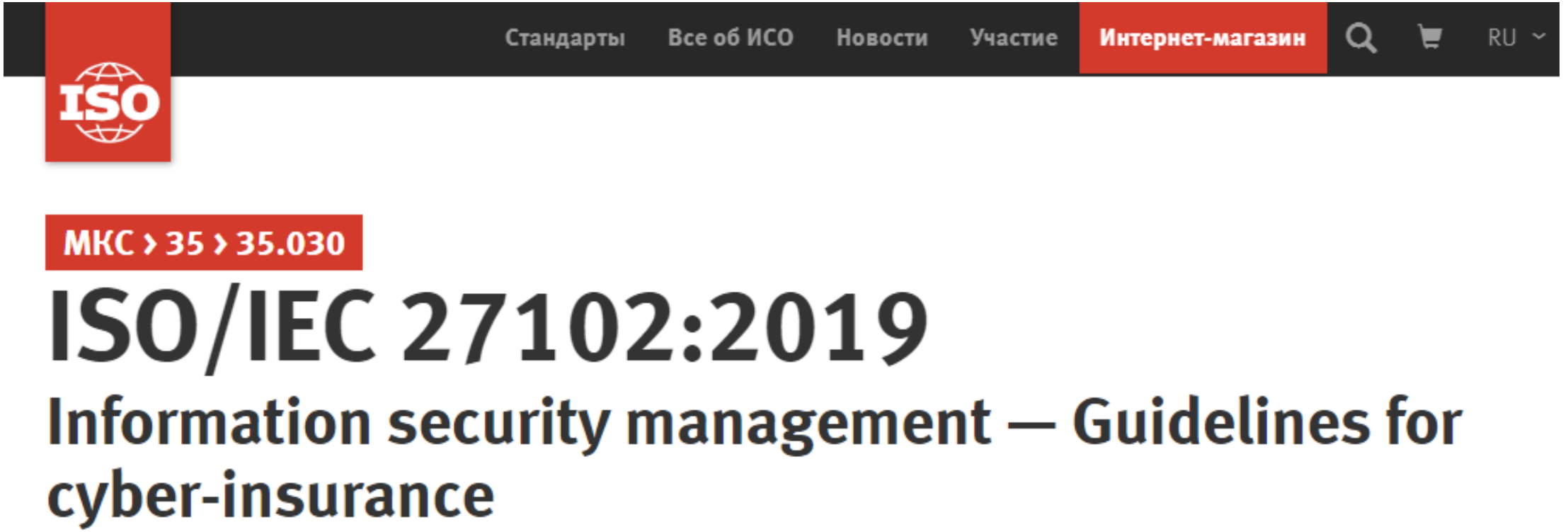
ISO/IEC 27005:2018

- **7. Поддержка и улучшение процесса управления рисками ИБ**

- Аналогично непрерывному мониторингу рисков следует постоянно поддерживать и улучшать сам процесс управления рисками для того, чтобы контекст, оценка и план обработки рисков оставались релевантными текущей ситуации и обстоятельствам. Все изменения и улучшения требуется согласовывать с заинтересованными сторонами. Критерии оценки и принятия рисков, оценка стоимости активов, имеющиеся ресурсы, активность конкурентов и изменения в законодательстве и контрактных обязательствах должны соответствовать актуальным бизнес-процессам и текущим целям компании. В случае необходимости нужно менять или совершенствовать текущий подход, методологию и инструменты управления рисками ИБ.

ISO/IEC 27005

Стандарт ISO/IEC 27102:2019



- Стандарт ISO/IEC 27102:2019 «Information security management — Guidelines for cyber-insurance» («**Управление информационной безопасностью. Руководство по киберстрахованию**») предлагает подходы к оценке необходимости приобретения киберстраховки как меры обработки рисков, а также к оценке и взаимодействию со страховщиком.

ISO/IEC 27102:2019

- Стандарт **ISO/IEC 27102:2019**, официально называемый "Information security management guidelines for cyber insurance", представляет собой руководство по управлению информационной безопасностью в контексте киберстрахования.
- Этот стандарт не сосредоточен непосредственно на технических аспектах оценки и управления рисками информационной безопасности, а скорее **выступает в качестве моста между мирами информационной безопасности и страхования.**

- **ISO/IEC 27102:2019 предоставляет рекомендации по:**
  - Пониманию концепции и принципов киберстрахования.
  - **Идентификации потенциальных рисков, которые можно передать страховщику.**
  - Разработке стратегии управления киберрисками, которая включает в себя страхование.
  - Пониманию взаимосвязи между мерами по управлению информационной безопасностью и киберстраховыми полисами.
  - Рассмотрению страхования как части комплексного подхода к управлению информационной безопасностью.

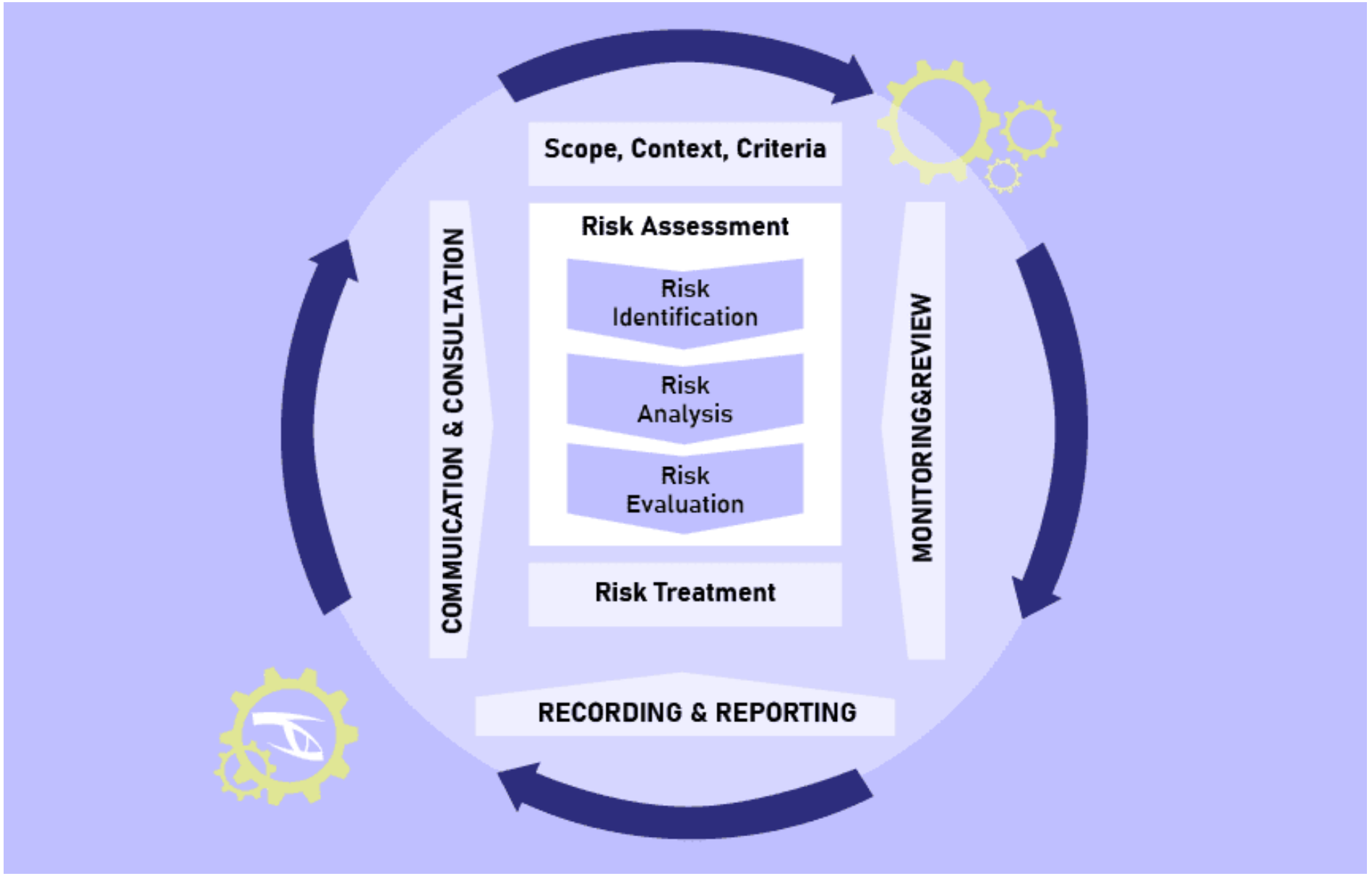
Серия стандартов ISO/IEC 31000:2018

- **Серия стандартов ISO/IEC 31000:2018** описывает подход к риск-менеджменту без привязки к ИТ/ИБ. В этой серии стоит отметить стандарт ISO/IEC 31010:2019 «Risk management — Risk assessment techniques» — на данный стандарт в его варианте ГОСТ Р ИСО/МЭК 31010-2011 «**Менеджмент риска. Методы оценки риска**» ссылается 607-П ЦБ РФ «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков».
- **Стандарт ISO/IEC 31000:2018 - соответствует ГОСТ Р ИСО 31000-2019 в РФ и СТБ ISO 31000-2020 в Р**

ISO 31000:2018

- **Данный стандарт входит в серию стандартов по управлению бизнес-рисками без привязки конкретно к рискам ИБ**.
- «Заглавным» стандартом является документ ISO 31000:2018 ”Risk management – Guidelines” («**Менеджмент риска — Руководства**»), который описывает фреймворк, принципы и сам процесс управления рисками.
- Описанный в данном документе процесс риск-менеджмента аналогичен ISO/IEC 27005:2018: определяются контекст, границы и критерии, проводится оценка рисков (состоящая из идентификации, анализа, оценки опасности рисков), далее идет обработка рисков с последующей коммуникацией, отчетностью, мониторингом и пересмотром.

ISO 31000:2018



Серия стандартов ISO 31000

- **В серию стандартов ISO 31XXX** на текущий момент входят следующие документы:
  - **ISO 31000:2018** ”Risk management – Guidelines” («**Менеджмент риска - Рекомендации**»), который в отечественной версии имеет название ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство».
  - **ISO/TR 31004:2013** "Risk management - Guidance for the implementation of ISO 31000" («**Менеджмент риска - Руководство по внедрению стандарта ISO 31000**»).
  - **IEC 31010:2019** ”Risk management - Risk assessment techniques” («**Менеджмент риска - Методы оценки риска**»). Данному стандарту соответствует отечественный **ГОСТ Р 58771-2019** «Менеджмент риска. Технологии оценки риска», пришедший на смену стандарту ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска».
  - **ISO 31022:2020** "Risk management - Guidelines for the management of legal risk" («**Менеджмент риска - Рекомендации по управлению юридическими рисками**»).
  - **IWA 31:2020** "Risk management - Guidelines on using ISO 31000 in management systems" («**Менеджмент риска - Рекомендации по использованию стандарта ISO 31000 в системах управления**»).

ISO 31000:2018

- **Стандарт ISO 31000:2018 предназначен для тех**, кто создает и сохраняет ценности, создаваемые компанией, путем управления рисками, принятия решений, выбора и достижения целей, а также с помощью улучшения эффективности процессов.
- **Подчеркивается, что управление рисками - это итеративный процесс**, направленный на выбор стратегии и принятие информированных управленческих решений при наличии внешних и внутренних факторов и воздействий, которые могут помешать достижению целей компанией.
- При этом указано, что **управление рисками должно осуществляться на всех уровнях компании**, включать взаимодействие со стейкхолдерами, а также учитывать внешние и внутренние факторы (т.н. «контекст»), включая социокультурные факторы.
- **Рекомендации**, которые приведены в стандарте, не являются специфичными для какой-либо отрасли и **могут быть скорректированы в процессе применения на всех уровнях управления компанией на протяжении всего её жизненного цикла**.

ISO 31000:2018

- Стандарт ИСО 31000 дает также достаточно простые определения ключевым терминам риск-менеджмента:
  - **риск (англ. risk)** - это воздействие неопределенности на достижение целей; при этом воздействием является позитивное и/или негативное отклонение от ожидаемого результата, приносящее возможности и угрозы;
  - **риск-менеджмент (англ. risk management)** - это скоординированные действия по управлению и контролю организации в области рисков;
  - **источник риска (англ. risk source)** - это элемент, который самостоятельно или в совокупности с другими факторами может увеличить риск;
  - **событие (англ. event)** - это возникновение или изменение определенного набора обстоятельств; при этом у события может быть одна или несколько причин и последствий, а само событие может быть источником риска;
  - **последствие (англ. consequence)** - это результат события, повлиявший на достижение целей; при этом последствия могут быть определенными и неопределенными, могут иметь положительное или отрицательное прямое или косвенное влияние на достижение целей, а также могут быть выражены качественно или количественно;
  - **мера управления (англ. control)** - мера, которая поддерживает и/или модифицирует риск; при этом меры управления могут включать в себя процессы, политики, устройства, практические действия.

ISO 31000:2018

- **В стандарте ISO 31000:2018** (ИСО 31000-2019) **подчеркивается, что цель управления рисками - это создание и сохранение создаваемых компанией ценностей**, для чего необходимо придерживаться нижеуказанных принципов управления рисками, помогающих организации управлять воздействием неопределенностей на достижение целей (т.е. на риски как таковые).

ISO 31000:2018

- **Эффективный процесс риск-менеджмента должен обладать следующими свойствами** (которые еще называются принципами ИСО 31000):
  - **интегрированный**, т.е. являющийся неотъемлемой частью любой деятельности компании;
  - **структурированный и всеобъемлющий**, т.е. приводящий к логически связанным и измеримым результатам;
  - **гибкий**, т.е. адаптируемый и соответствующий внешнему и внутреннему контексту организации и ее целям;
  - **вовлекающий**, т.е. обеспечивающий своевременное и корректное привлечение стейкхолдеров для учета их знаний, мнений и взглядов для повышения осведомленности и принятия более информированных решений при управлении риском;
  - **динамичный**, т.е. учитывающий изменение рисков при модификации контекста организации, вследствие чего риск-менеджмент ожидает, обнаруживает, признает и реагирует на такие изменения и события своевременно и должным образом.
  - **основывающийся на наилучшей информации**, т.е. учитывающий историческую и текущую информацию, прогнозы на будущее, любые ограничения и неопределенности данных сведений; при этом информация должна быть своевременной, точной и доступной релевантным стейкхолдерам;
  - **учитывающий человеческие и культурные факторы**, т.к. они оказывают существенное влияние на управление рисками на всех этапах и уровнях;
  - **непрерывно улучшающийся**, т.е. постоянно совершенствующийся на основе полученного опыта и знаний.

ISO 31000:2018 **Фреймворк (инфраструктура)**

- Фреймворк управления рисками по **ISO 31000:2018** (ИСО 31000-2019) состоит из следующих составляющих:
  - 1. Поддержка со стороны руководства.
  - 2. Интеграция.
  - 3. Создание фреймворка.
  - 4. Внедрение фреймворка.
  - 5. Оценка.
  - 6. Улучшение.

ISO 31000:2018 **Фреймворк**

- **1. Поддержка со стороны руководства.**
- **Задача топ-менеджмента состоит в обеспечении деятельности риск-менеджмента на высоком уровне**:
  - документальной поддержке в согласовании документов по управлению рисками,
  - выделении ресурсов,
  - назначении ответственных.
- Это помогает связать риск-менеджмент со стратегией, целями и культурой организации, учесть все обязательные и необязательные требования в области рисков, утвердить уровень риск-аппетита компании, скоммуницировать ценности риск-менеджмента между всеми стейкхолдерами, содействовать систематическому подходу в области мониторинга рисков, а также обеспечить актуальность фреймворка контексту организации.
- Если в организации есть внутренние надзорные органы, то они должны контролировать процессы управления рисками.

ISO 31000:2018 **Фреймворк**

- **2. Интеграция.**

- **Задачи риск-менеджмента должны решаться на всех уровнях компании соответствующими ответственными лицами**, при этом все сотрудники компании должны понимать важность обработки рисков. Риск-менеджмент должен быть частью организационной культуры компании, её бизнес-процессов, стратегии, целей.

ISO 31000:2018 **Фреймворк**

- **3. Создание фреймворка.**
- **3.1. Для создания корректного фреймворка (в стандарте ГОСТ 31000 термин «фреймворк» переведен как «инфраструктура») ответственные лица должны понимать внешний и внутренний контекст компании.**
- **Внешний контекст** состоит из оценки различных внешних факторов (социальных, политических, культурных, юридических, финансовых, технологических, экономических - как международных, так и локальных), ключевых драйверов и трендов, влияющих на цели компании, а также ожиданий и потребностей стейкхолдеров, контрактных обязательств и взаимоотношений, сложности и взаимозависимости сетей (технических, социальных, финансовых и т.д.).
- **Внутренний контекст** компании состоит из миссии и целей, управленческой структуры и ответственных лиц, стратегий, целей и политик, культуры компании, внутренних нормативных документов, возможностей (финансовых, человеческих, процессов, систем и технологий), данных, информационных систем и потоков, внутрикорпоративных взаимозависимостей и взаимосвязей.

ISO 31000:2018 **Фреймворк**

- **3. Создание фреймворка.**
- 3.2. **Поддержка со стороны руководства** должна выражаться в признании важности риск-менеджмента, внедрении механизмов управления рисками во все бизнес-процессы на всех уровнях компании, назначении ответственных лиц и выделении необходимых ресурсов, арбитраже конфликтных ситуаций, пересмотре и улучшении стратегий риск-менеджмента.

- 3.3. **Назначение организационных ролей, ответственных**, должностных обязанностей должно осуществляться руководством, при этом ему следует подчеркивать важность риск-менеджмента и назначать ответственных должностных лиц (владельцев риска).

ISO 31000:2018 **Фреймворк**

- **3. Создание фреймворка.**
- 3.4. **Выделение ресурсов** также осуществляется руководством, при этом ресурсы могут включать в себя сотрудников, компетенции, опыт, организационные процессы, методы и инструменты, документарное обеспечение деятельности, системы управления знаниями и информацией, обучающие курсы и профессиональное развитие.

- 3.5. **Внедрение методов коммуникации и консультирования** подразумевает обмен информацией с целевой аудиторией и получение обратной связи. Следует убедиться, что актуальная и точная информация корректно собирается и передается, а фидбек обрабатывается, что приводит к внедрению улучшений на основе полученной обратной связи.

ISO 31000:2018 **Фреймворк**

- **4. Внедрение фреймворка.**
- Внедрение состоит из следующих **этапов**:
  - **разработка плана** с учетом временных и иных ресурсов;
  - **определение** того, где, кем, как и когда будут приниматься определенные управленческие решения;
  - **изменение процессов** принятия решений по мере необходимости;
  - **проверка** того, что внутренние договоренности об управлении рисками ясны и соблюдаются.

ISO 31000:2018 **Фреймворк**

- **5. Оценка.**

- Для оценки эффективности работы фреймворка управления рисками компании следует периодически оценивать эффективность фреймворка в достижении целей, планов, индикаторов и ожидаемого поведения, а также определять, остается ли фреймворк пригодным для достижения целей компании.

ISO 31000:2018 **Фреймворк**

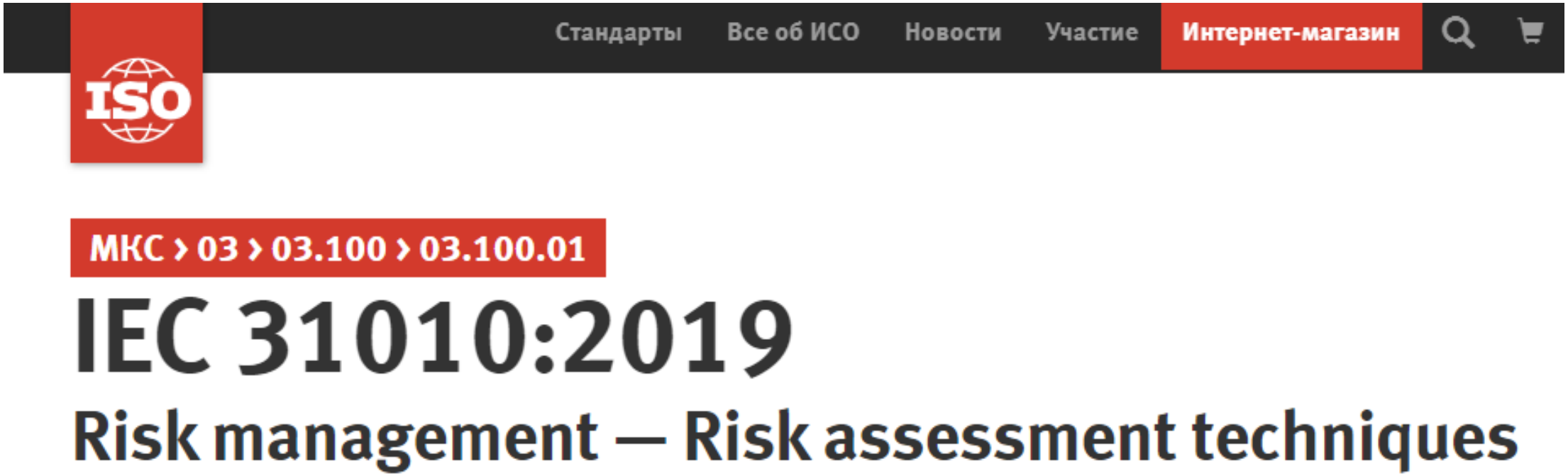
- **6. Улучшение.**

- Организациям следует непрерывно отслеживать актуальность внедренного фреймворка и адаптировать его под изменившийся внутренний или внешний контекст. Все выявленные недостатки и/или пути оптимизации должны быть учтены и запланировано их устранение и/или внедрение с назначением ответственных.

ISO 31000:2018 **Фреймворк**

- Сам **итеративный процесс** риск-менеджмента состоит из следующих этапов:
  - 1. Коммуникация и консультирование.
  - 2. Оценка границ процесса управления рисками, контекста и критериев риска.
  - 3. Оценка риска.
  - 3.1. Идентификация рисков.
  - 3.2. Анализ рисков.
  - 3.3. Оценка рисков.
  - 4. Обработка рисков.
  - 5. Мониторинг и пересмотр.
  - 6. Документирование и отчетность.

IEC 31010:2019



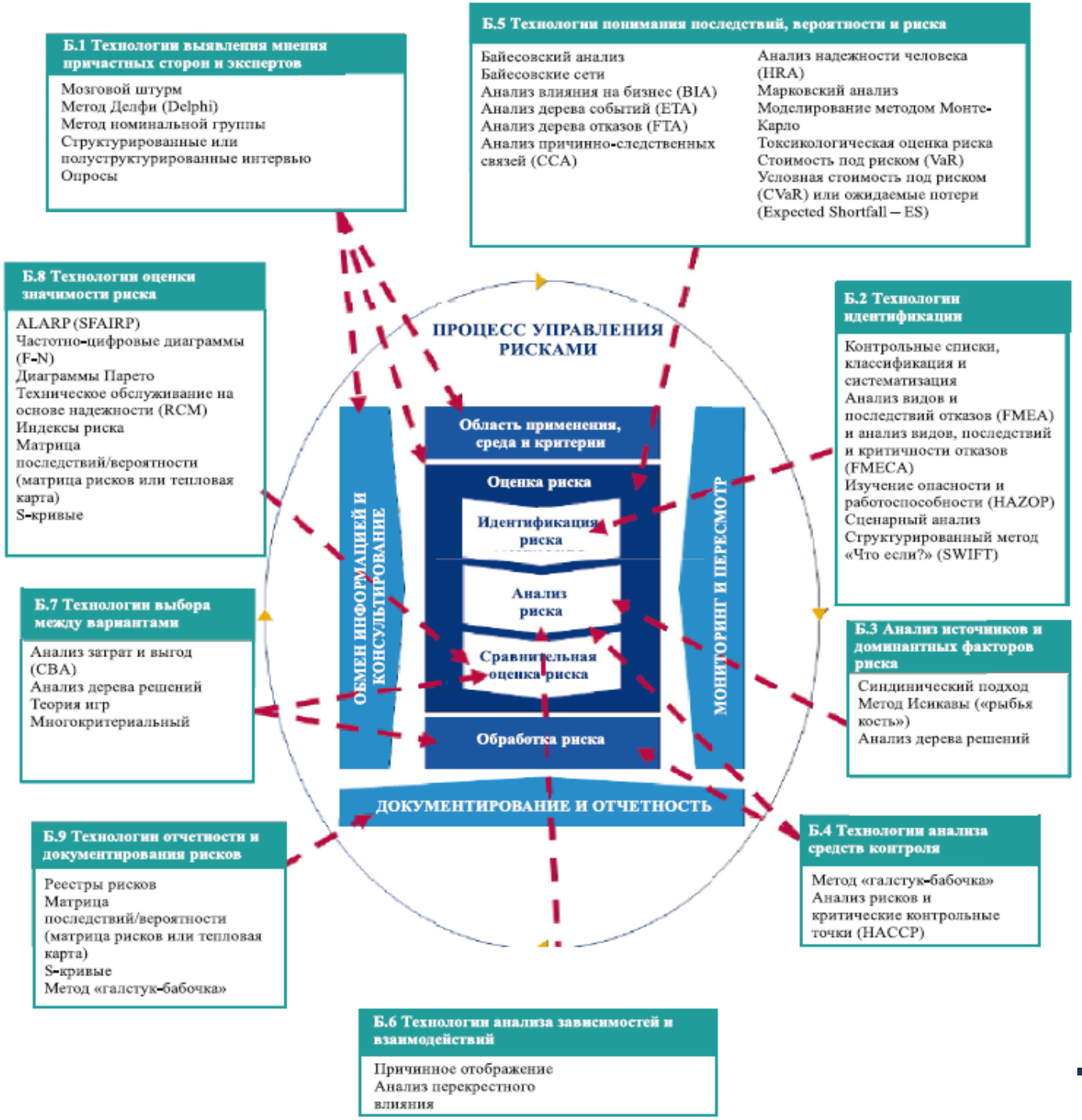
- **Стандарт IEC 31010:2019** примечателен тем, что в нем приведено более 40-ка разнообразных техник оценки риска, к каждой дано пояснение, указан способ применения для всех подпроцессов оценки риска (идентификация риска, определение источников и причин риска, анализ мер защиты, анализ последствий, вероятностей, взаимосвязей и взаимодействий, измерение и оценка уровня риска, выбор мер защиты, отчетность), а для некоторых техник приведены и практические примеры использования.
- Кроме того, на данный стандарт в его отечественном варианте ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» ссылается 607-П ЦБ РФ «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков».

IEC 31010:2019

- **ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска** (Risk management. Risk assessment technologies). Данный стандарт разработан с учетом основных нормативных положений международного стандарта МЭК **IEC 31010:2019*** «Менеджмент риска. Технологии оценки риска» (IEC 31010:2019 "Risk management - Risk assessment techniques", NEQ). Разработан **взамен ГОСТ Р ИСО/МЭК 31010-2011**
- https://docs.cntd.ru/document/1200170253
- https://upravlenie-riskami.ru/files/free/gost-r-58771-2019-menedgement-riska-tehnologii-otsenki-riska.pdf

ГОСТ Р 58771-2019

Применение технологий в процессе управления рисками



8. Методологии (стандарты) риск-менеджмента информационной безопасности в различных странах мира

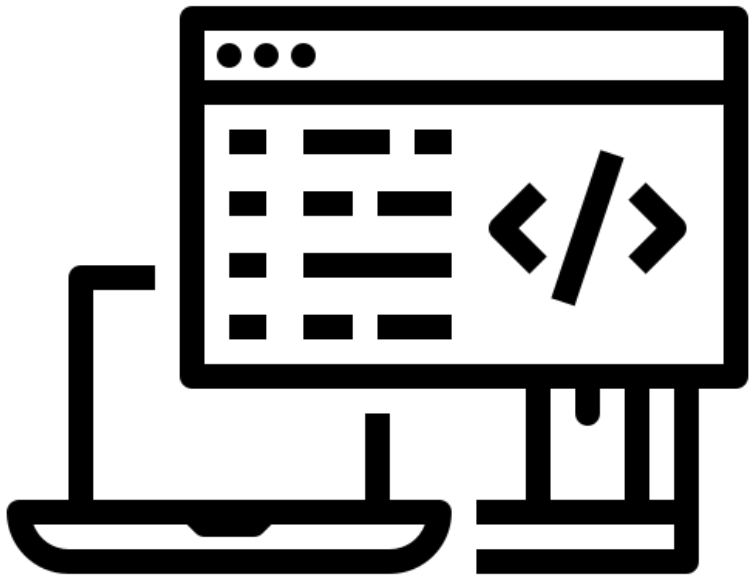
Китай

- **GB/T 33132-2016** — Information security technology — Information security risk processing implementation guide (Технология информационной безопасности - Руководство по внедрению обработки рисков информационной безопасности)

- **GB/Z 24364-2009** — Information security technology — Information security risk management guide (Технология информационной безопасности - Руководство по управлению рисками информационной безопасности)

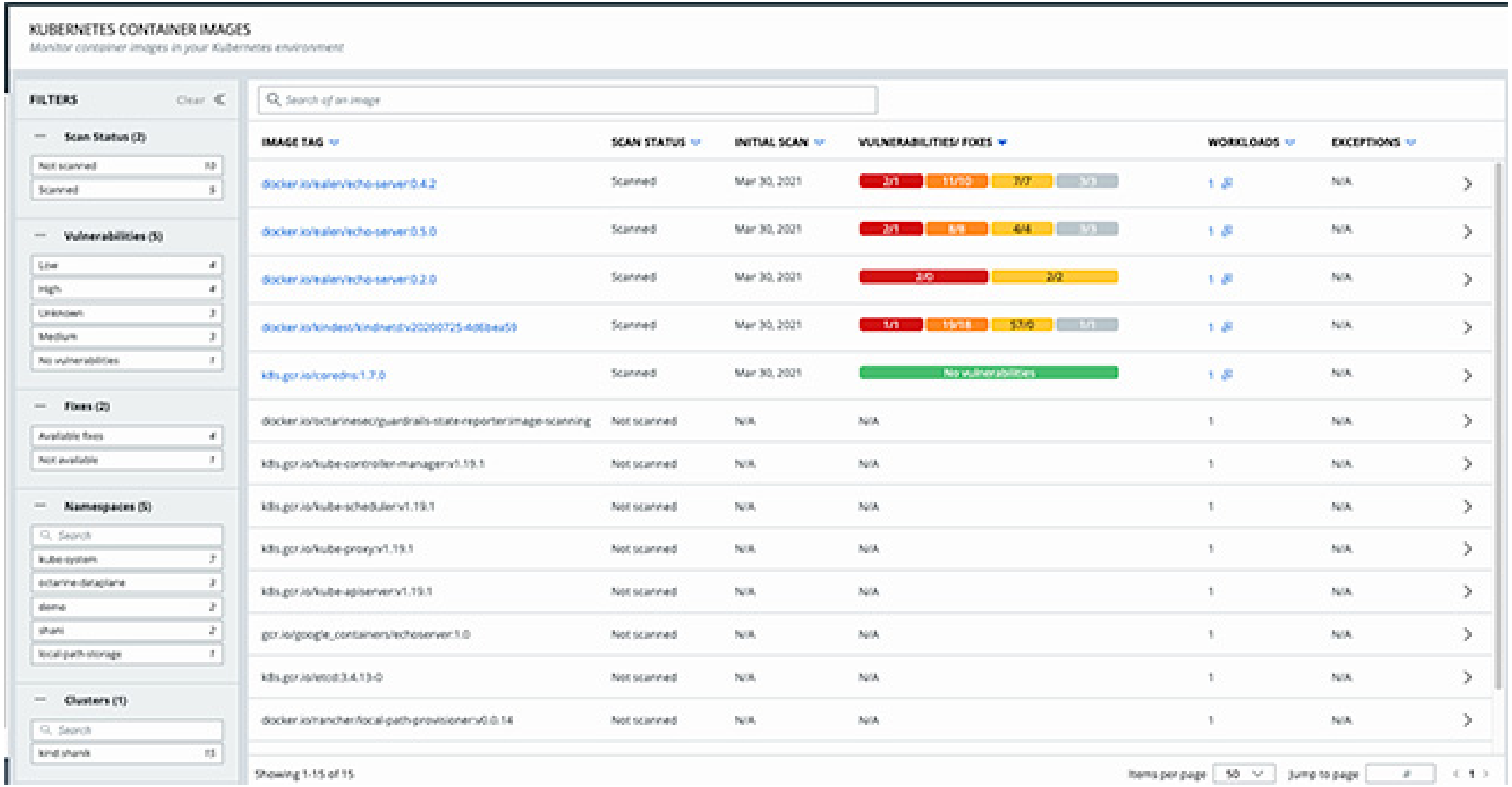
- **GB/T 20984-2007** — Information security technology — Information security risk assessment specification (Технология информационной безопасности - Спецификация оценки рисков информационной безопасности)

- **GB/T 31509-2015** — Information security technology — Implementation guide for information security risk assessment (Технология информационной безопасности - Руководство по внедрению оценки рисков информационной безопасности)



9. Специализированное программное обеспечение

VMware Carbon Black Cloud Container



https://www.carbonblack.com/products/vmware-carbon-black-cloud-container/

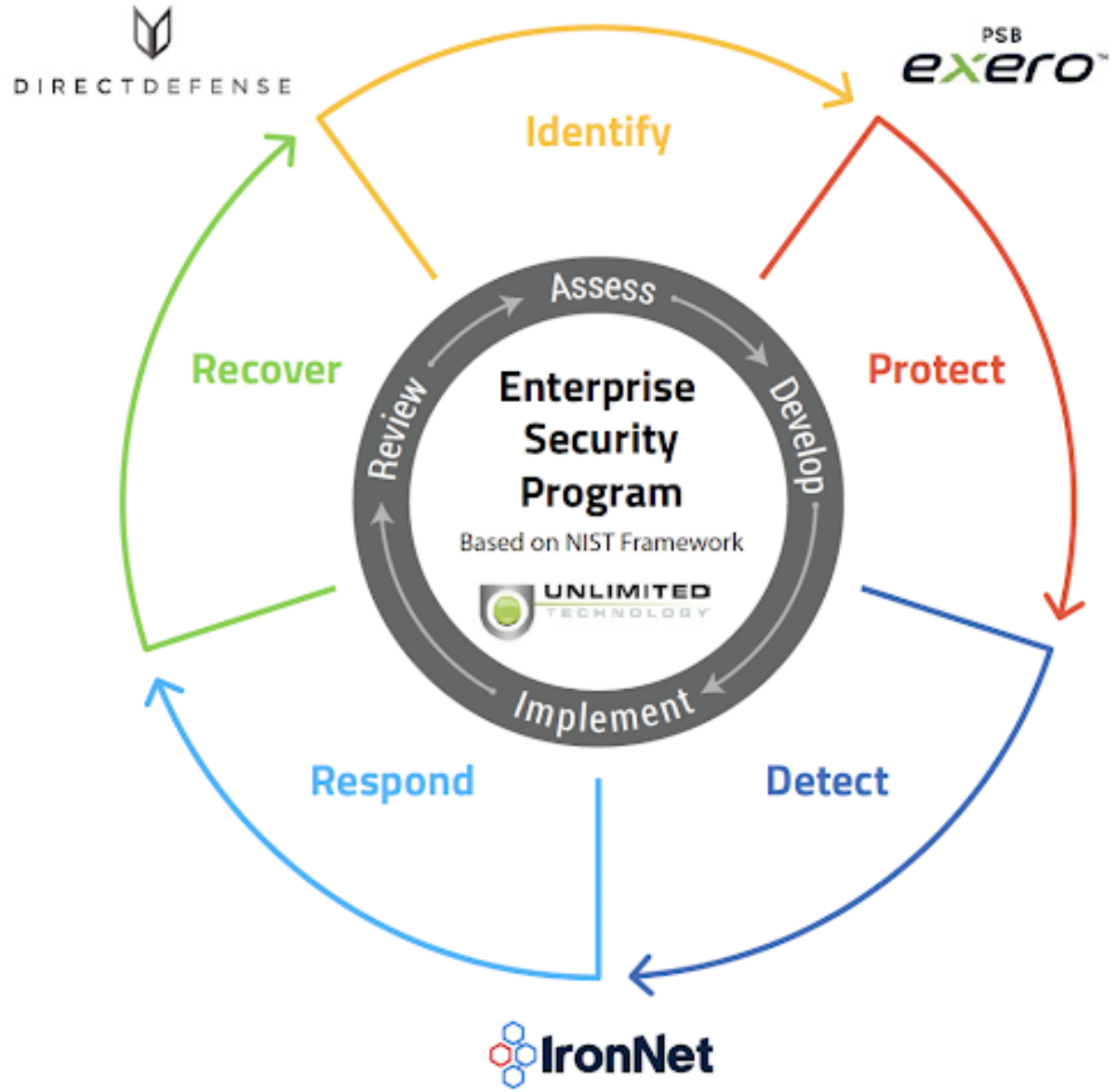
VMware Carbon Black Cloud Container

- **VMware Carbon Black Cloud Container – решение для обеспечения непрерывной видимости, безопасности и соответствия для всего жизненного цикла приложений Kubernetes, как облачных, так и локальных.** VMware Carbon Black Cloud Container обеспечивает видимость и контроль, необходимые группам безопасности приложений и DevOps для защиты кластеров Kubernetes и развернутых в них приложений.
- Решение обеспечивает мгновенную видимость всех рабочих нагрузок Kubernetes с возможностью обеспечения соответствия, безопасности и управления с единой панели мониторинга с полной видимостью состояния безопасности в кластерах Kubernetes. Решение также предоставляет сводную оценку рисков как от уязвимостей, так и от неправильных конфигураций.

Enterprise Security Program Review

- **Enterprise Security Program Review (ESPR) – сервис для обнаружения и реагирования на угрозы сетевой безопасности** (NDR), предлагаемый компанией IronNet Cybersecurity совместно с Unlimited Technology, Exero и DirectDefense.
- Первое в своем роде NDR-решение ESPR оценивает текущее и желаемое будущее состояние инфраструктуры организации в соответствии с национальными отраслевыми стандартами и технологиями кибербезопасности.
- ESPR проводит оценку, тестирование и анализ существующих мер безопасности в организации, анализирует подверженность рискам и помогает внедрять индивидуальные решения безопасности. Применяя целостный подход к кибербезопасности, решение устраняет киберриски, которые упускаются из виду поставщиками единых решений безопасности. ESPR - единственное комплексное решение для крупных и малых предприятий, обеспечивающее установку, модификацию и работу успешной платформы безопасности.
- https://www.ironnet.com/services/enterprise-security-program-review

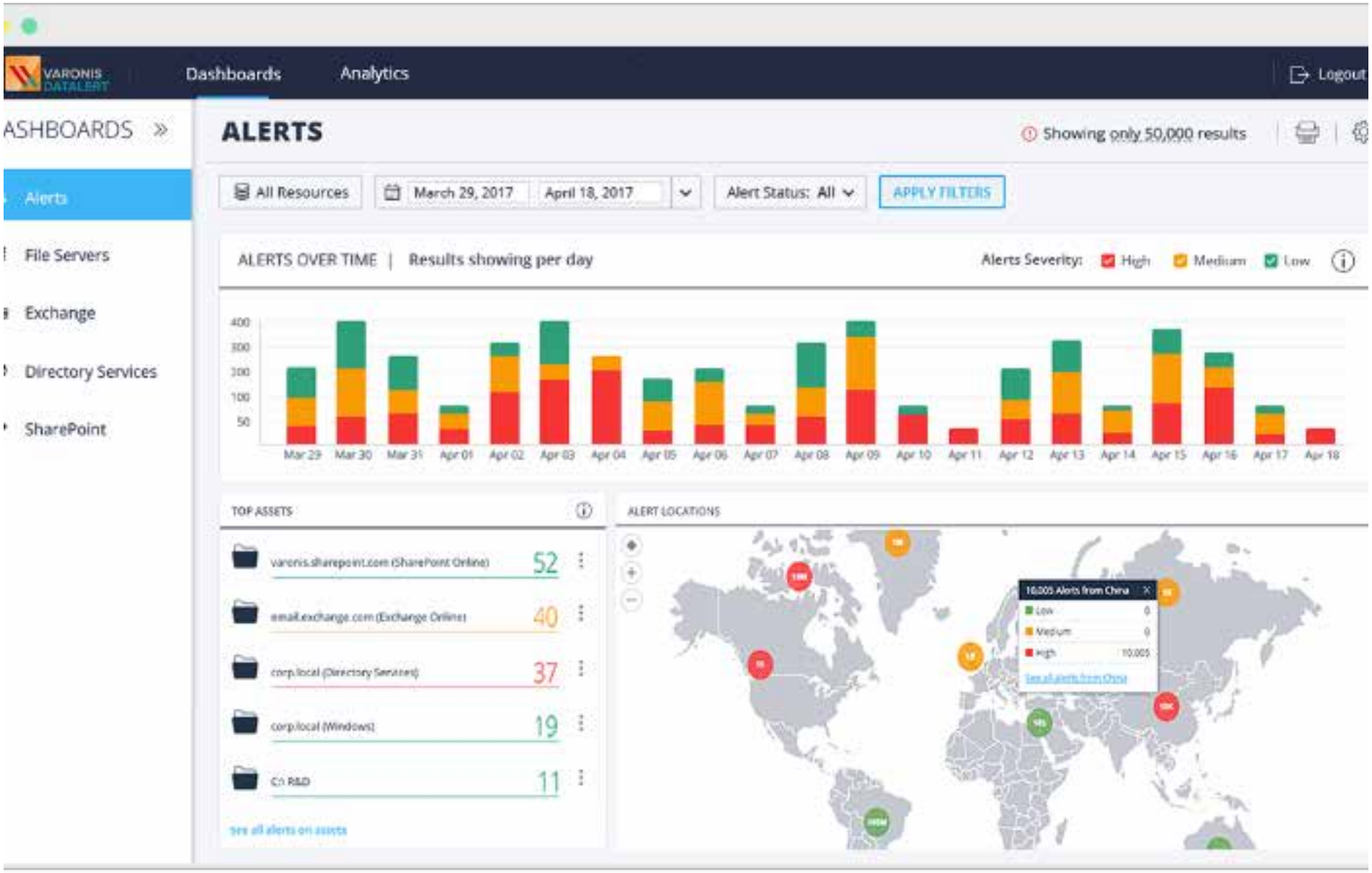
Enterprise Security Program Review



Varonis

- **Varonis – единая платформа кибербезопасности для защиты корпоративных данных от внутренних угроз и кибератак.**
- Представляет собой уникальное решение на рынке, которое объединяет контентный анализ данных, управление доступом и поведенческий анализ. Это насыщает систему более достоверными событиями и снижает число ложных срабатываний. Оповещения об аномальных всплесках активности в режиме реального времени позволяют проводить оперативное расследование инцидентов.
- Varonis значительно сокращает время обнаружения и реагирования на кибератаки.
- Кросплатформенный мониторинг событий в Windows, UNIX/Linux, NAS, Active Directory, SharePoint, Exchange и в облачных сервисах. Единая платформа Varonis обеспечивает прозрачность всех происходящих процессов и полный контроль для управления рисками и защиты наиболее ценных активов компании.
- Платформа кибербезопасности Varonis масштабируется, как никакая другая на рынке. Она прошла боевое тестирование в сетях с миллиардами событий ежедневно, анализируя петабайты данных.
- https://www.varonis.com/ru/data-security-insider-threat-compliance-software/
- https://info.varonis.com/demo/ru - Демонстрация возможностей

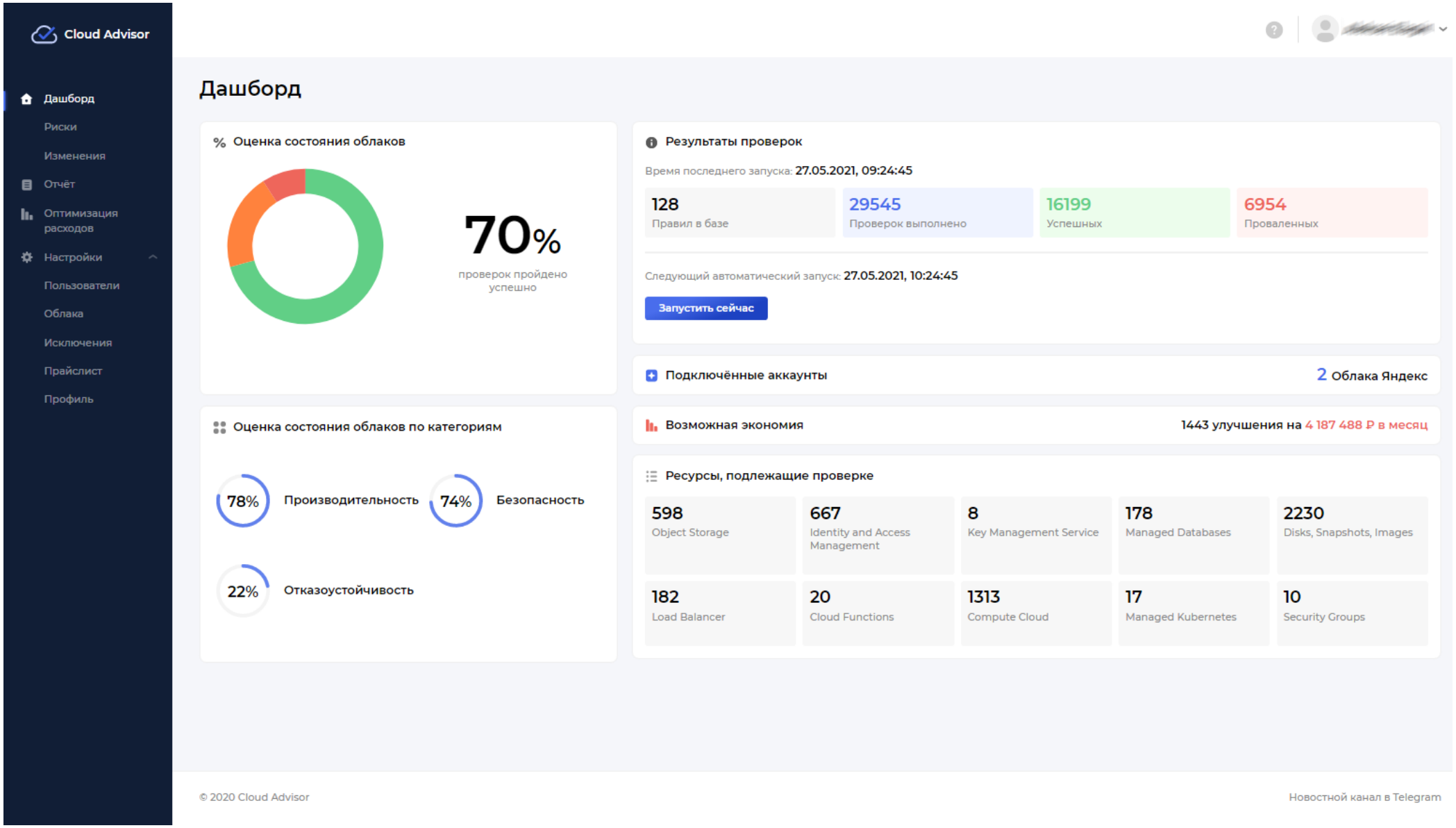
Varonis


VARONIS DATALERT
Dashboards
Analytics
Logout
ASHBOARDS
Alerts
File Servers
Exchange
Directory Services
SharePoint
ALERTS
Showing only 50,000 results
All Resources
March 29, 2017
April 18, 2017
Alert Status: All
APPLY FILTERS
ALERTS OVER TIME | Results showing per day
Alerts Severity: High Medium Low
400
300
200
100
50
Mar 29 Mar 30 Mar 31 Apr 01 Apr 02 Apr 03 Apr 04 Apr 05 Apr 06 Apr 07 Apr 08 Apr 09 Apr 10 Apr 11 Apr 12 Apr 13 Apr 14 Apr 15 Apr 16 Apr 17 Apr 18
TOP ASSETS
varonis.sharepoint.com (SharePoint Online) 52
email.exchange.com (Exchange Online) 40
corp.local (Directory Services) 37
corp.local (Windows) 19
R&D 11
see all alerts on assets
ALERT LOCATIONS
10,005 Alerts from China
Low 0
Medium 0
High 10,005
See all alerts from China

Cloud Advisor

- **Cloud Advisor - бесплатное решение для обеспечения безопасности, производительности, отказоустойчивости и оптимизации IT-инфраструктуры, расположенной в Яндекс.Облаке.** Продукт подключается к облаку клиента и автоматически проводит анализ инфраструктуры на подверженность воздействию актуальных угроз, соответствие проверенным практикам использования облачных сервисов и рекомендациям провайдера. **Его выпустили основатели компании Agnitum, известной по продукту Outpost Firewall.**
- По данным Gartner, “практически все успешные атаки на облачные сервисы являются результатом их неверной настройки пользователем, неграмотного управления и допущенных ошибок” (Отчет Innovation Insight for Cloud Security Posture Management, 25 января 2019). Cloud Advisor способен оперативно находить такие ошибки в быстро меняющейся облачной среде и предоставлять список необходимых действий для их исправления.
- Кроме того, продукт помогает организациям решить целый ряд актуальных задач, возникающих при использовании облака. В частности, Cloud Advisor позволит существенно снизить расходы благодаря выбору оптимальных ресурсов для виртуальных машин и выявлению неиспользуемых объектов. Также продукт способствует повышению скорости работы и эффективности облачной инфраструктуры посредством обнаружения перегруженных и некорректно работающих ресурсов.
- На данный момент продукт поддерживает Яндекс.Облако, поддержка других российских и западных облачных провайдеров будет доступна в ближайшее время. Продукт не требует установки дополнительных компонентов внутри инфраструктуры.
- https://www.cloudadvisor.ru

Cloud Advisor

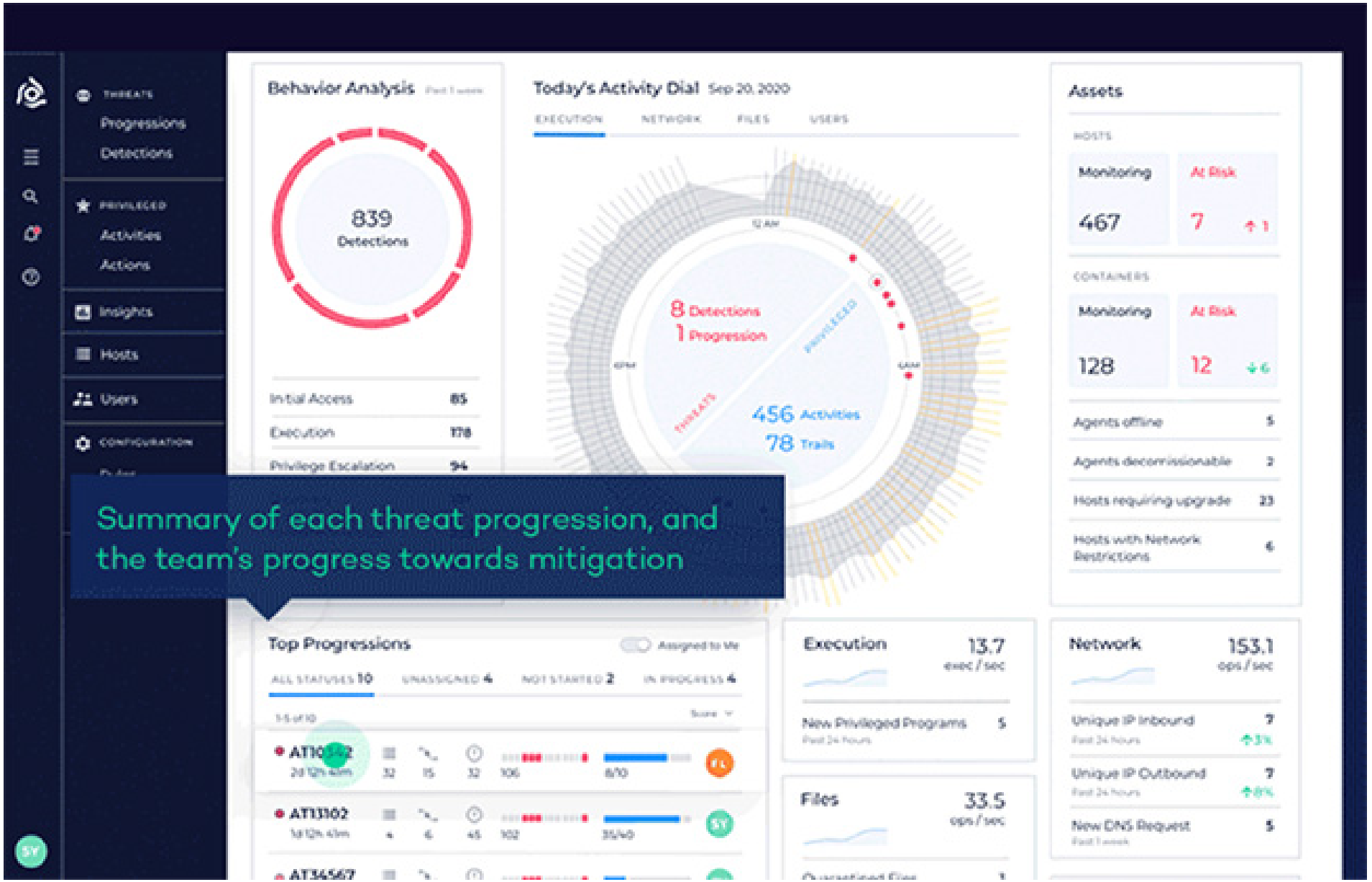


Confluera XDR

- **Confluera XDR** – платформа для обнаружения и реагирования с уникальной возможностью отслеживать угрозы, распространяющиеся в рабочей среде предприятия. Confluera XDR не просто отображает изолированные уведомления, а всесторонне интегрирует полученные из рабочей среды сигналы безопасности для того, чтобы предоставлять полную картину кибератаки в реальном времени. С Confluera группы безопасности могут перехватывать угрозы по мере их возникновения, а не устранять постфактум.

- https://www.confluera.com – Confluera
- https://www.confluera.com/product-cxdr-platform - Confluera CxDR Platform

Confluera XDR

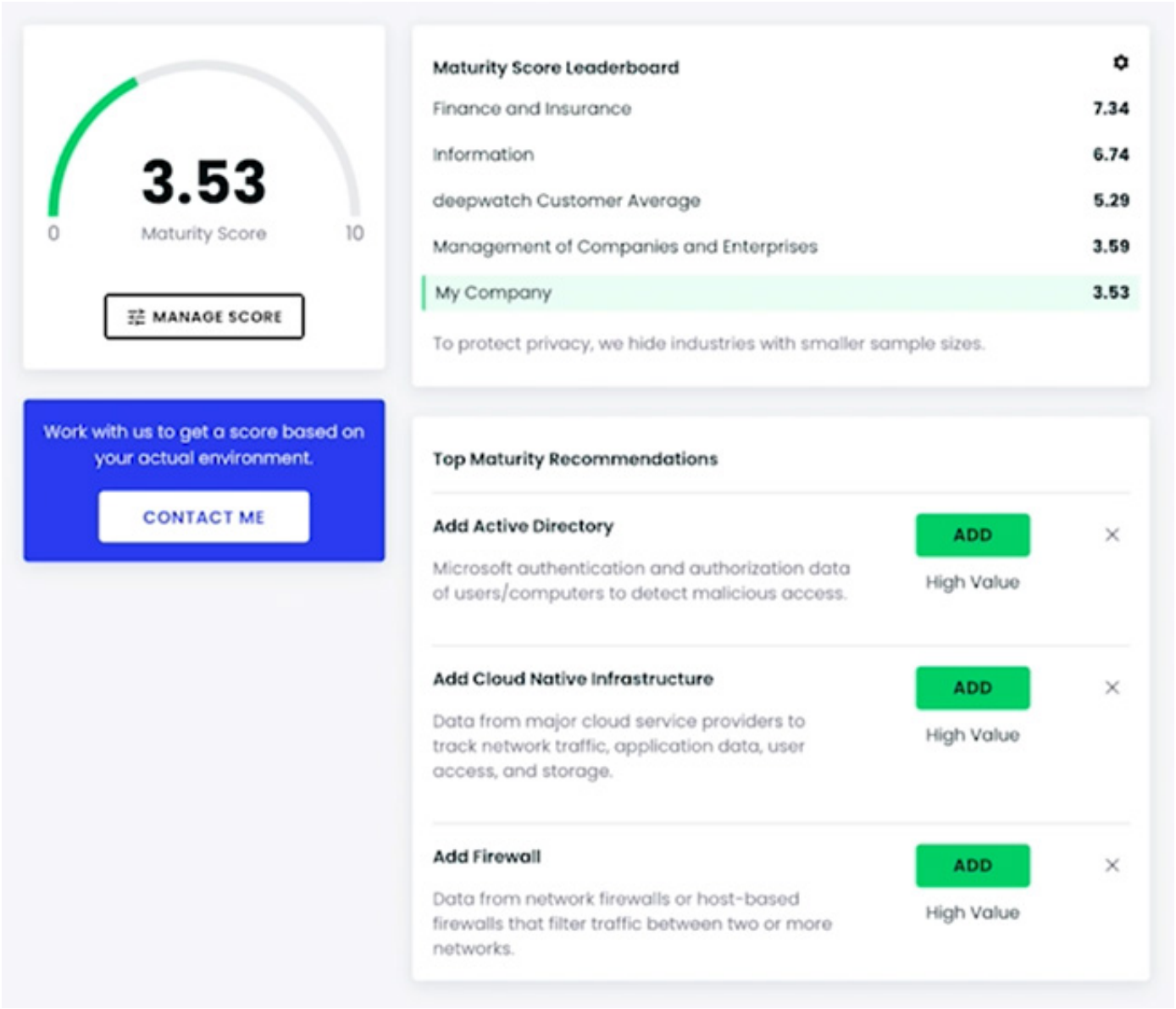


Deepwatch Lens Score

- **Deepwatch Lens Score** – приложение для специалистов, ответственных за измерение, мониторинг и повышение уровня зрелости SecOps своей компании. Deepwatch Lens Score позволяет директорам по информационной безопасности (CISO) быстро понять, как собираются источники данных и активная аналитика, какой у их компании на сегодняшний день показатель зрелости и как его улучшить. Мощное интуитивно понятное приложение предоставляет ценные данные и аналитическую информацию для руководителей по информационным технологиям всего за несколько минут.

- https://www.deepwatch.com/resource/deepwatch-lens-score/
- https://www.youtube.com/watch?v=4DLImYKOM4k

Deepwatch Lens Score

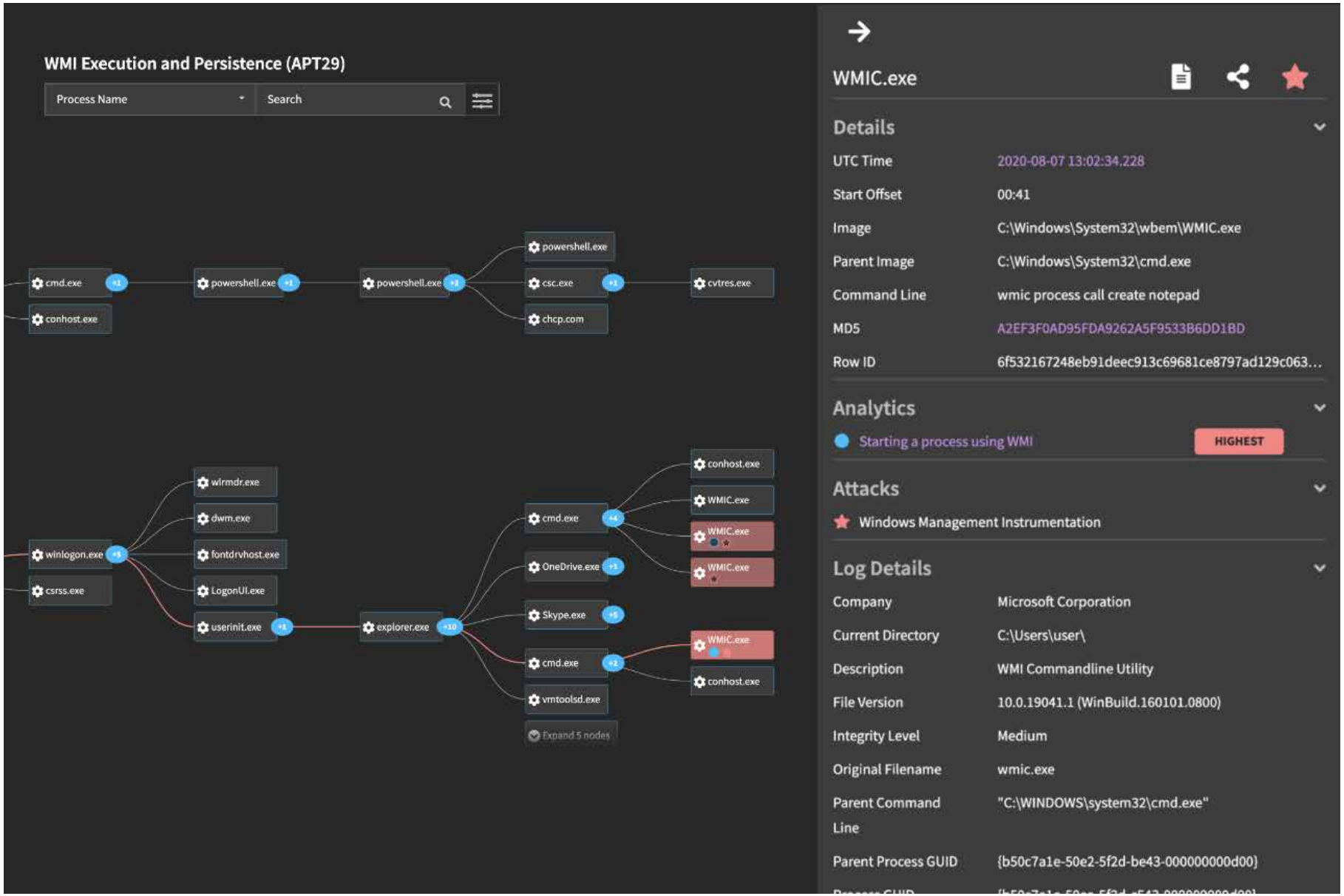


SnapAttack

- **Облачное программное решение SnapAttack** от компании Booz AllenHamilton объединяет весь жизненный цикл операций по обеспечению безопасности за счет объединения аналитики угроз и обнаружения хакеров. Это «фиолетовая» платформа для совместной работы, позволяющая «синим» и «красным» командам безопасности имитировать атаки, основываясь на собранных данных, делиться информацией о вредоносном поведении и разрабатывать аналитику поведенческого обнаружения, не зависящую от поставщика.

- https://www.boozallen.com/s/product/monitoring-threat-detection-mitigation-and-training.html
- https://www.boozallen.com/s/product/snapattack.html

SnapAttack

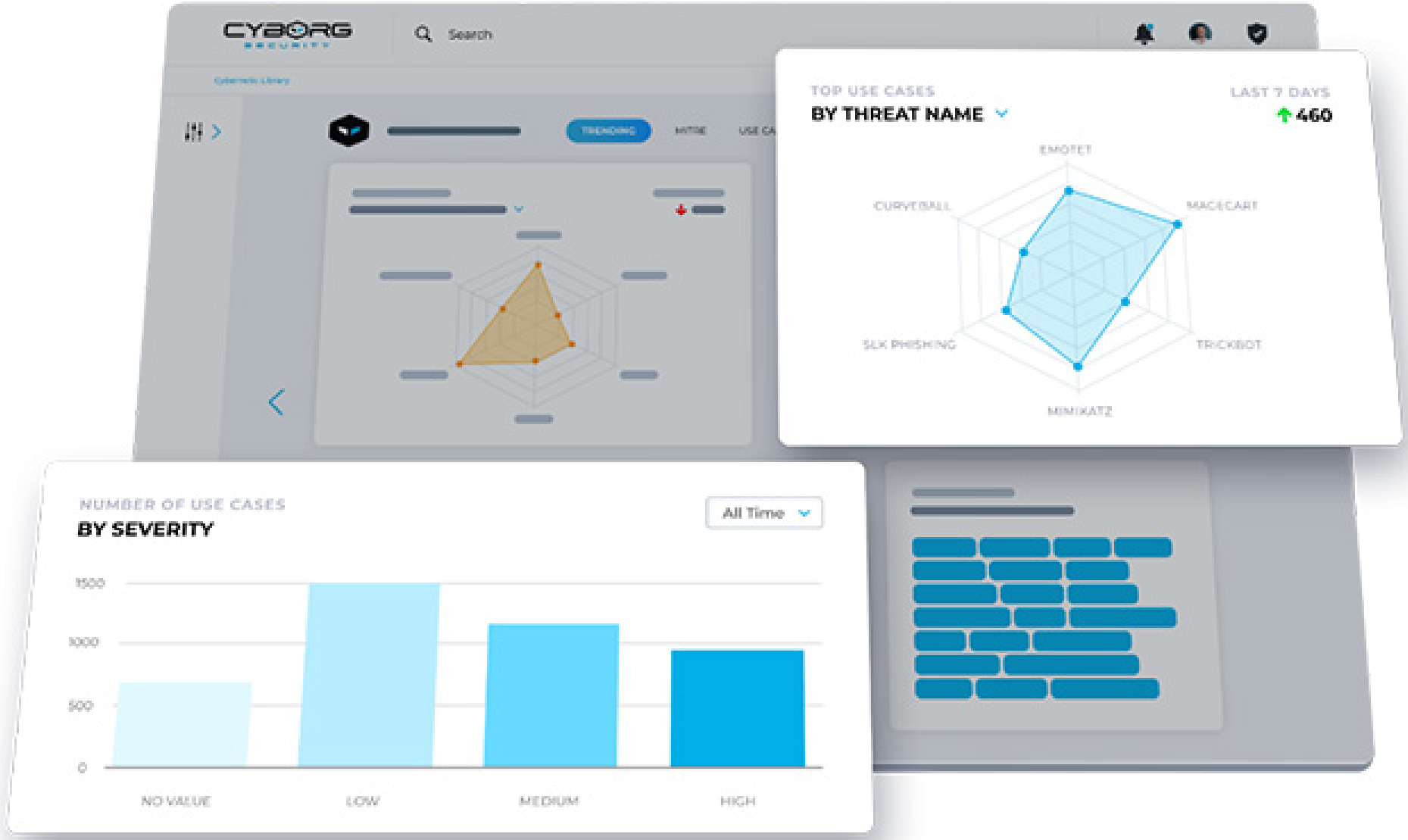

WMI Execution and Persistence (APT29)
Process Name
Search
cmd.exe
conhost.exe
powershell.exe
powershell.exe
powershell.exe
csc.exe
chcp.com
cvtres.exe
winlogon.exe
csrss.exe
wlrmdr.exe
dwm.exe
fontdrvhost.exe
LogonUI.exe
userinit.exe
explorer.exe
cmd.exe
OneDrive.exe
Skype.exe
cmd.exe
vmtoolsd.exe
Expand 5 nodes
conhost.exe
WMIC.exe
WMIC.exe
WMIC.exe
WMIC.exe
conhost.exe
WMIC.exe
Details
UTC Time 2020-08-07 13:02:34.228
Start Offset 00:41
Image C:\Windows\System32\wbem\WMIC.exe
Parent Image C:\Windows\System32\cmd.exe
Command Line wmic process call create notepad
MD5 A2EF3F0AD95FDA9262A5F9533B6DD1BD
Row ID 6f532167248eb91deec913c69681ce8797ad129c063...
Analytics
Starting a process using WMI
HIGHEST
Attacks
Windows Management Instrumentation
Log Details
Company Microsoft Corporation
Current Directory C:\Users\user\
Description WMI Commandline Utility
File Version 10.0.19041.1 (WinBuild.160101.0800)
Integrity Level Medium
Original Filename wmic.exe
Parent Command Line "C:\WINDOWS\system32\cmd.exe"
Parent Process GUID {b50c7a1e-50e2-5f2d-be43-000000000d00}

Cyborg Security HUNTER

- **Платформа HUNTER от компании Cyborg Security** предоставляет расширенные и контекстуализированные инструменты для поиска и обнаружения угроз, содержащие поведенческий контент для поиска угроз, эмуляцию угроз и подробные справочники. Платформа предоставляет организациям все необходимое для превращения ее аналитиков безопасности в квалифицированных «охотников» за киберугрозами.
- Платформа была разработана командой экспертов мирового класса по поиску угроз для того, чтобы предоставить расширенный контент для поиска и обнаружения угроз и тем самым обеспечить организациям возможность перехода от реактивной безопасности к упреждающему поиску угроз.
- Каждый пакет HUNTER был разработан специализированными исследователями угроз на основе анализа вредоносных программ и расследований инцидентов и сочетается с беспрецедентной контекстуализацией, полученной на основе передового анализа угроз.

- https://www.cyborgsecurity.com/blog/meet-cyborg-security-and-the-hunter-threat-hunting-platform/

Cyborg Security HUNTER

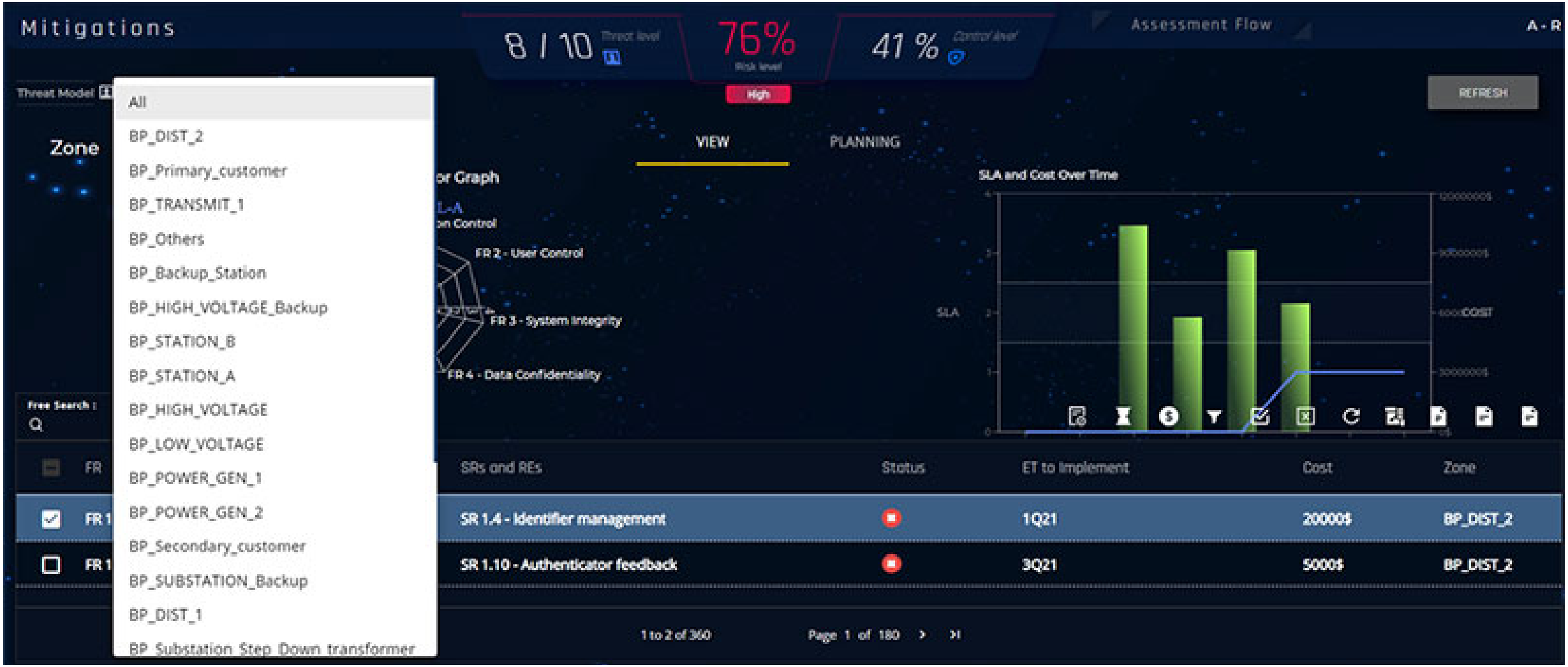


Radiflow CIARA

- **Cyber Industrial Automated Risk Analysis (CIARA) – платформа для анализа киберрисков на базе серии стандартов ISA/IEC 62443.** CIARA существенно упрощает пользователям АСУ ТП планирование снижения рисков и соблюдение нормативных требований для улучшения состояния безопасности своего предприятия.
- **CIARA** – это полностью автоматизированный инструмент для сбора данных об активах, анализа на основе данных и прозрачного расчета метрик рисков, включая оценку рисков для каждой зоны и бизнес-процесса на основе влияния на бизнес. Платформа является ответом на растущую цифровизацию производственных цехов (так называемая Четвертая промышленная революция), которая привела к росту киберугроз в то время, как процессы оценки рисков по-прежнему проводятся вручную и не позволяют решить проблему в полном объеме.

- https://radiflow.com
- https://radiflow.com/products/ciara-cyber-industrial-automated-risk-assessment/
- https://www.youtube.com/watch?v=2CsGVcoZSP4

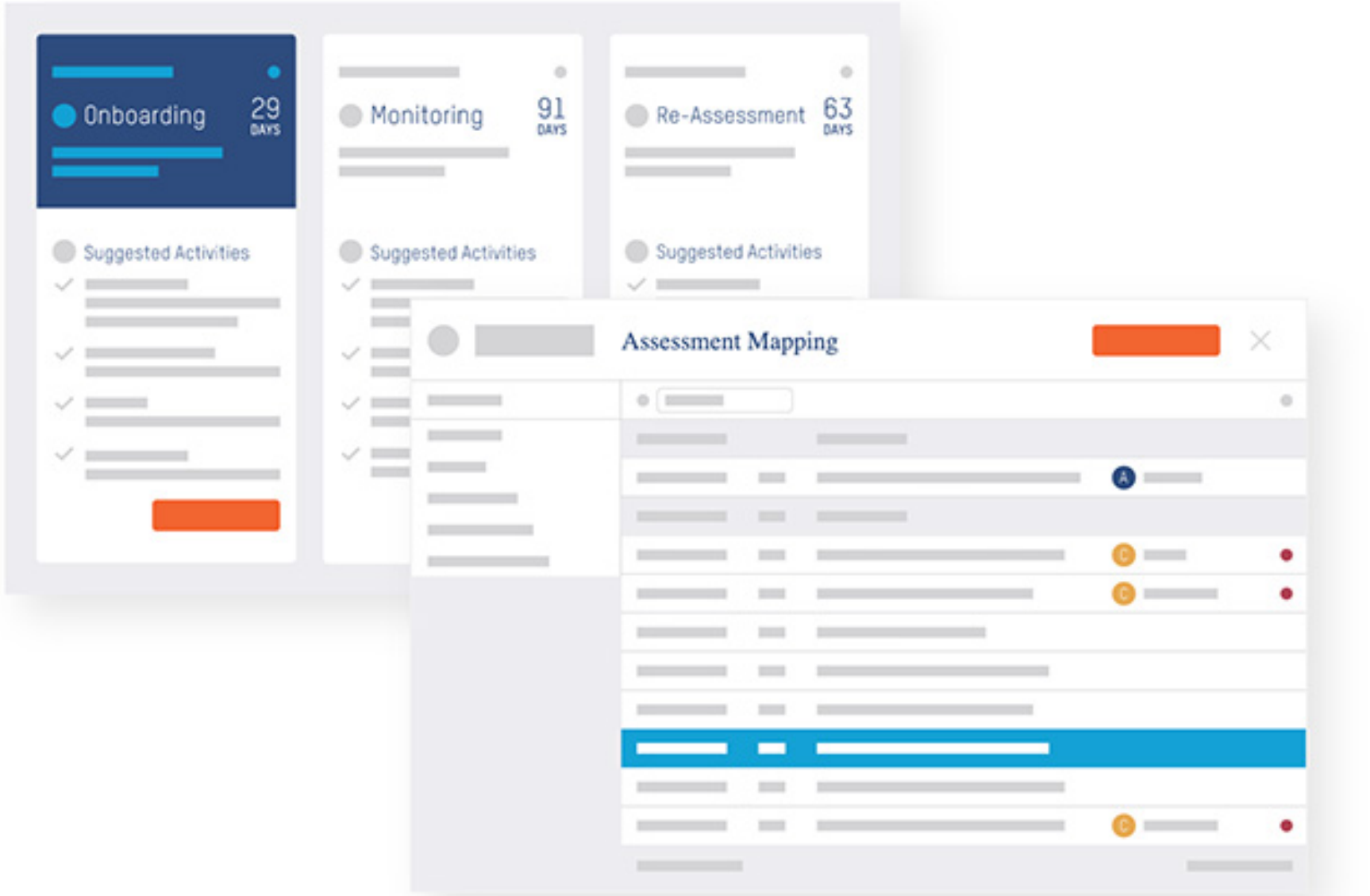
Radiflow CIARA



BitSight for Third-Party Risk Management

- **BitSight for Third-Party Risk Management – решение для управления киберрисками**. BitSight for Third-Party Risk Management немедленно обнаруживает риски, связанные с цепочкой поставок, и помогает предприятию сосредоточить свои ресурсы и вместе с поставщиками работать над снижением рисков.
- BitSight дает ИБ-специалистам представление о самых опасных проблемах, связанных с поставщиками. Это представление подкреплено данными, которые соответствуют потенциальным инцидентам и контексту безопасности от наиболее активного сообщества специалистов по рискам и безопасности.
- BitSight позволяет быстро запускать, расширять и оптимизировать сторонние программы управления рисками, используя уже имеющиеся у предприятия ресурсы.
- https://www.bitsight.com/third-party-risk-management#:~:text=BitSight%20for%20Third-Party%20Risk%20Management%20immediately%20exposes%20cyber%20risk,and%20measurable%20cyber%20risk%20reduction.

BitSight for Third-Party Risk Management



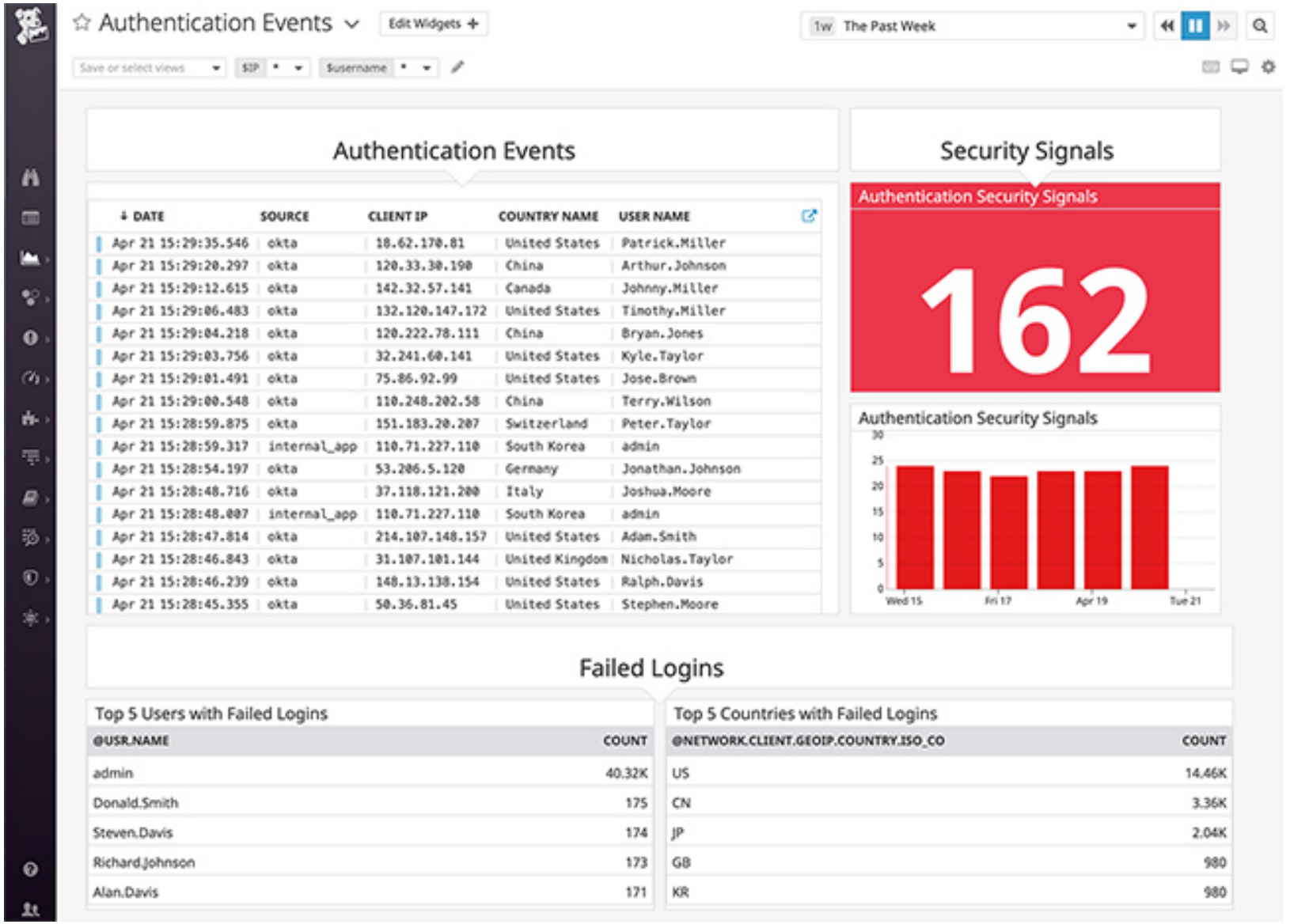
Obsidian Security

- **Платформа Obsidian обеспечивает быстрое обнаружение угроз, устранение утечек и усиление безопасности в SaaS-приложениях с помощью непрерывного мониторинга и аналитики без ущерба для рабочих процессов.** С помощью платформы группы безопасности предприятия могут отслеживать активность пользователей и получать своевременные оповещения для защиты как от случайных злоупотреблений, так и от инсайдерских угроз. Obsidian позволяет обнаруживать и реагировать на взломы учетных записей и утечки данных.
- Кроме того, платформа обеспечивает пользователям сервиса Zoom мониторинг, выявление и ответ на угрозы на корпоративном уровне. Obsidian генерирует аналитические данные и выдает предупреждения, связанные с различными рисками и угрозами.
- https://www.obsidiansecurity.com

Datadog Security Monitoring

- **Datadog Security Monitoring** объединяет разработчиков, операции и команды специалистов по безопасности на одной платформе. Datadog Security Monitoring отображает DevOps-контент, бизнес-показатели и сведения о безопасности на единой панели инструментов. Решение обнаруживает даже нестандартные угрозы и уведомляет о них ИБ-специалистов по электронной почте, Slack, Jira, PagerDuty или через web-перехватчик. В число обнаруживаемых угроз для приложений и инфраструктуры входят: целевые атаки, вредоносные IP-соединение, небезопасные конфигурации и пр.
- https://www.datadoghq.com
- https://docs.datadoghq.com/security_platform/

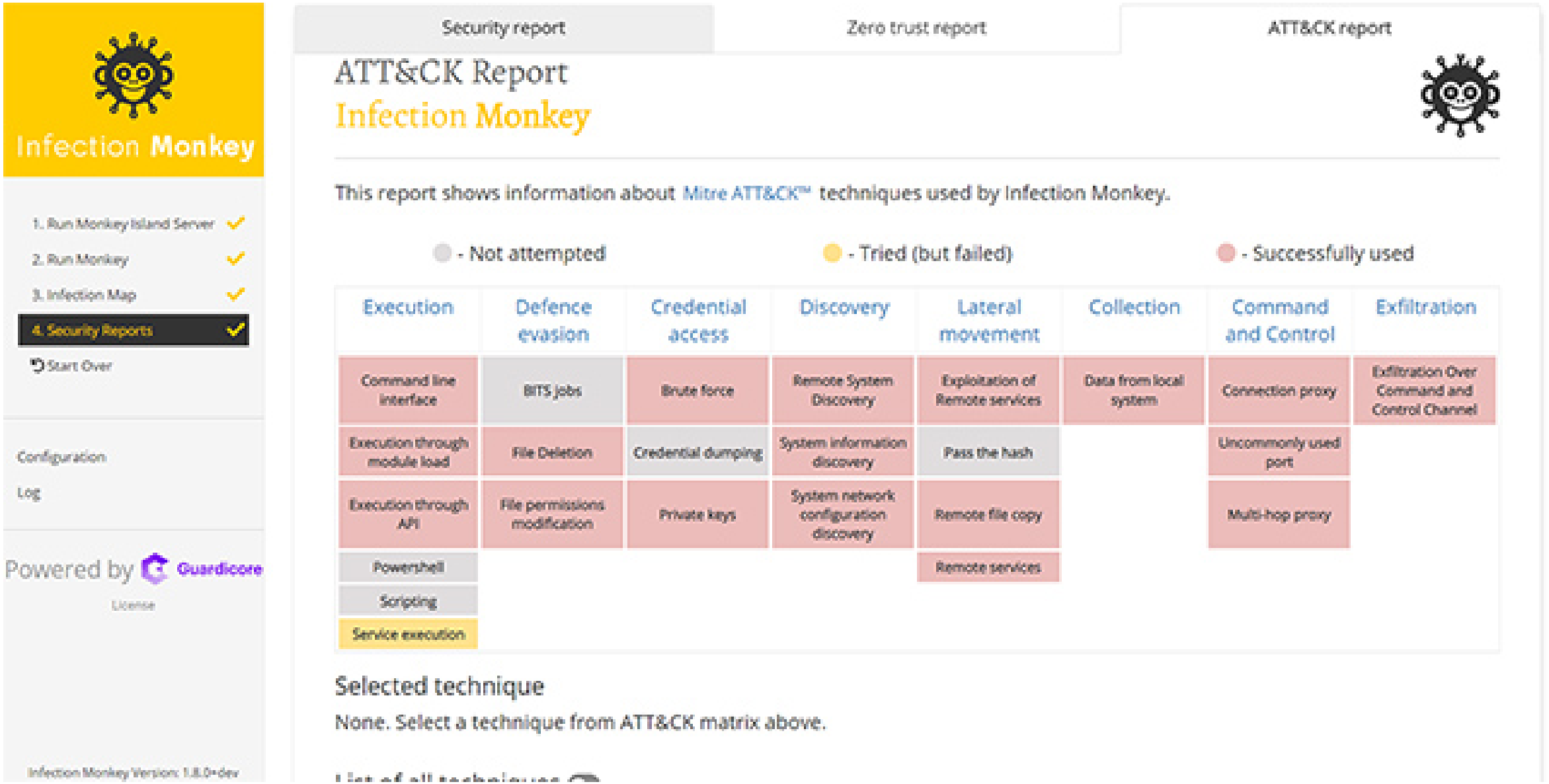
Datadog Security Monitoring



Guardicore Infection Monkey - FREE

- **Guardicore Infection Monkey – инструмент с открытым исходным кодом для моделирования атак.** Infection Monkey позволяет проводить оценку устойчивости частных и общедоступных облачных сред к атакам после взлома и боковым перемещениям (технике Lateral Movement). Позволяет оценить сеть с точки зрения Zero Trust и MITRE ATT&CK frameworks
- Для проведения оценки устойчивости среды достаточно лишь установить Infection Monkey на произвольную машину, и инструмент сам обнаружит угрозы безопасности, такие как кража учетных данных, взломанные машины и пр.
- Круглосуточный запуск Infection Monkey позволит выявлять появляющиеся новые угрозы безопасности и проверять используемые средства контроля безопасности при изменении среды. Инструмент предоставляет подробный отчет об обнаруженных угрозах вместе с советами по их исправлению. Для большей наглядности Infection Monkey также предоставляет визуальную карту сети с точки зрения потенциального злоумышленника.
- https://www.guardicore.com/infectionmonkey/

Guardicore Infection Monkey

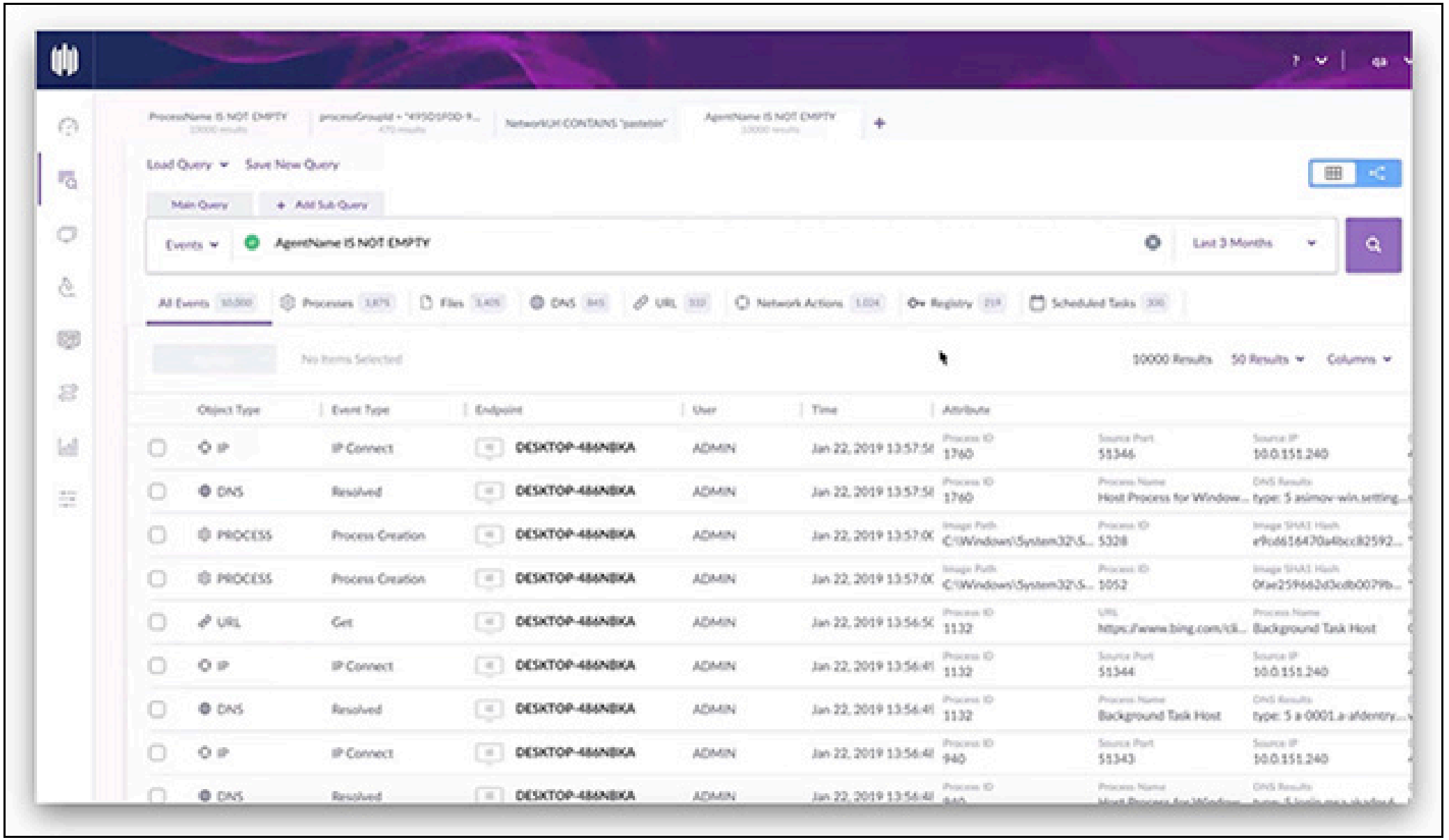


SentinelOne Singularity Platform

- **Singularity Platform** – единая платформа от компании SentinelOne для предотвращения, выявления и ответа на угрозы в контексте всех активов предприятия. Платформа обеспечивает широкий контекст для корпоративных сред с помощью множества предложений в единой консоли.
- Пользователи могут настроить на информационных панелях более 50 различных виджетов, определить интервалы между отчетами и полностью настроить информационные панели и отчеты для различных пользователей и аудиторий.
- Данные с платформы SentinelOne поступают на информационные панели в режиме реального времени и могут быть интегрированы с различными инструментами бизнес-аналитики, включая Tableau, Power BI, Splunk и Excel.

- https://www.sentinelone.com

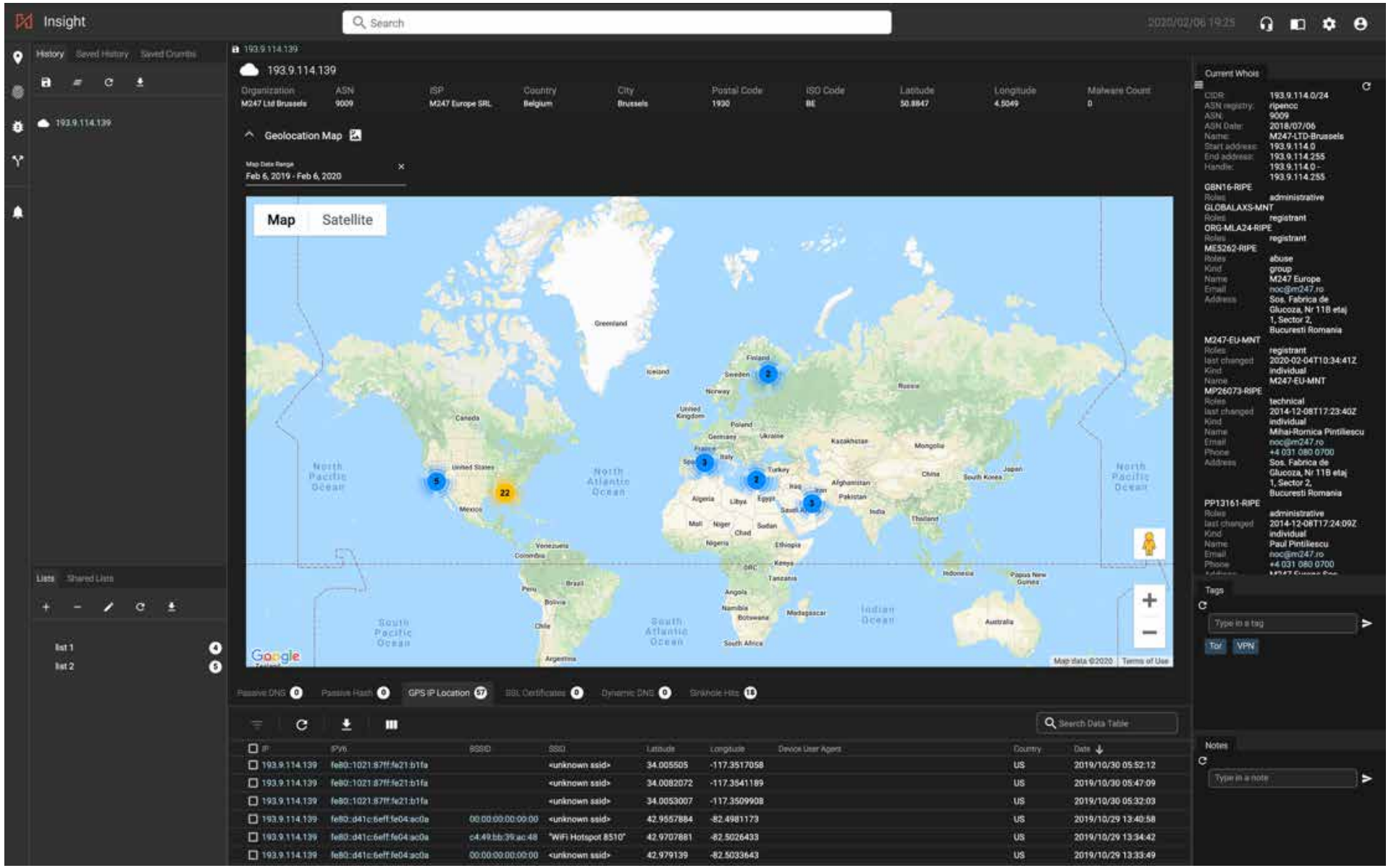
SentinelOne Singularity Platform



HYAS Insight

- **HYAS Insight** – решение для анализа и определения угроз, обеспечивающее видимость и производительность для аналитиков и исследователей безопасности. HYAS Insight позволяет аналитикам быстро связывать конкретные атаки и кампании с миллиардами известных индикаторов и показателей компрометации в режиме реального времени.
- Решение позволяет настраивать уведомления по электронной почте, телефону и пр. о создании каждого нового домена. Это позволит безопасникам выявлять попытки злоумышленников создать новую инфраструктуру.
- https://www.hyas.com/hyas-insight

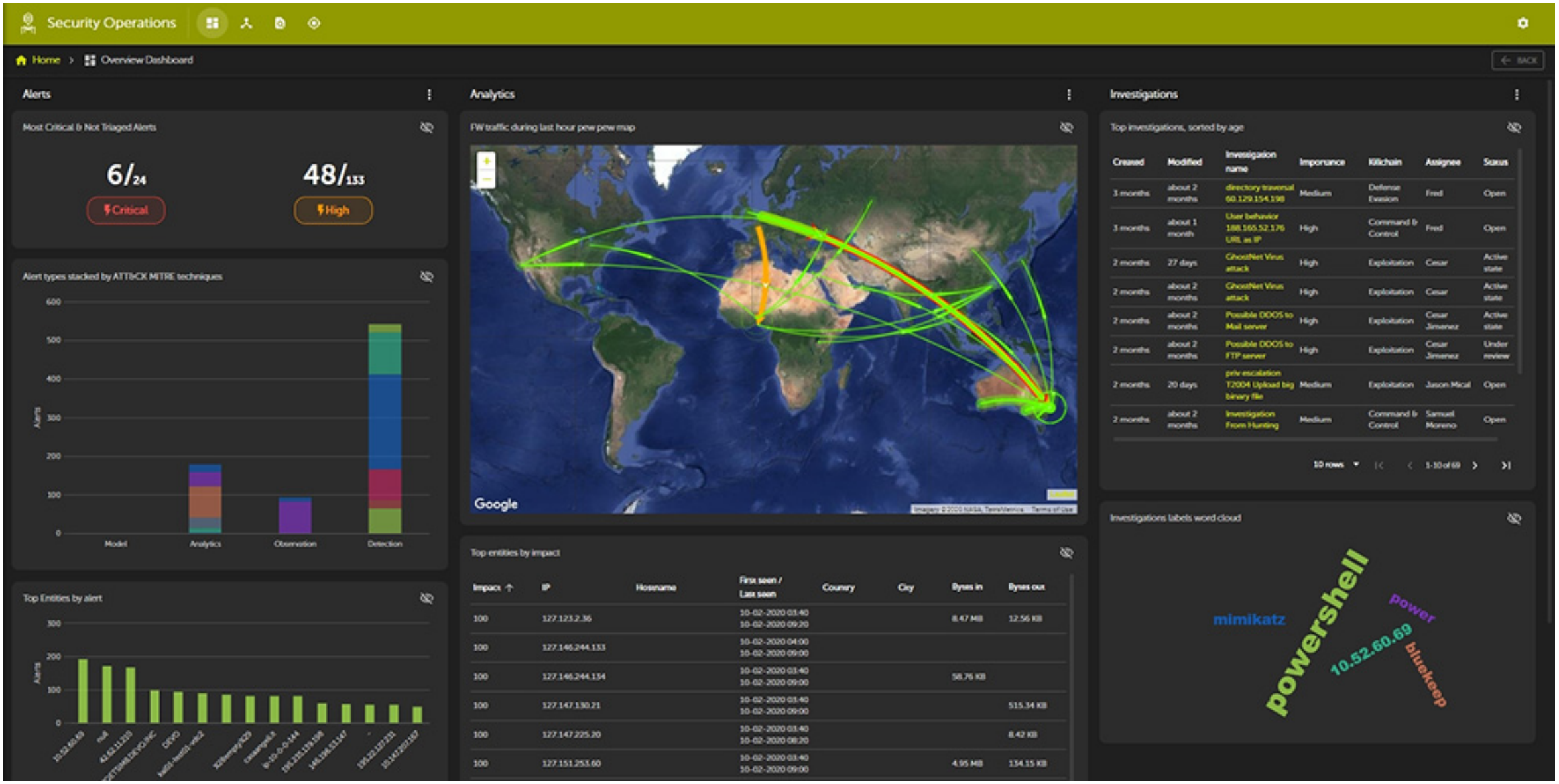
HYAS Insight



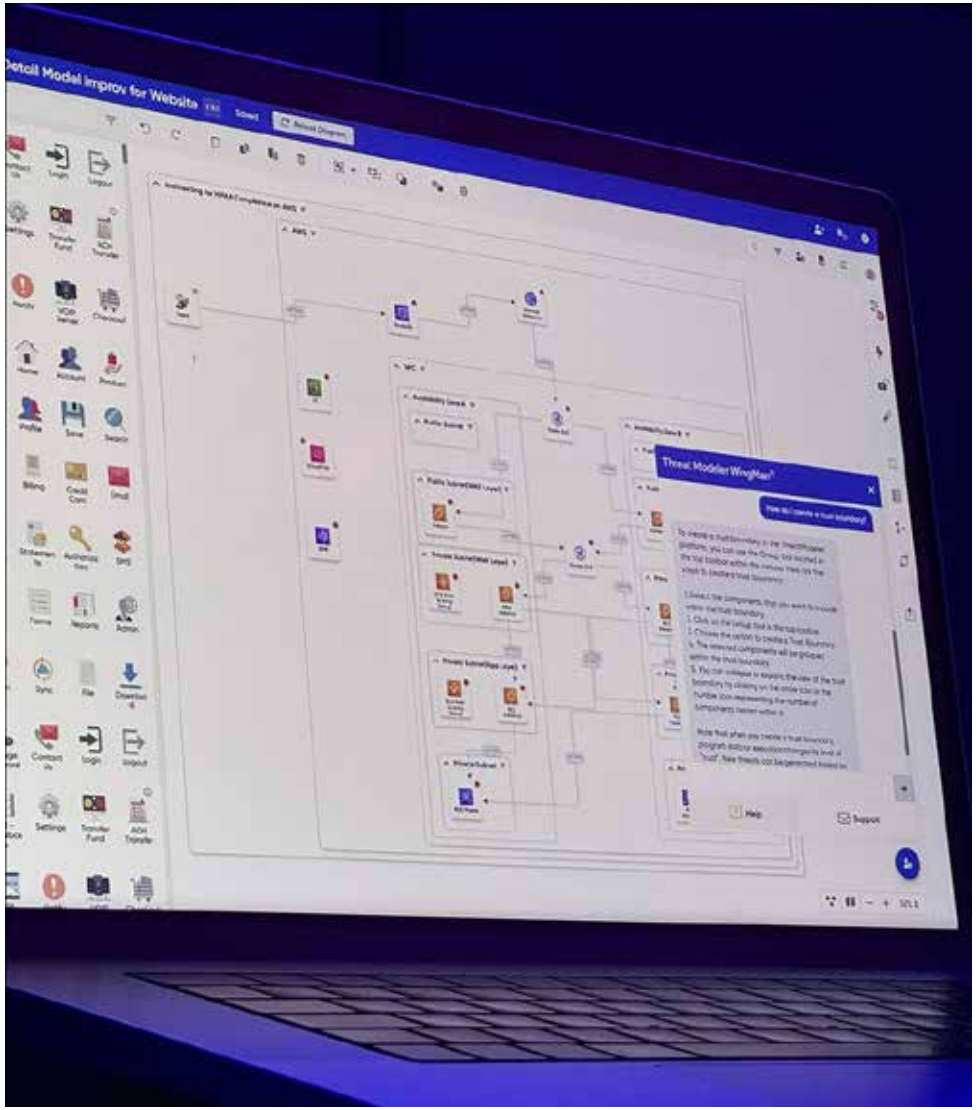
Devo Security Operations

- **Devo Security Operations** является первым решением, сочетающим в себе критически важные возможности безопасности с автоматическим обогащением, анализом угроз, совместной работой с сообществом, центральным хранилищем доказательств и оптимизированным рабочим процессом аналитика. Решение делает анализ безопасности более эффективным и помогает преобразовать операционный центр безопасности (SOC).
- Devo Security Operations избавляет аналитиков от необходимости использовать несколько разных инструментов или мануальных процессов для сбора данных, необходимых для выявления и расследования наиболее важных угроз. Devo предоставляет эту информацию аналитикам на протяжении всего жизненного цикла угрозы.
- https://www.devo.com/resources/devo-security-operations/

Devo Security Operations



ThreatModeler



- **Решение ThreatModeler** - позволяет DevOps защищать свою ИТ-среду и приложения с помощью автоматического моделирования угроз при разработке мобильных приложений и приложений Интернета вещей.
- С помощью платформы **ThreatModeler** пользователи проектируют, создают систему безопасности и управляют ею от разработки до развертывания, а программное обеспечение ThreatModeler мгновенно визуализирует поверхности атаки, устраняя недостатки в системе безопасности и сводя к минимуму распространение угроз в SDLC.
- https://info.threatmodeler.com/demo

Защита информации

Тема: Управление рисками информационной безопасности

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. Анализ международных документов по управлению рисками информационной безопасности. Часть 1 (2020) https://habr.com/ru/post/495236/
4. ISO 9001:2015 «Системы менеджмента качества. Требования» https://ksph.edu.kz/files/1368/mezhdunarodnyi_standart_ISO_9001_2015_rus.pdf
5. Управление рисками информационной безопасности https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/3%20июня.pdf
6. Управление ИТ-рисками. Общие подходы к управлению рисками. Часть 1 https://upr.ru/article/upravlenie-it-riskami-obschie-podhodi/
7. NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View (Управление риском информационной безопасности: Уровень организации, миссии, информационной системы) https://csrc.nist.gov/publications/detail/sp/800-39/final https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
8. NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy» («Фреймворк управления рисками для информационных систем и организаций: жизненный цикл систем для обеспечения безопасности и конфиденциальности»). https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Список использованных источников

9. NIST SP 800-30 «Guide for Conducting Risk Assessments» (Руководство по проведению оценок риска)
   https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
10. NIST SP 800-137 «Information Security Continuous Monitoring for Federal information Systems and Organizations» (Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций).
    https://csrc.nist.gov/publications/detail/sp/800-137/final
    https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
11. Анализ международных документов по управлению рисками информационной безопасности. Часть 2
    https://habr.com/ru/post/495986/
12. Стандарт ISO/IEC 27005:2018 «Information technology — Security techniques — Information security risk management» («Информационная технология. Методы и средства обеспечения
    https://www.iso.org/ru/standard/75281.html
13. Стандарт ISO/IEC 27102:2019 «Information security management — Guidelines for cyber-insurance» («Управление информационной безопасностью. Руководство по киберстрахованию»)
    https://www.iso.org/ru/standard/72436.html
14. ISO/IEC 31000:2018 Risk management — Guidelines
    https://www.iso.org/ru/standard/65694.html
15. ISO/IEC 30100-1:2016 Information technology — Home network resource management — Part 1: Requirements
    https://www.iso.org/ru/contents/data/standard/06/99/69908.html

Список использованных источников

16. ISO/IEC 30100-2:2016 Information technology — Home network resource management — Part 2: Architecture
https://www.iso.org/ru/contents/data/standard/06/80/68093.html
17. ISO/IEC 30100-3:2016 Information technology — Home network resource management — Part 3: Management application
https://www.iso.org/ru/contents/data/standard/05/67/56727.html
18. Применение стандарта ISO 31000
https://www.securityvision.ru/blog/primenenie-standarta-iso-31000/
19. IEC 31010:2019 Risk management — Risk assessment techniques
https://www.iso.org/ru/standard/72140.html
20. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска (Risk management. Risk assessment technologies).
https://docs.cntd.ru/document/1200170253
https://upravlenie-riskami.ru/files/free/gost-r-58771-2019-menedgement-riska-tehnologii-otsenki-riska.pdf
21. VMware Carbon Black Cloud Container
https://www.carbonblack.com/products/vmware-carbon-black-cloud-container/
22. VMware Carbon Black Cloud Container
https://www.securitylab.ru/software/518703.php
23. Enterprise Security Program Review
https://www.ironnet.com/services/enterprise-security-program-review
24. Enterprise Security Program Review
https://www.securitylab.ru/software/516109.php

Список использованных источников

25. Varonis
    https://www.varonis.com/ru/data-security-insider-threat-compliance-software/
    https://info.varonis.com/demo/ru
    https://www.securitylab.ru/software/515907.php
26. Cloud Advisor
    https://www.cloudadvisor.ru
    https://www.securitylab.ru/software/514518.php
27. Confluera
    https://www.confluera.com
28. Confluera CxDR Platform
    https://www.confluera.com/product-cxdr-platform
29. Confluera XDR
    https://www.securitylab.ru/software/513574.php
30. Deepwatch Lens Score
    https://www.deepwatch.com/resource/deepwatch-lens-score/
    https://www.youtube.com/watch?v=4DLImYKOM4k
    https://www.securitylab.ru/software/513312.php
31. SnapAttack
    https://www.boozallen.com/s/product/monitoring-threat-detection-mitigation-and-training.html
    https://www.boozallen.com/s/product/snapattack.html
    https://www.securitylab.ru/software/513161.php

Список использованных источников

32. Cyborg Security HUNTER
https://www.cyborgsecurity.com/blog/meet-cyborg-security-and-the-hunter-threat-hunting-platform/
https://www.securitylab.ru/software/513121.php

33. Radiflow CIARA
https://radiflow.com
https://radiflow.com/products/ciara-cyber-industrial-automated-risk-assessment/
https://www.youtube.com/watch?v=2CsGVcoZSP4

34. BitSight for Third-Party Risk Management
https://www.bitsight.com/third-party-risk-management#:~:text=BitSight%20for%20Third-Party%20Risk%20Management%20immediately%20exposes%20cyber%20risk,and%20measurable%20cyber%20risk%20reduction.
https://www.securitylab.ru/software/509015.php

35. Obsidian Security
https://www.obsidiansecurity.com
https://www.securitylab.ru/software/508096.php

36. Datadog Security Monitoring
https://www.datadoghq.com
https://docs.datadoghq.com/security_platform/
https://www.securitylab.ru/software/508044.php

37. Guardicore Infection Monkey – FREE
https://www.guardicore.com/infectionmonkey/
https://www.securitylab.ru/software/508042.php

Список использованных источников

38. SentinelOne Singularity Platform
    https://www.sentinelone.com
    https://www.securitylab.ru/software/506808.php

39. HYAS Insight
    https://www.hyas.com/hyas-insight
    https://www.securitylab.ru/software/506050.php

40. Devo Security Operations
    https://www.devo.com/resources/devo-security-operations/
    https://www.securitylab.ru/software/505133.php

41. Программное обеспечение для анализа рисков
    https://www.securitylab.ru/software/1297/

42. Применение риск-ориентированного подхода в DIS ISO 9001:2015 Специалист по СМК – Соколовская М.В. Использованы материалы Левшиной В.В., Левшина Л.М. – презентация
    http://www.myshared.ru/slide/985865/

43. Анализ международных документов по управлению рисками информационной безопасности. Часть 2
    https://habr.com/ru/post/495986/

44. Цикл Деминга, или PDCA: улучшение процессов разработки и управление качеством продукта
    https://skillbox.ru/media/management/tsikl_deminga/

45. Риски. Управление рисками
    https://ppt-online.org/183848

Список использованных источников

46. СТБ 34.101.70-2016. Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах. – Введ. 01.04.2017. - Минск : Госстандарт : БелГИСС, 2016. – 35 с.
47. Управление рисками организаций. Предотвращение утечек информации Как измерить риск? https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/ru_predotvrashenir_utechek_informacii_rus.pdf
48. Оценка киберрисков на основе анализа данных в открытых источниках https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/ocenka-kiberriskov-na-osnove-analiza-dannyh-v-otkrytyh-istochnikah.pdf
49. Интегрированный подход к управлению киберрисками https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/energy-resources/Russian/intergrated-approach-combat-cyber-risk-oil-gas-ru.pdf
50. Риск ИБ. Лекция 1 https://ppt-online.org/1387407
51. Управление информационной безопасностью. Тема 3. Концептуальные подходы к управлению рисками информационной безопасности – Толстой А.И., НИЯУ МИФИ, 2016 https://ppt-online.org/292147
52. Лекция 6. Нормативная база по управлению рисками информационной безопасности https://ppt-online.org/1153304
53. Управление рисками в рамках функционирования интегрированных систем менеджмента / Карманов В.В. - ИТМ ПНИПУ https://ppt-online.org/314865

Список использованных источников

54. BS 7799
    https://en.wikipedia.org/wiki/BS_7799
55. ISO/IEC 17799
    https://ru.wikipedia.org/wiki/ISO/IEC_17799
56. ISO / IEC 27002
    https://en.wikipedia.org/wiki/ISO/IEC_27002