Лекция 15: Управление рисками информационной безопасности

Тема: Управление рисками, политики и соответствие

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Добро пожаловать на лекцию 15. Сегодня мы рассмотрим управление рисками информационной безопасности — систематический процесс идентификации, оценки и обработки рисков безопасности. Это одна из важнейших тем нашего курса, поскольку управление рисками определяет все решения в области безопасности. Каждая мера защиты, которую мы внедряем, каждая политика, которую мы разрабатываем, каждый инструмент, который мы развёртываем, должны быть обоснованы рисками, которые они устраняют.

Позвольте начать с фундаментальной истины: мы не можем устранить все риски. Ресурсы безопасности конечны, угрозы неограниченны, а абсолютная безопасность сделала бы системы неработоспособными. Наша цель — не устранить риск, а управлять им, то есть снизить риск до приемлемого уровня, позволяя организации достигать своих целей.

Управление рисками отвечает на ключевые вопросы: Что может пойти не так? Насколько это вероятно? Насколько серьёзными будут последствия? Что мы должны предпринять? Соразмерен ли наш ответ риску?

Организации с развитой практикой управления рисками принимают более качественные решения в области безопасности. Они инвестируют туда, где это наиболее важно. Они избегают как недостаточной, так и чрезмерной защиты. Они могут обосновать свои программы безопасности перед руководством и регуляторами.

В течение следующих двух часов мы рассмотрим жизненный цикл управления рисками, методологии оценки, анализ активов и угроз, расчёт рисков, варианты обработки рисков, а также фреймворки, включая ISO 27005. Мы также обсудим растущие проблемы рисков третьих сторон и роль киберстрахования.

Часть 1: Жизненный цикл управления рисками

Понимание риска

Прежде чем перейти к процессу, давайте точно определим ключевые термины.

Риск — это потенциал потерь или ущерба при эксплуатации уязвимости угрозой. Риск имеет два измерения: вероятность и воздействие. Событие с высокой вероятностью и высоким воздействием представляет высокий риск. Событие с низкой вероятностью и низким воздействием представляет низкий риск.

Угроза — это всё, что может причинить ущерб: стихийное бедствие, злонамеренный субъект, случайное действие, системный сбой. Угрозы существуют вне зависимости от того, можем ли мы их контролировать.

Уязвимость — это слабость, которую может эксплуатировать угроза. Уязвимости существуют в технологиях, процессах и людях. Необновлённый сервер — это техническая уязвимость. Отсутствие проверок доступа — это процессная уязвимость. Необученный сотрудник — это человеческая уязвимость.

Актив — это нечто ценное, что мы хотим защитить. Активы включают данные, системы, людей, репутацию и физическую собственность.

Мера защиты — это средство обеспечения безопасности или контрмера, которая снижает риск путём предотвращения угроз, уменьшения уязвимостей или ограничения воздействия.

Фазы жизненного цикла

Управление рисками — это не разовое мероприятие, а непрерывный цикл. Жизненный цикл состоит из нескольких фаз:

Фаза 1: Определение контекста устанавливает область и критерии управления рисками. Какие активы мы защищаем? Каков аппетит к риску организации? Какие нормативные и бизнес-требования применяются?

Фаза 2: Идентификация рисков систематически выявляет активы, угрозы, уязвимости и существующие меры защиты. Мы задаём вопросы: Что у нас есть? Что может этому угрожать? Какие слабости существуют?

Фаза 3: Анализ рисков определяет вероятность и воздействие выявленных рисков. Он может быть качественным (высокий/средний/низкий), количественным (числовым) или полуколичественным (объединяющим оба подхода).

Фаза 4: Оценка рисков сопоставляет проанализированные риски с критериями для определения того, какие из них требуют обработки. Не все риски требуют действий — некоторые являются приемлемыми.

Фаза 5: Обработка риска выбирает и внедряет меры защиты для модификации риска. Варианты включают избежание, смягчение, передачу или принятие риска.

Фаза 6: Мониторинг и пересмотр отслеживает изменения в ландшафте рисков, проверяет эффективность мер защиты и инициирует повторную оценку при необходимости.

Коммуникация и консультирование осуществляются на протяжении всех фаз. Заинтересованные стороны должны понимать риски и участвовать в принятии решений.

Интеграция с бизнес-процессами

Управление рисками не должно существовать изолированно. Оно интегрируется со стратегическим планированием, управлением проектами, управлением изменениями и повседневными операциями.

Управление рисками информационной безопасности является подмножеством корпоративного управления рисками. Организации сталкиваются с финансовыми рисками, операционными рисками, стратегическими рисками и рисками соответствия наряду с рисками безопасности. Зрелые организации управляют всеми рисками через интегрированные фреймворки.

На уровне совета директоров риски безопасности всё чаще становятся предметом обсуждения. Нормативные требования 2025 и 2026 годов, включая правила SEC (Securities and Exchange Commission, Комиссия по ценным бумагам и биржам) в Соединённых Штатах и DORA (Digital Operational Resilience Act, Закон о цифровой операционной устойчивости) в Европе, требуют от советов директоров осуществлять надзор за рисками кибербезопасности. Руководители служб безопасности должны коммуницировать риски в бизнес-терминах, а не техническим жаргоном.

Часть 2: Методологии оценки рисков

Качественная оценка рисков

Качественная оценка использует описательные категории вместо числовых значений. Риски оцениваются как высокие, средние или низкие на основе экспертного суждения, а не расчётов.

Типичный качественный подход использует матрицу рисков. Одна ось представляет вероятность: редко, маловероятно, возможно, вероятно, почти наверняка. Другая ось представляет воздействие: незначительное, малое, умеренное, значительное, катастрофическое. Пересечение определяет уровень риска.

Преимущества качественной оценки включают простоту и быстроту. Она не требует точных данных о частотах или стоимости. Она доступна для нетехнических заинтересованных сторон.

Недостатки включают субъективность и неточность. Два эксперта могут оценить один и тот же риск по-разному. Сравнение рисков по категориям затруднено. Обосновать конкретные инвестиции сложно, когда риски описаны лишь как "высокие" или "средние".

Количественная оценка рисков

Количественная оценка присваивает числовые значения компонентам риска. Риск рассчитывается как:

Ожидаемые среднегодовые потери (ALE, Annualized Loss Expectancy) = Единовременные ожидаемые потери (SLE, Single Loss Expectancy) x Среднегодовая частота возникновения (ARO, Annualized Rate of Occurrence)

Единовременные ожидаемые потери (SLE) — это стоимость единичного инцидента. Среднегодовая частота возникновения (ARO) — это сколько раз в год мы ожидаем наступления инцидента. Ожидаемые среднегодовые потери (ALE) — это ожидаемые затраты за год.

Например: утечка данных может стоить 5 миллионов долларов (SLE). На основе отраслевых данных и наших мер защиты мы оцениваем вероятность наступления в 10% в год (ARO = 0,1). ALE = 5 000 000 x 0,1 = 500 000 долларов в год.

Это позволяет напрямую сравнивать с затратами на меры защиты. Если мера защиты стоит 200 000 долларов в год и снижает ALE с 500 000 до 100 000 долларов, мера обеспечивает чистую выгоду в 200 000 долларов (снижение на 400 000 минус 200 000 затрат).

Преимущества количественной оценки включают точность и сопоставимость. Она поддерживает финансовое принятие решений и расчёт рентабельности инвестиций.

Недостатки включают требования к данным и ложную точность. Точные значения SLE и ARO требуют исторических данных, которые могут отсутствовать. Рассчитанные значения выглядят более определёнными, чем они есть на самом деле. Отчёт IBM о стоимости утечки данных за 2024 год предоставляет полезные ориентиры: средняя стоимость утечки составила 4,88 миллиона долларов, однако отдельные инциденты варьировались весьма значительно.

Полуколичественные и гибридные подходы

Большинство организаций используют гибридные подходы. Они применяют качественные методы для первоначального отбора и используют количественный

анализ для приоритетных рисков, где имеются данные и инвестиционные решения требуют обоснования.

FAIR (Factor Analysis of Information Risk — факторный анализ информационного риска) — это популярный полуколичественный фреймворк. FAIR декомпозирует риск на частоту событий потерь и величину потерь, а затем далее декомпозирует каждый фактор. Он выдаёт вероятностные диапазоны, а не точечные оценки, признавая неопределённость.

Институт FAIR, основанный в 2016 году, значительно вырос. Крупные организации, включая многие компании из списка Fortune 500, используют FAIR для количественной оценки рисков. FAIR в настоящее время является международным стандартом (Open FAIR).

Часть 3: Идентификация и классификация активов

Почему активы важны

Невозможно защитить то, о существовании чего вы не знаете. Идентификация активов создаёт основу для управления рисками, определяя, что требует защиты.

Многие организации обнаруживают в ходе оценок, что у них есть неизвестные активы — теневые ИТ-системы, развёрнутые бизнес-подразделениями, забытые серверы, работающие в подсобных помещениях, данные, хранящиеся в несанкционированных местах. Каждый неизвестный актив — это неизвестный риск.

Категории активов

Информационные активы включают данные во всех формах: записи клиентов, интеллектуальную собственность, финансовые данные, операционные данные, информацию о сотрудниках. Данные часто являются наиболее ценным и наиболее атакуемым типом активов.

Технологические активы включают оборудование, программное обеспечение и сети: серверы, рабочие станции, мобильные устройства, приложения, базы данных, сетевое оборудование. Технологические активы обрабатывают и хранят информационные активы.

Физические активы включают помещения, оборудование и системы физической безопасности: центры обработки данных, офисы, системы контроля доступа, оборудование видеонаблюдения.

Человеческие активы — это люди, которые эксплуатируют системы и принимают решения: сотрудники, подрядчики, партнёры с доступом к системам. Люди являются одновременно и активами для защиты, и потенциальными уязвимостями.

Нематериальные активы включают репутацию, бренд, доверие клиентов и нормативный статус. Они могут быть повреждены инцидентами безопасности, даже если данные не были потеряны.

Инвентаризация активов

Ведение точной инвентаризации активов является сложной, но необходимой задачей. Ручные инвентаризации быстро устаревают. Автоматизированные средства обнаружения помогают, но имеют ограничения.

Для технологических активов используйте автоматизированное сканирование обнаружения для выявления устройств и систем. Базы данных управления конфигурациями (CMDB, Configuration Management Database) должны отслеживать взаимосвязи и принадлежность активов. Облачные среды требуют специализированных инструментов, поскольку активы могут создаваться и уничтожаться быстро.

Для информационных активов инструменты классификации данных и системы предотвращения утечки данных (DLP, Data Loss Prevention) помогают определить, где находятся конфиденциальные данные. Упражнения по картированию данных отслеживают потоки данных через системы.

Для всех активов назначьте владельца. Каждый актив должен иметь назначенного владельца, ответственного за его защиту. Принадлежность обеспечивает подотчётность при принятии решений о рисках.

Классификация активов

Классификация присваивает уровни конфиденциальности или критичности активам. Распространённые схемы классификации включают:

Классификация по конфиденциальности: Открытые, Внутренние, Конфиденциальные, Ограниченного доступа. Она определяет меры контроля доступа и процедуры обращения.

Классификация по критичности: Низкая, Средняя, Высокая, Критическая. Она определяет требования к доступности и приоритеты восстановления.

Нормативная классификация идентифицирует данные, подлежащие конкретным регуляторным требованиям: персональные данные по GDPR, данные платёжных карт по PCI DSS, медицинская информация по HIPAA.

Классификация должна быть практичной. Слишком много категорий создают путаницу. Классификация должна быть проверяемой и применимой. Маркируйте

данные и системы метками классификации. Автоматизируйте применение, где это возможно.

Часть 4: Моделирование угроз

Цель моделирования угроз

Моделирование угроз систематически выявляет, каким образом злоумышленники могут скомпрометировать системы. Оно меняет мышление от "что может пойти не так?" к "как бы атакующий подошёл к этому?"

Моделирование угроз ценно на этапе проектирования, до создания систем. Оно также ценно для существующих систем для выявления упущенных рисков. Оно создаёт общее понимание между командами безопасности, разработчиками и операционными подразделениями.

Модель угроз STRIDE

STRIDE — это модель категоризации угроз, разработанная в Microsoft. Аббревиатура представляет шесть категорий угроз:

Spoofing (подмена) предполагает выдачу себя за кого-то или что-то другое. Злоумышленник подделывает идентификацию пользователя для получения несанкционированного доступа. Злоумышленник подделывает сервер для проведения атаки типа "человек посередине".

Tampering (фальсификация) предполагает изменение данных или кода без авторизации. Злоумышленник фальсифицирует записи в базе данных. Злоумышленник модифицирует исполняемый код для внедрения вредоносного ПО.

Repudiation (отказ от ответственности) предполагает отрицание выполнения действия. Пользователь отрицает совершение транзакции. Злоумышленник удаляет журналы, чтобы скрыть свою деятельность.

Information Disclosure (раскрытие информации) предполагает предоставление информации неуполномоченным сторонам. Конфиденциальные данные раскрываются через ненадлежащие меры контроля доступа. Данные утекают через побочные каналы или сообщения об ошибках.

Denial of Service (отказ в обслуживании) предполагает недоступность систем. Злоумышленники потребляют ресурсы для предотвращения легитимного использования. Системы выводятся из строя вредоносными входными данными.

Elevation of Privilege (повышение привилегий) предполагает получение возможностей, превышающих авторизованные. Злоумышленник повышает

привилегии от пользователя до администратора. Изолированный процесс выходит за пределы песочницы.

Для каждого компонента системы рассмотрите, какие категории STRIDE применимы. Для каждой применимой категории определите конкретные сценарии атак. Для каждого сценария определите потенциальные меры защиты.

Моделирование угроз PASTA

PASTA (Process for Attack Simulation and Threat Analysis — процесс моделирования атак и анализа угроз) — это семиэтапная методология моделирования угроз, ориентированная на риски.

Этап 1: Определение целей устанавливает бизнес-цели и требования безопасности. Что мы защищаем и почему?

Этап 2: Определение технической области документирует техническую среду — архитектуру, технологии, потоки данных и границы доверия.

Этап 3: Декомпозиция приложения разбивает приложение на компоненты, идентифицируя точки входа, активы и уровни доверия.

Этап 4: Анализ угроз идентифицирует субъектов угроз, их возможности и мотивацию. Кто может атаковать и почему?

Этап 5: Анализ уязвимостей выявляет слабости, которые могут быть эксплуатированы угрозами, с использованием сканирования уязвимостей, анализа кода и анализа архитектуры.

Этап 6: Моделирование атак строит деревья атак, показывающие пути, которые могут использовать злоумышленники. Это моделирует перспективу атакующего.

Этап 7: Анализ рисков и воздействия оценивает бизнес-воздействие успешных атак и определяет приоритеты реагирования.

PASTA является более комплексным подходом, чем STRIDE, но требует больших усилий. Он особенно ценен для критических приложений, где тщательный анализ оправдан.

Интеграция аналитики угроз

Моделирование угроз выигрывает от аналитики угроз — информации о реальных угрозах, злоумышленниках и их методах.

Тактическая разведка описывает конкретные индикаторы компрометации: IP-адреса, хеши вредоносного ПО, шаблоны атак. Она поддерживает обнаружение и реагирование.

Операционная разведка описывает кампании и методы злоумышленников. Понимание способов действий злоумышленников помогает выявлять релевантные угрозы.

Стратегическая разведка описывает ландшафт угроз, новые тенденции и мотивацию злоумышленников. Она определяет приоритеты рисков и стратегию безопасности.

Источники включают коммерческих поставщиков аналитики угроз, отраслевые организации обмена информацией (ISAC, Information Sharing and Analysis Center), государственные органы (CISA, Cybersecurity and Infrastructure Security Agency — Агентство по кибербезопасности и защите инфраструктуры США; ENISA, European Union Agency for Cybersecurity — Агентство ЕС по кибербезопасности) и разведку из открытых источников (OSINT, Open Source Intelligence).

Фреймворк MITRE ATT&CK предоставляет базу знаний о тактиках и методах противника. Используйте ATT&CK для обеспечения того, чтобы модели угроз учитывали известные шаблоны атак.

Часть 5: Оценка уязвимостей и тестирование на проникновение

Оценка уязвимостей

Оценка уязвимостей выявляет слабости в системах, которые могут быть эксплуатированы угрозами. Она отвечает на вопрос: Где мы уязвимы?

Автоматизированное сканирование уязвимостей использует инструменты для выявления известных уязвимостей. Сетевые сканеры, такие как Nessus (от Tenable, разработчика решений управления уязвимостями), Qualys и OpenVAS, обнаруживают отсутствующие обновления, ошибки конфигурации и известные уязвимости в сетевых сервисах. Сканеры приложений выявляют уязвимости веб-приложений. Сканеры контейнеров и облачных сред охватывают современную инфраструктуру.

Ручная оценка уязвимостей дополняет автоматизацию. Некоторые уязвимости требуют анализа человеком для обнаружения — недостатки бизнес-логики, сложные цепочки атак, контекстно-зависимые слабости.

Оценка уязвимостей должна быть непрерывной. Новые уязвимости обнаруживаются ежедневно. По данным NIST National Vulnerability Database (NVD), в 2024 году было опубликовано более 30 000 CVE. Разовые оценки быстро устаревают.

Приоритизация уязвимостей

Не все уязвимости требуют немедленных действий. Приоритизация направляет усилия туда, где они наиболее важны.

Факторы для приоритизации включают:

Серьёзность: Насколько уязвимость легко эксплуатировать? Насколько серьёзным может быть потенциальное воздействие? CVSS (Common Vulnerability Scoring System — общая система оценки уязвимостей) предоставляет стандартизированные оценки серьёзности.

Экспозиция: Является ли уязвимая система доступной из интернета или внутренней? Могут ли злоумышленники до неё добраться?

Критичность актива: Насколько важна затронутая система? Критическая уязвимость в тестовой системе отличается от той же уязвимости в промышленной платёжной системе.

Доступность эксплойта: Является ли код эксплойта публично доступным? Активная эксплуатация в реальных условиях повышает срочность.

Компенсирующие меры: Снижают ли другие меры защиты эффективный риск? Уязвимая система за несколькими уровнями защиты отличается от системы, доступной напрямую.

SSVC (Stakeholder-Specific Vulnerability Categorization — категоризация уязвимостей для конкретных заинтересованных сторон) от CISA предоставляет деревья решений для приоритизации на основе статуса эксплуатации, технического воздействия и воздействия на миссию.

Тестирование на проникновение

Тестирование на проникновение выходит за рамки оценки уязвимостей и фактически эксплуатирует уязвимости. Тестировщики имитируют реальных злоумышленников, чтобы продемонстрировать, чего может достичь атакующий.

Внешнее тестирование на проникновение атакует организацию из интернета, как это сделал бы внешний злоумышленник.

Внутреннее тестирование на проникновение предполагает, что злоумышленник получил доступ к внутренней сети, проверяя, чего он мог бы достичь изнутри.

Тестирование на проникновение приложений фокусируется на конкретных приложениях, пытаясь скомпрометировать логику приложения, данные и нижележащие системы.

Тестирование методами социальной инженерии проверяет человеческие уязвимости через фишинг, телефонный претекстинг или попытки физического проникновения.

Учения красной команды представляют собой всесторонние имитации атак, проверяющие обнаружение и реагирование, а также предотвращение. Красные команды действуют скрытно, измеряя, сколько времени пройдёт до обнаружения защитниками.

Учения фиолетовой команды объединяют атакующих красной команды с защитниками синей команды, совместно работая над выявлением слабостей и улучшением обнаружения.

Требования и стандарты тестирования

Несколько стандартов регламентируют тестирование на проникновение:

PTES (Penetration Testing Execution Standard — стандарт выполнения тестирования на проникновение) предоставляет фреймворк для фаз тестирования от начала взаимодействия до отчётности.

Руководство по тестированию OWASP предоставляет комплексную методологию тестирования веб-приложений.

NIST SP 800-115 предоставляет техническое руководство по тестированию безопасности.

PCI DSS требует ежегодного тестирования на проникновение для торговых предприятий и поставщиков услуг, обрабатывающих платёжные карты.

Тестирование на проникновение должно выполняться квалифицированными тестировщиками, будь то внутренними или внешними. Отчёты должны приоритизировать выводы по бизнес-риску, а не только по технической серьёзности.

Часть 6: Расчёт рисков и варианты обработки

Расчёт рисков

Расчёт рисков объединяет оценки вероятности и воздействия для определения общих уровней риска.

В качественных подходах вероятность и категории воздействия объединяются с помощью матрицы рисков. Вероятное событие с значительным воздействием — это высокий риск. Маловероятное событие с малым воздействием — это низкий риск.

В количественных подходах рассчитывается ALE = SLE x ARO, как обсуждалось ранее. Более сложные подходы используют моделирование методом Монте-Карло для моделирования распределений рисков.

Оценки рисков обеспечивают возможность сравнения. Вы не можете устранить все риски одновременно, поэтому оценки помогают расставить приоритеты. Но помните, что оценки — это приближения, а не факты. Они должны информировать решения, а не подменять суждение.

Аппетит к риску и толерантность к риску

Аппетит к риску — это количество риска, которое организация готова принять в стремлении к своим целям. Стартап может принять высокий риск ради быстрого роста. Больница может принять очень малый риск в отношении безопасности пациентов.

Толерантность к риску определяет допустимые отклонения от целей. Система с целевым показателем доступности 99,9% может иметь толерантность к временным падениям до 99,5%, но не ниже 99%.

Эти концепции устанавливаются руководством, а не командами безопасности. Команды безопасности консультируют по рискам; руководство решает, какие риски приемлемы.

Варианты обработки

Когда риск превышает приемлемые уровни, существуют четыре варианта обработки:

Избежание риска полностью устраняет риск путём отказа от рискованной деятельности. Если система представляет неприемлемый риск, её можно вывести из эксплуатации. Если бизнес-функция представляет неприемлемый риск, от неё можно отказаться. Избежание уместно, когда затраты на смягчение превышают выгоды от деятельности.

Смягчение риска снижает вероятность или воздействие с помощью мер защиты. Технические меры, такие как межсетевые экраны и шифрование, снижают вероятность. Детективные меры, такие как мониторинг, обеспечивают быстрое реагирование. Меры восстановления, такие как резервное копирование, снижают воздействие.

Передача риска перекладывает риск на другую сторону. Киберстрахование передаёт финансовый риск инцидентов. Аутсорсинг передаёт операционный риск (хотя вы сохраняете подотчётность). Контракты могут передавать юридическую ответственность за определённые риски.

Принятие риска — это осознанное решение принять риск без дальнейшей обработки. Это уместно, когда риск находится в пределах аппетита, затраты на обработку превышают выгоду, или риск не может быть далее снижен. Принятие должно быть задокументировано и одобрено соответствующим руководителем.

Выбор мер защиты

При смягчении риска выбирайте меры защиты на основе:

Эффективность: Насколько мера снижает риск? Воздействует ли она на вероятность, воздействие или и то, и другое?

Стоимость: Каковы затраты на внедрение и эксплуатацию? Включите прямые затраты и операционное воздействие.

Осуществимость: Может ли мера быть внедрена и поддержана с учётом организационных ограничений?

Побочные эффекты: Создаёт ли мера новые риски или операционные затруднения?

Принципы эшелонированной защиты рекомендуют множественные перекрывающиеся меры. Если одна мера даёт сбой, другие обеспечивают защиту.

Часть 7: Фреймворк ISO 27005

Обзор ISO 27005

ISO 27005 — это международный стандарт по управлению рисками информационной безопасности. Являясь частью семейства ISO 27000, он предоставляет руководство по внедрению управления рисками в рамках системы менеджмента информационной безопасности (СМИБ), определённой ISO 27001.

Пересмотр ISO 27005, выпущенный в 2022 году, был приведён в соответствие с последней версией ISO 27001:2022 и учёл опыт внедрения. Он остаётся основополагающим руководством по управлению рисками в контексте информационной безопасности.

Процесс ISO 27005

Стандарт определяет процесс управления рисками со следующими действиями:

Определение контекста устанавливает область, границы и организацию управления рисками. Оно определяет критерии оценки рисков, критерии воздействия и критерии принятия рисков.

Идентификация рисков выявляет активы, угрозы, существующие меры защиты, уязвимости и потенциальные последствия. Стандарт предоставляет исчерпывающие перечни для рассмотрения.

Анализ рисков оценивает уровни рисков. ISO 27005 поддерживает как качественные, так и количественные подходы. Он подчёркивает необходимость учёта как вероятности, так и последствий.

Оценка рисков сопоставляет расчётный риск с критериями. Она определяет, какие риски требуют обработки, и расставляет приоритеты обработки.

Обработка риска выбирает варианты обработки и меры защиты. Стандарт ссылается на меры защиты из Приложения A ISO 27001 как на потенциальные средства обработки.

Принятие риска формально фиксирует принятие остаточных рисков. Решения о принятии должны быть задокументированы с авторизацией от соответствующих руководителей.

Коммуникация рисков обеспечивает поступление релевантной информации к лицам, принимающим решения, и заинтересованным сторонам на протяжении всего процесса.

Мониторинг и пересмотр рисков непрерывно отслеживает риски, меры защиты и сам процесс управления рисками.

Интеграция с ISO 27001

ISO 27001 требует от организаций определить процесс оценки рисков, проводить оценки рисков и внедрять обработку рисков. ISO 27005 предоставляет детальное руководство для выполнения этих требований.

Заявление о применимости, требуемое ISO 27001, непосредственно связано с обработкой рисков. Оно документирует, какие меры защиты внедрены, и обосновывает исключения на основе оценки рисков.

Организации, стремящиеся к сертификации ISO 27001, как правило, следуют ISO 27005 в части управления рисками, хотя стандарт не предписывает какой-либо конкретной методологии.

Практическое применение

При применении ISO 27005:

Адаптируйте процесс к вашей организации. Стандарт предоставляет принципы, а не жёсткие процедуры. Адаптируйте их к вашему размеру, отрасли и среде рисков.

Ведите документацию. ISO 27005 требует документирования решений, допущений и результатов. Это обеспечивает последовательность и поддерживает сертификацию.

Проводите регулярный пересмотр. Стандарт требует пересмотра рисков при существенных изменениях и через запланированные интервалы.

Используйте доступные ресурсы. Приложения ISO 27005 предоставляют примеры и руководства. Существуют отраслевые дополнения для таких секторов, как здравоохранение и финансы.

Часть 8: Управление рисками третьих сторон

Проблема третьих сторон

Современные организации зависят от множества третьих сторон: облачных провайдеров, поставщиков программного обеспечения, поставщиков услуг, бизнес-партнёров. Каждая третья сторона с доступом к вашим данным или системам расширяет вашу поверхность атаки.

Нарушения безопасности, связанные с третьими сторонами, распространены и дорогостоящи. Согласно отчёту Verizon Data Breach Investigations Report (DBIR) за 2024 год, значительный процент нарушений связан с третьими сторонами. Злоумышленники всё чаще нацеливаются на цепочку поставок, компрометируя одного поставщика для достижения множества клиентов.

Нормативные требования всё чаще касаются рисков третьих сторон. GDPR требует от контролёров обеспечить безопасность обработчиков. DORA требует от финансовых учреждений управлять рисками ИКТ-третьих сторон. Отраслевые стандарты, такие как PCI DSS, включают требования к третьим сторонам.

Компоненты программы управления рисками третьих сторон

Комплексная программа управления рисками третьих сторон включает:

Инвентаризация: Знайте всех третьих сторон с доступом к системам или данным. Теневые ИТ и несанкционированное использование SaaS создают неизвестные отношения с третьими сторонами.

Классификация: Классифицируйте третьих сторон по уровню риска на основе доступа к данным, доступа к системам и критичности. Не все третьи стороны требуют одинаковой тщательности проверки.

Оценка: Оценивайте безопасность третьих сторон до начала взаимодействия и периодически после этого. Методы включают анкетирование, анализ документации, оценки и непрерывный мониторинг.

Требования контрактов: Включите требования безопасности в контракты. Предусмотрите защиту данных, уведомление об инцидентах, права аудита и условия расторжения.

Непрерывный мониторинг: Риски третьих сторон меняются со временем. Отслеживайте инциденты безопасности, финансовые затруднения и существенные изменения.

Реагирование на инциденты: Планируйте действия при инцидентах с третьими сторонами. Как вы узнаете о нарушениях? Каковы ваши процедуры реагирования?

Методы оценки

Анкеты безопасности собирают информацию о мерах защиты третьих сторон. Стандартизированные анкеты, такие как SIG (Standardized Information Gathering) и CAIQ (Consensus Assessments Initiative Questionnaire, от Cloud Security Alliance — Альянса по облачной безопасности), позволяют проводить сравнение.

Анализ документации изучает сертификации третьих сторон (ISO 27001, SOC 2 — Service Organization Control), аудиторские отчёты и политики. Отчёты SOC 2 Type II особенно ценны, поскольку охватывают эффективность мер защиты за определённый период.

Техническая оценка может включать сканирование уязвимостей, тестирование на проникновение или анализ архитектуры безопасности для третьих сторон высокого уровня риска.

Оценки с выездом на место предусматривают физическое посещение помещений третьей стороны для отношений с наивысшим уровнем риска.

Сервисы непрерывного мониторинга обеспечивают постоянную видимость состояния безопасности третьих сторон, включая раскрытые учётные данные, уязвимости и индикаторы компрометации.

Нормативные требования к рискам третьих сторон

DORA (Digital Operational Resilience Act — Закон о цифровой операционной устойчивости) вступил в силу в январе 2025 года и налагает значительные требования на финансовые учреждения по управлению рисками ИКТ-третьих сторон, включая риск концентрации и стратегии выхода.

Директива NIS2 (Network and Information Security Directive 2, Директива о сетевой и информационной безопасности 2) требует управления безопасностью цепочки поставок для существенных и важных субъектов в множестве секторов.

Статья 28 GDPR требует от обработчиков данных предоставления достаточных гарантий и заключения соответствующих договоров.

Организации должны понимать, какие нормативные акты к ним применяются, и обеспечивать соответствие программ управления рисками третьих сторон предъявляемым требованиям.

Часть 9: Киберстрахование

Роль киберстрахования

Киберстрахование передаёт финансовый риск инцидентов безопасности страховщикам. При наступлении инцидентов страхование может покрыть расходы, включая:

Реагирование на инциденты: криминалистическое расследование, юридические консультации, кризисное управление.

Прерывание бизнеса: упущенные доходы во время простоев.

Затраты на утечку данных: уведомления, мониторинг кредитной истории, регуляторные штрафы (где они подлежат страхованию).

Выплаты выкупа: хотя всё чаще они ограничиваются или исключаются.

Ответственность перед третьими сторонами: претензии от пострадавших клиентов или партнёров.

Рынок киберстрахования 2025-2026

Рынок киберстрахования значительно развился. Премии стабилизировались после резкого роста в 2021-2023 годах, вызванного убытками от программ-вымогателей. Страховщики улучшили свои возможности по оценке рисков.

Ключевые тенденции рынка включают:

Ужесточение андеррайтинга: Страховщики требуют доказательств наличия конкретных мер защиты перед предоставлением покрытия. Многофакторная аутентификация, обнаружение и реагирование на конечных точках, практики резервного копирования и планы реагирования на инциденты обычно являются обязательными требованиями.

Ограничения покрытия программ-вымогателей: Многие полисы теперь исключают или устанавливают подлимиты на выплаты выкупа. Некоторые исключают выплаты, если жертвы не имели указанных мер защиты.

Покрытие возникающих рисков: Полисы всё чаще охватывают инциденты, специфичные для облака, социальную инженерию и атаки на цепочку поставок.

Регуляторные изменения: Некоторые юрисдикции рассматривают ограничения на возмещение выплат выкупа.

Выбор киберстрахования

При выборе киберстрахования:

Поймите свой профиль рисков. Какие инциденты наиболее вероятны? Сколько они будут стоить? Страхование должно покрывать значительные финансовые риски.

Тщательно изучите условия полиса. Лимиты покрытия, подлимиты, исключения и определения имеют огромное значение. "Утечка данных" может определяться узко или широко.

Убедитесь, что покрытие соответствует вашей среде. Традиционные полисы могут неадекватно покрывать инциденты в облаке или нарушения, связанные с третьими сторонами.

Рассмотрите покрытие регуляторных расходов. Штрафы по GDPR могут быть огромными; выясните, покрывает ли ваш полис регуляторные действия.

Ознакомьтесь с требованиями к реагированию на инциденты. Многие полисы требуют использования поставщиков, одобренных страховщиком. Изучите эти требования до наступления инцидентов.

Страхование как часть управления рисками

Страхование — это один из вариантов обработки риска, а не замена безопасности. Страховщики ожидают от страхователей поддержания разумного уровня безопасности. Претензии могут быть отклонены, если при андеррайтинге была допущена ложная информация или страхователи не поддерживали заявленные меры защиты.

Страхование не покрывает все расходы. Репутационный ущерб, долгосрочное бизнес-воздействие и нефинансовые последствия не подлежат страхованию.

Страхование должно дополнять, а не заменять инвестиции в безопасность. Используйте страхование для остаточного риска после внедрения соответствующих мер защиты.

Часть 10: Построение программы управления рисками

Элементы программы

Эффективная программа управления рисками включает:

Управление: Чёткие роли, обязанности и полномочия для принятия решений о рисках. Комитет по рискам или назначенный ответственный за управление рисками обеспечивает надзор.

Методология: Задокументированный подход к идентификации, оценке и обработке рисков. Последовательная методология обеспечивает возможность сравнения во времени.

Инструменты: Технологии, поддерживающие инвентаризацию активов, оценку рисков, отслеживание мер защиты и отчётность. Платформы GRC (Governance, Risk, and Compliance — управление, риск и соответствие) консолидируют эти функции.

Процессы: Регулярные циклы оценки, управление исключениями, процедуры эскалации и интеграция с управлением изменениями.

Отчётность: Регулярная отчётность руководству о состоянии рисков, тенденциях и ходе обработки. Панели мониторинга и метрики обеспечивают надзор.

Культура: Культура осведомлённости о рисках, при которой сотрудники понимают риски и свою роль в управлении ими.

Типичные трудности

Организации часто сталкиваются с трудностями в следующих областях:

Область охвата: Попытка оценить всё ведёт к поверхностным оценкам. Расставляйте приоритеты на основе критичности активов.

Качество данных: Оценки рисков хороши лишь настолько, насколько хороши их исходные данные. Инвестируйте в инвентаризацию активов и аналитику угроз.

Интеграция: Управление рисками, изолированное от бизнес-процессов, имеет ограниченное воздействие. Интегрируйте с управлением проектами, управлением изменениями и стратегическим планированием.

Вовлечение заинтересованных сторон: Управление рисками требует участия бизнес-подразделений, а не только ИТ. Выстраивайте отношения и делайте участие ценным.

Действие: Оценка без обработки ничего не даёт. Обеспечьте, чтобы оценка приводила к решениям и действиям.

Развитие зрелости

Зрелость управления рисками развивается со временем:

Начальный уровень: Ситуативное управление рисками, реактивные ответы.

Развивающийся уровень: Базовые процессы задокументированы, определённая последовательность.

Определённый уровень: Комплексная методология, регулярные оценки, интеграция с другими процессами.

Управляемый уровень: Количественное измерение рисков, улучшения на основе метрик.

Оптимизирующий уровень: Непрерывное совершенствование, предиктивные возможности, управление рисками встроено в культуру.

Большинство организаций работают на развивающемся или определённом уровне. Продвижение зрелости требует устойчивых инвестиций и поддержки со стороны руководства.

Заключение

Позвольте подвести итоги ключевых концепций сегодняшней лекции по управлению рисками информационной безопасности.

Мы начали с жизненного цикла управления рисками: определение контекста, идентификация, анализ, оценка, обработка и мониторинг. Управление рисками непрерывно, это не разовый проект.

Методологии оценки рисков варьируются от качественных (высокий/средний/низкий) до количественных (расчёты ALE) и гибридных подходов, таких как FAIR. Выбирайте методы, соответствующие вашим потребностям и доступным данным.

Идентификация и классификация активов создают основу для управления рисками. Невозможно защитить то, о существовании чего вы не знаете.

Моделирование угроз с использованием фреймворков STRIDE и PASTA систематически выявляет, каким образом злоумышленники могут скомпрометировать системы. Аналитика угроз обогащает моделирование реальными шаблонами атак.

Оценка уязвимостей выявляет слабости, тогда как тестирование на проникновение демонстрирует, чего фактически могут достичь злоумышленники. Приоритизируйте уязвимости на основе эксплуатируемости, экспозиции и критичности активов.

Расчёт рисков объединяет вероятность и воздействие. Варианты обработки включают избежание, смягчение, передачу и принятие. Выбирайте на основе аппетита к риску и анализа затрат и выгод.

ISO 27005 предоставляет международный фреймворк для управления рисками информационной безопасности, интегрируясь с ISO 27001 для внедрения СМИБ.

Управление рисками третьих сторон адресует расширенную поверхность атаки от поставщиков, партнёров и провайдеров услуг. DORA, NIS2 и другие нормативные акты всё чаще требуют наличия программ управления рисками третьих сторон.

Киберстрахование передаёт финансовый риск, но не заменяет безопасность. Рынок развился с ужесточением андеррайтинга и ограничениями на покрытие программ-вымогателей.

Для подготовки рассмотрите, как бы вы провели оценку рисков для знакомой вам организации. Определите ключевые активы, угрозы и уязвимости. Практикуйтесь в объяснении рисков бизнес-языком, а не техническим жаргоном.

На следующей лекции мы рассмотрим политики безопасности и соответствие — как организации кодифицируют требования безопасности и демонстрируют соответствие нормативным актам.

Вопросы для обсуждения

1. Как организации должны сообщать о рисках безопасности нетехническим заинтересованным сторонам и членам совета директоров?
2. Каковы ограничения методов количественной оценки рисков и когда качественная оценка более уместна?
3. Насколько эффективно киберстрахование как механизм передачи риска и каковы его ограничения?
4. Владелец малого бизнеса говорит: "Мы слишком малы, чтобы быть целью хакеров." Как бы вы ответили, используя концепции управления рисками?
5. Должны ли организации публично раскрывать все инциденты безопасности, даже незначительные? Каковы компромиссы между прозрачностью и репутацией?

Благодарю за внимание. Есть ли какие-либо вопросы?

Контрольные вопросы

1. Опишите жизненный цикл управления рисками и объясните, почему это непрерывный процесс.
2. Сравните качественные и количественные методологии оценки рисков. Каковы преимущества каждого подхода?
3. В чём разница между оценкой уязвимостей и тестированием на проникновение?
4. Перечислите четыре варианта обработки рисков и приведите пример сценария для каждого.
5. Каковы ключевые компоненты программы управления рисками третьих сторон?
6. Что такое реестр рисков и какую информацию он содержит?

Ключевые термины

- **ALE**: Ожидаемые среднегодовые потери (Annualized Loss Expectancy), ожидаемые денежные потери за год от риска
- **Классификация активов**: Категоризация активов по конфиденциальности и критичности для определения мер защиты
- **Дерево атак**: Иерархическая диаграмма, моделирующая различные пути, которыми злоумышленник может достичь цели
- **CVE**: Common Vulnerabilities and Exposures, каталог известных уязвимостей безопасности
- **Киберстрахование**: Страхование, покрывающее финансовые убытки от инцидентов кибербезопасности
- **FAIR**: Factor Analysis of Information Risk, фреймворк количественного анализа рисков
- **ISO 27005**: Международный стандарт по управлению рисками информационной безопасности
- **KPI**: Ключевой показатель эффективности (Key Performance Indicator), измеримая величина, показывающая, насколько эффективно достигаются цели безопасности
- **KRI**: Ключевой индикатор риска (Key Risk Indicator), метрика, используемая для раннего предупреждения о возрастающем воздействии рисков
- **PASTA**: Process for Attack Simulation and Threat Analysis, методология моделирования угроз
- **Тестирование на проникновение**: Санкционированные имитации атак для оценки безопасности системы
- **Принятие риска**: Признание риска и сознательное решение не предпринимать действий по его устранению
- **Аппетит к риску**: Уровень риска, который организация готова принять
- **Избежание риска**: Устранение деятельности или условий, создающих риск
- **Смягчение риска**: Внедрение мер защиты для снижения вероятности или воздействия риска
- **Толерантность к риску**: Конкретные границы допустимого отклонения риска от аппетита к риску организации
- **Передача риска**: Перенос риска на третью сторону через страхование или контракты
- **STRIDE**: Фреймворк моделирования угроз, классифицирующий угрозы по шести типам

- **Риск третьих сторон**: Риски безопасности, исходящие от поставщиков, партнёров и провайдеров услуг
- **Оценка уязвимостей**: Систематическая идентификация и оценка слабостей безопасности