Лекция 1: Основные понятия и терминология информационной безопасности

Тема: Основы информационной безопасности

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Здравствуйте. Добро пожаловать на нашу первую лекцию курса "Технологии информационной безопасности". В течение следующих трёх месяцев мы будем исследовать увлекательный и критически важный мир информационной безопасности. Сегодня мы начнём с фундаментальных понятий, на которых строится всё остальное.

Прежде чем перейти к конкретным технологиям, атакам или средствам защиты, нам необходимо установить общий понятийный аппарат. Информационная безопасность имеет свой собственный язык, и точное понимание терминов является обязательным. Одно неверно понятое понятие может привести к неправильно настроенной системе, а неправильно настроенная система может привести к нарушению безопасности, затрагивающему миллионы людей.

Позвольте начать с вопроса: кто из вас слышал об утечке данных в новостях в этом году? Полагаю, все подняли руку. Утечки данных стали настолько обычным явлением, что мы почти ожидаем их. По данным Cybersecurity Ventures, глобальный ущерб от киберпреступности, по прогнозам, достигнет 13 триллионов долларов к 2028 году. Эта сумма превышает ВВП (валовой внутренний продукт) большинства стран. Именно поэтому мы сегодня здесь.

Часть 1: Информационная безопасность и кибербезопасность

Начнём с уточнения двух терминов, которые часто используются как синонимы, но имеют различные значения: информационная безопасность и кибербезопасность.

Информационная безопасность, иногда называемая InfoSec, — это практика защиты информации от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. Обратите внимание, что это определение не указывает, каким образом хранится информация. Информационная безопасность охватывает бумажные документы в картотечном шкафу в той же мере, что и данные на облачном сервере. Если вы когда-нибудь видели табличку "Посторонним вход воспрещён" на двери — это информационная безопасность в действии.

Кибербезопасность — это подмножество информационной безопасности, которое конкретно занимается защитой электронных систем, сетей и данных от цифровых атак. Когда мы говорим о межсетевых экранах, системах обнаружения вторжений или вредоносном ПО, мы находимся в области кибербезопасности.

Вот практический способ понять разницу: если кто-то проникает в офис и крадёт распечатанные записи клиентов со стола, это инцидент информационной безопасности, но не инцидент кибербезопасности. Если кто-то удалённо взламывает базу данных и скачивает те же записи, это одновременно и инцидент информационной безопасности, и инцидент кибербезопасности.

На протяжении этого курса мы будем сосредоточены главным образом на кибербезопасности, но всегда помните, что она существует в более широком контексте информационной безопасности. Самый изощрённый межсетевой экран в мире не сможет вас защитить, если сотрудник оставит конфиденциальные документы в поезде.

Часть 2: Триада КЦД

Теперь мы подошли к наиболее фундаментальной модели в информационной безопасности: триаде КЦД. В нашем контексте КЦД означает **Конфиденциальность**, **Целостность** и **Доступность**. Эти три свойства составляют основу каждого решения в области безопасности, которое мы принимаем.

Позвольте нарисовать это на доске в виде треугольника. Каждая вершина представляет одно из этих свойств, и защищённая система должна поддерживать баланс всех трёх.

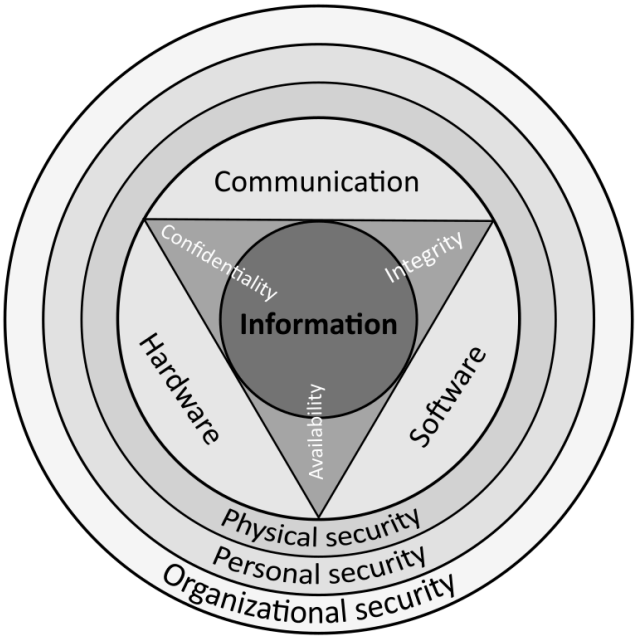


Рисунок 1: Модель информационной безопасности: триада КЦД (Конфиденциальность, Целостность, Доступность) с типами активов (Аппаратное обеспечение, Программное обеспечение, Коммуникации) и областями защиты (Физическая, Персональная, Организационная)

Конфиденциальность

Конфиденциальность означает обеспечение того, что информация доступна только тем, кто уполномочен на доступ к ней. Защищая конфиденциальность, мы предотвращаем несанкционированное раскрытие информации.

Подумайте о вашем банковском счёте. Только вы и уполномоченные сотрудники банка должны иметь возможность видеть баланс вашего счёта. Если бы случайный незнакомец мог просмотреть вашу финансовую информацию, это было бы нарушением конфиденциальности.

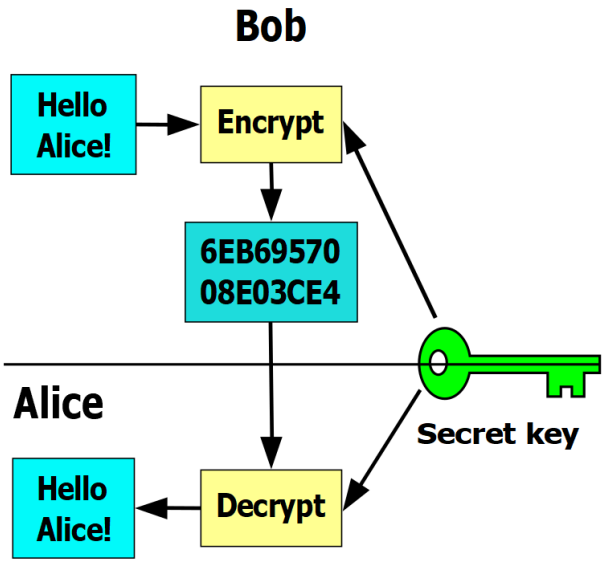
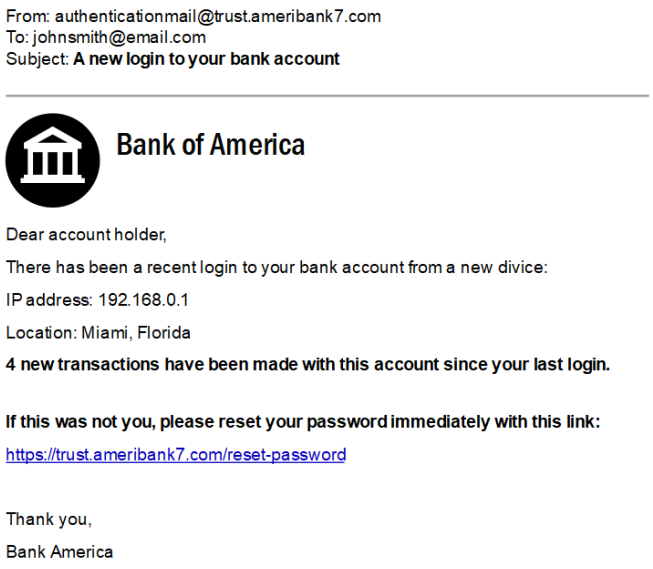


Рисунок 2: Симметричное шифрование (с секретным ключом): отправитель и получатель используют один и тот же ключ для защиты конфиденциальности сообщения

Конфиденциальности угрожают различные атаки:

- **Перехват данных**: кто-то перехватывает ваш сетевой трафик для чтения вашей электронной почты
- **Подглядывание через плечо**: кто-то наблюдает за тем, как вы вводите пароль
- **Социальная инженерия**: кто-то обманом заставляет вас раскрыть конфиденциальную информацию
- **Утечки данных**: злоумышленники похищают базы данных, содержащие персональную информацию


From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

Bank of America

Dear account holder,

There has been a recent login to your bank account from a new divice:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

Thank you,

Bank America

Рисунок 3: Пример фишингового письма как угроза конфиденциальности

Мы защищаем конфиденциальность с помощью:

- **Шифрование**: преобразование данных в нечитаемый формат без соответствующего ключа
- **Управление доступом**: обеспечение того, что только авторизованные пользователи могут получить доступ к определённым ресурсам
- **Аутентификация**: проверка личности пользователей перед предоставлением доступа
- **Физическая безопасность**: замки́, охрана и защищённые помещения

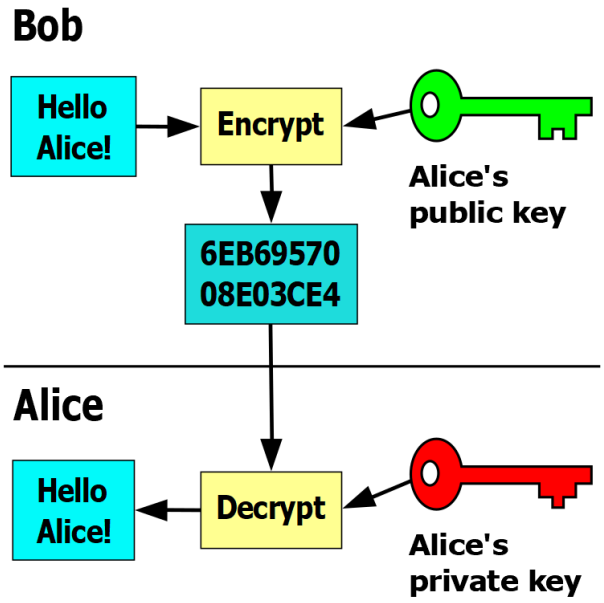


Рисунок 4: Асимметричное шифрование (с открытым ключом): зелёный открытый ключ шифрует, красный закрытый ключ расшифровывает, обеспечивая конфиденциальность без обмена секретом

Приведу реальный пример. В 2017 году утечка данных Equifax раскрыла персональную информацию 147 миллионов американцев. В 2023 году утечка 23andMe раскрыла чувствительные генетические данные почти 7 миллионов пользователей через подстановку учётных данных (credential stuffing). Урок здесь в том, что конфиденциальность требует постоянной бдительности как в отношении систем, так и в отношении доступа пользователей.

Целостность

Целостность означает обеспечение того, что информация остаётся точной, полной и неизменённой, за исключением изменений, внесённых уполномоченными сторонами. Защищая целостность, мы предотвращаем несанкционированную модификацию данных.

Рассмотрим систему медицинских записей. Если у пациента аллергия на пенициллин, эта информация должна оставаться точной в его медицинской карте. Если злоумышленник или программная ошибка изменят эту запись, последствия могут быть фатальными. Вот почему целостность так важна.

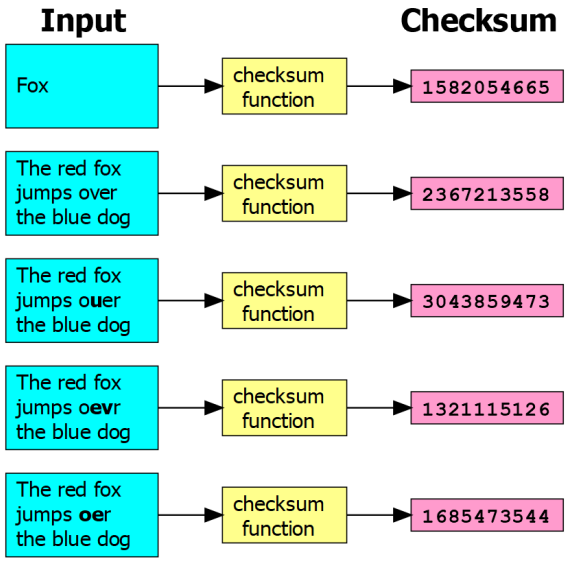


Рисунок 5: Обнаружение нарушения целостности с помощью контрольной суммы: любое изменение входных данных, даже один символ, даёт другую контрольную сумму

Целостности угрожают:

- **Атаки "человек посередине"**: злоумышленник перехватывает и модифицирует данные при передаче;
- **Вредоносное ПО**: вирусы или черви, которые повреждают или изменяют файлы;
- **Внутренние угрозы**: сотрудники, намеренно изменяющие записи;
- **Аппаратные сбои**: ошибки дисков, вызывающие повреждение данных;
- **Программные ошибки**: ошибки программирования, непреднамеренно изменяющие данные.

Мы защищаем целостность с помощью:

- **Хеширование**: создание цифрового отпечатка данных для обнаружения изменений;
- **Цифровые подписи**: криптографическая проверка источника и целостности данных;
- **Контроль версий**: отслеживание всех изменений для обнаружения несанкционированных модификаций;
- **Управление доступом**: ограничение круга лиц, которые могут изменять данные;
- **Контрольные суммы**: математическая проверка того, что данные не были изменены.

Вот пример, иллюстрирующий важность целостности. В 2010 году червь Stuxnet атаковал иранские ядерные объекты. Он не крал данные; вместо этого он

модифицировал инструкции, отправляемые центрифугам, заставляя их вращаться на неправильных скоростях, в то время как операторам отображались нормальные показания. Это была атака на целостность с физическими последствиями. Центрифуги разрушили сами себя, отбросив ядерную программу Ирана на годы назад.

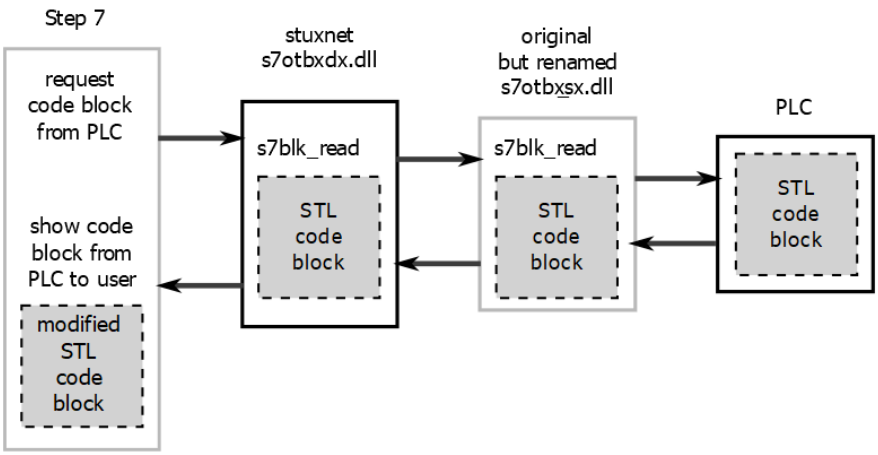


Рисунок 6: Атака Stuxnet: вредоносное ПО, перехватывающее связь с ПЛК

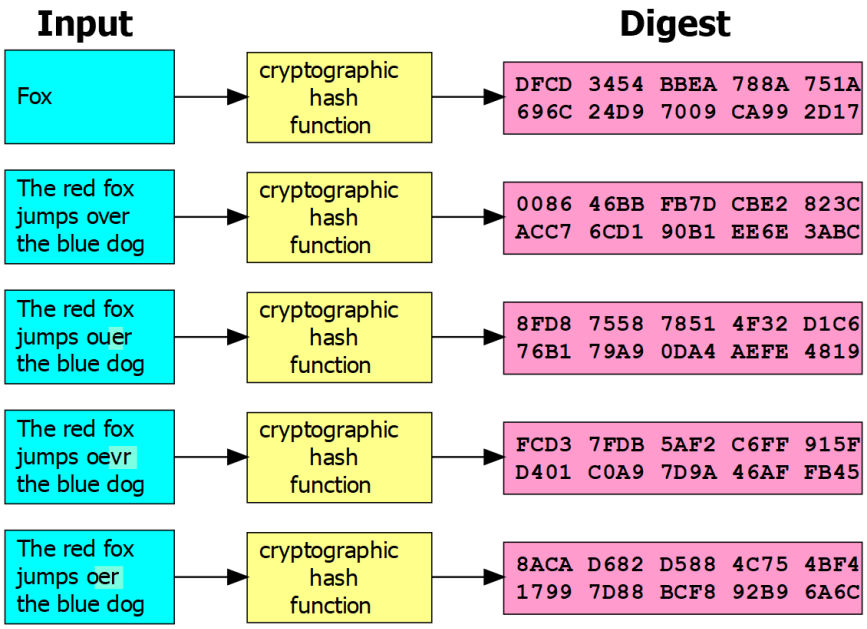


Рисунок 7: Криптографическая хеш-функция, порождающая дайджест фиксированной длины: любые входные данные любого размера дают непредсказуемый, уникальный дайджест

Доступность

Доступность означает обеспечение того, что информация и системы доступны авторизованным пользователям тогда, когда это необходимо. Защищая доступность, мы предотвращаем нарушение работы сервисов.

Представьте, что вам нужно снять деньги в банкомате, но системы банка не работают. Или представьте больницу, в которой врачи не могут получить доступ к записям пациентов во время экстренной ситуации. Доступность — это обеспечение работоспособности систем, когда они вам нужны.

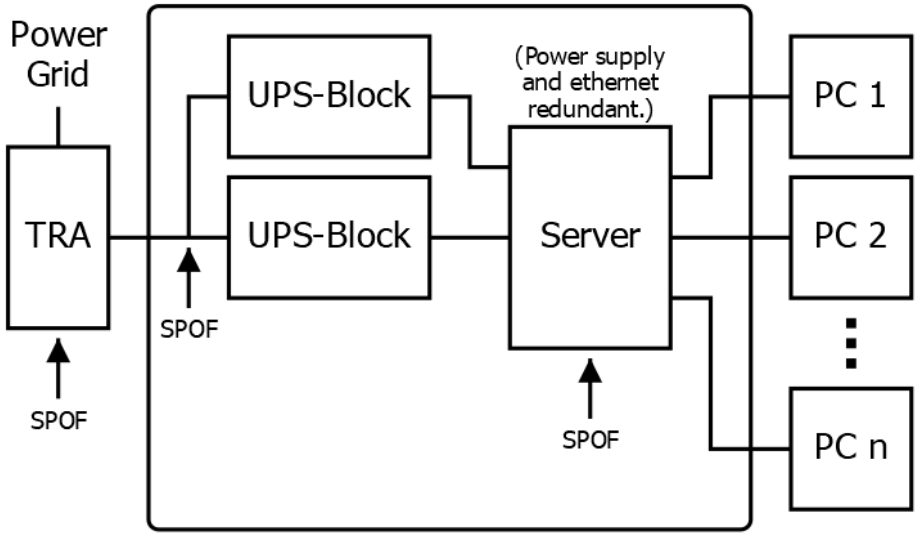


Рисунок 8: Единые точки отказа (SPOF) в системе: линия питания, трансформатор (TRA) и сервер являются точками SPOF, способными нарушить доступность, несмотря на резервирование UPS

Доступности угрожают:

- **Атаки типа "отказ в обслуживании" (DoS)**: перегрузка систем трафиком, делающая их недоступными;
- **Распределённые атаки типа "отказ в обслуживании" (DDoS - Distributed Denial of Sevice Attack)**: атаки DoS из множества источников одновременно;
- **Программы-вымогатели**: вредоносное ПО, шифрующее данные и делающее их недоступными до уплаты выкупа;
- **Аппаратные сбои**: отказы серверов, выход из строя дисков, сбои сети;
- **Стихийные бедствия**: наводнения, пожары, землетрясения, повреждающие инфраструктуру;
- **Перебои в электроснабжении**: отключения электричества, приводящие к остановке систем.

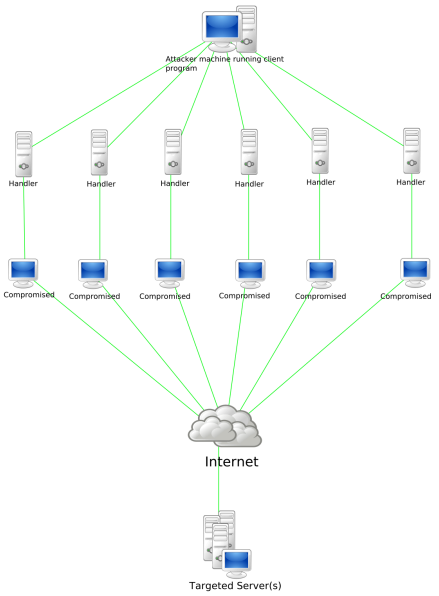


Рисунок 9: Архитектура DDoS-атаки (распределённая атака типа "отказ в обслуживании")

Мы защищаем доступность с помощью:

- **Резервирование**: наличие запасных систем, готовых взять на себя функции при отказе основных;
- **Резервное копирование**: регулярные копии данных, хранимые отдельно от оригинала;
- **Целевое время восстановления (RTO)** здесь критически важно то, что резервные копии бесполезны, если восстановление занимает недели (как это наблюдалось в недавних атаках программ-вымогателей, таких как MGM Resorts);
- **Планирование аварийного восстановления**: процедуры восстановления работы после серьёзного инцидента;
- **Балансировка нагрузки**: распределение трафика между несколькими серверами;
- **Защита от DDoS-атак**: системы, предназначенные для поглощения или отклонения массированных атак трафиком.

Приведу пример, связанный с доступностью. В 2016 году ботнет Mirai вывел из строя крупные интернет-сервисы через DDoS (Distributed Denial of Sevice Attack - распределённая атака типа "отказ в обслуживании"). Ещё более драматично то, что **сбой CrowdStrike (2024)** показал, как одно ошибочное обновление программного обеспечения может обрушить миллионы систем Windows по всему миру, заземлив авиарейсы и остановив работу больниц. Это продемонстрировало, что угрозы доступности могут исходить от доверенных поставщиков, а не только от злоумышленников.

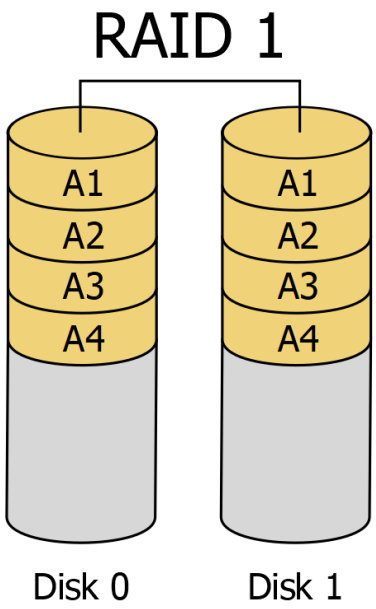


Рисунок 10: Зеркалирование дисков RAID 1: идентичные данные на двух дисках обеспечивают доступность системы при отказе одного диска

Балансировка триады

Вот что важно понять: эти три свойства часто вступают в противоречие друг с другом. Улучшение одного иногда может нанести ущерб другому.

Например, для максимизации конфиденциальности вы можете зашифровать все данные и потребовать несколько форм аутентификации. Но это может нанести ущерб доступности, поскольку авторизованным пользователям будет трудно быстро получить доступ к нужным данным.

Для максимизации доступности вы можете убрать все средства управления доступом и хранить данные на множестве серверов. Но это уничтожит конфиденциальность, потому что любой сможет получить доступ к чему угодно.

Специалисты по безопасности должны постоянно балансировать между этими конкурирующими требованиями, исходя из конкретного контекста и толерантности к риску своей организации. Универсально правильного ответа не существует.

Рисунок 11: Балансирование трёх свойств триады КЦД

Куб МакКамбера

Триада КЦД говорит нам, что защищать, но не где и не как. Куб МакКамбера, предложенный исследователем в области безопасности Джоном МакКамбером в 1991 году, расширяет модель КЦД до трёхмерной структуры.

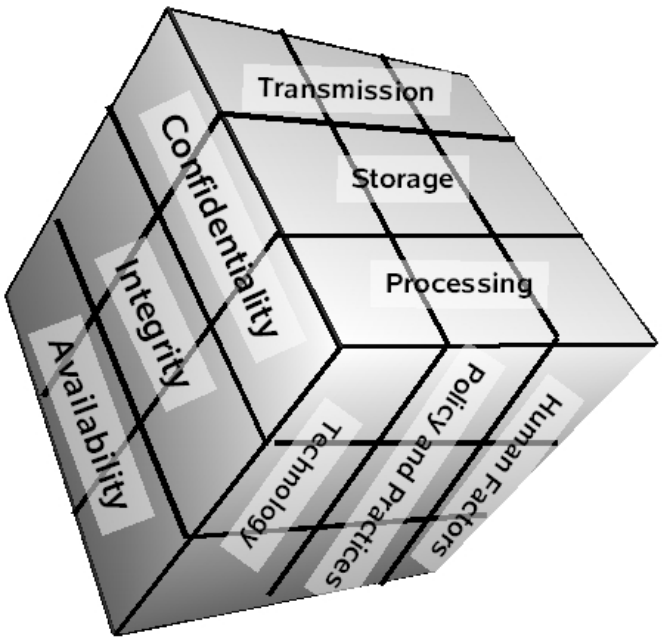


Рисунок 12: Куб Маккамбера: трёхмерная модель безопасности

Три измерения:

Измерение 1: Цели безопасности (КЦД)

Это три ключевых свойства, которые мы стремимся обеспечить: **Конфиденциальность** (защита информации от несанкционированного раскрытия), **Целостность** (гарантия точности и полноты данных) и **Доступность** (обеспечение своевременного доступа к информации авторизованными пользователями). Они представляют то, чего мы стремимся достичь.

Измерение 2: Состояния данных

- **Данные в состоянии покоя (хранение)**: информация, хранящаяся на носителях, таких как жёсткие диски, базы данных или резервные ленты. Угрозы: кража носителей информации, несанкционированный доступ к базам данных, шифрование программами-вымогателями. Защита: шифрование данных в состоянии покоя и управление доступом.
- **Данные в процессе передачи (передача)**: информация, передаваемая по сетям между системами. Угрозы: перехват данных, атаки "человек посередине", анализ сетевых пакетов. Защита: шифрование данных при передаче (TLS (Transport Layer Security), VPN (Virtual Private Network, виртуальная частная сеть), SSH (Secure Shell)).
- **Данные в процессе обработки (использование)**: информация, создаваемая, изменяемая или используемая в процессоре и памяти. Угрозы: переполнение буфера, вредоносное ПО для считывания памяти, несанкционированный доступ к работающим процессам. Защита: практики безопасного программирования, защита памяти, конфиденциальные вычисления (аппаратные доверенные среды выполнения).

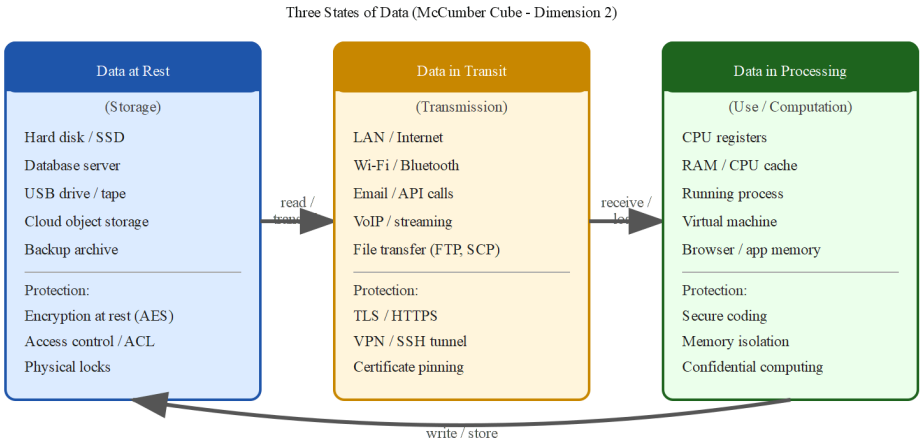


Рисунок 13: Три состояния данных: в покое (хранение), в передаче (передача) и в обработке (использование)

Измерение 3: Категории контрмер

Меры защиты подразделяются на три широкие категории: **Технологии** (аппаратные и программные средства: межсетевые экраны, шифрование, антивирусные программы), **Политики и практики** (правила, процедуры и регламенты, регулирующие работу с информацией) и **Обучение, Подготовка, Осведомлённость** (программы, помогающие людям понять риски безопасности и свои обязанности).

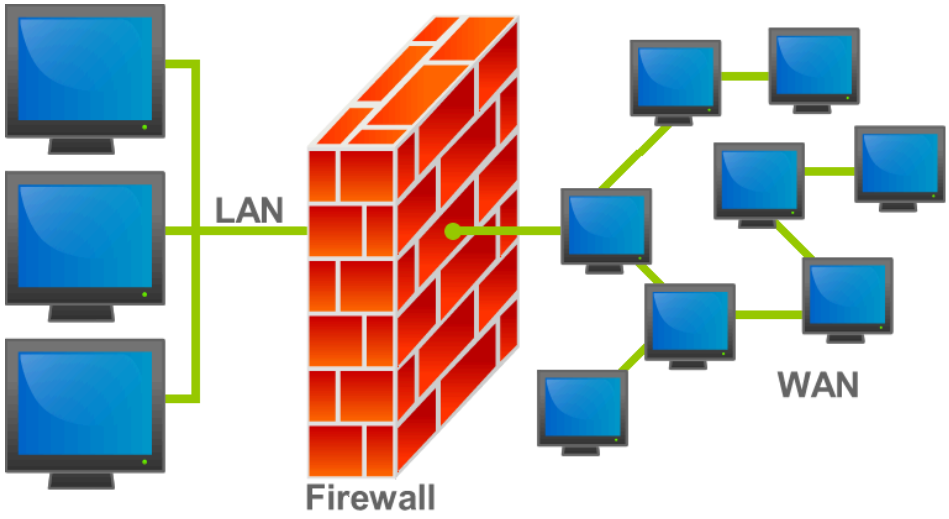


Рисунок 14: Межсетевой экран как технологическая контрмера: разделение локальной сети (LAN) и глобальной сети (WAN)

Куб МакКамбера образует 27 ячеек (3x3x3). Примеры:

- Конфиденциальность + Данные в состоянии покоя + Технологии = шифрование дисков AES (Advanced Encryption Standard) 256
- Целостность + Данные в процессе передачи + Технологии = цифровые подписи и TLS
- Доступность + Данные в процессе обработки + Политики = планы обеспечения непрерывности бизнеса
- Конфиденциальность + Данные в процессе передачи + Обучение = обучение сотрудников использованию VPN

Каждый анализ безопасности должен учитывать все три состояния данных. Распространённая ошибка состоит в том, что данные в состоянии покоя защищаются надёжным шифрованием, но передаются в незашифрованном виде, или сетевая передача защищена, но данные остаются незащищёнными в памяти.

Куб МакКамбера упоминается в курсе Cisco Cybersecurity Essentials.

Часть 3: За пределами триады КЦД — дополнительные свойства безопасности

Хотя триада КЦД хорошо служила нам на протяжении десятилетий, современные требования к безопасности расширились. Рассмотрим три дополнительных свойства, которые в настоящее время считаются необходимыми.

Аутентификация

Аутентификация — это процесс проверки того, что кто-то или что-то является тем, за кого (или что) себя выдаёт. Прежде чем применять какие-либо средства управления доступом, необходимо сначала установить, кто делает запрос.

Аутентификация обычно основывается на трёх первичных факторах:

- **Что-то, что вы знаете**: пароль или PIN-код (Personal Identification Number, персональный идентификационный номер);
- **Что-то, что вы имеете**: смарт-карта, телефон или токен безопасности;
- **Что-то, что вы есть**: биометрические данные, такие как отпечатки пальцев или распознавание лица.

Современные системы также используют **контекстные атрибуты** (иногда называемые "Что-то, что вы делаете" или "Где вы находитесь") для повышения безопасности без необходимости явных действий со стороны пользователя:

- **Местоположение**: GPS-координаты или IP-геолокация
- **Поведение**: ритм набора текста, шаблоны движения мыши или время суток

Многофакторная аутентификация (MFA) объединяет два или более первичных факторов. Когда вы входите в свой банковский аккаунт и получаете текстовое сообщение с кодом, вы используете два фактора: что-то, что вы знаете (ваш пароль), и что-то, что вы имеете (ваш телефон).

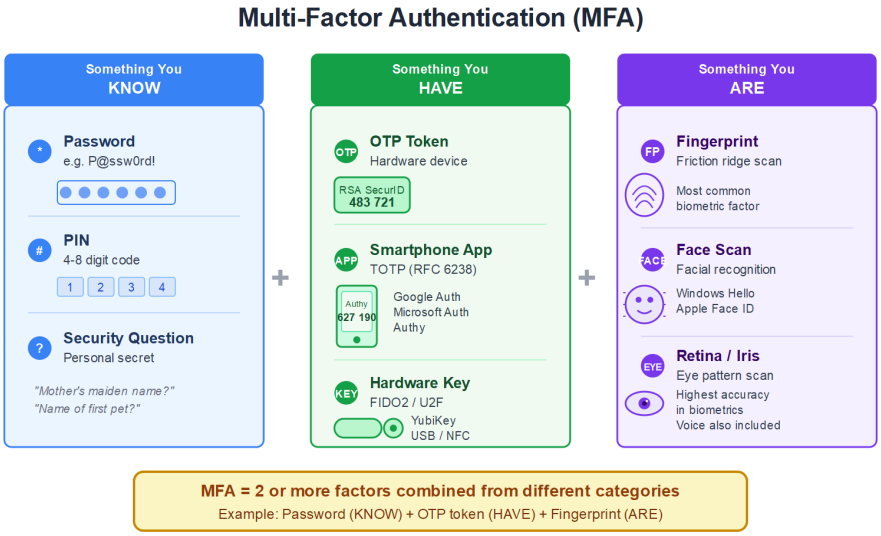


Рисунок 15: Аппаратные OTP-токены и приложение-аутентификатор на смартфоне: устройства фактора владения для многофакторной аутентификации

Контекстные атрибуты часто используются для **аутентификации на основе рисков (RBA)**, чтобы решить, необходимы ли дополнительные проверки.

Неотрекаемость

Неотрекаемость означает, что сторона не может отрицать совершение определённого действия. Если вы подписали договор, неотрекаемость гарантирует, что вы не сможете впоследствии утверждать, что не подписывали его.

В цифровом мире неотрекаемость достигается посредством цифровых подписей и всестороннего журналирования. Когда руководитель одобряет финансовую транзакцию своей цифровой подписью, он не может впоследствии отрицать, что одобрил её, поскольку криптографические доказательства подтверждают его участие.

Неотрекаемость имеет решающее значение для:

- Юридических доказательств в суде;
- Журналов аудита для соблюдения нормативных требований;
- Подотчётности в финансовых операциях;
- Предотвращения мошенничества.

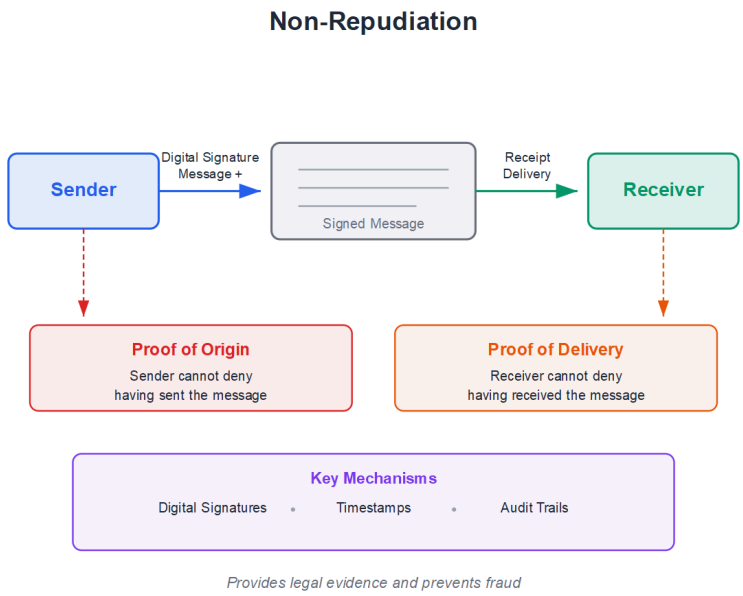


Рисунок 16: Неотказуемость: доказательство происхождения и доставки

Подотчётность

Подотчётность означает возможность отследить действия до субъекта, который их выполнил. Каждое действие в системе должно быть приписано конкретному пользователю или процессу.

Подотчётность требует:

- Строгой аутентификации для идентификации пользователей;
- Всестороннего журналирования для записи действий;
- Безопасного хранения журналов для предотвращения фальсификации;
- Регулярного просмотра журналов для обнаружения аномалий.

Без подотчётности невозможно расследовать инциденты, обеспечивать соблюдение политик или привлекать лиц к ответственности за их действия.

Часть 4: Активы, угрозы, уязвимости и риски

Теперь рассмотрим четыре взаимосвязанных понятия, являющихся фундаментальными для анализа безопасности: активы, угрозы, уязвимости и риски.

Активы

Актив — это всё, что имеет ценность и что организация хочет защитить. Активы могут быть материальными или нематериальными.

Материальные активы включают:

- Серверы и компьютеры
- Сетевое оборудование
- Здания и помещения
- Бумажные документы

Нематериальные активы включают:

- Данные и базы данных
- Программное обеспечение и приложения
- Интеллектуальную собственность
- Деловую репутацию
- Доверие клиентов

При проведении анализа безопасности мы должны прежде всего определить, что именно мы защищаем. Невозможно обезопасить то, о существовании чего вы не знаете.

Угрозы

Угроза — это любая потенциальная причина нежелательного инцидента, который может нанести ущерб активу или организации. Угрозы могут быть преднамеренными или случайными, внутренними или внешними.

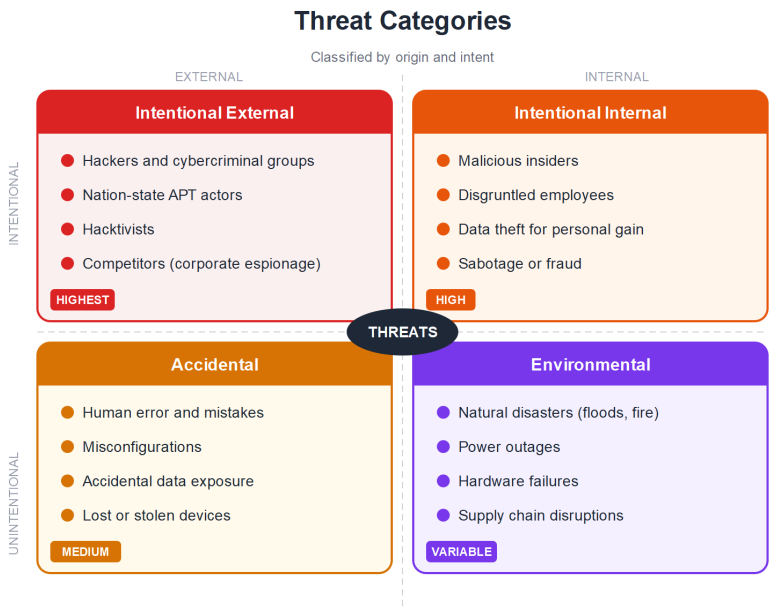


Рисунок 17: Категории угроз: преднамеренные, случайные и природные

Преднамеренные внешние угрозы

- Хакеры, стремящиеся к финансовой выгоде
- Государственные акторы, ведущие шпионаж
- Хактивисты, делающие политические заявления
- Конкуренты, похищающие коммерческие тайны

Преднамеренные внутренние угрозы

- Недовольные сотрудники, саботирующие системы
- Инсайдеры, похищающие данные для продажи
- Подрядчики, превышающие свои полномочия доступа

Случайные угрозы

- Сотрудники, переходящие по фишинговым ссылкам
- Администраторы, неправильно настраивающие системы
- Разработчики, вносящие ошибки в код

Природные угрозы

- Стихийные бедствия
- Перебои в электроснабжении
- Аппаратные неисправности

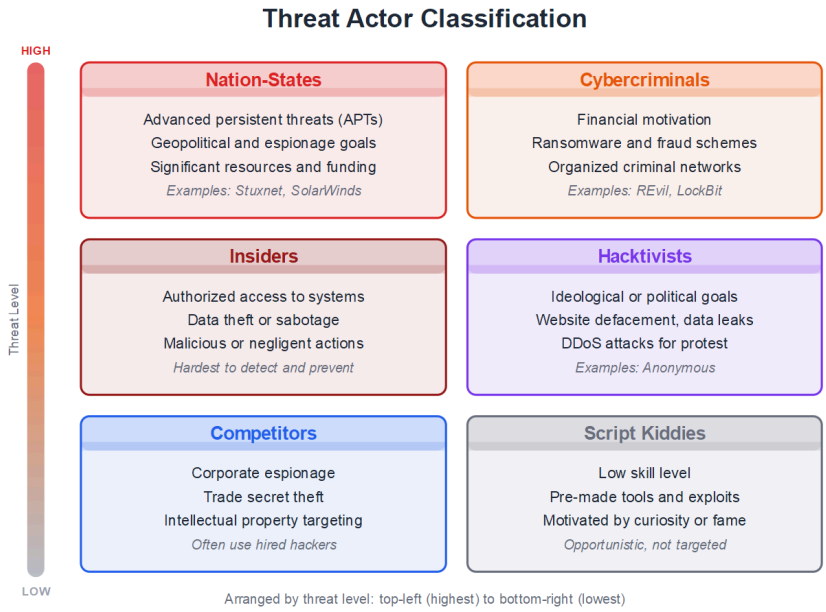


Рисунок 18: Классификация субъектов угроз в кибербезопасности

Уязвимости

Уязвимость — это слабое место, которое может быть использовано угрозой для получения несанкционированного доступа или нанесения ущерба. Уязвимости существуют в системах, процессах и людях.

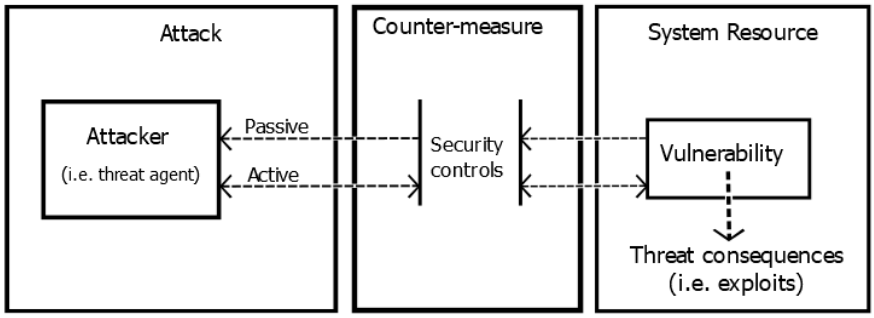


Рисунок 19: Модель угроз системы: активы, угрозы и уязвимости

Технические уязвимости

- Необновлённое программное обеспечение с известными недостатками безопасности
- Неправильно настроенные межсетевые экраны, пропускающие несанкционированный трафик
- Слабые алгоритмы шифрования, которые могут быть взломаны
- Пароли по умолчанию, которые не были изменены

Процессные уязвимости

- Отсутствие политик безопасности
- Недостаточное обучение сотрудников
- Неадекватные процедуры реагирования на инциденты
- Отсутствие проверок прав доступа

Человеческие уязвимости

- Подверженность социальной инженерии
- Склонность к использованию слабых паролей
- Несообщение о подозрительной деятельности
- Небрежность в соблюдении процедур

Риски

Риск — это потенциальная возможность потерь или ущерба, когда угроза использует уязвимость. Риск обычно рассчитывается как:

Риск = Угроза x Уязвимость x Ущерб

Или иногда в упрощённом виде:

Риск = Вероятность x Ущерб

Где вероятность — это шанс того, что угроза использует уязвимость, а ущерб — это последствия, если это произойдёт.

Проиллюстрирую примером. Предположим, ваша организация использует веб-сервер с устаревшим программным обеспечением, имеющим известную уязвимость. Угроза — это хакеры, которые могут использовать эту уязвимость. Уязвимость — это необновлённое программное обеспечение. Риск зависит от того, насколько вероятно, что злоумышленники обнаружат и воспользуются этой уязвимостью, и какой ущерб они смогут причинить.

Если сервер находится в публичном интернете и содержит данные кредитных карт клиентов, риск очень высок. Если сервер находится в изолированной сети и содержит только общедоступные маркетинговые материалы, риск значительно ниже.

Понимание рисков позволяет расставлять приоритеты в наших усилиях по обеспечению безопасности. Мы не можем защитить всё в равной степени, поэтому должны сосредоточиться в первую очередь на наиболее высоких рисках.

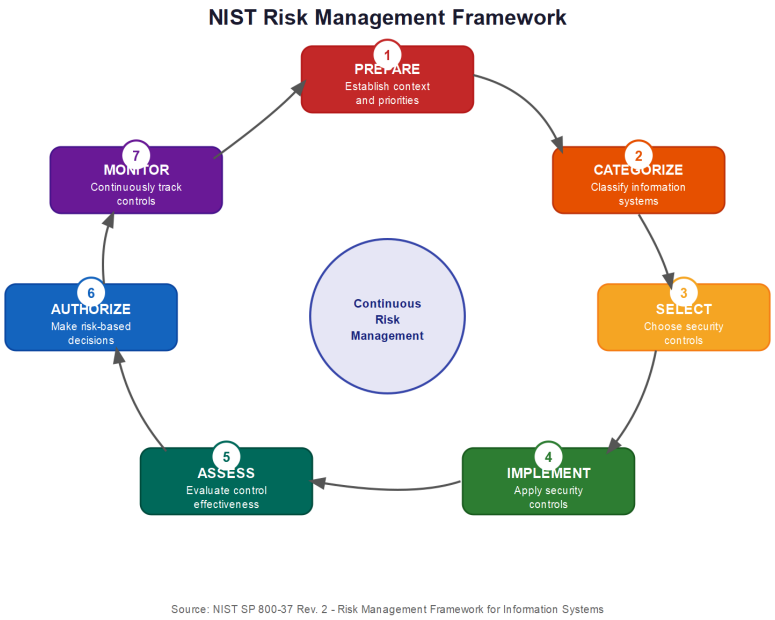


Рисунок 20: Система управления рисками NIST (National Institute of Standards and Technology, Национальный институт стандартов и технологий)

Часть 5: Инциденты безопасности и нарушения безопасности

Студенты часто путают эти термины, поэтому давайте их уточним.

Инцидент безопасности — это любое событие, потенциально ставящее под угрозу конфиденциальность, целостность или доступность информационного актива. К инцидентам относятся:

- Попытки атак, даже неуспешные
- Нарушения политик
- Сбои систем
- Подозрительная деятельность

Нарушение безопасности — это инцидент безопасности, который привёл к подтверждённому несанкционированному доступу к данным, приложениям, сервисам, сетям или устройствам. Все нарушения являются инцидентами, но не все инциденты являются нарушениями.

Вот пример: если кто-то пытается войти в ваш аккаунт с неправильным паролем — это инцидент. Если ему удаётся войти без авторизации — это нарушение безопасности.

Организации должны обнаруживать инциденты и нарушения, реагировать на них и извлекать уроки. Процедуры реагирования на инциденты, которые мы рассмотрим позже в этом курсе, определяют, как действовать в таких ситуациях.

Часть 6: Эшелонированная защита

Эшелонированная защита (Defense in Depth) — это стратегия безопасности, использующая несколько уровней защиты. Если один уровень выходит из строя, другие продолжают обеспечивать безопасность. Эта концепция заимствована из военной стратегии, где замки имели рвы, стены, башни и вооружённую охрану — каждый уровень усложнял проникновение.

В информационной безопасности эшелонированная защита включает:

- **Физический уровень**: охрана, замки́, ограждения, камеры видеонаблюдения;
- **Уровень периметра**: межсетевые экраны, системы обнаружения вторжений, демилитаризованные зоны;
- **Сетевой уровень**: сегментация сети, VPN, списки управления доступом;
- **Уровень хоста**: антивирусное программное обеспечение, хостовые межсетевые экраны, управление обновлениями;
- **Уровень приложений**: валидация входных данных, практики безопасного программирования, межсетевые экраны уровня приложений;
- **Уровень данных**: шифрование, управление доступом, предотвращение утечки данных;
- **Человеческий уровень**: обучение по информационной безопасности, политики, проверка биографических данных.

Каждый уровень противодействует различным угрозам и обеспечивает дополнительную защиту. Злоумышленник должен преодолеть несколько уровней, чтобы добраться до ценных активов, что значительно затрудняет успешные атаки.

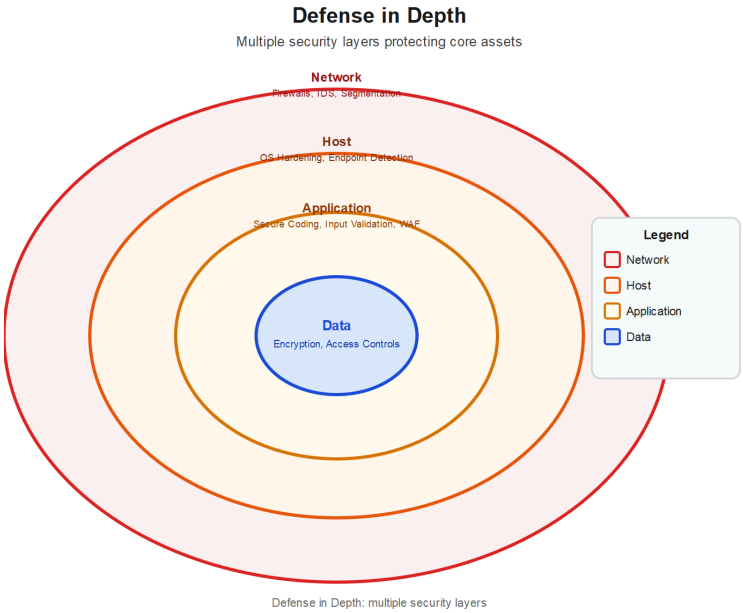


Рисунок 21: Эшелонированная защита: множественные уровни безопасности

Архитектура нулевого доверия (Zero Trust Archtecture)

В то время как традиционная эшелонированная защита полагается на сильный периметр, **Нулевое доверие** предполагает, что сеть уже скомпрометирована. Она работает по принципу "никогда не доверяй, всегда проверяй". Каждый запрос доступа полностью аутентифицируется, авторизуется и шифруется перед предоставлением доступа, независимо от того, откуда он исходит.

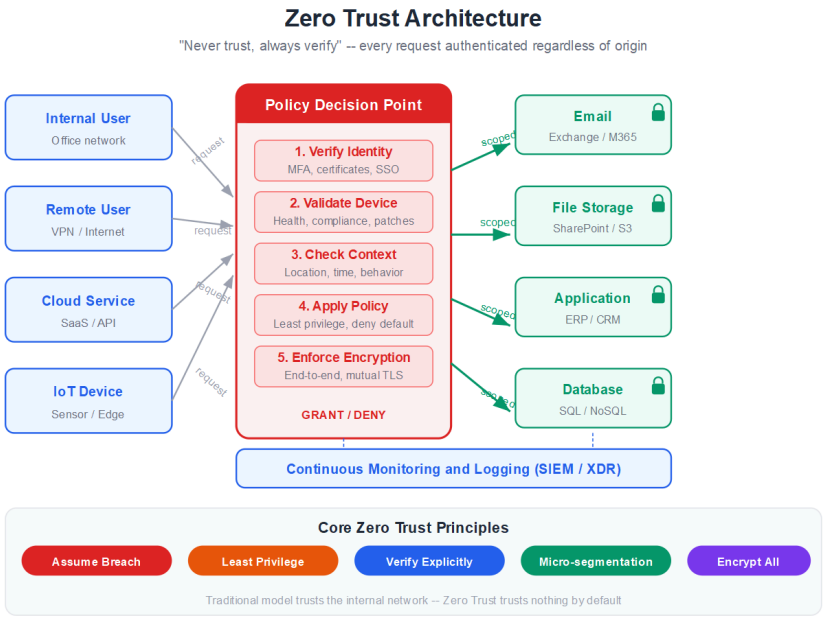


Рисунок 22: Архитектура нулевого доверия: явная проверка, минимальные привилегии

Часть 7: Безопасность на этапе проектирования и безопасность по умолчанию

Два принципа определяют, каким образом мы должны строить защищённые системы с самого начала.

Безопасность на этапе проектирования (Security by Design) означает учёт безопасности на протяжении всего жизненного цикла разработки, а не в качестве запоздалой мысли. Когда архитекторы проектируют здание, они включают пожарные выходы и спринклерные системы с самого начала. Они не добавляют их после завершения строительства. Тот же принцип применим к информационным системам.

Безопасность на этапе проектирования включает:

- Моделирование угроз на этапе сбора требований;
- Решения по безопасной архитектуре

- Тестирование безопасности на протяжении всей разработки
- Проверки безопасности перед развёртыванием

Безопасность по умолчанию (Security by Default) означает, что системы должны быть защищены в своей конфигурации по умолчанию. Пользователям не нужно включать функции безопасности; они должны явно отключать их при необходимости.

Примеры безопасности по умолчанию:

- Требование пароля сразу после установки
- Сетевые сервисы отключены, если явно не включены
- Шифрование включено по умолчанию
- Минимальные привилегии, предоставляемые по умолчанию

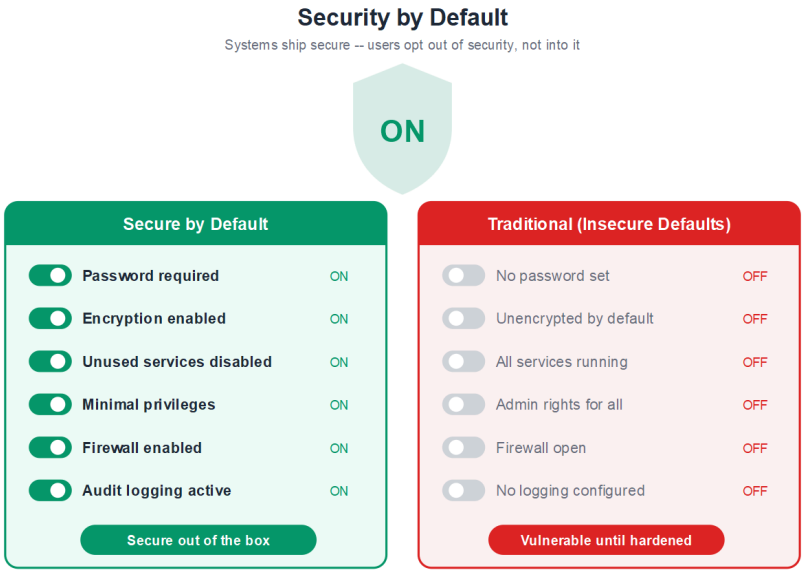


Рисунок 23: Безопасность по умолчанию: безопасная конфигурация из коробки

Противоположный подход, при котором системы поставляются незащищёнными и пользователи должны настраивать безопасность, приводит к бесчисленным уязвимостям, поскольку многие пользователи никогда не изменяют настройки по умолчанию.

Часть 8: Практическое применение

Завершим рассмотрением практического применения того, что мы узнали сегодня.

Сценарий 1: Проектирование нового приложения

Когда ваша организация разрабатывает новый клиентский портал, необходимо:

1. Определить активы: данные клиентов, учётные данные, записи транзакций
2. Определить угрозы: хакеры, злонамеренные инсайдеры, случайное раскрытие
3. Определить уязвимости: потенциальная SQL (Structured Query Language) инъекция, слабая аутентификация, недостаточное журналирование
4. Оценить риски: высокий риск хищения данных клиентов
5. Применить средства защиты: зашифровать данные (конфиденциальность), валидировать входные данные (целостность), развернуть резервные серверы (доступность)
6. Реализовать эшелонированную защиту: межсетевой экран, межсетевой экран уровня приложений (WAF), безопасное программирование, шифрование, мониторинг

Сценарий 2: Оценка поставщика

При выборе облачного провайдера задайте следующие вопросы:

- Как они защищают конфиденциальность? (Шифрование, управление доступом)
- Как они обеспечивают целостность? (Контрольные суммы, контроль версий)
- Каково их соглашение об уровне обслуживания (SLA) по доступности? (Гарантии бесперебойной работы, резервирование)
- Как они обрабатывают инциденты? (Процедуры реагирования, уведомления)
- Какие сертификаты у них есть? (ISO (International Organization for Standardization, Международная организация по стандартизации) 27001, SOC 2 (Service Organization Control Type 2))

Сценарий 3: Реагирование на попытку фишинга

Если сотрудник получает подозрительное электронное письмо:

1. Не переходить по ссылкам и не скачивать вложения
2. Сообщить группе безопасности (это инцидент)
3. Группа безопасности анализирует угрозу
4. Если учётные данные были скомпрометированы, это становится нарушением безопасности
5. Внедрить дополнительные средства защиты (обучение, фильтрация электронной почты)
6. Задокументировать извлечённые уроки

Часть 9: Современные инструменты управления рисками (EASM и GRC)

Управление внешней поверхностью атаки (EASM)

Инструменты EASM предназначены для обнаружения "неизвестных" рисков. Они сканируют интернет извне (как это сделал бы злоумышленник), чтобы найти каждый цифровой актив, которым владеет организация — включая забытые серверы, облачные хранилища или теневые ИТ.

- **Основная цель:** Обнаружение и картирование уязвимостей с внешней точки зрения.
- **Ключевые примеры:**
- **IONIX:** Фокусируется на картировании "реальной" поверхности атаки, включая сложные цифровые цепочки поставок и облачные зависимости.
- **UpGuard / SecurityScorecard:** Предоставляет "рейтинг безопасности" (подобно кредитному рейтингу) для вашей организации и ваших сторонних поставщиков.
- **Целевая аудитория:** Инженеры по безопасности, команды по анализу угроз.
- **Аналогия: Строительный инспектор.** Он ходит вокруг здания снаружи, выискивая трещины, открытые окна и сломанные замки́, о существовании которых вы не знали.

Управление, риски и соответствие (GRC)

Инструменты GRC — это внутренние "книги учёта" безопасности. Они отслеживают политики, аудиты и известные риски. Они помогают гарантировать, что организация соблюдает законы (например, GDPR (General Data Protection Regulation, Общий регламент по защите данных)) или стандарты (например, ISO 27001).

- **Основная цель:** Отслеживание соответствия, документирование внутренних рисков и управление аудитами.
- **Ключевые примеры:**
- **RSA Archer:** Традиционная платформа корпоративного уровня для управления корпоративными рисками и соответствием.
- **OneTrust:** Сильно сфокусирована на рисках конфиденциальности и управлении данными.
- **Целевая аудитория:** CISO (Chief Information Security Officer), риск-офицеры, менеджеры по соответствию.

- **Аналогия: Картотечный шкаф.** В нём хранятся чертежи, отчёты об инспекциях и сертификаты, подтверждающие, что здание юридически соответствует нормам.

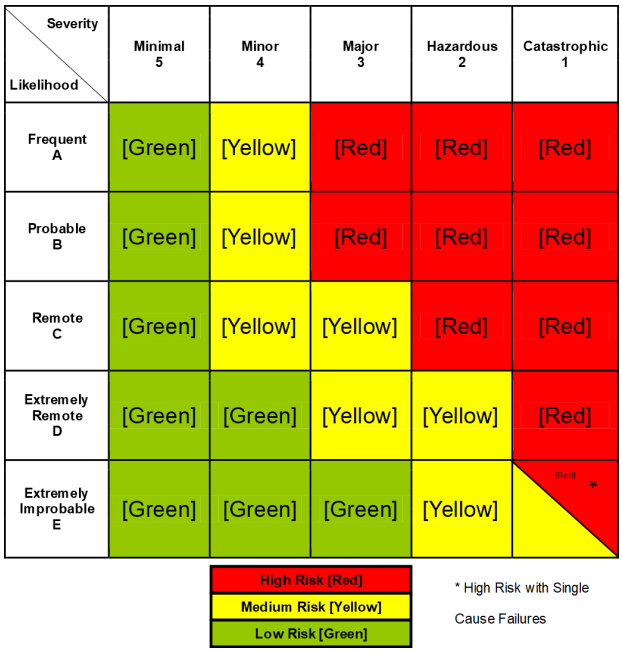


Рисунок 24: Матрица оценки рисков: вероятность и воздействие

Плюсы и минусы

Категория	Плюсы	Минусы
EASM	Находит немедленные технические угрозы; практически не требует ручной настройки для начала сканирования.	Может генерировать "шум" (ложные срабатывания); не говорит вам, как исправить политику, стоящую за риском.
GRC	Централизует все данные о рисках; необходим для прохождения аудитов и выполнения юридических требований.	Тяжёлая административная нагрузка; полагается на ручной ввод данных ("мусор на входе — мусор на выходе").

Заключение

Сегодня мы рассмотрели фундаментальные понятия, составляющие основу информационной безопасности:

1. **Информационная безопасность и кибербезопасность**: информационная безопасность защищает всю информацию; кибербезопасность сосредоточена на электронных системах

2. **Триада КЦД**: Конфиденциальность, Целостность и Доступность — три столпа безопасности
3. **Дополнительные свойства**: Аутентификация, неотрекаемость и подотчётность расширяют базовую модель
4. **Активы, угрозы, уязвимости и риски**: понимание этих взаимосвязей обеспечивает эффективное планирование безопасности
5. **Инциденты и нарушения**: инциденты — это потенциальные компрометации; нарушения — это подтверждённый несанкционированный доступ
6. **Эшелонированная защита**: множественные уровни защиты обеспечивают устойчивость
7. **Безопасность на этапе проектирования и по умолчанию**: встраивайте безопасность с самого начала

На следующей лекции мы подробно рассмотрим ландшафт угроз, изучим, кто нас атакует, почему они это делают и какие методы используют. Мы также обсудим такие фреймворки, как MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), которые помогают нам понимать и классифицировать угрозы.

Есть ли вопросы, прежде чем мы закончим?

Вопросы для обсуждения

1. В каких сценариях свойства триады КЦД могут вступать в противоречие друг с другом, и как организации должны разрешать такие конфликты?
2. Каким образом принцип "безопасность на этапе проектирования" меняет подход к разработке программного обеспечения по сравнению с традиционными подходами?
3. С какими основными трудностями сталкиваются организации при реализации эшелонированной защиты, и как их можно преодолеть?

Благодарю за внимание. Увидимся на следующем занятии.

Контрольные вопросы

1. Объясните различие между информационной безопасностью и кибербезопасностью. Как пересекаются и различаются их области охвата?
2. Дайте определение трём компонентам триады КЦД и приведите пример из реальной жизни, где каждый из них является основной задачей.

3. Каким образом аутентификация, неотрекаемость и подотчётность расширяют базовую модель КЦД?
4. Опишите взаимосвязь между активами, угрозами, уязвимостями и рисками. Как понимание этой цепочки помогает в планировании безопасности?
5. В чём разница между инцидентом безопасности и нарушением безопасности? Почему это различие важно?
6. Объясните стратегию эшелонированной защиты и приведите примеры средств защиты на трёх различных уровнях.
7. Что означает "безопасность на этапе проектирования" и чем она отличается от добавления безопасности после развёртывания?
8. Приведите пример сценария, в котором два элемента триады КЦД вступают в противоречие друг с другом.
9. Опишите три измерения Куба МакКамбера. Каким образом он расширяет триаду КЦД?
10. Объясните три состояния данных (в покое, при передаче, при обработке) и приведите пример угрозы и средства защиты для каждого.

Ключевые термины

- **Подотчётность**: свойство, обеспечивающее возможность однозначного отслеживания действий субъекта до этого субъекта
- **Актив**: всё, что имеет ценность для организации, включая данные, аппаратное обеспечение, программное обеспечение и персонал
- **Аутентификация**: процесс проверки заявленной идентичности
- **Доступность**: обеспечение своевременного и надёжного доступа авторизованных пользователей к информации и ресурсам
- **Данные в процессе обработки (Data in Processing)**: информация, создаваемая, изменяемая или используемая в процессоре и памяти
- **Данные в процессе передачи (Data in Transit)**: информация, передаваемая по сетям между системами
- **Данные в состоянии покоя (Data at Rest)**: информация, хранящаяся на носителях, таких как жёсткие диски, базы данных или резервные ленты
- **Нарушение безопасности**: подтверждённый инцидент, в ходе которого доступ к данным или их раскрытие произошли без авторизации
- **Триада КЦД**: три фундаментальные цели безопасности: Конфиденциальность, Целостность и Доступность

- **Конфиденциальность**: предотвращение несанкционированного раскрытия информации
- **Конфиденциальные вычисления (Confidential Computing)**: аппаратная технология защиты данных во время обработки в доверенных средах выполнения
- **Куб МакКамбера (McCumber Cube)**: трёхмерная модель безопасности, объединяющая цели КЦД, состояния данных и категории контрмер
- **Кибербезопасность**: защита электронных систем, сетей и данных от атак
- **Эшелонированная защита**: стратегия безопасности, использующая множественные уровни средств защиты
- **Инцидент**: потенциальная или предпринятая компрометация политик или практик безопасности
- **Информационная безопасность**: защита информации во всех формах от несанкционированного доступа, использования, раскрытия или уничтожения
- **Целостность**: обеспечение того, что данные не были модифицированы несанкционированным образом
- **Неотрекаемость**: гарантия того, что субъект не может отрицать совершение действия
- **Риск**: потенциальная возможность потерь в результате использования угрозой уязвимости
- **Безопасность по умолчанию**: системы, поставляемые с наиболее защищённой конфигурацией в качестве конфигурации по умолчанию
- **Безопасность на этапе проектирования**: встраивание безопасности в системы с самых ранних этапов проектирования
- **Угроза**: потенциальная причина нежелательного инцидента, который может привести к ущербу
- **Уязвимость**: слабое место в системе, которое может быть использовано угрозой