

Защита информации

Анастасия Полякова

Старший инженер безопасности в «Alibaba cloud»

Цель урока

Цель: познакомиться с информацией как объектом защиты компании и интереса злоумышленника, рассмотреть модель рисков и угроз, а также некоторые методы защиты информации.

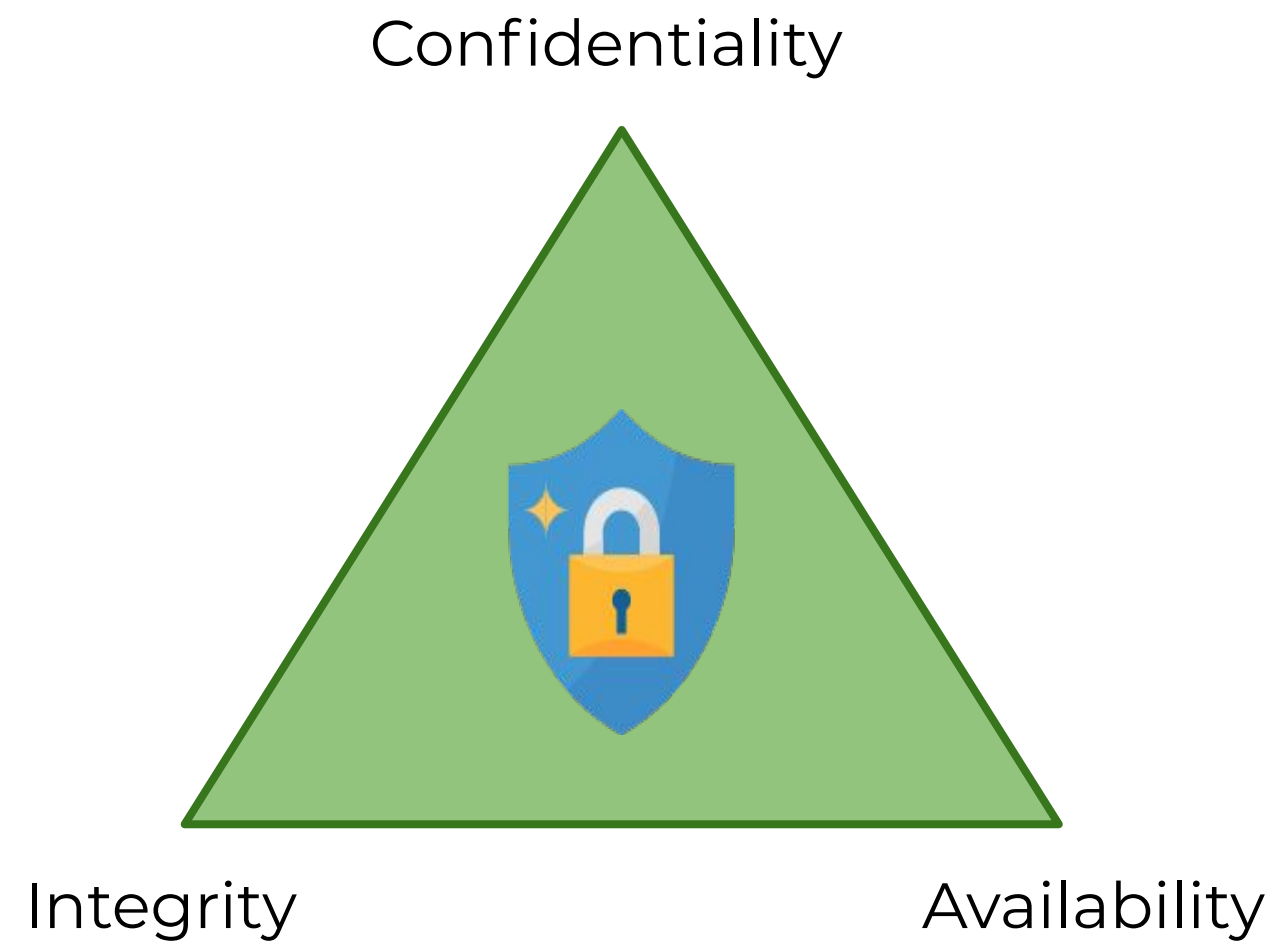
Информация как актив

Информация — сведения независимо от формы их представления.

Данные — форма представления информации.

CIA

- Конфиденциальность
- Целостность
- Доступность



Основная проблема защиты информации



Defender

Модель рисков

Модель рисков бизнеса отражает потенциальные потери организации в случае наступления определённого события.

Содержит перечень активов, процессов, потенциальных событий и их последствий, помогает оценить потенциальный ущерб при наступлении определённой рискованной ситуации и разработать меры управления рисками.

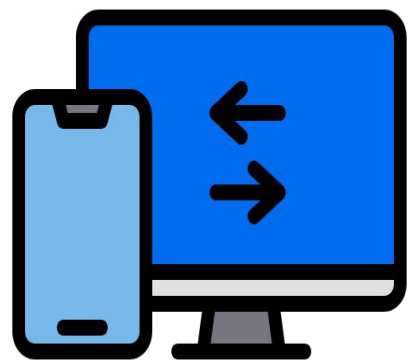
Модель угроз

Модель угроз информационной безопасности — это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

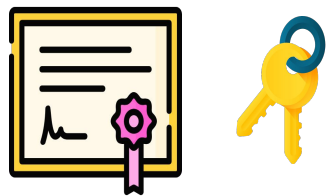
Построение модели угроз:

- определение источников угроз
- выявление критических объектов информационной системы
- определение перечня угроз для каждого критического объекта
- выявление способов реализации угроз
- оценка материального ущерба и других последствий возможной реализации угроз

Данные в состоянии покоя и передачи



Data in motion



Методы защиты:

- PKI (Public key infrastructure)



Data at rest



Методы защиты:

- шифрование
- физическая защита
- контроль доступа

РКИ и шифрование

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Инфраструктура открытых ключей (Public Key Infrastructure) — набор средств (технических, материальных и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптографических задач на основе закрытого и открытого ключей.

Вывод

Познакомились с информацией как объектом защиты компании и интереса злоумышленника, рассмотрели модель рисков и угроз, а также некоторые методы защиты данных в состоянии покоя и передачи.