Основы защиты информации

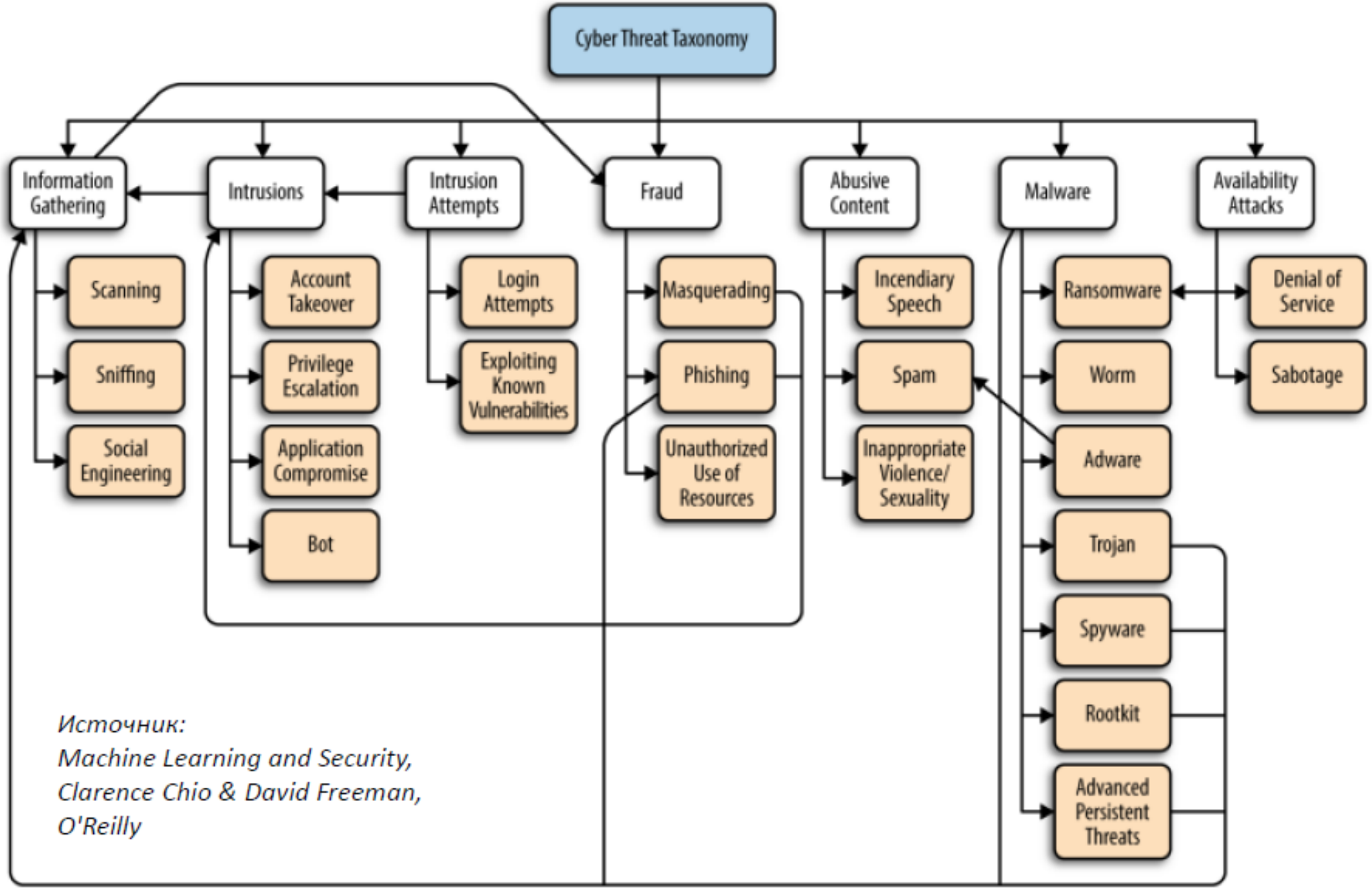
Информационная безопасность

Модель из трех категорий:

- Конфиденциальность
- Целостность
- Доступность

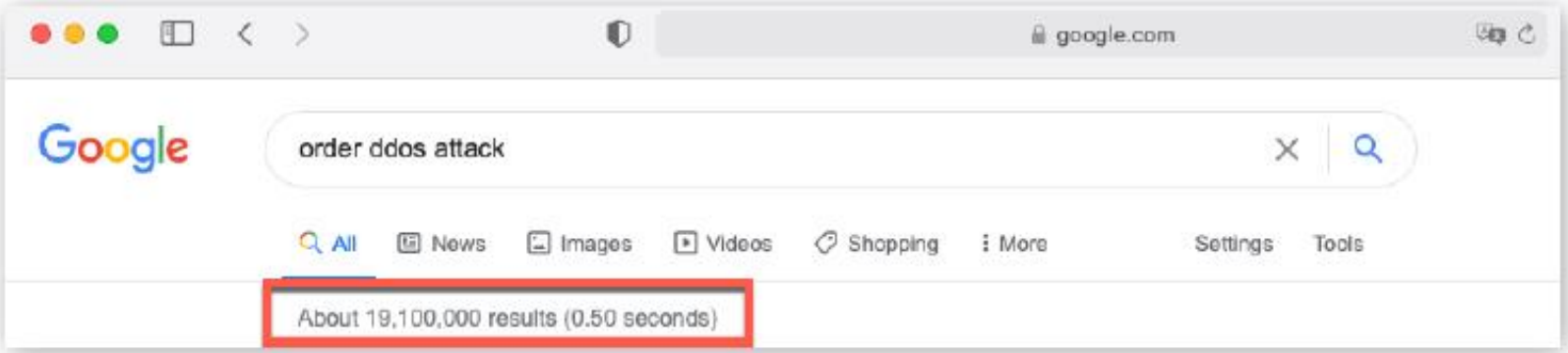
Составляющие информационной безопасности

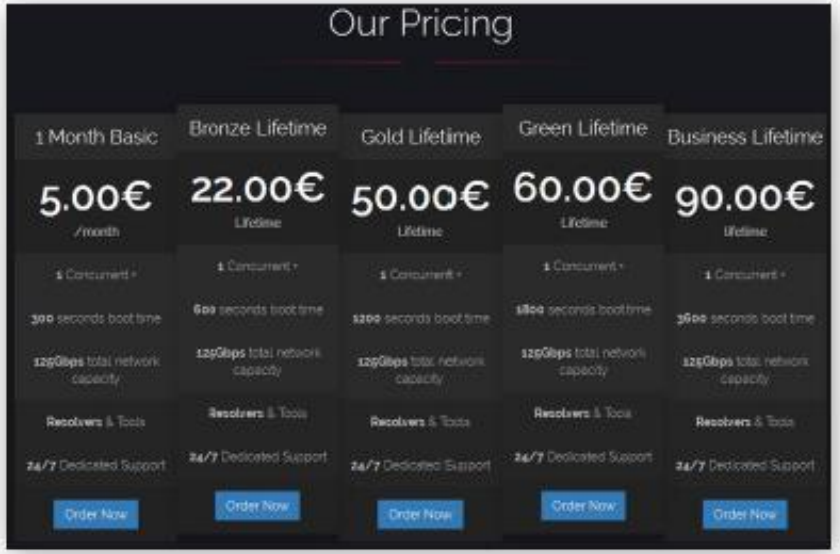
Классификация угроз

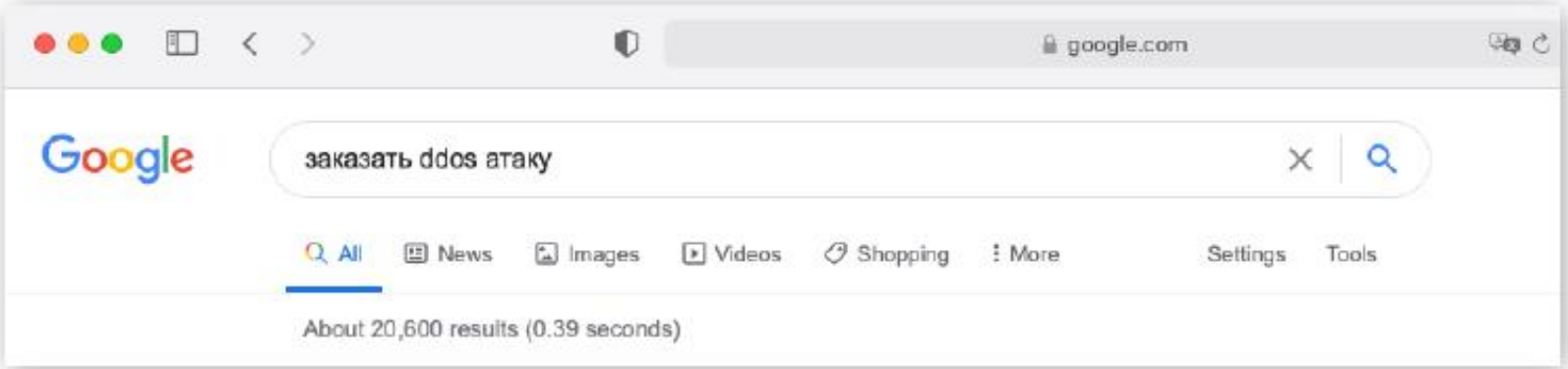


Источник:
Machine Learning and Security,
Clarence Chio & David Freeman,
O'Reilly

АТАКИ КАК СЕРВИС...







Классификация данных по уровням безопасности

- Для правительственных ИС:
  - совершенно секретно;
  - секретно;
  - конфиденциальная информации;
  - неклассифицированная информация.

Методы защиты информации

- Идентификация и аутентификация
- Управление доступом
- Протоколирование и аудит
- Экранирование
- Шифрование
- Антивирусная защита

Идентификация и аутентификация

Идентификация и аутентификация

- Токен – устройство выдающее одноразовые пароли.

Метод грубой силы

(brute-force attack)

Предполагает перебор всех возможных вариантов ключа шифрования до нахождения искомого ключа.

Если ключ содержит n бит, то число вариантов перебора - 2^n.

В среднем требуется 2^{n-1} тестовых операций

Проверка надежности пароля

https://blog.kaspersky.ru/password-check/

https://www.betterbuys.com/estimating-password-cracking-times/

Пример брутфорса

Предположим в пароле используются заглавные и строчные буквы латинского алфавита и цифры. Длина пароля – 8 символов.

Компьютер проверяет 10 млн вариантов в секунду.

Всего 62 символа, количество вариантов:

$$62^8 \sim 21834011 \cdot 10^7$$

В сутках 86 400 с. Всего требуется 253 суток.

Если для брутфорса используется сеть компьютеров (например, ботнет), времени потребуется существенно меньше.

Примерное время на брутфорс

Используем процессор: Intel Core i5 i5-4430

Перебор паролей в секунду: 10048090.42

Пароль	Строчные английские буквы и цифры (36 символов)	Строчные и заглавные английские буквы и цифры (62 символа)	Строчные и заглавные английские буквы, цифры и спецсимволы (72 символа)
6-символьный	3 минуты	1,5 часа	17 часов
8-символьный	3 дня	8 месяцев	16 лет
10-символьный	12 лет	2 600 лет	137 000 лет
12-символьный	15 000 лет	> 10 млн лет	>1 млрд лет

Управление доступом

- Уровни доступа:
  - Редактирование (удаление, добавление, изменение)
  - Просмотр (чтение)
  - Запрет доступа

Протоколирование и сетевой аудит

Протоколирование и сетевой аудит

Реализация протоколирования и аудита решает следующие задачи:

обеспечение подотчетности пользователей и администраторов;

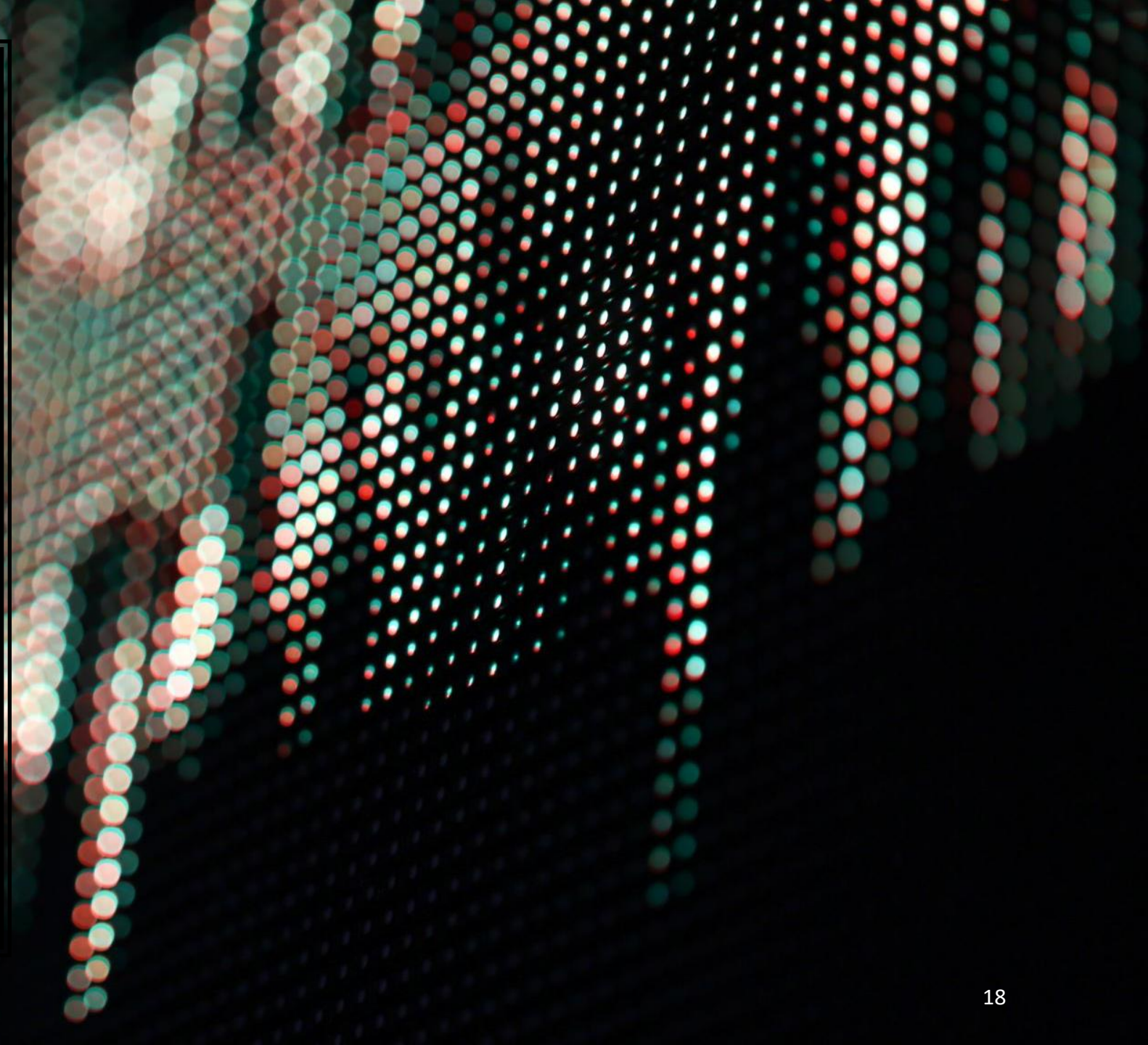
обеспечение возможности реконструкции последовательности событий;

обнаружение попыток нарушений информационной безопасности;

предоставление информации для выявления и анализа проблем.

Экранирование

- **Межсетевой экран** или **сетевой экран**

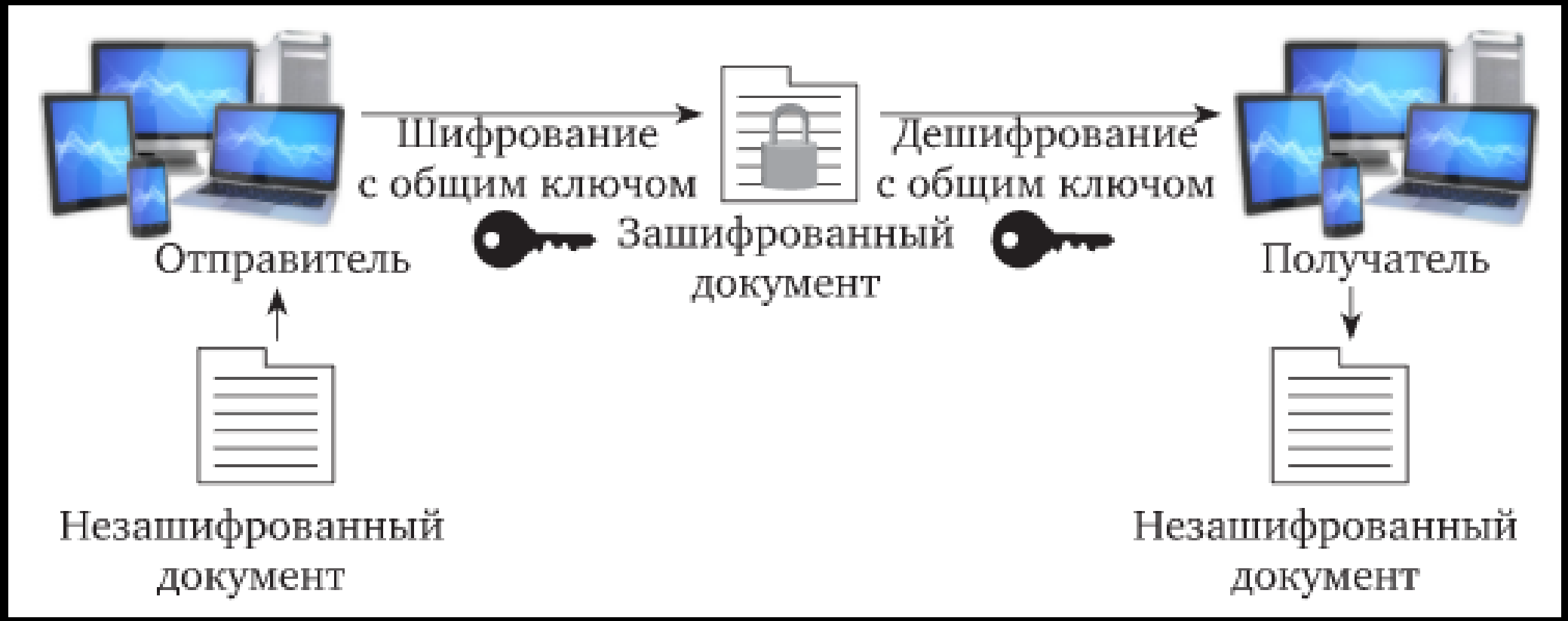


Шифрование

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

- шифрование;
- контроль целостности;
- аутентификация.

Различают два основных метода шифрования: симметричный и асимметричный.

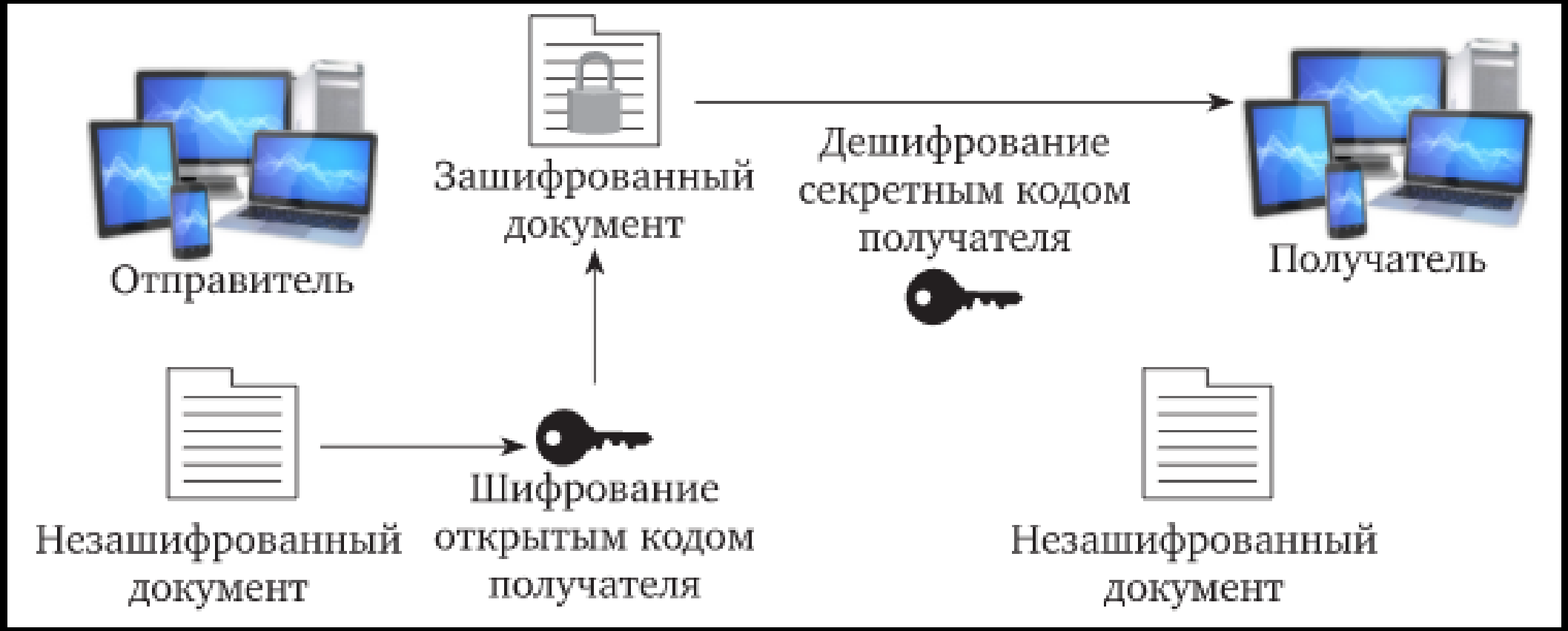


Симметричное шифрование

- Один и тот же ключ (хранящийся в секрете) используется и для шифрования, и для расшифровки данных.

Асимметричное шифрование

- Используются два ключа. Один из них, несекретный, применяется для шифрования, другой (секретный, известный только получателю) – для расшифровки.
- Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.



Асимметричное шифрование

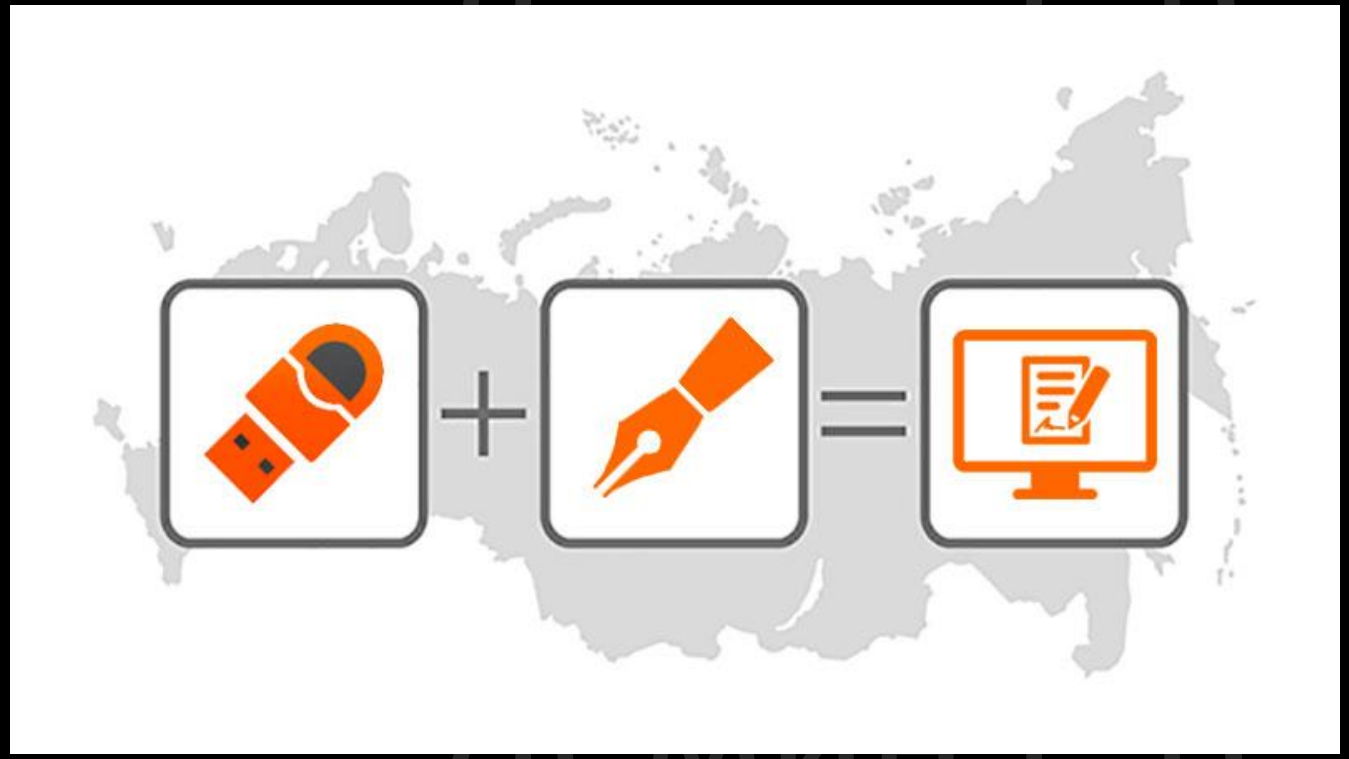
Асимметричное шифрование

ВАВТ ВАВТ

https://youtu.be/sGFbM-X6W_4

Электронная подпись

- **Электронная цифровая подпись (ЭЦП)**



Электронная подпись

Использование цифровой подписи позволяет осуществить:

- Контроль целостности передаваемого документа.
- Защиту от изменений (подделки) документа.
- Невозможность отказа от авторства.
- Доказательное подтверждение авторства документа.

Антивирусная защита

- **Компьютерный вирус**

Классификация вирусов

По способу заражения

- Резидентные
- Нерезидентные

По способу маскировки

- Шифрованный
- Полиморфный

Классификация вирусов

- По среде обитания
  - загрузочные
  - файловые
  - макро-вирусы
  - скрипт-вирусы

Классификация вирусов

- По особенностям алгоритма
  - Простейшие вирусы (вирусы-паразиты)
  - Вирусы-репликаторы (черви)
  - Вирусы-невидимки (стелс-вирусы)
  - Вирусы-мутанты
  - Квазивирусы или «троянские» программы

- Программы-фильтры или сторожа
- Программы-детекторы (сканеры)
- Полиморфные детекторы
- Программы-ревизоры (мониторы)
- Эвристические доктора
- Карантинные доктора
- Проактивная защита

Антивирусная программа

- www.anti-malware.ru
- www.av-comparatives.org
- www.av-test.org

Защита данных

Антивирус

Безопасные браузеры

Приватный wi-fi

Безопасные мессенджеры

VPN

Пароль и двухфакторная аутентификация

Виртуальная карта

Резервное копирование данных

Обновления