

Информационная безопасность

- § 75. Основные понятия
- § 76. Вредоносные программы
- § 77. Защита от вредоносных программ
- § 78. Шифрование
- § 79. Хэширование и пароли
- § 80. Современные алгоритмы шифрования
- § 81. Стеганография
- § 82. Безопасность в Интернете

Информационная безопасность

§ 75. Основные понятия

Что такое информационная безопасность?

Информационная безопасность — это защищённость информации от любых действий, в результате которых владельцам или пользователям информации может быть нанесён **недопустимый** ущерб.

Причины ущерба:

- **искажение** информации
- **утеря** информации
- **неправомерный доступ** к информации



Защита не должна стоить дороже возможных потерь!

Что такое защита информации?

Защита информации — это меры, направленные на то, чтобы не потерять информацию, не допустить её искажения и неправомерного доступа к ней.

Нужно обеспечить:

- **доступность** информации
- **целостность**
- **конфиденциальность**

отказ оборудования
или сайта

кража или искажение

доступ посторонних

Проблемы в сетях:

- много пользователей
- возможность незаконного подключения к сети
- уязвимости сетевого ПО
- атаки взломщиков и вредоносных программ

Защита информации

Закон «**Об информации, информационных технологиях и о защите информации**» от 27 июля 2006 г. № 149-ФЗ.

Средства защиты информации:

- **организационные**: распределение помещений и прокладку линий связи; политика безопасности организации
- **технические**: замки, решётки на окнах, системы сигнализации и видеонаблюдения и т.п.
- **программные**: доступ по паролю, шифрование, удаление временных файлов, защита от вредоносных программ и др.

Ограничение прав доступа

Сотрудники

- имеют право доступа только к тем **данным**, которые им **нужны** для работы
- не имеют права **устанавливать ПО**
- раз в месяц должны менять **пароли**



Один человек не должен иметь возможности причинить серьёзный вред!

инсайдеры!

Кибервойны

Кибервойны — это использование Интернета и информационных технологий одним государством с целью причинения вреда военной, технологической, экономической, политической, информационной безопасности и суверенитету другого государства.

2015. Группа правительственных экспертов ООН **Нормы ответственного поведения в киберпространстве:**

- государство отвечает за работу всех информационных систем и компьютерных сетей на своей территории;
- в киберпространстве необходимо соблюдать общие принципы международного права, закреплённые в Уставе ООН: суверенитет государств, невмешательство в их внутренние дела, мирное разрешение споров.

Информационная безопасность в России

2000 г. Доктрина информационной безопасности РФ

Национальные интересы России:

- соблюдение конституционных прав и свобод человека в области получения и использования информации;
- информационное обеспечение государственной политики РФ;
- развитие отечественных средств информатизации, телекоммуникации и связи;
- защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Информационная безопасность

§ 76. Вредоносные программы

Что такое компьютерный вирус?

Компьютерный вирус — это программа, способная создавать свои копии (не обязательно совпадающие с оригиналом) и внедрять их в файлы и системные области компьютера.



Основная черта — способность распространяться при запуске!

Вредоносные программы — это программы, предназначенные для незаконного доступа к информации, для скрытого использования компьютера или для нарушения работы компьютера и компьютерных сетей.

malware

Зачем пишут вирусы?

- вирусы-шутки
 - самоутверждение программистов
 - **взлом сайтов** через заражённый компьютер
 - перевод **денег** на другой счёт
 - платные **SMS** для разблокировки
 - рассылка **спама**
 - **шпионаж** (кража паролей ⇒ кража денег)
 - **DoS-атака** (*Denial of Service*) – отказ в обслуживании
- ботнет** – сеть из заражённых компьютеров, управляемая из единого центра



УК РФ, статья 273: до 7 лет лишения свободы!

Признаки заражения вирусом

- замедление работы компьютера
- уменьшение объема свободной оперативной памяти
- зависание, перезагрузка или блокировка компьютера
- ошибки при работе ОС или прикладных программ
- изменение длины файлов
- появление новых файлов
- рассылка спама



Чтобы выполнить какие-то действия, вирус должен оказаться в памяти и получить управление компьютером.

Что заражают вирусы?



Вирусы заражают программный код!

- исполняемые программы (* .**exe**)
- загрузочные секторы дисков (MBR = *Master Boot Record*)
- пакетные командные файлы (* .**bat**)
- драйверы (* .**sys**)
- библиотеки динамической загрузки (* .**dll**)
- документы с **макросами**
- веб-страницы (внедрение программы-**скрипта**)



Вирусы **НЕ** заражают файлы с **данными**:
тексты, рисунки, звук, видео!

Как распространяются вирусы?



Основные источники заражения – **флэшки и компьютерные сети!**

- запуск заражённого файла
- загрузка с заражённого диска
- автозапуск заражённого флэш-накопителя (**autorun.inf**)
- открытие заражённого документа с макросами
- открытие сообщения электронной почты
- запуск программы, полученной в письме
- открытие веб-страницы с вирусом
- установка активного содержимого для просмотра веб-страницы
- по сетям (**вирусы-черви**, без участия человека)

Типы вредоносных программ

по среде обитания

- файловые
- загрузочные
- макровирусы
- скриптовые вирусы
- сетевые вирусы

Полиморфные вирусы: при создании копии немного изменяют код.

Сетевые черви: посылают по сети пакеты (*эксплойты*), позволяющие выполнить код удалённо.

нужно ставить «заплатки» (исправления, «патчи»)

Почтовые черви: распространяются через исполняемые программы в приложении к письму.

Google: запрет пересылки исполняемых файлов

социальная инженерия:
спровоцировать на запуск файла

«Троянские» программы



Распространяются вместе с кодеками, червями, «кряками»!

- клавиатурные шпионы
- похитители паролей
- утилиты удалённого управления (*backdoor*)
- логические бомбы (уничтожают информацию на дисках)

Вирусы для мобильных устройств

- похищение паролей (атака на мобильные приложения банков)
- блокировка смартфона (вымогательство)
- рассылка SMS и MMS
- звонки на платные номера
- удалённое управление смартфоном
- ускорение разрядки батарей

Вирусы для мобильных устройств

Как получить вирус:

- Android: возможна установка файлов-приложений (* .apk) не из Google Play
- ССЫЛКИ ВО ВСПЛЫВАЮЩИХ ОКНАХ
- ССЫЛКИ В SMS
- сети Wi-Fi, Bluetooth

запрашивается
разрешение
пользователя

«черви»

Информационная безопасность

§ 77. Защита от вредоносных программ

Что такое антивирус?

Антивирус — это программа, предназначенная для борьбы с вредоносными программами.

Задачи:

- не допустить заражения
- обнаружить присутствие вируса
- удалить вирус без ущерба для остальных данных

Антивирусный комплекс

сканер

монитор

Антивирус-сканер («доктор»)

- защита «по требованию» (нужен запуск)
- поиск в файлах **сигнатур** вирусов, которые *есть в базе данных* **нужно обновлять!**
- после обнаружения – лечение или удаление
- эвристический анализ** – поиск кода, похожего на вирус



- лечит известные вирусы
- до запуска не занимает память и время процессора



- не может предотвратить заражение

Антивирус-монитор

- постоянная защита
- проверка файлов при файловых операциях
- проверка флэш-дисков
- перехват подозрительных действий
- проверка данных из Интернета
- защита от «фишинга» и спама



- предотвращает заражение, в том числе и неизвестными вирусами



- замедляет работу компьютера
- может мешать работе программ и ОС

Антивирусы

Коммерческие



AVP = *Antiviral Toolkit Pro* (www.avp.ru) – Е. Касперский



DrWeb (www.drweb.com) – И. Данилов



NOD32 (www.eset.com)

shareware



Есть бесплатные пробные версии!

Бесплатные



Security Essential

(http://www.microsoft.com/security_essentials/)



Avast Home (www.avast.com)



Antivir Personal (free-av.com)



AVG Free (free.grisoft.com)

Онлайновые антивирусы

- устанавливают на компьютер активный модуль (*ActiveX*), который проверяет файлы...
- или файл пересылается на сайт разработчика антивирусов

<http://www.kaspersky.ru/virusscanner>

<http://www.bitdefender.com>

<http://security.symantec.com>

<http://us.mcafee.com/root/mfs/default.asp>



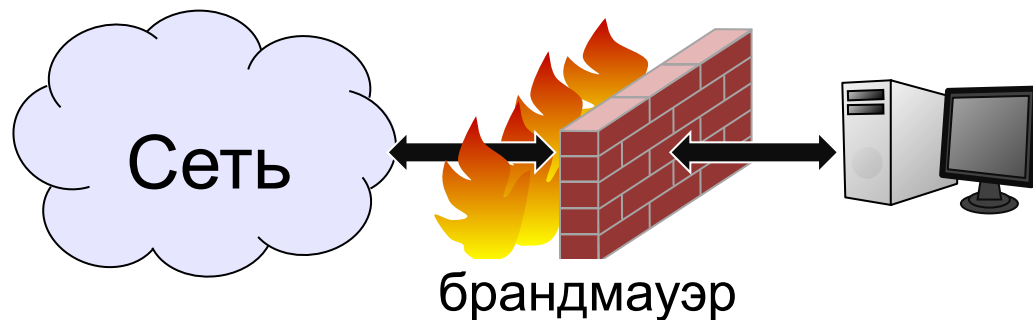
чаще всего не умеют
лечить, предлагает
купить антивирус

Сетевой экран

Брандмауэр (файервол)

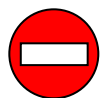
Контролирует

- подключения из внешней сети
- передачу данных из внутренней сети



Фильтрация пакетов:

- по адресам источника и приёмника
- по портам (каналам подключения)



не проверяет данные

Agnitum

Outpost

([www](http://www.agnitum.com)

([www](http://www.outpost.com)

([www.agnitum](http://www.agnitum.com)

([www.outpost](http://www.outpost.com)

Comodo Personal Firewall

([www.comodo](http://www.comodo.com)

([www.personalfirewall](http://www.personalfirewall.com)

([www.personalfirewall](http://www.personalfirewall.com)

([www.personalfirewall](http://www.personalfirewall.com)

([www.personalfirewall](http://www.personalfirewall.com)

бесплатно!



Меры безопасности

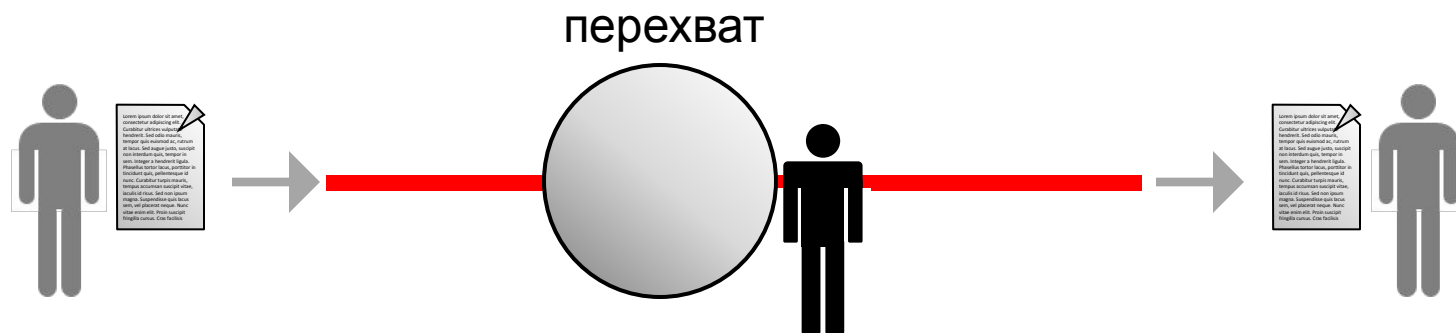
- делать резервные копии данных
- использовать сетевой экран (брандмауэр)
- использовать антивирус-монитор
- проверять флэш-диски антивирусом
- обновлять базы данных антивируса
- отключать автозапуск флэш-дисков
- не открывать подозрительные файлы (социальная инженерия!)
- не переходить по ссылкам в письмах
- использовать стойкие пароли
- менять пароли (раз в месяц)

Информационная безопасность

§ 78. Шифрование

Что такое шифрование?

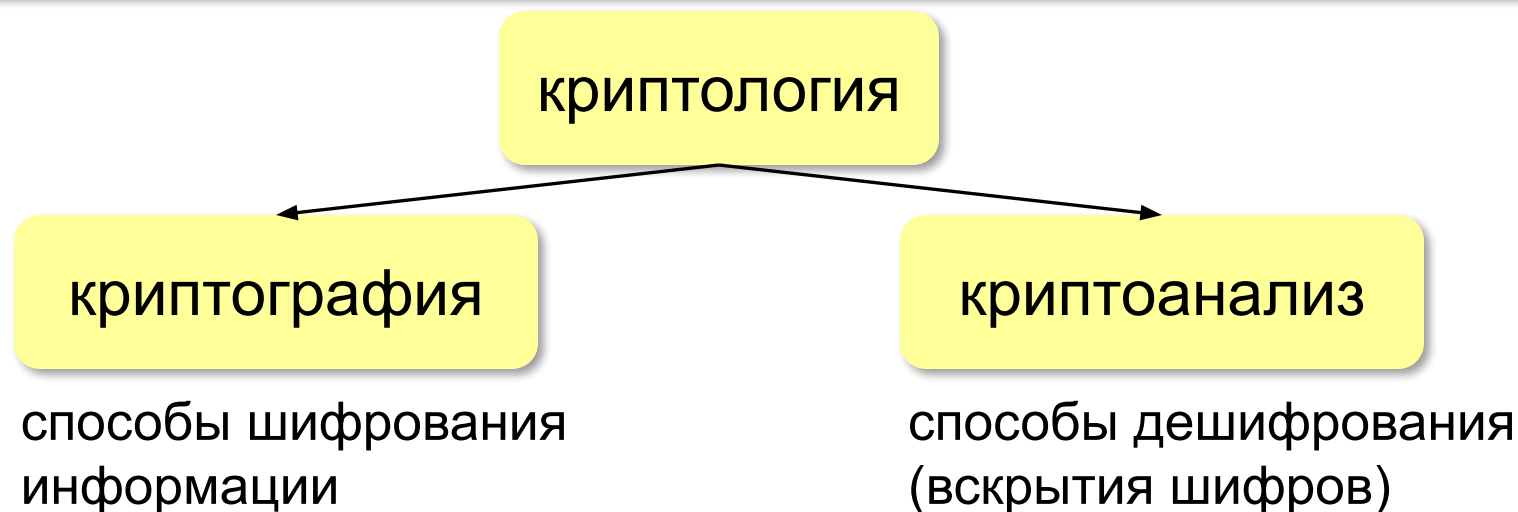
Проблема: передать информацию по **незащищенному** каналу связи.



Шифрование – это преобразование (кодирование) открытой информации в зашифрованную, недоступную для понимания посторонних.

Криптология

Криптология – наука о способах шифрования и дешифрования сообщений.



История (более 4000 лет):

- I (до IX в.) – замена одного алфавита на другой
- II (до XX в.) – многоалфавитные шифры
- III (XX в.) – электромеханические устройства
- IV (с 1970-х) – математическая криптология

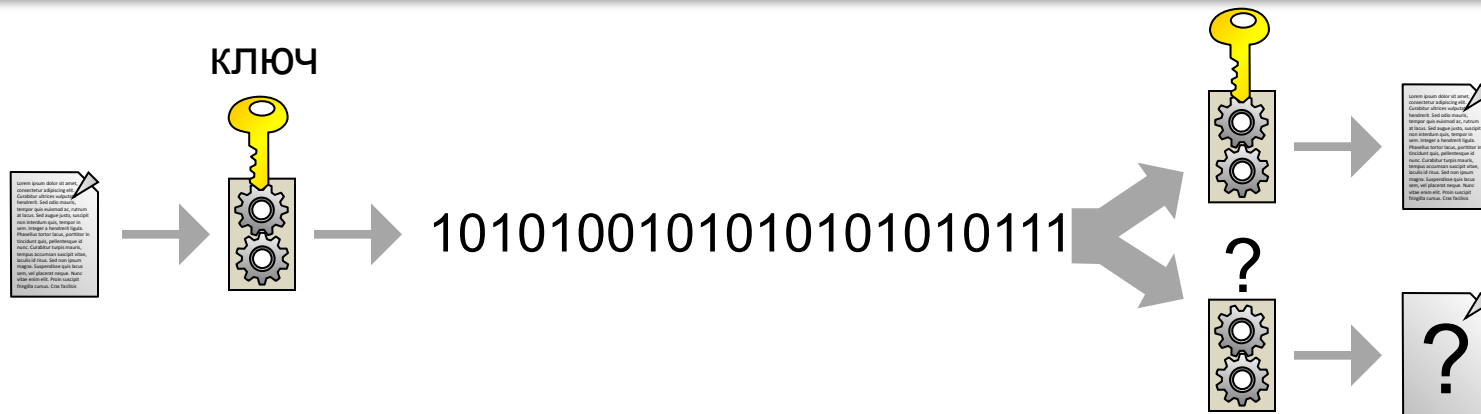
Шифрование и кодирование

Кодирование – нужен только алгоритм.



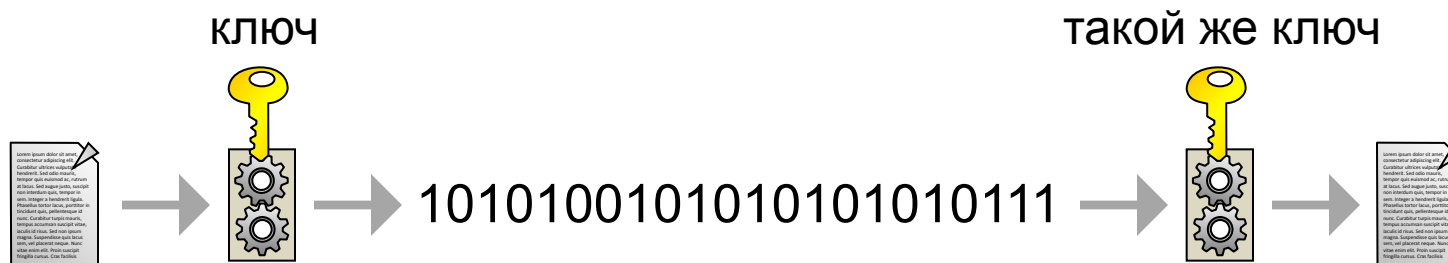
Шифрование – нужен алгоритм + ключ.

Ключ – это параметр алгоритма шифрования (шифра), позволяющий выбрать одно конкретное преобразование из всех возможных.

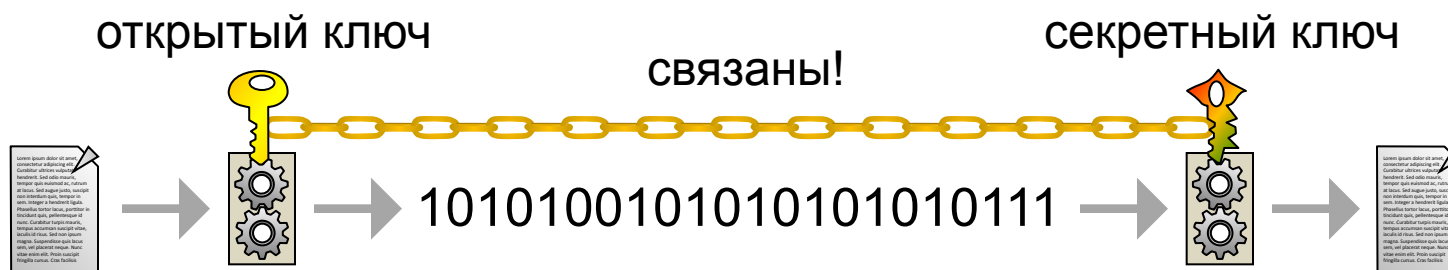


Типы шифров

Симметричные – один ключ для шифрования и расшифрования.



С открытым ключом – один (открытый) ключ для шифрования, второй (секретный) – для расшифрования.



Стойкость шифров

Криптостойкость – устойчивость шифра к расшифровке без знания ключа.



Любой шифр вскрывается!

почти... Кроме **одноразового блокнота** (шифра Вернама)

Криптостойкие шифры для расшифровки требуют:

- недостижимой вычислительной мощности или...
- недостижимого количества перехваченных сообщений или...
- недопустимо большого времени (информация становится неактуальной)

Шифр Цезаря



Пример:

ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ → ?

Результат:

ТУЛЫИО ЦЕЛЗИО ТСДИЗЛО

Шифр Цезаря

	А	Б	В	Г	Д	Е	Ж	З	...	Э	Ю	Я
коды	0	1	2	3	4	5	6	7		29	30	31

Преобразование кодов (сдвиг 3):

0 → 1 → 2 → ... 28 → 29 → 30 → 31 →

код буквы

сдвиг

код шифра

$$y = (x + k) \bmod n$$

число
символов
(32, без Ё)



Что служит ключом?



Если нумерацию начать с 1?

Шифр Цезаря (расшифровка)

Преобразование кодов ($k = 3$):

$0 \rightarrow$ $1 \rightarrow$ $2 \rightarrow$ $3 \rightarrow$ $4 \rightarrow$... $30 \rightarrow$ $31 \rightarrow$

Для $y < k$:

$$x = y - k + n$$

Для $y \geq k$:

$$x = y - k$$

Общая формула:

$$x = (y - k + n) \bmod n$$



Как доказать?

Шифр Цезаря



■ простота



■ легко вскрывается частотным анализом
(для достаточно больших текстов)

пробел	17,5%
О	9,0%
Е	7,2%
А	6,2%
И	6,2%
Т	5,3%
Н	5,3%
...	...

Шифр Виженера

Идея: при шифровании использовать несколько **разных** по величине сдвигов.

	А	Б	В	Г	Д	Е	Ж	З	...	Э	Ю	Я
коды	0	1	2	3	4	5	6	7		29	30	31

Ключ – кодовое слово, определяющее сдвиги.

ЗАБЕГ: сдвиги **7 – 0 – 1 – 5 – 3**

	П	Р	И	Ш	Е	Л		У	В	И	Д	Е	Л
сдвиг	7	0	1	5	3	7	0	1	5	3	7	0	1

Шифр Виженера



- простота
- если *длина ключа равна длине сообщения* и ключ – случайный набор букв, вскрыть практически невозможно



- вскрытие основано на повторении ключа
- если ключ – осмысленное слово, можно применить частотный анализ для данного языка

Информационная безопасность

§ 79. Хэширование и пароли

Проблема хранения паролей

- Пароли **нужно хранить**, иначе пользователи не смогут получить доступ к данным.
- Пароль **нежелательно хранить**, потому что базу паролей могут украсть, получив полный доступ к данным.

Задача:

- обеспечить нормальную работу пользователей с данными
- кража базы паролей не дает возможности получить доступ к данным

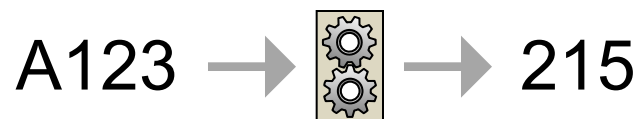
Что такое хэш-код?

Пароль: A123

Сумма кодов символов:

$$65 (\text{«A»}) + 49 (\text{«1»}) + 50 (\text{«2»}) + 51 (\text{«3»}) = 215$$

хэширование



хэш-код

Хэширование – это преобразование массива данных произвольного размера в битовую цепочку заданного размера (например, число).

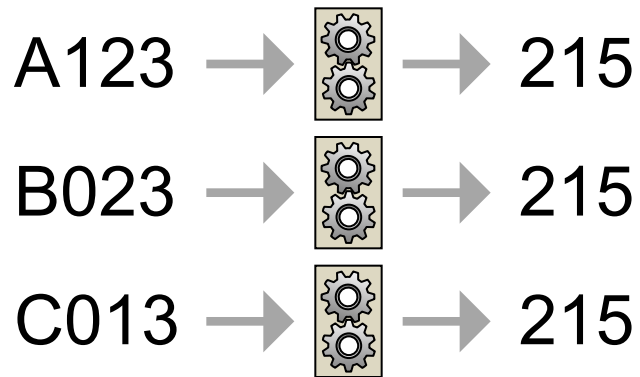


Можно ли по хэш-коду восстановить пароль?



Хэширование – необратимое шифрование!


Коллизии



Коллизия – это ситуация, когда разные исходные данные дают одинаковые хэш-коды.



Можно ли обойтись без коллизий?

4-байтный пароль →  → 2-байтное число

$2^{32} = 4,2$ млрд паролей $2^{16} = 65536$ кодов



Коллизии неизбежны!

Хэш-функции

Хэш-функция $H(M)$ – это правило построения хэш-кода t для произвольного массива данных M .

Требования:

- хэш-код очень сильно меняется при малейшем изменении исходных данных
- при известном хэш-коде t невозможно за приемлемое время найти сообщение M с таким хэш-кодом ($H(M) = t$)
- при известном сообщении M невозможно за приемлемое время найти сообщение M_1 с таким же хэш-кодом ($H(M) = H(M_1)$).



Что значит «за приемлемое время»?

Хэширование на практике

Алгоритмы: MD5, SHA-3, ГОСТ Р 34.11–2012.

Длина хэш-кода: 128, 160 или 256 бит.

Области применения:

- криптография (пароли)
- проверка правильности передачи данных (контрольные суммы)
- ускорение поиска (хэш-таблицы)

Правильный выбор пароля



- длина не менее 7-8 символов
- заглавные и строчные буквы + цифры + знаки (@#\$%^&*())
- случайный набор символов



- длина менее 7 символов
- только цифры
- часто используемые последовательности: «12345», «qwerty»
- дата рождения, номер телефона
- осмысленные слова

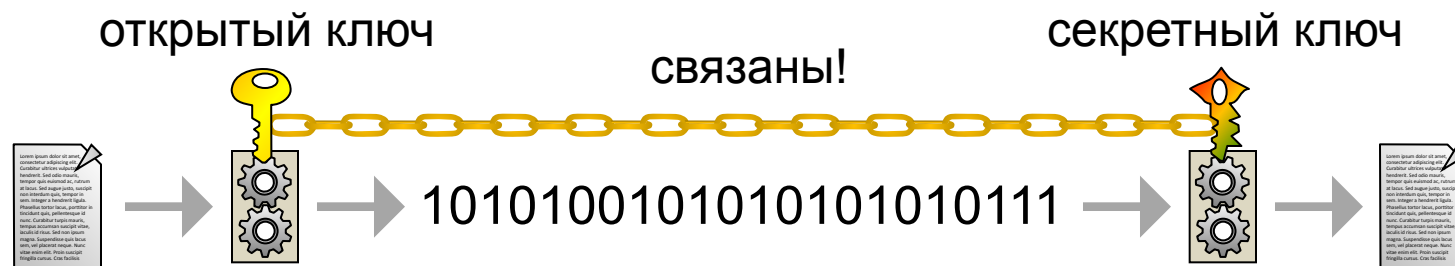
Информационная безопасность

§ 80. Современные алгоритмы шифрования

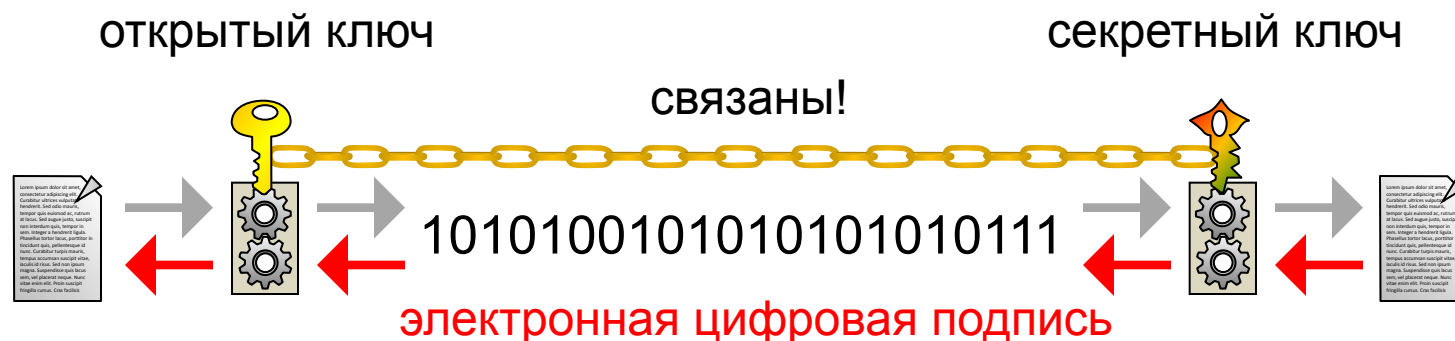
Алгоритм RSA

Р. Райвест (R. Rivest), А. Шамир (A. Shamir) и Л. Адлеман (L. Adleman), 1977.

Шифрование с открытым ключом:



Идея: применение открытого и секретного ключа восстанавливает сообщение:



Как построить ключи RSA?

1. Выбрать два **простых числа**, например,

$$p = 3, \quad q = 7$$

2. Вычислить

$$n = p \cdot q = 3 \cdot 7 = 21,$$

$$\phi = (p - 1) \cdot (q - 1) = 2 \cdot 6 = 12$$

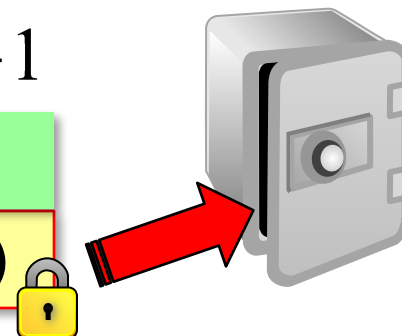
3. Выбрать число e ($1 < e < \phi$), которое не имеет общих делителей с ϕ : $e = 5$

4. Найти число d , для которого при некотором целом k выполняется условие: $d \cdot e = k \cdot \phi + 1$

$$d = 17: \quad 17 \cdot 5 = 7 \cdot 12 + 1$$

• **Открытый ключ:** (e, n) (5,21)

• **Секретный ключ:** (d, n) (17,21)



Алгоритм RSA

Шифрование: открытый ключ (e, n)

1. Сообщение – последовательность чисел в интервале $[0, n - 1]$.
2. Для каждого числа вычислить код

$$y = x^e \bmod n$$

Расшифровка: секретный ключ (d, n)

Для каждого кода вычислить число исходного сообщения:

$$x = y^d \bmod n$$

Алгоритм RSA: вычисление

Проблема:

очень большое число

$$y = x^e \bmod n$$

Упрощающая формула:

$$(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$$

Доказательство:

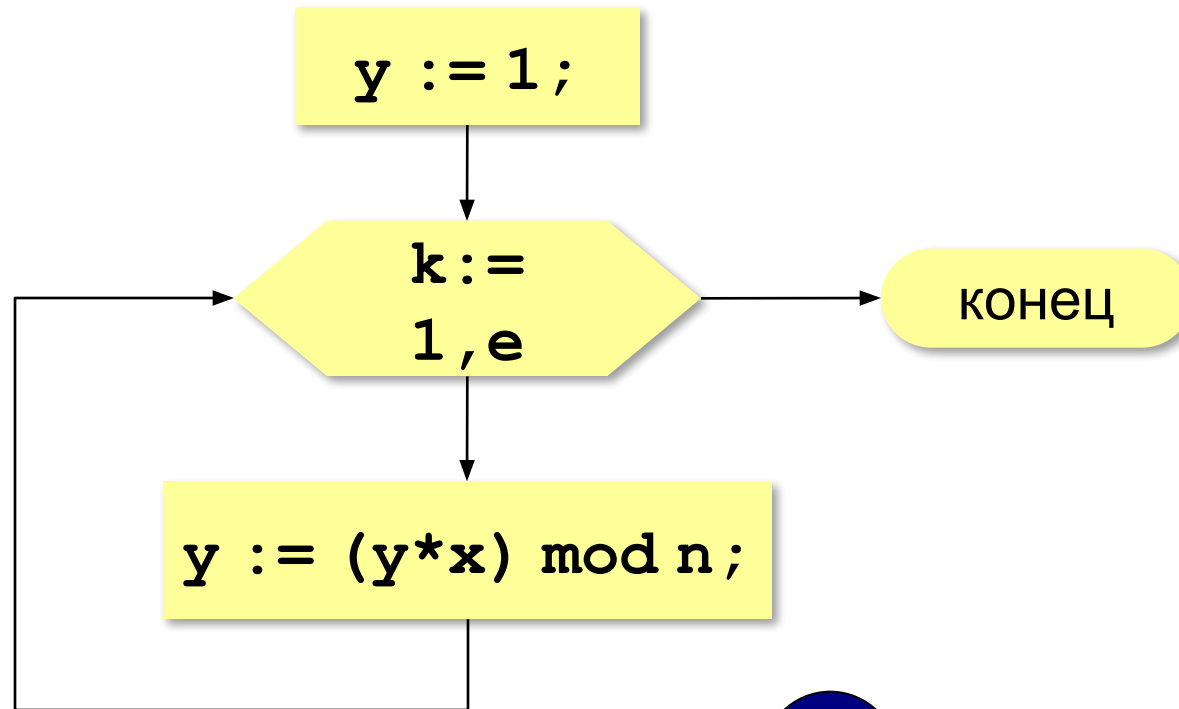
$$r_a = a \bmod n \quad \text{и} \quad r_b = b \bmod n$$

$$a = k \cdot n + r_a, \quad b = \ell \cdot n + r_b$$

$$\begin{aligned} (a + b) \bmod n &= [(k + \ell) \cdot n + r_a + r_b] \bmod n \\ &= (r_a + r_b) \bmod n \end{aligned}$$

Алгоритм RSA: вычисление

Вычисление $y = x^e \bmod n$



? Как быстрее?

Быстрое возведение в степень

$$x^e = \begin{cases} x^{e/2} \cdot x^{e/2}, & e - \text{чётное} \\ x^{e-1} \cdot x, & e - \text{нечётное} \end{cases}$$

2 умножения

Пример:

$$x^{100} = x^{64} \cdot x^{32} \cdot x^4$$

$$x^4 = [x^2]^2$$



Вместо 99!

3 умножения

1 умножение

$$x^{32} = [[[x^4]^2]^2]^2 \quad x^{64} = [x^{32}]^2$$

Программирование: $x^e = [b]^k \cdot p$

$$\begin{aligned} x^7 &= [x]^7 \cdot 1 = [x]^6 \cdot x = [x^2]^3 \cdot x = [x^2]^2 \cdot x^3 \\ &= [x^4]^1 \cdot x^3 = [x^4]^0 \cdot x^7 = x^7 \end{aligned}$$

Быстрое возведение в степень (+ mod)

```
def quickPowMod( x, e, n ):  
    b, k, y = x, e, 1  
    while k:  
        if k % 2 == 0:  
            k //= 2  
            b = (b * b) % n  
        else:  
            k -= 1  
            y = (b * y) % n  
    return y
```

```
def powMod( x, e, n ):  
    y = 1  
    for k in range(e):  
        y = (y*x) % n  
    return y
```

$$y = 123^{123456789} \bmod 1023$$

0,0000257 сек

28,5 сек

Алгоритм RSA: пример

Сообщение: 1 2 3

Шифрование: открытый ключ (e, n) (5,21)

$$1 \Rightarrow 1^5 \bmod 21 = 1$$

$$2 \Rightarrow 2^5 \bmod 21 = 32 \bmod 21 = 11$$

$$3 \Rightarrow 3^5 \bmod 21 = 243 \bmod 21 = 12$$

зашифрованное сообщение: **1 11 12**

Расшифровка: секретный ключ (d, n) (17,21)



$$1 \Rightarrow 1^{17} \bmod 21 = 1$$

$$11 \Rightarrow 11^{17} \bmod 21 = 2$$

$$12 \Rightarrow 12^{17} \bmod 21 = 3$$

расшифрованное сообщение: **1 2 3**

Алгоритм RSA: вскрытие

Задача: при известном открытом ключе (e, n)
найти секретный ключ d

Способ:

1) разложить n на взаимно-простые множители:

$$n = p \cdot q$$

2) вычислить

$$\varphi = (p - 1) \cdot (q - 1)$$

3) найти d , такое что при некотором k

$$d \cdot e = k \cdot \varphi + 1$$

Проблема: разложение большого числа на простые множители требует недостижимого объема вычислений (при длине $n > 1024$ бита)

Алгоритм RSA



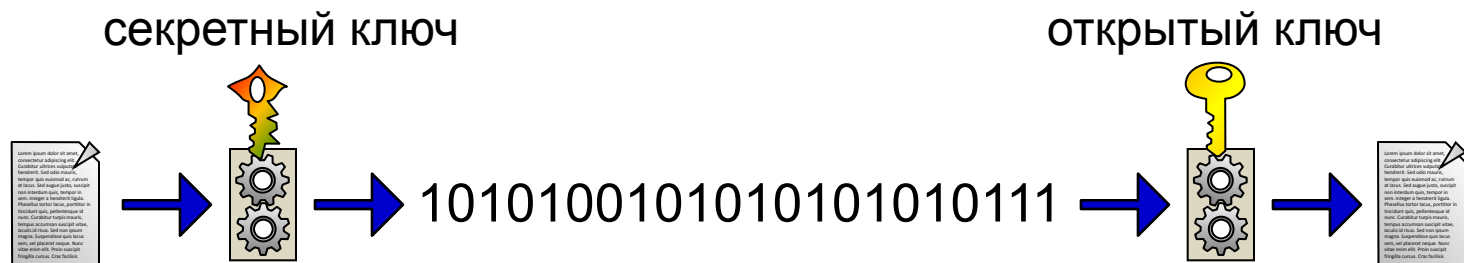
- для обмена открытыми ключами можно использовать незащищенный канал
- много готовых реализаций
- криптостойкость (при длине $n > 1024$ бита)



- медленная шифровка и (особенно) расшифровка
- при малом n взламывается

Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) – это набор символов, который получен в результате шифрования сообщения (или его хэш-кода) с помощью секретного ключа отправителя.



Применение:

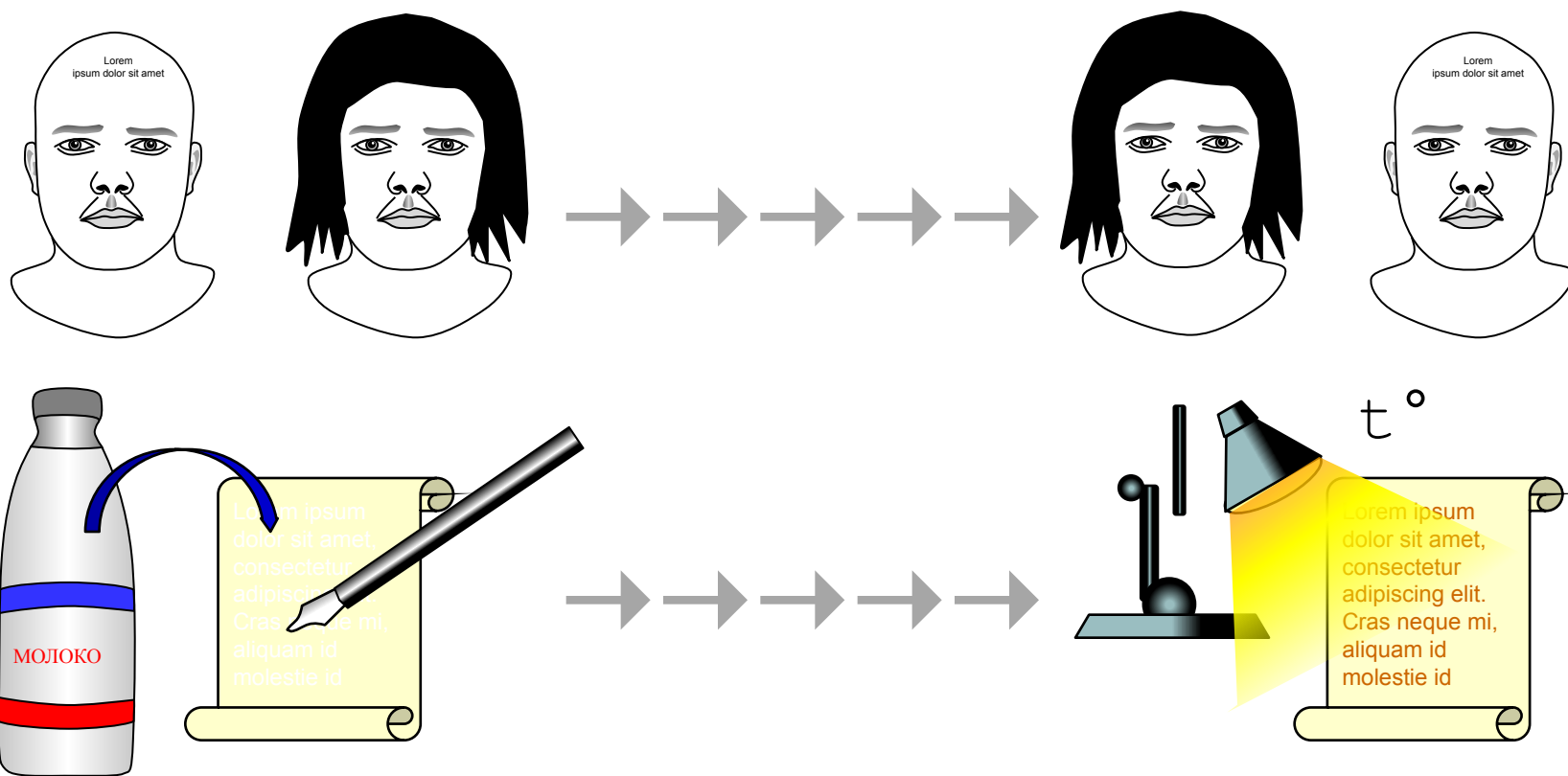
- доказательство авторства
- невозможность отказа от авторства
- защита от изменений (проверка целостности)

Информационная безопасность

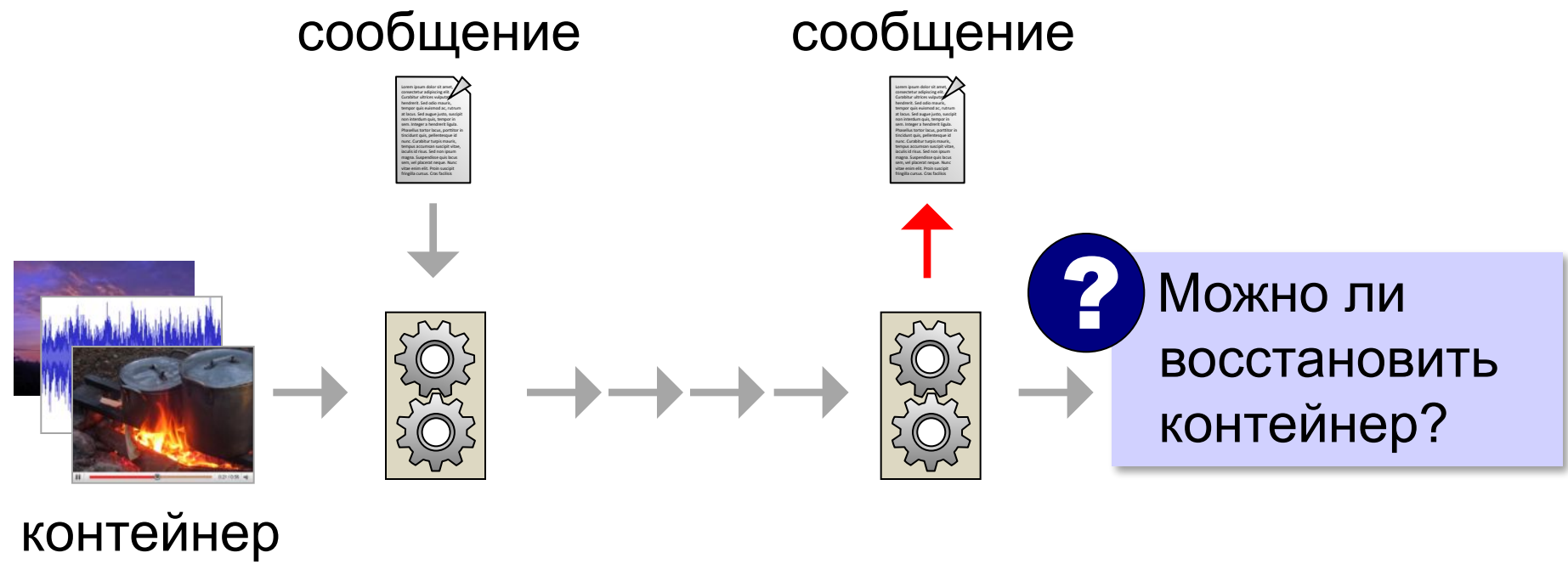
§ 81. Стеганография

Стеганография

Стеганография – это наука о скрытой передаче информации путем скрывания самого факта передачи информации.



Стеганография



Изменение младших битов данных: «И» = 11001000_2

1010110	0	1001010	0	0010101	0	0101001	0	1010101	0	1010101	1	1010101	1	1010111	1
---------	---	---------	---	---------	---	---------	---	---------	---	---------	---	---------	---	---------	---

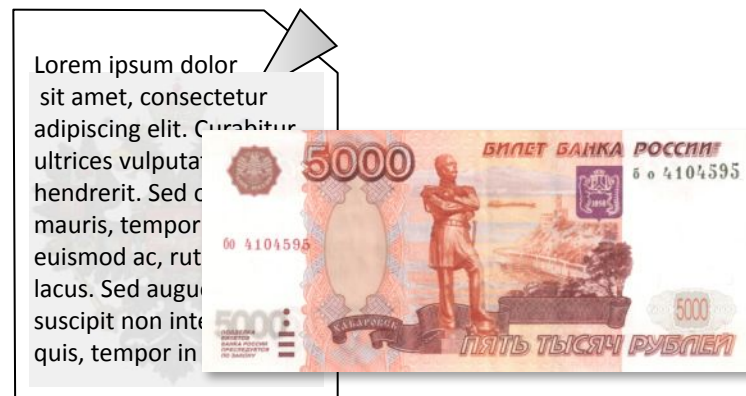
Цифровые водяные знаки

Обычные водяные знаки:

- «клеймо» изготовителя
- защита от подделок

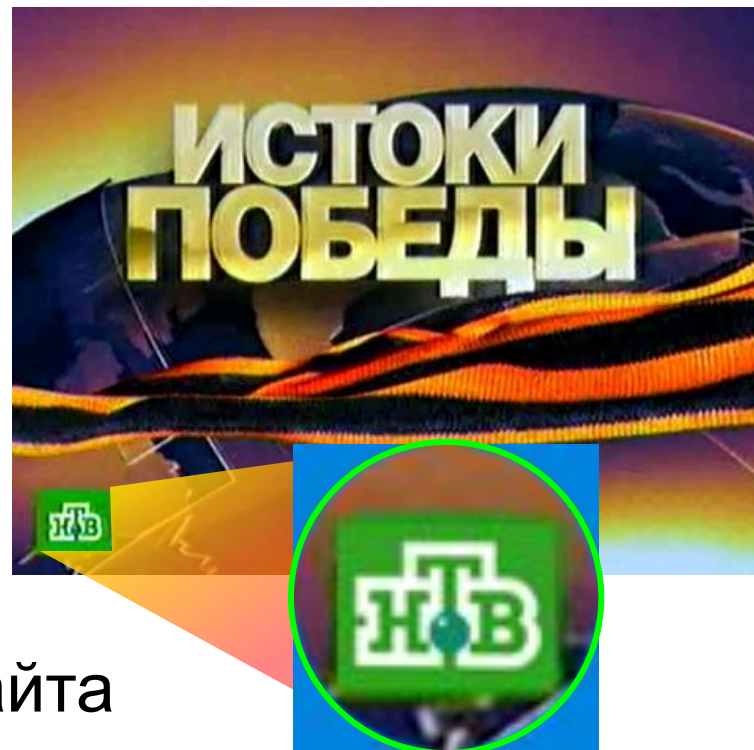
Цифровые водяные знаки:

- «клеймо» автора
- защита авторских прав



Цифровые водяные знаки

Видимые знаки:



- «клеймо» автора или сайта
- признак того, что информация защищена авторским правом
- затруднено незаконное использование

Информационная безопасность

§ 82. Безопасность в Интернете

Угрозы безопасности

Цели злоумышленников:

- **использование компьютера** для взлома других компьютеров, атак на сайты, рассылки спама, подбора паролей
- **кража** секретной информации — данных о банковских картах, паролей
- **мошенничество** (хищение путём обмана)
 - «нигерийские» письма (хищение денег)
 - «фишинг» (выманивание паролей через подставные сайты)
 - блокировка с требованием SMS

Правила личной безопасности

- не работать с правами **администратора**
- не запоминать **пароли** в браузере
- использовать флажок «**Чужой компьютер**»
- не использовать стандартные **секретные вопросы** (любимое блюдо, кличка собаки, девичья фамилия матери и т.п.)
- не размещать информацию, которая может **повредить**
- **шифровать** данные (архив с паролем)
- денежные операции – по протоколу **HTTPS**
(*Hypertext Transfer Protocol **Secure***)

Пароли

Методы взлома:

- личная информация
- подбор ответа на контрольный вопрос
- подбор слова по словарю
- полный перебор (*brute force* – метод грубой силы)

Плохие пароли:

- фамилия
- телефон
- слово из словаря
- только цифры
- последовательность букв с клавиатуры (*qwerty*)
- длина < 6 символов

Пароли

Хорошие пароли:

- не менее 7-8 символов
- заглавные и строчные буквы
- + цифры
- + специальные знаки
- не осмысленное слово



Лучше – случайная цепочка символов!

Конец фильма

ПОЛЯКОВ Константин Юрьевич

д.т.н., учитель информатики

ГБОУ СОШ № 163, г. Санкт-Петербург

kpolyakov@mail.ru

ЕРЕМИН Евгений Александрович

к.ф.-м.н., доцент кафедры мультимедийной

дидактики и ИТО ПГГПУ, г. Пермь

eremin@pspu.ac.ru

Источники иллюстраций

1. www.ntv.ru
2. en.wikipedia.org
3. иллюстрации художников издательства «Бином»
4. авторские материалы