Информационное общество и информационная безопасность

Введение в проблемы информационной безопасности

Запечников Сергей Владимирович

Национальный исследовательский ядерный университет «МИФИ»,
кафедра «Криптология и кибербезопасность»

Москва – 17 октября 2017

Что такое информационная безопасность?

Формально:

Информационная безопасность – это состояние защищенности информации, которой обладает человек, это исключение недопустимых рисков её уничтожения, искажения и утечки, которые могут привести к невосполнимым потерям или ущербу для лица, обладающего этой информацией.

Неформально:

Информационная безопасность – это проблема отношений между людьми: между отдельными людьми, между человеком и обществом, между сообществами людей, это проблема доверия между людьми. Одинаковых людей нет; поэтому в обществе существуют противоположные или противоречащие друг другу интересы, несовпадающие цели деятельности. Таким образом, информационная безопасность - это искусство людей совместно решать некоторые общие задачи в условиях конфликтных интересов, обезопасив себя от возможного негативного влияния посторонних лиц.

В каких сферах проявляются проблемы информационной безопасности?

- **Сфера глобальной политики, межгосударственные отношения.**
- **Военная сфера.**
- **Гуманитарная и нравственная сфера.**
- **Экономическая сфера.**
- **Финансовая сфера, сфера банковской деятельности.**
- **Техническая сфера.**

Информационная безопасность = защита информации + защита от информации

Проблемы информационной безопасности касаются каждого человека, живущего в обществе!

Основные аспекты информационной безопасности

Секретность (конфиденциальность)

– гарантии того, что содержание документа не станет известно лицам, которым документ не предназначен

Целостность

– гарантии того, что документ не был изменён в процессе движения от создателя к получателю

Подлинность

– гарантии того, что документ действительно был создан именно лицом, которое указано в качестве его автора

Целостность + **Подлинность** = **Аутентичность**

Неотказуемость

– гарантии невозможности отказаться от факта создания документа (ознакомления с документом)

Разграничение доступа

Анонимность

Др. аспекты безопасности

Политика и международные отношения

- **Разведка и контрразведка:**
  - ✓ **По назначению: военная, политическая, экономическая и пр.**
  - ✓ **По методам: агентурная разведка, радиоперехват, воздушно-космическая разведка и пр.**
  - ✓ **По территориальному принципу: внешняя разведка и оперативно-розыскная деятельность внутри государства.**

  Спецслужбы существовали и существуют практически во всех странах мира – важный инструмент добывания информации для принятия решений на государственном уровне.
- **Формирование общественного мнения при помощи СМИ:**

  пропагандистские компании, «заказные» публикации и передачи, эмоциональные оценки, отбор тем и информационных поводов, заказная и скрытая реклама, недобросовестная конкуренция.
- **«Информационная война»:**

  нагнетание обстановки на международной арене, информационное сопровождение «цветных революций» и т.п.

Информационная безопасность государства

Информационная безопасность государства **— состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.**

- **Защита информации, составляющей государственную тайну:**

  секретное делопроизводство, система допусков к информации, составляющей гостайну, обеспечение режима защиты гостайны в организациях, спецсвязь и пр.

- **Доктрина информационной безопасности РФ.**
- **Законотворчество, нормативно-правовая база:**

  федеральные законы, подзаконные акты, нормативно-технические документы (стандарты).

- **Образование и воспитание личности.**

Экономика и бизнес

- **Промышленный шпионаж и противодействие ему.**
- **Конкурентная разведка.**
- **Коммерческая тайна.**
- **Управление рисками, система менеджмента безопасности информации на предприятии.**
- **Кадровая проблема, доверие к персоналу, контроль доступа и пр.**

Финансы (1)

- **«Электронные деньги», системы розничных платежей и межбанковских расчетов, покупки в интернет-магазинах.**
- **Международные расчёты: система SWIFT (угроза отключения отдельных государств от системы международных расчетов).**
- **Дистанционное банковское обслуживание.**
- **Банковская тайна.**
- **Блокчейн и криптовалюты.**

Финансы (2)

- **Международные системы платежей по банковским картам.**

«Простые люди»

Риск стать жертвой криминальных действий, в первую очередь, мошенничества (как целенаправленного, так и нецеленаправленного):

- **При совершении покупок;**
- **При совершении банковских операций;**
- **При совершении сделок и заключении гражданско-правовых договоров (лидирует мошенничество на рынке недвижимости).**

Риск хищения и незаконного использования персональных данных и документов.

Особенно велики эти риски при использовании Интернета:

- **При поиске информации и использовании найденной информации;**
- **При работе с электронной почтой, при пользовании мессенджерами;**
- **При пользовании социальными сетями;**
- **При совершении и оплате покупок в интернет-магазинах;**
- **При использовании систем дистанционного банковского обслуживания;**

Школьники и студенты

Подвержены тем же рискам, что и все остальные: каким-то больше, каким-то меньше. Особенности:

- ✓ **активные пользователи Интернета;**
- ✓ **не хватает жизненного опыта, чтобы распознать честное и нечестное, законное и незаконное поведение (как своё собственное, так и других людей).**

Примеры: ребёнок может оказаться, как жертвой, так и агрессором:

ВЕСТИ.RU Новости Видео Фотолента Трансляции Сервисы

Live Церемония открытия XIX Всемирного фестиваля молодежи и студентов

Новости | Происшествия Все видео этой рубрики

2 сентября 2015 22:04 | Григорий Вдовин

Смерть за монитором: 22 дня компьютерных игр стоили подростку жизни

Подросток атаковал сайт администрации Курской области 830 раз

17-летний хакер пытался заразить сайт вредоносным ПО и взять его под контроль.

Поделиться

© Фото с сайта lenta.ru

Сценарии компьютерного мошенничества (1)

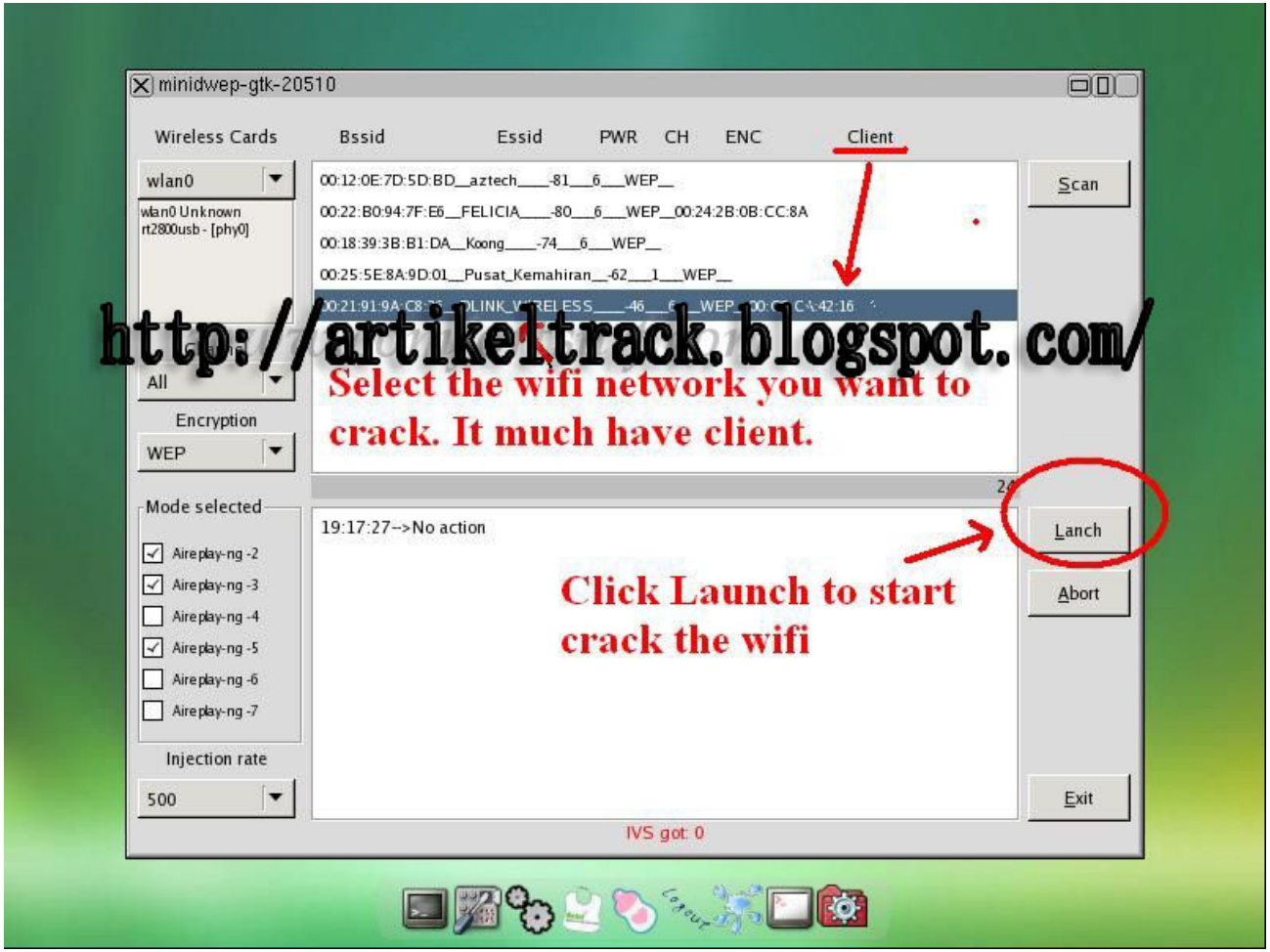
Что конкретно угрожает «простому человеку»?

Примеры:

1. **Вирус может зашифровать диск и требовать выкуп за его расшифрование:**

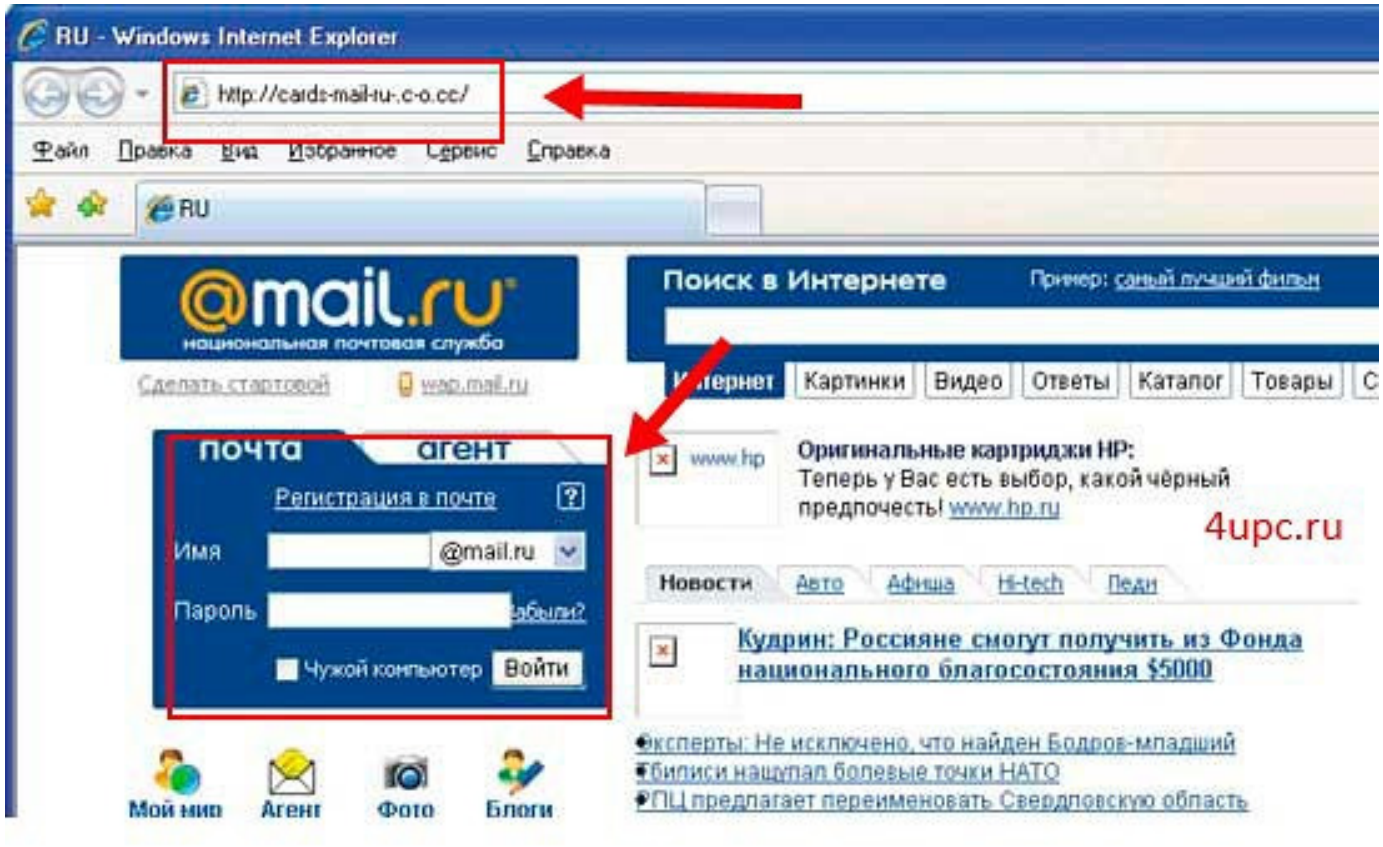
Сценарии компьютерного мошенничества (2)

2. **С помощью специальных компьютерных программ можно подобрать пароль и незаметно читать чужую электронную почту или подключаться к чужой сети Wi-Fi:**



Сценарии компьютерного мошенничества (3)

3. *«Социальная инженерия»*: фишинговый сайт может попытаться выманить данные банковской карты пользователя для последующего списания денег с карты мошенниками (по дизайну сайт имитирует сайт какой-либо известной компании либо интернет-магазина, но отличается адресом в строке браузера и на самом деле создан для сбора данных банковских карт невнимательных пользователей)



Компьютерная безопасность со стороны пользователя

Есть очень много угроз и рисков: их изучает наука о кибербезопасности. Чтобы защититься от них, начинать нужно с себя. Самое простое – соблюдать «технику безопасности» при работе на компьютере:

- **Установить антивирус (есть бесплатные, есть платные);**
- **Никогда и никому не передавать свои пароли от компьютера, сайтов, социальных сетей.**
- **Придумывать сложные пароли, не использовать в качестве пароля легкодоступную информацию (ФИО, адрес, дату рождения, почтовый индекс и пр.).**
- **Не записывать пароли на бумажках, периодически менять пароли в соц.сетях, электронной почте и пр.**
- **Не фотографировать и не выкладывать в Интернет фотографии своих документов (паспорта, свидетельства о рождении, загранпаспорта, виз и пр.), банковских карт, купленных билетов на все виды транспорта и массовые мероприятия.**
- **Не передавать по Интернету свои паспортные данные и сканы страниц паспорта без крайней необходимости – вместо этого договориться и привезти копии документов в офис в бумажном виде.**

Организационно-правовые методы обеспечения информационной безопасности

Государство также не оставляет людей один на один с угрозами информационной безопасности.

Законы РФ в сфере информационной безопасности:

- ✓ **Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.07.2017) "Об информации, информационных технологиях и о защите информации"**
- ✓ **Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" с изменениями, внесенными Федеральным законом от 29.07.2017 N 223-ФЗ**
- ✓ **Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»**

✓ Финансовая безопасность (1)

«Технику безопасности» также нужно соблюдать и при пользовании банковскими услугами:

При использовании банковских карт:

- **Никогда не записывать PIN-коды от банковских карт и никому не сообщать их, даже близким родственникам;**
- **Не хранить банковские карты вместе с паспортом (загранпаспортом);**
- **Никому и никогда не сообщать код из трёх цифр, написанный с обратной стороны банковской карты (для перевода средств на карту достаточно знать только 16-значный номер карты на лицевой стороне).**
- **Обязательно подключить СМС-информирование об операциях по банковской карте;**
- **При получении СМС об операции с банковской картой, которую не совершали, немедленно обратиться в банк и заблокировать карту до выяснения обстоятельств.**

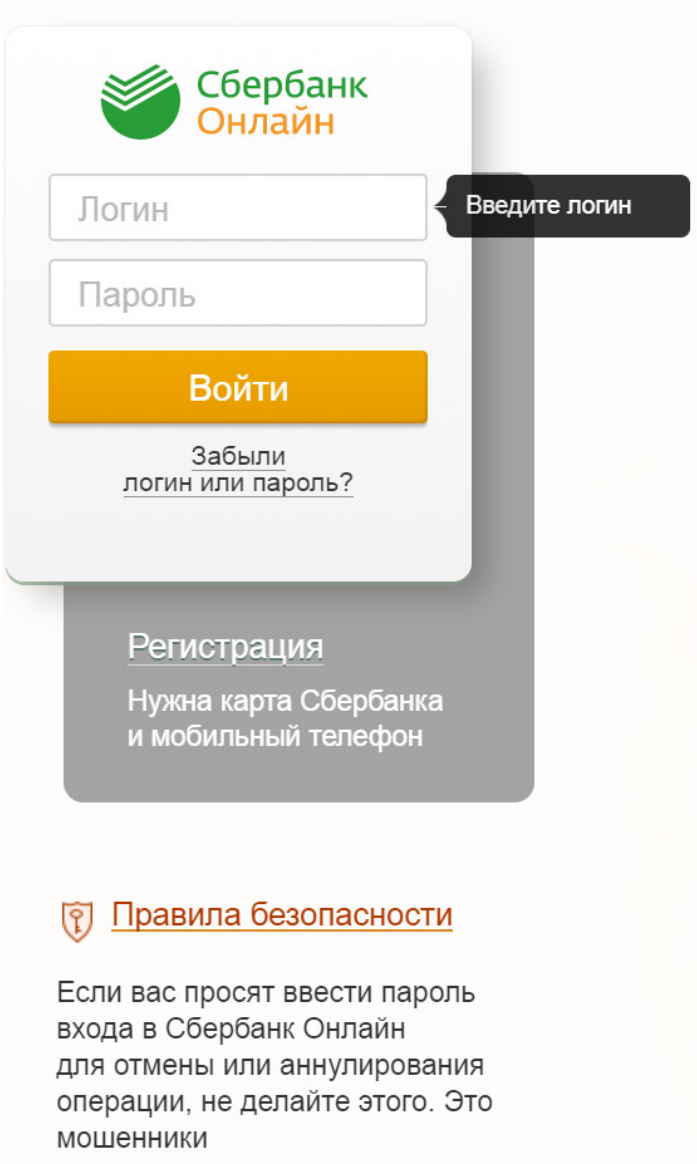
Финансовая безопасность со стороны пользователя (2)

При использовании систем дистанционного банковского обслуживания:

- **Обязательно иметь установленный на компьютере антивирус, без этого дистанционным банковским обслуживанием не пользоваться!**
- **Никому не сообщать пароль от учетной записи в системе ДБО!**

При пользовании мобильным телефоном, мессенджерами и социальными сетями:

- **Не реагировать на мошеннические сообщения и (или) звонки, полученные по СМС-каналу, в мессенджер, в соц.сетях и по любым другим каналам (или обязательно перепроверять такие сообщения):**
- **На сайте любого банка должны быть указаны телефоны, с которых могут звонить сотрудники с рекламными сообщениями, но и им не следует сообщать никаких персональных данных.**



Финансовая безопасность со стороны кредитно-финансовых организаций

1. **Мониторинг транзакций.**
2. **Одноразовые пароли для подтверждения операций.**
3. **СМС-информирование об операциях по счету.**
4. **«Горячая линия» для обращений клиентов.**
5. **Все важные операции – только в офисе при личном присутствии клиента.**

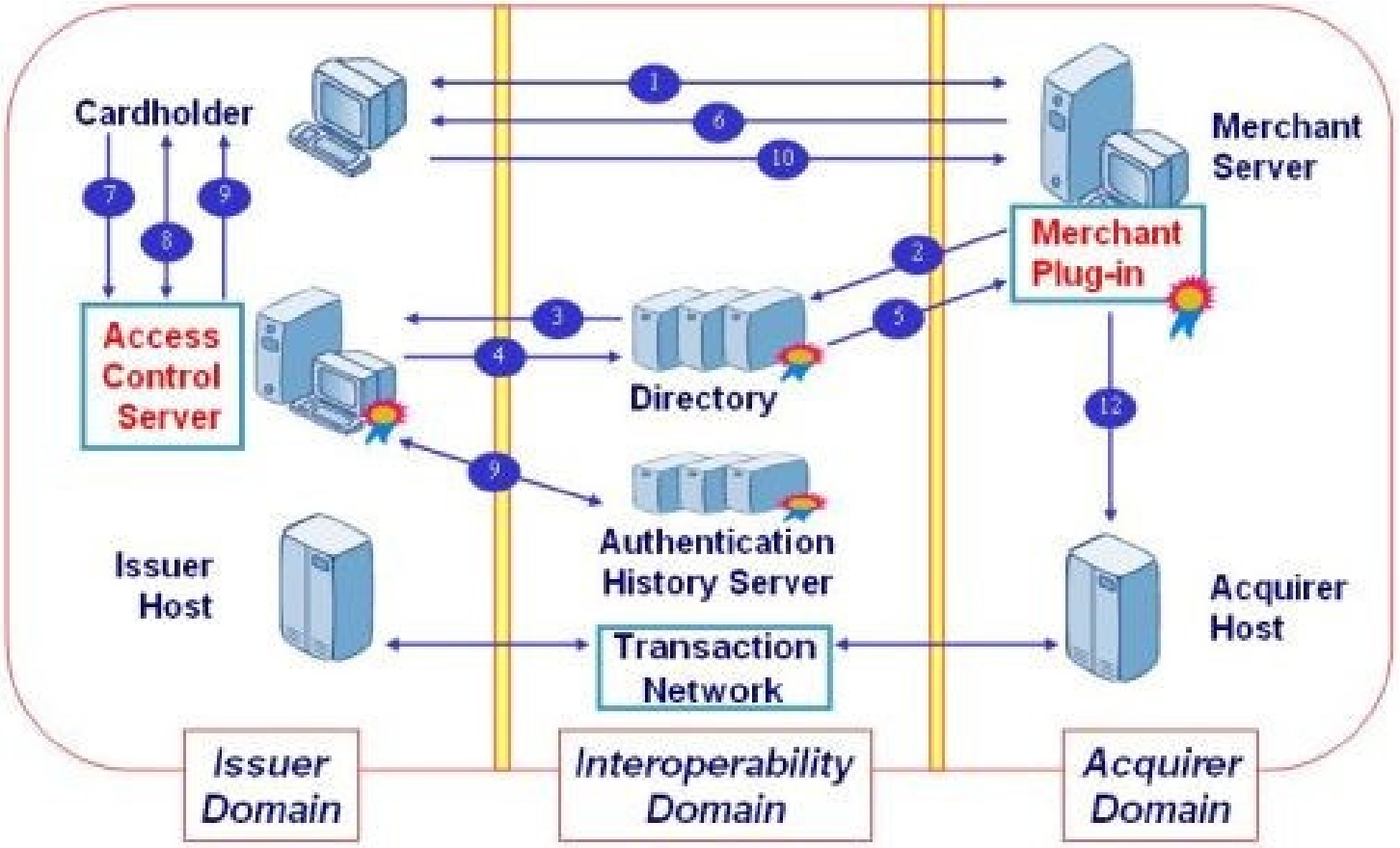


Рис. 2: Проведение онлайновой покупки

Методы защиты информации

Физические

Организационные

Организационно-правовые (юридические)

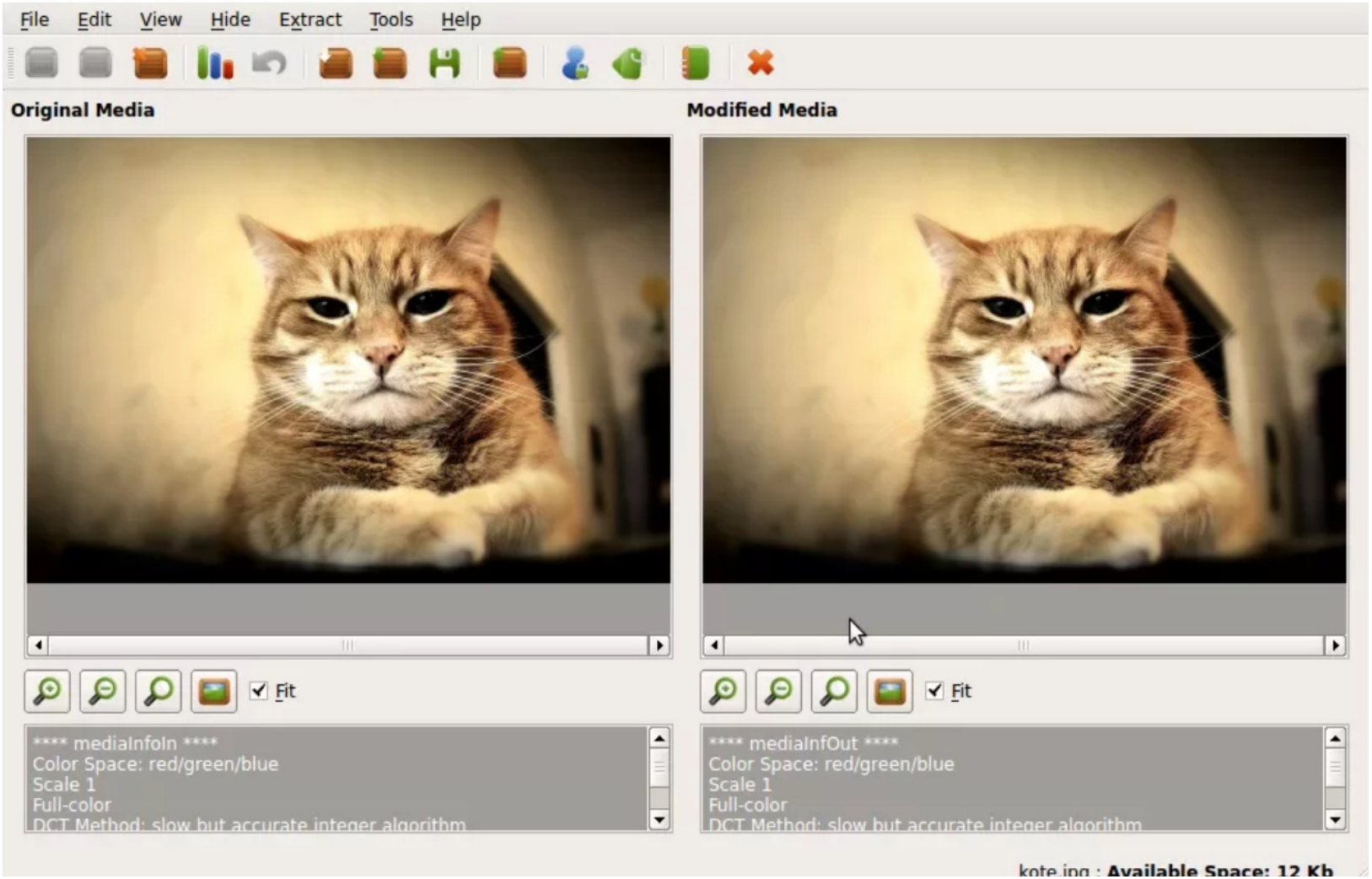
Стеганография

(греч. «письмо под крышей»)
– наука о методах сокрытия самих фактов существования и передачи каких-либо сообщений.

Криптография

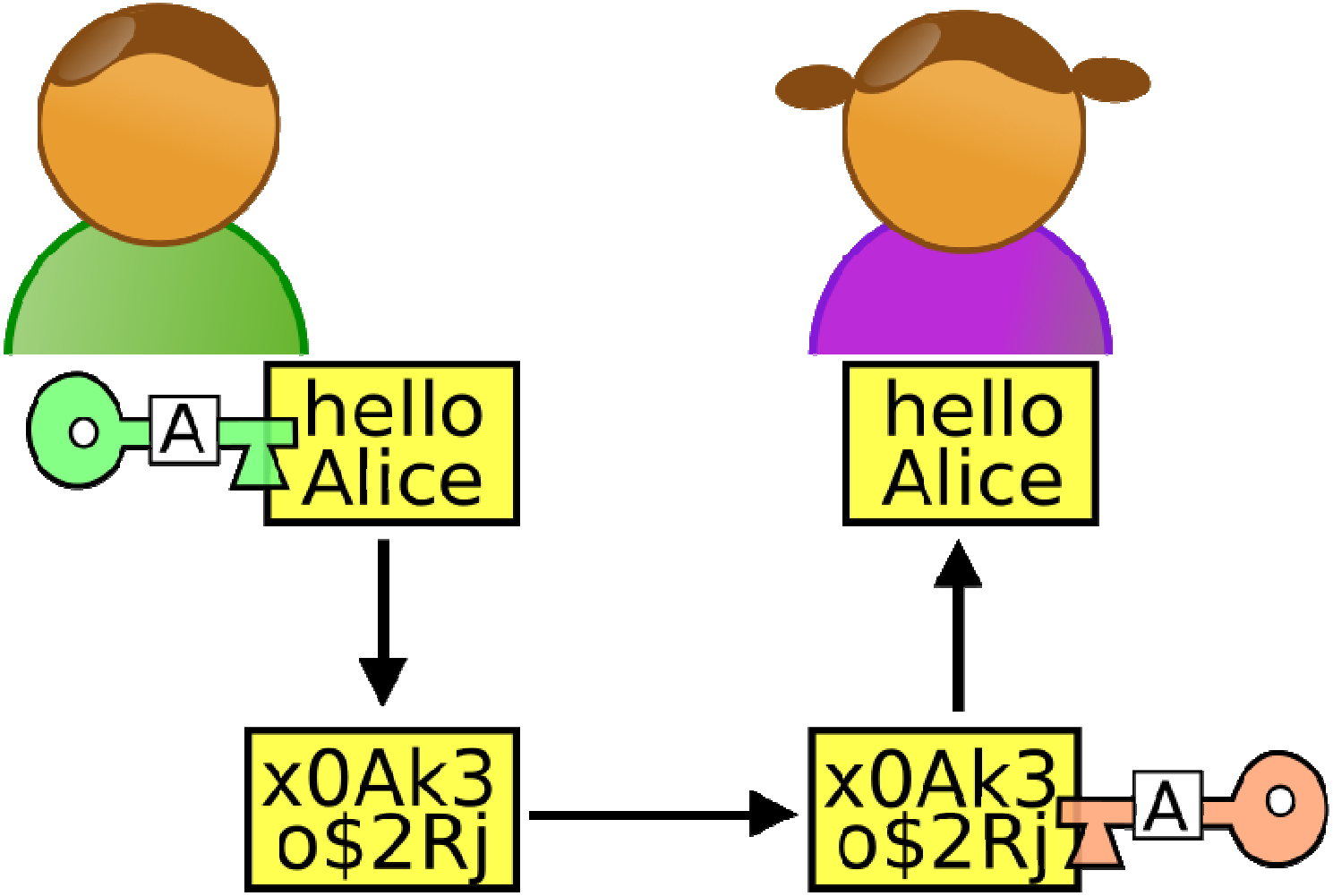
(греч. «тайное письмо»)
– самый надежный, эффективный, проверенный метод, **НО** при условии грамотного его применения.

Стеганография



Информация скрытно внедряется в файл другого типа (например, в графический файл)

Криптография



Текст преобразуется в нечитаемую, бессмысленную для человека форму

Будущее информационной безопасности

- **Применение искусственного интеллекта для обнаружения и предотвращения вторжений, для предотвращения мошенничества, для обнаружения спама и фишинговых сайтов.**

- **Применение блокчейн-технологий и «умных контрактов» для обеспечения доверия между сообществами пользователей, изначально не доверяющих друг другу.**

- **Информационная безопасность «Интернета вещей».**

Рекомендуемая литература

1. **Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия – Телеком, 2006.**
2. **Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. В 2-х томах. Том 2 –Средства защиты в сетях. – М.: Горячая линия – Телеком, 2008.**
3. **Малюк А.А., Полянская О.Ю., Алексеева И.Ю. Этика в сфере информационных технологий. – М.: Горячая линия – Телеком, 2011.**
4. **Малюк А.А. Защита информации в информационном обществе. – М.: Горячая линия – Телеком, 2015.**
5. **Малюк А.А. Глобальная культура кибербезопасности. – М.: Горячая линия – Телеком, 2017.**
6. **Малюк А.А., Горбатов В.С., Королев В.И. и др. Введение в информационную безопасность. – М.: Горячая линия – Телеком, 2011. – 288 с.**
7. **Ефимова Л. Л. Информационная безопасность детей. Российский и зарубежный опыт. – М.: Юнити, 2018. – 239 с.**
8. **Мельников В.П. Информационная безопасность: учебник для СПО. – М.: КноРус, 2018. – 270 с.**
9. **Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: Инфра-М, 2017. – 321 с.**

Спасибо за внимание!

Вопросы?