СГЮА

Дисциплина «Информационные технологии в профессиональной деятельности»

© доцент кафедры информационного права
и цифровых технологий,
кандидат социологических наук
Данилова Мария Анатольевна, 2021

Тема 6. Защита информации в компьютерных системах

План лекции

1. **Информационная безопасность. Понятие защиты информации. Принципы защиты информации. Категории защищаемой информации.**
2. **Угрозы, риски и пути утечки компьютерной информации.**
3. **Меры защиты информации. Классификация мер защиты (организационные, законодательные, программно-технические).**
4. **Программно-технические меры защиты информации.**

Информационная безопасность

Информационная безопасность — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Находиться в безопасности – значит находиться в таких условиях, которые можно контролировать в процессе своей деятельности.

Понятие защиты информации. Принципы защиты информации

Защита информации (информационных систем) - сохранение информации и данных, которое обеспечивает:

Конфиденциальность - защита важной (чувствительной, критической, ценной, конфиденциальной) информации от несанкционированного доступа.

Целостность — защита точности и полноты информации и программного обеспечения.

Доступность информации — обеспечение чтения информации, ее обработки (в частности, копирование, модификация и даже уничтожение) и основных услуг авторизованным пользователям в нужное для них время.

Категории защищаемой информации

- **Жизненно важная информация** — незаменимая для функционирования предприятия.
- **Важная информация** - та, которую можно восстановить, но процесс восстановления труден, длителен, связан с большими затратами.
- **Полезная информация** - нужная информация, которую в случае потери будет трудно восстановить, но и без нее возможна эффективная работа.
- **Несущественная информация** — та, которой организация не дорожит, незаконный потребитель (другое лицо или организация-нарушитель правил доступа к информации) иногда заинтересован даже в информации, которая для владельца свою актуальность и ценность потеряла.
- **Ценная информация** — информация, нарушение защиты которой внесет коммерческий ущерб.

Угрозы, риски и пути утечки компьютерной информации

Угроза безопасности в результате применения ИТ и ИС — это потенциальное действие или событие, которое может стать реальностью и привести к убыткам или нанести ущерб организации.

Информационный риск — это оцениваемая вероятность понести ущерб или утрату в результате осуществления угрозы; связан с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

Угрозы в сфере информационных технологий разделяют на *активные* и *пассивные*.

Пассивные угрозы связаны с нарушением защиты системы и утечкой информаций, использованием ее конкурентами, преступниками или сотрудниками в целях, которые вредят деятельности организации, но не сопровождаются повреждением информации.

Активные угрозы опасны повреждением информации, сбоями ее обработки и передачи.

Источники угроз в отношении компьютерной информации в порядке убывания рисков (вероятности):

1. Аппаратные и программные неисправности компьютерной системы, внезапное отключение питания; старение, повреждение носителей информации.
2. Намеренные действия персонала по хищению, повреждению информации.
3. Некомпетентность персонала.
4. Действие вредоносных программ.
5. Действие хакеров.
6. Организованные преступные группы.
7. Шпионаж, экономический, политический, военный.

Пути утечки компьютерной информации

1. **Несанкционированный доступ** в форме непосредственного общения к аппаратным и программным средствам компьютерных систем обработки (несанкционированное копирование и удаление), копирование, модификация защиты, прямое хищение СКТ или носителей.

2. **Удаленный перехват** побочного электромагнитного излучении и наводок от компьютера на расстоянии и расшифровка.

3. **Внедрение программных и технических средств** в автоматизированные системы («жучки-закладки» для отправки сигналов на расстояние, специальные программы: «диверсанты», «шпионы» или вирусы).

4. **Перехват информации**, передаваемой по сетям.

Меры защиты информации

Правовой уровень

Организационный уровень

Технический уровень

Административные мероприятия

1. Разработка политики безопасности
2. Разработка средств управления безопасностью
3. Распределение ответственности
4. Обучение персонала
5. Контроль за соблюдением политики безопасности

Физические мероприятия

- **Внешняя защита**
- **Охрана**
- **Ограничение доступа**
- **Визуальное наблюдение**

- **Распознавание**
- **Опознание людей**
- **Идентификация технических средств**

- **Внутренняя защита**

Управление доступом к компьютерной системе

Авторизация *– процедура, по которой пользователь при входе в систему опознается и получает права доступа, разрешенные системным администратором, к вычислительным ресурсам*

Идентификация *– предоставление компьютеру идентификатора (имя пользователя, логин)*

Аутентификация *- подтверждение подлинности пользователя*

Аутентификация производится предоставлением

1. ***Некоторой секретной информации*** (пароль или некоторый код)
2. ***Некоторого технического устройства*** (пластиковая карта, электронный ключ)
3. ***Некоторых биологических особенностей*** (дактилоскоия, цвет глаз и т.д.)

Разграничение доступа

Формы хранения паролей в компьютерах:

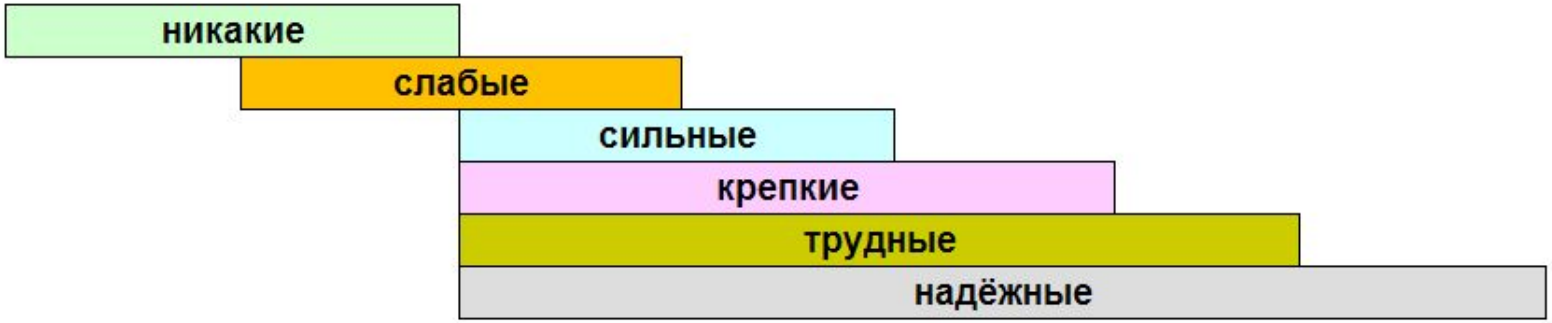
- **цифровая** – коды символов, составляющих пароль, преобразуются по какому–либо закону, обычно перекодируются и в окнах диалога подменяются звездочками;

- **шифрованная** – пароль обычно удлиняют, добавляя в него случайное число; удлиненный пароль шифруется и раскрыть его не зная алгоритмы удлинения и шифрования практически невозможно;

- **сжатая** – пароль сначала удлиняют, а затем с помощью специальных хэш–функций сжимают, получают хэш–образ пароля, который и хранят во внешней памяти

Классификация паролей

0	1	2	3	4	5	6
Одинаковые буквы одного алфавита или только цифры	Словарное слово	Строчные и прописные буквы на одном из языков	Символы не образуют словарное слово	Цифры совместно с символами	Символы двух языков	Специальные символы



Правила использования паролей

1. Количество символов в пароле 6 – 10.
2. В пароле должна отсутствовать смысловая нагрузка.
3. Обязательно должен быть определен максимальный срок действия пароля.
4. Обязательно должно быть определено количество повторных попыток набора пароля.
5. Усложнение паролей за счет введения в них символов двух языков, цифр, специальных символов.
6. Обязательное запоминание пароля без фиксации на носителе (бумажном, электронном или ином).

Виды паролей

1. Пароль на открытие файлов с документами
2. Пароль на изменение режима доступа к документу
3. Пароль на доступ к архиву.
4. Пароль на доступ в операционную систему.
5. Пароль на отмену спящего режима или на выключение режима хранителя экрана монитора.
6. Пароль на доступ к локальным сетевым ресурсам.
7. Пароль на доступ к глобальным сетевым ресурсам или сервисам

Преобразование информации к нечитаемому виду, исключающее ее несанкционированное раскрытие

Существуют три наиболее распространенных способа умышленного искажения читаемой информации.

- **Сжатие (архивирование) информации** – это процесс уменьшения объема файла или папки. Дополнительными преимуществами сжатия файлов являются возможность установления пароля на открытие (просмотр) архива и невозможность проникновения вирусов в некоторые архивы.

- **Перекодирование информации**. Компьютер отображает символы на экране в соответствии с заложенной в него кодовой страничкой (таблица соответствия символ – код). Если установить на компьютер или создать еще и свою кодовую таблицу, то можно после набора текста его перекодировать, т. е. записать в файл коды символов по новой таблице.

- **Шифрование информации** – в отличие от перекодирования позволяет избавиться от статистических свойств языка. При шифровании один и тот же символ исходного текста может быть закодирован разными кодами.

Пример шифрования

1 - А
2 - Б
3 - В
4 – Г
5 – Д
6 – Е
7 – Ж
8 – З
9 - И

В	А	З	А
3	1	8	1

Прибавим двойку к коду буквы

5	3	10	3
Д	В	К	В

Существуют две основные схемы шифрования:

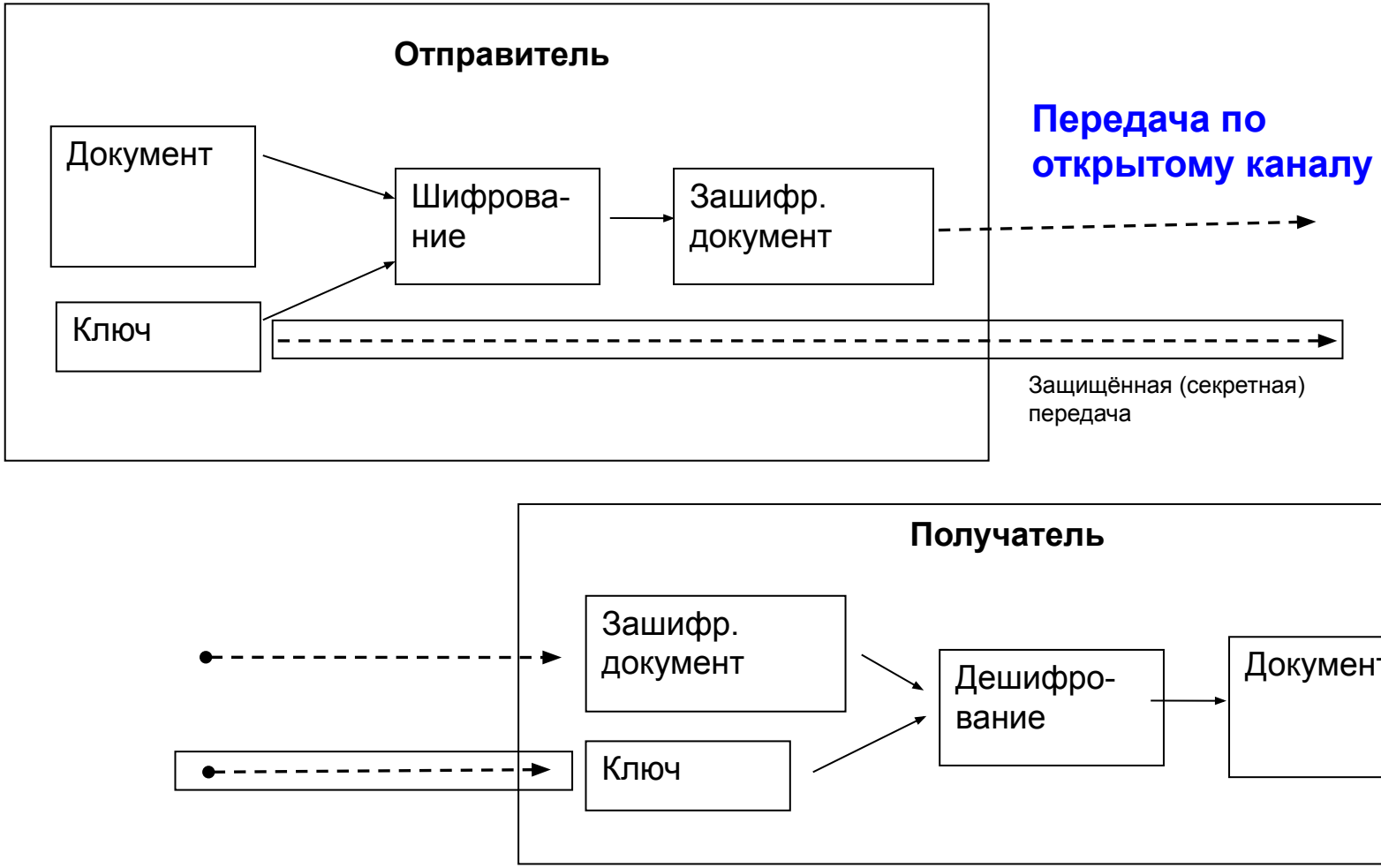
симметричная – использует для шифрования и дешифрования один и тот же ключ.

- **Недостаток – для работы дешифратора нужен тот же ключ, что и для шифрования.**
- **Достоинством симметричного шифрования является высокое быстродействие (важно при работе в сети).**

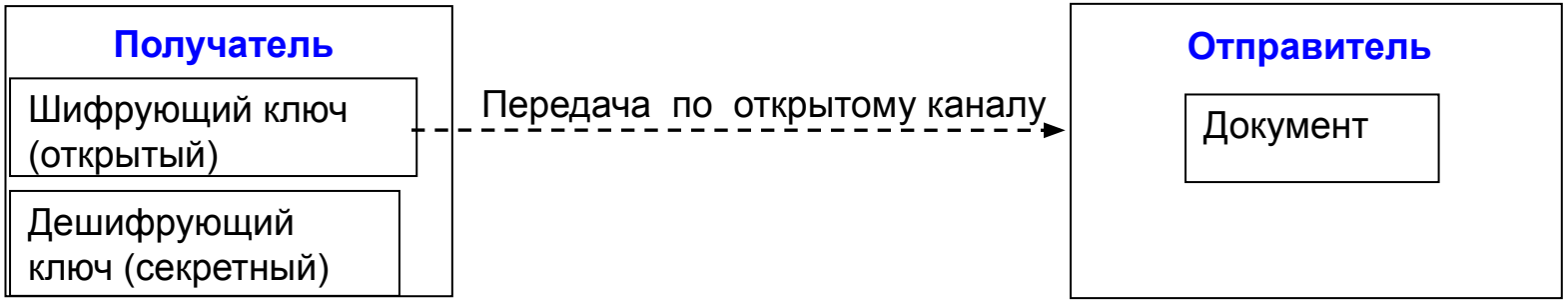
несимметричная – использует для работы два ключа, один для шифрования, другой для дешифрования.

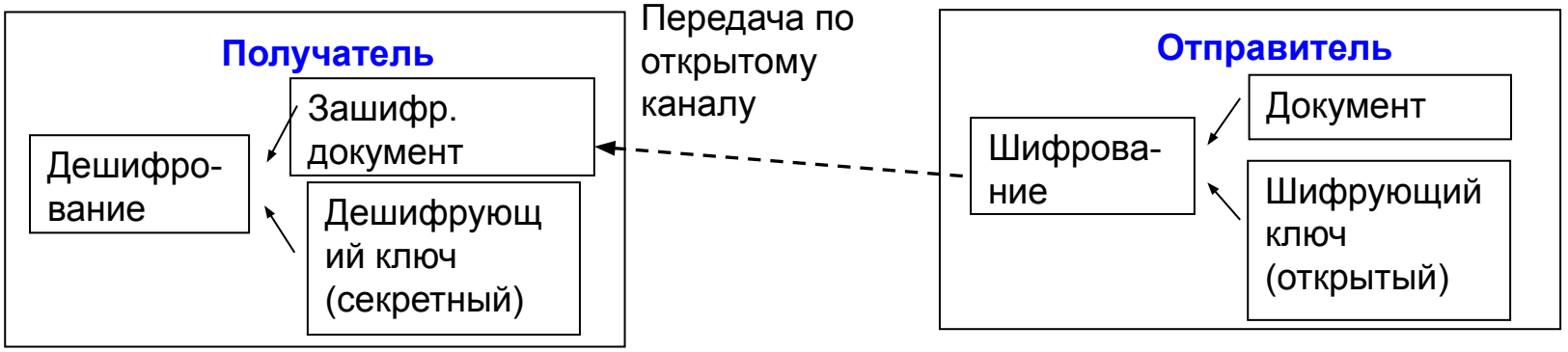
- **Недостаток несимметричных схем шифрования – значительно более медленная работа.**
- **Достоинства – возможность сделать второй ключ открытым, с возможностью его передачи.**

Симметричная схема шифрования



Асимметричная схема шифрования





Примеры использования несимметричной схемы шифрования

Электронная почта. Отправитель шифрует свое письмо открытым ключом получателя, но только получатель с помощью своего закрытого ключа может прочитать полученное письмо.

Электронная подпись - определяют авторство электронного документа и факт внесения в него изменений после подписания. Автор документа шифрует часть документа или весь его целиком своим закрытым, никому больше не известным ключом, и выкладывает документ для всеобщего обозрения. Содержимое документа или его зашифрованной части может расшифровать каждый, кто обладает открытым ключом.

электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Проверка подлинности открытого ключа

Злоумышленник может перехватить передачу открытого ключа и подменить его своим ключом.

Чтобы этого избежать, существуют удостоверяющие центры (УЦ). Эти центры обеспечивают своих клиентов надлежащим программным обеспечением, а также создают для них ключи ассиметричного шифрования и ключи для работы с ЭЦП.

При этом секретный ключ безопасным способом передаётся пользователю, а вместе с открытым ключом пользователь получает сертификат.

Квалифицированной электронной подписью является **электронная подпись**, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:
1) **ключ проверки электронной подписи** указан в квалифицированном сертификате;
2) для создания и проверки электронной подписи используются **средства электронной подписи**, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.
Федеральный закон от 6 апреля 2011 г. N 63-ФЗ

Хэширование информации

Хэш – набор символов фиксированной длины, который вычисляется для электронного документа произвольного размера. Размер хэша обычно невелик – несколько десятков символов.

При вычислении хэша выполняются следующие требования:

1. Самые незначительные изменения в документе приводят к генерации отличающихся хэшей;
2. Невозможно по хэшу восстановить документ (т.е. это необратимое преобразование);

Хэширование - преобразование, которое не шифрует исходный текст,

т.е. не приводит его к нечитаемому виду,

а создает очень короткий по сравнению с исходным текстом «слепок»

– набор символов, который используется

как новый реквизит передаваемого сообщения.

Как удалить информацию с компьютера

1. **Воспользоваться специальными утилитами**

Eraser HDD Auslogics BootSpeed

Удаляем защищённые и заблокированные файлы **Unlocker**

Удаляем сохранённые в браузере пароли

Internet Explorer - *Сервис - Свойства обозревателя – Содержание - Автозаполнение -Параметры - Удаление истории автозаполнения*

Chrome - Настройки - Показать дополнительные настройки - Пароли и формы - Управление сохранёнными паролями.

FireFox - Настройки - Защита - Сохранённые пароли.

Вредоносные программы

Статья 273 Уголовного Кодекса Российской Федерации («Создание, использование и распространение вредоносных программ для ЭВМ») вводит следующее определение:

«… программы для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети…»

Malware, **malicious software**

Классификация вредоносных программ

1. Троянские программы («троянские кони», «троянцы», «трояны»)
2. Компьютерные вирусы
3. Сетевые черви
4. Хакерские утилиты и прочие вредоносные программы

Троянские программы.

Создаются для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. Представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Вирусы и черви.

Обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.

Вирусы, в свою очередь, делятся

по типу заражаемых файлов (файловые, загрузочные, макро-,);

по способу прикрепления к файлам и т. д.

Троянские программы

Создаются для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей.

Не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Некоторые действия троянцев

- **Загрузка из сети (*downloader*).**
- **Распаковка другой вредоносной программы, уже содержащейся внутри файла (*dropper*).**
- **Кража паролей, учетных записей и др.**
- **Блокировка запуска ОС, блокировка антивирусных программ**
- **Участие в DDoS – атаках**
- **Распространение спама**

Сетевые черви

Проникают на компьютер через локальные и глобальные сети, способны создавать свои копии.

Используют уязвимости в программном обеспечении. Применяются для рассылки спама или для DDoS-атак.

Размножаются и распространяются с огромной скоростью и могут вызвать эпидемии.

Могут работать «в связке» с троянцами.

Компьютерные вирусы

Способы проникновения:

- **Сменные накопители**
- **Электронная почта,**
- **Интернет**

Источники заражения:

- **Исполняемые программы**
- **Веб-страницы, содержащие активное содержимое**
- **Вложенные файлы электронной почты**
- **Файлы Office, Flash и других программ, содержащие макросы.**

Компьютерные вирусы

Компьютерная программа или код программы, выполняющая несанкционированные пользователем действия, имеющая способность к размножению.

Вирусы делятся :

по типу заражаемых файлов (файловые, загрузочные, макро-,);

по поражаемым операционным системам;

по способу прикрепления к файлам и т. д.

Прочие вредоносные программы

Предназначаются для автоматизации создания других вирусов, червей или троянских программ, организации DDoS-атак на удаленные сервера, взлома других компьютеров, отслеживания действий на клавиатуре и т.п.


Угрозы
0.029
0.0143
0.0813
0.1424
0.7331
трояны
вирусы
черви
рекламное/шпионское П/О
другое

Категории 20 сайтов, откуда пользователи чаще всего переходили по вредоносным ссылкам, % переходов.

СГЮА

Спасибо за внимание!