

# ПРЕЗЕНТАЦИЯ ПО ТЕМЕ:

## Средства защиты информации.

Выполнил: Студент группы 1-БУ-15

Латынцев В.В.

- В информатике в наибольшей степени рассматриваются основные виды защиты информации при работе на компьютере и в телекоммуникационных сетях.
- Компьютеры — это технические устройства для быстрой и точной (безошибочной) обработки больших объёмов информации самого разного вида. Но, несмотря на постоянное повышение надёжности их работы, они могут выходить из строя, ломаться, как и любые другие устройства, созданные человеком. Программное обеспечение также создается людьми, способными ошибаться.

- Конструкторы и разработчики аппаратного и программного обеспечения прилагают немало усилий, чтобы обеспечить **защиту** информации:
- от сбоев оборудования;
- от случайной потери или искажения информации, хранящейся в компьютере;
- от преднамеренного искажения, производимого, например, компьютерными вирусами;
- от несанкционированного (нелегального) доступа к информации (её использования, изменения, распространения).
- К многочисленным, далеко не безобидным ошибкам компьютеров добавилась и компьютерная преступность, грозящая перерасти в проблему, экономические, политические и военные последствия которой могут стать катастрофическими.

- При защите информации от **сбоев оборудования** используются следующие основные методы:
- периодическое **архивирование** программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);
- автоматическое **резервирование** файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.

- **Защита от случайной** потери или **искажения** информации, хранящейся в компьютере, сводится к следующим методам:
- автоматическому запросу на подтверждение команды, приводящей к изменению содержимого какого-либо файла. Если вы хотите удалить файл или разместить новый файл под именем уже существующего, на экране дисплея появится диалоговое окно с требованием подтверждения команды либо её отмены;
- установке специальных атрибутов документов. Например, многие программы-редакторы позволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;
- возможности отменить последние действия. Если вы редактируете документ, то можете пользоваться функцией отмены последнего действия или группы действий, имеющейся во всех современных редакторах. Если вы ошибочно удалили нужный файл, то специальные программы позволяют его восстановить, правда, только в том случае, когда вы ничего не успели записать поверх удаленного файла;
- разграничению доступа пользователей к ресурсам файловой системы, строгому разделению системного и пользовательского режимов работы вычислительной системы. Защита информации от преднамеренного искажения часто еще называется защитой от вандализма.

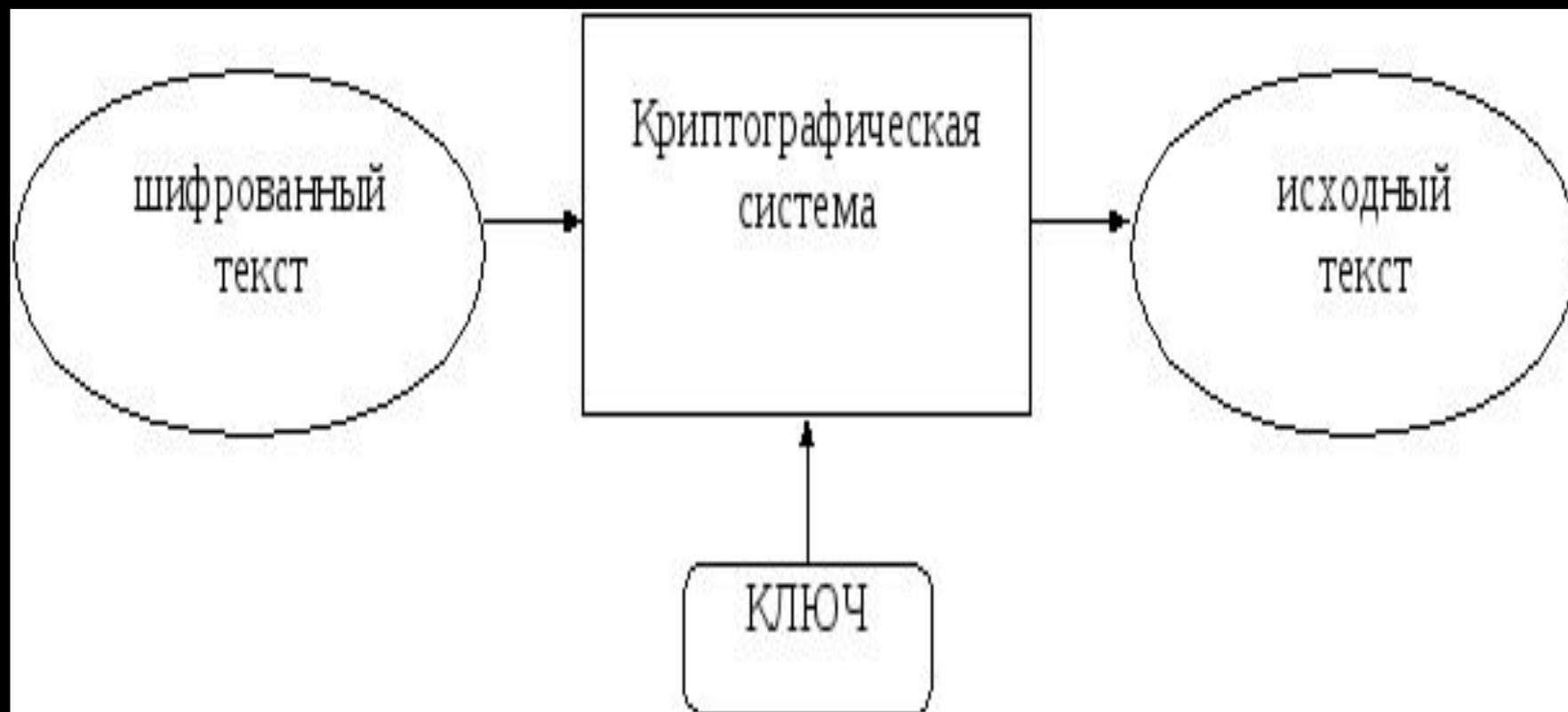
- **Компьютерный вирус** представляет собой специально написанный небольшой по размерам фрагмент программы, который может присоединяться к другим программам (файлам) в компьютерной системе. Например, вирус может вставить себя в начало некоторой программы, так что каждый раз при выполнении этой программы первым будет активизироваться вирус. Во время выполнения вирус может производить намеренную порчу, которая сейчас же становится заметной, или просто искать другие программы, к которым он может присоединить свои копии. Если «заражённая» программа будет передана на другой компьютер через сеть или дискету, вирус начнёт заражать программы на новой машине, как только будет запущена переданная программа. Таким способом вирус переходит от машины к машине. В некоторых случаях вирусы потихоньку распространяются на другие программы и не проявляют себя, пока не произойдёт определённое событие, например, наступит заданная дата, начиная с которой они будут «разрушать» всё вокруг. Разновидностей компьютерных вирусов очень много. Среди них встречаются и невидимые, и самомодифицирующиеся.

- Для защиты от вирусов можно использовать:
- общие методы защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные антивирусные программы.



- Многие методы защиты информации от несанкционированного (нелегального) доступа возникли задолго до появления компьютеров.
- Одним из таких методов является шифрование.
- Проблема защиты информации путем её преобразования, исключающего её прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптологии (kryptos — тайный, logos — наука) — ровесница истории человеческого языка. Более того, письменность сама по себе была вначале криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры. Криптология разделяется на два направления — криптографию и криптоанализ. Цели этих направлений прямо противоположны. Криптография занимается поиском и исследованием методов шифрования информации. Она даёт возможность преобразовывать информацию таким образом, что её прочтение (восстановление) возможно только при знании ключа. Сфера интересов криптоанализа — исследование возможностей расшифровки информации без знания ключей.

- **Ключ** — информация, необходимая для беспрепятственного шифрования и дешифрования текста.



- Первые криптографические системы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке уже использовал шифр, получивший его имя. Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Появление вычислительной техники ускорило разработку и совершенствование криптографических методов.

## Примеры шифров замены

*Шифр Цезаря.* Заключается в замене букв открытого текста (верхней строки) на буквы (нижней строки) в соответствии с таблицей:

↑	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Например, слово CAESAR шифровалось бы как:

FDHVDU

- Основные направления использования этих методов — передача конфиденциальной информации по каналам связи (например, по электронной почте), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.
- Проблема использования криптографических методов в современных информационных системах становится в настоящее время особенно актуальной. С одной стороны, расширилось использование телекоммуникационных сетей, по которым передаются большие объёмы информации государственного, коммерческого, военного и частного характера, не допускающего возможность доступа к ней посторонних лиц. С другой стороны, появление новых мощных аппаратных и программных средств, эффективных технологий дешифрования снизило надёжность криптографических систем, ещё недавно считавшихся практически не раскрываемыми.

- Другим возможным методом защиты информации от несанкционированного доступа является применение **паролей**.
- Пароли позволяют контролировать доступ как к компьютерам, так и к отдельным программам или файлам. К сожалению, иногда пароль удается угадать, тем более, что многие пользователи в качестве паролей используют свои имена, имена близких, даты рождения.



- Существуют программные средства от «вскрытия» паролей. Чтобы противостоять попыткам угадать пароль, операционные системы могут быть спроектированы таким образом, чтобы отслеживать случаи, когда кто-то многократно употребляет неподходящие пароли (первый признак подбора чужого пароля). Кроме того, операционная система может сообщать каждому пользователю в начале его Сеанса, когда в последний раз использовалась его учётная запись. Этот метод позволяет пользователю обнаружить случаи, когда кто-то работал в системе под его именем. Более сложная защита (называемая ловушкой) — это создание у взломщика иллюзии успешного доступа к информации на время, пока идет анализ, откуда появился этот взломщик.

- Одной из распространённых форм нарушения информационного права является незаконное копирование программ и данных, в частности находящихся на коммерчески распространяемых носителях информации.
- Для предотвращения нелегального копирования файлов используются специальные программно-аппаратные средства, например «электронные замки», позволяющие сделать с дискеты не более установленного числа копий, или дающие возможность работать с программой только при условии, что к специальному разъёму системного блока подключено устройство (обычно микросхема), поставляемое вместе с легальными копиями программ. Существуют и другие методы защиты, в частности, административные и правоохранные.
- Обеспечить надёжную защиту информации может только применение комплекса самых разнообразных методов.

# ИСТОЧНИКИ:

- Макарова Н.В. Программа по информатике (системно-информационная концепция). К комплекту учебников по информатике 5-11 класс. Санкт-Петербург: Питер.2000г.
- Информатика. 5-11 класс. /Под ред. Н.В. Макаровой. – СПб.: Питер, 2001
- Коляда М.Г. Окно в удивительный мир информатики. ИКФ «Сталкер»,1997
- Шафрин Ю.А. Основы компьютерной технологии. Учебное пособие для 7 – 11 классов по курсу «Информатика и вычислительная техника» - Москва: АБФ,1996
- Ефимова О.В., Моисеева М.В., Ю.А. Шафрин Практикум по компьютерной технологии. Примеры и упражнения. Пособие по курсу «Информатика и вычислительная техника» - Москва: АБФ,1997
- Горячев А., Шафрин Ю. Практикум по информационным технологиям. М.: Лаборатория базовых знаний, 2001
- Семакин И.Г., Шеина Т.Ю. Преподавание курса информатики в средней школе. М.: Лаборатория базовых знаний, 2002
- Симонович С.В., Евсеев Г.А. Практическая информатика. Учебное пособие для средней школы. Универсальный курс. – Москва: АСТ-ПРЕСС: Информ-Пресс, 1998
- Симонович С.В. Компьютер в вашей школе. М.: АСТ-ПРЕСС: Информком-Пресс, 2001
- Симонович С.В., Евсеев Г.А. Занимательный компьютер. Книга для детей, учителей и родителей. Москва: АСТ-ПРЕСС: Информком-Пресс, 2002

<http://www.metod-kopilka.ru>