Конспект урока на тему

«Защита информации»

**Тип урока:**

Урок изучения новых знаний

**Образовательная цель урока:**

Изучение и первичное закрепление знаний;
Актуализация ведущих знаний;
Ввести понятия: защита информации, компьютерный вирус;
Рассмотреть различные способы защиты информации.

**План урока:**

1.  Организационная часть (приветствие, проверка присутствующих учащихся, запись даты и темы в тетрадь)

3 мин.

2.  Объяснение нового материала

30 мин.

3.  Самостоятельная работа учащихся

10 мин.

4.  Домашнее задание

2 мин.

**Конспект урока:**

Человеку свойственно ошибаться. Любое техническое устройство также подвержено сбоям, поломкам, влиянию помех. Ошибка может произойти при реализации любого информационного процесса. Велика вероятность ошибки при кодировании информации, её обработке и передаче. Результатом ошибки может стать потеря нужных данных, принятие ошибочного решения, аварийная ситуация (слайд 1).

**Пример.** *Вы неверно выразили свою мысль и невольно обидели собеседника.
Вы произнесли не то слово, которое хотели (оговорились), и ваши слушатели вас не поняли. Вы правильно выбрали метод решения задачи на контрольной работе, но ошиблись в арифметических расчётах и в результате получили ошибочный ответ.*

Чем больше информации передаётся и обрабатывается, тем труднее избежать ошибок. В обществе хранится, передаётся и обрабатывается огромное количество информации и отчасти поэтому современный мир очень хрупок, взаимосвязан и взаимозависим. Информация, циркулирующая в системах управления и связи, способна вызвать крупномасштабные аварии, военные конфликты, дезорганизацию деятельности научных центров и лабораторий, разорение банков и коммерческих организаций. Поэтому информацию нужно уметь защищать от искажения, потери, утечки, нелегального использования.

**Пример.** *Компьютерная система ПВО Североамериканского континента однажды объявила ложную ядерную тревогу, приведя в боевую готовность вооружённые силы. А причиной послужил неисправный чип стоимостью 46 центов — маленький, размером с монету, кремниевый элемент.*

**Пример.** *В 1983 году произошло наводнение в юго-западной части США. Причиной стал компьютер, в который были введены неверные данные о погоде, в результате чего он дал ошибочный сигнал шлюзам, перекрывающим реку Колорадо.*

**Пример.** *В 1971 году на нью-йоркской железной дороге исчезли 352 вагона. Преступник воспользовался информацией вычислительного центра, управляющего работой железной дороги, и изменил адреса назначения вагонов. Нанесённый ущерб составил более миллиона долларов.*

Развитие промышленных производств принесло огромное количество новых знаний, и одновременно возникло желание часть этих знаний хранить от конкурентов, защищать их. Информация давно уже стала продуктом и товаром, который можно купить, продать, обменять на что-то другое. Как и всякий товар, она требует применения специальных методов для обеспечения сохранности.

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 постоянной 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 (слайд 2):

* 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.

Проблема вандализма заключается в появлении таких бедствий, как компьютерные вирусы и компьютерные червяки. Оба этих термина придуманы более для привлечения внимания общественности к проблеме, а не для обозначения некоторых приёмов 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.

Термин**«червяк»** обычно относится к автономной программе, которая копирует себя по всей сети, размещаясь в разных машинах. Как и вирусы, эти программы могут быть спроектированы для самотиражирования и для проведения «диверсий».

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.

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 нераскрываемыми.

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 правоохранительные.

Обеспечить надёжную защиту информации может только применение комплекса самых разнообразных методов.

Проект эскиза доски

Ведение урока сопровождается демонстрацией презентации [**Домашнее задание** Разгадайте кроссворд.](http://www.metod-kopilka.ru/go.html?href=http%3A%2F%2Fwww.metod-kopilka.ru%2F%3Bline-height%3A+100%25)



**По горизонтали**
1. Пятая тенденция современного процесса развития ит, которая заключается в стирании различий между сферами материального производства и информационного бизнеса, в максимальной диверсификации видов деятельности фирм и корпораций, взаимопроникновении различных отраслей промышленности, финансового сектора и сферы услуг
2. Интерактивная технология, обеспечивающая работу с неподвижными изображениями,  видеоизображением, анимацией, текстом и аудиоинформацией
3. Метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму
4. Система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую
5. Устройство связи, аналогичное мосту, выполняющее функции передачи пакетов в соответствии с определенными протоколами, обеспечивающее соединение лвс на сетевом уровне
7. Функция защиты управления доступом
9. Организованный социально-экономический и научно-технический процесс создания условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти и местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов
10. Необходимость предотвращения утечки (разглашения) какой-либо информации
12. Такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности
13. Информация формируется объектом управления и отражает внутреннюю экономическую ситуацию, а также степень влияния на нее внешней среды
15. Самый простой тип устройства для соединения однотипных лвс, он ретранслирует все принимаемые пакеты из одной лвс в другую
16. Система информационных объектов (статей), объединенных между собой направленными связями, образующими сеть
17. Предоставление определённому лицу или группе лиц прав на выполнение определённых действи
18. Метод защиты информации путем ее криптографического закрытия
19. Опознавание подписи
21. Такой метод защиты, который побуждает пользователя и персонал системы не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм
22. Действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов
23. Устройство связи, позволяющее соединить лвс с одинаковыми и разными системами сигналов

**По вертикали**
1. Один из видов угроз безопасности
6. Процедура проверки подлинности
8. Модель, которая предполагает переход на следующий этап после полного окончания работ по предыдущему этапу
11. Информация разрабатывается управленческим аппаратом в соответствии с целями управления и информацией о сложившейся экономической ситуации, об окружающей среде
12. Метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.)
14. Может быть симметричным и асимметричным
20. Автоматизированный словарь, отображающий семантические отношения между лексическими единицами дескрипторного информационно-поискового языка и предназначенный для поиска слов по их смысловому содержанию

**Используемая литература:**

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