Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 6»
городского округа город Кумертау
Республики Башкортостан

ПРАВОВАЯ ОХРАНА ПРОГРАММ И ДАННЫХ

/урок информатики в 8 классе/

учитель информатики
Николаева Галина Николаевна

Кумертау, 2014

Цель урока: ввести понятия: защита информации.

Задачи

Образовательная: рассмотреть различные способы защиты информации.

Развивающая: развитие мышления, познавательных интересов, навыков работы на компьютере, работы с программным обеспечением.

Воспитательная: воспитание информационной культуры учащихся, внимательности, аккуратности, дисциплинированности, усидчивости.

Ход урока

1. Орг. момент.

Приветствие, проверка присутствующих. Объяснение хода урока.

2. Теоретическая часть

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.

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.

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:

- 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).

Несанкционированный доступ - доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Несанкционированный доступ - получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

Несанкционированный доступ к информации (НСД) - Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами руководящий документ Гостехкомиссии "Защита от НСД. Термины и определения" (утверждён решением председателя Гостехкомиссии России от 30 марта 1992 г.).

Причины несанкционированного доступа к информации:

- ошибки конфигурации (прав доступа, файрволов, ограничений на массовость запросов к базам данных);
- слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников);
- ошибки в программном обеспечении;
- злоупотребление служебными полномочиями (воровство резервных копий, копирование информации на внешние носители при праве доступа к информации);
- прослушивание каналов связи при использовании незащищённых соединений внутри ЛВС;
- использование клавиатурных шпионов, вирусов и троянов на компьютерах.

Физическая защита:

При защите информации от сбоев оборудования используются следующие основные методы:

1. Периодическое архивирование программ и данных.
2. Автоматическое резервирование файлов.

Защита от случайной потери или искажения информации, хранящейся в компьютере, сводится к следующим методам:

1. 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;*
2. 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;*
3. 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;*
4. Разграничению доступа пользователей к ресурсам файловой системы, строгому разделению системного и пользовательского режимов работы вычислительной системы.

3.Домашнее задание § 2.8, стр. 72-79, повторить главу 2

ПРИЛОЖЕНИЕ 1

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно - вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -

наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, -

наказывается лишением свободы на срок до четырех лет.