Защита файлов и управление доступом к ним.

Тип урока: изучение нового учебного материала.

Цель урока: обеспечить усвоение учащимися понятия «защита информации»; что является правом собственности, и на какие категории делится; основные виды преступлений; воспитание мотивов учения, положительного отношения к знаниям; соблюдение законов; воспитание дисциплинированности; развитие познавательных умений.

Структура урока.

1.Организационный момент и постановка цели.

1.1. Проверка готовности группы к уроку.

1.2. Приветствие. Отмечаю отсутствующих в журнале.

2.Ознакомление с новым учебным материалом.

По существу сфера безопасности называется не защита информации, а защита прав собственности на нее.

Информация – это знания, т.е. отражение действительности в сознании человека. Информация не является математическим объектом, но как объект права собственности копируется за счет математических носителей. Перемещение таких носителей к другому субъекту неизбежно влечет нарушение прав собственности на информацию.

Право собственности включает в себя 3 правомочных собственника:

1.Право распоряжения – определяется, кому эта информация могла быть предоставлена.

2.Право владения – иметь информацию в неизменном виде.

3.Право пользования – использовать информацию в своих интересах.

Субъект права собственности на информацию может передать часть своих прав не теряя их сам к другим субъектам.

В федеральном законе *«Об информации, информатизации и защите информации»* от 20.02.95г. было введено понятие ***документирование информации с ограниченным доступом,*** которое распространяется на информацию, отнесенную к государственной тайне и конфиденциальную.

Цель защиты информации заключается в защите прав собственности на нее и задач безопасности, которая заключается в защите ее от утечки, модификации и утрате.

Информация как коммерческая тайна.

Понятие введено в 1991 году после вступления в силу закона «О предприятиях СССР» (ст.33).

Коммерческая тайна – это информация, которая не является государственным секретом, связанная с производством технологий, управлением организационной и другой деятельностью, разглашение которой может принести ущерб предприятию.

С развитием человеческого общества, появлением частной собственности, борьбой за власть – информация приобретает цену.

Ценной становится информация, овладение которой дает выигрыш.

Эффективное решение вопросов защиты информации может быть успешным при условии использования комплексного подхода и построению информационной безопасности.

Появление электронных денег привело к возможности их красть.

Хакер – компьютерный хулиган, получающий удовольствие оттого, что ему удается проникнуть в другой компьютер.

Кракер – вор, взломщик, в отличии от хакера ворует информацию, выкачивает ценные информационные банки.

И широкое распространение получили компьютерные вирусы.

Для того, чтобы остановить нарушителя необходимо определить возможные точки приложения его усилий и установить на его пути систему преград.

Ценность информации является критерием принятия решения на защиту информации. Для оценки информации требуется ее разделить на категории.

По важности:

1.Жизненноважная – незаменимая.

2.Важная – которая могла быть заменена и восстановлена.

3.Полезная – трудно восстановить, но без нее можно работать.

4.Несущественная, ненужная организму.

Эти уровни согласуются с принципом деления информации по уровню секретности.

Уровень секретности – это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной или секретной информации.

Компьютерная преступность.

Компьютерных преступлений, как преступлений специфических в юридическом смысле не существует.

Компьютерные преступления условно можно разделить на 2 большие категории:

I Преступления связанные с вмешательством в работу компьютера;

II Преступления использующие компьютеры, как необходимые компьютерные средства.

Основные виды преступлений связанные с вмешательством в работу компьютеров.

I. Несанкционированный доступ к информации. Несанкционированный доступ осуществляется с использованием чужого имени, изменением физических адресов технических устройств, модификацией программного и информационного обеспечения, хищением носителя информации, установка аппаратуры записи подключаемым каналам передачи данных.

II. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводя из строя компьютерную систему.

Разновидности «логических бомб».

1.Временная бомба – срабатывает по достижению определенного момента времени;

2. «Троянский конь» - тайно вводится в чужую программу команды позволяющие осуществлять новые, непланировавшиеся владельцем программы функции, но одновременно сохраняют работоспособность;

2-а. Безобидно выглядящий кусок программы вставляют не команды выполняющие грязную работу, а команды формирующие эти команды и после выполнения уничтожающие их.

III. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных компонентов, приведение к тяжким последствиям.

IV. Подделка компьютерной информации. Разновидность несанкционированного доступа с той разницей, что пользоваться им может не посторонний пользователь, а саморазработчик.

Идея преступления состоит в подделке выходной информации компьютера с целью имитации работоспособности больших систем.

V. Хищение компьютерной информации.

Виды преступлений, в которых компьютер является средством достижения цели.

1.Разработка сложных математических моделей, входными данными в которых являются возможности условий проведения преступления, а выходными данными – рекомендации по выбору оптимального варианта действий преступника.

2.«Воздушный змей» простейший случай: открывается в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно постепенно повышающимися суммами.

Предупреждение компьютерных преступлений.

При разработке компьютерных систем, выход из строя или ошибки, в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными.

Выделим некоторые меры направленные на предупреждение преступления:

1.***Технические меры:*** защита от несанкционированного доступа, резервное копирование особо важных компьютерных систем, установка оборудования обнаружения и тушения пожара, оборудование обнаружения воды, принятие конструктивных мер защиты от хищения, саботажа, диверсий, оснащение помещений замками, сигнализацией и т.д.

2.***Организационные меры:*** охрана вычислительного центра, тщательный подбор персонала, наличие плана восстановления работоспособности центра после выхода из строя, выбор места расположения центра и т.д.

3.***Правовые меры:*** разработка норм устанавливающих ответственность за компьютерные преступления, защита авторских прав программиста и т.д.

Защита данных в компьютерных сетях.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбоев и нарушении прав доступа, которые могут привести к уничтожению и нежелательной модификации данных. Среди таких потенциальных угроз можно выделить:

1.Сбои оборудования:

а)сбои кабельной системы;

б)перебой электропитания;

в)сбои дисковых систем;

г)сбои систем архивации данных;

д)сбои работы серверов, рабочих станций, сетевых карт и т.д.

2.Потери информации из-за некорректной работы ПО:

а)потеря или изменения данных при ошибках ПО;

б)потери при заражении системы компьютерными вирусами.

3.Потери связанные с несанкционированным доступом:

а)несанкционированное копирование, уничтожение или подделка информации;

б)ознакомление с конфиденциальной информацией, составляющую тайну, посторонними людьми.

4.Потери информации связанные с неправильным хранением архивных данных.

5.Ошибка обслуживающего персонала и пользователя:

а) случайное уничтожение или изменение данных

б) некорректное использование программного и аппаратного обеспечения ведущее к уничтожению или изменению данных

Многочисленные виды защиты информации объединяются в три основные класса:

1. средства физической защиты
2. программные средства защиты
3. административные меры защиты

3.Задание на дом.

Домашнее задание будет заключаться в следующем: выучить конспект по тетради.

4.Подведение итогов.

Спасибо за работу. Занятие окончено.

Список использованной литературы

1. Михеева Е.В. Информационные технологии в профессиональной деятельности: учеб. пособие. – М.: Проспект, 2009. – 448с.
2. Черноскутова И.А. Информатика. Учебное пособие для среднего профессионального образования. – СПб.: Питер, 2005. – 272 с.