**Урок информатики в 10 классе по теме:**

**«Информационная безопасность сетевой технологии работы»**

**Цель урока:** ознакомление учащихся с понятием информационной безопасности.

**Тип урока:** урок изучения нового материала.

**Форма урока:** индивидуальная, групповая.

**Оборудование:** ноутбук, проектор.

**Ход урока:**

*1. Организационный момент: постановка целей урока.*

*2. Проверка домашнего задания.*

Учащиеся сдают письменное домашнее задание по вопросам предыдущей темы:

а) В чем заключается поиск интернет-ресурсов по URL-адресам?

б) В чем заключается поиск информации по рубрикатору поисковой системы?

в) В чем заключается поиск информации по ключевым словам?

г) Принципы формирования запросов.

*3. Изучение нового материала.*

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Выделяют следующие основные направления информационной безопасности:

1. Организационные меры;

2. Антивирусные программы;

3. Защита от нежелательной корреспонденции;

4. Персональные сетевые фильтры.

**1. Организационные меры.**

Любой пользователь может обеспечить защиту информации на своем компьютере, выполняя следующие действия.

1. Резервное копирование (сохранение) файлов на дискеты, компакт-диски, ZIP-драйвы, стримеры и другие магнитные носители;

2. Проверка с помощью антивирусных программ всех дискет и компакт-дисков, а также файлов, полученных по электронной почте или из Интернета, перед их использованием или запуском;

3. Использование и регулярное обновление антивирусных программ и антивирусных баз.

**2. Антивирусные программы.**

        Дня обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Различают следующие виды антивирусных программ:

**Программы-детекторы** осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

**Программы-доктора** или фаги, а также **программы-вакцины** не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известными полифагами являются программы Aidstest, Scan, Norton AntiVirus и Doctor Web.

**Программа-ревизоры** относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf фирмы «Диалог-Наука».

**Программы-фильтры** или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Например:

* попытки коррекции файлов с расширениями СОМ и ЕХЕ;
* изменение атрибутов файлов;
* прямая запись на диск по абсолютному адресу;
* запись в загрузочные сектора диска.
* загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не «лечат» файлы и диски. К недостаткам программ-сторожей можно отнести их «назойливость», а также возможные конфликты с другим программным обеспечением. Примером программы-фильтра является программа Vsafe, входящая в состав утилит операционной системы MS DOS.

**Вакцины** или **иммунизаторы** – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

        Теперь обратимся непосредственно к «заразителям».

**Вирусы** можно классифицировать по следующим признакам:

        В зависимости **от среды обитания** вирусы можно разделить на **сетевые**, **файловые, загрузочные и файлово-загрузочные.** Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения СОМ и ЕХЕ. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

**По способу заражения** вирусы делятся на **резидентные** и **нерезидентные**. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

**По степени воздействия** вирусы можно разделить на следующие виды: **неопасные**, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;**опасные** вирусы, которые могут привести к различным нарушениям в работе компьютера; **очень опасные**, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

**По особенностям алгоритма** вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - **паразитические**, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить**вирусы-репликаторы**, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Известны**вирусы-невидимки**, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего незараженные участки диска. Наиболее трудно обнаружить **вирусы-мутанты**, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые **квазивирусные или "троянские" программы**, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

*4. Физкультминутка.*

Мы все вместе улыбнемся,

Подмигнем слегка друг другу,

Вправо, влево повернемся (повороты влево-вправо)

И кивнем затем по кругу (наклоны влево-вправо)

Все идеи победили,

Вверх взметнулись наши руки (поднимают руки вверх- вниз)

Груз забот с себя стряхнули

И продолжим путь науки (встряхнули кистями рук)

*5. Продолжение изучения нового материала.*

**3. Защита от нежелательной корреспонденции.**

Одной из наиболее многочисленных групп вредоносных программ являются почтовые черви. Львиную долю почтовых червей составляют так называемые пассивные черви, принцип действия которых заключается в попытке обмануть пользователя и заставить его запустить зараженный файл.

Схема обмана очень проста: зараженное червем письмо должно быть похожим на письма, часто встречающиеся в обычной почте: письма от друзей со смешным текстом или картинкой; письма от почтового сервера, о том, что какое-то из сообщений не может быть доставлено; письма от провайдера с информацией об изменениях в составе услуг; письма от производителей защитных программ с информацией о новых угрозах и способах защиты от них и другие подобные письма.

При рассылке зараженных писем, червь составляет их текст по заданному автором вируса шаблону и таким образом все зараженные этим червем письма будут похожи.

Практически аналогичным образом формулируется и проблема защиты от спама - нежелательной почты рекламного характера. И для решения этой проблемы есть специальные средства - **антиспамовые фильтры**, которые можно применять и для защиты от почтовых червей.

Самое очевидное применение - это при получении первого зараженного письма (в отсутствие антивируса это можно определить по косвенным признакам) отметить его как нежелательное и в дальнейшем все другие зараженные письма будут заблокированы фильтром.

Более того, почтовые черви известны тем, что имеют большое количество модификаций незначительно отличающихся друг от друга. Поэтому антиспамовый фильтр может помочь и в борьбе с новыми модификациями известных вирусов с самого начала эпидемии. В этом смысле антиспамовый фильтр даже эффективнее антивируса, т. к. чтобы антивирус обнаружил новую модификацию необходимо дождаться обновления антивирусных баз.

**4. Персональные сетевые фильтры.**

В последние годы на рынке средств защиты информации появилось большое количество пакетных фильтров, так называемых брандмауэров, или файрволов (fire-wall), — межсетевых экранов. Файрволы полезны и на индивидуальном уровне. Рядовой пользователь почти всегда заинтересован в дешевом или бесплатном решении своих проблем. Многие файрволы доступны бесплатно. Некоторые файрволы поставляются вместе с операционными системами, например Windows XP и Vac OS. Если вы используете одну из этих операционных систем, основной файрвол у вас уже установлен.

Файрвол (брандмауэр) — это программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только авторизованные соединения. Брандмауэр защищает соединенную с Интернетом локальную сеть или отдельный персональный компьютер от проникновения извне и исключает возможность доступа к конфиденциальной информации.

Популярные бесплатные файрволы:

• Zone Alarm;

• Kerio Personal Firewall 2;

• Agnitum’s Outpost

Недорогие файрволы с бесплатным или ограниченным сроком использования:

• Norton Personal Firewaall;

• Black ICE PC Protection

• MCAfee Personal Firewall

• Tiny Personal Firewall

Представленный список может стать хорошей отправной точкой для выбора персонального файрвола, который позволит вам пользоваться Интернетом, не опасаясь заразиться компьютерными вирусами.

*6. Итог урока.*

Что нового Вы узнали на уроке?

Было ли интересно работать на уроке?

Чему вы научились?

Справились ли вы с поставленной в начале урока целью?

*7. Домашнее задание.*

Заполнить карточку «Информационная безопасность»