

**Общеобразовательные цели:**

* - знать основы электронных коммуникаций;
* Типы угроз;

**Воспитательные цели:**

* Воспитание коммуникативных свойств личности;
* Воспитание толерантности;
* Воспитание сетевой этики.

**Развивающие цели:**

* Формирование познавательного интереса;
* Развитие навыков общения в сети

**Ход урока**

**Учитель:** Если говорить об угрозах информационно-технического характера, можно выделить такие элементы как кража информации, вредоносное ПО, хакерские атаки, СПАМ, халатность сотрудников, аппаратные и программные сбои, финансовое мошенничество, кража оборудования.

-Согласно статистике применительно к этим угрозам, можно привести следующие данные (по результатам исследований, проведённых в России компанией InfoWath):

Кража информации – 64%

Вредоносное ПО – 60%

Хакерские атаки – 48%

Спам – 45%

Халатность сотрудников – 43%

Аппаратные и программные сбои – 21%

Кража оборудования – 6%

Финансовое мошенничество – 5%

Как видно, из приведенных данных, наиболее распространены кража информации и вредоносное ПО.

**Вирусы**

-Под компьютерным вирусом принято понимать программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самотиражирования.

Все вирусы можно объединить в следующие основные группы:

Загрузочные вирусы (boot – вирусы) — инфицируют загрузочные секторы жестких дисков и дискет, помещая в нем команды запуска на исполнение самого вируса, который находится где-то в другом месте компьютера.

Файловые вирусы — заражают исполняемые файлы (с расширением .com, .exe, .sys), путем дописывания своей основной части («тела») в конец заражаемой программы, «головы» - в его начало. Вирус, находящийся в памяти, заражает все любой запущенный после этого исполняемый файл.

Загрузочно-файловые вирусы способны поражать как код загрузочных секторов, так и код файлов.

**Сетевые вирусы.**

Загрузочные вирусы (boot – вирусы)

Макро-вирусы.

Заражает файлы документов, например текстовые документы. После загрузки заражённого документа постоянно находится в оперативной памяти до закрытия документа.

«Червь».

это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети.

Особенностью червей, отличающих их от других вирусов, является то, что они не несут в себе ни какой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

«Логические бомбы» - скрипты и апплеты.

И хотя основные функции доступа к содержимому вашего диска здесь отключены, некоторые мелкие неприятности это может доставить. Кстати, в последнее время создатели некоторых сайтов (как правило, из разряда «только для взрослых») освоили любопытный вариант скриптов (на базе JavaScript), способных при открытии такой Web-страницы не только «прописать» адрес данного сайта в качестве «домашнего» (естественно, не спрашивая у посетителя разрешения), но и внести его непосредственно в системный реестр Windows в качестве «базового».

«Троянские кони».

Это модули, присоединяемые к каким-либо нормальным программам, распространяемым по сети, или «забрасываемые» в ваш компьютер несанкционированным способом.

Цель «троянского коня» - воровать ценную информацию (пароли доступа, номера кредитных карточек и т. п.) и передавать ее тому, кто этого «коня» запустил.

**Почтовые вирусы.**

Чаще всего заражение начинается с получения неизвестно от кого письма, содержащего исполняемую программу-«зародыш» . Когда ничего не подозревающий пользователь запустит такую программу на исполнение, содержащийся в ней вирус «прописывается» в системе и, обращаясь к содержимому адресной книги, начинает тайком от вас рассылать всем абонентам свои копии-зародыши в качестве вложений.

Дополнительные типы вирусов

Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные программы.

Шпионские программы

Шпионская программа (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации.

Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы

Одной из разновидностей шпионских программ являются :

Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения.

Фарминг – это замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта.

основной целью злоумышленников, использующих Фарминг, является завладение личной финансовой информацией пользователя. Отличие заключается только в том, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

Каналы распространения

Дискеты

Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.

Флеш-накопители (флешки)

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

Электронная почта

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

Системы обмена мгновенными сообщениями

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

Веб-страницы

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

Интернет и локальные сети (черви)

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.