Защита

**Выполнила: Немова Ирина,
студенка 23 группы**

Введение

- *Информация является важным объектом правовых отношений в современном обществе. Технологическая революция в области информации, начавшаяся в последней трети XX века и продолжающаяся до сих пор, определила появление таких явлений как "информационные войны" и "информационный терроризм". Поэтому важное место в политике национальной безопасности в настоящее время занимает информационная безопасность. Вообще, технологическая революция в области информации связана прежде всего с развитием кибернетики, которое привело к созданию информационных систем управления. Вслед за этим повсеместно в массовом порядке стали внедряться персональные компьютеры, что в свою очередь повлекло за собой ускоренные темп развития телекоммуникационных технологий. Затем персональные компьютеры стали объединять в компьютерные сети, вначале локальные, а затем и глобальные. Одновременно с колоссальным ростом популярности Интернета возникает беспрецедентная опасность разглашения персональных данных, критически важных корпоративных ресурсов. Кроме того, с каждым днём растёт объём деловых операций, совершаемых через Интернет.*
- *Повышение информационной безопасности становится неотложной задачей, решения которой в равной мере требуют и конечные пользователи, и компании.*
- *Важное значение приобретает также защита информации в персональном компьютере, особенно если приходится часто выходить в Интернет. Поэтому особое внимание нужно уделять защите компьютера и устанавливать и регулярно обновлять антивирусные программы. Вот почему так важно следить за развитием технологий в области информационной безопасности.*

Информационная безопасность. Компьютерные вирусы

- Персональные компьютеры, глобальную сеть Интернет и электронную почту стараются испортить хакеры - компьютерные хулиганы и вредители — создатели многочисленных компьютерных вирусов.
- Цель их — навредить или отомстить какому-либо отдельному лицу, организации или даже всему человечеству в лице пользователей Интернета.
- Компьютерные вирусы представляют собой программы, мешающие работе операционной системы, уничтожающие файлы и папки. Некоторые из них способны полностью разрушить информацию на диске, а самые "злобные" способны выводить из строя аппаратуру множества компьютеров и наносить огром

- *Каковы же пути проникновения компьютерных вирусов? "Заразить" ими компьютер можно разными способами: через зараженные дискеты, при получении электронной почты (через почтовые вложения) или даже просто при просмотре сайтов Интернета, особенно материалов "только для взрослых".*
- *Компьютерный вирус — это программа, без ведома пользователя внедряющаяся в компьютеры и производящая там различные несанкционированные действия.*
- *Самое опасное свойство, обязательное для компьютерного вируса - это его способность "размножаться", т. е. создавать свои дубликаты и внедрять их в вычислительные сети и (или) файлы, сие темные области компьютера.*
- *Компьютерные вирусы относятся к классу программ, называемых вредоносными кодами.*
- *В группу вредоносных кодов также входят так называемые "черви" и "троянские кони". Их отличие от вирусов состоит в том, что "программа-червь распространяется по компьютерным сетям (локальным или глобальным), не прибегает к "размножению". Вместо этого она автоматически, без ведома пользователя, рассылает свой оригинал, например, по электронной почте.*

"Троянские" программы вообще лишены каких-либо встроенных функций распространения: они попадают на компьютеры исключительно с помощью своих авторов. "Троянские" программы попадают в компьютеры под видом полезных, забавных или прибыльных программ.

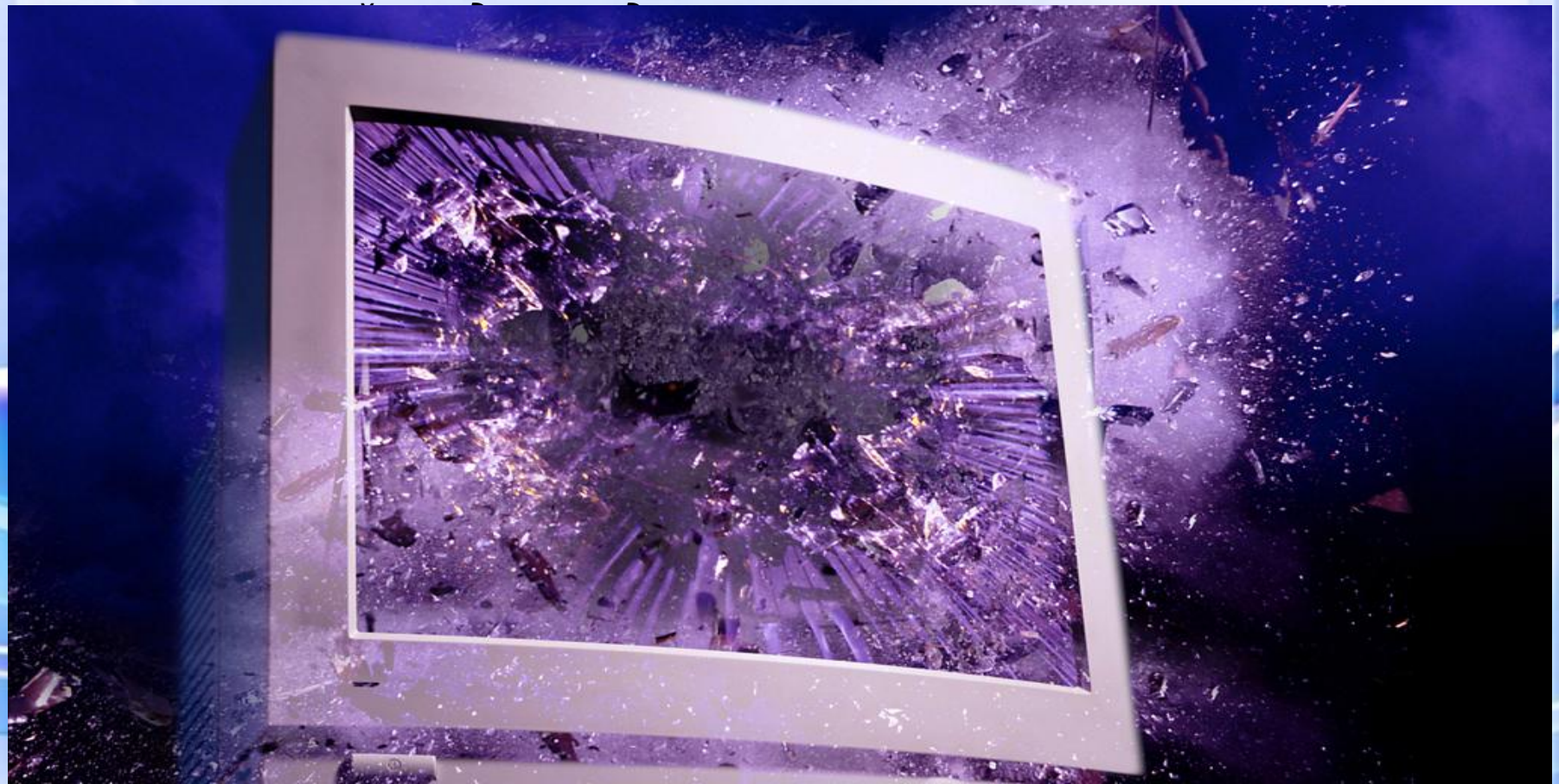
Например, пользователю приходит письмо по электронной почте с предложением запустить присланный файл, где лежит крупная сумма денег. После запуска этого файла в компьютер незаметно попадает программа, совершающая различные нежелательные действия.

Например, она может шпионить за владельцем зараженного компьютера (следить, какие сайты он посещает, какие использует пароли для доступа в Интернет и т. п.) и затем отсылать полученные данные своему автору. За последние годы появились

Типичный пример — макровирус "Melissa", вызвавший крупную вирусную "эпидемию". Он распространялся по сетям как обычный интернет-червь. "LoveLetter" ("Любовное письмо") — также помесь сетевого червя и вируса. В более сложных случаях вредоносная программа может содержать в себе характеристики всех трех типов (таков, например, вирус BABYLON).

В настоящее время зарегистрировано более 50 000 компьютерных вирусов. Их число постоянно растет, появляются совершенно новые, ранее не известные типы.

Классифицировать вирусы становится труднее год от года. Они наносят



Антивирусные программы

- **Борьба с компьютерными вирусами ведется с помощью антивирусных программ. Она напоминает извечную борьбу меча и щита: чем сильнее оружие, тем совершеннее становятся средства защиты от него. Так, по мере появления и совершенствования компьютерных вирусов совершенствуются антивирусные программы.**
- **Установка на ваш компьютер антивирусной программы - это единственный действенный способ борьбы с компьютерными вирусами. Таких программ существует множество, но самыми популярными в нашей стране являются антивирусные программы DoctorWeb и антивирусный пакет AVP (AntiviralToolkitPro) лаборатории Е. Касперского (так называемый антивирус Касперского).**
- **Находит применение и антивирусная программа NortonAntivirus.**
- **Наибольшую популярность у пользователей приобрел антивирус Касперского.**
- **Координация отдельных его частей осуществляется из центра управления ControlCentre. Через него запускается обновление баз (Updater) через Интернет, монитор и сканер.**
- **Существует несколько методов обеспечения антивирусной безопасности.**

Один из них — *антивирусный сканер.* Принцип работы этой программы заключается в просмотре всех файлов, загрузочных секторов и памяти в целях обнаружения в них программного кода вируса.Главный недостаток сканера — неспособность отслеживать различные модификации вируса. Для каждой из них антивирусным компаниям приходилось выпускать отдельное обновление антивирусной базы.Поэтому на время между появлением новой модификации вируса и выходом соответствующего антивируса пользователь остается незащищенным. Антивирусные сканеры осуществляют проверку только тогда, когда вы их запускаете. Они анализируют содержимое памяти, отыскивают вирусы, найдя, лечат или удаляют зараженные файлы.

Однако пользователи очень часто забывают проверять сомнительные файлы, загруженные, например, из Интернета, и в результате сами заражают компьютер. Сканер способен определить факт заражения только после того, как в системе уже появился вирус.

- Другой метод — *антивирусный монитор,* который работает постоянно.Эта программа проверяет всю информацию, которую программы собираются писать на диск или держат в памяти.
- В комплект современных антивирусных программ входят: сканер, монитор, утилита для автоматического обновления антивирусной базы через Интернет и планировщик для запуска и обновления антивирусной программы по расписанию.

Основные правила "компьютерной гигиены"

- 1. Обязательно проверяйте с помощью антивирусного сканера все дискеты, компакт-диски и другие мобильные носители информации, а также файлы, получаемые из сети Интернет и электронной почты.
- 2. Никогда не открывайте файлы, присылаемые по электронной почте неизвестными вам людьми, и прежде всего спам.
- 3. Проводите полную антивирусную проверку вашего компьютера после получения его из ремонтных служб. Ремонтники пользуются одними и теми же дискетами для проверки всех компьютеров — они очень легко могут занести вирус с другого компьютера!
- 4. Своевременно, не реже одного раза в неделю, устанавливайте "заплатки" в защите Windows и InternetExplorer через сеть Интернет.
- 5. Для повышения сохранности ваших данных периодически проводите резервную архивацию информации на независимые носители, например оптические диски CD-R, CD-RW.
- 6. Будьте осторожны, допуская других пользователей к вашему компьютеру.
- 7. Остерегайтесь регистрации своего электронного почтового адреса в Интернете, особенно на сомнительных сайтах.
- 8. Обновляйте свою антивирусную базу через сеть Интернет не реже одного раза в неделю.

Заключение

Новые виды вычислительной техники и связи создали уникальные возможности для включения информации в хозяйственный оборот и распространения на неё статуса товара.

Информация превратилась в одно из важнейших средств воздействия на общественные отношения, стала одним из ценнейших товаров. Любой же товар требует защиты, особенной защиты требует такой "нематериальный" товар как информация. Именно поэтому информационная безопасность в настоящее время является одной из самых развивающихся областей современной науки. Это в равной степени относится как к технической, так и правовой стороне вопроса, касающегося информационной безопасности.

Практически каждый из нас в повседневной жизни сталкивается с результатами труда специалистов по информационной безопасности. Антивирусы, межсетевые экраны, авторизация и разграничение доступа, системы обнаружения и предотвращения атак, сканеры безопасности, системы контроля содержимого и антиспама – всё это результаты развития технологий информационной безопасности. Ведущие вузы страны открывают факультеты информационной безопасности, где готовят крайне востребованных специалистов, способных обеспечивать информационную безопасность в любой сфере человеческой деятельности, будь то политика, экономика или область высоких технологий.

СПАСИБО ЗА ВНИМАНИЕ