Российский Государственный Социальный Университет,
Факультет Информационных Технологий

Компьютерные вирусы и антивирусные программы

Темы курса лекций

1. Введение. Компьютерные вирусы. Общие характеристики
2. Хронология возникновения вирусов.
3. Общие подходы к антивирусной защиты.
4. Антивирусные средства и системы.
5. Антивирусы. Общие характеристики.
6. Антивирус Касперского.
7. Антивирус Dr.Web.
8. Обзор других антивирусных программ.
9. Сравнение антивирусных программ.

Подготовка к экзамену. Пробное тестирование.

Компьютерные вирусы и антивирусные программы

Определение компьютерного вируса

1. Вирус – это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.

2. Активизация компьютерного вируса может вызвать уничтожение программ и данных, и даже уничтожение составляющих компьютера (системного блока).

Типичный размер вируса: 200 - 5000 байт.
Всего вирусов белее 60 тысяч.

Компьютерные вирусы и антивирусные программы

Согласно **ГОСТ Р. 51188-98 «Испытания программных средств на наличие компьютерных вирусов»**:

Вирус — программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения.
Компьютерный вирус относится к вредоносным программам».

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному Кодексу (глава 28, статья 273).

Компьютерные вирусы и антивирусные программы

Признаки появления вирусов

- Неправильная работа нормально работающих программ
- Частые зависания и сбои в работе ПК
- Медленная работа ПК
- Изменение размеров файлов
- Исчезновение файлов и каталогов
- Неожиданное увеличение количество файлов на диске
- Уменьшение размеров свободной оперативной памяти
- Вывод на экран неожиданных сообщений и изображений
- Подача непредусмотренных звуковых сигналов
- Невозможность загрузки Операционной Системы.

Компьютерные вирусы и антивирусные программы

Классификация вирусов

1) по среде обитания вируса

По среде обитания вирусы можно разделить на сетевые, файловые и загрузочные.

Сетевые вирусы распространяются по компьютерной сети,
файловые внедряются в выполняемые файлы (подвид - макро-вирусы),
загрузочные - в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record).

Классификация вирусов

Сетевые вирусы

Для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей.

Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.

Есть несколько разновидностей сетевых вирусов.

Классификация вирусов

Разновидности сетевых вирусов

Почтовые вирусы. Эти вирусы распространяются в сообщениях электронной почты. Они имеют две особенности. Во-первых, подобный вирус может внедриться на компьютер только по беспечности пользователя, который должен сам открыть ему дорогу. Во-вторых, почтовый вирус обычно сам организует свою рассылку по списку контактов в адресной книге зараженного компьютера. Это, в некотором роде, вирус быстрого действия: едва попав на компьютер, он тут же размножается, рассылая электронную почту, и может немедленно приступать к вредоносным действиям. Это самая «популярная» категория вирусов сегодняшнего дня.

Классификация вирусов

Разновидности сетевых вирусов

Сетевые черви. Крайне редкая категория вирусоподобных программ, требующая от ее автора высокого профессионального уровня. В отличие от вируса сетевой червь — это постоянно работающая программа, способная проникнуть в другую систему, сформировать там свою копию и запустить ее исполнение. «Естественной средой» для сетевых червей являются серверные системы.

Классификация вирусов

Разновидности сетевых вирусов

Программы-агенты. Агентские, или троянские, программы не содержат ни средств размножения, ни, как правило, явных средств нанесения вреда.. Их задача иная — предоставить постороннему человеку контроль над компьютером. Чаще всего злоумышленник действует через Интернет. Агентская программа попадает на компьютер подобно вирусу (обычно вместе с зараженным исполняемым файлом). Она автоматически устанавливается подобно обычному приложению и явным образом себя не проявляет.

Классификация вирусов

Программы-агенты.

Троянские программы обычно работают как серверы — они ожидают команды от «хозяина». «Скрытая» программа может сделать все, что угодно. Типичные способы использования — похищение конфиденциальной информации (копирование файлов, перехват паролей, регистрация нажатий клавиш), «логическая бомба» (вредоносное воздействие по команде или в заданное время), неавторизованный прокси-сервер (злоумышленник выполняет противоправные действия против «третьих» систем, ис пользуя подконтрольный компьютер), дезактивация средств защиты. Подобные программы применяют и для организации широкомасштабных сетевых атак.

Классификация вирусов

Разновидности сетевых вирусов

Псевдовирусы.

К этой категории можно отнести не столько реальные вирусные и вирусоподобные программы, сколько слухи. В частности, к числу «псевдовирусов» относятся вирусы, сжигающие мониторы и процессоры, ломающие жесткие диски, а также гипнотизирующие пользователя скрытыми картинками на экране монитора. Таких вирусов сегодня нет, и вряд ли они появятся в ближайшем будущем. Другую группу псевдовирусов образуют электронные круговые письма.

Классификация вирусов

Файловые вирусы

При своем размножении тем или иным способом используют файловую систему операционной системы.

Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS и др.).

При запуске файла сначала выполняется вирусный код и только потом — сама программа. Это широко распространенная и весьма разнообразная категория вирусов, различающихся по способам заражения и способам сокрытия своего присутствия от беглого контроля. Формат исполняемых файлов и динамических библиотек весьма «рыхлый», так что вирус может спрятать в них свой код, не изменяя размера файла. Но сегодня подобные вирусы постепенно уходят в прошлое: прямой обмен исполняемыми файлами между пользователями заметно сократился по сравнению с прошлыми годами.

Классификация вирусов

Макро-вирусы

Являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Макровирус записывает себя в стандартный шаблон документа, после чего дописывает свой код ко всем создаваемым или открываемым документам. В последних версиях программы *Word* защита от макровирусов заметно усилена, но *Word* — не единственная программа, имеющая язык макрокоманд.

Классификация вирусов

Загрузочные вирусы

Заражают загрузочный сектор гибкого диска или винчестера.

При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.

Классификация вирусов

2) **по способу заражения среды обитания**

Способы заражения делятся на резидентный и нерезидентный.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

Классификация вирусов

3) по деструктивным возможностям

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;

Классификация вирусов

4) **по особенностям алгоритма вируса.**

По особенностям алгоритма можно выделить следующие группы вирусов:

- компаньон-вирусы (companion) - это вирусы, не изменяющие файлы.
- вирусы-“черви” (worm) - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Классификация 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 распространяются вирусы и другие вредоносные программы.

Компьютерные вирусы и антивирусные программы

Компьютерные вирусы и антивирусные программы

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную
- информацию о своих действиях в системе;

прочие программы, тем или иным способом намеренно

- наносящие прямой или косвенный ущерб данному или
- удалённым компьютерам.

Компьютерные вирусы и антивирусные программы

Каналы распространения

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. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,*** в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров.

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

Создатели вредоносных программ

Основная масса вирусов и троянских программ в прошлом создавалась студентами и школьниками, которые только что изучили язык программирования, хотели попробовать свои силы, но не смогли найти для них более достойного применения.

Такие вирусы писались и пишутся по сей день только для самоутверждения их авторов.

Компьютерные вирусы и антивирусные программы

Вторую группу создателей вирусов также составляют молодые люди (чаще — студенты), которые еще не полностью овладели искусством программирования.

Из-под пера подобных «умельцев» часто выходят вирусы крайне примитивные и с большим числом ошибок («студенческие» вирусы). Жизнь подобных вирусописателей стала заметно проще с развитием интернета и появлением многочисленных веб-сайтов, ориентированных на обучение написанию компьютерных вирусов.

Часто здесь же можно найти готовые исходные тексты, в которые надо всего лишь внести минимальные «авторские» изменения и откомпилировать рекомендуемым способом.

Компьютерные вирусы и антивирусные программы

Третью, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы.

Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами.

Такие вирусы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, ошибки в системах безопасности операционных сред, социальный инжиниринг и прочие хитрости.

Компьютерные вирусы и антивирусные программы

Отдельно стоит четвертая группа авторов вирусов — «исследователи», которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д.

Часто авторы подобных вирусов не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные интернет-ресурсы, посвященные созданию вирусов.

При этом опасность, исходящая от таких «исследовательских» вирусов, тоже весьма велика — попав в руки «профессионалов» из предыдущей группы, эти идеи очень быстро появляются в новых вирусах.