Вирусы и антивирусная защита

Классификация вирусов

Компьютерный вирус — это специально написанная небольшая программа, которая может приписывать себя к другим программам (то есть заражать их), а также выполнять различные вредные действия на компьютере. Копии вирусной программы сохраняют способность дальнейшего распространения.

Процесс внедрения вирусом своей копии в другую программу, файлы или системную область диска называется **заражением,** а программа или иной объект, содержащий вирус — **зараженным**.

В мировых электронных сетях циркулируют более 1 миллиона различных вирусов.

По данным Института компьютерной безопасности, авторы вирусов, как правило, мужчины в возрасте 19-35 лет, отличающиеся неординарными способностями и, как правило, избравшие компьютер сферой своей профессиональной деятельности. Впрочем, зафиксировано довольно много случаев, когда вирусы создавали подростки в возрасте 12-15 лет.

Авторы вирусов действуют из совершенно различных побуждений. Некоторые из них действуют по политическим мотивам. Иногда раздражение вызывает деятельность той или иной кампании — чаще всего страдает Microsoft.

Во всем мире «охотой» на авторов разрушительных вирусов занимаются не более 500 организаций. В США, стране с наиболее развитой интернет-инфраструктурой, «охотой» на авторов разрушительных вирусов занимаются **ФБР** и Министерство Национальной Безопасности.

На сегодняшний день в мире известно множество вирусов. Вирусы заражают, как правило, исполняемые файлы (программы). В последнее время появились и так называемые *макровирусы,* они заражают не исполняемые файлы, а документы офисных приложений (таких как Microsoft Word и Microsoft Excel). Макровирус занести в компьютер очень просто: достаточно открыть в приложении Word зараженный документ.

На рис.1 приведена возможная классификация вирусов.

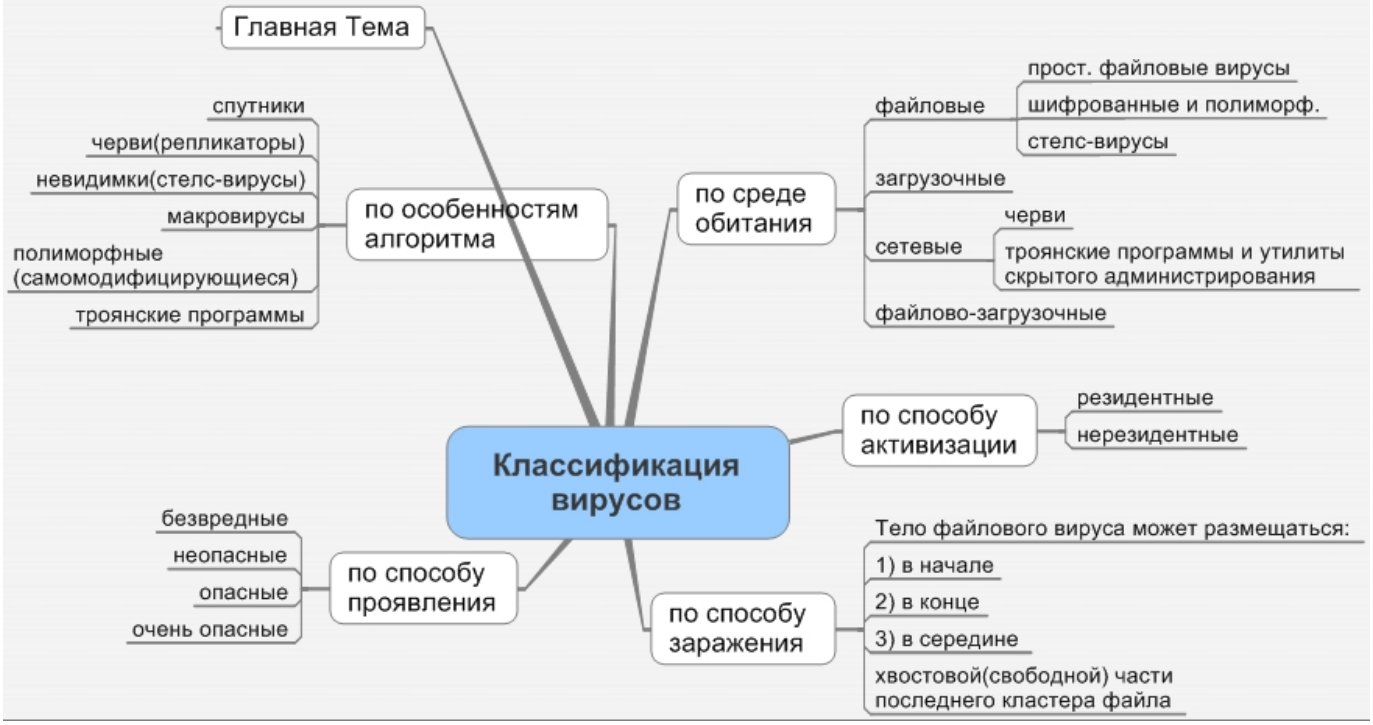

Рис.1

Основные источники вирусов:

1. дискета, на которой находятся зараженные вирусом файлы;
2. компьютерная сеть, в том числе система электронной почты и Internet;
3. жесткий диск, на который попал вирус в результате работы с заражен-ными программами;
4. вирус, оставшийся в оперативной памяти после предшествующего пользователя.

□ ***По среде обитания*** вирусы разделяются на **файловые, загрузочные и сетевые.**

1. *Файловые вирусы* внедряются как в исполняемые файлы, так и в файлы документов текстовых процессоров.
2. *Загрузочные вирусы* заражают системную область диска.
3. *Сетевые вирусы* распространяются по компьютерным сетям (например, черви и трояны).
4. Существуют также *файлово-загрузочные вирусы*, которые зара-жают и программы, и загрузочные секторы.

□ ***Способ заражения*** среды обитания зависит от самой среды. Заражен-

ная вирусом среда называется ***вирусоносителем.*** Тело файлового вируса может при заражении размещаться

1. в конце;
2. начале;
3. середине;
4. или хвостовой (свободной) части последнего кластера файла.

□ ***По способу активизации*** вирусы разделяются на резидентные и нерезидентные.

1. *Резидентные вирусы* при заражении оставляют в оперативной памяти резидентную часть, которая затем перехватывает обращения операционной системы к объектам, зараженным вирусом: файлам, загрузочным секторам, и внедряется в них. Резидентные вирусы сохраняют свою активность вплоть до выключения или перезагрузки компьютера.
2. *Нерезидентные вирусы* остаются активными ограниченное время и активизируются в определенные моменты, например, при запуске зараженных программ или при обработке документов текстовым процессором.

□ ***Проявлениями*** (деструктивными действиями) вирусов могут быть различные влияния на работу компьютера. По проявлению вирусы можно разделить на безвредные, неопасные, опасные и очень опасные.

1. При заражении *безвредными вирусами* происходит уменьшение объема свободной оперативной памяти или памяти на дисках.
2. Заражение *неопасными вирусами* приводит также к уменьшению объема свободной оперативной памяти или памяти на дисках или непонятным системным сообщениям, музыкальным и визуальным эффектам и т.д.
3. *Опасные вирусы* производят замедление загрузки и работы компьютера, непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов, ошибки при загрузке операционной системы, невозможность сохранять файлы в нужных каталогах.
4. *Очень опасные вирусы* являются причиной исчезновения файлов, форматирования жесткого диска, невозможности загрузки файлов или операционной системы.

□ ***По особенностям алгоритмов*** различаются следующие вирусы: спутники, черви (репликаторы), макровирусы, невидимки (стелс-вирусы), самомодифицирующиеся вирусы (мутанты).

1. *Вирусы-спутники* файлов не изменяют, а для выполняемых программ создают одноименные программы типа COM, которые при

выполнении исходной программы запускаются первыми, а затем передают управление исходной программе.

2. *Вирусы-черви* — это сетевые вирусы (вирусы-репликаторы), распространяющиеся по компьютерным сетям. Попав из сети в компьютер, они, помимо действий на данном компьютере, отыскивают в операционной системе адреса других сетей и отсылают по ним свои копии. Практически всегда червями применяются «двойные расширения». В этом случае присоединенный файл имеет имя вроде: «Docl.doc.pif», «pict.jpg.com». То есть пользователь думает, что файл является документом или картинкой, а тот на самом деле является исполняемым файлом с расширением вроде: EXE, COM, PIF, SCR, BAT, CMD и т.п. Если такой файл «открыть», то тело червя активизируется. Очень часто почтовые черви призваны для того, чтобы установить на зараженный компьютер троянскую программу или утилиту скрытого администрирования и сообщить адрес компьютера творцу червя. Нередко просто уничтожают информацию или делают невозможной дальнейшую работу на компьютере. При размножении они загружают каналы связи и нередко настолько, что полностью парализуют работу человека или целой организации.
3. *Макровирусы* распространяются и по сетям, а средой их обитания являются файлы, имеющие возможность содержать фрагменты кода программ на Visual Basic. Это могут быть, например, файлы документов для Microsoft Word или электронные письма. Появившись в 1995 г., сегодня они составляют большую часть всех вирусов. Опасность макровирусов заключается еще и в том, что распространяется вирус целиком в исходном тексте. Фактически вирусы этого класса способны парализовать работу целого офиса, а то даже и не одного.
4. *Невидимки, или стелс-вирусы*. Их очень трудно обнаружить. Простейший способ маскировки — при заражении файла вирус "делает вид", что длина файла не изменилась.
5. *Самомодифицирующиеся вирусы* меняют свою структуру и код по случайному закону, и их очень трудно обнаружить. Их называют также полиморфными. Две копии одного и того же вируса этого типа могут не содержать одинаковых последовательностей байтов.

Наряду с компьютерными вирусами существуют и другие опасные программы, которые маскируются под полезные, нужные, но содержат средства незаконных, разрушительных операций, получили название "троянских коней". Главное отличие «троянов» от всех перечисленных выше творений человеческого разума — это то, что троянские программы не размножаются сами. Они единоразово устанавливаются на компьютер и долгое время выполняют

свои функции. При этом троянский конь не может самостоятельно переместиться с одного компьютера в локальной сети на другой. Часто они являются спутниками сетевых или почтовых червей.

Все **троянские программы** можно разделить на **три основных класса по выполняемым действиям:**

1. *Логические (временные) бомбы* — программы, различными методами удаляющие/модифицирующие информацию в определенное время, либо по какому-то условию. (например, черная пятница, начинает действовать, когда пятница совпадает с 13 – ым числом.)
2. *Шпионы* — собирающие информацию (имена, пароли, нажатия на клавиши) и складирующие ее определенным образом, а нередко и отправляющие собранные данные по электронной почте или другим методом.
3. *Удаленное управление компьютером* или получение команд от злоумышленника (через локальную/ глобальную сеть, по электронной почте, в файлах, от других приложений, например, тех же червей или вирусов).

Одинаково опасны все три типа программ. Каждый из них способен либо уничтожить данные, либо украсть ценную информацию (хотя бы те же имена и пароли доступа к различным ресурсам).

Средства предотвращения заражения

К общим средствам, помогающим предотвратить заражение и его разрушительные последствия относят:

1. ***резервное копирование*** информации (создание копий файлов и системных областей жестких дисков);
2. если даже ни один антивирус не среагировал на файл, который был подучен из сети, ***не торопитесь его запускать***. Подождите неделю. Если этот файл окажется заражен новым неизвестным вирусом, то**,** скорее всего кто-нибудь «наступит на грабли» раньше вас и своевременно сообщит об этом;
3. ***избежание пользования случайными и неизвестными программами.*** Чаще всего вирусы распространяются вместе с компьютерными программами;
4. ***перезагрузка компьютера перед началом работы***, в частности, в случае, если за этим компьютером работали другие пользователи;

5. ***ограничение доступа к информации***, в частности физическая защита дискеты во время копирования файлов с нее;
6. ***разные антивирусные программы*** (антивирусы). И если вы активно пользуетесь Интернетом, рекомендуем обновлять антивирус минимум раз в неделю (хотя конечно идеально было бы обновляться каждый день).

Классификация антивирусных программ

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы, позволяющие выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные (характерные для вирусов) действия.

Антивирусные программы следует применять наряду с регулярным резервированием данных и использованием профилактических мер, позволяющих уменьшить вероятность заражения вирусом.

Антивирусные программы (антивирусы) — это программы, способные либо обнаружить вирус, либо и обнаружить и обезвредить вирус.

Рис.2 **Одна из возможных классификаций антивирусных программ.**

Антивирусные программы	**Достоинства**	**Недостатки**
Детекторы (полифаги)	• Универсальность; • Возможность лечить.	• Большие размеры антивирусных баз; • Небольшая скорость; • Необходимость периодически обновлять версию программы.
Ревизоры	• Выдают сообщение только о подозрительных изменениях; • Возможность лечить.	Невозможность обнаружить вирус в новых файлах.
Сторожа (блокировщики)	Обнаружение вируса на ранних стадиях (пока не успел размножиться).	Если вирус обращается непосредственно к BIOS, то он не будет обнаружен.

Существует несколько типов антивирусных программ. **Эти программы различаются выполняемыми функциями.**

1. **Программы-детекторы (полифаги)** позволяют обнаруживать файлы, зараженные одним из известных вирусов. Для этого они используют так называемые «**маски**».
   Маской вируса называют некоторую постоянную последовательность программного кода, специфичную для этого вируса.
   Если программа обнаруживает такую последовательность, то файл подлежит лечению.
   Некоторые программы также выполняют эвристический анализ файлов и системных областей дисков, что часто (но не всегда) позволяет обнаруживать новые, не известные программе-детектору вирусы.
   Многие полифаги позволяют «**лечить**» зараженные файлы или диски, удаляя из них вирусы.
   К достоинствам полифагов относится их универсальность.
   К недостаткам можно отнести большие размеры используемых антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов, что приводит к небольшой скорости поиска вирусов.
   Для программ-детекторов следует периодически обновлять их версии.

2. **Программы-ревизоры** запоминает сведения о состоянии файлов и системных областей дисков, т.е. принцип работы основан на подсчете контрольных сумм и некоторой другой информации: длины файлов, даты их последней модификации. Эти сведения сохраняются в базе данных антивируса. При следующих запусках ревизоры сравнивают состояния данных с подсчитанными. При выявлении несоответствий об этом сообщается пользователю.
   К достоинствам ревизоров относится то, что их можно настроить так, чтобы они выдавали сообщения только о подозрительных изменениях, не беспокоя лишний раз пользователя. Часто программы-ревизоры позволяют «**лечить**» зараженные файлы и диски, удаляя из них вирусы (практически все типы).
   К недостаткам относится то, что они не могут обнаружить вирус в новых файлах, так как в их базе данных отсутствует информация об этих файлах.
3. **Программы-сторожа (или блокировщики**) располагаются резидентно в ОП и проверяют на наличие вирусов запускаемые файлы и вставляемые дискеты. При наличие вируса об этом сообщается пользователю.
   Многие программы-сторожа перехватывают те действия, которые используются вирусами для размножения и нанесения вреда (форматирование жесткого диска или запись в загрузочный сектор).
   Пользователь может разрешить или запретить выполнение соответствующий операции.
   К достоинствам - программы-сторожа позволяют обнаружить вирусы на ранних стадиях, пока вирус не успел размножиться.
   К недостаткам относится то, что если вирусы обращаются непосредственно к программам BIOS системы, то вирус не будет перехвачен.

Примеры некоторых антивирусов (в алфавитном порядке).

Aladdin Knowledge Systems eSafe
Command AntiVirus
Doctor Web
Eset NOD 32
Kaspersky Antivirus
Network Associates McAfee VirusScan
Norman Virus Control
Panda Antivirus Platinum
Symantec Norton AntiVirus