1. **Вредоносное ПО:**

Компьютерным вирусом называется программа, которая обладает способностью создавать свои копии, и внедрять их в различные объекты и ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Заражение программы, как правило, выполняется таким образом, чтобы вирус получил управление раньше самой программы. Для этого он либо встраивается в начало программы, либо имплантируется в ее тело так, что первой командой зараженной программы является безусловный переход на компьютерный вирус, текст которого заканчивается аналогичной командой безусловного перехода на команду вирусоносителя, бывшую первой до заражения. Получив управление, вирус выбирает следующий файл, заражает его, возможно, выполняет какие-либо другие действия, после чего отдает управление вирусоносителю.

Первичное заражение происходит в процессе наступления инфицированных программ из памяти одной машины в память другой, причем в качестве средства перемещения этих программ могут использоваться как носители информации (оптические диски, флэш-память и т.п.), так и каналы вычислительных сетей. Вирусы, использующие для размножения сетевые средства, сетевые протоколы, управляющие команды компьютерных сетей и электронной почты, принято называть сетевыми.

Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликации (саморазмножения) и проявления. В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации в компьютере или на внешних носителях.

Физическая структура компьютерного вируса достаточно проста. Он состоит из головы и, возможно, хвоста. Под головой вируса понимается его компонента, получающая управление первой. Хвост – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют несегментированными, тогда как вирусы, содержащие голову и хвост, — сегментированными.

Наиболее существенные признаки компьютерных вирусов позволяют провести следующую их классификацию.

Существует несколько подходов к классификации компьютерных вирусов по их характерным особенностям:

— по среде обитания вируса;

— по способу заражения;

— по деструктивным возможностям;

— по особенностям алгоритма работ.

По среде обитания вирусы подразделяются на:

Файловые вирусы — вирусы поражающие исполняемые файлы, написанные в различных форматах. Соответственно в зависимости от формата, в котором написана программа это будут EXE или COM вирусы.

Загрузочные вирусы — вирусы поражающие загрузочные сектора (Boot сектора) дисков или сектор содержащий системный загрузчик(Master Boot Record) винчестера.

Сетевые вирусы — вирусы, распространяющиеся в различных компьютерных сетях и системах.

Макро вирусы — вирусы поражающие файлы Microsoft Office

Flash вирусы — вирусы поражающие микросхемы FLASH памяти BIOS.

По способу заражения вирусы делятся на:

Резидентные вирусы — вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы — вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

По деструктивным возможностям вирусы подразделяются на:

Безвредные вирусы — это вирусы ни как не влияющие на работу компьютера за исключение, быть может, уменьшения свободного места на диске и объема оперативной памяти.

Неопасные вирусы — вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий.

Опасные вирусы — это вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей.

Очень опасные вирусы — это вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

По особенностям алгоритма работы вирусы можно подразделить на:

Вирусы спутники(companion) — эти вирусы поражают EXE-файлы путем создания COM-файла двойника, и поэтому при запуске программы запустится, сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения «инфицированная» программа не изменяется.

Вирусы «черви» (Worms) — вирусы, которые распространяются в компьютерных сетях. Они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Иногда они оставляют временные файлы на компьютере но некоторые могут и не затрагивать ресурсы компьютера за исключением оперативной памяти и разумеется процессора.

«Паразитические» — все вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы не являются вирусами-спутниками и вирусами червями.

«Стелс-вирусы» (вирусы-невидимки, stealth) — представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков подставляют вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

«Полиморфные» (самошифрующиеся или вирусы-призраки, polymorphic) — вирусы, достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

«Макро-вирусы» — вирусы этого семейства используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы, заражающие текстовые документы редактора Microsoft Word.

По режиму функционирования:

— резидентные вирусы (вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам);

— транзитные вирусы (вирусы, которые выполняются только в момент запуска зараженной программы).

По объекту внедрения:

— файловые вирусы (вирусы, заражающие файлы с программами);

— загрузочные вирусы (вирусы, заражающие программы, хранящиеся в системных областях дисков).

В свою очередь, файловые вирусы подразделяются на вирусы, заражающие:

— исполняемые файлы;

— командные файлы и файлы конфигурации;

— составляемые на макроязыках программирования, или файлы, содержащие макросы (макровирусы — разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office );

— файлы с драйверами устройств;

— файлы с библиотеками исходных, объектных, загрузочных и оверлейных модулей, библиотеками динамической компоновки и т.п.

Загрузочные вирусы подразделяются на вирусы, заражающие:

— системный загрузчик, расположенный в загрузочном секторе и логических дисков;

— внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков.

По степени и способу маскировки:

— вирусы, не использующие средств маскировки;

— stealth-вирусы (вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных);

— вирусы-мутанты (MtE-вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса).

В свою очередь, MtE-вирусы делятся:

— на обычные вирусы-мутанты, в разных копиях которых различаются только зашифрованные тела, а дешифрованные тела вирусов совпадают;

— полиморфные вирусы, в разных копиях которых различаются не только зашифрованные тела, но и их дешифрованные тела.

Наиболее распространенные типы вирусов характеризуются следующими основными особенностями.

Файловый транзитный вирус целиком размещается в исполняемом файле, в связи, с чем он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу.

Файловый резидентный вирус отличается от нерезидентного логической структурой и общим алгоритмом функционирования. Резидентный вирус состоит из так называемого инсталлятора и программ обработки прерываний. Инсталлятор получает управление при активизации вирусоносителя и инфицирует оперативную память путем размещения в ней управляющей части вируса и замены адресов в элементах вектора прерываний на адреса своих программ, обрабатывающих эти прерывания. На так называемой фазе слежения, следующей за описанной фазой инсталляции, при возникновении какого-либо прерывания управление получает соответствующая подпрограмма вируса. В связи с существенно более универсальной по сравнению с нерезидентными вирусами общей схемой функционирования резидентные вирусы могут реализовывать самые разные способы инфицирования.

Stealth-вирусы пользуются слабой защищенностью некоторых операционных систем и заменяют некоторые их компоненты (драйверы дисков, прерывания) таким образом, что вирус становится невидимым (прозрачным) для других программ.

Полиморфные вирусы содержат алгоритм порождения дешифрованных тел вирусов, непохожих друг на друга. При этом в алгоритмах дешифрования могут встречаться обращения практически ко всем командам процессора Intel и даже использоваться некоторые специфические особенности его реального режима функционирования.

Макровирусы распространяются под управлением прикладных программ, что делает их независимыми от операционной системы. Подавляющее число макровирусов функционирует под управлением текстового процессора Microsoft Word. В то же время известны макровирусы, работающие под управлением таких приложений, как Microsoft Excel, Lotus Ami Pro, Lotus 1-2-3, Lotus Notes, в операционных системах фирм Microsoft и Apple.

Сетевые вирусы, называемые также автономными репликативными программами, или, для краткости, репликаторами, используют для размножения средства сетевых операционных систем. Наиболее просто реализуется размножение в тех случаях, когда сетевыми протоколами возможно и в тех случаях, когда указанные протоколы ориентированы только на обмен сообщениями. Классическим примером реализации процесса электронной почты является репликатор Морриса. Текст репликатора передается от одной ЭВМ к другой как обычное сообщение, постепенно заполняющее буфер, выделенный в оперативной памяти ЭВМ-адресата. В результате переполнения буфера, инициированного передачей, адрес возврата в программу, вызвавшую программу приема сообщения, замещается на адрес самого буфера, где к моменту возврата уже находится текст вируса. Тем самым вирус получает управление и начинает функционировать на ЭВМ-адресате.

«Лазейки», подобные описанной выше обусловленные особенностями реализации тех или иных функций в программном обеспечении, являются объективной предпосылкой для создания и внедрения репликаторов злоумышленниками.

Эффекты, вызываемые вирусами в процессе реализации ими целевых функций, принято делить на следующие группы:

— искажение информации в файлах либо в таблице размещения файлов (FAT-таблице), которое может привести к разрушению файловой системы в целом;

— имитация сбоев аппаратных средств;

— создание звуковых и визуальных эффектов, включая, например, отображение сообщений, вводящих оператора в заблуждение или затрудняющих его работу;

— инициирование ошибок в программах пользователей или операционной системе.

**2. Ассоциативная карта:**



1. **Концептуальная карта:**

