УДК 004.056.57

Общая классификация компьютерных вирусов.

Харченко А.Ю.

Белгородский государственный аграрный университет имени В.Я. Горина (Россия, 308503, Белгородская область, Белгородский район, п. Майский, ул. Вавилова, 1), e-mail kharchenkoa97@yandex.ru

Аннотация: **в данной статье приводится общая классификация компьютерных вирусов. Компьютерным вирусом называется программа, содержащая так называемый вредоносный код, которая обладает способностью к саморепликации, иными словами 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. Пользователи цифровой техники, а в частности компьютеров, находятся под постоянно растущей угрозой, исходящей от компьютерных вирусов и вредоносных программ. Поскольку разнообразие компьютерных вирусов слишком велико, то они, как и их биологические прообразы, нуждаются в классификации. Вирусы можно разделить на классы по следующим основным признакам: по деструктивному воздействию, по способу заражения, по среде обитания, по особенностям алгоритма. Определив к какому типу относится вирус можно оценить степень угрозы, метод борьбы и уровень необходимой защиты против данного вида вредоносного воздействия. Приведенная в данной статье классификация не может считаться полной, так как прогресс не стоит на месте, появляются всё новые и новые интеллектуальные устройства и соответственно вирусы, работающие на них.**

Ключевые слова: **компьютерный вирус, программа, компьютер, система.**

General classification of computer viruses.

Kharchenko A.Yu.

Belgorod State Agrarian University named after V.Ya. Gorin (Russia, 308503, Belgorod region, Belgorod region, Maisky settlement, Vavilov street, 1), e-mail kharchenkoa97@yandex.ru

Abstract: **this article provides a general classification of computer viruses. A computer virus is a program that contains a so-called malicious code that has the ability to self-replicate, in other words, the ability to create copies of itself, and integrate them into various objects and resources of computer systems, networks, etc. without the user's knowledge. At the same time, copies retain the ability to spread further. Users of digital technology, and in particular computers, are under a constantly growing threat emanating from computer viruses and malicious programs. Since the variety of computer viruses is too great, they, like their biological prototypes, need to be classified. Viruses can be divided into classes according to the following main features: destructive effects, the method of infection, the habitat, the features of the algorithm. Having determined to what type the virus belongs, it is possible to assess the degree of threat, the method of struggle and the level of necessary protection against this type of harmful influence. The classification cited in this article can not be considered complete, because progress does not stand still, there are more and more new intelligent devices and, accordingly, viruses that work on them.**

Key words: **computer virus, program, computer, system.**

К началу двадцать первого века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет еще одна составляющая - информация. Это самые разнообразные сведения, сообщения, известия, знания, умения.

В середине прошлого столетия появились специальные устройства - компьютеры, ориентированные на хранение и преобразование информации и произошла компьютерная революция.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них [5].

Компьютерный вирус - это специально написанная небольшая по размерам программа, имеющая специфический алгоритм, направленный на тиражирование копии программы, или её модификацию и выполнению действий развлекательного, пугающего или разрушительного характера.

Программа, внутри которой находится вирус, называется зараженной. С началом работы такой программы вирус получает доступ ко всей операционной системе. Вирус находит и заражает другие программы, а также выполняет какие-либо вредоносные действия. Например, портит файлы или таблицу размещения файлов на диске, занимает оперативную память и т.д. После того, как вирус выполнит свои действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Поэтому далеко не сразу пользователь узнаёт о присутствии вируса в машине [1].

К числу наиболее характерных признаков заражения компьютера вирусами относятся следующие:

- прекращение работы или изменение в рабочем режиме отдельных видов программного обеспечения, которое еще недавно было полностью исправным;
- снижение скорости или прекращение загрузки операционной системы;
- резкое изменение скорости работы компьютера в сторону снижения;
- исчезновение файлов, размещённых на жестком диске;
- изменения внешнего вида и размеров файлов;
- увеличение или уменьшение количества файлов на внешнем или жестком носителе;
- сокращение размеров свободной оперативной памяти;
- зависания и явные сбои в работе компьютерной техники;
- постоянное появление информации об ошибках;
- сигналы антивирусной программы об обнаружении вирусного ПО;

- появление самозагружающихся программ, сообщений или изображений [2].

В настоящее время известно более 50000 программных вирусов, которые классифицируют по следующим признакам:

1. По деструктивному воздействию

- Безвредные вирусы. Они не мешают работе компьютера, но могут уменьшать объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.
- Опасные вирусы. К ним относятся вирусы, которые могут привести к определенным сбоям в работе операционной системы или некоторых программ.

2. По способу заражения

- Резидентные вирусы. Чаще всего эти вирусы являются одной из разновидностей файловых и загрузочных. Причем самой опасной разновидностью. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются 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.

3. По среде обитания

- Файловые вирусы. До появления Интернета именно эти вирусы были самыми распространенными. На сегодняшний день известны зловредные программы, заражающие все типы выполняемых объектов любой операционной системы (для Windows опасности подвергаются исполняемые файлы (.exe, .com), командные файлы (.bat), драйвера (.sys), динамические библиотеки (.dll) и т. д.). Заражение происходит следующим образом. Вирус записывает свой код в файл-жертву. Кроме того, зараженный файл специальным образом изменяется. В результате при обращении к нему операционной системы (запуск пользователем, вызов из другой программы и т. п.) управление передается в первую очередь коду вируса, который может выполнить любые действия, заданные ему создателем. После выполнения своих действий вирус передает управление программе, которая выполняется нормальным образом. В следствии чего пользователь может долго не догадываться о заражении компьютера, если на нем не установлено специальное ПО.

- Загрузочные вирусы. Эти вирусы заражают загрузочные сектора жестких дисков. Принцип их действия заключается в следующем. Вирус добавляет свой код к одной из специальных программ, которые начинают выполняться после включения компьютера до загрузки операционной системы. В принципе в задачу этого ПО как раз и входят подготовка и запуск ОС. Таким образом, вирус получает управление и может выполнить определенные действия, например, записать себя в оперативную память. И только после этого будет загружаться операционная система. Вот только вирус уже будет находиться в памяти и сможет контролировать ее работу.
- Макровирусы. Эти вирусы представляют собой программы, которые выполнены на языках, встроенных в различные программные системы. Чаще всего жертвами становятся файлы, созданные различными компонентами Microsoft Office (Word, Excel и т.д.). Встроенный в эти программные продукты Visual Basic прекрасно подходит для написания макровирусов. Принцип их действия очень прост. Вирус записывает себя в DOT-файл, в котором содержатся все глобальные макросы, часть из которых он подменяет собой. После этого все файлы, сохраненные в этой программе, будут содержать макровирус. При этом он может выполнять множество различных деструктивных действий вплоть до удаления всех документов.
- Сетевые вирусы. Главной особенностью этих вирусов является возможность работы с различными сетевыми протоколами. То есть они могут различными путями записывать свой код на удаленном компьютере. Наибольшее распространение в наше время получили интернет-черви. Эти вирусы чаще всего используют для своей работы электронную почту, «прицепляясь» к письму. При этом на новом компьютере они либо автоматически выполняются, либо различными способами подталкивают пользователя к своему запуску [6].

4. По особенностям алгоритма

- 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 и «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 [3].

Любой вирус, независимо от принадлежности к определенным классам, должен иметь три функциональных блока: блок заражения (распространения), блок маскировки и блок выполнения деструктивных действий. Разделение на функциональные блоки означает, что к определенному блоку относятся команды программы вируса, выполняющие одну из трех функций, независимо от места нахождения команд в теле вируса.

После передачи управления вирусу, как правило, выполняются определенные функции блока маскировки. Например, осуществляется расшифровка тела вируса. Затем вирус осуществляет функцию внедрения в незараженную среду обитания. Если вирусом должны выполняться деструктивные воздействия, то они выполняются либо безусловно, либо при выполнении определенных условий.

Завершает работу вируса всегда блок маскировки. При этом выполняются, например, следующие действия: шифрование вируса (если функция шифрования реализована), восстановление старой даты изменения файла, восстановление атрибутов файла, корректировка таблиц ОС и др.

Последней командой вируса выполняется команда перехода на выполнение зараженных файлов или на выполнение программ ОС.

Для удобства работы с известными вирусами используются каталоги вирусов. В каталог помещаются следующие сведения о стандартных свойствах вируса: имя, длина,

заражаемые файлы, место внедрения в файл, метод заражения, способ внедрения в ОП для резидентных вирусов, вызываемые эффекты, наличие (отсутствие) деструктивной функции и ошибки. Наличие каталогов позволяет при описании вирусов указывать только особые свойства, опуская стандартные свойства и действия [4].

Знание классификации компьютерных вирусов позволяет оценить степень угрозы, метод борьбы и уровень необходимой защиты ПО от вредоносных воздействий.

Список литературы:

1. Алексеев Е.Г., Богатырев С.Д. Информатика. Мультимедийный электронный учебник. - URL: http://inf.e-alekseev.ru/text/Virus.html (дата обращения: 24.04.2018).
2. Как понять есть ли вирусы на компьютере? [Электронный ресурс] - URL: https://treeone.ru/126-priznaki-zarazheniya-kompyuternym-virusom / (дата обращения: 24.04.2018).
3. Классификация компьютерных вирусов [Электронный ресурс]. - URL: http://izi.vlsu.ru/teach/books/921/theory3.html (дата обращения: 24.04.2018).
4. Классификация компьютерных вирусов [Электронный ресурс]. - URL:http://sumk.ulstu.ru/docs/mszki/Zavgorodnii/10.1.html (дата обращения: 24.04.2018).
5. Компьютерные вирусы [Электронный ресурс]. - URL: http://www.km.ru/referats/75F9F2F1DD0D41249ABCAC2DD9777BDC / (дата обращения: 24.04.2018).
6. Компьютерные вирусы [Электронный ресурс]. - URL: http://trinity.e-stile.ru/tema-7-kompyuternye-virusy/ (дата обращения: 24.04.2018).