Новый подход к преподаванию темы «Компьютерные вирусы»

Н.Д. Григорян, И.Л. Мирзоян

Тема «Компьютерные вирусы» — важная составляющая предмета «Информатика» и в рамках преподавания этого предмета заслуживает особого внимания.

Специалистами разработаны различные способы преподавания этой темы. Мы хотим предложить новый подход, разработанный непосредственно в процессе преподавания, который позволяет детально проанализировать сущность компьютерных вирусов — как внешнюю, так и внутреннюю, выявить тесную взаимосвязь между биологическими и компьютерными вирусами, провести сравнительный анализ наиболее распространённых видов вирусов, определить методы борьбы с ними, рассмотреть моральную сторону вирусописания и осознать, что лучший метод лечения — это профилактика.

Взаимосвязь между биологическими и компьютерными вирусами

Компьютерный вирус — это программа, обладающая способностью размножаться, внедряться в программы, передаваться по линиям связи, сетям обмена информацией, выводить из строя системы управления.

Размножение компьютерного вируса посредством Всемирной сети Интернет происходит аналогично распространению биологического вируса в организме человека посредством кровеносной системы (в этом можно убедиться, исследовав математические модели распространения вирусов в Интернете и человеческом организме и рассмотрев сходность получающихся дифференциальных уравнений).

Цикл жизни компьютерного вируса (так же, как и биологического) обычно включает следующие периоды: внедрение, инкубационный, репликация (самозаражение) и проявление, причём инкубационный период — это один из самых опасных периодов как в случае компьютерного, так и биологического вируса, так как именно на этом этапе вирус выполняет свойственные ему вредоносно-целевые функции.

Учёные придумывают противоядия для борьбы с тем или иным штаммом биологического вируса, а микроорганизмы, в свою очередь, приспосабливаются, эволюционируют, становясь в определённом смысле более совершенными. Примерно то же происходит и с компьютерными вредоносными программами.

Анализ внешнего вида некоторых известных компьютерных вирусов и вредоносных программ

Так как человеческая физиология устроена так, что человек легче воспринимает информацию, которую видит, особое внимание полезно уделить работам румынского художника Алекса Драгулеску, специализирующегося на трёхмерных изображениях. Он воспроизвёл внешний вид множества известных компьютерных вирусов и вредоносных программ, опираясь на вполне объективные данные — частоту и длительность обращений компьютерных вирусов к API, памяти и файловой системе.

Исследование разновидностей компьютерных вирусов и их враждебного воздействия

Современные компьютерные вирусы обладают широкими возможностями враждебного воздействия, начиная от безобидных шуток и кончая серьёзными повреждениями аппаратуры.

Рассмотрим разновидности компьютерных вирусов и остановимся на некоторых из них.

Файловые вирусы — это вирусы, которые при размножении используют какую-либо операционную систему. Внедрение файлового вируса возможно во все исполняемые файлы популярных операционных систем — DOS, Windows, MacOS, UNIX и т.д.

Файловый нерезидентный 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 тем, что заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память ПЭВМ.

Существуют следующие основные разновидности файловых вирусов: обычные, которые встраивают свой код в файл, по возможности не нарушая его функциональности, а также на overwriting, паразитические (parasitic), компаньон-вирусы (companion), вирусы-черви и т.д.

- Overwriting-вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое, после чего файл перестаёт работать и не восстанавливается. Такие вирусы быстро обнаруживают себя, так как операционная система и приложения перестают работать.
- Parasitic-вирусы изменяют содержимое файлов, оставляя при этом сами файлы полностью или частично работоспособными. Такие вирусы подразделяются на вирусы, записывающиеся в начало, в конец и в середину файлов.
- Companion-вирусы не изменяют заражаемых файлов, а создают для заражаемого файла файл-двойник, причём при запуске заражённого файла управление получает именно этот двойник, т. е. вирус.
- Файловые черви (worms) являются разновидностью компаньон-вирусов, однако не связывают своё

присутствие с каким-либо выполняемым файлом. При размножении они только копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

• Макровирусы являются программами на макроязыках, встроенных в некоторые системные обработки данных (текстовые редакторы, электронные таблицы и т.д.). Они заражают документы и электронные таблицы ряда офисных редакторов. Для размножения они используют возможности макроязыков и при их помощи переносят себя из одного заражённого файла в другие. Вирусы этого типа получают управление при открытии заражённого файла и идентифицируют файлы, к которым впоследствии идёт обращение из соответствующего офисного приложения — Word, Excel и пр.

• Скрипт-вирусы — это вирусы, написанные на скрипт-языках, таких как Visual Basic script, Java Script и др. Они, в свою очередь, делятся на вирусы для DOS, для Windows, для других систем. Помимо описанных классов существует большое количество сочетаний: например файлово-загрузочный вирус, заражающий как файлы, так и загрузочные секторы дисков, или сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

• Стелс-вирусы (невидимки) скрывают факт своего присутствия в системе. Они изменяют информацию таким образом, что файл появляется перед пользователем в незаражённом виде, например, временно лечат заражённые файлы.

• Полиморфик-вирусы используют шифрование для усложнения процедуры определения вируса. Эти вирусы не содержат постоянных участков кода, что достигается шифрованием основного тела вируса и модификациями программы-расшифровщика. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Именно поэтому полиморфик-вирус невозможно обнаружить при помощи выявления участков постоянного кода, специфичных для конкретного вируса.

Анализ наиболее распространённых средств нейтрализации вирусов

Наиболее распространённые средства нейтрализации вирусов — программные антивирусы. Антивирусы появились более десяти лет назад, в первое время они распространялись как бесплатное противоядие. Не было должной поддержки и сервиса, поскольку проекты были некоммерческими. Как индустрия служба создания и предоставления антивирусных программ оформилась примерно в 1992 году.

Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы: детекторы, фаги, вакцины, прививки, ревизоры, мониторы.

• Детекторы обеспечивают выявление вирусов посредством просмотра исполняемых файлов и поиска так называемых сигнатур — устойчивых последовательностей байтов, имеющихся в телах известных вирусов. Наличие сигнатуры в каком-либо

файле свидетельствует о его заражении соответствующим вирусом. Антивирус, обеспечивающий возможность поиска различных сигнатур, называют полидетектором.

• Фаги выполняют функции, свойственные детекторам, но, кроме того, «излечивают» инфицированные программы посредством «выкусывания» («пожирания») вирусов из их тел. По аналогии с полидетекторами фаги, ориентированные на нейтрализацию различных вирусов, именуют полифагами.

• Вакцины. В отличие от детекторов и фагов, вакцины по своему принципу действия напоминают сами вирусы. Вакцина имплантируется в защищаемую программу и запоминает ряд количественных и структурных характеристик последней.

Если вакцинированная программа не была к моменту вакцинации инфицированной, то при первом же после заражения запуске произойдёт следующее.

Активизация вирусоносителя приведёт к получению управления вирусом, который, выполнив свои целевые функции, передаст управление вакцинированной программе. В последней, в свою очередь, сначала управление получит вакцина, которая выполнит проверку соответствия заполненных ею характеристик аналогичным характеристикам, полученным в текущий момент. Если указанные наборы характеристик не совпадают, то делается вывод об изменении текста вакцинированной программы вирусом. Характеристиками, используемыми вакцинами, могут быть длина программы, её контрольная сумма и т.п.

• Прививки. Принцип действия прививок основан на учёте того обстоятельства, что любой вирус, как правило, помечает инфицированные программы каким-либо признаком с тем, чтобы не выполнять их повторное заражение. В ином случае имело бы место многократное инфицирование, сопровождаемое существенным и поэтому легко обнаруживаемым увеличением объёма заражённых программ.

Прививка, не внося никаких других изменений в текст защищаемой программы, помечает её тем же признаком, что и вирус, который, таким образом, после активизации и проверки наличия указанного признака считает её инфицированной и «оставляет в покое».

• Ревизоры обеспечивают слежение за состоянием файловой системы, используя для этого подход, аналогичный реализованному в вакцинах. Программа-ревизор в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра файлов.

Если при этом обнаруживается, что согласно имеющейся системной информации файл с момента предшествующего просмотра не обновлялся пользователем, а сравниваемые наборы характеристик не совпадают, то файл считается инфицированным.

Характеристики исполняемых файлов, получаемые в ходе очередного просмотра, запоминаются в отдельном файле, в связи с чем увеличения длин исполняемых файлов, имеющего место при вакцинировании, в данном случае не происходит.

Другое отличие ревизоров от вакцин состоит в том, что каждый просмотр исполняемых файлов ревизором требует повторного запуска.

• Монитор представляет собой резидентную программу, обеспечивающую перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающую у пользователей подтверждение на выполнение операций, следующих за прерыванием. В случае запрета или отсутствия подтверждения монитор блокирует выполнение пользовательской программы.

Антивирусы рассмотренных типов существенно повышают вирусозащиту отдельных ПЭВМ и информационно-вычислительных сетей в целом, однако в связи со свойственными им ограничениями, естественно, не являются панацеей. Так, для разработки детекторов, фагов и прививок нужно иметь тексты вирусов, что возможно только для выявленных вирусов.

Рассмотрение морально-этической стороны вирусописания

Компьютерные вирусы — это первый удачный эксперимент по созданию искусственной жизни с неудачным выбором формы её жизнедеятельности. Борьба программистов-вирусописателей и создателей антивирусов приводит к эволюции этой формы жизни.

Вероятно, многие задумывались над вопросом: какие же качества человеческой психики приводят к такому парадоксальному феномену, как вирусописание? Ведь вирусописатели не получают за свой труд денег, преследуются по закону, сами страдают от вирусных атак и тем не менее продолжают свою деятельность. Было бы интересно исследовать состояние здоровья программистов-вирусописателей на выявление наличия у них разных биологических вирусов, так как только нездоровый человек способен разрушать компьютерные системы, от которых в некоторой степени зависит его безопасность.

При разработке методики преподавания была выявлена необходимость исследовать и анализировать психологическое воздействие компьютерных вирусов на поведение пользователя. Такое воздействие — хорошая среда для проведения разнообразных исследований, так как психологический аспект этого исследования актуален и необходим, ведь с каждым днём в геометрической прогрессии возрастает как количество вирусов и видов их вредоносного воздействия, так и число пользователей, вовлечённых в борьбу с вредоносными программами. Исследование должно быть продолжено, так как его результаты могут показать закономерную взаимосвязь психологического воздействия на поведение человека как компьютерного, так и биологического вирусов.