3. Проблема вирусного заражения программного обеспечения

Содержание темы:

3.1. Компьютерные вирусы и их классификация.
3.2. Структура современных вирусных программ.
3.3. Основные каналы распространения компьютерных вирусов.
3.4. Методы антивирусной защиты.
3.5. Методы обнаружения компьютерных вирусов.
3.6. Методы удаления компьютерных вирусов.

3.1. Компьютерные вирусы и их классификация

*Впервые термин **компьютерный вирус** ввел в употребление специалист из США Ф. Коэн в 1984 г.*

Компьютерный вирус – это автономно функционирующая программа, обладающая одновременно тремя ***свойствами:***

- способностью к включению своего кода в тела других файлов и системных областей памяти компьютера;
- последующему самостоятельному выполнению;
- самостоятельному распространению в компьютерных системах.

3.1. Компьютерные вирусы и их классификация (продолжение)

Компьютерные вирусы классифицируются по следующим признакам:

1) По способу распространения в КС:
   - **файловые вирусы**, заражающие файлы одного или нескольких типов;
   - **загрузочные вирусы**, заражающие загрузочные сектора жестких дисков и дискет;
   - **комбинированные вирусы**, способные заражать и файлы, и загрузочные сектора дисков.
2) По способу заражения других объектов КС:
   - **резидентные вирусы**, часть кода которых постоянно находится в оперативной памяти компьютера и заражает другие объекты КС;
   - **нерезидентные вирусы**, которые заражают другие объекты КС в момент открытия уже зараженных ими объектов.

3.1. Компьютерные вирусы и их классификация (продолжение)

3) По деструктивным возможностям:
   - **безвредные вирусы**, созданные в целях обучения, однако снижающие эффективность работы КС за счет потребления ее ресурсов (времени работы центрального процессора, оперативной и внешней памяти и др.);
   - **неопасные вирусы**, создающие различные звуковые и видеоэффекты;
   - **опасные и очень опасные вирусы**, вызывающие сбои в работе программного и (или) аппаратного обеспечения компьютера, потерю программ и данных.
4) По особенностям реализуемого алгоритма:
   - **вирусы-спутники**, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы (при открытии зараженного файла открывается файл с кодом вируса, а после выполнения предусмотренных автором действий открывается исходный файл);

3.1. Компьютерные вирусы и их классификация (продолжение)

- **паразитические вирусы**, которые изменяют содержимое заражаемых объектов;
- **вирусы-невидимки («стелс»-вирусы)**, в которых путем перехвата обращений операционной системы к зараженным объектам и возврата вместо них незараженных данных скрывается факт присутствия вируса в КС (при собственном обращении к дисковой памяти вирусы-невидимки также используют нестандартные средства для обхода средств антивирусной защиты);
- **вирусы-призраки (полиморфные вирусы)**, каждая следующая копия которых в зараженных объектах отличается от предыдущих (не содержит одинаковых цепочек команд за счет применения шифрования).

3.2. Структура современных вирусных программ

3.2.1. Загрузочные вирусы

Они заражают главный загрузочный сектор жесткого диска (Master Boot Record, MBR), загрузочный сектор системной дискеты или загрузочного компакт-диска (Boot Record, BR), подменяя находящиеся в них программы начальной загрузки и загрузки операционной системы своим кодом.

Исходное содержимое этих секторов сохраняется в одном из свободных секторов диска или непосредственно в теле вируса.

3.2.1. Загрузочные вирусы (продолжение)

После заражения MBR, являющегося первым сектором нулевой головки нулевого цилиндра жесткого диска, вирус получает управление сразу по завершении работы процедуры проверки оборудования (POST) и программы BIOS Setup.

Получив управление, ***загрузочный вирус выполняет следующие действия:***

1) копирование своего кода в конец оперативной памяти компьютера, уменьшая тем самым размер ее свободной части;
2) переопределение «на себя» нескольких прерываний BIOS, в основном связанных с обращением к дискам;
3) загрузка в оперативную память компьютера истинной программы начальной загрузки, в функции которой входит просмотр таблицы разделов жесткого диска, определение активного раздела, загрузка и передача управления программе загрузки операционной системы активного раздела;
4) передача управления истинной программе начальной загрузки.

3.2.1. Загрузочные вирусы (продолжение)

Аналогичным образом работает и загрузочный вирус в BR, замещая программу загрузки операционной системы.

Формой заражения компьютера загрузочным вирусом является попытка загрузки с компакт-диска или дискеты, загрузочный сектор которых заражен вирусом. Эта ситуация возникает, когда зараженный диск остается в дисководе при выполнении перезагрузки операционной системы. После заражения главного загрузочного сектора жесткого диска вирус распространяется при первом обращении к любому незараженному диску.

Загрузочные вирусы, как правило, относятся к группе резидентных вирусов.

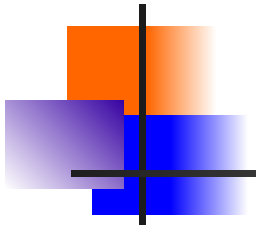
Изменение в BIOS порядка использования дисковых устройств при загрузке устранит один из каналов заражения компьютера загрузочными вирусами.

3.2. Структура современных вирусных программ

3.2.2. Файловые вирусы

Они заражают файлы различных типов. При заражении вирус записывает свой код в начало, середину или конец файла либо сразу в несколько мест. Исходный файл изменяется таким образом, что после его открытия управление немедленно передается коду вируса. ***Код вируса выполняет следующую последовательность действий:***

1) заражение других файлов и (комбинированные вирусы) системных областей дисковой памяти;
2) установка в оперативной памяти собственных резидентных модулей (резидентные вирусы);
3) выполнение других действий, зависящих от реализуемого вирусом алгоритма;
4) продолжение обычной процедуры открытия файла (например, передача управления исходному коду зараженной программы).



3.2.2. Файловые вирусы (продолжение)

Вирусы в файлах документов, созданных программами пакета Microsoft Office, распространяются с помощью включенных в них **макросов** (процедур на языке программирования Visual Basic for Applications, VBA). Поэтому такие вирусы иногда называют ***макровирусами***.

VBA поддерживает автоматически выполняемые макросы, связанные с определенными событиями (например, с открытием документа) или определенными действиями пользователя (например, при вызове команды сохранения документа). Документ Microsoft Office может также содержать макросы, автоматически получающие управление при нажатии пользователем определенной комбинации клавиш на клавиатуре или достижении некоторого момента времени (даты, времени суток).

3.3. Основные каналы распространения компьютерных вирусов:

- электронная почта, сообщения которой могут содержать зараженные присоединенные файлы;
- свободное и условно свободное программное обеспечение, размещенное на общедоступных узлах сети Интернет и случайно или намеренно зараженное вирусами;
- локальные компьютерные сети организаций;
- обмен зараженными файлами на дискетах или записываемых компакт-дисках;
- использование нелицензионных компакт-дисков с программным обеспечением и другими информационными ресурсами.

3.4. Методы антивирусной защиты:

- Физическое или логическое отключение накопителей на гибких магнитных дисках и компакт-дисках *(для логического отключения в Windows 7: открыть окно «Компьютер», выбрать диск, изменить его свойства)*.
- Разграничение прав отдельных пользователей и групп на доступ к папкам и файлам операционной системы и других пользователей.
- Ограничение времени работы в КС привилегированных пользователей (для выполнения действий в КС, не требующих дополнительных полномочий, администраторы должны использовать учетную запись с обычными привилегиями).
- Использование, как правило, только лицензионного программного обеспечения.
- Выделение не подсоединенного к локальной сети компьютера для тестирования полученного из ненадежных источников программного обеспечения.

3.4. Методы антивирусной защиты (продолжение):

- Использование встроенной в программы пакета Microsoft Office защиты от потенциально опасных макросов *(более подробно см. далее)*.
- Использование свойств обозревателя Microsoft Internet Explorer *(более подробно см. далее)*.
- Защита от заражения загрузочными вирусами, устанавливаемая с помощью программы BIOS Setup (параметр Anti-Virus Protection или аналогичный функции Advanced BIOS Features или аналогичной). Включение этой защиты обеспечит выдачу предупреждающего сообщения при попытке записи в загрузочные сектора дисковой памяти. К недостаткам подобной защиты от заражения вирусами относится то, что она может быть отключена кодом вируса прямым редактированием содержимого энергонезависимой CMOS-памяти, хранящей настройки, которые были установлены программой BIOS Setup.
- Использование антивирусных программ.

3.4.1. Защита от потенциально опасных макросов в программах пакета Microsoft Office

Эта защита устанавливается в пакете Microsoft Office 2003 с помощью команды меню «Сервис | Макрос | Безопасность».

Возможен выбор одного из четырех уровней защиты:

1) Очень высокая. Разрешается запуск только макросов, установленных в надежных расположениях. Все остальные подписанные и неподписанные макросы отключаются.

   Для полного отключения всех макросов можно задать уровень безопасности «Очень высокая» и отключить макросы, установленные в надежных расположениях. Чтобы отключить макросы, установленные в надежных расположениях, следует выбрать меню «Сервис | Макрос | Безопасность», а затем перейти на вкладку «Надежные издатели» и снять флажок «Доверять всем установленным надстройкам и шаблонам».

3.4.1. Защита от потенциально опасных макросов в программах пакета Microsoft Office (продолжение)

2) Высокая. Выполнение неподписанных макросов автоматически запрещается. Порядок обработки подписанных макросов определяется источником макроса и состоянием подписи:
   - *Надежный источник. Подпись верна. Выполнение макросов автоматически разрешается, затем файл открывается.*
   - *Неизвестный автор. Подпись верна. Выводится диалоговое окно со сведениями о сертификате. Выполнение макросов может быть разрешено только в том случае, если пользователь укажет, что он доверяет автору и центру сертификации.*
   - *Любой автор. Подпись неверна, вероятны вирусы. Пользователь получает предупреждение о том, что макросы, вероятно, заражены вирусами. Выполнение макросов автоматически запрещается.*
   - *Любой автор. Подпись сделана после истечения срока действия сертификата, либо после отзыва сертификата. Пользователь предупреждается об истечении срока действия сертификата. Выполнение макросов автоматически запрещается.*

3.4.1. Защита от потенциально опасных макросов в программах пакета Microsoft Office (продолжение)

3) Средняя. При открытии содержащего макросы документа решение об отключении этих макросов будет приниматься самим пользователем. Если подпись неверна, пользователь получает предупреждение о том, что макросы, вероятно, заражены вирусами. В этом случае выполнение макросов автоматически запрещается.
4) Низкая. Все макросы в открываемом документе будут выполняться (корпорация Microsoft рекомендует устанавливать данный уровень безопасности только при наличии антивирусных программ на компьютере пользователя и полной уверенности в безопасности открываемых документов).

3.4.1. Защита от потенциально опасных макросов в программах пакета Microsoft Office (продолжение)

Программа пакета Microsoft Office «Цифровой сертификат для проектов VBA» создает подписанный цифровой сертификат, который может использоваться с персональными макросами только на данном компьютере.

Для получения подписи под макросами документа Microsoft Office необходимо открыть окно системы программирования Microsoft Visual Basic. В этом окне выполняется команда «Tools | Digital Signature» и в появившемся окне цифровой подписи выбирается сертификат открытого ключа ЭЦП, который в дальнейшем будет использован для проверки подписи.

Установка защиты от потенциально опасных макросов не позволяет отделить макросы, расширяющие функциональность приложений Microsoft Office, от макросов, содержащих вирусы. Кроме того, некоторые из макровирусов, получив однажды управление, могут понизить уровень безопасности до самого низкого и тем самым блокировать встроенную защиту от макросов.

3.4.2. Использование свойств обозревателя Microsoft Internet Explorer

Необходимо в меню «Сервис» выбрать пункт «Свойства обозревателя» и перейти на вкладку «Безопасность». Всем узлам зоны *Интернет* (в нее не входят узлы, отнесенные к другим зонам) целесообразно назначить ***высокий уровень безопасности***, в соответствии с которым будут, в частности, отключены:

- возможность загрузки файлов с этих узлов;
- выполнение интерактивного содержимого.

3.5. Методы обнаружения компьютерных вирусов:

1) Просмотр (сканирование) проверяемых объектов (системных областей дисковой и оперативной памяти, а также файлов заданных типов) в поиске **сигнатур** (уникальных последовательностей байтов) известных вирусов. Соответствующие программные средства называют **сканерами**, а при наличии дополнительной функции удаления обнаруженных вирусов – **полифагами**.

Недостатки программ-сканеров и полифагов:

- необходимость постоянного обновления баз данных сигнатур известных вирусов, которые используются при поиске;
- неспособность обнаружения новых вирусов;
- недостаточная способность обнаружения сложных полиморфных вирусов.

Примеры полифагов: Kaspersky Anti-Virus, Dr.Web, Nod32.

3.5. Методы обнаружения компьютерных вирусов (продолжение):

2) Обнаружение изменений в объектах КС путем сравнения их вычисленных при проверке хеш-значений с эталонными (или проверки электронной цифровой подписи (ЭЦП) для этих объектов). При вычислении хеш-значений объектов могут учитываться и характеристики (атрибуты) проверяемых файлов. Подобные программные средства называют **ревизорами**, или **инспекторами**. Потенциально они могут обнаружить и новые вирусы.

Недостатки программ-ревизоров:

- не все изменения проверяемых объектов вызываются вирусным заражением (например, обновление отдельных компонентов операционной системы, легальное изменение файлов документов);
- программы-ревизоры не могут помочь при записи на жесткий диск компьютера уже зараженного файла, хотя могут обнаружить заражение вирусом новых объектов.

Пример ревизора: ADinf.

3.5. Методы обнаружения компьютерных вирусов (продолжение):

3) Эвристический анализ – проверка системных областей памяти и файлов с целью обнаружения фрагментов исполнимого кода, характерного для компьютерных вирусов (например, установка резидентной части кода вируса). Потенциально эвристические анализаторы способны обнаружить (с определенной вероятностью) любые новые разновидности компьютерных вирусов.

Недостаток эвристического анализа: из-за того, что при эвристическом сканировании ищутся не вредоносные объекты как таковые, а объекты, похожие на них, возможны ложные срабатывания.

Пример эвристического анализатора: Dr.Web.

3.5. Методы обнаружения компьютерных вирусов (продолжение):

4) Постоянное присутствие в оперативной памяти компьютера с целью контроля всех подозрительных действий других программ: попыток изменения загрузочных секторов дисков, установки резидентного модуля и т.п. Подобные программы называются **мониторами**. Мониторы также автоматически проверяют на наличие известных вирусов все устанавливаемые дискеты и компакт-диски, открываемые файлы и запускаемые программы. Обычно мониторы используют общую со сканерами базу сигнатур вирусов и загружаются в оперативную память в процессе загрузки операционной системы.

Недостаток программ-мониторов: снижение эффективности работы КС за счет потребления процессорного времени и уменьшения размера свободной оперативной памяти.

Примеры программ-мониторов: Kaspersky Anti-Virus, Dr.Web, Nod32.

Большинство современных комплексов антивирусных программ включают в свой состав полифаги (с дополнительной функцией эвристического анализа), мониторы и, реже, инспекторы (ревизоры).

3.6. Методы удаления компьютерных вирусов

При автоматическом удалении вирусов, обнаруженных антивирусными программами, могут применяться два основных метода:

1) удаление уже известных вирусов с помощью заранее разработанного алгоритма лечения файлов, зараженных данным типом вируса;
2) попытка удаления неизвестных до этого времени вирусов на основе сведений об общих принципах работы вирусов и (или) предварительно сохраненной информации о незараженном файле.

Рекомендуется перед удалением обнаруженных вирусов выполнить копирование зараженных файлов на резервный носитель информации, чтобы не потерять ценных данных.

3.6. Методы удаления компьютерных вирусов (продолжение)

Сложные разновидности даже известных вирусов не всегда могут быть удалены, а зараженные ими файлы восстановлены. Поэтому ***для обязательной подготовки к возможному заражению объектов КС вирусами необходимо:***

- подготовить защищенную от записи системную дискету или загрузочный компакт-диск, записав на них последние версии антивирусных программ и баз сигнатур известных вирусов;
- постоянно обновлять версии установленного в КС антивирусного программного обеспечения;
- регулярно проверять объекты КС антивирусными программами;
- проверять на наличие вирусов файлы, присоединенные к входящим сообщениям электронной почты;
- регулярно выполнять резервное копирование наиболее важных файлов;
- отключить максимально возможное число каналов распространения вирусов (см. подраздел 3.3).

Литература

Методы и средства защиты информации в компьютерных системах: учеб. пособие для студ. высш. учеб. заведений / П.Б. Хорев. – М.: Издательский центр «Академия», 2008. – 256 с.