Федеральное агентство по образованию Российской Федерации ГОУ ВПО

Факультет социологии и философии

# Кафедра социологии

Реферат

"Информационная безопасность. Вредоносное ПО. Вирусы, шпионское ПО, руткиты"

Ижевск 2008г.

Содержание

Введение

1. Информационная безопасность

1.1 Понятие информационной безопасности

1.2 Проблемы информационной безопасности

2. Вредоносное ПО

2.1 Троянские кони, программные закладки и сетевые черви

2.2 Вирусы

2.3 Шпионское ПО

2.4 Руткиты

Заключение

Список использованной литературы

Введение

Компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации. Отдельные сферы деятельности (системы государственного управления, банки, информационные сети и т. п.) требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования в соответствии с характером и важностью решаемых задач.

1. Информационная безопасность

1.1 Понятие информационной безопасности

Говоря об информационной безопасности имеют в виду компьютерную безопасность. Информация, находящаяся на электронных носителях играет большую роль в жизни современного общества. Причины уязвимости такой информации различны: огромные объемы, многоточечность и возможная анонимность доступа, возможность "информационных диверсий"... Все это делает задачу обеспечения защиты информации большой проблемой. Понятие "компьютерной" информационной безопасности в целом - более широкое по сравнению с информационной безопасностью относительно "традиционных" носителей.

Информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. А также это меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

Для поддержания режима информационной безопасности особенно важны программно-технические меры, поскольку основная угроза компьютерным системам исходит от них самих: сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п. Напомним названия ключевых механизмов обеспечения информационной безопасности:

- идентификация и аутентификация;

- управление доступом;

- протоколирование и аудит;

- криптография;

- экранирование.

1.2 Проблемы информационной безопасности

Широкое внедрение информационных технологий в жизнь современного общества привело к появлению ряда общих проблем информационной безопасности:

* необходимо гарантировать непрерывность и корректность функционирования важнейших информационных систем (ИС), обеспечивающих безопасность людей и экологической обстановки;
* необходимо обеспечить защиту имущественных прав граждан, предприятий и государства в соответствии с требованиями гражданского, административного и хозяйственного права (включая защиту секретов и интеллектуальной собственности);
* необходимо защитить гражданские права и свободы, гарантированные действующим законодательством (включая право на доступ к информации).

Следует знать, что любая информационная система потенциально уязвима. И эта уязвимость по отношению к случайным и предумышленным отрицательным воздействиям выдвинула проблемы информационной безопасности в разряд важнейших, определяющих принципиальную возможность и эффективность применения ряда ИС в гражданских и военных отраслях.

Основная работа по снижению дестабилизирующих факторов в области информационной безопасности - раскрыть собственно суть проблемы, конкретизировать дестабилизирующие факторы и представить основные методы, способные значительно повысить защищенность ИС. Эта проблема в значительной степени решается посредством методов, средств и стандартов, поддерживающих системный анализ, технологию разработки и сопровождения программных систем (ПС) и баз данных (БД).

Обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

2. Вредоносное ПО

Вредоносное ПО - это класс программ, предназначенных для выполнения различных несанкционированных пользователем действий, иногда направленных на причинение ущерба (уничтожение или повреждение данных, замедление работы и т. д.).

В наше время даже человек, не связанный с компьютерами, приблизительно знает, что такое компьютерный вирус. Однако не каждый знает, что компьютерные вирусы - только часть вредоносного программного обеспечения. На самом деле не каждая программа, которая может негативно повлиять на работу компьютера, является вирусом.

Существуют следующие основные виды вредоносного ПО:

* Троянские кони, программные закладки и сетевые черви;
* Вирусы;
* Шпионское ПО;
* Руткиты;
* Прочие вредоносные программы.

2.1 Троянские кони, программные закладки и сетевые черви

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы – вносить в них разрушающие функции. Также это программа, которая на первый взгляд осуществляет легитимные действия, но ее выполнение может нанести серьезный вред. Троянские кони часто применяются для получения паролей с компьютеров. В отличие от вируса, троянский конь сам себя не тиражирует.

"Троянские кони" представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб ВС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

Возможные деструктивные функции, реализуемые "троянскими конями" и программными закладками:

1. Уничтожение информации. Конкретный выбор объектов и способов уничтожения зависит только от фантазии автора такой программы и возможностей ОС. Эта функция является общей для троянских коней и закладок.

2. Перехват и передача информации. В качестве примера можно привести реализацию закладки для выделения паролей, набираемых на клавиатуре.

3. Целенаправленная модификация кода программы, интересующей нарушителя. Как правило, это программы, реализующие функции безопасности и защиты.

Сетевой червь - программа, которая тиражирует себя на жестком диске компьютера, в его памяти и по сети, загружая тем самым ресурсы системы. Червь отличается от вируса тем, что не несет в себе никакой "логической бомбы", его единственное назначение — самотиражирование. Некоторые черви распространяются через сообщения электронной почты.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

Если "троянские кони" наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа "червь", действующих в компьютерных сетях, – взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды.

2.2 Вирусы

Вирусы получили широкое распространение в компьютерной технике. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность... 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.

Вирусы классифицируются по следующим основным признакам:

1. среда обитания

2. способ заражения

3. степень воздействия

4. особенности алгоритма работы

По среде обитания вирусы можно разделить на:

1. файловые

2. загрузочные

3. файлово-загрузочные

4. сетевые

5. макро-вирусы

По способу заражения вирусы делятся на:

1. резидентные

2. нерезидентные

По степени воздействия вирусы можно разделить на следующие виды:

1. неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках. Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах

2. опасные вирусы, которые могут привести к различным нарушениям в работе компьютера.

3. очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

## Макро-вирусы:

Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и Office. Существуют также макро-вирусы, заражающие документы баз данных Microsoft Access.

## Файловые вирусы:

К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо или каких-либо ОС.

Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств.

## Сетевые вирусы:

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

Способы противодействия компьютерным вирусам можно разделить на несколько групп:

1.профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения;

2.методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса;

3.способы обнаружения и удаления неизвестного вируса.

Oдним из oбщeпpинятыx мeтoдoв профилактики заболеваний ПК являeтcя иcпoльзoвaниe пpoгpaмм, кoтopыe тщaтeльнo oбcлeдyют диcки, пьrтaяcь oбнapyжить и oбeзвpeдить виpycы. Boзмoжнo тaкжe иcпoльзoвaниe peзидeнтньrx пpoгpaмм DOS, пocтoяннo пpoвepяющиx вaшy cиcтeмy на виpycы. Peзидeнтныe пpoгpaммы имеют cлeдyющee пpeимyщecтвo: oни пpoвepяют вce пpoгpaммы нa виpycы при кaждoм иx вьшoлнeнии. Peзидeнтныe пpoгpaммы должны быть oчeнь тщaтeльнo paзpaбoтaны, т.к. инaчe oни бyдyт зaдepживaть зaгpyзкy и выпoлнeниe пpoгpaмм. Hepeзидeнтныe пpoгpaммы эффeктивны пpи нeoбxoдимocти oднoвpeмeннoгo oбcлeдoвaния вceй cиcтeмы нa виpycы и иx oбeзвpeживaния. Oни пpeдcтaвляют coбoй cpeдcтвo, дoпoлняющee peзидeнтныe пporpaммы.

Компьютерные вирусы – это одна из основных проблем связанных с компьютером, поэтому Bы дoлжны пoмнить o нeoбxoдимocти peгyляpнoгo выпoлнeния aнтивиpycнoй пpoгpaммы. K coжaлeнию, кaк пoкaзывaeт oпыт, oб этoм чacтo зaбывaют. Пpeнeбpeжeниe пpoфилaктичecкими пpoвepкaми вaшero кoмпьютepa yвeличивaет pиcк инфициpoвaния нe тoлькo вaшeй кoмпьютepнoй cиcтeмы, нo и pacпpocтpaнeния виpyca нa дpyгиe кoмпьютepы.

2.3 Шпионское ПО

Шпионским ПО называют любую программу, файлы Cookie или записи реестра, которые тайно собирают информацию о вашей деятельности в Интернете. Такие программы используются для передачи этих данных компаниям, использующим их в рекламных целях. Однако по данным Коалиции по борьбе со шпионским ПО (Anti-spyware Coalition) шпионское ПО становится все более вредоносным и все чаще используется для кражи данных с помощью методов, которые сложно обнаружить. Многие люди считают, что шпионское ПО нарушает неприкосновенность личной жизни.

Откуда же берется шпионское ПО? Распространители шпионского ПО часто добавляют его в пакет с другим программным обеспечением. Как правило, оно загружается в комплекте с условно-бесплатными программами или файлами из систем совместного доступа, таких как Kazaa, Limewire или Morpheus, а также с веб-сайтов с экранными заставками, виджетами и содержимым "для взрослых". Для распространения нежелательных программ также используются слабые места систем безопасности и мошеннические приемы.

Многие люди считают, что шпионское ПО нарушает неприкосновенность личной жизни. Помимо этого, шпионское ПО является раздражающей помехой для пользователя. Такие программы устанавливаются без ведома пользователя, наносят значительный урон системе безопасности и самостоятельно восстанавливаются после удаления. Кроме потенциального вреда компьютерной системе, они являются источником навязчивых всплывающих окон, отображают оскорбительные материалы, замедляют работу компьютера и конфликтуют с другими программами. Чрезмерное количество шпионского ПО на компьютере приводит к регулярным сбоям и зависаниям.

Лучший способ защитить себя от шпионского ПО при работе с Интернетом – предупредительные меры. Своевременно узнавайте о новых угрозах и используйте безопасные методы работы с Интернетом:

* Выполните чистку компьютера с помощью антивирусных программ и программ для защиты от шпионского ПО.
* Своевременно устанавливайте новейшие исправления средств защиты браузера и операционной системы.
* По возможности активируйте функцию автоматического обновления программного обеспечения.
* Установите более высокий уровень безопасности и конфиденциальности браузера.
* Не загружайте файлы из Интернета необдуманно и будьте предельно осторожны при использовании одноранговых сетей.
* Не щелкайте всплывающую рекламу. Если вы это сделаете, рекламные окна начнут размножаться.
* С помощью средства проверки репутации, расположенного в верхней части страниц WOT, ознакомьтесь с оценочной картой репутации того или иного веб-сайта.

Шпионское ПО, как правило, разрабатывается компаниями, которые пытаются заработать различными незаконными способами. В этом случае, они собирают информацию о пользователях для того, чтобы определить их пристрастия и предпочтения. Затем эта информация используется этими компаниями для собственных нужд или для продажи третьим лицам.

2.4 Руткиты

Руткиты вовсе не новое явление, поскольку их появление связывают еще с UNIX-платформами. Однако, за последние годы этот вид вредоносного ПО стал всё чаще использоваться для маскировки вредоносных кодов в зараженных компьютерах.

Руткит (от англ. root kit, то есть "набор root'а") — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе. Термин Rootkit исторически пришёл из мира UNIX, и под этим термином понимается набор утилит или специальный модуль ядра, которые взломщик устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Этот набор, как правило, включает в себя разнообразные утилиты для "заметания следов" вторжения в систему, сниферы, сканеры, кейлоггеры, троянские программы, замещающие основные утилиты UNIX (в случае неядерного руткита). Rootkit позволяет взломщику закрепиться во взломанной системе и скрыть следы своей деятельности путём сокрытия файлов, процессов, а также самого присутствия руткита в системе.

Руткиты можно классифицировать в соответствии со следующими характеристиками:

Постоянство существования:

- Постоянный руткит активируется при каждом запуске системы. Для этого ему необходимо хранить свой код внутри компьютера, а также нужен способ для автоматического самозапуска.

- С другой стороны, непостоянный руткит не способен автоматически перезапускаться после перезагрузки системы.

Способ выполнения руткита:

- Режим пользователя: данный вид руткита перехватывает системные запросы и фильтрует информацию, возвращаемую API (Application Programming Interface). Наиболее известный руткит, принадлежащий к данном увиду, это Hacker Defender.

- Режим ядра (ядро операционной системы): такие руткиты модицируют структуру данных ядра, а также перехватывают собственный API ядра. Это наиболее надежный и действенный способ перехвата системы.

Война против руткитов – это настоящая вооруженная борьба, в рамках которой создатели руткитов разрабатывают новые способы для того, чтобы оставаться незамеченными, а антивирусные компании предпринимают ответные меры для того, чтобы защитить своих клиентов.

Для обнаружения руткитов в системе можно использовать следующие технологии:

* Сигнатурное обнаружение: действенная технология, которая успешно применяестя антивирусными компаниями уже на протяжении многих лет. Данная технология основана на сканировании файлов и их сравнении с коллекцией сигнатур известного вредоносного ПО
* Эвристическое или поведенческое обнаружение: идентифицирует руткиты путем распознавания любых отклонений в нормальной деятельности компьютера.
* Обнаружение по сравнению: Результаты, возвращенные операционной системой, сравниваются с результатами, полученными посредством низкоуровневых запросов – наличие каких-либо различий свидетельствует о присутствии в системе руткита.
* Обнаружение на основе целостности: отпределяет наличие руткита путем сравнения файлов и памяти с надежным тестовым статусом.

Каждая из перечисленных технологий имеет свои ограничения, поэтому рекомендуется сочетать различные технологии. Также необходимо учесть, что некоторые их этих руткитов специально разработаны для того, чтобы не быть обнаруженными лидирующими на рынке антивирусными компаниями.

Заключение

Cегодня необходимо уметь работать с ПК и знать программное обеспечение. В современном обществе совокупность знаний и навыков в области вычислительной техники ценится особенно высоко. Для творческой личности компьютер предоставляет неограниченные возможности самосовершенствования. Если пользователь хочет иметь плоды своей работы в целости и сохранности, если не хочет, чтобы деньги с его счёта были сняты недоброжелателями и о подробностях его жизни узнали посторонние люди, он просто обязан установить на своём ПК антивирусные программы, которые борются с компьютерными вредоносными программами.

Список использованной литературы

1)Галатенко В., Информационная безопасность, "Открытые системы", N 4,5,6, 1995.

2)С. Симонович, Г. Евсеев, А. Алексеев "Windows. Лаборатория мастера" Москва, "АСТпресс" 2000

3)А. Алексеев "Информатика 2001" Москва, "Дрофа" 2001

4)Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. – М.: "СОЛОН-Р", 2001.

5)Левин А.Ш. Самоучитель полезных программ. 4-е издание. – СПБ.: Питер, 2005.

6)http://www.viruslist.com – Все угрозы.

7)http://www.bytemag.ru – BYTE/Россия – Что нужно знать о компьютерных вирусах.

8)http://www.ucheba.ru – Информация для студентов.