Средства защиты информации

1. Необходимость защиты информации

Многообразие информации, циркулирующей в обществе, в том числе передаваемой по сетям, приводит к возникновению различных факторов, угрожающих ее безопасности. Информационная безопасность – состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере.

Под угрозой безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов. Реализованную угрозу называют атакой. Можно указать, как минимум, две причины потери информации. Первая – объективная, связанная с выходом из строя аппаратуры (например, поломка жесткого диска с необратимой потерей отдельных секторов), порча отдельных файлов вследствие сбоев электропитания и т.д. Вторая – человеческий фактор - связана с ошибками разработчиков информационных систем (программ) и их пользователей, а также с чьими-то предумышленными действиями.

Существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа в вычислительных системах и сетях. В их числе:

* чтение остаточной информации в памяти компьютера после выполнения санкционированных запросов;
* копирование носителей информации и файлов информации с преодолением мер защиты;
* маскировка под зарегистрированного пользователя;
* маскировка под запрос системы;
* использованием *программных ловушек*[[1]](#footnote-1);
* использование недостатков операционной системы;
* незаконное подключение к аппаратуре и линиям связи;
* злоумышленный вывод из строя механизмов защиты;
* внедрение и использование компьютерных вирусов.

Угрозы безопасности информации возникают и при использовании электронной почты. К ним относятся:

* Адреса электронной почты используются для рассылки *спама*[[2]](#footnote-2) . Адрес попадает в базы данных спамеров незаконным путем.
* Адреса электронной почты в Интернете легко подделать. Практически нельзя сказать наверняка, кто написал и послал электронное письмо.
* Электронные письма могут быть легко модифицированы. Стандартное *SMTP*[[3]](#footnote-3) - письмо не содержит средств проверки целостности.
* Существует ряд мест, где содержимое письма может быть прочитано теми, кому оно не предназначено. Электронное письмо скорее похоже на открытку — его могут прочитать на каждой промежуточной станции.
* Нет гарантий доставки электронного письма. Хотя некоторые почтовые системы предоставляют пользователям возможность получить сообщение о доставке, часто такие уведомления означают лишь то, что почтовый сервер получателя (а не обязательно сам пользователь) получил сообщение.
* Почтовая бомба — это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя.
* Фишинг (англ. phishing, от phony – обман и fishing – рыбная ловля, выуживание) − вид интернет-мошенничества, цель которого получить идентификационные данные пользователей. Организаторы рассылают письма, в которых созданы ссылки на сайты, которые являются копией настоящих.
* «Нигерийские письма» − вид интернет-мошенничества, цель которого поиск жертвы, которая будет переводить деньги за несуществующие товары, услуги, мероприятия.

Обеспечение безопасности информации при работе на автономно работающих компьютерах и в сетях достигается комплексом организационных, технических и программных мер.

Защита информации – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостность, доступность и, если нужно, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

2. Методы защиты информации

Рассмотрим основные методы защиты информации.

Ограничение доступа к информации заключается в создании некоторой *физической*[[4]](#footnote-4) замкнутой преграды вокруг объекта защиты с организацией контрольного доступа лиц, связанных с объектом защиты по своим функциональным обязанностям, т.е. выделение специальных территорий, специальных зданий и помещений, создание контрольно-пропускного режима. **Задача подобных средств ограничения доступа** – исключить случайный и преднамеренный доступ посторонних лиц к комплексам средств автоматизации. Ограничение доступа к информации обеспечивается и с помощью аппаратных средств с самым различными принципами действия. Так, в целях контроля доступа к внутренним линиям связи и технологическим органам управления используется аппаратура контроля вскрытия устройств.

Распределение доступа к информации заключается в разделении информации на части и организации доступа к ним пользователей в соответствии с их функциональными обязанностями и полномочиями. Деление информации может производиться по степени важности или секретности, по функциональному назначению и другим признакам. **Задача этого метода** – существенно затруднить преднамеренный перехват информации нарушителем, предусмотреть механизм разделения привилегий при доступе к особо важным данным.

Для ограничения и распределения доступа к информации используется идентификация объектов – установление их подлинности в вычислительной системе и допуск к информации ограниченного пользования. Для этого каждому объекту или субъекту присваивается уникальный номер (образ, имя или число).

В вычислительной системе объектами идентификации являются:

* человек (оператор, пользователь, должностное лицо);
* технические средства (ЭВМ, носители информации);
* информация (программы, документы, распечатки).

В качестве идентификаторов личности для реализации разграничения широко распространено применение паролей, которые записываются на специальные носители (*электронные ключи*[[5]](#footnote-5) или карточки). Установление подлинности объекта может производиться человеком, аппаратным устройством, программой, вычислительной системой и т.д.

Криптографическое преобразование информации. Этот метод повышает безопасность передачи данных в сетях ЭВМ, данных в удаленных устройствах памяти и при обмене информацией между удаленными объектами. Защита информации методом *криптографического преобразования*[[6]](#footnote-6) заключается в преобразовании ее составных частей (слов, букв, цифр, слогов) с помощью специальных алгоритмов и аппаратных решений. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключей, обеспечивающего каждый раз оригинальное представления информации при использовании одного и того же алгоритма или устройства. Без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования. Для ознакомления с зашифрованной информацией применяется процесс декодирования информации. Появление и развитие электронных элементов позволили разработать недорогие устройства, обеспечивающие преобразование информации.

3. Компьютерные вирусы

При работе с современным персональным компьютером пользователя может подстерегать множество неприятностей: потеря данных, «зависание» системы, выход из строя отдельных частей компьютера и др. Одной из причин этих проблем наряду с ошибками в программном обеспечении и неумелыми действиями оператора ПК могут быть проникшие в систему компьютерные вирусы. Это едва ли не главные враги компьютера, которые подобно биологическим вирусам размножаются, записываясь в системные области диска или присоединяясь к файлам, и производят различные нежелательные действия, которые зачастую имеют катастрофические последствия.

Причины появления распространения компьютерных вирусов, с одной стороны, скрываются в теневых сторонах человеческой личности (зависть, месть, тщеславие), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы ПК.

Компьютерный вирус – это специально написанная программа, как правило, небольшая по размерам, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области дисков и в вычислительные сети (причем эти копии сохраняют способность к размножению) с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.

Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется **заражением**, а объект, содержащий вирус (программа или иной), является **зараженным**.

Основными путями проникновения вирусов в компьютер являются съемные носители информации (диски и флэш-карты), а также компьютерные сети. Заражение жесткого диска вирусом может произойти при загрузке компьютера с диска, содержащего вирус. Такое заражение может быть и случайным, например, если системную дискету не вынули из дисковода и перезагрузили компьютер. Заразить дискету гораздо проще – вирус может попасть на нее, даже если дискету просто вставили в дисковод зараженного компьютера и просмотрели ее содержимое. **Зараженный диск** – это диск, в загрузочном секторе которого находится вирус.

После запуска программы, содержащей вирус, становится возможным заражение других файлов. **Зараженный файл** – это файл, содержащий внедренный в него вирус.

При заражении компьютера вирусом очень важно своевременно его обнаружить, так как действия вирусов могут наносить большой вред владельцам компьютеров. Приведем основные признаки проявления вирусов:

* невозможность загрузки операционной системы;
* прекращение работы или неправильная работа ранее успешно функционировавших программ;
* блокировка ввода с клавиатуры;
* замедление работы компьютера;
* изменение размеров, даты и времени создания файлов;
* значительное увеличение количества файлов на диске;
* исчезновение файлов и каталогов или искажение их содержимого;
* существенное уменьшение размера свободной оперативной памяти;
* блокировка записи на жесткий диск;
* непредусмотренное требование снять защиту с дискеты;
* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* частые «зависания» и сбои в работе компьютера.

Перечисленные признаки необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому иногда затруднена правильная диагностика состояния компьютера.

Сегодня известно огромное количество вирусов. Так, в антивирусных базах «Касперского» содержится более 6,5 млн. записей (на начало 2012 г.). Как и обычным вирусам, для размножения компьютерным вирусам нужен **носитель** – здоровая программа или документ, в котором они прячут участки своего программного кода.

Сам вирус невелик, редко его размер измеряется килобайтами. В тот момент, когда пользователь запускает на своем компьютере программу или открывает документ, вирус активизируется и заставляет компьютер следовать его инструкциям. Это приводит к удалению какой-либо информации, причем чаще всего безвозвратно. Современные вирусы могут испортить не только программы, но и «железо». Например, уничтожают содержимое BIOS материнской платы или повреждают жесткий диск.

Вирусы появились более 40 лет назад. Именно тогда, в конце 1960-х гг., когда о ПК можно было читать лишь в фантастических романах, в нескольких больших ЭВМ, располагавшихся в крупных исследовательских центрах США, обнаружились очень необычные программы. Они не выполняли распоряжения человека, как другие программы, а действовали сами по себе. Причем своими действиями они сильно замедляли работу компьютера, но при этом ничего не портили и не размножались.

В 1970-х гг. были зарегистрированы первые вирусы, способные к размножению и получившие собственные имена. Так, большой компьютер Univac 1108 «заболел» вирусом Pervading Animal, а компьютеры семейства IBM-360/370 были заражены вирусом Christmas Tree.

В 1980-х годах число активных вирусов измерялось уже сотнями. А появление и распространение ПК породило настоящую эпидемию – счет вирусов пошел на тысячи. Правда, термин «компьютерный вирус» появился только в 1984 г. (впервые его использовал в своем докладе на конференции по информационной безопасности сотрудник Лехайского университета США Ф. Коуэн).

Первые компьютерные вирусы были простыми и неприхотливыми, не скрывались от пользователей и скрашивали свое разрушительное действие (удаление файлов, разрушение логической структуры дисков) выводимыми на экран картинками и шутками («Назовите точную высоту горы Килиманджаро в миллиметрах! При введении неправильного ответа все данные на вашем винчестере будут уничтожены!»). Выявить такие вирусы было нетрудно, так как они присоединялись к исполняемым (.exe, .com) файлам, изменяя их оригинальные размеры.

Позднее вирусы стали прятать свой программный код так, что ни один антивирус не мог его обнаружить. Такие вирусы назывались невидимками. В 1990-х годах вирусы стали мутировать, т.е. постоянно изменять свой программный код, при этом пряча его в различных участках жесткого диска. Такие вирусы-мутанты стали называть полиморфными. В 1995 году после появления операционной системы Windows 95 были зарегистрированы вирусы, работающие под управлением Windows. Примерно через полгода были обнаружены вирусы, которые действовали в документах, подготовленных в программах пакета Microsoft Office. Долгое время заражение вирусами файлов документов считалось невозможным, так как документы не содержали исполнимых программ. Однако программисты корпорации Microsoft встроили в текстовый процессор Word и табличный процессор Excel язык программирования VBA, предназначенный для создания специальных дополнений к процессорам (макросов). Эти макросы сохранялись в теле документов Microsoft Office и легко могли быть заменены вирусами. После открытия зараженного файла вирус активизировался и заражал все документы пакета. Первоначально макровирусы наносили вред только текстовым документам, позднее стали уничтожать информацию. Весомый вклад в распространение вирусов внесла сеть Интернет. Впервые внимание общественности к проблеме интернет-вирусов было привлечено после появления знаменитого «червя Морриса»[[7]](#footnote-7), распространившегося по всей мировой сети. А к 1998 году Интернет стал главным поставщиком вирусов. Возник даже целый класс интернет-вирусов, названных *троянскими*. Поначалу эти программы не причиняли вреда компьютеру и хранящейся в нем информации, зато с легкостью могли украсть логин и пароль для доступа к сети, а также другую секретную информацию.

В течение 1998-1999 гг. мир потрясли несколько разрушительных вирусных атак – в результате деятельности вирусов Chernobyl, Melissa и Win95.CIH были выведены из строя около миллиона компьютеров во всех странах мира (вирусы портили жесткий диск и уничтожали BIOS материнской платы).

Для защиты от компьютерных вирусов следует соблюдать основные правила работы на ПК:

* установить на компьютере современное вирусное программное обеспечение и постоянно обновлять его;
* перед считывание информации с переносных источников памяти (дискет лазерных дисков и флэш-карт) всегда проверять их на наличие вирусов;
* при переносе на компьютер файлов в архивированном виде проверять сам архив или файлы в процессе их распаковки на жесткий диск (такая возможность предусмотрена современными антивирусными программами);
* использовать антивирусные программы для контроля всех файлов, получаемых из компьютерных сетей;
* периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования памяти, системных областей дисков и файлов, предварительно загрузив операционную систему с защищенного от записи системного диска (компакт-диска или флэш-карты);
* защищать дискеты (флэш-карты) от записи при работе на других компьютерах, если на них не должна производиться запись информации;
* обязательно делать архивные копии информации на альтернативных носителях (дисках или флэш-картах).

1. Программы-ловушки – это резидентные программные модули, обеспечивающие после их запуска легального или несанкционированного (скрытного внедрения) съем информации с одного или нескольких информационных внутренних или внешних каналов информационной системы, компьютера или доступной части сети, например, путем перехвата соответствующих прерываний. По способу доставки и внедрения программы– ловушки можно разделить на вирусные, сетевые или файловые. [↑](#footnote-ref-1)
2. Спам (англ. spam) — массовая рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать. Также, название распространяемых материалов. Распространителей спама называют спамерами. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Доля спама в мировом почтовом трафике составляет от 60% (2006) до 80% (2011). [↑](#footnote-ref-2)
3. SMTP (англ. Simple Mail Transfer Protocol — простой протокол передачи почты) — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. [↑](#footnote-ref-3)
4. Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников. [↑](#footnote-ref-4)
5. Электронный ключ — электронное устройство, имеющее память, с записанной в ней аутентификационной информацией, с возможностью считывания этой информации неким идентифицирующим / аутентифицирующим устройством. [↑](#footnote-ref-5)
6. Криптографические средства ­– это специальные математические и алгоритмические средства защиты информации, передаваемой по системам сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования. [↑](#footnote-ref-6)
7. Червь Морриса (англ. Morris worm) или интернет-червь 2 ноября 1988 (англ. Internet worm of November 2, 1988) — один из первых сетевых червей, распространяемых через Интернет. Написан аспирантом Корнеллского университета Робертом Таппаном Моррисом, и запущен 2 ноября 1988 года в Массачусетском технологическом институте. Это был первый вирус (парализовал работу шести тысяч интернет-узлов в США), получивший значительное внимание в средствах массовой информации. Он привёл к первой судимости в США по Computer Fraud and Abuse Act 1986 года. [↑](#footnote-ref-7)