**Методы и средства защиты**

Проблема создания системы защиты информации включает две взаимодополняющие задачи: 1) разработка системы защиты информации (ее синтез); 2) оценка разработанной системы защиты информации. Вторая задача решается путем анализа ее технических характеристик с целью установления, удовлетворяет ли система защиты, информации комплексу требований к данным системам. Такая задача в настоящее время решается почти исключительно экспертным путем с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Методы и средства обеспечения безопасности информации показаны на рис. 7.2. Рассмотрим основное содержание представленных методов защиты информации, которые составляют основу механизмов защиты.

*Препятствия —* методы физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).

*^ Управление доступом -* метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств). Управление доступом включает следующие функции защиты:

* идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
* опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
* проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
* разрешение и создание условий работы в пределах установленного регламента;
* регистрацию (протоколирование) обращений к защищаемым ресурсам;
* регистрацию (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

*Маскировка —* метод защиты информации путем ее криптографического закрытия. Этот метод широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.

*Регламентация —* метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

*Принуждение —* метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

*Побуждение —* метод защиты, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких, как технические, программные, организационные, законодательные и морально-этические. К. основным средствам защиты, используемым для создания механизма обеспечения безопасности, относятся следующие.

*^ Технические средства* реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические. Под *аппаратными средствами* принято понимать технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Например, система опознания и разграничения доступа к информации (посредством паролей, записи кодов и другой информации на различные карточки). *Физические средства* реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, источники бесперебойного питания, электромеханическое оборудование охранной сигнализации. Так, различают наружные системы охраны («Ворон», *^ GUARDWIR, FPS* и др.), ультразвуковые системы *(Cyclops* и т. д.), системы прерывания луча *(Pulsar* 30В и т. п.), телевизионные системы *(VМ216* и др.), радиолокационные системы («ВИТИМ» и т. д.), система контроля вскрытия аппаратуры и др.

*^ Программные средства* представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации. В такую группу средств входят: механизм шифрования (криптографии — специальный алгоритм, который запускается уникальным числом или битовой последовательностью, обычно называемым шифрующим ключом; затем по каналам связи передается зашифрованный текст, а получатель имеет свой ключ для дешифрования информации), механизм цифровой подписи, механизмы контроля доступа, механизмы обеспечения целостности данных, механизмы постановки графика, механизмы управления маршрутизацией, механизмы арбитража, антивирусные программы, программы архивации (например, *zip, rar, arj* и др.), защита при вводе и выводе информации и т. д.

*^ Организационные средства* защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, использование, эксплуатация).

*^ Морально-этические средства* защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их обычно ведет к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

*^ Законодательные средства* защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Все рассмотренные средства защиты разделены на *формальные* (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и *неформальные* (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

В настоящее время наиболее острую проблему безопасности (даже в тех системах, где не требуется сохранять секретную информацию, и в домашних компьютерах) составляют вирусы. Поэтому здесь остановимся на них подробнее. *Компьютерный вирус —* это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т. е. «заражать» их), а также выполнять различные нежелательные действия на компьютере (например, портить файлы или таблицы размещения файлов на диске, «засорять» оперативную память и т. д.).

Основным средством защиты от вирусов служит *архивирование.* Другие методы заменить его не могут, хотя и повышают общий уровень защиты. Архивирование необходимо делать ежедневно. Архивирование заключается в создании копий используемых файлов и систематическом обновлении изменяемых файлов. Это дает возможность не только экономить место на специальных архивных дисках, но и объединять группы совместно используемых файлов в один архивный файл, в результате чего гораздо легче разбираться в общем архиве файлов. Наиболее уязвимыми считаются таблицы размещения файлов, главного каталога и бутсектор. Файлы рекомендуется периодически копировать на специальную дискету. Их резервирование важно не только для защиты от вирусов, но и для страховки на случай аварийных ситуаций или чьих-то действий, в том числе собственных ошибок.

В целях профилактики для защиты от вирусов рекомендуется:

* работа с дискетами, защищенными от записи;
* минимизация периодов доступности дискет для записи;
* разделение дискет между конкретными ответственными пользователями;
* разделение передаваемых и поступающих дискет;
* разделение хранения вновь полученных программ и эксплуатировавшихся ранее;
* проверка вновь полученного программного обеспечения на наличие в них вируса тестирующими программами;
* хранение программ на жестком диске в архивированном виде.

Для того чтобы избежать появления компьютерных вирусов, необходимо соблюдать прежде всего следующие меры:

* не переписывать программное обеспечение с других компьютеров, если это необходимо, то следует принять перечисленные выше меры;
* не допускать к работе на компьютере посторонних лиц, особенно если они собираются работать со своими дискетами;
* не пользоваться посторонними дискетами, особенно с компьютерными играми.

Можно выделить следующие типичные ошибки пользователя, приводящие к заражению вирусами:

* отсутствие надлежащей системы архивации информации;
* запуск полученной программы без ее предварительной проверки на зараженность и без установки максимального режима защиты винчестера с помощью систем разграничения доступа и запуска резидентного сторожа;
* выполнение перезагрузки системы при наличии установленной в дисководе *^ А* дискеты (при этом *BIOS* делает попытку загрузиться именно с этой дискеты, а не с винчестера; в результате, если дискета заражена бутовым вирусом, происходит заражение винчестера);
* прогон всевозможных антивирусных программ, без знания типов диагностики одних и тех же вирусов разными антивирусными программами;
* анализ и восстановление программ на зараженной операционной системе.

В настоящее время наиболее популярные в России антивирусные средства АО «ДиалогНаука»:

* полифаг *Aidstest (полифаг-* это программа, выполняющая действия обратные тем, которые производит вирус при заражении файла, т. е. пытающаяся восстановить файл);
* ревизор *Adinf;*
* лечащий блок *AdinfExt;*
* полифаг для «полиморфиков» *Doctor Web.*

Существуют *программы-фильтры,* проверяющие, имеется ли в файлах (на указанном пользователем диске) специальная для данного вируса комбинация байтов. Используется также специальная обработка файлов, дисков, каталогов — вакцинация: запуск *программ-вакцин,* имитирующих сочетание условий, в которых начинает работать и проявляет себя данный тип вируса. В качестве примера резидентной программы для защиты от вирусов можно привести программу *VSAFF* фирмы *Carmel Central Point Software.* B качестве программ ранней диагностики компьютерного вируса могут быть рекомендованы программы *CRCLIST* и *CRCTEST.*