***ТЕМА: ОСУЩЕСТВЛЕНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.***

***Понятие безопасности компьютерной информации. Объекты и элементы защиты данных в компьютерных системах.***

Создание всеобщего информационного пространства, массовое применение персональных компьютеров и внедрение компьютерных систем породили необходимость решения комплексной проблемы ***защиты информации.***

***Под защитой информации принято понимать использование различных средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения надежности передаваемой, хранимой и обрабатываемой информации.***

Защитить информацию -это значит:

• обеспечить физическую целостность информации, т.е. не допустить искажений или уничтожения элементов информации;

• не допустить подмены (модификации) элементов информации при сохранении ее целостности;

• не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;

• быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями.

Процессы по нарушению надежности информации можно классифицировать на ***случайные и злоумышленные***(преднамеренные).В первом случае источниками разрушительных, искажающих и иных процессов являются непреднамеренные, ошибочные действия людей, технические сбои и др.; во втором случае -злоумышленные действия людей. Однако независимо от причин на­рушения надежности информации это чревато самыми различны­ми последствиями.

Учитывая, что для построения надежной системы защиты требуются значительные материаль­ные и финансовые затраты, необходимо перед построением сис­темы защиты разрабатывать некоторую оптимизационную мо­дель, позволяющую достичь максимального результата при за­данном или минимальном расходовании ресурсов. Для расчета затрат, обеспечивающих требуемый уровень защищенности ин­формации, необходимо по крайней мере знать: полный (если это возможно) перечень угроз информации, потенциальную опас­ность для информации каждой из угроз, размеры затрат, необхо­димые для нейтрализации каждой из угроз.

Следует напомнить, что если в первые десятилетия активного использования ПК основную опасность представляли хакеры, или «электронные разбойники», которые подключались к компьюте­рам в основном через телефонную сеть, то в последнее десятиле­тие нарушение надежности информации прогрессирует через про­граммы -компьютерные вирусы и через глобальную сеть Интер­нет.

Практика функционирования СОД показывает, что существу­ет достаточно много способов несанкционированного доступа к информации:

• просмотр;

• копирование и подмена данных;

• ввод ложных программ и сообщений в результате подклю­чения к каналам связи;

• чтение остатков информации на ее носителях;

• прием сигналов электромагнитного излучения и волнового характера;

• использование специальных программных и аппаратных «заглушек» и т.п.

Следовательно, необходимы разработка и внедрение не от­дельных локальных (пусть и очень важных) мероприятий по за­щите информации, а создание многоступенчатой непрерывной и управляемой архитектуры безопасности информации. Защищать необходимо не только информацию, содержащую государствен­ную или военную тайну, но и информацию коммерческого и кон­фиденциального (личного) содержания. Надо заметить, что на объект защиты обычно воздействует некоторая совокупность де­стабилизирующих факторов. При этом характер и уровень воз­действия одних факторов могут совершенно не зависеть от харак­тера и уровня других.

Однако возможна и иная ситуация, когда характер и уровень взаимодействия взаимозависимых факторов существенно зависят от влияния других, явно или скрыто усиливающих такие воздей­ствия. Точно так же и средства защиты могут быть как независи­мыми с точки зрения эффективности защиты, так и взаимозависи­мыми. Надо признать, что, несмотря на разработку сложнейших механизмов и средств защиты, колоссальные финансовые затраты на эти мероприятия, любая компьютерная система защиты пока еще не является полностью надежной от ее взлома.

Для обеспечения достаточно высокой безопасности данных надо найти компромисс между стоимостью защитных мероприятий, неудобствами при использовании мер защиты и важностью защища­емой информации. Только на основе тщательного анализа много­численных взаимодействующих факторов можно принять более или менее разумное и эффективное решение о сбалансированности меры защиты от конкретных источников опасности.

Надежная защита информации в разрабатываемых и функци­онирующих системах обработки данных может быть эффектив­ной, если она будет надежной на всех *объектах*и во всех *элемен­тах* системы, которые могут быть подвергнуты угрозам.

*Под****объектом защиты*** *понимается такой структурный компонент системы, в котором находится или может находиться подлежащая защите информация.*

*Под****элемен­том защиты****- совокупность данных, которая может содержать подлежащие защите сведения*.

Практика показывает, что информация в процессе ввода, хра­нения, обработки, вывода и передачи подвергается *различным слу­чайным воздействиям*, в результате которых на аппаратном уров­не происходят физические изменения в сигнальных формах пред­ставления информации. Если в каком-то или в каких-то разрядах цифрового кода, несущего информацию, произошло инвертиро­вание двоичного знака (с 1на 0или наоборот) и оно не обнаружено специальными аппаратными средствами функционального контроля, то при дальнейшей обработке информации либо будет по­учен неверный результат, либо сообщение направится по ложному адресу, либо произойдут другие нежелательные события (разрушение, модификация, утечка информации и др.).

На программном уровне в результате случайных воздействий может произойти изменение алгоритма обработки информации на непредусмотренный и, как следствие этого, -прекращение или модификация процесса, в результате которого опять же возможны разрушение или утечка информации (при перепутывании, например, адресата).

Причинами случайных воздействий при функционировании компьютерных систем могут быть:

• отказы и сбои аппаратуры в случае ее некачественного исполнения и физического старения;

• помехи в каналах и на линиях связи от воздействия внешней среды;

• аварийные ситуации (пожар, наводнение, выход из строя электропитания и др.);

• схемные и системотехнические ошибки и просчеты разработчиков и производителей ПК;

• алгоритмические и программные ошибки;

• ошибки человека при работе с ПК.

*Злоумышленные или преднамеренные угрозы* -результат активного воздействия человека на объекты и процессы по самым различным причинам (материальный интерес, желание навредить, развлечение с самоутверждением своих способностей и др.).

В качестве *объектов защиты* информации в системах обработки данных можно выделить следующие:

• терминалы пользователей (персональные компьютеры, рабочие станции сети);

• терминал администратора сети или групповой абонентский узел;

• узел связи;

• средства отображения информации,

• средства документирования информации;

• машинный зал (компьютерный или дисплейный) и хранилище носителей информации;

• внешние каналы связи и сетевое оборудование;

• накопители и носители информации.

В соответствии с приведенным выше определением в качестве *элементов защиты* выступают блоки (порции, массивы, потоки и др.) информации в объектах защиты, в частности:

• данные и программы в основной памяти компьютера;

• данные и программы на внешнем машинном носителе (гиб­ком и жестком дисках);

• данные, отображаемые на экране монитора;

• данные, выводимые на принтер при автономном и сетевом использовании ПК;

• пакеты данных, передаваемые по каналам связи;

• данные, размножаемые (тиражируемые) с помощью копировально-множительного оборудования;

• отходы обработки информации в виде бумажных и магнит­ных носителей;

• журналы назначения паролей и приоритетов зарегистриро­ванным пользователям;

• служебные инструкции по работе с комплексами задач;

• архивы данных и программного обеспечения и др.

Доступ к объектам и элементам защиты информации теоре­тически и практически возможен для двух категорий лиц: закон­ных пользователей и нарушителей.

При отсутствии на рабочем месте законного пользователя или при его халатном отношении к своим должностным обязаннос­тям, при недостаточной защите информации квалифицирован­ный нарушитель может осуществить путем ввода соответствую­щих запросов (команд) несанкционированный доступ к инфор­мации. При достаточно свободном доступе в помещение, где размещены средства ВТ, можно визуально наблюдать информа­цию на средствах отображения и документирования, а также по­хитить носители с информацией (дискеты, ленты, листинги и др.) либо снять с них копию. При бесконтрольной загрузке в компь­ютер программы нарушитель может модифицировать данные и алгоритмы, ввести вредоносную программу типа «троянский конь», с помощью которой впоследствии он может реализовывать нужные для себя функции.

Особо опасна ситуация, когда нарушителем является пользо­ватель компьютерной системы, имеющий согласно своим функ­циональным обязанностям законный доступ к одной части информации, но обращающийся к другой за пределами своих пол­номочий.

Несанкционированный доступ к информации может происхо­дить во время технического обслуживания (профилактики или ремонта) компьютеров за счет прочтения информации на машин­ных и других носителях, несмотря на ее удаление (стирание) пользователем обычными методами. Другой способ -прочтение информации с носителя во время его транспортировки без охра­ны внутри объекта или региона.

Несанкционированное ознакомление с информацией возмож­но путем непосредственного подключения нарушителем «шпи­онских» средств к каналам связи и сетевым аппаратным сред­ствам.

Несанкционированное ознакомление с информацией подраз­деляется на ***пассивное и активное***. В первом случае не происходит нарушения информационных ресурсов, и нарушитель лишь по­лучает возможность раскрывать содержание сообщений, исполь­зуя это в дальнейшем в своих корыстных целях. Во втором слу­чае нарушитель может выборочно изменить, уничтожить, пере­упорядочить и перенаправить сообщения, задержать и создать поддельные сообщения и др.

Для обеспечения безопасности информации в личных компь­ютерах и особенно в офисных системах и компьютерных сетях проводятся различные мероприятия, объединяемые понятием ***«си­стема защиты информации».***

***Система защиты информации -это совокупность организа­ционных (административных) и технологических мер, программ­но-технических средств, правовых и морально-этических норм, направленных на противодействие угрозам нарушителей с целью сведения до минимума возможного ущерба пользователям и вла­дельцам системы.***

Исследования практики функционирования систем обработ­ки данных и компьютерных сетей показали, что существует дос­таточно много возможных направлений утечки информации и путей несанкционированного доступа к ней в системах и сетях:

• перехват электронных излучений;

• принудительно электромагнитное облучение (подсветка) ли­ний связи;

• применение «подслушивающих» устройств;

• дистанционное фотографирование;

• перехват акустических волновых излучений;

• хищение носителей информации и производственных отхо­дов систем обработки данных;

• считывание информации из массивов других пользователей;

• чтение остаточной информации в аппаратных средствах;

• копирование носителей информации и файлов с преодоле­нием мер защиты;

• модификация программного обеспечения путем исключения или добавления новых функций;

• использование недостатков операционных систем и приклад­ных программных средств;

• незаконное подключение к аппаратуре и линиям связи, в том числе в качестве активного ретранслятора;

• злоумышленный вывод из строя механизмов защиты;

• маскировка под зарегистрированного пользователя и при­своение себе его полномочий;

• введение новых пользователей;

• внедрение компьютерных вирусов.

Кроме того, система защиты не должна допускать, чтобы:

• злоумышленник мог снять с себя ответственность за форми­рование ложной или разрушающей информации;

• были отказы от фактов получения информации, которая фак­тически была получена, но в другое время;

• подтверждались сообщения о посылке кому-то информации, которая на самом деле не посылалась;

• в передаваемой информации содержалась другая (вредонос­ная) информация;

• в число пользователей попадали без регистрации новые лица, чтобы не удалялись и не модифицировались действующие лица;

• отдельные пользователи незаконно расширяли свои полно­мочия по доступу к информации и процессам ее обработки;

• создавались помехи обмену сообщениями между пользова­телями с целью нарушения и искажения передаваемой инфор­мации.

Учитывая важность, масштабность и сложность решения про­блемы сохранности и безопасности информации, рекомендуется разрабатывать архитектуру безопасности в несколько этапов:

• анализ возможных угроз;

• разработка системы защиты;

• реализация системы защиты;

• сопровождение системы защиты.

Этап разработки системы защиты информации предусматри­вает использование различных ***комплексов мер и мероприятий организационно-административного, технического, программно-аппаратного, технологического, правового, морально-этическо­го характера и др.***

***Организационно-административные средства защиты*** сводят­ся к регламентации доступа к информационным и вычислитель­ным ресурсам, функциональным процессам систем обработки дан­ных, к регламентации деятельности персонала и др. Их цель -в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Наиболее типичные организацион­но-административные средства:

• создание контрольно-пропускного режима на территории, где располагаются средства обработки информации;

• изготовление и выдача специальных пропусков;

• мероприятия по подбору персонала, связанного с обработ­кой данных;

• допуск к обработке и передаче конфиденциальной инфор­мации только проверенных должностных лиц;

• хранение магнитных и иных носителей информации, пред­ставляющих определенную тайну, а также регистрационных жур­налов в сейфах, не доступных для посторонних лиц;

• организация защиты от установки прослушивающей аппа­ратуры в помещениях, связанных с обработкой информации;

• организация учета использования и уничтожения докумен­тов (носителей) с конфиденциальной информацией;

• разработка должностных инструкций и правил по работе с компьютерными средствами и информационными массивами;

• разграничение доступа к информационным и вычислитель­ным ресурсам должностных лиц в соответствии с их функциональ­ными обязанностями.

***Технические средства защиты*** призваны создать некоторую физически замкнутую среду вокруг объекта и элементов защиты. В этом случае используются такие мероприятия:

• установка средств физической преграды защитного конту­ра помещений, где ведется обработка информации (кодовые зам­ки; охранная сигнализация -звуковая, световая, визуальная без записи и с записью на видеопленку);

• ограничение электромагнитного излучения путем экраниро­вания помещений, где происходит обработка информации, лис­тами из металла или специальной пластмассы;

• осуществление электропитания оборудования, отрабаты­вающего ценную информацию, от автономного источника пи­тания или от общей электросети через специальные сетевые фильтры;

• применение, во избежание несанкционированного дистанци­онного съема информации, жидкокристаллических или плазмен­ных дисплеев, струйных или лазерных принтеров соответственно с низким электромагнитным и акустическим излучением;

• использование автономных средств защиты аппаратуры в виде кожухов, крышек, дверец, шторок с установкой средств кон­троля вскрытия аппаратуры.

***Программные средства и методы*** защиты активнее и шире других применяются для защиты информации в персональных компьютерах и компьютерных сетях, реализуя такие функции защиты:

* как разграничение и контроль доступа к ресурсам;
* регист­рация и анализ протекающих процессов, событий, пользовате­лей;
* предотвращение возможных разрушительных воздействий на ресурсы;
* криптографическая защита информации;
* идентифи­кация и аутентификация пользователей и процессов и др.

В настоящее время наибольший удельный вес в этой группе мер в системах обработки экономической информации составля­ют *специальные пакеты программ* или *отдельные программы*, включаемые в состав программного обеспечения с целью реали­зации задач по защите информации.

***Технологические средства защиты информации*** -это комплекс мероприятий, органично встраиваемых в технологические про­цессы преобразования данных. Среди них:

• создание архивных копий носителей;

• ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти компьютера;

• регистрация пользователей компьютерных средств в журна­лах;

• автоматическая регистрация доступа пользователей к тем или иным ресурсам;

• разработка специальных инструкций по выполнению всех технологических процедур и др.

***К правовым и морально-этическим мерам и средствам защиты*** относятся действующие в стране законы, нормативные акты, рег­ламентирующие правила обращения с информацией и ответствен­ность за их нарушение; нормы поведения, соблюдение которых способствует защите информации.

Примером действующих законодательных актов в Российс­кой Федерации, которыми регламентированы цивилизованные юридические и моральные отношения в сфере информационно­го рынка, являются законы РФ «Об информации, информатиза­ции и защите информации» от 20.02.1995г. №24-ФЗ; «О право­вой охране программ для ЭВМ и баз данных» № 5351 -4от 9.07.1993г. в редакции Федерального закона от 19.07.95 № 110-ФЗ и др.; при­мером предписаний морально-этического характера -«Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США».

В компьютерных системах сосредоточивается информация, право на пользование которой принадлежит определенным ли­цам или группам лиц, действующим в порядке личной инициати­вы или в соответствии с должностными обязанностями. Чтобы обеспечить безопасность информационных ресурсов, устранить возможность несанкционированного доступа, усилить контроль санкционированного доступа к конфиденциальной либо к подле­жащей засекречиванию информации, *внедряются различные сис­темы опознавания, установления подлинности объекта(субъек­та) и разграничения доступа*. В основу построения таких систем закладывается принцип допуска и выполнения только таких об­ращений к информации, в которых присутствуют соответствую­щие признаки разрешенных полномочий.

Ключевыми понятиями в этой системе являются ***"идентифи­кация"***и***"аутентификация".*Идентификация*- это присвоение ка­кому-либо объекту или субъекту уникального имени или образа.*Аутентификация*- это установление подлинности, т.е. провер­ка, является ли объект (субъект) действительно тем, за кого он себя выдает.***

Конечная цель процедур идентификации и аутентификации объекта (субъекта) -допуск его к информации ограниченного пользования в случае положительной проверки либо отказ в до­пуске в случае отрицательного исхода проверки.

Объектами идентификации и аутентификации могут быть:

люди (пользователи, операторы и др.);

технические средства (мо­ниторы, рабочие станции, абонентские пункты);

документы (руч­ные, распечатки и др.);

магнитные носители информации;

инфор­мация на экране монитора, табло и др.

Установление подлинности объекта может производиться ап­паратным устройством, программой, человеком и т.д. При этом для защиты информации в компьютерных системах должна обес­печиваться конфиденциальность образов и имен образов.

При обмене информацией между человеком и компьютером (либо только между компьютерами в сети) должна быть предус­мотрена взаимопроверка подлинности взаимодействующих объектов. Необходимо, чтобы каждый из объектов (субъектов) хранил в своей памяти, не доступной для посторонних, список имен (образов) объектов (субъектов), с которыми производится обмен информацией.

Один из наиболее распространенных методов аутентифика­ции -присвоение лицу или другому имени пароля и хранение его значения в вычислительной системе.***Пароль - это совокупность символов, определяющая объект (субъект).***При выборе пароля возникают вопросы о его размере, стойкости к несанкциониро­ванному подбору, способам его применения. Естественно, чем больше длина пароля, тем большую безопасность будет обеспе­чивать система, ибо потребуются большие усилия для его отгадывания. При этом выбор длины пароля в значительной степени определяется развитием технических средств, их элементной ба­зой и быстродействием. К примеру, если пользователь в качестве своего пароля использует четырехразрядное десятичное число, то компьютерная программа, выполнив перебор чисел от 0000 до 9999 (9999комбинаций) по так называемому «лобовому мето­ду», сумеет распознать код.

Четырехзначный пароль, в котором используются цифровые символы и 26букв латинского алфавита (то есть всего 36воз­можных знаков), требует более трудоемкого процесса распозна­вания, ибо он допускает Зб4, или 1679616,уникальных комбина­ций; при пятизначной длине пароля число комбинаций возраста­ет до 365 = 60 466 176.Увеличивая длину пароля и число используемых символов, можно увеличить число возможных ком­бинаций, повышая время на лобовой взлом пароля.

Сейчас широко применяются много символьные пароли с раз­рядностью более 10знаков.

Наиболее высокий уровень безопасности достигается в слу­чае деления пароля на две части: одну 3-6-значную, легко запо­минаемую человеком, и вторую, содержащую количество знаков, определяемое требованиями к защите и возможностями техни­ческой реализации системы. Эта часть помещается на специаль­ный физический носитель - карточку, устанавливаемую пользо­вателем в специальное считывающее устройство.

В случае применения пароля как средства аутентификации необходимо заменять его на новый не реже одного раза в год. чтобы снизить вероятность его перехвата путем прямого хище­ния носителя, снятия его копии и даже физического принужде­ния человека. Пароль вводится пользователем в начале взаимо­действия с компьютерной системой, иногда и в конце сеанса (в особо ответственных случаях пароль нормального выхода может отличаться от входного). Для правомочности пользователя мо­жет предусматриваться ввод пароля через определенные проме­жутки времени.

Пароль как средство обеспечения безопасности может исполь­зоваться для идентификации и установления подлинности тер­минала, с которого входит в систему пользователь, а также для обратного установления подлинности компьютера по отношению к пользователю.

Учитывая важность пароля как средства повышения безопас­ности информации от несанкционированного использования, сле­дует соблюдать некоторые меры предосторожности, в том числе:

• не хранить пароли в вычислительной системе в незашифро­ванном виде;

• не печатать и не отображать пароли в явном виде на терми­нале пользователя;

• не использовать в качестве пароля свое имя или имена род­ственников, а также личную информацию (дата рождения, номер домашнего или служебного телефона, название улицы и др.);

• не использовать реальные слова из энциклопедии или тол­кового словаря;

• выбирать длинные пароли;

• использовать смесь символов верхнего и нижнего регистров клавиатуры;

• использовать комбинации из двух простых слов, соединен­ных специальными символами (например, +, =и др.);

• придумывать новые слова (абсурдные или даже бредового содержания);

• чаще менять пароль.

Для идентификации пользователей могут применяться слож­ные в плане технической реализации системы, обеспечивающие установление подлинности пользователя на основе анализа его индивидуальных параметров: отпечатков пальцев, рисунка линий руки, радужной оболочки глаз, тембра голоса и др. Но пока эти приемы носят скорее рекламный, чем практический характер.

Более широкое распространение нашли *физические методы идентификации* с использованием носителей кодов паролей. Та­кими носителями являются пропуска в контрольно-пропускных системах; пластиковые карты с именем владельца, его кодом, под­писью; пластиковые карточки с магнитной полосой, содержащей около 100байт информации, которая считывается специальным считывающим устройством (используются как кредитные карточ­ки, карточки для банкоматов и др.); пластиковые карты, содер­жащие встроенную микросхему (smart-card); карты оптической памяти и др.

Одно из интенсивно разрабатываемых направлений по обес­печению безопасности информации -идентификация и установ­ление подлинности документов *на основе электронной цифровой подписи* -ныне простирается от проведения финансовых и бан­ковских операций до контроля за выполнением различных дого­воров. Естественно, при передаче документов по каналам связи применяется факсимильная аппаратура, но в этом случае к полу­чателю приходит не подлинник, а лишь копия документа с копи­ей подписи, которая в процессе передачи может быть подвергну­та повторному копированию для использования ложного доку­мента.

**Электронная цифровая подпись *представляет собой способ шифрования с помощью криптографического преобразования и является паролем, зависящим от отправителя, получателя и со­держания передаваемого сообщения.***Для предупреждения повтор­ного использования подпись должна меняться от сообщения к сообщению.

 ***Компьютерные вирусы. Средства и приемы обеспечения защиты информации от вирусов.***

Массовое использование ПК в сетевом режиме, включая вы­ход в глобальную сеть Интернет, породило проблему заражения их компьютерными вирусами.

**Компьютерным вирусом*принято называть специально на­писанную, обычно небольшую по размерам программу, способ­ную самопроизвольно присоединяться к другим программам (т.е. заражать их), создавать свои копии (не обязательно пол­ностью совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера и в другие объединенные с ним компьютеры с целью нарушения нормальной работы программ, порчи файлов и каталогов, создания различных помех при ра­боте на компьютере.***

Способ функционирования большинства вирусов -это такое изменение системных файлов компьютера, чтобы вирус начинал свою деятельность при каждой загрузке. Всякий раз, когда пользователь копирует файлы на гибкий диск или посылает ин­фицированные файлы по модему, переданная копия вируса пы­тается установить себя на новый диск.

Обычно вирус разрабатывается так, чтобы он появился, ког­да происходит некоторое событие вызова, например, пятница 13-е, другая дата, определенное число перезагрузок зараженного или какого-то конкретного приложения, процент заполнения же­сткого диска и др.

После того как вирус выполнит нужные ему действия, он пе­редает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной. Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто и не замечает, что компьютер работает со «странностями». К призна­кам появления вируса можно отнести:

• замедление работы компьютера;

• невозможность загрузки операционной системы;

• частые «зависания» и сбои в работе компьютера;

• прекращение работы или неправильную работу ранее успеш­но функционировавших программ;

• увеличение количества файлов на диске;

• изменение размеров файлов;

• периодическое появление на экране монитора неуместных сообщений;

• уменьшение объема свободной оперативной памяти;

• заметное возрастание времени доступа к жесткому диску;

• изменение даты и времени создания файлов;

• разрушение файловой структуры (исчезновение файлов, ис­кажение каталогов и др.);

• загорание сигнальной лампочки дисковода, когда к нему нет обращения, и др.

Надо заметить, что названные симптомы необязательно вы­зываются компьютерными вирусами, они могут быть следстви­ем других причин, поэтому компьютер следует периодически диагностировать.

Во многих странах действуют законодательные меры по борь­бе с компьютерными преступлениями и злоумышленными действи­ями, разрабатываются антивирусные программные средства, од­нако количество новых программных вирусов возрастает. Лиц, которые используют свои знания и опыт для несанкционирован­ного доступа к информационным и вычислительным ресурсам, к получению конфиденциальной и секретной информации, к совер­шению вредоносных действий, называют хакерами. Деятельность хакеров зачастую бывает социально опасной.

В мае 2000г. вирус под названием "Iloveyou» (Я тебя люблю), распространенный по электронной почте, поразил сотни тысяч персональных компьютеров в США и странах Европы. Это, по оценкам специалистов, принесло в первые же дни эпидемии до1млрд долл. убытков фирмам и неприятности простым пользо­вателям. Зараженными оказались даже компьютерные системы британского парламента и американского конгресса.

По более детализированной схеме классификации компьютер­ных злоумышлеников делят на хакеров (hacker), кракеров (cracker) и фрикеров (phracer).

Действия хакеров, или компьютерных хулиганов, могут нано­сить существенный вред владельцам компьютеров и владельцам (создателям) информационных ресурсов, так как приводят к про­стоям компьютеров, необходимости восстановления испорченных данных либо к дискредитации юридических или физических лиц, например, путем искажения информации на электронных досках объявлений или на WEB-серверахв Интернете. Мотивы действий компьютерных злоумышленников самые различные: стремление к финансовым приобретениям; желание навредить и отомстить руководству организации, из которой по тем или иным причинам уволился сотрудник; психологические черты человека (зависть, тщеславие, желание проявить свое техническое превосходство над другими, просто хулиганство и пр.).

Основными путями заражения компьютеров вирусами явля­ются съемные диски (дискеты и CD-ROM) и компьютерные сети. Заражение жесткого диска компьютера может произойти при заг­рузке компьютера с дискеты, содержащей вирус. Для усиления безопасности необходимо обращать внимание на то, как и отку­да получена программа (из сомнительного источника, имеется ли наличие сертификата, эксплуатировалась ли раньше и т.д.). Од­нако главная причина заражения компьютеров вирусами -отсут­ствие в операционных системах эффективных средств защиты информации от несанкционированного доступа.

По данным специальной литературы, к концу 1998г. в миро­вой практике было зарегистрировано более 20тыс. компьютер­ных вирусов, и каждую неделю появляется около десяти новых вирусов. На рис.1 изображены излюбленные места обитания вирусов.

В зависимости от среды обитания вирусы классифицируются на загрузочные, файловые, системные, сетевые, файлово-загрузочные.

***Загрузочные вирусы*** внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска.

***Файловые вирусы*** внедряются в основном в исполняемые фай­лы с расширением .СОМ и .ЕХЕ.

***Системные вирусы*** проникают в системные модули и драйве­ры периферийных устройств, таблицы размещения файлов и таб­лицы разделов.

***Сетевые вирусы*** обитают в компьютерных сетях; файлово-загрузочные (многофункциональные) поражают загрузочные секто­ры дисков и файлы прикладных программ.

**Рис. 1. Среда обитания вирусов.**

По способу заражения среды обитания вирусы подразделяют­ся на резидентные и на нерезидентные.

Резидентные вирусы при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая затем пе­рехватывает обращение операционной системы к другим объек­там заражения, внедряется в них и выполняет свои разрушитель­ные действия вплоть до выключения или перезагрузки компьюте­ра. Нерезидентные вирусы не заражают оперативную память ПК и являются активными ограниченное время.

Алгоритмическая особенность построения вирусов оказывает влияние на их проявление и функционирование. Так, репликаторные программы благодаря своему быстрому воспроизводству приводят к переполнению основной памяти, при этом уничто­жение программ-репликаторов усложняется, если воспроизводи­мые программы не являются точными копиями оригинала. В ком­пьютерных сетях распространены программы-черви. Они вычис­ляют адреса сетевых компьютеров и рассылают по этим адресам свои копии, поддерживая между собой связь. В случае прекра­щения существования «червя» на каком-либо ПК оставшиеся отыскивают свободный компьютер и внедряют в него такую же программу.

«Троянский конь» -это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о чем пользователь и не догадывается (например, собирает информацию об именах и паролях, записывая их в специальный файл, до­ступный лишь создателю данного вируса), либо разрушает фай­ловую систему.

Логическая бомба -это программа, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логичес­кий механизм. Например, такая вирусная программа начинает работать после некоторого числа прикладной программы, комп­лекса, при наличии или отсутствии определенного файла или за­писи файла и т.д.

Программы-мутанты, самовоспроизводясь, воссоздают ко­пии, которые явно отличаются от оригинала.

Вирусы-невидимки, или стелс-вирусы, перехватывают обраще­ния операционной системы к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Такие вирусы при обращении к файлам используют достаточно ориги­нальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

Макровирусы используют возможности макроязыков, встро­енных в офисные программы обработки данных (текстовые ре­дакторы, электронные таблицы и т.д.).

По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяются безвред­ные, неопасные, опасные и разрушительные вирусы.

Безвредные вирусы не оказывают разрушительного влияния на работу ПК, но могут переполнять оперативную память в резуль­тате своего размножения.

Неопасные вирусы не разрушают файлы, но уменьшают сво­бодную дисковую память, выводят на экран графические эффек­ты, создают звуковые эффекты и т.д. Опасные вирусы нередко при­водят к различным серьезным нарушениям в работе компьютера;

разрушительные -к стиранию информации, полному или частич­ному нарушению работы прикладных программ. Необходимо иметь в виду, что любой файл, способный к загрузке и выполне­нию кода программы, является потенциальным местом, куда мо­жет внедриться вирус.

Массовое распространение компьютерных вирусов вызвало разработку антивирусных программ, позволяющих обнаруживать и уничтожать вирусы, «лечить» зараженные ресурсы.

В основе работы большинства антивирусных программ лежит принцип поиска сигнатуры вирусов. *Вирусная сигнатура* -это некоторая уникальная характеристика вирусной программы, ко­торая выдает присутствие вируса в компьютерной системе. Обыч­но в антивирусные программы входит периодически обновляе­мая база данных сигнатур вирусов. Антивирусная программа про­сматривает компьютерную систему, проводя сравнение и отыскивая соответствие с сигнатурами в базе данных.

По методу работы антивирусные программы подразделяются на фильтры, ревизоры доктора, детекторы, вакцины и другие.

*Программы-фильтры*, или «сторожа», постоянно находятся в оперативной памяти, являясь резидентными, и перехватывают все запросы к операционной системе на выполнение подозрительных действий. Такими действиями могут быть попытки изменения файлов, за­писи в загрузочные секторы диска и др.

При каждом запросе на такое действие на экран компьютера выдается сообщение. Пользователь дол­жен либо разрешить выполнение действия, либо запретить его. Раздражающая пользователя, «назойливость», и уменьшение свободного объема оперативной памяти из-за постоянного нахождения в ней «сторожа», являются главными недостатками этих программ. К тому же про­граммы-фильтры не «лечат» файлы или диски, для этого необхо­димо использовать другие антивирусные программы. Примерами программ-сторожей являются AVP,AntiVirusforWindowsи др..

Более надежным средством защиты от вирусов *считаются програм­мы-ревизоры.*Они запоминают исходное состояние программ, ка­талогов и системных областей диска (до заражения компьютера), а затем периодически сравнивают текущее со­стояние с исходным. При выявлении несоответствий (по длине файла, дате модификации, коду циклического контроля файла и др.) сообщение об этом выдается пользователю. Примером про­грамм-ревизоров являются программа Adinfфирмы «Диалог-На­ука» и дополнение к ней в видеAdinfCureModule.

*Программы-доктора*не только обнаруживают, но и «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса. Программы этого типа делятся на фаги и полифаги. Последние служат для обнаружения и уничтожения большого количества разнообразных вирусов. Наибольшее рас­пространение в России имеют такие полифаги, как MSAntiVirus,AidtestиDoctorWeb, которые непрерывно обновляются для борь­бы с появляющимися новыми вирусами.

*Программы-детекторы* позволяют обнаруживать файлы, за­раженные одним или несколькими известными разработчикам программ вирусами.

*Программы-вакцины*, или иммунизаторы, относятся к резиден­тным программам. Они модифицируют программы и диски та­ким образом, что это не отражается на работе программ, но ви­рус, от которого производится вакцинация, считает их уже зара­женными и не внедряется в них.

К настоящему времени зарубежными и отечественными фир­мами и специалистами разработано большое количество антиви­русных программ. Многие из них, получившие широкое призна­ние, постоянно пополняются новыми средствами для борьбы с вирусами и сопровождаются разработчиками.

**9.3. Криптографический метод защиты информации**

Криптографическое преобразование -один из наиболее эф­фективных методов, резко повышающих безопасность:

• передачи данных в компьютерных сетях;

• данных, хранящихся в удаленных устройствах памяти;

• информации при обмене между удаленными объектами.

**Криптография – *это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений.***

Криптография известна с древнейших времен, однако она все­гда оставалась привилегией правительственных и военных учреж­дений. Изменение ситуации связывается с публикацией в 1949г. книги К. Шеннона по теории информации и кибернетике, когда к криптографическим методам преобразования информации обра­тились многие ученые, банковские и коммерческие системы.

Защита информации методом криптографического преобра­зования заключается в приведении ее к неявному виду путем пре­образования составных частей информации (букв, цифр, слогов, слов) с помощью специальных алгоритмов либо аппаратных средств и кодов ключей.

**Ключ**-***это изменяемая часть криптогра­фической системы, хранящаяся в тайне и определяющая, какое шифрующее преобразование из возможных выполняется в дан­ном случае.***

Сущность криптографических методов заключается в следующем. Готовое к передаче сообщение, будь то данные, речь или графическое изображение того или иного документа, обычно называется открытым, или незащищенным, текстом или сообщением. В процессе передачи такого сообщения по незащищенным каналам связи оно может быть легко перехвачено или отслежено подслушивающим лицом посредством его умышленных или неумышленных действий.

Для преобразования (шифрования) используется некоторый алгоритм или устройство, реализующее заданный алгоритм, кото­рые могут быть известны широкому кругу лиц. Само же управле­ние процессом шифрования осуществляется с помощью периоди­чески меняющегося кода ключа, обеспечивающего каждый раз ори­гинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа позволяет от­носительно быстро, просто и надежно расшифровать текст. Одна­ко без знания ключа эта процедура может оказаться практически невыполнимой даже при использовании компьютера.

К методам криптографического преобразования применимы следующие требования:

• метод должен быть достаточно устойчивым к попыткам рас­крытия исходного текста на основе зашифрованного;

• обмен ключа не должен быть труден для запоминания;

• затраты на защитные преобразования должны быть прием­лемы при заданном уровне сохранности информации;

• ошибки в шифровании не должны приводить к явной потере информации;

• длина зашифрованного текста не должна превышать длину исходного текста.

Существует несколько методов защитных преобразований, ко­торые можно подразделить на четыре основные группы: переста­новки, замены (подстановки), аддитивные и комбинированные ме­тоды.

Для методов перестановки и замены (подстановки) характерна короткая длина ключа, а надежность защиты определяется слож­ностью алгоритмов преобразования, и, наоборот, для аддитивных методов характерны простые алгоритмы и длинные ключи.

Названные четыре метода криптографического преобразова­ния относятся к методам симметричного шифрования, т.е. один и тот же ключ используется и для шифрования, и для дешифрова­ния. Однако в последние годы учеными разработан метод несим­метричного шифрования, при котором для шифрования приме­няется один ключ, называемый открытым, а для дешифрования другой -закрытый.

Основными методами криптографического преобразования считаются методы перестановки и замены. Суть первого метода заключается в разбиении исходного текста на блоки, а затем в записи этих блоков и чтении шифрованного текста по разным путям геометрической фигуры, например, запись исходного тек­ста -по строкам матрицы, а чтение -по ее столбцам.

Шифрование методом замены заключается в том, что симво­лы исходного текста (блока), записанные в одном алфавите, заме­няются символами другого алфавита в соответствии с принятым ключом преобразования.

Комбинация этих методов породила так называемый произ­водный шифр, обладающий сильными криптографическими воз­можностями. Этот комбинированный метод принят в США в качестве стандарта для шифрования данных, а также в отечествен­ном ГОСТе 28147-89.Алгоритм метода реализуется как аппаратно, так и программно, но базовый алгоритм рассчитан на реали­зацию с помощью электронных устройств специального назна­чения, что обеспечивает высокую производительность и упрощенную организацию обработки информации. Налаженное в ряде стран Запада промышленное производство аппаратуры для криптографического шифрования позволяет резко повысить бе­зопасность коммерческой информации при ее хранении и элект­ронном обмене в компьютерных системах.