ЗАЩИТА ИНФОРМАЦИИ ОТ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ УГРОЗ

Развитие компьютерной техники и ее широкое внедрение в различные сферы человеческой деятельности вызвало рост числа противозаконных действий, объектом или орудием совершения которых являются электронно-вычислительные машины. Путем различного рода манипуляций, т.е. внесения изменений в информацию на различных этапах ее обработки, в программное обеспечение, овладения информацией нередко удается получать значительные суммы денег, уклоняться от налогообложения, заниматься промышленным шпионажем, уничтожать программы конкурентов и т.д.

Защита информации вызывает необходимость системного подхода; т.е. здесь нельзя ограничиваться отдельными мероприятиями. Системный подход к защите информации требует, чтобы средства и действия, используемые для обеспечения информационной безопасности -организационные, физические и * программно-технические -рассматривались как единый комплекс взаимосвязанных, взаимодополняющих и взаимодействующих мер. Один из основных принципов системного подхода к безопасности информации – принцип «разумной достаточности», суть которого: стопроцентной защиты не существует ни при каких обстоятельствах, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы.

Защита информации от потери и разрушения

Рассмотрим моменты, связанные с защитой информации на персональном компьютере, не интегрированном в сеть.

Потеря информации может произойти, например, п о следующим причинам:

1) нарушение работы компьютера;
2) отключение или сбои питания;
3) повреждение носителей информации;
4) ошибочные действия пользователя;
5) действие компьютерных вирусов;
6) несанкционированные умышленные действия других лиц.

Защита от компьютерных вирусов и несанкционированного доступа будут рассматриваться в отдельных разделах. Предотвратить причины 1–4 можно резервированием данных, что является наиболее общим и простым выходом. Средства резервирования таковы:

• программные средства, входящие в состав большинства комплектов утилит, для создания резервных копий - MS Backup, Norton Backup;
• создание архивов на внешних носителях информации.

Резервирование рекомендуется делать регулярно - раз в день, месяц, после окончания работы с использованием соответствующих программных средств и устройств. Так, для резервирования больших массивов информации по стоимости на единицу хранения наиболее выгодны магнитные ленты. Они также отличаются повышенной надежностью.

В случае потери информация может быть восстановлена'.

1) с использованием резервных данных;
2) без использования резервных данных.

Во втором случае применяются следующие особенности удаления файлов и каталогов:

• стирается первая буква имени файла;
• из FAT стирается информация о занятых секторах (сложности, если файл фрагментирован).

Для успешного восстановления данных необходимо чтобы:

• после удаления файла на освободившееся место не была записана новая информация
• файл не был фрагментирован (для этого необходимо регулярно выполнять операцию дефрагмен-тации с помощью, например, утилиты Speedisk из пакета Norton Utilites).

Восстановление производится следующими программными средствами:
• Undelete из пакета утилит t)OS;
• Unerase из комплекта утилит Norton Utilites.

Если данные представляют особую ценность для пользователя, то можно применять защиту от уничтожения:
1) присвоить файлам атрибут Read Only;
2) использовать специальные программные средства для сохранения файлов после удаления его пользователем, имитирующие удаление, например утилиту SmartCan из пакета Norton Utilites. В этом случае при удалении файлы переписываются в скрытый каталог, где и хранятся определенное число дней, которое пользователь может установить сам. Размер каталога ограничен, и при заполнении его наиболее старые файлы стираются и замещаются вновь удаленными.

Необходимо отметить, что большую угрозу для сохранности данных представляют нарушения в системе подачи питания - отключение напряжения, всплески и падения напряжения, импульсные помехи и т.д.. Практически полностью избежать потерь информации в таких случаях можно применяя источники бесперебойного питания, на рынке которых лидирует американская фирма APC. Источники бесперебойного питания выпускаются в трех основных модификациях: offline, line-interactive и online. Устройства offline - это недорогие устройства для массового пользователя, устраняющие основные виды сетевых помех и обеспечивающие переход на питание от аккумуляторных батарей при отключении питания. Модификация line-interactive подразумевает устройства, анализирующие параметры входного питания и принимающие решения о переходе на батарейное питание в случае превышения заданных допустимых значений. В устройствах online применяется двойное или тройное преобразование: переменного входного напряжения в постоянное (одно или два) с последующим преобразованием в переменное. Как результат, на выходе получается идеально отфильтрованное питание, полностью безопасное для нагрузки, а при отключении электроэнергии не происходит даже кратковременного перерыва в подаче питания на выход. Устройства очень дороги, поэтому применяются для питания серверов и другого критичного оборудования. 322

Защита информации от несанкционированного доступа

Несанкционированный доступ – чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Проблема несанкционированного доступа к информации обострилась и приобрела особую значимость в связи с развитием компьютерных сетей, прежде всего глобальной сети Internet. Однако несанкционированный доступ в компьютерные сети имеет свои характерные особенности, поэтому его имеет смысл рассматривать отдельно.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.

Для успешной защиты своей информации пользователь должен иметь абсолютно ясное представление о возможных путях несанкционированного доступа. Перечислим основные типовые пути несанкционированного получения информации:
• хищение носителей информации и производственных отходов;
• копирование носителей информации с преодолением мер защиты;
• маскировка под зарегистрированного пользователя;
• мистификация (маскировка под запросы системы);
• использование недостатков операционных систем и языков программирования;
• использование программных закладок и программных блоков типа «троянский конь»;
• перехват электронных излучений;
• перехват акустических излучений;
• дистанционное фотографирование;
• применение подслушивающих устройств;

• злоумышленный вывод из строя механизмов защиты и т.д.

Для защиты информации от несанкционированно доступа применяются:

I. Организационные мероприятия,

II. Технические средства.

III. Программные средства.

IV. Криптография.

Организационные мероприятия включают в себя:

• пропускной режим;

• хранение носителей и устройств в сейфе (дискеты, монитор, клавиатура и т.д.);

• ограничение доступа лиц в компьютерные помещения и т.д.

Технические средства включают в себя различные аппаратные способы защиты информации:

• фильтры, экраны на аппаратуру;

• ключ для блокировки клавиатуры;

• устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т.д.;

• электронные ключи на микросхемах и т.д.

Программные средства защиты информации разработка специального программного обеспечения, которое бы не позволяло постороннему человеку, не знакомому с этим видом защиты, получать информацию из системы. Программные средства включают в себя:

• парольный доступ – задание полномочий пользователя;

• блокировка экрана и клавиатуры с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilites;

• использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом и т.д.

Под криптографическим способом защиты информации подразумевается ее шифрование при вводе в компьютерную систему.

Основными видами несанкционированного доступа к данным являются следующие:

• чтение;

• запись, и соответственно требуется защита данных:

• от чтения;

• от записи.

Защита данных от чтения автоматически подразумевает и защиту от записи, ибо возможность записи при отсутствии возможности чтения практически бессмысленна.

Защита от чтения осуществляется:

• наиболее просто – на уровне DOS введением атрибута Hidden для файлов;

• наиболее эффективно – шифрованием.

Защита от записи осуществляется:

• установкой атрибута Read Only для файлов;

• запрещением записи на дискету – рычажок или наклейка);

• запрещением записи через установки BIOS – дисковод не установлен.

При защите данных от чтения возникают две основные проблемы:

1. Как надежно зашифровать данные?

2. Как надежно уничтожить данные?

Проблемы надежного уничтожения данных заключаются в следующем:

• при удалении файла информация не стирается полностью;

• даже после форматирования дискеты и диска данные могут быть восстановлены с помощью специальных технических и программных средств по остаточному магнитному полю.

Для надежного удаления используют, например, утилиту Wipeinfo из пакета Norton Utilites. Данные стираются путем выполнения нескольких циклов (не меньше трех) записи на место удаляемых данных случайной последовательности нулей и единиц.

Для шифрования данных можно использовать утилиту Diskreet из пакета Norton Utilites. Используются два метода шифрования:

• быстрый собственный метод;

• медленный стандартный метод. | Для шифрования нужно выбрать требуемые файлы и набрать пароль. Исходные данные уничтожаются. При расшифровке данных используется исходный пароль.

Более общий подход состоит в создании секретного диска. Он создается средствами Diskreet. При введении пароля диск раскрывается и с ним можно работать как с обычным логическим диском. При этом все данные расшифровываются. В любой момент диск можно закрыть, при этом все данные вновь окажутся зашифрованными, j

На практике обычно используются комбинированные спо- \ собы защиты информации от несанкционированного доступа.

Обеспечение защиты информации в компьютерных сетях

Опасность злоумышленных несанкционированных действий над информацией приняла особенно угрожающий характер с развитием компьютерных сетей. Большинство систем обработки информации создавалось как обособленные объекты: рабочие станции, ЛВС, большие универсальные компьютеры и т.д. Каждая система использует свою рабочую платформу (MS DOS, Windows, Novell), а также разные сетевые протоколы (TCP/IP, VMS, MVS). Сложная организация сетей создает благоприятные предпосылки для совершения различного рода правонарушений, связанных с несанкционированным доступом к конфиденциальной информации. Большинство операционных систем, как автономных, так и сетевых, не содержат надежных механизмов защиты информации.

Следствием опасности сетевых систем стали постоянно увеличивающиеся расходы и усилия на защиту информации, доступ к которой можно осуществить через сетевые каналы связи. Сохранить целостность данных можно только при условии принятия специальных мер контроля доступа к данным и шифрования передаваемой информации. Разные системы нуждаются в разных степенях защиты. Актуальной стала задача объединения систем с различными степенями защищенности (например, на платформах Unix и Windows).

Необходимо иметь четкое представление о возможных каналах утечки информации и путях несанкционированного доступа* к защищаемой информации. Только в этом случае возможно построение эффективных механизмов защиты информации в компьютерных сетях1.

Угрозы безопасности сети

Пути утечки информации и несанкционированного доступа в компьютерных сетях в основной своей массе совпадают с таковыми в автономных системах (см. выше). Дополнительные возможности возникают за счет существования каналов связи и возможности удаленного доступа к информации. К ним относятся:

• электромагнитная подсветка линий связи;
• незаконное подключение к линиям связи;
• дистанционное преодоление систем защиты;
• ошибки в коммутации каналов;
• нарушение работы линий связи и сетевого оборудования.

Вопросы безопасности сетей решаются в рамках архитектуры безопасности, в структуре которой различают:

• угрозы безопасности;
• службы (услуги) безопасности;
• механизмы обеспечения безопасности.

Под угрозой безопасности понимаются действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы принято делить на две группы:

1) непреднамеренные, или случайные;
2) умышленные.

Случайные угрозы возникают как результат ошибок в программном обеспечении, выхода из строя аппаратных средств, неправильных действий пользователей или администратора сети и т. п.

Умышленные угрозы преследуют цель нанесения ущерба пользователям и абонентам сети и в свою очередь подразделяются на активные и пассивные.

Пассивные угрозы направлены на несанкционированное использование информационных ресурсов сети, но при этом не оказывают влияния на ее функционирование. Примером пассивной угрозы является получение информации, циркулирующей в каналах сети, посредством прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования сети посредством целенаправленного воздействия на ее аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы, искажение сведений в пользовательских базах данных или системной информации и т.п.

К основным угрозам безопасности относятся:

• раскрытие конфиденциальной информации;
• компроментация информации;
• несанкционированный обмен информацией;
• отказ от информации;
• отказ в обслуживании;
• несанкционированное использование ресурсов сети;
• ошибочное использование ресурсов сети.

Угрозы раскрытия конфиденциальной информации реализуются путем несанкционированного доступа к базам данных.

Компрометация информации реализуется посредством внесения несанкционированных изменений в базы данных.

Несанкционированное использование ресурсов сети является средством раскрытия или компрометации информации, а также наносит ущерб пользователям и администрации сети.

Ошибочное использование ресурсов является следствием ошибок, имеющихся в программном обеспечении ЛВС.

Несанкционированный обмен информацией между абонентами сети дает возможность получать сведения, доступ к которым запрещен, т.е. по сути приводит к раскрытию информации.

Отказ от информации состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки.

Отказ в обслуживании представляет собой весьма распространенную угрозу, источником которой является сама сеть. Подобный отказ особенно опасен в случаях, когда задержка с предоставлением ресурсов сети может привести к тяжелым для абонента последствиям.

Службы безопасности сети

Службы безопасности сети указывают направления нейтрализации возможных угроз безопасности. Службы безопасности находят свою практическую реализацию в различных механизмах безопасности. Одна и та же служба безопасности может быть реализована с использованием разных механизмов безопасности или их совокупности.

Протоколы информационного обмена в сетях делятся на две большие группы: типа виртуального соединения и дейтаграммные, в соответствии с которыми сети также принято делить на виртуальные и дейтаграммные.

В сетях типа виртуального соединения передача информации между абонентами организуется по так называемому виртуальному каналу и происходит в три этапа: создание канала (соединение), собственно передача, уничтожение канала (разъединение). Сообщения разбиваются на блоки, которые передаются в порядке их следования в сообщении.

В дейтаграммных сетях пакеты (дейтаграммы) сообщения передаются от отправителя к получателю независимо друг от друга по различным маршрутам, в связи с чем порядок доставки пакетов может не соответствовать порядку их следования в сообщении. Виртуальная сеть в концептуальном плане реализует принцип организации телефонной связи, тогда как дейщраммная – почтовой.

Международная организация стандартизации (МОС) определяет следующие службы безопасности:

1) аутентификация (подтверждение подлинности);
2) обеспечение целостности;
3) засекречивание данных;
4) контроль доступа;
5) защита от отказов.

Службы 4 и 5 едины для дейтаграммных и виртуальных сетей. Службы 1–3 характеризуются определенными отличиями, обусловленными особенностями используемых в сетях протоколов.

Служба аутентификации

Данная служба применительно к виртуальным сетям называется службой аутентификации объекта (одноуровневого) и обеспечивает подтверждение того факта, что отправитель информации является именно тем, за кого он себя выдает. Применительно к дейтаграммным сетям служба аутентификации называется службой аутентификации источника данных.

Службы целостности

Под целостностью понимается точное соответствие отправленных и полученных данных между собой. Службы целостности для рассматриваемых сетей выглядят следующим образом.

Виртуальные сети:

• служба целостности соединения с восстановлением;
• служба целостности соединения без восстановления;
• служба целостности выборочных полей соединения.

Дейтаграммные сети:

• служба целостности без соединения;
• служба целостности выборочных полей без соединения. Под полями понимаются отдельные определенные элементы блоков или пакетов передаваемых данных. Под восстановлением понимаются процедуры восстановления данных, уничтоженных (Или потерянных в результате обнаружения искажений, вставок или повторов в блоках, или дейтаграммах. В службах целостности дейтаграммных сетей наличие процедур восстановления не предусматривается.

Службы засекречивания данных

Службы засекречивания данных:

• служба засекречивания соединения – обеспечивает секретность всех данных, пересылаемых объектами по виртуальному каналу;
• служба засекречивания без соединения – обеспечивает секретность данных, содержащихся в каждой отдельной дейтаграмме;
• служба засекречивания отдельных полей соединения;
• служба засекречивания трафика – нейтрализует возможность получения сведений об абонентах сети и характере использования сети.

Механизмы безопасности

Среди механизмов безопасности сетей, предусмотренных МОС, обычно выделяют следующие основные:

• шифрование;
• контроль доступа;
• цифровая подпись.

Шифрование применяется для реализации служб засекречивания и используется в ряде других служб.

Механизмы контроля доступа обеспечивают реализацию одноименной службы безопасности, осуществляют проверку полномочий объектов сети, т.е. программ и пользователей, на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется в точке инициализации связи, в промежуточных точках, а также в конечной точке.

Механизмы контроля доступа делятся на две основные группы:

- аутентификация объектов, требующих ресурса, с последующей проверкой допустимости доступа, для которой используется специальная информационная база контроля доступа;
- использование меток безопасности, связываемых с объектами; наличие у объекта соответствующего мандата дает право на доступ к ресурсу.

Самым распространенным и одновременно самым ненадежным методом аутентификации является парольный доступ. Более совершенными являются пластиковые карточки и электронные жетоны. Наиболее надежными считаются методы аутентификации по особым приметам личности, так называемые биометрические методы.

Цифровая подпись используется для реализации служб аутентифиацш и защиты от отказов. По своей сути она призвана служить электронным аналогом реквизита «подпись», используемого на бумажных документах. Механизм цифровой подписи базируется на использовании способа шифрования с открытым ключом. Знание соответствующего открытого ключа дает возможность получателю электронного сообщения однозначно опознать его отправителя.

Дополнительными механизмами безопасности, предусмотренными МОС, являются следующие:

• обеспечение целостности данных;
• аутентификация;
• подстановка трафика;
• управление маршрутизацией;
• арбитраж.

Механизмы обеспечения целостности данных направлены на реализацию одноименной службы как применительно к отдельному блоку данных, так и к потоку данных. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Возможны и более простые методы контроля целостности потока данных, например нумерация блоков, дополнение их меткой времени и т.д.

Механизмы обеспечения аутентификации используются для реализации одноименной службы, различают одностороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов одного уровня проверяет подлинность другого, тогда как во втором – проверка является взаимной. На практике механизмы аутентификации, как правило, совмещаются с контролем доступа, шифрованием, цифровой подписью и арбитражем.

Механизмы подстановки трафика используются для реализации службы засекречивания потока данных. Они основываются на генерации объектами сети фиктивных блоков, их шифровании и организации их передачи по каналам сети.

Механизмы управления маршрутизацией используются для реализации служб засекречивания. Эти механизмы обеспечивают выбор маршрутов движения информации по сети.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами сети, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтвердить упомянутые характеристики.

В общем случае для реализации одной службы безопасности может использоваться комбинация нескольких механизмов безопасности.

Зашита операционных систем и обеспечение безопасности распределенных баз данных

Операционная система и аппаратных средства сети обеспечивают защиту ресурсов сети, одним из которых является сама ОС, т. е. входящие в нее программы и системная информация. Поэтому в сетевой ОС ЛВС должны быть так или иначе реализованы механизмы безопасности.

Принято различать:

• пассивные объекты защиты (файлы, прикладные программы, терминалы, области оперативной памяти и т. п.)

• активные субъекты (процессы), которые могут выполнять над объектами определенные операции.

Защита объектов реализуется операционной системой посредством контроля за выполнением субъектами совокупности правил, регламентирующих указанные операции. Указанную совокупность иногда называют статусом защиты. Операции, которые могут выполняться над защищенными объектами, принято называть правами доступа, а права доступа субъекта по отношению к конкретному объекту – возможностями. В качестве формальной модели статуса защиты в ОС чаще всего используется так называемая матрица контроля доступа.

Достаточно простым в реализации средством разграничения доступа к защищаемым объектам является механизм колец безопасности.

Защита файлов в ОС организована следующим образом. С каждым файлом связывается множество прав доступа: чтение, обновление и (или) выполнение (для исполняемых файлов). Владелец файла, т. е. создавшее его лицо, пользуется по отношению к файлу всеми правами. Часть этих прав он может передать членам группы - лицам, которым он доверяет сведения, имеющиеся в файле.

Доступ к ресурсам ОС чаще всего ограничен средствами зашиты по паролям. Пароль может быть использован и в качестве ключа для шифрования-дешифрования информации в пользовательских файлах. Сами пароли также хранятся в зашифрованном виде, что затрудняет их выявление и использование злоумышленниками. Пароль может быть изменен пользователем, администратором системы либо самой системой по истечении установленного интервала времени.

Защита распределенных баз данных

Обеспечение распределенных баз данных безопасности распределенных баз данных (РБД) косвенно реализуется сетевой ОС. Однако все указанные механизмы и средства инвариантны конкретным способам представления информации в БД. Подобная инвариантность приводит к тому, что в случае непринятия специальных мер все пользователи СУБД имеют равные права по использованию и обновлению всей информации, имеющейся в базе данных. В то же время указанная информация, как и при ее неавтоматизированном накоплении и использовании, должна быть разбита на категории по грифу секретности, группам пользователей, которым она доступна,а также по операциям над нею, которые разрешены указанным группам. Реализация этого процесса требует разработки и включения в состав СУБД специальных механизмов защиты.

Принятие решения о доступе к той или иной информации, имеющейся в РБД, может зависеть от следующих факторов:

1) времени и точки доступа;
2) наличия в БД определенных сведений;
3) текучесть состояния СУБД;
4) полномочий пользователя;
5) предыстории обращения к данным.

Случай 1. Доступ к БД с каждого терминала ЛВС может быть ограничен некоторым фиксированным отрезком времени.

Случай 2. Пользователь может получить из БД интересующие его сведения только при условии, что база данных содержит некоторую взаимосвязанную с ними информацию определенного содержания.

Случай 3. Обновление информации в некоторой БД может быть разрешено пользователю только в те моменты времени, когда она не обновляется другими пользователями.

Случай 4. Для каждого пользователя прикладной программы устанавливаются индивидуальные права на доступ к различным элементам базы данных. Эти права регламентируют операции, которые пользователь может выполнять над указанными элементами. Например, пользователю может быть разрешен отбор элементов БД, содержащих информацию о товарах, предлагаемых на бирже, но запрещено обновление этих сведений.

Случай 5. В основе этого фактора лежит то обстоятельство, что информацию пользователь может получить не непосредственным отбором тех или иных элементов БД, а косвенным путем, т. е. посредством анализа и сопоставления ответов СУБД на последовательно вводимые запросы (команды на обновление данных). В связи с этим для обеспечения безопасности информации в БД в общем случае необходимо учитывать предысторию обращения к данным.

Организация защиты информации в корпоративной сети

Обеспечение безопасности информации в крупных автоматизированных системах является сложной задачей. Реальную стоимость содержащейся в таких системах информации подсчитать сложно, а безопасность информационных ресурсов трудно измерить или оценить.

Объектом защиты в современных АИС выступает территориально распределенная гетерогенная сеть со сложной структурой, предназначенная для распределенной обработки данных, часто называемая корпоративной сетью. Характерной особенностью такой сети является то, что в ней функционирует оборудование самых разных производителей и поколений, а также неоднородное программное обеспечение, не ориентированное изначально на совместную обработку данных.

Решение проблем безопасности АИС заключается в построении целостной системы защиты информации. При этом защита от физических угроз, например доступа в помещения и утечки информации за счет ПЭМИ, не вызывает особых проблем. На практике приходится сталкиваться с рядом более общих вопросов политики безопасности, решение которых обеспечит надежное и бесперебойное функционирование информационной системы. Главными этапами построения политики безопасности являются следующие:

• обследование информационной системы на предмет установления ее организационной и информационной структуры и угроз безопасности информации;
• выбор и установка средств защиты;
• подготовка персонала работе со средствами защиты;
• организация обслуживания по вопросам информационной безопасности;
• создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается концепция информационной безопасности ИС, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

• организация сети организации;
• существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;
• организация хранения информации в ИС;
• организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);
• регламентация допуска персонала к той или иной информации;
• ответственность персонала за обеспечение безопасности.

В конечном итоге на основе концепции информационной безопасности ИС создается схема безопасности, структура которой должна удовлетворять следующим условиям:
1. Защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи.
2. Разграничение потоков информации между сегментами сети.
3. Защита критичных ресурсов сети.
4. Защита рабочих мест и ресурсов от несанкционированного доступа.
5. Криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда 10-15% стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

Защита от несанкционированного проникновения и утечки информации

Основным источником угрозы несанкционированного проникновения в АИС является канал подключения к внешней сети, например, к Internet. Вероятность реализации угрозы зависит от множества факторов, поэтому говорить о едином способе защиты в каждом конкретном случае не представляется возможным. Распространенным вариантом защиты является применение межсетевых экранов или брандмауэров.

Брандмауэр - барьер между двумя сетями: внутренней и внешней, обеспечивает прохождение входящих и исходящих пакетов в соответствии с правилами, определенными администратором сети. Брандмауэр устанавливается у входа в корпоративную сеть и все коммуникации проходят через него. Возможности межсетевых экранов позволяют определить и реализовать правила разграничения доступа как для внешних, так и для внутренних пользователей корпоративной сети, скрыть, при необходимости, структуру сети от внешнего пользователя, блокировать отправку информации по «запретным» адресам, контролировать использование сети и т.д. Вход в корпоративную сеть становится узким местом, прежде всего для злоумышленника.

Выбор брандмауэров достаточно широк. В качестве рекомендации необходимо отметить, что желательно ориентироваться на продукты, сертифицированные Гос-техкомиссией России. Несмотря на более высокую стоимость (сертифицированный экран стоит в среднем на 10-15% дороже несертифицированного), применение сертифицированных межсетевых экранов дает ряд преимуществ в решении юридических аспектов организации защиты конфиденциальной информации, а также некоторую гарантию качества реализации защитных механизмов в соответствии с руководящими документами, действующими в нашей стране.

Разграничение потоков информации между сегментами сети

В зависимости от характера информации, обрабатываемой в том или ином сегменте сети, и от способа взаимодействия между сегментами реализуют один из следующих вариантов.

В первом варианте не устанавливается никакого разграничения информационных потоков, т.е. защита практически отсутствует. Такой вариант оправдан в случаях, когда ни в одном из взаимодействующих сегментов не хранится и не обрабатывается критичная информация или когда сегменты сетевой информационной системы содержат информацию одинаковой важности и находятся в одном здании, в пределах контролируемой зоны.

Во втором варианте разграничение достигается средствами коммуникационного оборудования (маршрутизаторы, переключатели и т.п.). Такое разграничение не позволяет реализовать защитные функции в полном объеме поскольку, во-первых, коммуникационное оборудование изначально не рассматривается как средство защиты и, во-вторых, требуется

детальное представление о структуры сети и циркулирующих в ней информационных потоков.

В третьем варианте предполагается применение брандмауэров. Данный способ применяется, как правило, при организации взаимодействия между сегментами через сеть Internet, когда уже установлены брандмауэры, предназначенные для контроля за потоками информации между информационной системой и сетью Internet.

Защита критичных ресурсов АИС

Наиболее критичными ресурсами корпоративной сети являются серверы, а основным способом вмешательства в нормальный процесс их функционирования – проведение атак с использованием уязвимых мест в аппаратном и программном обеспечении. Атака может быть реализована как из внешней сети, так и из внутренней. Основная задача заключается не столько в своевременном обнаружении и регистрации атаки, сколько в противодействии ей.

Наиболее мощными инструментами защиты, предназначенными для оперативного реагирования на подобные нападения, являются специальные системы, наподобие системы RealSecure, производимой американской корпорацией Internet Security Systems, Inc., которые позволяют своевременно обнаружить и предотвратить наиболее известные атаки, проводимые по сети.

Защита рабочих мест и ресурсов от несанкционированного доступа

До настоящего времени большинство автоматизированных систем ориентируется только на встроенные защитные механизмы сетевых операционных систем. При правильном администрировании такие механизмы обеспечивают достаточную защиту информации на серверах корпоративной сети.

Однако обработка информации, подлежащей защите, производится на рабочих станциях, подавляющее большинство которых (более 90%) работает под управлением MS DOS или Windows'95 и не имеет средств обеспечения безопасности, так как эти операционные системы не содержат встроенных механизмов защиты. Как следствие, на незащищенном рабочем месте может обрабатываться критичная информация, доступ к которой ничем не ограничен. Для рабочих станций рекомендуется применять дополнительные средства защиты, часть из которых описана в предыдущем разделе.

Криптографическая защита информационных ресурсов

Шифрование является одним из самых надежных способов защиты данных от несанкционированного ознакомления. Особенностью применения подобных средств в России является жесткая законодательная регламентация. Для защиты конфиденциальной информации разрешается применять только сертифицированные ФАПСИ продукты. В настоящее время в корпоративных сетях они устанавливаются только на тех рабочих местах, где хранится информация, имеющая очень высокую степень важности.

Этапы построения политики безопасности

По окончании работ первого этапа - обследования информационной системы - необходимо иметь полное представление о том, в каком состоянии находится корпоративная сеть и о том, что нужно сделать, чтобы обеспечить в ней защиту информации.

На основе данных обследования можно перейти ко второму этапу - выбору, приобретению, установке, настройке и эксплуатации систем защиты в соответствии с разработанными рекомендациями.

Любое средство защиты создает дополнительные неудобства в работе пользователя, при этом препятствий тем больше, чем меньше времени уделяется настройке систем защиты. Администратор безопасности должен ежедневно обрабатывать данные регистрации, чтобы своевременно корректировать настройки, обеспечивающие адаптацию к изменениям в технологии обработки информации. Без этого любая система защиты, какой бы хорошей она ни была, обречена на медленное вымирание.

Третий этап - обучение администраторов безопасности работе со средствами защиты. В процессе обучения администратор получает базовые знания о технологии обеспечения

информационной безопасности, об имеющихся в операционных системах подсистемах безопасности и о возможностях систем защиты, о технологических приемах, используемых при их настройке и эксплуатации.

Четвертый этап - информационное обслуживание по вопросам безопасности. Наличие своевременной информации об уязвимых местах и способах защиты способствует принятию адекватных мер обеспечения безопасности. Источники подобных сведений - книги, журналы, Web-серверы и т.п. Однако администратор безопасности не всегда имеет достаточное количество времени для поиска необходимых сведений в этом море информации. Поэтому при выборе системы защиты необходимо учитывать возможности обеспечения последующей информационной поддержки.

Пятый этап - периодический аудит системы информационной безопасности. Корпоративная сеть является постоянно изменяющейся структурой: появляютсяновые серверы и рабочие станции, меняется программное обеспечение и его настройки, состав информации, персонал, работающий в организации, и т.д. Все это приводит к тому, что степень защищенности системы постоянно изменяется и, что наиболее опасно, снижается.

Чтобы адаптировать систему информационной безопасности к новым условиям работы, необходимо отслеживать изменения и своевременно реагировать на них. Многие работы по анализу состояния защищенности корпоративной сети могут быть выполнены при помощи специальных программных средств, например Internet Scanner и System Security Scanner из семейства SAFESUITE корпорации Internet Security Systems Inc. Такие программные средства существенно облегчают работу администратора безопасности по поиску ошибок в настройках и выявлению критичного программного обеспечения, а также позволяют в автоматизированном режиме отслеживать состояние корпоративной сети, своевременно обнаруживать и устранять возможные источники проблем.

Составной частью работ пятого этапа является корректировка плана защиты в соответствии с реальным состоянием корпоративной сети, поскольку самая совершенная схема рано или поздно устаревает и становится препятствием на пути совершенствования технологии обработки данных.

Следует помнить, что не существует стандартных решений, одинаково хорошо работающих в разных условиях. Всегда возможны и необходимы дополнения к рассмотренному общему плану организации защиты корпоративной сети, учитывающие особые условия той или иной организации. Однако реализация комплекса рассмотренных мероприятий с учетом возможных дополнений способна обеспечить достаточный уровень защищенности информации в корпоративной сети.