**РЕФЕРАТ**

по дисциплине

**Информационные технологии в маркетинге**

на тему

**Защита информации в экономических информационных системах (ЭИС)**

**1. Виды угроз безопасности ЭИС**

Наряду с интенсивным развитием вычислительных средств и систем передачи информации все более актуальной становится проблема обеспечения ее безопасности. Меры безопасности направлены на предотвращение несанкционированного получения информации, физического уничтожения или модификации защищаемой информации.

Зарубежные публикации последних лет показывают, что возможности злоупотреблений информацией, передаваемой по каналам связи, развивались и совершенствовались не менее интенсивно, чем средства их предупреждения. В этом случае для защиты информации требуется не просто разработка частных механизмов защиты, а организация комплекса мер, т.е. использование специальных средств, методов и мероприятий с целью предотвращения потери информации. В этом смысле сегодня рождается новая современная технология — технология защиты информации в компьютерных информационных системах и в сетях передачи данных.

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

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

Угрозы принято делить на случайные, или непреднамеренные, и умышленные. Источником первых могут быть ошибки в программном обеспечении, выходы из строя аппаратных средств, неправильные действия пользователей или администрации и т.п. Умышленные угрозы преследуют цель нанесения ущерба пользователям АИТ и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

К основным угрозам безопасности информации относят:

раскрытие конфиденциальной информации;

компрометация информации;

несанкционированное использование информационных ресурсов;

ошибочное использование ресурсов;

несанкционированный обмен информацией;

отказ от информации;

отказ от обслуживания.

Средствами реализации угрозы раскрытия конфиденциальной информации могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), другими лицами наносит ее владельцам существенный ущерб.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Несанкционированное использование информационных ресурсов, с одной стороны, является средством раскрытия или компрометации информации, а с другой — имеет самостоятельное значение, поскольку, даже не касаясь пользовательской или системной информации, может нанести определенный ущерб абонентам и администрации. Этот ущерб может варьировать в широких пределах — от сокращения поступления финансовых средств до полного выхода АИТ из строя.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее может привести к разрушению, раскрытию или компрометации указанных ресурсов. Данная угроза чаще всего является следствием ошибок в программном обеспечении АИТ.

Несанкционированный обмен информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен, что по своим последствиям равносильно раскрытию содержания маркетинговой информации.

Отказ от информации состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения «техническим» путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИТ. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных или даже антимонопольных действий.

Основными типовыми путями несанкционированного доступа к информации, сформулированными на основе анализа зарубежной печати, являются:

перехват электронных излучений;

принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;

применение подслушивающих устройств (закладок);

дистанционное фотографирование;

перехват акустических излучений и восстановление текста принтера;

хищение носителей информации и документальных отходов;

чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

копирование носителей информации с преодолением мер защиты;

маскировка под зарегистрированного пользователя;

мистификация (маскировка под запросы системы);

использование программных ловушек;

использование недостатков языков программирования и операционных систем;

включение в библиотеки программ специальных блоков типа «Троянский конь»;

незаконное подключение к аппаратуре и линиям связи;

злоумышленный вывод из строя механизмов защиты;

внедрение и использование компьютерных вирусов.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерных вирусов, ибо эффективной защиты против них разработать не удалось. Остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности.

**2. Методы и средства защиты информации в экономических информационных системах**

угроза безопасность информация защита

При разработке АИТ возникает проблема по решению вопроса безопасности информации, составляющей коммерческую тайну, а также безопасности самих компьютерных информационных систем.

Современные АИТ обладают следующими основными признаками:

содержат информацию различной степени конфиденциальности;

при передаче данных имеют криптографическую защиту информации различной степени конфиденциальности;

отражают иерархичность полномочий субъектов, открывают доступ к программам, к АРМ, файл-серверам, каналам связи и информации системы; необходимость оперативного изменения этих полномочий;

организуют обработку информации в диалоговом режиме, в режиме разделения времени между пользователями и в режиме реального времени;

обеспечивают управление потоками информации как в локальных сетях, так и при передаче по каналам связи на далекие расстояния;

регистрируют и учитывают попытки несанкционированного доступа, события в системе и документах, выводимых на печать;

обеспечивают целостность программного продукта и информации в АИТ;

устанавливают наличие средств восстановления системы защиты информации, а также обязательный учет магнитных носителей;

создают условия для физической охраны средств вычислительной техники и магнитных носителей.

Организационные мероприятия и процедуры, используемые для решения проблемы безопасности информации, решаются на всех этапах проектирования и в процессе эксплуатации АИТ. Существенное значение при проектировании придается предпроектному обследованию объекта. На этой стадии проводятся следующие действия:

устанавливается наличие конфиденциальной информации в разрабатываемой АИТ, оцениваются уровень конфиденциальности и объемы такой информации;

определяются режимы обработки информации (диалоговый, телеобработки и реального времени), состав комплекса технических средств, общесистемные программные средства и т.д.;

анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;

определяется степень участия персонала, функциональных служб, научных и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности;

вводятся мероприятия по обеспечению режима секретности на стадии разработки системы.

Среди организационных мероприятий по обеспечению безопасности информации важное место принадлежит охране объекта, на котором расположена защищаемая АИТ (территория здания, помещения, хранилища информационных носителей). При этом устанавливаются соответствующие посты охраны, технические средства, предотвращающие или существенно затрудняющие хищение средств вычислительной техники, информационных носителей, а также исключающие несанкционированный доступ к АИТ и линиям связи.

Функционирование системы защиты информации от несанкционированного доступа как комплекса программно-технических средств и организационных (процедурных) решений предусматривает:

учет, хранение и выдачу пользователям информационных носителей, паролей, ключей;

ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа);

оперативный контроль за функционированием систем защиты секретной информации;

контроль соответствия общесистемной программной среды эталону;

приемку включаемых в АИТ новых программных средств;

контроль за ходом технологического процесса обработки финансово-кредитной информации путем регистрации анализа действий пользователей;

сигнализацию опасных событий и т.д.

Следует отметить, что без надлежащей организационной поддержки программно-технических средств защиты информации от несанкционированного доступа и точного выполнения ; предусмотренных проектной документацией процедур в должной мере не решить проблему обеспечения безопасности информации, какими бы совершенными эти программно-технические средства ни были.

Создание базовой системы зашиты информации в АИТ основывается на следующих принципах:

Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты.

Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки. Пользователям предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения» автоматизированной обработки доступной им конфиденциальной информации.

Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в АИТ без ее предварительной регистрации.

Обеспечение надежности системы защиты, т.е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

«Прозрачность» системы защиты информации для общего, прикладного программного обеспечения и пользователей АИТ.

Экономическая целесообразность использования системы защиты. Он выражается в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации АИТ без системы защиты информации.

Проблема создания системы защиты информации включает две взаимодополняющие задачи:

разработку системы защиты информации (ее синтез);

оценку, разработанной системы защиты информации.

Вторая задача решается путем анализа технических характеристик защиты информации с целью установления соответствия ее требованиям, предъявляемым к таким системам.

В настоящее время подобные задачи решаются практически исключительно экспертным путем с помощью сертификации средств системы защиты информации и ее аттестации в процессе внедрения.

Раскроем основное содержание представленных средств и методов защиты информации, которые представляют основу механизмов защиты.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом — метод защиты информации с помощью регулирования использования всех ресурсов компьютерной информационной системы банковской деятельности (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 (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;

реагирование (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, когда пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение — метод защиты, побуждающий пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и «неписанных»).

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты. К основным средствам защиты, используемым для создания механизма защиты, относятся следующие.

Технические средства представляют электрические, электромеханические и электронные устройства. Вся совокупность указанных средств делится на аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу:

Физическими средствами являются автономные устройства и системы (замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации и др.).

Программные средства — это программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах ее жизненного цикла (проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, испытание, 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. Подобные нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциаций пользователей ЭВМ США.

Законодательные средства защиты определяются законодательными актами страны, регламентирующими правила пользования, обработки и передачи информации ограниченного доступа и устанавливающими 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 (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность).

Для реализации мер безопасности используются различные механизмы шифрования (криптографии). Криптография — это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Сущность криптографических методов заключается в следующем.

Готовое к передаче сообщение — будь то данные, речь либо графическое изображение того или иного документа, — обычно называется открытым, или незащищенным, текстом (сообщением). В процессе передачи такого сообщения по незащищенным каналам связи оно может быть легко перехвачено или отслежено подслушивающим лицом посредством умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к сообщению оно зашифровывается, преобразуясь в шифрограмму, или закрытый текст. Санкционированный пользователь, получив сообщение, дешифрует или раскрывает его посредством обратного преобразования криптограммы, вследствие чего получается исходный открытый текст.

Метод преобразования в криптографической системе определяется используемым специальным алгоритмом, действие которого определяется уникальным числом или битовой последовательностью, обычно называемым шифрующим ключом.

Каждый используемый ключ может производить различные шифрованные сообщения, определяемые только этим ключом. Для большинства систем закрытия схема генератора ключа может представлять собой либо набор инструкций, команд, либо часть, узел аппаратуры (hardware), либо компьютерную программу (software), либо все это вместе. Однако в любом случае процесс шифрования/дешифрования определяется единственно выбранным специальным ключом. Таким образом, чтобы обмен зашифрованными сообщениями проходил успешно, и отправителю, и получателю необходимо знать правильную ключевую установку и хранить ее в тайне.

Следовательно, надежность любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее этот ключ должен быть известен другим пользователям сети, чтобы они могли свободно обмениваться зашифрованными сообщениями. Криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации, поскольку подслушивающее лицо, пассивно перехватывающее сообщение, будет иметь дело только с зашифрованным текстом. В то же время истинный получатель, приняв сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

Шифрование может быть симметричным и асимметричным. Первое основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Второе характеризуется тем, что для шифрования используется один общедоступный ключ, а для дешифрования — другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Наряду с шифрованием внедряются следующие механизмы безопасности:

цифровая (электронная) подпись;

контроль доступа;

обеспечение целостности данных;

обеспечение аутентификации;

постановка графика;

управление маршрутизацией;

арбитраж или освидетельствование.

Механизмы цифровой подписи основываются на алгоритмах асимметричного шифрования и включают две процедуры: формирование подписи отправителем и ее опознавание (верификацию) получателем- Первая процедура обеспечивает шифрование блока данных либо его дополнение криптографической контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя.

Механизмы контроля доступа осуществляют проверку полномочий объектов АИТ (программ и пользователей) на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке.

Механизмы обеспечения целостности данных применяются к отдельному блоку и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока и обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

Различают одностороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов проверяет подлинность другого, во втором случае проверка является взаимной.

Механизмы постановки графика, называемые также механизмами заполнения текста, используются для засекречивания потока данных. Они основываются на генерации объектами АИТ фиктивных блоков, их шифровании и организации передачи по каналам сети. Тем самым нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по скомпрометированным (небезопасным) физически ненадежным каналам.

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

В АИТ при организации безопасности данных используется комбинация нескольких механизмов.

**3. Основные виды защиты, используемые в АИТ маркетинговой деятельности**

В практической маркетинговой деятельности применение мер и средств защиты информации включает следующие самостоятельные направления:

защиту информации от несанкционированного доступа;

защиту информации в системах связи;

защиту юридической значимости электронных документов;

защиту конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;

защиту информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;

защиту от несанкционированного копирования и распространения программ и ценной компьютерной информации.

Для каждого направления определяются основные цели и задачи.

Под несанкционированным доступом понимается нарушение установленных правил разграничения доступа, последовавшее в результате случайных или преднамеренных действий пользователей либо других субъектов системы разграничения, являющейся составной частью системы защиты информации.

Субъекты, совершившие несанкционированный доступ к информации, называются нарушителями. С точки зрения защиты информации несанкционированный доступ может иметь следующие последствия: утечку обрабатываемой конфиденциальной информации, ее искажение или разрушение в результате умышленного нарушения работоспособности АИТ.

Нарушителями могут быть:

штатные пользователи АИТ;

сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение системы;

обслуживающий персонал (инженеры);

другие сотрудники, имеющие санкционированный доступ к АИТ (в том числе подсобные рабочие, уборщицы и т.д.).

Доступ к АИТ посторонних лиц, не принадлежащих к указанным категориям, исключается организационно-режимными мерами.

Под каналом несанкционированного доступа к информации понимается последовательность действий лиц и выполняемых ими технологических процедур, которые либо выполняются несанкционированно, либо обрабатываются неправильно в результате ошибок персонала и/или сбое оборудования, приводящих в конечном итоге к факту несанкционированного доступа. Выявление всех каналов несанкционированного доступа проводится в ходе проектирования путем анализа технологии хранения, передачи и обработки информации, определенного порядка проведения работ, разработанной системы защиты информации и выбранной модели нарушителя.

Защита конфиденциальной и ценной информации от несанкционированного доступа и модификации призвана обеспечить решение одной из наиболее важных задач защиты имущественных прав владельцев и пользователей ПЭВМ — защиту собственности, воплощенную в обрабатываемой с помощью ПЭВМ информации от всевозможных злоумышленных покушений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб.

Центральной проблемой защиты информации от несанкционированного доступа является разграничение функциональных полномочий и доступа к информации, направленное не только на предотвращение возможности потенциального нарушителя «читать» хранящуюся в ПЭВМ информацию, но и на предотвращение возможности нарушителя модифицировать ее штатными и нештатными средствами.

Требования по защите информации от несанкционированного доступа направлены на достижение (в определенном сочетании) трех основных свойств защищаемой информации:

конфиденциальность (засекреченная информация должна быть доступна только тому, кому она предназначена);

целостность (информация, на основе которой принимаются важные решения, должна быть достоверной, точной и защищена от возможных непреднамеренных и злоумышленных искажений);

готовность (информация и соответствующие информационные службы должны быть доступны, готовы к обслуживанию всегда, когда в них возникает необходимость).

В основе контроля доступа к данным лежит система разграничения доступа между пользователями АИТ и информацией, обрабатываемой системой. Для успешного функционирования любой системы разграничения доступа необходимо решение следующих задач:

невозможность обхода системы' разграничения доступа действиями, находящимися в рамках выбранной модели;

гарантированная идентификация пользователя, осуществляющего доступ к данным (аутентификация пользователя).

Одним из эффективных методов увеличения безопасности АИТ является регистрация. Система регистрации и учета, ответственная за ведение регистрационного журнала, позволяет проследить за тем, что происходило в прошлом, и соответственно перекрыть каналы утечки информации. В регистрационном журнале фиксируются все осуществленные или неосуществленные попытки доступа к данным или программам. Содержание регистрационного журнала может анализироваться как периодически, так и непрерывно.

В регистрационном журнале ведется список всех контролируемых запросов, осуществляемых пользователями системы.

Система регистрации и учета осуществляет:

регистрацию входа-выхода субъектов доступа в систему/из системы либо регистрацию загрузки и инициализации операционной системы и ее программного останова (регистрация выхода из системы или останов не проводится в моменты аппаратного отключения АИТ), причем в параметрах регистрации указывается:

время и дата входа-выхода субъекта доступа в систему/из системы или загрузки/останова системы; результат попытки входа — успешный или неуспешный (при попытке несанкционированного доступа), идентификатор (код или фамилия) субъекта, предъявляемый при попытке доступа;

регистрацию и учет выдачи печатных (графических) документов на «твердую копию»;

регистрацию запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;

регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

учет всех защищаемых носителей информации с помощью их любой маркировки. Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи/приема; должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.

Защита информации в системах связи направлена на предотвращение возможности несанкционированного доступа к конфиденциальной и ценной информации, циркулирующей по каналам связи различных видов. Данный вид защиты преследует достижение тех же целей: обеспечение конфиденциальности и целостности информации. Наиболее эффективным средством защиты информации в неконтролируемых каналах связи является применение криптографии и специальных связных протоколов.

Защита юридической значимости электронных документов оказывается необходимой при использовании систем и сетей для обработки, хранения и передачи информационных объектов, содержащих приказы, платежные поручения, контракты и другие распорядительные, договорные, финансовые документы. Их общая особенность заключается в том, что в случае возникновения споров (в том числе и судебных) должна быть обеспечена возможность доказательства истинности факта того, что автор действительно фиксировал акт своего волеизъявления в отчуждаемом электронном документе. Для решения данной проблемы используются современные криптографические методы проверки подлинности информационных объектов, связанные с применением так называемых «цифровых подписей». На практике вопросы защиты значимости электронных документов решаются совместно с вопросами защиты компьютерных информационных систем.

Защита информации от утечки по каналам побочных электромагнитных излучений и наводок — важный аспект защиты конфиденциальной и секретной информации в ПЭВМ от несанкционированного доступа со стороны посторонних лиц. Данный вид защиты направлен на предотвращение возможности утечки информативных электромагнитных сигналов за пределы охраняемой территории. При этом предполагается, что внутри охраняемой территории применяются эффективные режимные меры, исключающие возможность бесконтрольного использования специальной аппаратуры перехвата, регистрации и отображения электромагнитных сигналов. Для защиты от побочных электромагнитных излучений и наводок широко применяется экранирование помещений, предназначенных для размещения средств вычислительной техники, а также технические меры, позволяющие снизить интенсивность информативных излучений самого оборудования (ПЭВМ и средств связи).

В некоторых ответственных случаях может потребоваться дополнительная проверка вычислительного оборудования на предмет возможного выявления специальных закладных устройств финансового шпионажа, которые могут быть внедрены с целью регистрации или записи информативных излучений компьютера, а также речевых и других несущих уязвимую информацию сигналов.

Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ приобрела за последнее время особую актуальность. Масштабы реальных проявлений «вирусных эпидемий» оцениваются сотнями тысяч случаев «заражения» персональных компьютеров. Хотя некоторые из вирусных программ оказываются вполне безвредными, многие из них имеют разрушительный характер. Особенно опасны вирусы для компьютеров, входящих в состав однородных локальных вычислительных сетей. Некоторые особенности современных компьютерных информационных систем создают благоприятные условия для распространения вирусов. К ним, в частности, относятся:

необходимость совместного использования программного обеспечения многими пользователями;

трудность ограничения в использовании программ;

ненадежность существующих механизмов защиты;

разграничения доступа к информации в отношении противодействия вирусу и т.д.

Имеют место два направления в методах защиты от вирусов:

применение «иммуностойких» программных средств, защищенных от возможности несанкционированной модификации (разграничение доступа, методы самоконтроля и самовосстановления);

использование специальных программ-анализаторов, осуществляющих постоянный контроль за возникновением отклонений в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности (например, обнаружение нарушений целостности программного обеспечения), а также входной контроль новых программ перед их использованием (по характерным признакам наличия в их теле вирусных образований).

Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации является самостоятельным видом защиты имущественных прав, ориентированной на охрану интеллектуальной собственности, воплощенной в виде программ ПЭВМ и ценных баз данных. Данная защита обычно осуществляется с помощью специальных программных средств, подвергающих защищаемые программы и базы данных предварительной обработке (вставка парольной защиты, проверки по обращению к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабочей ПЭВМ по ее уникальным характеристикам и т.д.), которая приводит исполнимый код защищаемой программы и базы данных в состояние, препятствующее его выполнению на «чужих» машинах.

Для повышения защищенности применяются дополнительные аппаратные блоки (ключи), подключаемые к разъему принтера или к системной шине ПЭВМ, а также шифрование файлов, содержащих исполнимый код программы. Общим свойством средств защиты программ от несанкционированного копирования является ограниченная стойкость такой защиты, ибо, в конечном счете, исполнимый код программы поступает на выполнение в центральный процессор в открытом виде и может быть прослежен с помощью аппаратных отладчиков. Однако это обстоятельство не снижает потребительские свойства средств защиты до нуля, так как основная цель их применения — максимально затруднить, хотя бы временно, возможность несанкционированного копирования ценной информации.

Контроль целостности программного обеспечения проводится с помощью внешних средств (программ контроля целостности) и внутренних средств (встроенных в саму программу).

Контроль целостности программ внешними средствами выполняется при старте системы и состоит в сравнении контрольных сумм отдельных блоков программ с их эталонными суммами. Контроль целостности программ внутренними средствами выполняется при каждом запуске программы на выполнение и состоит в сравнении контрольных сумм отдельных блоков программ с их эталонными суммами. Такой контроль используется в программах для внутреннего пользования.

Одним из потенциальных каналов несанкционированного доступа к информации является несанкционированное искажение прикладных и специальных программ нарушителем с целью получения конфиденциальной информации. Подобные действия могут преследовать цель изменения правил разграничения доступа или обхода их (при внедрении в прикладные программы системы защиты) либо организацию незаметного канала получения конфиденциальной информации непосредственно из ; прикладных программ (при внедрении в прикладные программы). Одним из методов противодействия этому является контроль целостности базового программного обеспечения, осуществляемый с помощью специальных программ. Однако данный метод недостаточен, поскольку предполагает, что программы контроля целостности не могут быть подвергнуты модификации нарушителем.

При защите коммерческой информации, как правило, используются любые существующие средства и системы защиты данных от несанкционированного доступа, но в каждом случае следует реально оценивать важность защищаемой информации и ущерб, который может нанести ее утрата.

Чем выше уровень защиты, тем она дороже. Сокращение затрат идет в направлении стандартизации технических средств. В ряде случаев исходя из конкретных целей и условий рекомендуется применять типовые средства, прошедшие аттестацию, даже если они уступают индивидуально изготовленным по некоторым параметрам.

Защита информации может решаться разными методами, но наибольшей надежностью и эффективностью обладают (а для каналов связи являются единственно целесообразными) системы и средства, построенные на базе криптографических методов. В случае использования иных методов большую сложность составляет доказательство достаточности реализованных мер и обоснование надежности системы защиты от несанкционированного доступа.

Необходимо иметь в виду, что подлежащие защите сведения могут быть получены «противником» не только за счет проникновения в ЭВМ, которые с достаточной степенью надежности могут быть предотвращены (например, все данные хранятся только в зашифрованном виде), но и за счет побочных электромагнитных излучений и наводок на цепи питания и заземления ЭВМ, а также проникновения в каналы связи. Все без исключения электронные устройства, блоки и узлы ЭВМ в той или иной мере излучают побочные сигналы, причем они могут быть достаточно мощными и распространяться на расстояния от нескольких метров до нескольких километров. Наибольшую опасность представляет получение «противником» информации о ключах. Восстановив ключ, можно предпринять успешные действия по завладению зашифрованными данными, которые, как правило, оберегаются менее серьезно, чем соответствующая открытая информация. С этой точки зрения выгодно отличаются именно аппаратные и программно-аппаратные средства защиты от несанкционированного доступа, для которых побочные сигналы о ключевой информации существенно ниже, чем для чисто программных реализаций.

Итак, определяющим фактором при выборе и использовании средств защиты является надежность защиты.

**Список литературы**

1. Титоренко Г.А. Автоматизированные информационные технологии в экономике. М.: ЮНИТИ, 2008.
2. Быкова Е.В., Стоянова Е.С. Финансовое искусство коммерции. М.: Перспектива, 2009.
3. Тихомиров В.П., Хорошилов А.В. Введение в информационный выбор. М.: Финансы и статистика, 2009.
4. Ковальков В.П. Эффективные технологии в маркетинге. Спб.: Экономическое образование, 2008.
5. Глазьев В.П. Операционные технологии межбанковского финансового рынка. М.: ЮНИТИ, 2009.