УВАЖАЕМЫЕ СТУДЕНТЫ! Изучите приведенную лекцию, законспектируйте основные понятия, дайте ответы на контрольные вопросы.

Ответы на вопросы, фотоотчет, предоставить преподавателю на e-mail: r.bigangel@gmail.com до 23.03.2023.

При возникновении вопросов по приведенному материалу обращаться по следующему номеру телефона: (072)111-37-59, (Viber, WhatsApp), vk.com: https://vk.com/daykini

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

Лекция 41 (продолжение)
Защита программного средства

Интерес к вопросам защиты информации в последнее время вырос, что связывают с возрастанием роли информационных ресурсов в конкурентной борьбе, расширением использования сетей, а, следовательно, и возможностей несанкционированного доступа к хранимой и передаваемой информации. Развитие средств, методов и форм автоматизации процессов хранения и обработки информации и массовое применение персональных компьютеров делают информацию гораздо более уязвимой. Информация, циркулирующая в них, может быть незаконно изменена, похищена или уничтожена. Основными факторами, способствующими повышению ее уязвимости, являются следующие:

· увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

· сосредоточение в единых базах данных информации различного назначения и принадлежности;

· расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и информационной базы;

· усложнение режимов работы технических средств вычислительных систем: широкое внедрение мультипрограммного режима, а также режима разделения времени;

· автоматизация межмашинного обмена информацией, в том числе на больших расстояниях.

Поэтому основной проблемой, которую должны решить проектировщики при создании системы защиты данных в ИБ, является проблема обеспечения безопасности хранимых данных, предусматривающая разработку системы мер обеспечения безопасности, направленных на предотвращение

несанкционированного получения информации, физического уничтожения или модификации защищаемой информации. Вопросы разработки способов и методов защиты данных в информационной базе являются только частью проблемы проектирования системы защиты в ЭИС и в настоящее время получили большую актуальность. Этим вопросам посвящено много работ, но наиболее полно и системно они изложены в работах [2,12,38,41,59].

Чтобы разработать систему защиты, необходимо, прежде всего, определить, что такое "угроза безопасности информации", выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным. В литературе предложены различные определения угрозы в зависимости от ее специфики, среды проявления, результата ее воздействия, приносимого ею ущерба и т. д. Так в работе [2] под угрозой понимается целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой в системе информации и приводит к ее случайному или предумышленному изменению или уничтожению.

В работе [12] предлагается под "угрозой безопасности информации" понимать "действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и обрабатываемые средства".

Случайные угрозы включают в себя ошибки, пропуски и т.д., а также события, не зависящие от человека, например природные бедствия. Бедствия бывают природными или вызванными деятельностью. Меры защиты от них ─ в основном, организационные. К ошибкам аппаратных и программных средств относятся повреждения компьютеров и периферийных устройств (дисков, лент и т. д.), ошибки в прикладных программах и др.

К ошибкам по невниманию, довольно часто возникающим во время технологического цикла обработки, передачи или хранения данных, относятся ошибки оператора или программиста, вмешательство во время выполнения тестовых программ, повреждение носителей информации и др.

Преднамеренные угрозы могут реализовать как внутренние для системы участники процесса обработки данных (персонал организации, сервисное звено и т. д.), так и люди, внешние по отношению к системе, так называемые "хакеры".

Авторы [2] на примере практической деятельности коммерческих банков перечисляют основные виды угроз безопасности хранимой информации; средства их устранения, к которым они относят:

- копирование и кража программного обеспечения;
- несанкционированный ввод данных;
- изменение или уничтожение данных на магнитных носителях;
- саботаж;
- кража информации;

· раскрытие конфиденциальной информации, используя несанкционированный доступ к базам данных, прослушивание каналов и т.п.;

· компрометация информации 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;

· несанкционированное использование информационных ресурсов, которое может нанести определенный ущерб и этот ущерб может варьироваться от сокращения поступления финансовых средств до полного выхода ЭИС из строя;

· ошибочное использование информационных ресурсов, которое может привести к их разрушению, раскрытию или компрометации, что является следствием ошибок, имеющихся в программном обеспечении ЭИС;

· несанкционированный обмен информацией между абонентами, который может привести к получению одним из них сведений, доступ к которым ему запрещен, что по своим последствиям равносильно раскрытию содержания хранимой информации;

· отказ в обслуживании, представляющий собой угрозу, источником которой может являться ЭИС, особенно опасен в ситуациях, когда задержка с предоставлением информационных ресурсов, необходимых для принятия решения, может стать причиной нерациональных действий руководства предприятия.

Под "несанкционированным доступом" понимается нарушение установленных правил разграничения доступа, последовавшее в результате случайных или преднамеренных действий пользователей или других субъектов системы разграничения, являющейся составной частью системы защиты информации. Субъекты, совершившие несанкционированный доступ к информации, называются нарушителями. Нарушителем может быть любой человек из следующих категорий: штатные пользователи ЭИС; сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение системы; обслуживающий персонал (инженеры); другие сотрудники, имеющие санкционированный доступ к ЭИС.

С точки зрения защиты информации несанкционированный доступ может иметь следующие последствия: утечка обрабатываемой конфиденциальной информации, а также ее искажение или разрушение в результате умышленного разрушения работоспособности ЭИС.

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 или сбоя оборудования, приводящих к несанкционированному доступу. Действия нарушителя можно разделить на четыре основные категории.

1. Прерывание ─ прекращение нормальной обработки информации, например, вследствие разрушения вычислительных средств. Отметим, что прерывание может иметь серьезные последствия даже в том случае, когда сама информация никаким воздействиям не подвергается.

2. Кража, или раскрытие ─ чтение или копирование информации с целью получения данных, которые могут быть использованы либо злоумышленником, либо третьей стороной.

3. Видоизменение информации.

4. Разрушение ─ необратимое изменение информации, например, стирание данных с диска.

К основным способам несанкционированного получения информации, сформулированным по данным зарубежной печати, относят:

· применение подслушивающих устройств (закладок);

· дистанционное фотографирование;

· перехват электронных излучений;

· принудительное электромагнитное облучение (подсветка) линий связи с целью осуществления паразитной модуляции несущей;

· мистификация (маскировка под запросы системы);

· перехват акустических излучений и восстановление текста принтера;

· хищение носителей информации и производственных отходов;

· считывание данных из массивов других пользователей;

· чтение остаточной информации из памяти системы после выполнения санкционированных запросов;

· копирование носителей информации с преодолением мер защиты;

· маскировка под зарегистрированного пользователя;

· использование программных ловушек;

· незаконное подключение к аппаратуре и линиям связи;

· вывод из строя механизмов защиты.

Для обеспечения защиты хранимых данных используется несколько методов и механизмов их реализации. В литературе выделяют следующие способы защиты:

· физические (препятствие);

· законодательные;

· управление доступом;

· криптографическое закрытие.

Физические способы защиты основаны на создании физических препятствий для злоумышленника, преграждающих ему путь к защищаемой информации (строгая система пропуска на территорию и в помещения с аппаратурой или с носителями информации). Эти способы дают защиту только от "внешних" злоумышленников и не защищают информацию от тех лиц, которые обладают правом входа в помещение.

Законодательные средства защиты составляют законодательные акты, которые регламентируют правила использования и обработки информации ограниченного доступа и устанавливают меры ответственности за нарушения этих правил.

Управление доступом представляет способ защиты информации путем регулирования доступа ко всем ресурсам системы (техническим, программным, элементам баз данных). В автоматизированных системах информационного обеспечения должны быть регламентированы; порядок работы пользователей и персонала, право доступа к отдельным файлам в базах данных и т.д. Управление доступом предусматривает следующие функции защиты:

· идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора: имени, кода, пароля и т. п);

· аутентификацию ─ опознание (установление подлинности) объекта или субъекта по предъявляемому им идентификатору;

· авторизацию ─ проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

· разрешение и создание условий работы в пределах установленного регламента;

· регистрацию (протоколирование) обращений к защищаемым ресурсам;

· реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Самым распространенным методом установления подлинности является метод паролей. Пароль представляет собой строку символов, которую пользователь должен ввести в систему каким-либо способом (напечатать, набрать на клавиатуре и т. п.). Если введенный пароль соответствует хранящемуся в памяти, то пользователь получает доступ ко всей информации, защищенной этим паролем. Пароль можно использовать и независимо от пользователя для защиты файлов, записей, полей данных внутри записей и т.д. Используют различные виды паролей:

1. Простой пароль. Пользователь вводит такой пароль с клавиатуры после запроса, а компьютерная программа (или специальная микросхема) кодирует его и сравнивает с хранящимся в памяти эталоном. Преимущество простого пароля в том, что его не нужно записывать, а недостаток ─ в относительной легкости снятия защиты. Простой пароль рекомендуется использовать для защиты данных небольшого значения и стоимости.

2. Пароль однократного использования. Пользователю выдается список из N паролей, которые хранятся в памяти компьютера в зашифрованном виде. После использования пароль стирается из памяти и вычеркивается из списка, так что перехват пароля теряет смысл. Такой пароль обеспечивает более высокую степень безопасности, но более сложен. Имеет он и другие недостатки. Во-первых, необходимо где-то хранить список паролей, так как запомнить его практически

невозможно, а в случае ошибки в процессе передачи пользователь оказывается в затруднительном положении: он не знает, следует ли ему снова передать тот же самый пароль или послать следующий. Во-вторых, возникают чисто организационные трудности: список может занимать много места в памяти, его необходимо постоянно изменять и т. д.

3. Пароль на основе выборки символов. Пользователь вводит из пароля отдельные символы, позиции которых задаются с помощью преобразования случайных чисел или генератора псевдослучайных чисел. Очевидно, пароль следует менять достаточно часто, поскольку постороннее лицо может в конце концов составить пароль из отдельных символов.

4. Метод "запрос-ответ". Пользователь должен дать правильные ответы на набор вопросов, хранящихся в памяти компьютера и управляемый операционной системой. Иногда пользователю задается много вопросов, и он может сам выбрать те из них, на которые он хочет ответить. Достоинство этого метода состоит в том, что пользователь может выбрать вопросы, а это дает весьма высокую степень безопасности в процессе включения в работу.

5. Пароль на основе алгоритма. Пароль определяется на основе алгоритма, который хранится в памяти компьютера и известен пользователю. Система выводит на экран случайное число, а пользователь, с одной стороны, и компьютер, ─ с другой, на его основе вычисляют по известному алгоритму пароль. Такой тип пароля обеспечивает более высокую степень безопасности, чем многие другие типы, но более сложен и требует дополнительных затрат времени пользователя.

6. Пароль на основе персонального физического ключа. В памяти компьютера хранится таблица паролей, где они записаны как в зашифрованном, так и в открытом видах. Лицам, допущенным к работе в системе, выдается специальная магнитная карточка, на которую занесена информация, управляющая процессом шифрования. Пользователь дожен вставить карточку в считывающее устройство и ввести свой пароль в открытом виде. Введенный пароль кодируется с использованием информации, записанной на карточке, и ищется соответствующая точка входа в таблицу паролей. Если закодированный пароль соответствует хранящемуся эталону, подлинность пользователя считается установленной. Для такого типа пароля существует угроза того, что на основе анализа пары "шифрованный пароль ─ открытый пароль" злоумышленник сможет определить алгоритм кодирования. Поэтому рекомендуется применять стойкие схемы шифрования.

Парольная защита широко применяется в системах защиты информации и характеризуется простотой и дешевизной реализации, малыми затратами машинного времени, не требует больших объемов памяти. Однако парольная защита часто не дает достаточного эффекта по следующим причинам:

1. Обычно задают слишком длинные пароли. Будучи не в состоянии запомнить пароль, пользователь записывает его на клочке бумаги, в записной книжке и т. п., что сразу делает пароль уязвимым.

2. Пользователи склонны к выбору тривиальных паролей, которые можно подобрать после небольшого числа попыток.

3. Процесс ввода пароля в систему поддается наблюдению даже в том случае, когда вводимые символы не отображаются на экране.

4. Таблица паролей, которая входит обычно в состав программного обеспечения операционной системы, может быть изменена, что нередко и происходит. Поэтому таблица паролей должна быть закодирована, а ключ алгоритма декодирования должен находиться только у лица, отвечающего за безопасность информации.

5. В систему может быть внесен "троянский конь", перехватывающий вводимые пароли и записывающий их в отдельный, поэтому при работе с новыми программными продуктами необходима большая осторожность.

При работе с паролями рекомендуется применение следующих правил и мер предосторожности:

· не печатать пароли и не выводить их на экран;

· часто менять пароли ─ чем дольше используется один и тот же пароль, тем больше вероятность его раскрытия;

· каждый пользователь должен хранить свой пароль и не позволять посторонним узнать его;

· всегда зашифровывать пароли и обеспечивать их защиту недорогими и эффективными средствами;

· правильно выбирать длину пароля (чем она больше, тем более высокую степень безопасности будет обеспечивать система) так как тем труднее будет отгадать пароль.

Основным методом защиты информации от несанкционированного доступа является также метод обеспечения разграничения функциональных полномочий и доступа к информации, направленный на предотвращение не только возможности потенциального нарушителя "читать" хранящуюся в ПЭВМ информацию, но и 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 и точной и должна быть защищена от возможных непреднамеренных и злоумышленных искажений);

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

Вторым методом, дополняющим первый, является разработка процедуры контроля доступа к данным, которая призвана для решения двух задач:

· сделать невозможным обход системы разграничения доступа действиями, находящимися в рамках выбранной модели;

· гарантировать идентификацию пользователя, осуществляющего доступ к данным.

Одним из основных методов увеличения безопасности ЭИС является регистрация пользователей и всех их действий, для чего необходимо разработать "Систему регистрации и учета", ответственную за ведение регистрационного журнала, которая позволяет проследить за тем, что происходило в прошлом, и соответственно перекрыть каналы утечки информации. В "Регистрационном журнале" фиксируются все осуществленные и неосуществленные попытки доступа к данным или программам и ведется список всех контролируемых запросов, осуществляемых пользователями системы.

Одним из потенциальных каналов несанкционированного доступа к информации является несанкционированное изменение прикладных и специальных программ нарушителем с целью получения конфиденциальной информации. Эти изменения 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). Например, в работе [47], приводятся следующие виды вредительских программ.

1. Лазейки (trapdoors). Лазейка представляет собой точку входа в программу, благодаря чему открывается непосредственный доступ к некоторым системным функциям. Лазейки обычно вставляют во время проектирования системы. Системные программисты организуют их при отладке программы, но по завершении ее разработки их надо устранить. Обнаружить лазейки можно путем анализа работы программ.

2. Логические бомбы (logic bombs). Логическая бомба ─ это компьютерная программа, которая приводит к повреждению файлов или компьютеров. Повреждение варьируется от искажения данных до полного стирания всех файлов и/или повреждения компьютера. Логическую бомбу, как правило, вставляют во время разработки программы, а срабатывает она при выполнении некоторого условия (время, дата, кодовое слово).

3. Троянские кони (trojan horses). Троянский конь ─ это программа, которая приводит к неожиданным (и обычно нежелательным) последствиям в системе. Особенностью троянского коня является то, что пользователь обращается к этой

программе, считая ее полезной. Троянские кони способны раскрыть, изменить или уничтожить данные или файлы. Их встраивают в программы широкого пользования, например в программы обслуживания сети, электронной почты и др. Антивирусные средства не обнаруживают эти программы, но системы управления доступом в больших компьютерах обладают механизмами идентификации и ограничения их действия. В "Оранжевой книге" Национального центра защиты компьютеров США ведется постоянно обновляемый список известных программ этого рода.

4. Червяки (worms). Червяк ─ это программа, которая распространяется в системах и сетях по линиям связи. Такие программы подобны вирусам в том отношении, что они заражают другие программы, а отличаются от них тем, что они не способны самовоспроизводиться. В отличие от троянского коня червяк входит в систему без ведома пользователя и копирует себя на рабочих станциях сети.

5. Бактерии (bacteria). Этот термин вошел в употребление недавно и обозначает программу, которая делает копии самой себя и становится паразитом, перегружая память и процессор.

6. Вирусы (viruses). Определения вируса весьма разнообразны, как и сами вирусы. Утвердилось определение доктора Фредерика Коуэна (Frederick Cohen): "Компьютерный вирус ─ это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса (или его разновидность)". Объектами вируса являются: операционная система, системные файлы, секторы начальной загрузки дисков, командный файл, таблица размещения файлов (FAT), файлы типа COM или EXE, файл CONFIG.SYS. В зависимости от области распространения и воздействия вирусы делятся на разрушительные и неразрушительные, резидентные и нерезидентные, заражающие сектор начальной загрузки, системные файлы, прикладные программы и др.

К числу методов противодействия этому относится метод контроля целостности базового программного обеспечения специальными программами. Однако этот метод недостаточен, поскольку предполагает, что программы контроля целостности не могут быть подвергнуты модификации нарушителем.

Надежность защиты может быть обеспечена правильным подбором основных механизмов защиты, некоторые из них рассмотрим ниже.

Механизм регламентации, основанный на использовании метода защиты информации, создает такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Механизм аутентификации. Различают одностороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов

проверяет подлинность другого, тогда как во втором случае проверка является взаимной.

Криптографические методы защиты информации. Эти методы защиты широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на дискетах. Для реализации мер безопасности используются различные способы шифрования (криптографии), суть которых заключается в том, что данные, отправляемые на хранение, или сообщения, готовые для передачи, зашифровываются и тем самым преобразуются в шифрограмму или закрытый текст. Санкционированный пользователь получает данные или сообщение, дешифрует их или раскрывает посредством обратного преобразования криптограммы, в результате чего получается исходный открытый текст. Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (или битовой последовательностью) обычно называемым шифрующим ключом.

В современной криптографии существует два типа криптографических алгоритмов*:*

1. классические алгоритмы, основанные на использовании закрытых, секретных ключей (симметричные);

2. алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ (асимметричные). В настоящее время находят широкое практическое применение в средствах защиты электронной информации алгоритмы с секретным ключом.

Рассмотрим кратко особенности их построения и применения.

1. Симметричное шифрование**,** применяемое в классической криптографии, предполагает использование одной секретной единицы ─ ключа, который позволяет отправителю зашифровать сообщение, а получателю расшифровать его. В случае шифрования данных, хранимых на магнитных или иных носителях информации, ключ позволяет зашифровать информацию при записи на носитель и расшифровать при чтении с него. Секретные ключи представляют собой основу криптографических преобразований, для которых, следуя правилу Керкхофа, стойкость хорошей шифровальной системы определяется лишь секретностью ключа.

Все многообразие существующих криптографических методов специалисты сводят к следующим классам преобразований [47]:

Моно- и многоалфавитные подстановки ─ наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Перестановки ─ несложный метод криптографического преобразования, используемый, как правило, в сочетании с другими методами.

Гаммирование ─ метод, который заключается в наложении на открытые данные некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры ─ представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем "чистые" преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

Самым простым способом шифрования является способ, который заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом. Под гаммой шифра понимается псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для шифрования открытых данных и расшифровывания зашифрованных данных.

Для генерации гаммы применяют программы для ЭВМ, которые называются генераторами случайных чисел. При этом требуется, чтобы, даже зная закон формирования, но не зная ключа в виде начальных условий, никто не смог бы отличить числовой ряд от случайного.

В работе [47] формулируются три основных *требования* к криптографически стойкому генератору псевдослучайной последовательности или гаммы.

1. Период гаммы должен быть достаточно большим для шифрования сообщений различной длины.

2. Гамма должна быть трудно предсказуемой. Это значит, что если известны тип генератора и кусок гаммы, то невозможно предсказать следующий за этим куском бит гаммы с вероятностью выше x. Если криптоаналитику станет известна какая-то часть гаммы, он все же не сможет определить биты, предшествующие ей или следующие за ней.

3. Генерирование гаммы не должно быть связано с большими техническими и организационными трудностями.

Таким образом, стойкость шифрования с помощью генератора псевдослучайных чисел зависит как от характеристик генератора, так и ─ причем в большей степени ─ от алгоритма получения гаммы.

Процесс расшифровывания данных сводится к повторной генерации гаммы шифра при известном ключе и наложения такой гаммы на зашифрованные данные. Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию и поэтому неприменим для серьезных информационных систем.

Сегодня реализовано довольно много различных алгоритмов криптографической защиты информации. Среди них можно назвать алгоритмы

DES, Rainbow (США); FEAL-4 и FEAL-8 (Япония); B-Crypt (Великобритания); алгоритм шифрования по ГОСТ 28147-89 (Россия) и ряд других, реализованных зарубежными и отечественными поставщиками программных и аппаратных средств защиты. Рассмотрим алгоритмы, наиболее широко применяемые в зарубежной и отечественной практике.

Алгоритм, изложенный в стандарте DES (Data Encryption Standard), принят в качестве федерального стандарта в 1977 г., наиболее распространен и широко применяется для шифрования данных в США. Этот алгоритм был разработан фирмой IBM для собственных целей. Однако после проверки Агентством Национальной Безопасности (АНБ) США он был рекомендован к применению в качестве федерального стандарта шифрования. Этот стандарт используется многими негосударственными финансовыми институтами, в том числе банками и службами обращения денег. Алгоритм DES не является закрытым и был опубликован для широкого ознакомления, что позволяет пользователям свободно применять его для своих целей.

При шифровании применяется 64-разрядный ключ. Для шифрования используются только 56 разрядов ключа, а остальные восемь разрядов являются контрольными. Алгоритм DES достаточно надежен. Он обладает большой гибкостью при реализации различных приложений обработки данных, так как каждый блок данных шифруется независимо от других. Это позволяет расшифровывать отдельные блоки зашифрованных сообщений или структуры данных, а следовательно, открывает возможность независимой передачи блоков данных или произвольного доступа к зашифрованным данным. Алгоритм может реализовываться как программным, так и аппаратным способами. Существенный недостаток этого алгоритма ─ малая длина ключа.

В настоящее время близится к завершению разработка нового американского стандарта шифрования AES (aes.nist.gov). Национальный институт стандартов и технологий США (NIST) объявил о соответствующем конкурсе, предъявив следующие условия: длина ключа должна составлять 128, 192 или 256 бит, длинна блоков данных ─ 128 бит. Кроме того, новый алгоритм должен работать быстрее DES.

Алгоритм шифрования, определяемый российским стандартом ГОСТ 28.147-89. "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования", является единым алгоритмом криптографической защиты данных для крупных информационных систем, локальных вычислительных сетей и автономных компьютеров. Этот алгоритм может реализовываться как аппаратным, так и программным способами, удовлетворяет всем криптографическим требованиям, сложившимся в мировой практике, и, как следствие, позволяет осуществлять криптографическую защиту любой информации, независимо от степени ее секретности.

В алгоритме ГОСТ 28147 ─ 89 в отличие от алгоритма DES используется 256-разрядный ключ, представляемый в виде восьми 32-разрядных чисел. Расшифровываются данные с помощью того же ключа, посредством которого они были зашифрованы. Алгоритм ГОСТ 28147 ─ 89 полностью удовлетворяет всем требованиям криптографии и обладает теми же достоинствами, что и другие алгоритмы (например DES), но лишен их недостатков. Он позволяет обнаруживать как случайные, так и умышленные модификации зашифрованной информации. Крупный недостаток этого алгоритма ─ большая сложность его программной реализации и низкая скорость работы.

Из алгоритмов шифрования, разработанных в последнее время, большой интерес представляет алгоритм RC6 фирмы RSA Data Security. Этот алгоритм обладает следующими свойствами:

· адаптивностью для аппаратных средств и программного обеспечения, что означает использование в нем только примитивных вычислительных операций, обычно присутствующих на типичных микропроцессорах;

· быстротой, т.е. в базисных вычислительных операциях операторы работают на полных словах данных;

· адаптивностью на процессоры различных длин слова. Число w бит в слове ─ параметр алгоритма;

· наличием параметра, отвечающего за "степень перемешивания", т.е. число раундов (итераций до 255). Пользователь может явно выбирать между более высоким быстродействием и более высоким перемешиванием;

· низким требованием к памяти, что позволяет реализовывать алгоритм на устройствах с ограниченной памятью;

· использованием циклических сдвигов, зависимых от данных, с "переменным" числом.

· простотой и легкостью выполнения.

Алгоритм RC6 работает на четырех модулях w-бит слов и использует только четыре примитивных операции (и их инверсии), длина ключа до 2040 бит (255 байт). Алгоритм открыт для публикаций и полностью документирован, т.е. процедуры шифрования и расшифровывания "прозрачны" для пользователя.

2. Алгоритмы с обратным ключом - асимметричные алгоритмы шифрования. Эти алгоритмы называемые также системами с открытым ключом, являются перспективными системами криптографической защиты. Их суть состоит в том, что ключ, используемый для шифрования, отличен от ключа расшифровывания. При этом ключ шифрования не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа шифрования невозможно. Для расшифровывания используется специальный секретный ключ. При этом знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Суть криптографических систем с открытым ключом сводится к тому, что в них используются так называемые необратимые функции (иногда их называют односторонними или однонаправленными), которые характеризуются следующим свойством: для данного исходного значения с помощью некоторой известной функции довольно легко вычислить результат, но рассчитать по этому результату исходное значение чрезвычайно сложно.

Известно несколько криптосистем с открытым ключом, например схема Т. Эль-Гамаля (T. El Gamal), в которой используется идея криптосистемы, предложенная У. Диффи (W. Diffie) и М. Э. Хеллманом (M. E. Hellman), криптосистема RSA и др.

Наиболее разработана система RSA, предложенная в 1978 г. Алгоритм RSA назван по первым буквам фамилий его авторов: Р. Л. Райвеста (R. L. Rivest), А. Шамира (A. Shamir) и Л. Адлемана (L. Adleman). RSA ─ это система коллективного пользования, в которой каждый из пользователей имеет свои ключи шифрования и расшифровывания данных, причем секретен только ключ расшифровывания.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации. Существует еще одна область применения этого алгоритма ─ цифровые подписи, подтверждающие подлинность передаваемых документов и сообщений.

Асимметричные криптосистемы считаются перспективными, так как в них не используется передача ключей другим пользователям и они легко реализуются как аппаратным, так и программным способами.

Однако системы типа RSA имеют свои недостатки. Они работают значительно медленнее, чем классические, и требуют длины ключа порядка 300-600 бит. Поэтому все их достоинства могут быть сведены на нет низкой скоростью их работы. Кроме того, для ряда функций уже найдены алгоритмы инвертирования, т.е. доказано, что они не являются необратимыми. Для функций, используемых в системе RSA, такие алгоритмы не найдены, но нет и строгого доказательства необратимости используемых функций.

Проектируемая надежная криптографическая система должна удовлетворять таким требованиям:

· процедуры шифрования и расшифровывания должны быть "прозрачны" для пользователя;

· дешифрование закрытой информации должно быть максимально затруднено;

· содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма;

· надежность криптозащиты не должна зависеть от содержания в секрете самого алгоритма шифрования (примерами этого являются как алгоритм DES, так и алгоритм ГОСТ 28147 ─ 89).

Стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Криптографические системы также помогают решить проблему аутентификации (установления подлинности) принятой информации, поскольку подслушивающее лицо, пассивным образом перехватывающее сообщение, будет иметь дело только с зашифрованным текстом.

Механизм обеспечения целостности данных применяется как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но недостаточным условием целостности потока. Целостность блока 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.

Защита от несанкционированного копирования ценной компьютерной информации является самостоятельным видом защиты имущественных прав, ориентированных на проблему защиты интеллектуальной собственности, воплощенной в виде 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, и т.д.), которая приводит исполняемый код защищаемой базы данных в состояние, препятствующее его выполнению на "чужих" машинах.

Для повышения защищенности применяются дополнительные аппаратные блоки (ключи), подключаемые к разъему принтера или системной шине ПЭВМ.

Необходимо иметь в виду, что подлежащие защите сведения могут быть получены "противником" не только за счет осуществления "проникновения" к ЭВМ, которые с достаточной степенью надежности могут быть предотвращены (например, все данные хранятся в зашифрованном виде), но и за счет побочных электромагнитных излучений и наводок на цепи питания и заземления ЭВМ, а также каналы связи.

Все без исключения электронные устройства, блоки и узлы ЭВМ в той или иной мере имеют излучение, причем подобные побочные сигналы могут быть достаточно мощными и могут распространяться на расстояния от нескольких метров до нескольких километров. При этом наибольшую опасность представляет

получение "противником" информации о ключах. Восстановив ключ, можно предпринять ряд успешных действий по овладению зашифрованными данными, которые, как правило, охраняются менее тщательно, чем соответствующая открытая информация.

С этой точки зрения выгодно отличаются аппаратные и программно-аппаратные средства защиты от несанкционированного доступа, для которых побочные сигналы о ключевой информации существенно ниже, чем для чисто программных реализаций