**Введение**

В последнее время все чаще стал встречаться термин – «информационное общество». С точки зрения анализа изменения производительных сил и производственных отношений, «информационное общество» может быть определено как общество, в котором основным предметом труда большей части людей являются информация и знания, а орудием труда - информационные технологии. Информационные технологии, основанные на новейших достижениях электронно-вычислительной техники, которые получили название новых информационных технологий (НИТ), находят все большее применение в различных сферах деятельности. Новые информационные технологии создают новое информационное пространство и открывают совершенно новые, ранее неизвестные и недоступные возможности, которые коренным образом меняют представления о существовавших ранее технологиях получения и обработки информации. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Все больше и больше отраслей человеческой деятельности становятся настолько сильно пронизаны этими новыми информационными технологиями, насколько и зависимы от них. Предоставляя огромные возможности, информационные технологии, вместе с тем, несут в себе и большую опасность, создавая совершенно новую, мало изученную область для возможных угроз, реализация которых может приводить к непредсказуемым и даже катастрофическим последствиям. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. Сбой в информационных технологиях применяемых в управлении атомными станциями или химическими предприятиями может привести к экологическим катастрофам. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать. Ущерб от возможной реализации угроз можно свести к минимуму, только приняв меры, которые способствуют обеспечению информации. Под угрозой безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы подразделяются на случайные (непреднамеренные) и умышленные. Источником первых могут быть ошибочные действия пользователей, выход из строя аппаратных средств и другие.

Умышленные угрозы подразделяются на пассивные и активные. Пассивные угрозы не разрушают информационные ресурсы. Их задача - несанкционированно получить информацию. Активные угрозы преследуют цель нарушать нормальный процесс функционирования систем обработки информации, путем разрушения или радиоэлектронного подавления линий, сетей, вывода из строя компьютеров, искажения баз данных и т.д. Источниками активных угроз могут быть непосредственные действия физических лиц, программные вирусы и т.д.

1. **Электронная документация: определение и особенности**

Электронные документы можно разделить на два основных типа: неформализованные (произвольные) и служебные (официальные) Неформализованный электронный документ — это любое сообщение, записка, текст, записанный на машинном носителе. Под служебным электронным документом понимается записанное на машинном носителе электронное сообщение, реквизиты которого оформлены в соответствии с нормативными требованиями.

Под электронным документом (ЭД) следует понимать структурированный информационный объект, в соответствие которому может быть поставлена совокупность файлов, хранящихся на накопителе компьютера. Необходимым признаком ЭД является «регистрационная карточка», состоящая из реквизитов документа, содержащих перечень необходимых данных о нем. Согласно законодательству, электронным является документ, в котором информация представлена в электронно-цифровой форме.

Электронные документы по сравнению с бумажными обладают следующими преимуществами:

- более низкая стоимость и время передачи электронного документа из одного места в другое;

- более низкая стоимость и время тиражирования ЭД;

- более низкая стоимость архивного хранения ЭД;

- возможность контекстного поиска;

- новые возможности защиты документов;

- упрощение подготовки ЭД в сочетании с широкими возможностями;

- принципиально новые возможности представления ЭД. Документ может иметь динамическое содержание (например, аудио-, видеовставки).

Основные принципы построения системы электронного документооборота:

- соответствие требованиям стандартов на формы и системы документации;

- распределенность;

- масштабируемость;

- модульность;

- открытость;

- переносимость на другие аппаратные платформы.

Основными функциями системы электронного документооборота являются:

- регистрация документов;

- контроль исполнения документов;

- создание справочников и работа с ними;

- контроль движения бумажного и электронного документа, ведение истории работы с документами;

- создание и редактирование реквизитов документов;

- формирование отчетов по документообороту предприятия;

- импорт документов из файловой системы и Интернета; </P< index>

создание документа прямо из системы на основе шаблона (прямая интеграция);

- работа с версиями документа, сложными многокомпонентными и многоформатными документами, вложениями;

- электронное распространение документов;

- работа с документами в папках;

- получение документов посредством сканирования и распознавания.

- уменьшением затрат на доступ к информации и обработку документов.

Системы документооборота обычно внедряются, чтобы решать определенные задачи, стоящие перед организацией. К таким задачам можно отнести следующие:

- обеспечение более эффективного управления за счет автоматического контроля выполнения, прозрачности деятельности всей организации на всехх уровнях;

- поддержка эффективного накопления, управления и доступа к информации и знаниям;

- исключение бумажных документов из внутреннего оборота предприятия;

исключение необходимости или существенное упрощение и удешев ление хранения бумажных документов за счет наличия оперативного электронного архива;

- экономия ресурсов за счет сокращения издержек на управление по токами документов в организации;

- поддержка системы контроля качества, соответствующей международным нормам;

- обеспечение кадровой гибкости за счет большей формализации деятельности каждого сотрудника и возможности хранения всей предыстории его деятельности;

- протоколирование деятельности предприятия в целом (внутренние служебные расследования, анализ деятельности подразделений, выявление «горячих точек» в деятельности);

- оптимизация бизнес-процессов и автоматизация механизма их выполнения и контроля.

1. **Защита электронных документов**

По мере своего развития любая организация сталкивается с необходимостью введения электронного документооборота. Естественно, электронные документы имеют различную степень конфиденциальности и могут содержать сведения от полностью открытых до являющихся коммерческой тайной самой организации или ее партнеров. Кроме того, возникает проблема достоверности электронных документов, полученных, скажем, по электронной почте, поскольку подписать такой документ обычной подписью и удостоверить печатью невозможно. Вывод: электронный документооборот должен сопровождаться различными организационно-техническими мерами, позволяющими защитить передаваемые по компьютерным сетям электронные документы, как от несанкционированного прочтения, так и от случайной или преднамеренной модификации.  
Защита электронного документооборота актуальна для различных задач: защита документооборота промышленных предприятий, обеспечение конфиденциальности информации в медицинских учреждениях, защита электронных документов, обеспечивающих функционирование платежной сети в банковской сфере.  
Наиболее остро вопрос защиты документооборота стоит для организаций, имеющих территориально-распределенную структуру. Такие организации могут иметь несколько локальных вычислительных сетей (ЛВС), расположенных в разных местах, в том числе в различных регионах России, и вынуждены использовать для передачи информации различные неконтролируемые глобальные вычислительные сети (ГВС) общего пользования, например, сеть Internet.  
В данной статье описаны методы защиты передаваемых в ГВС электронных документов. Кроме того, изложенные ниже рекомендации будут полезны и для организаций, имеющих единственную ЛВС, поскольку применяемые методы защиты не будут являться избыточными и в этом случае.

При электронном документообороте возникают различные угрозы со стороны пользователей ГВС, которые можно разделить на две основные категории:

* + угрозы конфиденциальности информации,
  + угрозы целостности информации.

Наиболее надежным средством обеспечения конфиденциальности информации является шифрование.            Шифрование - это процесс преобразования открытых данных в закрытые по определенному криптографическому алгоритму с использованием секретного ключевого элемента – ключа шифрования.

В данной статье рассматривается симметричное шифрование. Данный термин означает, что для зашифрования и последующего расшифрования информации используется одно и то же криптографическое преобразование.   
Секретный элемент криптографического преобразования – ключ шифрования – может храниться, например, в файле на дискете, или на каком-либо другом ключевом носителе, что рассмотрено в данной статье ниже. Необходимо, чтобы все пользователи, предполагающие обмениваться зашифрованными документами, получили определенный набор ключей шифрования, что позволило бы получателям расшифровывать документы, предварительно зашифрованные отправителями.  
Простейший случай – все абоненты компьютерной сети организации получают один и тот же секретный ключ шифрования. Как и все простое, такая схема имеет ряд недостатков:

* + Все абоненты сети имеют один и тот же ключ шифрования. Таким образом, любые зашифрованные этим ключом документы могут быть расшифрованы любым абонентом сети, т. е., невозможно отправить некий документ какому-либо абоненту лично.
  + При компрометации ключа шифрования (утере, хищении и т. д.) под угрозой нарушения конфиденциальности окажется весь документооборот, ключи шифрования придется срочно менять. Если же, например, факт компрометации ключа шифрования обнаружен не сразу, останется только догадываться, сколько документов (и какой важности) успел прочитать злоумышленник.
  + Такие ключи необходимо передавать «из рук в руки», т. е., невозможно, например, переслать по электронной почте, что неудобно.

Первые два недостатка устраняются, например, при использовании ключевой системы типа «полная матрица».

Такая «полная матрица» содержит матрицу ключей для связи «каждый с каждым» (ключи парной связи), т. е., матрица содержит ключи для связи абонентов попарно. Это означает, что каждый из ключей матрицы доступен только двум из абонентов сети. Каждый абонент снабжается «сетевым набором» – строкой ключей из данной матрицы, предназначенных для его связи с остальными абонентами сети. Таким образом, существует возможность посылать документы кому-либо, зашифровав их на ключе «для двоих», что делает документ недоступным для остальных. Проще и с компрометацией – при утере какого-либо ключа стоит бояться лишь за те документы, которые посылались владельцами конкретного ключа друг другу. Соответственно, новый ключ взамен скомпрометированного необходимо заменить только у двух абонентов, а не у всех.  
И снова о недостатках:

* + При необходимости послать один и тот же документ нескольким абонентам в зашифрованном виде, его следует зашифровывать несколько раз (по числу адресатов), а потом еще и не перепутать, кому какой из зашифрованных файлов отсылать.
  + Остается необходимость передачи ключей «из рук в руки».

Схема шифрования документов, позволяющая создавать один зашифрованный файл для передачи нескольким абонентам с использованием ключей парной связи, рассмотрена ниже.

Проблема передачи ключей решается путем применения схемы открытого распределения ключей. Это означает, что с помощью определенного алгоритма ключ шифрования «делится» на секретную и открытую части. Секретная часть, называемая «секретным ключом», хранится у его владельца, а открытая часть («открытый ключ») передается всем остальным абонентам сети. Таким образом, каждый абонент сети имеет в своем распоряжении свой собственный секретный ключ и набор открытых ключей всех остальных абонентов. С помощью своего секретного ключа и открытого ключа абонента-адресата абонент-отправитель вычисляет ключ парной связи, с помощью которого зашифровывает документы, предназначенные данному получателю. Получатель же, с помощью своего секретного ключа и имеющегося у него открытого ключа отправителя, вычисляет тот же ключ парной связи, с помощью которого может эти документы расшифровать.

Таким образом, путем использования схемы с открытым распределением ключей достигаются те же положительные моменты, что и при использовании схемы «полная матрица», но также и нейтрализуется недостаток – проблема распределения ключей. Открытые ключи можно распределять свободно по открытым каналам связи, поскольку, даже имея полный набор открытых ключей всех абонентов сети, злоумышленник не сможет расшифровать конфиденциальный документ, поскольку он предназначен конкретному адресату. То же самое относится и к другим абонентам сети, поскольку документ зашифрован на ключе парной связи, который могут вычислить только отправитель и получатель – у остальных попросту не хватает исходных данных для вычисления ключа парной связи.  
Ключ парной связи может вычисляться, например, с помощью алгоритма Диффи-Хеллмана. Данный алгоритм (а также множество других) подробно описан в вышедшей в 1999 году в издательстве «Радио и Связь» книге Ю.В.Романца, П.А.Тимофеева и В.Ф.Шаньгина «Защита информации в компьютерных системах и сетях». Тем, кому наиболее интересна тема предлагаемой статьи, особенно рекомендую прочитать данную книгу.

Еще одно существенное достоинство открытого распределения ключей состоит в том, что одни и те же ключи могут быть использованы и для шифрования документов, и для электронной подписи. При использовании других ключевых схем это недостижимо.

Электронная цифровая подпись (ЭЦП) – средство, позволяющее на основе криптографических методов установить авторство и целостность электронного документа.

Секретный ключ (СК) генерируется абонентом сети. ЭЦП формируется на основе СК и вычисленного с помощью хэш-функции значения хэша документа. Хэш представляет собой некоторое значение, однозначно соответствующее содержимому документа-файла. При изменении хотя бы одного символа в документе, хэш документа изменится. Подобрать же изменения в документе таким образом, чтобы хэш документа не изменился, при использовании современных алгоритмов ЭЦП (например, ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94) попросту невозможно.  
СК может быть зашифрован на пароле. Открытый ключ (ОК) вычисляется как значение некоторой функции из СК и используется для проверки ЭЦП. ОК может свободно распространяться по открытым каналам связи, таким образом, ОК должен быть передан всем абонентам сети, с которыми планируется обмен защищенной информацией. При проверке ЭЦП вычисляется значение хэша документа; таким образом, любые изменения документа приведут к другому значению хэша, и вычисленная ЭЦП измененного документа не совпадет с переданной, что явится сигналом нарушения его целостности.

Как уже было сказано, для шифрования и ЭЦП может быть использована одна и та же пара ключей абонента.

Комплексный метод защиты

Естественно, для защиты и конфиденциальности, и целостности информации следует использовать в комплексе шифрование и ЭЦП, что также можно совместить с каким-либо дополнительным сервисом, например, сжатием информации (архивацией). В качестве примера таких систем следует привести специализированный архиватор электронных документов Crypton ArcMail, предлагаемый фирмой «АНКАД». Алгоритм создания специализированного архива (архива для передачи по сети) приведен на рис. 5.  
Создаваемый таким образом файл-архив можно передавать по сети без каких-либо опасений. При создании архива исходные файлы подписываются на секретном ключе абонента сети, после чего файлы сжимаются и получаемый в результате сжатия архив шифруется на случайном временном ключе. Абоненты, которым предназначается архив, могут расшифровать его с помощью записанного в архив зашифрованного временного ключа. Временный ключ зашифровывается на парно-связном ключе, вычисляемом по алгоритму Диффи-Хеллмана из СК отправителя и открытого ключа ЭЦП (ОК) абонента-адресата. Таким образом, достигаются следующие цели:

* + Передаваемые электронные документы снабжаются кодом подтверждения достоверности – ЭЦП, который защищает их от нарушения целостности или подмены.
  + Документы передаются в защищенном виде, что обеспечивает их конфиденциальность.
  + Абоненты-адресаты могут расшифровать документы, используя свой СК и ОК отправителя.
  + Абоненты сети, которым не предназначается данный архив, не могут прочитать его содержимое, поскольку не имеют временного ключа и не могут его вычислить.
  + Дополнительный сервис – уменьшение объема информации, обусловленное архивацией.

Проблемы распределения и хранения ключей

При использовании ЭЦП и описанного выше метода комплексной защиты электронных документов, применяемые в алгоритме ключевые элементы должны распределяться следующим образом: СК должен находиться у его владельца, парный ему ОК должен быть передан владельцем всем абонентам сети, с которыми он хочет обмениваться защищенной информацией.

ОК не являются секретными, но существует возможность их подмены. Например, возможна ситуация, что у злоумышленника есть доступ на компьютер, на котором абонент №1 хранит открытые ключи. Злоумышленник считывает интересующие его сведения (ФИО, должность, …) из ОК, например, абонента №2, после чего генерирует где-либо СК и ОК с такими данными и заменяет на компьютере абонента №1 ОК абонента №2 на фиктивный. После чего злоумышленник может подписать любой документ своим СК с данными абонента №2 и переслать его абоненту №1. При проверке ЭЦП такого документа будет выдано сообщение типа «Подпись лица (ФИО, должность, …) верна», что, мягко говоря, введет в заблуждение абонента №1. Таким образом, очевидно, что необходима защита и открытых ключей. Такую защиту можно обеспечить несколькими способами.

Использование персональной дискеты.

Собственный СК и открытые ключи других абонентов могут быть записаны на персональную дискету, доступ к которой должен быть только у ее владельца. Однако, при большом количестве абонентов сети и большом потоке документов такой вариант нецелесообразен, так как замедляется обработка документов.

Смысл данного варианта состоит в использовании ключей-сертификатов. Предположительно, существует некий сертификационный центр (СЦ), в котором на специальном ключе (ключе-сертификате) подписывается открытый ключ абонента сети перед передачей его другим абонентам. Открытый ключ-сертификат должен храниться у всех абонентов сети для проверки целостности всех используемых в сети ОК. При таком варианте рекомендуется при проверке ЭЦП какого-либо документа автоматически проверять подпись соответствующего ОК (что обычно и делается автоматически программными средствами).

Таким образом, сами ОК могут храниться в открытом виде, а персональная дискета, помимо СК владельца, должна содержать еще и ключ-сертификат.  
СЦ рекомендуется совместить с центром генерации ключей (ЦГК). В этом случае, это будет выделенное рабочее место, используемое как для генерации ключей абонентов, так и для их сертификации и рассылки абонентам. Даже в случае генерации ключей непосредственно абонентами на местах, СЦ можно использовать для рассылки абонентам заверенных открытых ключей.

Данная схема особенно рекомендуется при организации электронного документооборота между несколькими юридическими лицами.

Порядок распределения ключей состоит в следующем:

* + Абонент создает персональную дискету с собственными ключами. Секретный ключ закрывается паролем.
  + Для собственного ОК формируется подпись на собственном СК. ОК записывается на дискету для передачи.
  + Создается юридический документ на бумаге (например, письмо), в котором указываются: данные о владельце (Ф.И.О., должность, место работы), сам ОК (распечатка в шестнадцатеричном виде), полномочия владельца (перечень документов, которые уполномочен удостоверять владелец открытого ключа). Данный документ должен быть оформлен таким образом, чтобы иметь юридическую силу в случае возникновения спорных вопросов о принадлежности подписи и полномочиях владельца. Если в письме не установлено полномочий, то они определяются по должности и месту работы.
  + Данный документ вместе с ОК пересылается в СЦ.
  + СЦ проверяет юридическую силу полученного документа, а также идентичность ОК на дискете и в документе.

В ответ абонент получает:

* + - сертифицированные ОК всех абонентов (в том числе, и свой),
    - сертифицированные файлы с полномочиями владельцев ОК,
    - ключ-сертификат, как в виде файла, так и в виде юридического документа.
    - Владелец проверяет истинность ключа-сертификата, а также подписи всех полученных им ОК и файлов. При успешной проверке ОК записываются в соответствующий каталог, а ключ-сертификат – на персональную дискету.

При такой организации работ абонент формирует ЭЦП документов и не заботится об обмене открытыми ключами и полномочиями. Однако большая нагрузка по рассылке ОК и полномочий ложится на СЦ. Для пресечения фальсификации ОК сертификационный центр должен использовать организационные меры, о которых будет сказано ниже. В том случае, если у абонента сети остаются какие-либо сомнения относительно конкретного ОК, он может запросить распечатку ОК и полномочия напрямую у его владельца.  
Можно оставить за СЦ только сертификацию ключей и полномочий, освободив его от рассылки ОК. В этом случае, при первой посылке в любой адрес документов, абоненту необходимо послать по этому адресу также сертифицированные ОК и полномочия.

В общем случае, сертификационных центров может быть несколько. Пользователь может сертифицировать свой ОК в разных, не связанных друг с другом, СЦ. Кроме того, СЦ могут быть связаны в сеть с любой необходимой иерархической организацией для обмена либо только ключами-сертификатами, либо дополнительно еще и открытыми ключами. Тогда пользователю достаточно сертифицировать ОК только в одном из таких СЦ для обмена информацией с абонентами всех охватываемых СЦ сетей.

При большом количестве абонентов сети рекомендуется использование баз данных (БД) ОК. В этом случае, вместо отдельных ОК, сертификационный центр пересылает абоненту одинаковый для всех абонентов файл БД, содержащий все используемые ОК.

Согласно сказанному выше, персональная дискета должна содержать следующее:

* + СК владельца;
  + открытые ключи-сертификаты по числу сертификационных центров.

В качестве ключа сертификационного центра может быть использован собственный СК абонента; в этом случае, при получении ОК другого абонента, его необходимо подписать. При этом на персональную дискету следует записать свой ОК для проверки целостности ОК других абонентов.

Вместо персональной дискеты может быть использован другой ключевой носитель, например электронная таблетка Touch Memory (TM) или смарт-карта (SC), что иногда предпочтительнее использованию ключевой дискеты, поскольку, например, с SC ключи шифрования могут быть непосредственно загружены в устройство криптографической защиты данных, минуя оперативную память компьютера.

1. Использование систем защиты от несанкционированного доступа (ЗНСД).

Нет необходимости в специальных мерах по защите ключей в том случае, если используется система ЗНСД, блокирующая доступ на компьютер неавторизованных пользователей, либо использующая прозрачное шифрование информации на компьютере абонента.

В том случае, если используются персональные дискеты с централизованной генерацией ключей абонентов, использование систем ЗНСД все же необходимо для защиты ЦГК.

Организационные мероприятия

Следует учесть, что использование любых систем защиты документооборота будет недостаточным без введения организационных мер. К ним можно отнести следующее:

* + Разграничение доступа на рабочие места, как административными мерами (напр., разграничение доступа в помещения), так и с использованием различных систем ЗНСД, что особенно актуально для тех же ЦГК и СЦ.
  + Выделение на предприятии должностного лица (администратора по безопасности), отвечающего за функционирование систем защиты документооборота. Основные функции администратора по безопасности:
  + Разработка и контроль практического осуществления мероприятий по обеспечению безопасного функционирования систем защиты.
  + Периодический контроль целостности систем защиты, состояния охранной сигнализации и соблюдения режима охраны помещений, в которых расположены системы защиты.
  + Периодический контроль журналов операций, автоматически создаваемых программными модулями, входящими в системы защиты.
  + Хранение резервных копий ключевых носителей всех операторов, работающих в системах защиты.
  + Предотвращение получения злоумышленниками ключевых носителей и их тиражирования владельцами. Рекомендуется использовать в качестве ключевых носителей микропроцессорные SC.

# Заключение

Нужно четко представлять себе, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в информационных системах. В то же время можно существенно уменьшить риск потерь при комплексном подходе к вопросам безопасности. Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока специалистами не произведен соответствующий анализ. Анализ должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь и др.) и предоставить информацию для определения подходящих средств защиты – административных, аппаратных, программных и прочих. В России на рынке защитных средств, присутствуют такие продукты как Кобра, Dallas Lock, Secret Net, Аккорд, Криптон и ряд других. Однако обеспечение безопасности информации - дорогое дело. Большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей и потому нерентабельной и неконкурентноспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование, протоколирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Поэтому главное при определении мер и принципов защиты информации это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска с другой..

# СПИСОК ЛИТЕРАТУРЫ

1. П. Зегжда, «Теория и практика. Обеспечение информационной безопасности». - Москва, 1996.
2. “Энциклопедия компьютерных вирусов Евгения Касперского” – электронная версия от 16.10.1999 г.
3. Л.Хофман, «Современные методы защиты информации», - Москва, 1995.
4. Бюллетень лаборатории информационных технологий NIST за май 1999 г. Э. Леннон " Компьютерные атаки: что это такое и как защититься от них"
5. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. - 1994. - N5.
6. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: "Единая Европа", 1994.
7. Громов В.И. Васильев Г.А "Энциклопедия компьютерной безопасности" (электронный сборник 1999 год)
8. Д. Ведеев Защита данных в компьютерных сетях / Открытые системы Москва, 1995, №3,
9. Косарев В.П. и др. Под ред. Косарева В.П. и Еремина Л.В. Компьютерные системы и сети: Учеб. Пособие - М.: Финансы и статистика ,1999г.
10. Баричев С. “Введение в криптографию” - электронный сборник
11. Вьюкова Н.И., Галатенко В.А. “Информационная безопасность систем управления базами данных” 1996 – статья в электронном журнале.