Виды защиты, используемые в автоматизированных информационных системах

Одной из оборотных сторон компьютерных информационных технологий является обострение **проблемы защиты информации.** Данные в компьютерной форме сосредоточивают в физически локальном и небольшом объеме огромные массивы информации, несанкционированный доступ к которой или ее разрушение могут приводить порой к катастрофическим последствиям и ущербу. Возможность быстрого, во многих случаях практически мгновенного, и без следов копирования огромных массивов данных, находящихся в компьютерной форме, в том числе и удаленно расположенных, дополнительно **провоцирует злоумышленников** на несанкционированный доступ к информации, ее несанкционированную модификацию или разрушение.

Вместе с тем теоретическая проработка вопросов обеспечения безопасности информации и их практическая реализация долгое время отставали от уровня развития программной индустрии СУБД, и в коммерческих продуктах средства обеспечения безопасности данных стали появляться лишь в 90-х годах.

Импульсы развития и первые исследования теории и практики обеспечения безопасности данных в компьютерных системах были обусловлены, прежде всего, потребностями военной сферы, где проблема безопасности в целом, и компьютерной безопасности в частности стоят особенно остро. Начало этим процессам было положено исследованиями вопросов защиты компьютерной информации, проведенными в конце 70-х — начале 80-х годов национальным центром компьютерной безопасности (NCSC — National Computer Security Center) Министерства обороны США. Результатом этих исследований явилось издание Министерством обороны США в 1983 г. документа под названием **«Критерии оценки надежных компьютерных систем»,** впоследствии по цвету обложки получившего название **«Оранжевой книги».** Данный документ стал фактически первым стандартом в области создания защищенных компьютерных систем и впоследствии основой организации системы сертификации компьютерных систем по критериям защиты информации.

Подходы к построению и анализу защищенных систем, представленные в «Оранжевой книге», послужили методологической и методической базой для дальнейших исследований в этой сфере. В 1991 г. NCSC был издан новый документ — Интерпретация «Критериев оценки надежных компьютерных систем» в применении к понятию надежной системы управления базой данных, известный под сокращенным названием TDI или «Розовой книги», конкретизирующий и развивающий основные положения «Оранжевой книги» по вопросам создания и оценки защищенных СУБД.

В конце 80-х — начале 90-х годов аналогичные исследования по проблемам компьютерной безопасности были проведены во многих странах и созданы соответствующие национальные стандарты в этой сфере. В нашей стране Государственной технической комиссией при Президенте РФ были разработаны и в 1992 г. опубликованы **«Руководящие документы по защите от несанкционированного доступа к информации»,** определяющие требования, методику и стандарты построения защищенных средств вычислительной техники и автоматизированных систем.

Понятие и модели безопасности данных

Исследования по проблемам защиты компьютерной информации, проведенные в конце 70-х—начале 80-х годов, развитые впоследствии в различных приложениях и закрепленные в соответствующих стандартах, определяют в качестве составных элементов понятия безопасности информации три компонента:

• **конфиденциальность** (защита от несанкционированного доступа);

• **целостность** (защита от несанкционированного изменения информации);

• **доступность** (защита от несанкционированного удержания информации и ресурсов, защита от разрушения, защита работоспособности).

Составляющим безопасности информации противостоят соответствующие угрозы. Под угрозой безопасности информации понимается осуществляемое или потенциально осуществимое воздействие на компьютерную систему, которое прямо или косвенно может нанести ущерб безопасности информации. Угрозы реализуют или пытаются реализовать **нарушители** информационной безопасности.

Формализованное описание или представление комплекса возможностей нарушителя по реализации тех или иных угроз безопасности информации называют **моделью нарушителя (злоумышленника).**

Качественное описание комплекса организационно-технологических и программно-технических мер по обеспечению защищенности информации в компьютерной системе (АИС) называют **политикой безопасности.** Формальное (математическое, алгоритмическое, схемотехническое) выражение и формулирование политики безопасности называют **моделью безопасности.**

Модель безопасности включает:

• модель компьютерной (информационной) системы;

• критерии, принципы, ограничения и целевые функции защищенности информации от угроз;

• формализованные правила, ограничения, алгоритмы, схемы и механизмы безопасного функционирования системы.

В основе большинства моделей безопасности лежит **субъектно-объектная модель** компьютерных систем, в том числе и баз данных как ядра автоматизированных информационных систем. База данных АИС разделяется на **субъекты базы данных** (активные сущности), **объекты базы данных** (пассивные сущности) и порождаемые действиями субъектов **процессы над объектами** (см. рис. 1).

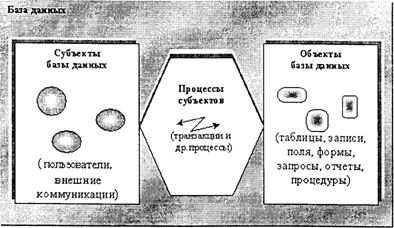


Рис. 1. База данных АИС в моделях безопасности данных

Определяются два основополагающих принципа безопасности функционирования информационных систем:

**• персонализация** (идентификация) и **аутентификация** (подтверждение подлинности) всех субъектов и их процессов по отношению к объектам;

**• разграничение полномочий субъектов** по отношению к объектам и обязательная проверка полномочий любых процессов над данными.

Соответственно в структуре ядра СУБД выделяется дополнительный компонент, называемый **монитором** (сервером, менеджером, ядром) **безопасности** (Trusted Computing Base— ТСВ), который реализует определенную **политику безопасности** во всех процессах обработки данных. Если в схемотехническом аспекте компьютерную систему представить как совокупность ядра, включающего компоненты представления данных и доступа (манипулирования) к данным, а также надстройки, которая реализует интерфейсные и прикладные функции, то роль и место монитора безопасности можно проиллюстрировать схемой, приведенной на рис. 2.

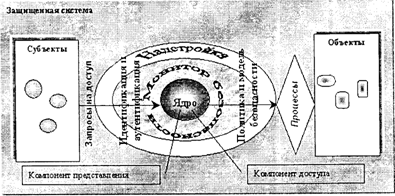
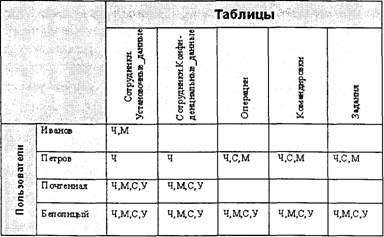


Рис. 2. Схематический аспект защиты информации в компьютерных системах

В узком смысле политика безопасности, реализуемая монитором безопасности компьютерной системы, собственно и определяет модель безопасности (вторая и третья компоненты).

Простейшая **(одноуровневая)** модель безопасности данных строится на основе **дискреционного** (избирательного)**принципа разграничения доступа,** при котором доступ к объектам осуществляется на основе **множества разрешенных отношений доступа** в виде троек — «субъект доступа – тип доступа – объект доступа». Наглядным и распространенным способом формализованного представления дискреционного доступа является матрица доступа, устанавливающая перечень пользователей (субъектов) и перечень разрешенных операций (процессов) по отношению к каждому объекту базы данных (таблицы, запросы, формы, отчеты). На рис. 3 приведен пример, иллюстрирующий матрицу доступа.



Обозначения: Ч – чтение; М – модификация; С – создание; У – удаление (записей)

Рис. 3. Модель безопасности на основе матрицы доступа (дискреционный принцип разграничения доступа)

Важным аспектом моделей безопасности является управление доступом. Существует два подхода:

• добровольное управление доступом;

• принудительное управление доступом.

При **добровольном управлении доступом** вводится так называемое **владение объектами.** Как правило, владельцами объектов являются те субъекты базы данных, процессы которых создали соответствующие объекты. Добровольное управление доступом заключается в том, что права на доступ к объектам определяют их владельцы. Иначе говоря, соответствующие ячейки матрицы доступа заполняются теми субъектами (пользователями), которым принадлежат права владения над соответствующими объектами базы данных. В большинстве систем права владения объектами могут передаваться. В результате при добровольном управлении доступом реализуется полностью децентрализованный принцип организации и управления процессом разграничения доступа.

Такой подход обеспечивает гибкость настраивания системы разграничения доступа в базе данных на конкретную совокупность пользователей и ресурсов, но затрудняет общий контроль и аудит состояния безопасности данных в системе.

**Принудительный подход к управлению доступом** предусматривает введение единого централизованного **администрирования доступом.** В базе данных выделяется специальный доверенный субъект (администратор), который (и только он), собственно, и определяет разрешения на доступ всех остальных субъектов к объектам базы данных. Иначе говоря, заполнять и изменять ячейки матрицы доступа может только администратор системы.

Принудительный способ обеспечивает более жесткое централизованное управление доступом. Вместе с тем он является менее гибким и менее точным в плане настройки системы разграничения доступа на потребности и полномочия пользователей, так как наиболее полное представление о содержимом и конфиденциальности объектов (ресурсов) имеют, соответственно, их владельцы.

На практике может применяться комбинированный способ управления доступом, когда определенная часть полномочий на доступ к объектам устанавливается администратором, а другая часть владельцами объектов.

Исследования различных подходов к обеспечению информационной безопасности в традиционных (некомпьютерных) сферах и технологиях показали, что одноуровневой модели безопасности данных недостаточно для адекватного отражения реальных производственных и организационных схем. В частности традиционные подходы используют **категорирование информационных ресурсов по уровню конфиденциальности** (совершенно секретно — СС, секретно — С, конфиденциально — К, и т. п.). Соответственно субъекты доступа к ним (сотрудники) также категорируются по соответствующим уровням доверия, получая так называемого **допуска** (допуск степени 1, допуск степени 2 и т. д.). Понятие допуска определяет **мандатный (полномочный) принцип разграничения доступа к информации.** В соответствии с мандатным принципом работник, обладающий допуском степени «1», имеет право работать с любой информацией уровня «СС», «С» и «К». Работник с допуском «2» соответственно имеет право работы с любой информацией уровня «С» и «К». Работник с допуском «3» имеет право работать с любой информацией только уровня «К».

Мандатный принцип построения системы разграничения доступа в СУБД реализует **многоуровневую модель безопасности данных,** называемую еще моделью Белл — ЛаПадула (по имени ее авторов — американских специалистов Д. Белла и Л. ЛаПадула), которая иллюстрируется схемой, приведенной на рис. 4.

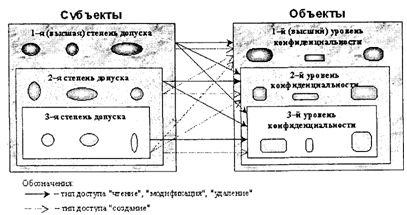


Рис. 4. Модель безопасности данных Белл — ЛаПадула (мандатный принцип разграничения доступа)

В модели Белл — ЛаПадула объекты и субъекты категорируются по иерархическому мандатному принципу доступы. Субъект, имеющий допуск 1-й (высшей) степени, получает доступ к объектам 1-го (высшего) уровня конфиденциальности и автоматически ко всем объектам более низких уровней конфиденциальности (т. е. к объектам 2-го и 3-го уровней). Соответственно, субъект со 2-й степенью допуска имеет доступ ко всем объектам 2-го и 3-го уровней конфиденциальности, и т. д.

В модели Белл — ЛаПадула устанавливаются и поддерживаются два основных ограничения политики безопасности:

• запрет чтения вверх (no read up — NRU);

• запрет записи вниз (no write down — NWD).

Ограничение NRU является логическим следствием мандатного принципа разграничения доступа, запрещая субъектам читать данные из объектов более высокой степени конфиденциальности, чем позволяет их допуск.

Ограничение NWD предотвращает перенос (утечку) конфиденциальной информации путем ее копирования из объектов с высоким уровнем конфиденциальности в неконфиденциальные объекты или в объекты с меньшим уровнем конфиденциальности.

Ограничения NRU и NWD приводят к тому, что по разным типам доступа («чтение», «создание», удаление», «запись») в модели Белл—ЛаПадула устанавливается разный порядок доступа конкретного субъекта к объектам. В частности, в схеме, приведенной на рис. 7.4, может показаться странным, что по типу доступа «создание» субъект (процесс) с допуском степени 3 (низшей) имеет возможность создавать объекты (записи) в объектах более высокого уровня конфиденциальности. Такой подход, тем не менее, отражает реальные жизненные ситуации, когда работники, к примеру, кадрового подразделения могут заполнять формализованные карточки на новых сотрудников, направляя их в специальную картотеку личных данных сотрудников организации и порождая первые документы личных дел новых сотрудников, но не имеют при этом собственно самого доступа к этой картотеке по другим типам операций (чтение, удаление, изменение).

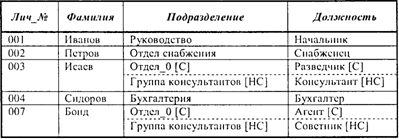
Мандатный принцип разграничения доступа, опять-таки исходя из дополнительных способов разграничения доступа к конфиденциальной информации, наработанных в «бумажных» технологиях, в частности в военной сфере, может дополняться элементами **функционально-зонального принципа разграничения доступа.** В соответствии с функционально-зональным принципом, защищаемые сведения, помимо категории конфиденциальности, получают признак функциональной тематики (зоны), например сведения по артиллерии, сведения по авиации, и т. д. Соответственно, каждый работник, имеющий определенный допуск к конфиденциальным сведениям, еще по своим функциональным обязанностям имеет определенный профиль деятельности, который предоставляет допуск или уточняет сферу допуска к категорированным сведениям только соответствующей тематики. Такой подход предоставляет более гибкие и точные возможности организации работы с конфиденциальными сведениями и в СУБД реализуется через технику профилей и ролей пользователей.

На практике в реальных политиках мониторов безопасности баз данных чаще всего применяется дискреционный принцип с принудительным управлением доступом, «усиливаемый» элементами мандатного принципа в сочетании с добровольным управлением доступом (допуска субъектов устанавливает и изменяет только администратор, уровень конфиденциальности объектов устанавливают и изменяют только владельцы). В распределенных СУБД могут также применяться элементы функционально-зонального разграничения доступа в виде жесткой привязки объектов и субъектов к определенным устройствам, а также выделении специальных зон, областей со «своей» политикой безопасности.

При реализации политик и моделей безопасности данных в фактографических АИС на основе реляционных СУБД возникают специфические проблемы разграничения доступа на уровне отдельных полей таблиц. Эти проблемы связаны с отсутствием в реляционной модели типов полей с множественным (многозначным) характером данных.

Поясним суть подобных проблем следующим образом. Предположим, в базе данных имеется таблица с записями по сотрудникам с полями «Лич\_№», «Фамилия», «Подразделение», «Должность». Предположим также, что в структуре организации имеется засекреченное подразделение «Отдел\_0», известное для всех непосвященных под названием «Группа консультантов». Соответственно поля «Подразделение», «Должность» для записей сотрудников этого подразделения будут иметь двойные значения — одно истинное (секретное), другое для прикрытия (легенда). Записи таблицы «Сотрудники» в этом случае могут иметь вид:

Таблица 1



В таблице знаком [С] обозначены секретные значения, знаком [НС] несекретные значения соответствующих полей. Как видно из приведенной таблицы, требования первой нормальной формы в таких случаях нарушаются.

Более того, даже если взять более простой случай, когда конфиденциальные данные по некоторым полям пользователям, не имеющим соответствующей степени допуска, просто не показываются, т.е. такой пользователь «видит» в секретных полях некоторых записей просто пустые значения, то тем не менее возникают **косвенные каналы нарушения конфиденциальности.** Так как на самом деле в соответствующем поле данные имеются, то при попытке записи в эти поля неуполномоченный на это пользователь получит отказ, и, тем самым, «почувствует» что-то неладное, подозрительное, скажем, в отношении записи сотрудника с личным номером 007. Это и есть косвенный канал.

В более общем виде под косвенным каналом нарушения конфиденциальности подразумевается механизм, посредством которого субъект, имеющий высокий уровень благонадежности, может предоставить определенные аспекты конфиденциальной информации субъектам, степень допуска которых ниже уровня конфиденциальности этой информации.

В определенной степени проблему многозначности и косвенных каналов можно решать через нормализацию соответствующих таблиц, разбивая их на связанные таблицы, уровень конфиденциальности которых, или конфиденциальности части записей которых, будет различным.

Другие подходы основываются на расширении реляционной модели в сторону многозначности и допущения существования в таблицах кортежей с одинаковыми значениями ключевых полей.

Технологические аспекты защиты информации

Практическая реализация политик и моделей безопасности, а также аксиоматических принципов построения и функционирования защищенных информационных систем обусловливает необходимость решения ряда программно-технологических задач, которые можно сгруппировать по следующим направлениям:

• технологии идентификации и аутентификации;

• языки безопасности баз данных;

• технологии обеспечения безопасности повторного использования объектов;

• технологии надежного проектирования и администрирования.

Идентификация и аутентификация

Технологии идентификации и аутентификации являются обязательным элементом защищенных систем, так как обеспечивают аксиоматический принцип персонализации субъектов и, тем самым, реализуют первый (исходный) программно-технический рубеж защиты информации в компьютерных системах.

Под **идентификацией** понимается различение субъектов, объектов, процессов по их образам, выражаемым именами.

Под аутентификацией понимается проверка и подтверждение подлинности образа идентифицированного субъекта, объекта, процесса.

Как вытекает из самой сути данных понятий, в основе технологий идентификации и аутентификации лежит идеология статистического распознавания образов, обусловливая, соответственно, принципиальное наличие ошибок первого (неправильное распознавание) и второго (неправильное нераспознавание) рода. Методы, алгоритмы и технологии распознавания направлены на обеспечение задаваемых вероятностей этих ошибок при определенных стоимостных или иных затратах.

В системотехническом плане структуру систем идентификации/аутентификации можно проиллюстрировать схемой, приведенной на рис. 5.

При регистрации объекта идентификации/аутентификации в системе монитором безопасности формируется его образ, информация по которому подвергается необратимому без знания алгоритма и шифра-ключа, т. е. криптографическому, преобразованию и сохраняется в виде ресурса, доступного в системе исключительно монитору безопасности. Таким образом формируется информационный массив внутренних образов объектов идентификации/аутентификации.

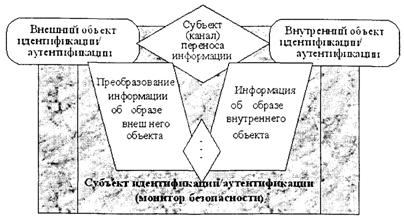


Рис. 5. Системотехнический аспект идентификации/аутентификации

Впоследствии при идентификации/аутентификации (очередной вход в систему пользователя, запрос процесса на доступ к объекту, проверка подлинности объекта системы при выполнении над ним действий и т. д.) объект через канал переноса информации передает монитору безопасности информацию о своем образе, которая подвергается соответствующему преобразованию. Результат этого преобразования сравнивается с соответствующим зарегистрированным внутренним образом, и при их совпадении принимается решение о распознавании (идентификации) и подлинности (аутентификации) объекта.

Информационный массив внутренних образов объектов идентификации/аутентификации является критическим ресурсом системы, несанкционированный доступ к которому дискредитирует всю систему безопасности. Поэтому помимо всевозможных мер по исключению угроз несанкционированного доступа к нему сама информация о внутренних образах объектов идентификации/аутентификации находится в зашифрованном виде.

Формирование образов осуществляется на разной методологической и физической основе в зависимости от объекта идентификации/аутентификации (пользователь-субъект; процесс; объект-ресурс в виде таблицы, формы, запроса, файла, устройства, каталога и т. д.). В общем плане для идентификации/аутентификации пользователей-субъектов в компьютерных системах могут использоваться их биометрические параметры (отпечатки пальцев, рисунок радужной оболочки глаз, голос, почерк и т. д.), либо специальные замково-ключевые устройства (смарт-карты, магнитные карты и т. п.). Однако при доступе непосредственно в АИС (в базы данных), чаще всего используются парольные системы идентификации/аутентификации.

Парольные системы основаны на предъявлении пользователем в момент аутентификации специального секретного (известного только подлинному пользователю) слова или набора символов — пароля. Пароль вводится пользователем с клавиатуры, подвергается криптопреобразованию и сравнивается со своей зашифрованной соответствующим образом учетной копией в системе. При совпадении внешнего и внутреннего парольного аутентификатора осуществляется распознавание и подтверждение подлинности соответствующего субъекта.

Парольные системы являются простыми, но при условии правильной организации подбора и использования паролей, в частности, безусловного сохранения пользователями своих паролей втайне, достаточно надежным средством аутентификации, и, в силу данного обстоятельства, широко распространены.

Основной недостаток систем парольной аутентификации заключается в принципиальной оторванности, отделимости аутентификатора от субъекта-носителя. В результате пароль может быть получен тем или иным способом от законного пользователя или просто подобран, подсмотрен по набору на клавиатуре, перехвачен тем или иным способом в канале ввода в систему и предъявлен системе злоумышленником.

В результате внутренний образ субъекта существенно расширяется и появляется возможность варьирования аутентификатора при каждом следующем входе пользователя в систему. При входе пользователя в систему монитор безопасности (субъект аутентификации) формирует случайную выборку вопросов и, чаще всего, по статистическому критерию «n из m» принимает решение об аутентификации.

В системах коллективного вхождения парольную аутентификацию должны одновременно пройти сразу все зарегистрированные для работы в системе пользователи. Иначе говоря, поодиночке пользователи работать в системе не могут. Вероятность подбора, перехвата и т. д. злоумышленником (злоумышленниками) сразу всех паролей, как правило, существенно меньше, и, тем самым, надежность подобных систем аутентификации выше.

Аутентификации в распределенных информационных системах в принципе должны подвергаться и объекты (ресурсы, устройства), а также процессы (запросы, пакеты и т. д.). Аутентифицированный (подлинный) пользователь, обращаясь к объектам системы и порождая соответствующие процессы, должен, в свою очередь, убедиться в их подлинности, например, отправляя распечатать сформированный в базе данных конфиденциальный отчет на сетевой принтер, специально предназначенный для распечатки соответствующих конфиденциальных документов.

Как правило, для аутентификации объектов применяются технологии асимметричных криптосистем, называемых иначе системами с открытым ключом, рассмотрение которых выходит за допустимый объем данного пособия.

Для аутентификации процессов широкое распространение нашли технологии меток (дескрипторов) доступа.

**Технология меток** или **дескрипторов доступа** отражает сочетание одноуровневой и многоуровневой моделей безопасности данных и основывается на присвоении администратором системы всем объектам и субъектам базы данных специальных дескрипторов доступа, содержащих набор параметров уровня конфиденциальности, допустимых операциях, допустимых имен объектов или субъектов доступа и других особых условий доступа. Субъект доступа, инициируя в соответствии со своим дескриптором (меткой) разрешенный процесс, передает ему свою метку доступа (помечает своей меткой). Ядро безопасности СУБД (ТСВ) проверяет **подлинность метки процесса,** сравнивая ее с меткой доступа пользователя-субъекта, от имени которого выступает процесс. При положительном результате метка доступа процесса сравнивается с меткой доступа объекта, операцию с которым намеревается осуществлять процесс. Если дескрипторы доступа процесса и объекта совпадают (или удовлетворяют правилам и ограничениям политики безопасности системы), монитор безопасности разрешает соответствующий доступ, т. е. разрешает осуществление процесса (операции).

Проверка подлинности метки процесса предотвращает возможные угрозы нарушения безопасности данных путем формирования субъектом для инициируемого им процесса такой метки, которая не соответствует его полномочиям.

Для проверки подлинности меток в системе формируется специальный **файл (массив) учетных записей.** При регистрации нового пользователя в системе для него создается учетная запись, содержащая его идентификационный номер (идентификатор), парольный аутентификатор и набор дескрипторов доступа к объектам базы данных (метка доступа). При инициировании пользователем (субъектом) какого-либо процесса в базе данных и передаче ему своей метки доступа ядро безопасности СУБД подвергает метку процесса криптопреобразованию, сравнивает ее с зашифрованной меткой соответствующего субъекта (пользователя) в массиве учетных записей и выносит решение о подлинности метки.

Массив учетных записей, в свою очередь, является объектом высшей степени конфиденциальности в системе, и доступен только администратору. Ввиду исключительной важности массива учетных записей для безопасности всей системы помимо шифрования его содержимого принимается ряд дополнительных мер к его защите, в том числе специальный режим его размещения, проверка его целостности, документирование всех процессов над ним.

Таким образом, на сегодняшний день наработан и используется развитый набор технологий идентификации/аутентификации в защищенных компьютерных системах. Вместе с тем основные бреши безопасности чаще всего находятся злоумышленниками именно на этом пути.

Список использованной литературы

1. Астахова Л. В. Информатика. Часть 1. Социальная информатика: Учебная пособие. - Челябинск, 2002. - 245 с.

2. Бизнес и безопасность. - КМЦ "Центурион", 2002.

3. Информационная безопасность: Учеб. для вузов по гуманитар. и социально- экон. специальностям. - М.: Междунар. отношения: Летописец, 2002.

4. Степанов Е. А., Корнеев И. К. Информационная безопасность и защита информации. - М.: ИНФРА-М, 2003.

5. Чалдаева Л. А. Информационная безопасность компании. / Л. А. Чалдаев, А. А. Килячков // Финансы и кредит. - 2002. - № 18. - С. 32-37.

6. Ярочкин В. И. Коммерческая информация фирмы. Утечка или разглашение? - М.: 2003