УДК 681.3

DOI: 10.18664/ikszt.v0i1.51555

МИРОШНИК М.А. д.т.н., профессор (УкрГАЖТ)

Разработка средств защиты информации в распределенных компьютерных системах и сетях

Приведено описание комплекса средств защиты информации, обрабатываемой в распределенных вычислительных сетях с протоколом TCP / IP, от несанкционированного доступа, с использованием механизмов разграничения доступа и криптографической защиты. Анализируются современные модели и средства защиты секретной информации в компьютерных базах данных. Предлагается формализованный подход к обеспечению безопасности распределенных баз данных, который опирается на принципы взаимодействия и защиты объектов в компьютерных сетях.

Ключевые слова: *распределенные сети, сеть, доступ, аутентификация, шифрование, защита информации, базы данных, модели безопасности.*

1. Введение

Защита компьютерных сетей (КС) в значительной степени зависит от организации в ней доступа к информации, которая включает в себя обработанные данные и различные сведения о фактах, событиях, явлениях и состояния объектов КС. Информация накапливается в базах данных (БД), словарях, репозиториях, хранилищах и обрабатывается пользователями (приложениями, процессами); она может быть открытой для одних пользователей и закрытой для других или быть доступной только для определенной категории пользователей с соответствующими правами и полномочиями.

Обеспечение безопасности информации в сети - это способность КС защищать информацию от случайных или преднамеренных воздействий, различного рода поломок и отказов в системе, наносящих ущерб инфраструктуре КС. Вопросам безопасности информации стали уделять внимание в конце прошлого века. В наше время появились первые модели защиты информации для высших органов власти и мощных коммерческих структур.

Поскольку основной вред информации, как правило, наносится преступными действиями (вирусами, взломами секретных ключей, похищением данных и т.д.), для борьбы с ними создаются различные механизмы безопасности, включающие организационные, технические и программные мероприятия и средства защиты информации [2-5].

Краеугольным камнем в решении проблем безопасности является специальный документ «Критерии оценки надежности компьютерных систем», который определяет стандартизированный подход к оценке компьютерной безопасности на основе четырех уровней (классов): D, C, B , A. Уровни C и B в свою очередь задаются несколькими подклассами: C1, C2 и B1, B2, B3.

Данный подход служил источником развития фундаментальных и прикладных исследований в области безопасности различных систем, сетей и БД. Сложились общие концепции и модели безопасности информации, направления обеспечения разрешенных доступов. Среди них модели истинности, разграничения доступа, передачи прав и др. [2-3].

Основными аспектами моделей защиты информации являются: доступность (своевременное обеспечение доступа к информации пользователей с полномочиями или привилегиями), целостность (правильность, неперекрученность информации в любое время, защита ее от неверных модификаций и несанкционированного доступа) и конфиденциальность (запрет на ознакомление с информацией лиц, не имеющих прав или полномочий) [5]. Все три аспекта тесно соприкасаются, и достаточно часто для их достижения используется один и тот же механизм.

В данной статье продолжаются исследования, посвященные вопросам безопасности и защиты распределенных компьютерных сред [2-5], в направлении обеспечения безопасности БД.

2. Средства защиты информации от несанкционированного доступа в распределенных вычислительных сетях

По мере развития Интернет и информационных технологий все большую привлекательность для различных организаций в качестве инструмента для автоматизации бизнес-процедур, документооборота, финансовых операций приобретают виртуальные частные сети (Virtual Private Network -VPN).

В общем случае VPN - это объединение локальных вычислительных сетей (ЛВС) или отдельных компьютеров, подключенных к распределенной вычислительной сети (РВС) общего пользования, в единую виртуальную (наложенную) сеть. VPN,

создаваемые на базе РВС общего пользования (и, в первую очередь, Интернет), являются хорошей альтернативой изолированным корпоративным сетям, обладающей рядом несомненных достоинств [1, 2]:

- низкая стоимость арендуемых каналов и коммуникационного оборудования;
- развитая (в географическом смысле) топология сети;
- высокая надежность за счет наличия параллельных каналов передачи;
- легкость масштабирования (подключения новых ЛВС или пользователей);
- легкость конфигурирования.

Однако необходимо не забывать, что создание VPN, решая одну проблему - существенное сокращение расходов на эксплуатацию собственной корпоративной сети, выдвигает на первое место другую - обеспечение безопасности обрабатываемой информации.

Комплекс PostCrypt-VPN предназначен для защиты информации, обрабатываемой в РВС с протоколом TCP/IP, от угроз целостности, конфиденциальности и доступности с использованием механизмов разграничения доступа и криптографической защиты. В состав PostCrypt-VPN входят программные модули-агенты средств защиты клиента и сервера, функционирующие на рабочих станциях (РС), имеющих доступ к РВС, автоматизированные рабочие места (АРМ) управления и администрирования и АРМ управления ключами центра сертификации открытых ключей (ОК).

Модуль-агент средств защиты клиента реализует следующие функции:

- прием запросов на установление защищенных соединений с сервером приложений от зарегистрированных РС;
- установление связи по протоколу TCP с модулем-агентом средств защиты сервера, функционирующим на противоположной стороне виртуального соединения;
- строгую аутентификацию модуля-агента средств защиты сервера с использованием механизма электронной цифровой подписи (ЭЦП) по алгоритму, установленному ГОСТ 34.310-95, 34.311-95;
- выработку сеансового ключа для шифрования данных, передаваемых по виртуальному соединению, обмен сеансовыми ключами, зашифрованными на ключе шифрования ключей (КШК), выработанном по схеме Диффи-Хеллмана, с модулем-агентом средств защиты сервера;
- шифрование/расшифрование данных, передаваемых по виртуальному соединению, по алгоритму, установленному ГОСТ 28147-89.

Модуль-агент средств защиты сервера реализует следующие функции:

- прием запросов на установление защищенных соединений с сервером приложений от зарегистрированных модулей-агентов средств защиты клиента;
- строгую аутентификацию модуля-агента средств защиты клиента с использованием механизма электронной цифровой подписи (ЭЦП), по алгоритму, установленному ГОСТ 34.310-95, 34.311-95;
- выработку сеансового ключа для шифрования данных, передаваемых по виртуальному соединению, обмен сеансовыми ключами, зашифрованными на ключе шифрования ключей (КШК), выработанном по схеме Диффи-Хеллмана, с модулем-агентом средств защиты клиента;
- установление связи по протоколу TCP с приложением сервера;
- шифрование/расшифрование данных, передаваемых по виртуальному соединению, по алгоритму, установленному ГОСТ 28147-89.

АРМ управления и администрирования реализуют:

- генерацию ключей ЭЦП пользователей комплекса с сохранением секретных ключей (СК) на специальных носителях (дискета, TouchMemory) и открытых ключей (ОК) в базе данных окрытых ключей (БД ОК);
- управление обменом ОК ЭЦП пользователей комплекса между собой через специально выделенную организацию, выступающую в качестве центра сертификации ОК, или напрямую;
- настройку параметров объектов защиты, входящих в состав ВЗС, и защищенных соединений, используемых для доступа к ВЗС.

АРМ управления ключами центра сертификации ОК реализует:

- генерацию ключей ЭЦП администратора центра сертификации ОК с сохранением СК на специальных носителях (дискета, Touch Memory) и ОК в БД ОК;
- управление приемом ОК пользователей комплекса, сертификацией данных ОК и передачей их в АРМ управления и администрирования объектов защиты.

Реализуемая технология управления криптографическими ключами соответствует требованиям [1]. В терминах нормативного документа системы технической защиты информации НД ТЗИ 2.5-0004-99 “Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа”, программные средства защиты информации, входящие в состав комплекса PostCrypt-VPN, реализуют следующие функциональные услуги безопасности:

{КВ-2, ЦВ-2, ДР-2, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НО-1, НЦ-1, НВ-2 }.

Разграничение доступа пользователей к защищаемым ресурсам осуществляется в соответствии с концепцией диспетчера доступа. В соответствии с данной концепцией все элементы вычислительной системы относятся к одному из следующих классов:

Объект-пользователь – пользователь, который пытается получить доступ к определенной информации. В соответствии с реализуемой средствами комплекса политикой безопасности объекты-пользователи делятся на уполномоченных управлять средствами защиты (администраторов) и обычных пользователей.

Объект-процесс – порождаемый пользователем процесс, который пытается получить доступ к определенной информации. В соответствии с реализуемой средствами комплекса политикой безопасности объектами-процессами являются приложения (процессы, функционирующие на РС ЛВС). Субъекты доступа представляются своими сетевыми адресами (IP - адрес).

Пассивный объект – пассивный источник/приемник информации, которая нуждается в защите. В соответствии с реализуемой средствами комплекса политикой безопасности защищаемыми объектами являются ресурсы серверов приложений (прикладные сервисы), представленные своими транспортными адресами (IP-адрес:порт) [4].

База данных авторизации – информация, определяющая права доступа (атрибуты доступа) объектов-пользователей и объектов-процессов к пассивным объектам.

База данных регистрации – записи о запросах и предоставлении доступа субъектов к объектам.

Механизм контроля (диспетчер доступа) – средства, которые реализуют функции защиты и обеспечивают безопасность информации путем управления созданием объектов-пользователей, объектов-процессов и пассивных объектов, предоставления объектам-пользователям и объектам-процессам доступа к пассивным объектам на основании проверки хранящихся в базе данных авторизации атрибутов доступа пользователя, процесса и пассивного объекта, с выполнением при этом регистрации событий (действий пользователей и процессов) в БД регистрации, т.е. реализуют правила разграничения доступа (ПРД), принятые в системе, и способствуют соблюдению политики безопасности информации, принятой в организации.

В комплексе реализовано административное разграничение доступа. Это означает, что управление потоками информации между пользователями, процессами и объектами осуществляют только специально авторизованные пользователи (администраторы). Для каждого защищаемого ресурса (прикладного сервиса) администратор защиты может установить список доступа, в котором перечислены пользователи и процессы, имеющие права доступа к нему. Обычные пользователи изменять права доступа субъектов к объектам, а также выполнять любые другие функции управления системой защиты не могут.

Для получения доступа к защищаемому ресурсу сервера приложений приложение-клиент, функционирующее на РС ЛВС, инициирует запрос к модулю-агенту средств защиты клиента, функционирующему в этой же ЛВС (рис. 1). Модуль-агент средств защиты клиента по списку доступа проверяет права РС на доступ к защищаемому ресурсу по ее сетевому адресу (реализуя услугу НВ-1) и, если доступ разрешен, в свою очередь инициирует запрос на установление защищенного соединения к модуль-агенту средств защиты сервера, функционирующему в ЛВС сервера приложений.

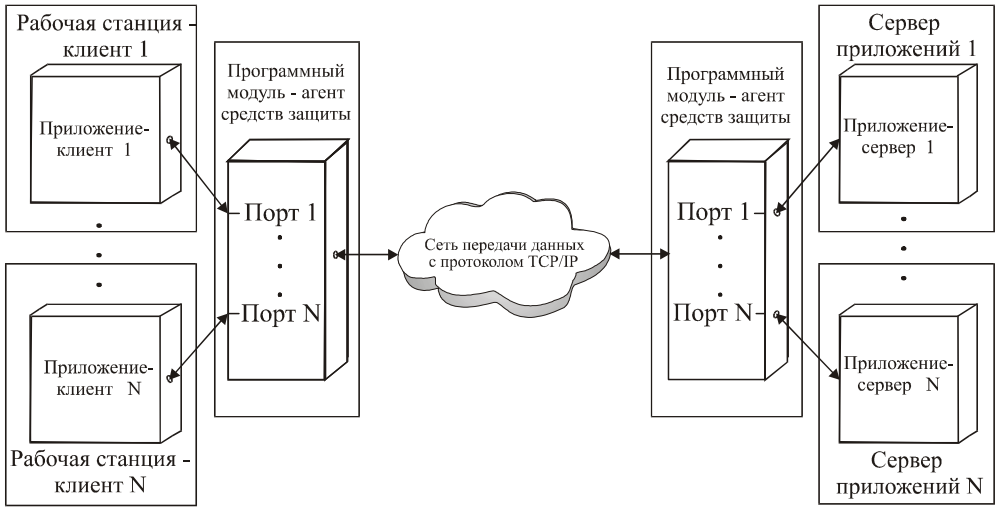

Рис. 1. Локальная вычислительная сеть

В процессе установления защищенного соединения модуль-агент средств защиты сервера проверяет полномочия соответствующего модуля-агента средств защиты клиента на доступ к защищаемым ресурсам по его сетевому адресу (реализуя услугу НВ-1) и, если такой доступ разрешен, клиентский и серверный модули-агенты средств защиты выполняют взаимную строгую аутентификацию (реализуя услугу НВ-2), после чего согласовывают сеансовый ключ шифрования, с использованием которого в процессе обмена шифруются с обеспечением целостности (реализуются услуги КВ-2, ЦВ-2) все данные, передаваемые по TCP-соединению. Взаимная строгая аутентификация выполняется с применением несимметричных криптографических алгоритмов.

После завершения взаимной аутентификации модуль-агент средств защиты сервера устанавливает соединение с защищаемым ресурсом. Все взаимодействие модулей - агентов средств защиты между собой, а также с клиентским и серверным приложением осуществляется на транспортном уровне (четвертый уровень модели взаимодействия открытых систем). При этом на одном и том же узле РВС могут функционировать одновременно как модуль-агент средств защиты клиента (для обеспечения защиты исходящих соединений), так и модуль-агент средств защиты сервера (для обеспечения защиты входящих соединений), причем как исходящие, так и входящие соединения могут устанавливаться с любыми другими узлами ВЗС (в соответствии с выполненными настройками параметров защищенных соединений), а максимальное количество защищенных соединений ограничивается только возможностями соответствующей ОС.

В процессе установления защищенного соединения между модулями-агентами средств защиты, а также обмена данными между клиентским и серверным модулями-агентами средств защиты в специальные файлы протоколов, защищенные от модификации, в реальном времени выводятся сообщения обо всех критичных для безопасности событиях (реализуется услуга НР-2).

Обмен данными между клиентским (серверным) приложением и клиентским (серверным) модулем-агентом средств защиты происходит без доступа в РВС и защищается с использованием средств соответствующих ОС и прикладных программных средств.

При организации ВЗС программные средства комплекса могут использоваться в двух вариантах: для реализации защищенного доступа к ресурсам защищаемой подсети с их межсетевым экранированием и для реализации защищенного доступа к ресурсам сервера приложений.

При реализации защищенного доступа к ресурсам защищаемой подсети с их межсетевым экранированием программный модуль-агент средств защиты клиента запускается на рабочих станциях, на которых функционируют приложения-клиенты, осуществляющие доступ к ресурсам защищаемой подсети, а программный модуль-агент средств защиты сервера - на специально выделенном компьютере (выполняющем функции межсетевого экрана), имеющем два сетевых интерфейса (рис. 2). Запросы на установление защищенных соединений принимаются модулем-агентом средств защиты клиента только от приложений, функционирующих на тех рабочих станциях, которым разрешен доступ к защищаемым ресурсам (выполняется фильтрация запросов на сетевом уровне) и передаются модулю-агенту средств защиты сервера.

Модуль-агент средств защиты сервера принимает запросы на установление защищенных соединений от модулей-агентов средств защиты клиентов через отдельный сетевой интерфейс (интерфейс 2), проверяет полномочия по доступу к защищаемым ресурсам с сетевого адреса данной рабочей станции (выполняет фильтрацию запроса на сетевом и транспортном уровне). При подтверждении полномочий по доступу клиентский и серверный модули-агенты средств защиты выполняют взаимную строгую аутентификацию, согласовывают сеансовый ключ шифрования, с использованием которого в процессе обмена шифруются с обеспечением целостности все данные, передаваемые между клиентской рабочей станцией и межсетевым экраном, после чего агент средств защиты сервера устанавливает через другой сетевой интерфейс (интерфейс 1) соединение с соответствующим серверным приложением. При этом в ОС межсетевого экрана отключается автоматическая ретрансляция IP-пакетов с сетевого интерфейса 1 на сетевой интерфейс 2 и наоборот, что позволяет скрыть от внешнего мира (экранировать) ресурсы серверов, функционирующих в защищаемой подсети, сделав их доступными только для оснащенных средствами защиты и зарегистрированных в БД модуля-агента средств защиты сервера рабочих станций.

При реализации защищенного доступа к ресурсам сервера приложений с использованием комплекса PostCrypt-VPN программный модуль-агент средств защиты сервера запускается непосредственно на сервере приложений, а программный модуль-агент средств защиты клиента - на рабочей станции, на которой функционирует приложение-клиент (рис. 3). Запросы на установление защищенных соединений принимаются модулем-агентом средств защиты клиента только от приложений, функционирующих на той же рабочей станции, что и агент защиты клиента. Принятый запрос передается модулю-агенту средств защиты сервера, который проверяет полномочия по доступу к защищаемому ресурсу с сетевого адреса

данной рабочей станции (выполняет фильтрацию запроса на сетевом и транспортном уровне). При подтверждении полномочий по доступу клиентский и серверный модули-агенты средств защиты выполняют взаимную строгую аутентификацию, согласовывают сеансовый ключ шифрования, с использованием которого в процессе обмена шифруются с обеспечением целостности все данные, которыми обмениваются клиентское и серверное приложения, после чего агент средств защиты сервера устанавливает соединение с соответствующим серверным приложением. При этом приложение-сервер конфигурируется таким образом, чтобы допускать обработку запросов только от модуля - агента средств защиты сервера (только с сетевого адреса сервера приложений).

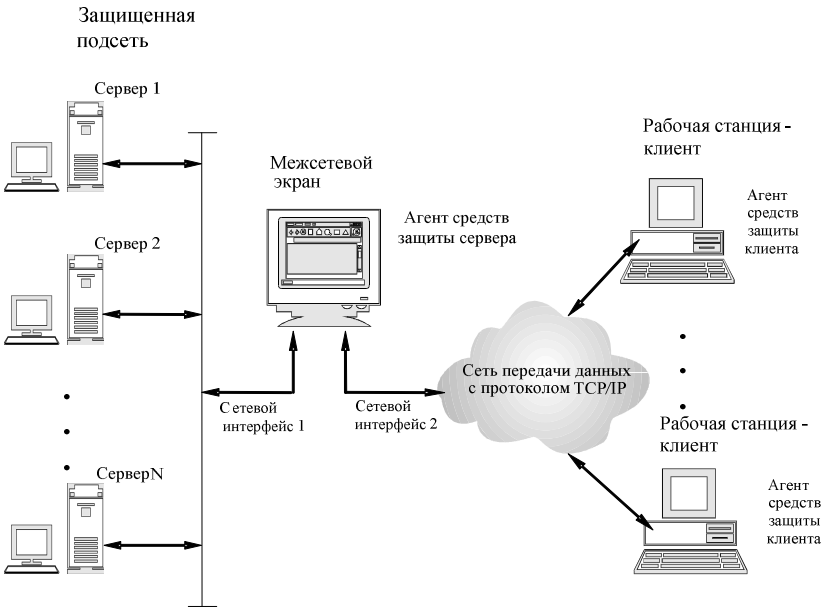

Рис. 2. Доступ к защищенной компьютерной сети

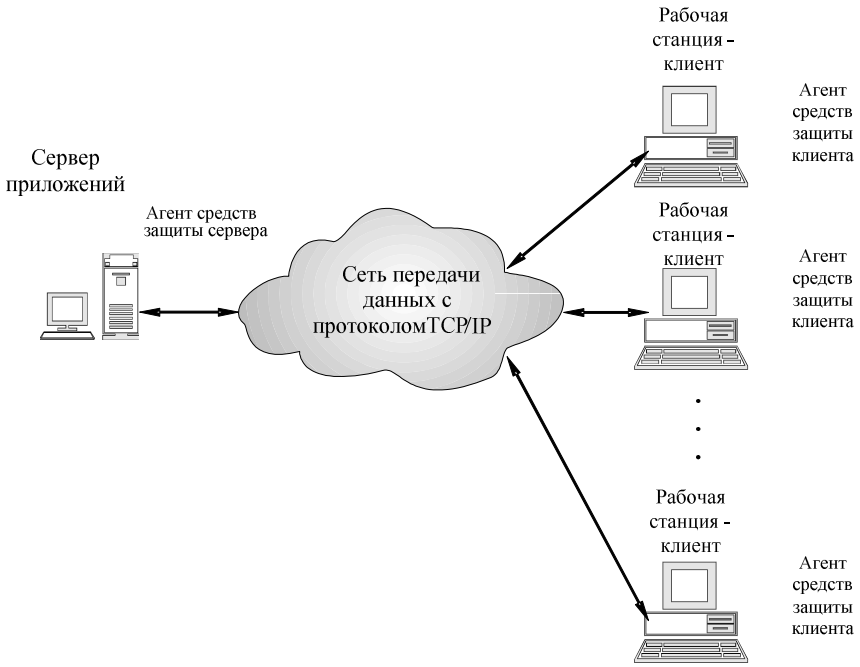

Рис. 3. Рабочая станция, на которой функционирует приложение-клиент

3. Системный подход к защите распределенных БД

В двухзвенный архитектуре «клиент - сервер» прикладная часть выполняется клиентом (на рабочей станции, узле сети и т. П.), А сервер осуществляет доступ к БД. В случае сложности и емкости прикладной обработки в эту архитектуру добавляется сервер приложений, который берет на себя основную логику обработки информации и доступа к БД. При этом БД может быть централизованной (один сервер) или распределенной (несколько серверов). В распределенной БД основным условием сохранения данных является автономность и отсутствие прямых и транзитивных связей между таблицами, расположенных в удаленных разделах БД. Поскольку это условие ограничивает целостность данных, то в состав сервера включаются хранимые процедуры, с помощью которых устанавливаются ссылки на другие разделы БД.

Как правило, защита БД осуществляет специальный сервер. В его функции входит обеспечение парольной защиты, шифрования, установка прав доступа к объектам БД, защита полей и записей таблиц и т.д.

Пароли устанавливаются конечными пользователями или администраторами БД, хранятся в защищенном виде в специальных файлах и используются сервером при доступе пользователей к БД.

Шифрование осуществляется с помощью ключей фиксированной и нефиксированной длины для засекречивания сохраненной в БД информации или при передаче информации в сети от отправителя к получателю и наоборот.

Установка прав доступа к БД заключается в регистрации пользователей для защиты от несанкционированного доступа. Прав доступа относятся: чтение, модификация, добавление, удаление, изменение структур таблиц и т. Др. С помощью разрешенных для каждого пользователя прав осуществляется контроль их доступа к объектам БД и принимаются меры для защиты отдельных строк, столбиков, полей или БД в целом.

К основным мероприятиям по проведению защиты данных БД относятся:

– режимные, включающие парольную, криптографическую проверки пользователей и т.д.;

– технологические, содержащие резервное копирование данных, правильное их хранение, эксплуатацию и др.;

– системные, с процедурами автоматизированной проверки полномочий и истинности пользователей, которые запрашивают доступ к данным, их привилегий, аудита событий, происходящих и т.д.

Режимные и технологические мероприятия поддерживаются методическими материалами и стандартами, регламентирующими действия группы лиц, ответственных за безопасность БД. Системные - образуют сервис безопасности, включающий сервер БД с функциями защиты.

Особенностью распределенных БД (РБД) является размещение отдельных разделов данных на разных узлах сети, информация о расположении которых отражается в глобальном словаре данных и используется при доступе к РБД различных пользователей.

Для обеспечения безопасности распределенных, многоуровневых и других БД в состав сервера БД включаются хранимые процедуры проверки прав и полномочий пользователей, определенные моделями защиты, средствами контроля доступа, реализованными в сервисе безопасности БД. На рисунки 4 приведен пример архитектуры распределенной системы управления базой данных (СУБД) с защитой информации.

Рис. 4. Пример архитектуры распределенной СУБД с защитой информации

Пользователи 1, 2, ..., N обращаются к данным через сервис безопасности, контролирует доступ и выполняет только разрешенные операции над БД, в которых содержатся отдельно вполне секретные, секретные и несекретные данные. В запросах на доступ к совершенно секретным, секретным и конфиденциальным данным указываются права и / или полномочия пользователя, проверяются сервисом безопасности по списку контроля доступа и таблицей полномочий.

Для работы с секретной информацией в БД могут быть приведены многозначные отношения в виде множества кортежей с тем же самым значением первичного ключа.

Примером такого отражения могут служить данные о сотрудниках военного заведения, для которых под одинаковой фамилией указаны, наряду с их реальными званиями и видами деятельности, также фальшивые данные для их прикрытия. БД с такими данными требуют многоуровневой защиты, или использование механизмов маскировки данных пустыми значениями.

При модификации пустых значений многоуровневую защиту СУБД может выдать отказ в доступе, если у пользователя (или процесса) отсутствуют полномочия на проведение модификаций в искомом кортежи данных. Модификация обычно проводится с помощью косвенного канала, представляет собой механизм, благодаря которому пользователь, который обладает высоким уровнем полномочий и прав, может предоставить информацию пользователю с меньшими правами и полномочиями [3].

Многоуровневая защита данных может производиться с помощью мандатного управления доступом, основанная на свойствах модели Белла-ЛаПадула для производных базовых отношений и SQL-представления. Современный язык SQL содержит операторы защиты данных: grant и revoke. Оператор grant дает возможность предоставлять привилегии для доступа и модификации объектов, а также передавать другим пользователям права на привилегии (с помощью конструкции with grant option). Оператор revoke позволяет отбирать права, предоставленные ранее некоторому пользователю. Многие SQL-ориентированных СУБД имеют собственные средства безопасности БД, реализованы на средствах защиты данных на языке SQL.

Для обеспечения безопасности неоднородных систем мультибаз применяются мощные средства многоуровневой защиты данных, защищены базы данных и информационные менеджеры, которые управляют защитой данных. Пользователь, который имеет определенные полномочия, получает доступ к мультибаз только в том случае, когда в запросе указан соответствующий параметр аутентификации. СУБД с многоуровневой защитой обычно расширяются языковыми средствами DDL (Definition Data Language), которые предназначены для спецификации классов безопасности относительно мультиуровневых языка SQL.

Степень безопасности в объектно-ориентированных БД ниже, чем в развитых реляционных СУБД. Принципы многоуровневой защиты, разработанные для реляционных баз данных, такие, как многозначность и модель Белла-ЛаПадула, получили развитие в объектно-ориентированной системе SODA (Secure Object-oriented Database). В ней модель Белла-ЛаПадула объединенная со стратегией присваивания меток безопасности двух видов: объектов и переменных объектов.

В первом случае классификация объектов осуществляется путем определения одного общего класса для всего кортежа или для одного его объекта.

Во втором случае каждому переменному объекту присваивается независимая метка, соответствует диапазону классификации объектов на уровне элементов кортежей, при котором каждый столбик отношение имеет собственный допустимый диапазон классификации, а элемент кортежа - индивидуальную классификацию, независимую от других элементов.

С помощью таких меток классифицируются составные или несоставные объекты объектно-ориентированных БД, и создается набор правил для управления уровнями защиты классов объектов и отношений между объектами.

Рассмотренные модели безопасности ориентированы на поддержку нескольких уровней защиты и касаются преимущественно БД с реляционной архитектурой. Эффективность моделей существенно повышается, если дополнительно применяется шифрование информации. Однако каждая из рассмотренных и любая другая известная модель не предоставляют полной защиты информации.

В связи с бурным развитием компьютерных сетей, электронной коммерции и электронного бизнеса с использованием Интернет все большую актуальность приобретает проблема обеспечения безопасности РБД и серверов БД. Используя объектно-ориентированный подход любую распределенную БД, взаимодействует с пользователями, можно рассматривать как сетевую структуру, для которой применяются разработанные для сетевых сред методы обеспечения безопасности и защиты информации.

Совместное рассмотрение моделей, методов и средств взаимодействия и обеспечения безопасности объектов КМ [4] с вышеизложенными моделями защиты информации позволяет по-новому взглянуть на вопросы безопасности информации в среде РБД.

Предложенная в [4] модель взаимодействия (МВ) объектов компьютерной сети, примененной к РБД, позволяет описать модель безопасной работы РБД в следующем виде:

$$МВ\ (РБД) = \{\{БД_i\}, \{I_i\}, \{K_j\}, \{ОД_{ji}\}, M_{РБД}\},$$

где $РБД = \bigcup_i БД_i$, $БД_i$ – независимая локальная компонента РБД с номером i;

I_i, $БД_i – I_i$ -информация, хранящаяся в $БД_i$;

$I_i = \bigcup_{n \in |I_i|} I_{i_n}$, I_{i_n} – информационные объекты $БД_i$;

$|I_i|$ - мощность (количество) объектов в I_i;

K_j – пользователь данной РБД с номером j;

$ОД_{ji} = \bigcup_{n \in |I_i|} ОД_{ji_n}$, $ОД_{ji_n}$ – операция доступа пользователя K_j к объекту I_{i_n};

Доступ пользователя K_j к объекту I_{i_n} выражается соотношением

$$K_j(ОД_{ji_n}) = I_{i_n}.$$

Модель безопасности [8], примененной к РБД, принимает вид

$$M_{РБД} = \{M_З, УГР, I_З\},$$

где $M_З$ – модель защиты сервиса безопасности РБД;

УГР – совокупность внешних и внутренних умышленных и неумышленных угроз;

$I_З$ – защищенные информационные ресурсы РБД.

В свою очередь $M_З = \{M_{КМ}, M_{ЗІ}\}$, где $M_{КМ}$ – модель защиты компьютерной сети, в которой функционирует данная РБД. $M_{КМ}$ базируется на механизмах авторизации, аутентификации, парольной и ролевого защиты, ограничения и контроля доступа, блокировки услуг, аудита и др. [5]; $M_{ЗІ}$ – это модели защиты информации, основанные на понятиях полномочий, истинности, разграничения доступа, передачи прав и т.п., рассмотренных выше.

В терминах предложенного формализма условие безопасной работы РБД записывается в виде

$$K_j(ОД_{ji_n}) = \begin{cases} I_{i_n}, & якщо \quad ОД_{ji_n} \in M_З, \\ \varnothing, & якщо \quad ОД_{ji_n} \notin M_З \end{cases}$$

для всех $I_{i_n} \subset I_З$.

4. Выводы

Проанализированы наиболее часто используемые в практике и теоретически обоснованы модели защиты информации в компьютерных системах. Рассмотрены особенности реализованных средств защиты данных в среде реляционных, распределенных, объектно-ориентированных СУБД.

Подано формализованный подход к обеспечению безопасности распределенных баз данных, основанный на интеграции моделей и средств взаимодействия и безопасности объектов в компьютерных сетях с моделями защиты информации. Данный подход в сочетании с организационными, режимными и системными средствами безопасности КС обеспечивает не только высокий уровень защиты данных, но и достаточный уровень защиты РБД от многих угроз, возникающих в КС.

Литература

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999.
2. Мирошник М.А. Диагностические эксперименты в системах защиты информации на сетях клеточных автоматов. / М.А. Мирошник, Я.Ю.Королева // Інформаційно-керуючі системи на залізничному транспорті. – 2009. – №4. – С. 142–145.
3. Мирошник М.А. Методы эффективного кодирования внутренних состояний микропрограммных автоматов. / М.А. Мирошник, Я.Ю.Королева, // Технология приборостроения. – 2011. – №1. – С. 12–16.
4. Miroshnik M. Uses of programmable logic integrated circuits for implementations of data encryption standard and its experimental linear cryptanalysis. / Miroshnik M., Kovalenko M. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – №6, с.36-45.
5. Мирошник М.А. Методы защиты цифровой информации в распределенных компьютерных сетях. Інформаційно-керуючі системи на залізничному транспорті. – 2014. – №5. – с. 66-70.

Мірошник М.А. Розробка засобів захисту інформації в розподілених комп'ютерних системах та мережах. Наведено опис комплексу засобів захисту інформації, що обробляється в розподілених обчислюваних мережах з протоколом TCP/IP, від несанкціонованого доступу, з використанням механізмів розмежування доступу та криптографічного захисту. Аналізуються сучасні моделі та засоби захисту секретної інформації в комп'ютерних базах даних. Пропонується формалізований підхід до забезпечення безпеки розподілених баз даних, що спирається на принципи взаємодії та захисту об'єктів у комп'ютерних мережах.

Ключові слова: розподілені мережі, мережеві атаки, мережа, доступ, автентифікація, шифрування, захист інформації, бази даних, моделі безпеки.

Miroshnik M.A. Development of information security in distributed computer systems and networks. A description of the information protection system for wide-area TCP/IP networks, based on access mediation and cryptography security mechanisms is given. Modern models and means of the secret information protection in computer data bases are analyzed. A formalized approach to the safety of distributed data bases that is based on principles of interaction and protection of network objects is suggested.

Key words: distributed networks, network protocols, network attacks, routed service, authentication, encryption, data protection, database security model.

Рецензент д.т.н., профессор Листровой С.В. (УкрГАЖТ)

Поступила 01.12.2014г.