КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

A.V. Palagin, N.I. Alishov, V.A. Marchenko, V.A. Shirokov

TECHNOLOGY OF PROTECTION OF BIG DATABASES FROM NOT AUTHORIZED COPYING

The technology of protection of big databases (DB) or their significant part from copying by the not authorized user or the user possessing a full set of privileges is offered. The brief analysis of existing technologies of protection and their lacks is considered. The hardware device of protection of a DB is described and also the algorithm of realization, technology of protection with application of the given device is considered.

Предлагается технология защиты больших баз данных или их значительной части от копирования несанкционированным пользователем или пользователем, обладающим полным набором привилегий. Приводится краткий анализ существующих технологий защиты и их недостатков. Описывается аппаратное устройство защиты БД, а также рассматривается алгоритм реализации, технологии защиты с применением данного устройства.

УДК 681.324

А.В. ПАЛАГИН, Н.И. АЛИШОВ,
В.А. МАРЧЕНКО, В.А. ШИРОКОВ

ТЕХНОЛОГИЯ ЗАЩИТЫ БОЛЬШИХ БАЗ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Введение. Вопросу безопасности баз данных (БД) и их защиты посвящено множество статей, научных работ и исследований. На основе этих работ можно сформулировать несколько основных проблем в данной области, связанных с обеспечением безопасности:

защита БД от несанкционированного доступа;

защита канала передачи между серверной и клиентской частью;

организация криптографической защиты содержимого БД.

Анализ современных аппаратно-программных средств защиты БД показывает, что большинство готовых решений более-менее успешно решают две первые проблемы. Что касается организации криптографической защиты содержимого БД, то несмотря на наличие современных криптоустойчивых алгоритмов шифрования, данная проблема далека от возможных эффективных решений. Инциденты последних лет с утечкой информации из баз данных транснациональных корпораций, а также госучреждений показывают, что проблема защиты БД обусловливает разработки новых технологий организации доступа к информационным ресурсам [1].

Одним из наиболее часто встречающихся сценариев хищения БД является её полное копирование на внешний носитель или утеря одного из устройств хранения во время транспортировки. Данный сценарий показывает

слабую защищённость физических носителей БД (жесткий диск, ленточный носитель, оптический носитель) и объектов хранения в файловой системе. За сохранность этих объектов отвечает операционная система (ОС), что является слабым звеном защиты (рис. 1). Так как программное обеспечение (ПО) СУБД управляет и соответственно контролирует только логические объекты БД, то естественно оно не отвечает за управление доступом к объектам файловой системы, из которых состоит БД.

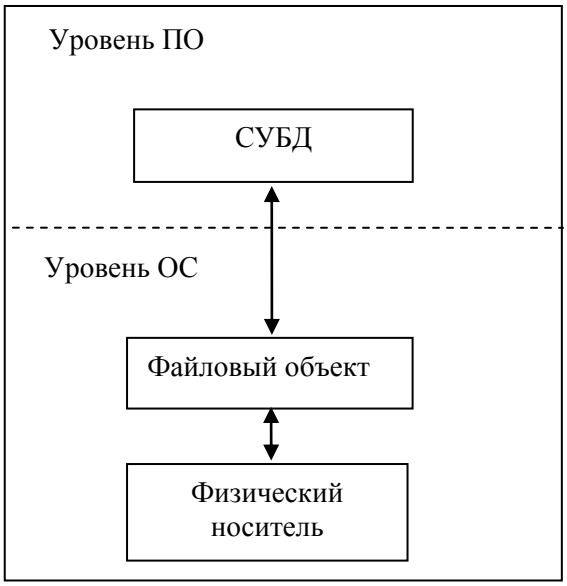

РИС. 1. Разграничение полномочий между ОС и СУБД

Для защиты БД на уровне ОС есть несколько путей:
- шифрование средствами ОС на уровне физического носителя;
- шифрование средствами ОС на уровне файлового объекта;
- шифрование средствами СУБД на уровне логических объектов БД.

Первый метод защиты ориентирован на защиту физического носителя БД, но не позволяет защитить от копирования объектов файловой системы. В основном этот метод используется в системах резервного копирования и во время транспортировки БД на физических носителях. При этом БД не защищена от копирования в виде файлового объекта для легального пользователя ОС, даже если этот пользователь не является пользователем самой БД.

Второй метод решает проблему защиты от легального пользователя ОС, но если он не является легальным пользователем БД. В противном случае он абсолютно бесполезен, так как БД можно скопировать средствами самой СУБД в другой файловый объект.

Постановка задачи. Главная задача при защите БД от копирования – защита логических объектов БД от копирования как несанкционированным пользователем, так и пользователем, обладающим полным набором привилегий. Эта задача решается путем шифрования логических объектов БД.

Такой способ защиты предусматривает реализацию шифрования средствами СУБД или средствами разрабатываемого под конкретную базу ПО. При реализации шифрования средствами СУБД технология разработки дополнительного ПО не изменяется или изменяется незначительно. Все процедуры шифрования-расшифрования происходят на промежуточном уровне между БД и СУБД (рис. 2). Однако современные СУБД не поддерживают или поддерживают частично шифрование логических объектов БД [2]. Поэтому единственный способ гарантированной защиты БД от копирования является реализация функций шифрования на уровне изолированного ПО, разрабатываемого под конкретную БД.

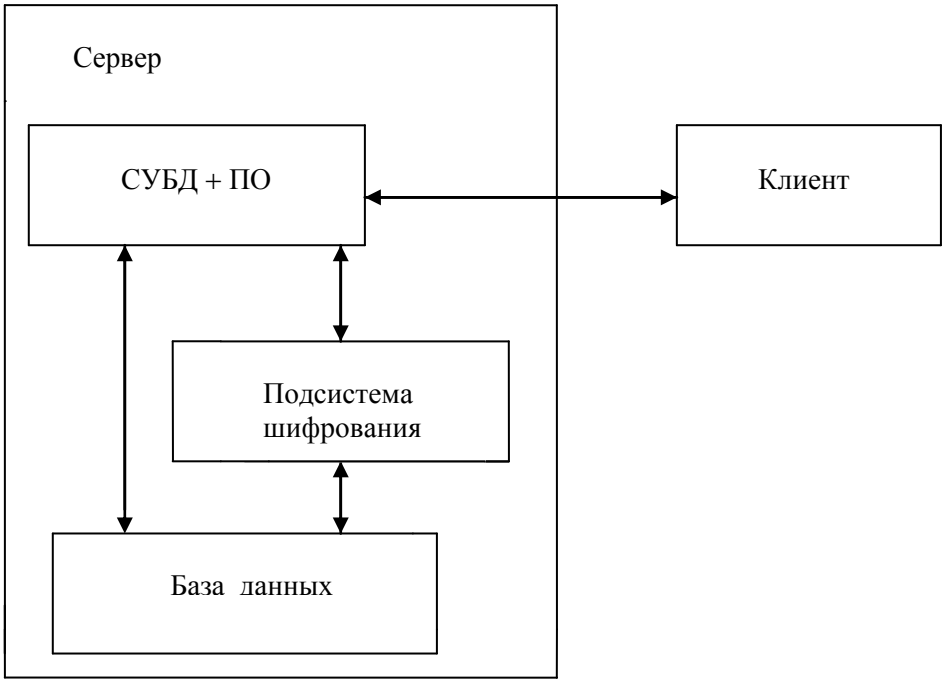

РИС. 2. Организация взаимодействия между СУБД и БД

Методы решения задачи. Предлагаемая технология направлена на обеспечение защиты от копирования больших баз данных (БД) или их значительных частей несанкционированным пользователем или пользователем, обладающим полным набором привилегий. Разработанный способ защиты предполагает применение аппаратного ключа (электронного ключа) со встроенным алгоритмом шифрования, а также специальных алгоритмов взаимодействия между про-

граммным обеспечением, реализующим БД, и функциями, предоставляемыми электронным ключом [3].

Использование аппаратного устройства шифрования позволяет представить алгоритм шифрования вместе с ключом в виде черного ящика, что не позволяет считать эти данные любому пользователю независимо от набора привилегий. В качестве криптоалгоритма предлагается использование асимметричных алгоритмов [4], так как они позволяют любому пользователю зашифровать данные, и соответственно записать их в БД, но не позволяют их расшифровывать без наличия закрытого ключа, записанного внутрь устройства.

Вычислительное устройство (электронный ключ) защиты больших БД от копирования представляет собой схему, состоящую из нескольких функциональных блоков (рис. 3).

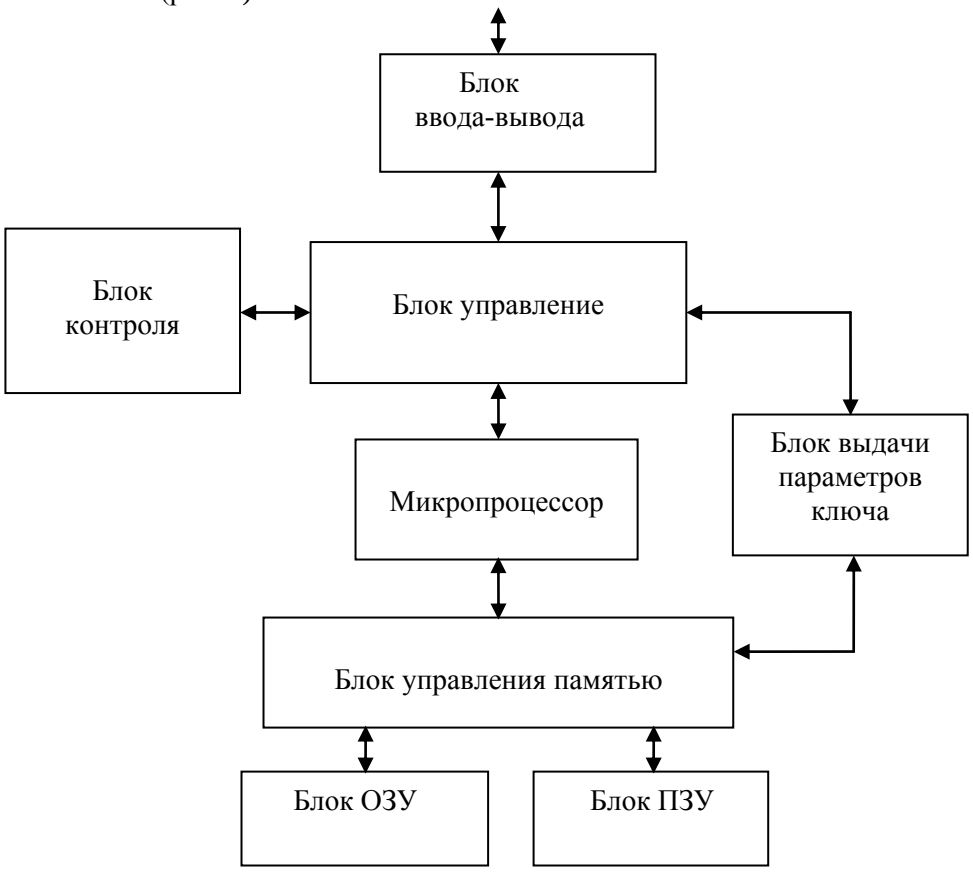

РИС. 3. Функциональная схема устройства

Блоком ввода-вывода называется интерфейсная часть электронного ключа, обеспечивающая связь вычислительного устройства с локальным компьютером,

на котором это устройство установлено. Данный блок используется для организации информационного обмена между ключом и защищаемой БД.

Блок управления организовывает связь разных функциональных блоков электронного ключа (вычислительного устройства) с внешним миром, контролирует информационные потоки внутри устройства.

Блок контроля выполняет такие функции:

- анализ скорости нажатия клавиш;
- анализ количества запросов к аппаратному ключу из защищаемой БД за единицу времени;
- введение дополнительных задержек при выполнении очередного запроса.

Этот блок позволяет противодействовать некоторым методам считывания всей БД или значительной её части за относительно малый промежуток времени. Однако он не обеспечивает защиту БД от копирования тех ее записей, которые выдаются на экран монитора, или от перехвата расшифрованных данных при их передаче от электронного ключа к центральному компьютеру.

Микропроцессор реализует функции управления процессом шифрования-расшифрования, а также реализует сам алгоритм шифрования.

Блок выдачи параметров ключа управляет выдачей параметров шифрования, служебных данных, а также открытого ключа по запросу внешнего пользователя. Сами данные хранятся в недоступном для внешнего пользователя участке памяти для защиты их от несанкционированного пользователя.

Блок управления памятью контролирует обмен данными между разными участками памяти и другими функциональными блоками, такими, как микропроцессор и блок выдачи параметров ключа.

Блок ОЗУ служит для размещения промежуточных данных вычислений и имеет достаточный объём для проведения необходимых операций криптоалгоритма.

Блок ПЗУ предназначен для размещения таких данных, как начальные параметры инициализации криптоалгоритма, открытый ключ шифрования, закрытый ключ шифрования, порядковый номер ключа и др.[5]. Этот блок является энергонезависимым и сохраняет свои данные после отключения устройства от компьютера.

Технология применения разработанного способа защиты БД предполагает выполнение нескольких этапов. На первом этапе при создании защищённой БД выбранный электронный ключ инициализируется следующими значениями:

- открытый ключ шифрования и другие параметры, доступные несанкционированному пользователю;
- закрытый ключ шифрования и другие параметры, недоступные пользователю;
- начальные параметры инициализации криптосистемы.

Эти параметры генерируются и проверяются с помощью известных математических методов и алгоритмов[6].

На следующем этапе выбирается набор полей БД, которые будут подвергаться шифрованию, а также разрабатывается специальное ПО, которое реали-

зует функции обмена данными между БД и устройством и контролирует процесс шифрования и расшифрования. Возможен вариант шифрования с использованием программной реализации алгоритма с открытым ключом и параметрами криптосистемы, полученными по запросу от электронного ключа. После реализации данного этапа БД можно считать защищённой от полного копирования или копирования её значительной части [7].

Обязательное условие использования защищенной БД – наличие подключенного к компьютеру вычислительного устройства (электронного ключа).

Этапы технологического процесса производства и эксплуатации аппаратно-программных средств защиты больших БД от несанкционированного копирования.

Настройка готового устройства. При настройке устройства необходимо выполнить над ключом несколько операций: генерация связки ключей типа открытый-закрытый; проверка на уязвимость сгенерированной пары ключей; расчёт параметров инициализации криптосистемы с использованием специализированного ПО.

Успешное завершение этих операций позволяет гарантировать криптостойкость выбранных параметров криптосистемы, от которых зависит уровень защищенности всей БД.

Запись рассчитанных значений в электронный ключ. Это один из наиболее уязвимых этапов при изготовлении секретного ключа, так как существует возможность перехвата его значений. Реализация определённых организационных мер в рамках предлагаемого способа, а также полная автоматизация процесса генерации требуемых значений и последующей их записи в ключ устраняет эту уязвимость. Альтернативным вариантом является генерация параметров криптосистемы, а также связки открытый-закрытый ключ внутри устройства что полностью исключает возможность перехвата. Однако существует вероятность генерации уязвимых параметров криптосистемы к методам криптоанализа и прямого перебора.

Создание защищенных БД. На этапе создания защищённой БД решаются несколько очень важных задач: выбор полей для защиты; разработка ПО с учетом использования защиты БД; шифрование готовой БД; проверка работоспособности готового продукта.

Выбор полей для защиты. Поскольку современные несимметричные криптоалгоритмы обладают сравнительно невысокой скоростью шифрования, их использование для шифрования всей БД очень накладно и малопроизводительно. В этом случае целесообразно зашифровать только некоторые поля БД, представляющие особый интерес для злоумышленника, а также несущие основную информационную нагрузку. Выбор таких полей целиком зависит от разработчика БД и требует особой тщательности. После составления списка полей, подлежащих шифрованию, разработчик переходит к следующей процедуре.

Разработка ПО с учетом использования защиты БД. При разработке ПО необходимо организовать обмен между ключом и БД, используя набор специализированных функций для работы с ключом. При любом запросе содержи-

мое зашифрованных полей БД передается в ключ с флагом соответствующей операции.

Шифрование готовой БД. После создания БД осуществляется шифрование выбранных полей. Оно может выполняться двумя способами – с использованием готового устройства или с помощью встроенного ПО, открытого ключа и параметров инициализации криптосистемы, считанных из готового устройства.

Проверка работоспособности готового продукта. После шифрования БД необходимо выполнить окончательную проверку работоспособности готового программного продукта в связке с ключом.

Особенности использования технологии. Особенностью предлагаемой технологии защиты является то, что подготовленная БД не может работать без электронного ключа, установленного в порту ввода-вывода компьютера. Соответственно и любая физическая копия БД вместе с необходимым ПО тоже неработоспособна. Наиболее уязвимым в данной технологии защиты является сам электронный ключ, так как его утрата или поломка приводит к неработоспособности исходной БД, а его хищение вместе с копией БД позволяет злоумышленнику использовать БД в своих целях.

Заключение. Предлагаемая технология позволяет организовать защиту больших БД от несанкционированного копирования, а вместе с определёнными организационными мерами минимизировать риск использования БД злоумышленником в своих целях. При этом следует учесть, что для задачи защиты БД от несанкционированного доступа к данным следует использовать технологии построения систем разграничения прав доступа к БД. Такая интеграция разных технологий позволяет существенно повысить защищённость БД от разнообразных угроз. Использование аппаратного устройства для шифрования позволяет минимизировать угрозы использования программных уязвимостей и архитектурных недостатков СУБД для считывания информации из БД.

1. *Зенкин Д.* Офисные предатели опаснее хакеров. http://www.cnews.ru/newcom/index.shtml?2004/11/01/167428
2. *Сабанов А.* О дополнительных возможностях защиты данных в среде СУБД Oracle9i.http://www.bytemag.ru/Article.asp?ID=3861
3. *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.
4. *Саломаа А.* Криптография с открытым ключом. – М.: Мир, 1996. – 318 с.
5. *Защита* сетевого периметра: Пер. с англ. / С. Норткатт, Л. Зелстер, С. Винтерс и др. – Киев: ООО ТИД «ДС», 2004. – 672 с.
6. *Черемушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.
7. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
8. *Конноллн,Томас, Бегг, Карелии.* Базы данных. Проектирование, реализация и сопровождение. Теория и практика: 3-е изд. : Пер. с англ. – М.: Издательский дом "Вильяме", 2003. – 1440 с.

Получено 23.02.2006