УДК 004.089

А.Л. Додохов, А.Г. Сабанов

К вопросу о защите персональных данных с использованием СУБД Oracle

Рассмотрена задача возможности применения СУБД Oracle для хранения и обработки персональных данных. Разработан метод шифрования конфиденциальной информации в соответствии с ГОСТ 28147–89.

Ключевые слова: СУБД Oracle, шифрование, персональные данные.

В настоящее время в связи с вступлением в силу Федерального закона от 25 июля 2011 г. №261-ФЗ «О внесении изменений в Федеральный закон №152-ФЗ «О персональных данных» вопросу разработки практических методов защиты персональных данных (ПДн) уделяется повышенное внимание.

Как известно, самые большие базы данных, содержащие персональные данные (ПДн), используют промышленные масштабируемые СУБД. Одной из самых распространенных в России является СУБД Oracle. Как показано в работе [1], эта СУБД имеет в настоящее время самые развитые встроенные сервисы безопасности в сравнении с другими СУБД, однако встроенные средства шифрования не удовлетворяют требованиям российского законодательства и для защиты ПДн необходима разработка наложенных средств в соответствии с ГОСТ – 28147–89, глубоко интегрированных с безопасными сервисами, заложенными вендором. Как известно, разработка таких решений является сложной задачей, поскольку к ним одновременно предъявляются повышенные и противоречащие друг другу требования как по производительности, так и по безопасности – для задачи шифрования бах данных давно известна зависимость: чем лучше зашифрованы данные, тем больше падает производительность вычислений с данными.

В данной работе приводится метод построения решения по защите персональных данных на платформе Oracle в соответствии с требованиями российского законодательства, который позволяет рассчитывать на его широкое практическое применение.

Постановка задачи. Одно из самых уязвимых мест при передаче, обработке и хранении персональных данных – это непосредственно базы данных (БД), где содержатся ПДн. Для БД известны следующие основные функции защиты информации:

- защита доступа – доступ к данным пользователь получает только при успешном прохождении им процедур идентификации и аутентификации;
- разграничение доступа – каждый пользователь, включая администратора, имеет доступ только к необходимой ему согласно занимаемой должности информации;
- шифрование данных – шифровать необходимо как передаваемые в сети данные для защиты от перехвата, так и данные, записываемые на носитель, для защиты от кражи носителя и несанкционированного просмотра/изменения нештатными средствами системы управления БД (СУБД);
- аудит доступа к данным – действия с критичными данными должны протоколироваться. Доступ к журналу не должны иметь пользователи, на которых он ведется.

Задачу данной работы можно сформулировать следующим образом: необходима разработка средства криптографической защиты конфиденциальной информации (не составляющей государственную тайну), при ее хранении в логической структуре реляционных таблиц на серверах баз данных. В качестве операционной среды для работы серверных компонентов рассматривается окружение сервера баз данных Oracle версий 9i, 10g, 11g. В качестве операционной среды для работы клиентских компонентов, как правило, используется операционная система Windows XP и выше.

Главным требованием к разрабатываемому решению является возможность его использования в существующих прикладных задачах без их существенной переделки.

Кроме этого, основными бизнес-задачами обеспечения безопасности при построении решения являются:

- разделение доступа и персонификация действий пользователей, это требование вытекает из требований закона [2] и рекомендаций [3];

• защита от администраторов СУБД и сетевого администратора, что объясняется тем, что, как правило, все крупные утечки из баз данных производятся злоумышленниками, получившими права администратора;

• прозрачность решения для существующих и разрабатываемых приложений;

• возможность предоставления защищенного удаленного доступа.

Основные рассматриваемые роли:

• администратор безопасности;

• администратор;

• привилегированный пользователь;

• пользователь;

• гость.

Архитектура предлагаемого решения. В основе предлагаемого решения лежит классическая клиент-серверная архитектура. Основные криптографические преобразования производятся на стороне сервера.

В процессе разработки метода предложенное в итоге решение получило название «средство криптографической защиты информации (СКЗИ) «Крипто БД». Схема реализации решения представлена на рис. 1.

СКЗИ «Крипто БД» является наложенным средством защиты, реализованным с использованием только документированных возможностей, предоставляемых СУБД Oracle. Криптографическое ядро СКЗИ реализовано на языке PL/SQL и Java, также штатно поддерживаемом сервером БД.

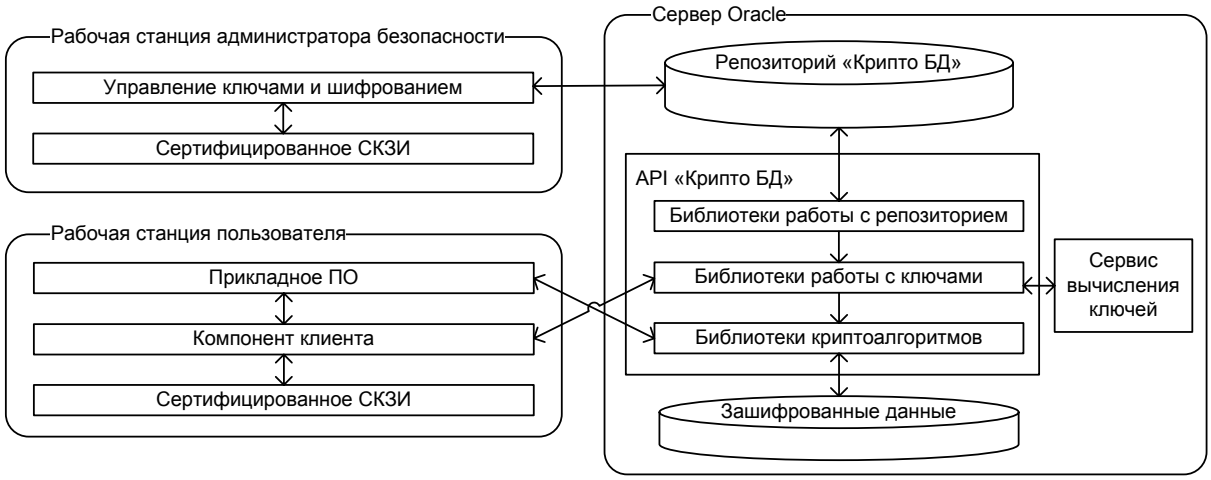

Рис. 1. Схема реализации СКЗИ «Крипто БД»

Основные компоненты СКЗИ «Крипто БД»:

• библиотеки, реализующие алгоритмы шифрования;

• библиотеки работы с ключами шифрования;

• сервис вычисления ключей шифрования;

• библиотеки работы с репозиторием;

• библиотеки и утилиты для управления ключами шифрования;

• библиотеки и утилиты для зашифрования и расшифрования.

Архитектура СКЗИ «Крипто БД» реализует хранение ключевой информации таким образом, что среда функционирования криптосредства (СФК) не имеет к этой информации непосредственного доступа. Ни один из компонентов СКЗИ «Крипто БД» не передаёт другому компоненту ни ключи шифрования в явном виде, ни адреса этих объектов. Вместо этого используются идентификаторы соответствующих ключей, не содержащие их адреса.

Применение СКЗИ «Крипто БД». СКЗИ «Крипто БД» предназначено для использования в существующем и во вновь разрабатываемом прикладном программном обеспечении.

Взаимодействие приложения и серверного компонента «Крипто БД». Общая схема работы приложения, которое использует зашифрованные с помощью СКЗИ «Крипто БД» данные, приведена на рис. 2.

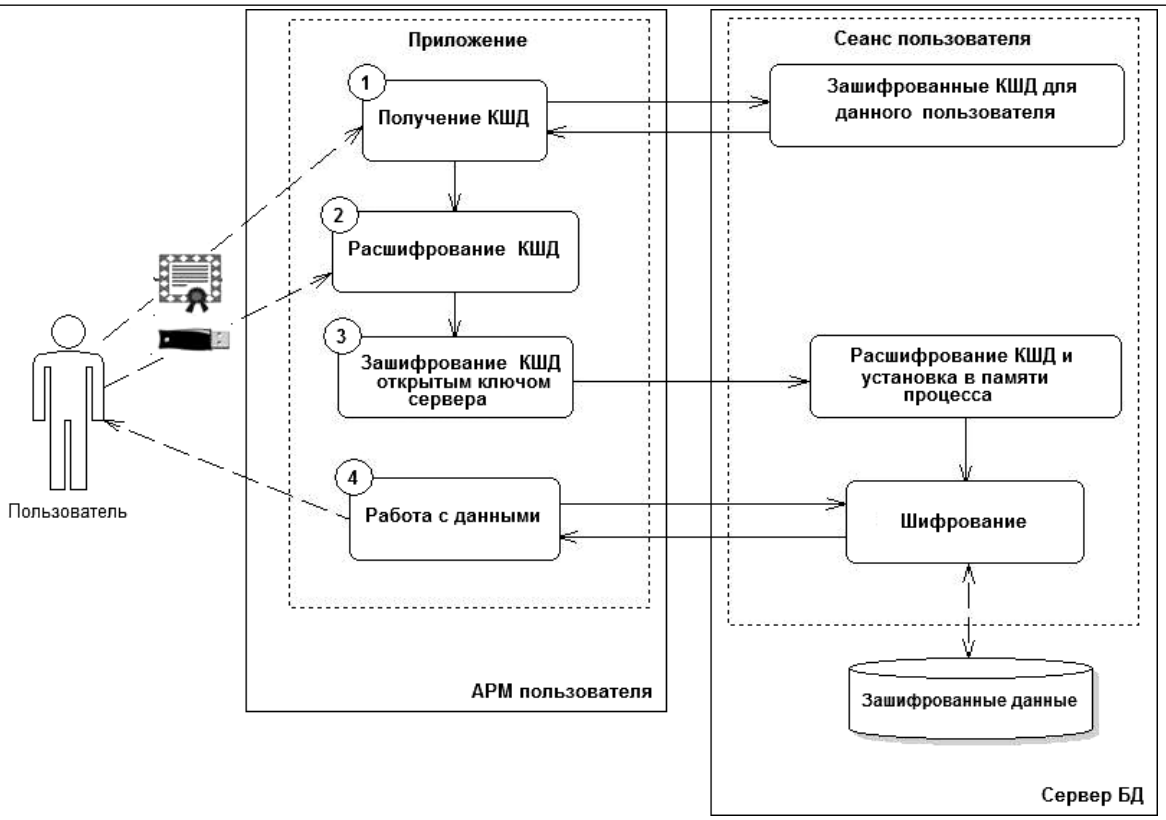

Рис. 2. Схема работы приложения с зашифрованными данными средствами СКЗИ «Крипто БД»

После успешной аутентификации и авторизации пользователя приложения на сервере БД создаётся процесс в памяти (сеанс пользователя БД), который обеспечивает взаимодействие приложение клиента – сервер БД. В этот момент компонент клиента «Крипто БД» (см. рис. 1) выполняет следующие действия (нумерация в соответствии с рис. 2):

1. Получение зашифрованных ключей шифрования данных (КШД):

• определяется факт подключения смарт-карт или USB-ключей (далее по тексту – смарт-карты) к АРМ пользователя;

• читается список сертификатов на подключенных смарт-картах;

• извлекаются зашифрованные КШД из репозитория «Крипто БД» (см. рис.1) с использованием в качестве идентификатора пользователя его сертификата;

• каждый КШД передаётся вместе с открытым ключом сервера БД и случайным числом (вырабатывается сервисом вычисления ключей (см. рис. 1), которые также зашифрованы открытым ключом соответствующего сертификата пользователя.

2. Расшифрование КШД:

• полученные зашифрованные значения КШД, открытый ключ сервера и случайное число расшифровываются компонентом клиента с использованием стандартного интерфейса, реализованного соответствующим поставщиком криптографии, установленным на АРМ пользователя (см. рис. 1). На данном этапе производится дополнительная авторизация пользователя (ввод PIN-кода смарт-карты) для получения доступа к закрытому ключу.

3. Зашифрование КШД на отрытом ключе сервера:

• непосредственно после расшифрования КШД, открытого ключа сервера, случайного числа, КШД зашифровывается на открытом ключе сервера БД. Полученное значение и расшифрованное случайное число передаются сервису вычисления ключей (см. рис. 1);

• сервис вычисления ключей идентифицирует сеанс обмена ключами, используя полученное значение случайного числа. Далее, закрытым ключом сервиса КШД расшифровывается и кэшируется в сеансе пользователя.

4. Работа с зашифрованными данными:

• чтение и запись зашифрованных данных производится через слой промежуточных представлений, которые реализуют вызовы API "Крипто БД. Промежуточные представления автоматически создаются «Крипто БД» в момент первичного зашифрования таблиц.

Основные характеристики СКЗИ «Крипто БД»

Размеры ключей.

Размеры ключей для защиты ключей шифрования:

- закрытый ключ – 256 бит;
- открытый ключ – 512 бит (ГОСТ Р 34.10–2001).

Размеры ключей шифрования – 256 бит.

Реализованные алгоритмы криптографического преобразования

Реализован алгоритм криптографического преобразования, соответствующий ГОСТ 28147–89, в режимах:

- простой замены (ECB);
- гаммирования (OFM);
- гаммирования с обратной связью (CFB);
- сцепления блоков (CBC);
- простой замены с диверсификацией ключа шифрования (ECB-UKM);
- гаммирования с диверсификацией ключа шифрования (OFB-UKM);
- гаммирования с обратной связью с диверсификацией ключа шифрования (CFB-UKM);
- сцепления блоков с диверсификацией ключа шифрования (CBC-UKM);
- простой замены с выработкой имитовставки (ECB-MAC);
- гаммирования с выработкой имитовставки (Counter mode-MAC);
- гаммирования с обратной связью и выработкой имитовставки (CFB-MAC);
- сцепления блоков с выработкой имитовставки (CBC-MAC);
- простой замены с диверсификацией ключа шифрования и выработкой имитовставки (ECB-MAC-UKM);
- гаммирования с диверсификацией ключа шифрования и выработкой имитовставки (OFB-MAC-UKM);
- гаммирования с обратной связью, с диверсификацией ключа шифрования и выработкой имитовставки (CFB-MAC-UKM);
- сцепления блоков с диверсификацией ключа шифрования и выработкой имитовставки (CBC-MAC-UKM).

Совместимость предлагаемого решения с программным обеспечением других разработчиков. СКЗИ «Крипто БД» совместимо с ПО, в котором реализованы российские криптографические алгоритмы, поддержка сертификатов открытых ключей X.509 и защищённый обмен сообщениями (CMS) в соответствии с документами RFC 4357, 4490 и 4491.

Архитектура предлагаемого решения, применение в нем только промышленных решений, открытых стандартов и рекомендаций, а также выполненные пилотные проекты в ряде государственных структур позволяют предполагать, что в более 80% случаев интеграция данного решения с ПО сторонних разработчиков будет проходить в «прозрачном» режиме, т.е. не потребует доработок программного обеспечения при внедрении в существующие информационные системы.

Заключение. Встроенные в СУБД Oracle алгоритмы криптографии, применяемой для защиты данных, ключей шифрования, контроля целостности, не соответствуют требованиям законодательства РФ. Встраивание внешних криптоалгоритмов разработчиками Oracle не предусмотрено. Для применения СУБД Oracle для защиты персональных данных разработан метод наложенных средств шифрования, использующий алгоритмы ГОСТ 28147–89. Данный метод может быть использован для защиты конфиденциальных данных, в частности персональных данных. Предложенное решение в виде СКЗИ «Крипто БД» успешно прошло сертификацию по требованиям ФСБ России к СКЗИ класса КС1 (исполнение 1) и КС2 (исполнение 2). Согласно полученному сертификату соответствия СФ/124-1569 данное СКЗИ может использоваться для криптографической защиты информации, не составляющей государственную тайну, хранящейся в таблицах баз данных под управлением СУБД Oracle.

Литература

1. Додохов А.Л. Исследование применения СУБД Oracle для защиты персональных данных/ А.Л. Додохов, А.Г. Сабанов// Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – №2(24). – С. 267–270.

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в ред. от 25 июля 2011 г.) [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/ cgi/online.cgi?req=doc;base=LAW;n=117587, свободный (дата обращения: 02.10.2012).

3. Нормативно-методический документ ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 г. [Электронный ресурс]. – Режим доступа: http://www.fz152.ru/media/files/laws/07-2-fsb/mr.doc, свободный (дата обращения: 02.10.2012).

Додохов Александр Леонидович
Руководитель направления защиты баз данных ЗАО «Аладдин Р.Д.», Москва
Эл. почта: a.dodokhov@aladdin-rd.ru
Тел.: 8-903-585-94-34

Сабанов Алексей Геннадьевич
Канд. техн. наук, заместитель генерального директора ЗАО «Аладдин Р.Д.»
Эл. почта: a.sabanov@aladdin-rd.ru
Тел.: 8-985-924-52-09

Dodokhov A.L., Sabanov A.G.

On the issue of personal data protection by means of Oracle database

The opportunity of Oracle Data Base use for data privacy storing and processing is investigated. The confidential information encrypting method in accordance to GOST 28147-89 is designed.

Keywords: Oracle Data Base, encryption, data privacy.
