Российские криптоалгоритмы в среде ORACLE – решение задач по защите персональных данных

В статье представлено одно из первых российских решений, обеспечивающих управление ключами шифрования и криптографическую защиту данных в СУБД Oracle, в соответствии с требованиями российского законодательства.

Александр Додохов – руководитель направления защиты баз данных, компания Aladdin

Ника Комарова – руководитель направления маркетинговых коммуникаций и PR, компания Aladdin

Введение

Использование систем управления базами данных зарубежного производства в свете реализации требований законодательства по защите персональных данных (ПДн) грозит обернуться серьезной проблемой. Согласно отчету IDC[1], в настоящее время на рынке реляционных СУБД лидирует корпорация Oracle, контролирующая 44,3% соответствующего сегмента. По некоторым оценкам, масштаб использования ПО Oracle только в российском госсекторе приближается к 80%. Обеспечение защиты информации, хранящейся в таких базах данных, сегодня становится едва ли не самой приоритетной задачей для подавляющего большинства государственных структур и организаций крупного корпоративного сегмента.

Итак, задача поставлена, но как ее решать? Попробуем проанализировать сложившуюся ситуацию и представить вариант выхода из нее.

В типичной СУБД западного образца настройка ролей пользователей по умолчанию, как правило, не соответствует реальным должностным обязанностям сотрудников. Это может привести к некорректному распределению полномочий, избыточность которых чревата утечкой конфиденциальных данных.

В Европе и США проблему утечки данных, в основном, решают с помощью механизмов защиты, встраиваемых в прикладное ПО, через которое пользователь работает с СУБД. Отечественный разработчик прикладного ПО редко задается подобными вопросами. В этой связи у владельцев ИТ-системы с интегрированной СУБД есть по большому счету три пути. Первый – ничего не делать и ждать скандала после утечки конфиденциальных данных. Второй – перекроить свою систему, фактически выстроив ее с нуля. И третий – самый желанный – обойтись малой кровью и кастомизировать используемую систему. В свете приближения 1 января 2010 г., когда все информационные системы, оперирующие персональными данными, должны быть приведены в соответствие требованиям Федерального Закона "О персональных данных", прикладное решение этой задачи может обернуться серьезной головной болью для большинства крупных операторов ПДн.

Представители регуляторов постоянно говорят о том, что никаких особенных продуктов для защиты ПДн не потребуется: арсенал уже представлен на рынке. Однако технические и программные средства защиты информации (СЗИ) должны удовлетворять нормативным требованиям, т.е. пройти соответствующую процедуру в системах сертификации ФСТЭК. Если мы имеем дело с высоким классом ИСПДн, то речь уже идет об обязательном применении средств криптографической защиты (СКЗИ), причем на базе ГОСТ. При использовании СКЗИ сертификацию предстоит пройти уже по линии ФСБ России, а в этом случае, при всем богатстве выбора альтернативного криптоалгоритма, удовлетворяющего требованиям регулятора, нет. Сама же реализация требований по обеспечению безопасности информации в средствах защиты возлагается на их разработчиков.

Что остается делать операторам персональных данных? Желающих заменить исправно функционирующую "буржуйскую" СУБД аналогичной системой отечественной разработки найдется немного. Тому есть немало веских причин, начиная от отсутствия прямого "товара-заменителя" и заканчивая нерентабельностью такого проекта. Между тем, все СУБД зарубежных разработчиков созданы с учетом международных стандартов и там, где это требуется, используют западную криптографию на базе DES, 3DES, AES и др. Это создает весьма туманные перспективы для их аттестации, согласно требованиям Федерального Закона "О персональных данных" и нормативной базы за авторством ФСТЭК и ФСБ.

Не все одинаковые

Твердая позиция государства в отношении обеспечения защиты персональных данных граждан за короткое время привела к формированию новообразовавшегося сегмента рынка "средств защиты персданных". В основном на нем представлены в срочном порядке перепозиционированные решения, "заточенные" под выполнение требований регуляторов, а также давно знакомые продукты, спешно прошедшие сертификацию

*) IDC "Worldwide Embedded Database Management Systems 2008 Vendor Shares".

в соответствующих центрах. Непростая экономическая ситуация и непредсказуемость ряда бизнес-процессов не способствуют инвестированию в разработку новых программных и аппаратных средств для удовлетворения спроса, разжигаемого приближающимся часом икс. Иной подход демонстрируют немногие компании. Одна из них – компания Aladdin, с 2004 г. занимающаяся разработкой решений для защиты данных в среде Oracle.

Как и следовало ожидать, система защиты для БД Oracle разработки Aladdin базируется на флагманском продукте компании – eToken, ключевом носителе в формате USB-устройства. Сертифицированное по линии ФСБ новое СКЗИ получило название "Крипто БД". Система предназначена для работы со всей линейкой Oracle Database Server 9i, 10g и 11g, потенциально оперирующих персональными данными в российских организациях коммерческого и государственного секторов. Какие задачи выполняет eToken "Крипто БД"? Это:

- *разграничение доступа* – каждый пользователь, включая администратора, может иметь доступ только к необходимой ему информации согласно занимаемой должности;
- *защита доступа* – доступ к данным может быть предоставлен пользователю только после успешного прохождения процедур идентификации и аутентификации;
- *шифрование данных* – для защиты от перехвата шифровать необходимо данные, передаваемые по сети, а также данные, записываемые на носитель; защита самого носителя от кражи и несанкционированного просмотра/модификации, хранимых в его памяти данных, осуществляется иными средствами вне системы управления БД;
- *аудит доступа к данным* – действия с критичными данными должны протоколироваться. Доступ к протоколу не должны иметь пользователи, на которых он ведется.

Таким образом, eToken "Крипто БД" представляет собой сертифицированное решение, интегрирующее основные компоненты защиты БД. Применение СКЗИ eToken "Крипто БД" обеспечивает соблюдение норм законодательства РФ и требований руководящих документов, определяющих состав мер и технических средств, для защиты информационных систем обработки персональных данных. Построение защиты в СУБД Oracle на базе продукта реализует выполнение требований для ИСПДн К2 до уровня защиты 1Г включительно. К этим требованиям относятся:

- идентификация, проверка подлинности и контроль доступа субъектов в систему;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрация и учет входа (выхода) субъектов доступа в (из) систему (узел сети);
- контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- периодическое тестирование СЗИ, восстановление СЗИ.

Иные уровни защиты могут быть достигнуты при усилении eToken "Крипто БД" дополнительными средствами обеспечения информационной безопасности.

Особенности eToken "Крипто БД"

eToken "Крипто БД" – это полноценное средство криптографической защиты информации, предназначенное для применения в государственных структурах и корпорациях, где эксплуатируется множество унаследованных приложений, с которыми необходимо интегрировать систему защиты. Архитектура решения такова, что СКЗИ функционирует в среде сервера базы данных, что позволяет защитить информационные системы персональных данных, независимо от их архитектуры – защита реализована на уровне доступа к колонкам таблиц БД. Что касается взаимодействия с ПО Oracle, СКЗИ eToken "Крипто БД" функционирует в нем на прикладном уровне, не нарушая целостности программного обеспечения Oracle, что полностью соответствует условиям лицензионного соглашения производителя СУБД.

Внедрение СКЗИ eToken "Крипто БД" позволяет расширить возможности встроенных в СУБД Oracle подсистем идентификации, аутентификации и шифрования данных. Так, штатные функции СУБД в части подтверждения подлинности аутентификационных данных для предоставления доступа к тем или иным ресурсам, в основном ориентированы на управление правами непривилегированных пользователей. Администраторы же имеют фактически неограниченные возможности для доступа к любой интересующей их информации. При подобном подходе возникает риск превышения должностных полномочий и появления угрозы утечки информации вследствие инсайдерских действий. Причем, в случае возникновения инцидента, отследить действия инсайдера и доказать его причастность к нарушению политики информационной

Рис. 1. Сертифицированный ключевой носитель eToken PRO, реализованный на базе технологий смарт-карт.

безопасности, практически невозможно, поскольку штатные средства СУБД не позволяют проводить аудит действий привилегированных пользователей.

"Надстройка" в виде системы строгой аутентификации на базе Aladdin eToken повышает уровень информационной безопасности путем разграничения доступа к данным, согласно должностным обязанностям и полномочиям как обычных групп пользователей, так и привилегированных – администраторов.

Аналогичный подход по усилению имеющегося функционала СУБД реализуется и в подсистеме шифрования. Специфика использования СУБД Oracle связана с обработкой и хранением огромного массива постоянно обновляемых и дополняемых данных. Шифрование всей этой информации в "нагруженной" СУБД вносит ощутимые задержки в работу с ней и существенно увеличивает нагрузку на аппаратные ресурсы. Адекватной альтернативой является технология селективного (выборочного) шифрования, что позволяет защищать только одну или несколько колонок таблицы. Используя eToken "Крипто БД" можно оставить доступными для всех групп пользователей колонки таблицы, содержащие имя и фамилию сотрудника, а информацию о его расовой принадлежности или, скажем, состоянии здоровья – зашифровать. Это обеспечит конфиденциальность данных и "освободит" от излишней нагрузки серверные мощности.

Поднятая проблема отслеживания действий администраторов решается с помощью системы аудита eToken "Крипто БД", предоставляющей широкие возможности протоколирования. Вновь выполняя функции "надстройки" над штатными функциями СУБД, продукт позволяет анализировать и фиксировать все действия в сети, независимо от уров-

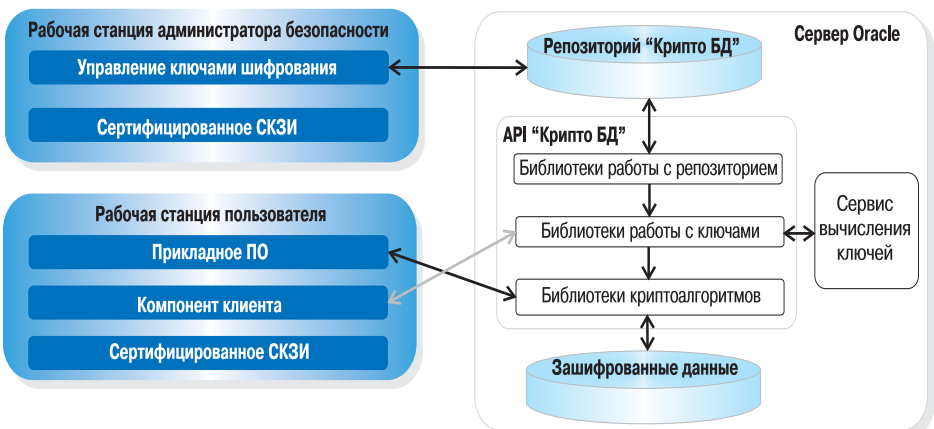

Рис. 2. Схема реализации СКЗИ "Крипто БД".

Рис. 3. Для каждого пользователя прикладной системы создается ключевая пара (открытый и закрытый ключи) при помощи ПО выбранного криптопровайдера.

ня привилегий. Статистические "срезы" активности администраторов и пользователей в дальнейшем могут применяться при служебных расследованиях инцидентов в области информационной безопасности, предоставляя доказательную базу при назначении штрафных санкций.

Состав решения и функционирование системы

Основу eToken "Крипто БД" составляет серверный компонент, устанавливаемый в БД, а также клиентский компонент, работающий под операционными системами Microsoft Windows XP или Vista. В системе используются три вида ключей – открытые, закрытые и симметричные. Длина открытого ключа составляет 512 бит (согласно ГОСТ Р 34.10-2001), закрытого – 256 бит. Для шифрования используется симметричный ключ длиной 256 бит. Для хранения ключей и сертификатов пользователей, имеющих право на доступ к системе, применяются сертифицированные ключевые носители eToken PRO, реализованные на базе технологий смарт-карт (рис 1).

eToken "Крипто БД" обладает встроенной системой шифрования и реализует криптоалгоритм ГОСТ 28147-89 в режимах простой замены (ECB), гаммирования (Counter mode), гаммирования с обратной связью (CFB) и сцепления блоков (CBC). Применение российских криптоалгоритмов для защиты персональных данных в Oracle реализуется благодаря поддержке криптопровайдеров Crypto Pro CSP компании "КриптоПро", Signal-COM CSP компании Сигнал-КОМ, МагПро CSP от "КриптоКом", а также Домен КС2 разработки фирмы "Инфотекс". К слову, для разработчиков предоставляется документированный программный интерфейс к функциям СКЗИ, реализующим шифрование, работу с ключами шифрования и репозиторием защищенных объектов.

Установка служб и приложений системы происходит на серверах баз данных Oracle, клиентских рабочих станциях пользователей, работающих со СКЗИ, а также на рабочей станции администратора безопасности, которая является важнейшим узлом в системе управления шифрованием данных (рис. 2). Для каждого пользователя прикладной системы создается ключевая пара (открытый и закрытый ключи) при помощи ПО выбранного криптопровайдера. Закрытый ключ при этом сохраняется на ключевом носителе, в роли которого выступает USB-устройство eToken (рис. 3). Принадлежность открытого ключа пользователю обеспечивается сертификатом, изданным для данного открытого ключа. В дальнейшем сертификат открытого ключа в виде файла используется администратором безопасности для защиты ключей ифрования, доступных для данного пользователя. Чтобы исключить любую возможность перехвата передаваемых по сети ПД, канал передачи данных между рабочей станцией пользователей и сервером БД должен быть защищен, а на самом ПК и сервере БД должны отсутствовать средства отладки и разработки, а также другое неавторизованное ПО.

Архитектура СКЗИ eToken "Крипто БД" подразумевает использование симметричного криптографического алгоритма общего ключа шифрования (ключ шифрования для одной колонки таблицы базы данных Oracle совпадает с ключом расшифрования). Ключи шифрования защищаются в соответствие с алгоритмом согласования ключей по ГОСТ 34.10-2001 на открытых ключах пользователей. Для получения доступа к конфиденциальным данным каждому пользователю информационной системы назначается персональный ключевой носитель eToken. В защищенной области памяти носителя надежно сохраняется ключевая информация пользователя, в том числе неизвлекаемый закрытый ключ и цифровые сертификаты. Хранение ключевой информации в отдельном адресном пространстве обеспечивает дополнительную защиту объектов СКЗИ от любой активности недоверенной среды рабочего места пользователя (пользовательских приложений, вредоносных программ и т.п.).

Использование специализированных ключевых носителей в комплексе с надежной системой шифрования, построенной на базе отечественной криптографии, позволяет минимизировать риск компрометации закрытого ключа, обеспечить неотрекаемость от совершенных пользователем действий и исключить риск утечки конфиденциальных данных. Даже если сам носитель будет украден, его наличие все равно не позволит злоумышленнику получить доступ к данным без знания PIN-кода ключа.

eToken совместим с большинством программных продуктов, и, в частности, успешно интегрируется с системами авторизации всех решений корпорации Microsoft, что позволяет говорить не только о защите одного или нескольких объектов, но и о переходе на систему однократной аутентификации (Single Sign On) для всех приложений, что делает процесс предоставления прав доступа одинаково безопасным на всех участках IT-инфраструктуры.

Кастомизация СУБД с помощью внедрения СКЗИ eToken "Крипто БД" на сегодняшний день является адекватным решением технической стороны задачи обеспечения соответствия ряду требований нормативной базы по защите персональных данных. Более того, на текущий момент – это фактически безальтернативное решение, полностью готовое к использованию. Подчеркнем, что применение СКЗИ eToken "Крипто БД" позволит реализовать технические меры защиты. Для обеспечения комплексного подхода, декларируемого руководящими документами, необходимо принять ряд организационных мер, а также подготовить соответствующую документацию, включающую разработку регламентов на обслуживание ИСПДн и ее эксплуатацию.

Один из вопросов, который может стоять при внедрении системы СКЗИ eToken "Крипто БД", – доля накладных затрат, требующихся при шифровании данных. Как показывает тестирование, в среднем, они не превышают 15–20%.

Вместо заключения – защита БД: перспективы развития

Как отмечают в своем отчете аналитики IDC, необходимость приведения систем в соответствие с положениями ФЗ-152 серьезно поддержит отрасль информационной безопасности. Без сомнения, выход Федерального закона РФ N152-ФЗ "О персональных данных" задает новый импульс к развитию систем комплексной защиты баз данных. Несмотря на то, что с момента обнародования закона прошло 3 года, большинство поставщиков услуг и продуктов в области защиты БД только начали активизироваться в этой области. Все больше решений проходит сертификацию, и все больше интеграторов предлагают услуги по аудиту на соответствие систем операторов ПД требованиям законодательства. На эти предложения постепенно появляется устойчивый спрос, и чем ближе 1 января 2010 г., тем выше он будет.

Появление защищенных систем хранения и обработки ИСПДн, полностью соответствующих букве закона и нормативной базе, это не прогноз на будущее – это требование сегодняшнего дня. Технологии, удовлетворяющие потребности операторов персональных данных, независимо от масштаба организации, отрасли и специфики деятельности, уже присутствуют на рынке. И, если отбросить домыслы относительно переноса сроков по исполнению требований ФЗ-152, трезво оценить время, оставшееся на подготовку собственной информационной системы к аттестации, – станет ясно, что тянуть уже нельзя. Пора действовать. Чем позже отдельно взятый оператор ПД это осознает, тем сложнее будет его задача и тем дороже ее решение.

Александр Додохов,
руководитель направления защиты баз данных, компания Aladdin

Ника Комарова,
руководитель направления маркетинговых коммуникаций и PR, компания Aladdin