Аладдин РД
www.aladdin-rd.ru

Защита информации в базах данных

Система обеспечения безопасного доступа и хранения персональных данных с хранением ключевой информации на электронных ключах и смарт-картах

Справочная информация

для специалистов
по информационной
безопасности и ИТ

Оглавление

Термины, определения и сокращения

№	Термин/определение	Описание
1	«Крипто БД»	Наименование продукта
2	Прикладное ПО	ПО, использующее информацию из колонок таблиц, защищенную с помощью «Крипто БД»
3	БД / БД Oracle	База данных, база данных Oracle.
4	ПДн, ИСПДн	Персональные данные (в рамках определения в ФЗ-152), информационная система обработки персональных данных
5		

Назначение «Крипто БД»

Средство криптографической защиты «Крипто БД» предназначено для обеспечения конфиденциальности информации с помощью криптографического преобразования, а также для контроля целостности с помощью выработки и проверки имитовставки.

Основные характеристики

- Реализация алгоритма ГОСТ 28147-89 в различных режимах для шифрования колонок таблиц на сервере БД;
- Реализация механизма управления ключами шифрования данных;
- Дискретная и мандатная модели разделения доступа;
- Контроль целостности собственного ПО и служебной информации;
- Аудит и мониторинг доступа к зашифрованным данным;
- Консоль управления шифрованием, ключами, пользователями, аудитом и т.д.

Область применения «Крипто БД»

- Информационные системы с приложениями «Клиент-сервер»
    - возможно прозрачное встраивание в 95% ИСПДн
- Многозвенные приложения информационных систем
    - требуется дополнительный анализ ИСПДн в зависимости от потребностей заказчика
- Терминальный доступ

        - возможно прозрачное встраивание в 95% ИСПДн
- Автоматические процессы
        - прозрачное встраивание
- Облачные системы (IaaS, SaaS)
        - прозрачное встраивание (применение шифрующего прокси)

Ограничение применения

- Криптографическая защита по классам КС1, КС2;
- Не применимо для защиты гостайны;
- ОС сервера БД Oracle:
    - MS Win 2003/2008, RHE Linux, SLES Linux, IBM AIX, HP-UX, Oracle Solaris (Intel/SPARC), IBM z SLES Linux;
- ОС клиента:
    - MS Win XP/Vista 32/64 бит;
- Версии сервера Oracle Database:
    - 9i, 10g, 11g (SE/SE1/EE);
- Деградация производительности (время отклика) 5-35%;
- Не поддерживается шифрование индекс-организованных таблиц;
- Не поддерживаются объектные типы данных, типы данных LONG, LONG RAW, BFILE;
- Индексирование только по строгому совпадению;
- Не работоспособно в кластерных конфигурациях Oracle (Real Application Cluster).

Сертификация

СКЗИ «Крипто БД» имеет сертификат соответствия ФСБ по классам защиты КС1, КС2 № СФ/124-1569, действительный до 06.11.2013 г.

Использование «Крипто БД» в облачных средах

Для защиты ПДн в системах, предоставляющих "облачные" сервисы, использование функциональности «Крипто БД» также возможно. Для облачной инфраструктуры - IaaS - (например, хостинг СУБД Oracle) применение «Крипто БД» не отличается от традиционного. Для сервисов SaaS требуется применение дополнительного компонента - шифрующего прокси.

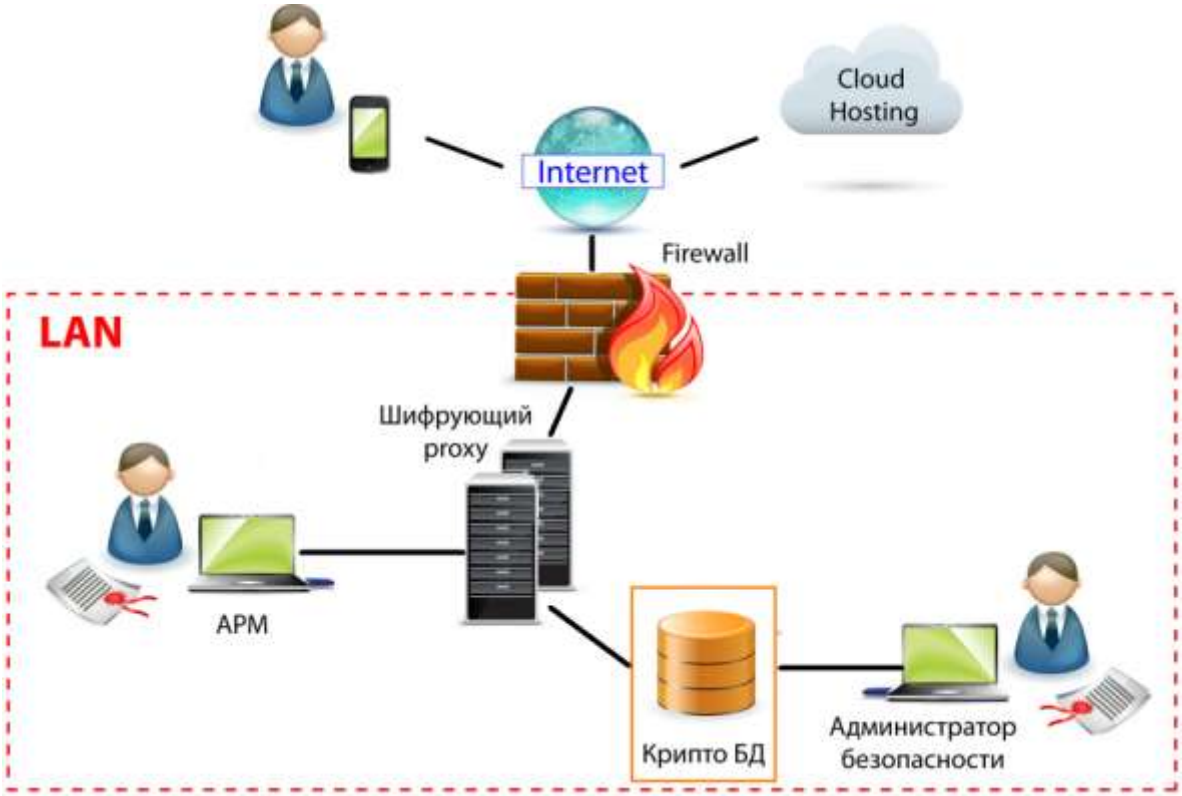
Шифрующий прокси

Шифрующий прокси предназначен для защиты информации (ПДн) для приложений, развёрнутых в облаке. Для таких приложений характерны следующие особенности:

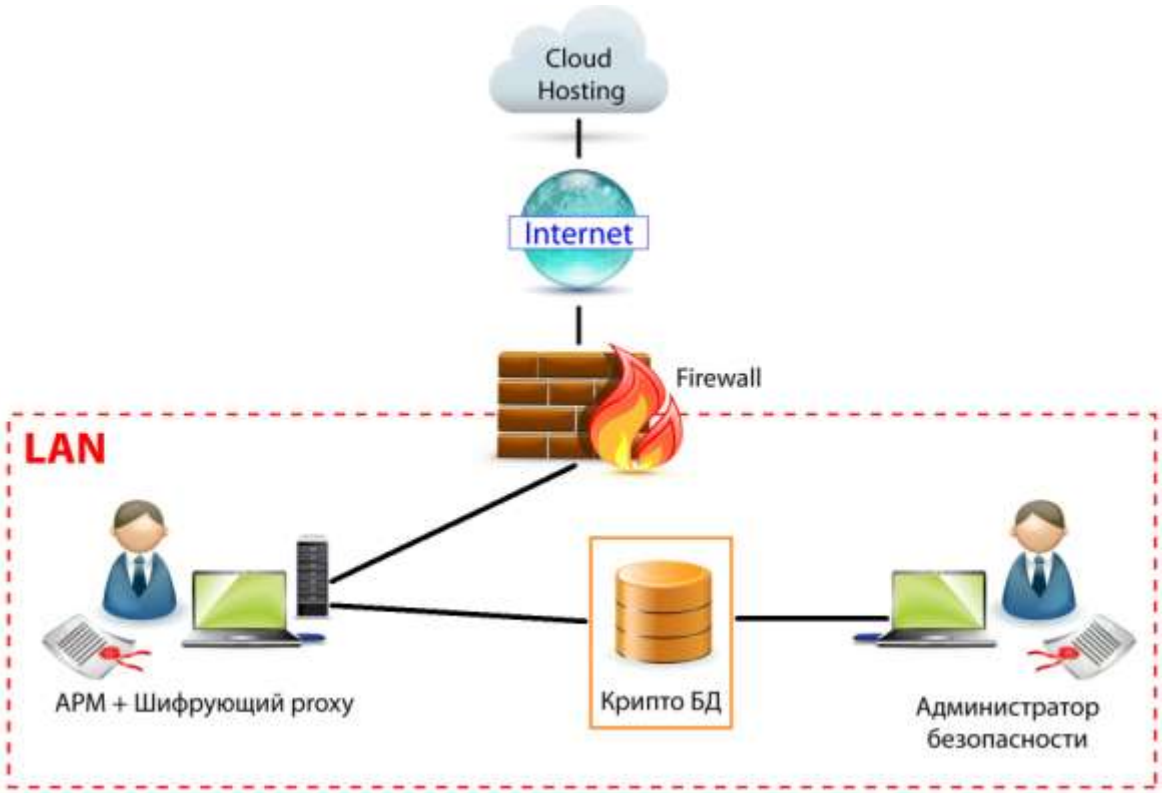
- невозможно развёртывание какого-либо ПО, не предусмотренного данным приложением;
- неизвестна структура и способ хранения информации;
- полный контроль за хранящейся информацией имеет хостер данного сервиса;
- интерфейс пользователя формируется интернет-браузером.

Шифрующий прокси функционирует в локальной сети клиента облачного сервиса и "на лету" расшифровывает / зашифровывает данные поступающие / отправляемые браузером пользователя. Для операций шифрования, управления ключами шифрования, разделением доступа используется инфраструктура ПО «Крипто БД», также установленного в локальной сети. Таким образом, управление информацией, составляющих ПДн, ключами и другой критичной информацией осуществляется в пределах контролируемого периметра организации. На хранение и обработку в облако передаются обезличенные данные, хостер не имеет доступа к ключам шифрования и передача данных может осуществляться по незащищённым каналам. Такой подход полностью соответствует требованиям регуляторов в части защиты ИСПДн. Ниже приведены две схемы использования шифрующего прокси для использования совместно с приложениями SaaS.

Шифрующий прокси в режиме шлюза



Шифрующий прокси в режиме клиента



Техническое описание «Крипто БД»

«Крипто БД» представляет собой программно-аппаратный комплекс для обеспечения усиления функций безопасности при:

- хранении информации, предназначенной для прикладного ПО, в таблицах базы данных;
- аудите доступа к информации, предназначенной для прикладного ПО.

Структурно программно-аппаратный комплекс «Крипто БД» состоит из следующих компонентов:

- набор программных модулей «SecurLogon для Oracle»;
- пакет хранимых процедур сервера БД;
- консоль Администратора безопасности и инсталлятор объектов (eToken «Крипто БД»);
- электронный ключ в форм-факторе USB-ключа или смарт-карты с набором драйверов.

Модуль «SecurLogon для Oracle»

Предназначен для использования приложениями, построенными по двухуровневой (клиент-сервер) архитектуре. Основной функцией модуля является обеспечение доступа со стороны клиентского программного обеспечения 0racle9i/10g/11g Database Client for Windows 2000/XP/Vista/7 к хранилищу сертификатов, расположенному на электронном ключе, а также вычисление и установка ключей шифрования. Модуль устанавливается на клиентских рабочих станциях и функционирует на них как служба операционной системы.

Пакет хранимых процедур сервера БД

Предназначен для обработки запросов клиентских приложений при доступе к защищенной информации, хранящейся в таблицах БД Oracle. Устанавливается непосредственно на сервере БД Oracle в виде пакета хранимых процедур, написанных на процедурном языке СУБД PL/SQL и Java, и может использоваться приложениями, имеющими как двух - (клиент-сервер БД) так и трехуровневую (клиент - сервер приложений - сервер БД) архитектуру. Основными функциями, реализуемым пакетом хранимых процедур, является установка параметров сессии приложения, получение и передача ключей шифрования, вызов модулей, реализующих алгоритмы шифрования, и регистрация событий доступа к защищенным данным (аудит/мониторинг).

Консоль Администратора безопасности.

Предназначена для централизованного управления шифрованием данных, ключами шифрования, резервным сохранением и восстановлением ключей, настройками аудита.

Пользователи и роли

№	Роль пользователя	Описание
1	Обычный пользователь	Пользователь данной роли имеет легальный доступ к БД в рамках своих привилегий, установленных для него Администратором СУБД

2	Легальный пользователь	Пользователь данной роли имеет легальный доступ к БД в рамках своих привилегий, установленных для него Администратором СУБД, а также права на доступ к защищенным данным, установленными для него Администратором безопасности
3	Администратор ОС	Пользователь данной роли имеет полный доступ к ресурсам ОС, но не имеет доступа к БД (штатными средствами СУБД)
4	Администратор СУБД	Пользователь данной роли имеет полный доступ к ресурсам СУБД; к ресурсам ОС (файлы, порты и т.п.) - доступ в рамках объектов, составляющих инфраструктуру СУБД
5	Администратор безопасности	Пользователь данной роли имеет полный доступ к ресурсам СУБД, составляющим ПО системы. Доступа к данным прикладного ПО и системным ресурсам ОС и СУБД не имеет.

Описание функций системы

Группа	Описание
Общие	Общие функциональные возможности системы
Аутентификация	Безопасная аутентификация, хранение ключевой информации (сертификаты/ закрытые ключи)
Управление ключами	Генерация, передача, хранение ключей шифрования; создание резервных копий и восстановление ключей шифрования
Защита данных	Применение алгоритмов шифрования, управление шифрованием
Аудит/мониторинг	Организация аудита, ключи аудита, управление аудитом
Защита ПО	Защита ПО, составляющего систему, ключи шифрования, передача данных по сети

1. Общие функциональные возможности системы

1.1. Доступ к защищаемым системой данным.

Система должна обеспечить ограничение доступа к защищенным данным и данным аудита в соответствие с матрицей доступа, приведенной в таблице 1.1. Наличие доступа (+) означает возможность для роли доступа данного типа без нарушения штатного режима функционирования СУБД, ПО системы и прикладного ПО и получения информации из защищенных таблиц в открытом (расшифрованном) виде.

Таблица 1.1. Матрица доступа.

		Обычный пользователь	Легальный пользователь	Администратор ОС	Администратор СУБД	Администратор безопасности
	Чтение/изменение защищенной колонки в таблице БД	-	+	-	-	-
	Чтение/сбор данных аудита	-	-	-	-	+
	Чтение/изменение служебной информации, относящейся к системе (настройки аудита/мониторинга)	-	-	-	-	+

2. Аутентификация

Раздел требований	Описание
Аутентификация	Система поддерживает аутентификацию в СУБД следующими методами: - по имени пользователя и паролю - средствами ОС (Kerberos etc) - по протоколу SSL.
Хранилище ключевого материала	Поиск цифровых сертификатов, предназначенных для аутентификации по протоколу SSL, должен производиться только в физическом хранилище, ассоциированным со смарт-картой или USB-ключом.

3. Управление ключами

Генерация	Система должна обеспечить генерацию ключей шифрования различной длины, в соответствие с выбранным алгоритмом шифрования. Генерация должна производиться на рабочей станции Администратором безопасности, далее, ключи сохраняются здесь же после зашифрования на открытом ключе сертификата Администратора безопасности.
Случайные значения ключей	Для генерации ключей используется программный датчик случайных чисел, предусмотрена возможность использовать аппаратный генератор случайных чисел.
Привилегии для генерации ключей	Генерация ключей шифрования производится только пользователями с ролью Администратор безопасности.
Резервное копирование ключей шифрования	Система позволяет сохранять незашифрованные копии ключей шифрования в файле на рабочей станции Администратора безопасности, защищенном паролем. Предусмотрено также использование пороговой схемы 2/3.
Восстановление ключей шифрования	Система позволяет восстанавливать ключи шифрования из резервной копии, сохраненной в файле.
Хранилище мастер-ключей	Ключи шифрования хранятся на рабочей станции Администратора безопасности, зашифрованные на открытом ключе его сертификата пользователя.

Ключи пользователей	Для каждого из пользователей с ролью Легальный пользователь копии ключей шифрования хранятся зашифрованными на открытом ключе сертификата соответствующего пользователя. Идентификация копий ключей шифрования производится по отличительному имени (DN), извлекаемого из поля Subject сертификата пользователя, предъявленного при аутентификации.
Регистрация ключа шифрования	Система позволяет регистрировать ключи шифрования для пользователей, принимая в качестве идентификатора пользователя его сертификат (X.509) в виде файла. Идентификатор впоследствии может быть изменен на произвольный.
Пакетная регистрация ключа шифрования	Система позволяет регистрировать ключ шифрования для группы пользователей в пакетном режиме, принимая в качестве идентификатора пользователей их сертификаты (X.509) в виде файла (файлов).
Резервное копирование ключей шифрования пользователей	Система позволяет сохранять ключи шифрования пользователей в файле на рабочей станции Администратора безопасности.
Восстановление ключей шифрования пользователей	Система позволяет восстанавливать ключи шифрования пользователей из ранее сохраненного файла.
Удаление ключей шифрования пользователей	Система позволяет удалять ключи шифрования для пользователей по их идентификаторам. Операция удаления возможна в пакетном режиме.
Передача ключей шифрования	Ключи шифрования не существуют в расшифрованном виде ни в одном контексте, исключая защищенную сессию пользователя на сервере БД.
Условия передачи ключа шифрования	Расшифрованное значение ключа шифрования вычисляется на рабочей станции пользователя и передается в сессию БД после следующих событий: - успешной аутентификации - успешной проверки подлинности серверного ПО системы - успешного получения зашифрованной копии ключа шифрования - успешного зашифрования на открытом ключе сертификата сервера БД
Регистрация событий с вычислением ключей	Система отслеживает неудачные попытки вычисления ключей и фиксирует их в журнале событий на рабочей станции пользователя.

4. Защита данных и ПО системы

Алгоритмы	Система предоставляет возможность применения произвольных симметричных алгоритмов шифрования. Процедуры (процессы), реализующие симметричные алгоритмы шифрования, реализованы на стороне сервера БД и выполняются в контексте сервера БД.
Защита ПО системы	До использования системой процедуры, реализующие алгоритмы шифрования, проверяются на достоверность.
Служебная информация	Информация по защищенным таблицам/колонкам хранится в БД в схеме пользователя - Администратора безопасности.

5. Аудит/мониторинг

Настройки аудита	Информация, касающаяся установок аудита (таблица, колонка, операция, пользователи) хранится на рабочей станции Администратора безопасности.
Регистрация событий	Регистрацию событий и передачу данных аудита/мониторинга осуществляет пакет хранимых процедур в асинхронном режиме. Регистрации подлежат события доступа к данным, защищенным средствами ПО системы.
Сбор и обработка	Сбор данных аудита/мониторинга осуществляется процедурами-коллекторами, доступными для пользователя - Администратора безопасности.
Защита от несанкционированной модификации служебных объектов	Система осуществляет проверку целостности служебных объектов (промежуточных представлений и триггеров)

6. Защита ПО системы и лицензирование

Лицензирование	Работа системы возможна только при наличии на смарт- карте/USB-ключе установленной электронной лицензии.
Защита ПО	Чтение зашифрованных ключей и установка ключей шифрования возможно только после проверки целостности ПО системы
Модули, подлежащие контролю	Проверяется целостность следующих модулей системы: - пакеты хранимых процедур - процедуры, реализующие алгоритмы шифрования