Аладдин рд

"Крипто БД"

Система предотвращения утечек конфиденциальной информации из баз данных

- Надёжная гарантия конфиденциальности защищаемой информации
- Комплексная защита доступа и данных
- Разграничение доступа и аудит
- Возможность поэтапного внедрения решения без прерывания бизнес-процессов

Внесено в Единый реестр отечественного ПО для госзакупок

Задачи

Развитие сложных информационных систем, использование облачных сервисов, мобильная обработка данных и многие другие современные тенденции возможны только за счёт активного применения СУБД в основе архитектуры. Доля информационных систем, не использующих базы данных, стремится к нулю. Вместе с этим уровень сложности самих СУБД значительно повышается. В этих условиях существенно возрастают риски утечек конфиденциальной информации из СУБД. В потенциальную группу риска современной СУБД включены не только внешние злоумышленники, но и внутренние сотрудники, а также администраторы СУБД, обладающие максимальным набором прав доступа к конфиденциальной информации. При большом количестве пользователей в системе мониторинг и выявление возможных действий злоумышленника и персонализация ответственности за эти действия становятся сложными и дорогостоящими задачами. Возникает необходимость применения простых и эффективных методов защиты информации в СУБД.

Решение

"Крипто БД" представляет собой средство криптографической защиты информации (СКЗИ), обеспечивающее надёжное предотвращение утечек конфиденциальной информации, обрабатываемой СУБД.

Отечественное ПО

Решение является полностью отечественной разработкой, реализует поддержку российских стандартов криптографии и функционирует на распространённых платформах СУБД:

"Крипто БД" для СУБД Oracle;

"Крипто БД" для СУБД MS SQL;

"Крипто БД" для СУБД Tibero;

"Крипто БД" для Postgre SQL.

"Крипто БД" — это комплексная защита баз данных:

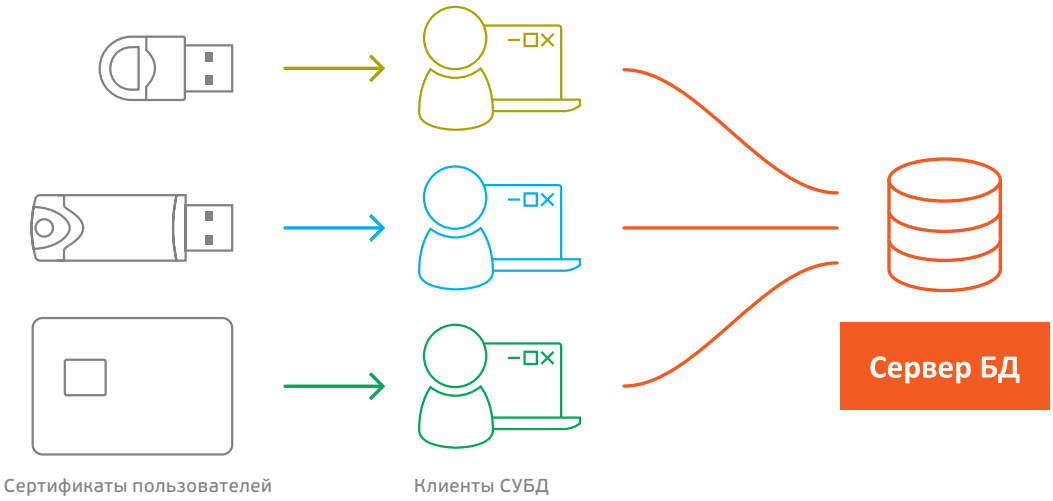
- защита данных в таблицах криптографическими методами;
- гибкое управление ключами шифрования;
- использование USB-ключей или смарт-карт для двухфакторной аутентификации пользователей;
- расширение возможностей разделения доступа к СУБД;
- мониторинг и аудит доступа к зашифрованным данным;
- прозрачная интеграция с большинством существующих приложений;
- поддержка клиент-серверных и многозвенных приложений.

Защита данных в СУБД с помощью шифрования кардинально снижает риски возможной кражи носителей информации, несанкционированного просмотра информации и её изменения. Такой метод также позволяет реализовать надёжное ограничение прав администраторов СУБД при попытках доступа к защищаемой информации. Безопасность защищаемых данных существенно повышается за счёт применения на клиентских рабочих станциях строгой двухфакторной аутентификации, с помощью аппаратных средств – USB-ключей или смарт-карт. Встроенный механизм аудита обеспечивает сбор данных, подтверждающих факты доступа к зашифрованной информации. Риск утечек конфиденциальной информации из СУБД существенно снижается, поскольку в ней невозможно работать под чужим именем, и все действия пользователя персонализируются и протоколируются (исключён фактор недоказуемости).

Общая схема работы

Приложение клиента на основании данных в сертификате получает доступ в определённую БД с соответствующими правами.

Если с помощью данного USB-ключа или смарт-карты вычислен ключ шифрования, зашифрованные данные будут доступны пользователю.



Преимущества использования

- Существенное повышение уровня информационной безопасности
- Надёжное предотвращение утечек конфиденциальной информации СУБД
- Возможность поэтапного внедрения решения без прерывания бизнес-процессов и усиление функций защиты информационных систем
- Соответствие решения требованиям законодательства
- Отсутствие затрат на управление паролями
- Возможность построения защищённых информационных систем как клиент-серверной, так и многозвенной архитектуры
- Защита данных и резервных копий от несанкционированного доступа (в том числе со стороны администраторов баз данных и операционных систем)
- Возможность формирования доказательной базы доступа к критичной информации на основании данных аудита

Системные требования

На клиентских рабочих местах

- Операционная система Microsoft Windows XP/Vista/7/8.1/10 (32/64 бит)
- Oracle Client 9.2 или выше, ODBC для Microsoft SQL Server или ADO.Net, Tibero Client 5 или выше
- Драйверы смарт-карт eToken PKI клиент 4.5 и выше, также SAC 8.0, JC Client 1.0/Единый Клиент JaCarta/Клиент Крипто БД 2.0

На сервере

- СУБД Oracle 9i/10g/11g/12c, Standard Edition One/Two, Standard Edition, Enterprise Edition
- СУБД Microsoft SQL Server 2005–2014 (32/64 бит)
- СУБД Tibero 5/6
- СУБД Postgre SQL 6.x

Как приобрести и установить

Решение поставляется партнёрами (в т.ч. дистрибьюторами) компании "Аладдин Р.Д.". Поставки для клиентских станций производятся комплектами.

В состав комплекта входят:

- CD-ROM с необходимыми ПО и инструкциями;
- краткое руководство по установке и работе;
- USB-ключи или смарт-карты с клиентской лицензией на использование продукта (по числу рабочих мест).

Для последующего увеличения числа рабочих мест необходимо приобрести дополнительные лицензии и USB-ключи (или смарт-карты).

Нам доверяют

Компания "Аладдин Р.Д." имеет репутацию надёжного партнёра, способного в сжатые сроки реализовать поставку продуктов и решений, а также провести их доработку под требования заказчика.

Комплексные решения на их основе востребованы в различных секторах отечественной экономики, в том числе в государственно-административном, банковском, топливно-энергетическом и ряде других.

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17.
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17.
Лицензия Министерства обороны РФ № 1384 от 22.08.16.
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011.
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15.
Apple Developer.

+7 (495) 223-00-01 aladdin@aladdin-rd.ru **Web**: www.aladdin-rd.ru

ID: 1407-060917