Система защиты баз данных и предотвращения утечек конфиденциальной информации

Крипто БД

- Технология обезличивания баз данных
- Прозрачное селективное шифрование критически важных полей баз данных
- Поддержка платформ Oracle, Microsoft SQL, Tibero, PostgreSQL
- Не требует внесения изменений в уже работающие приложения
- Сертификаты ФСБ России до класса КС3

Аладдин

Проблемы защиты баз данных в современных СУБД

Развитие сложных информационных систем, использование облачных сервисов, мобильная обработка данных и многие другие современные тенденции возможны только за счёт активного применения систем управления базами данных (СУБД). Это привело к тому, что СУБД применяются практически во всех ИТ-системах. При этом уровень сложности СУБД значительно повысился. В этих условиях существенно возросли риски утечки конфиденциальной информации из СУБД.

Потенциальную угрозу для конфиденциальной информации, обрабатываемой в современной СУБД, представляют не только внешние злоумышленники, но и собственные сотрудники организации, особенно администраторы СУБД, обладающие максимальным набором прав доступа к конфиденциальной информации.

При наличии большого количества пользователей мониторинг и выявление возможных действий злоумышленников и персонализация ответственности за эти действия становятся сложными и дорогостоящими задачами. В этих условиях применение простых и эффективных методов защиты информации в СУБД становится особенно актуальным.

"Крипто БД" — эффективное средство защиты от утечек из СУБД

"Крипто БД" — первая сертифицированная в России система предотвращения утечек информации из высокопроизводительных СУБД Oracle, Microsoft SQL Server, PostgreSQL и Tibero.

Для предотвращения утечек информации в "Крипто БД" используется композитный метод защиты: шифрование таблиц баз данных с применением российских криптографических алгоритмов ГОСТ 28147-89 или ГОСТ Р 34.12 2015 дополняется использованием строгой двухфакторной аутентификации пользователей с помощью USB-токенов или смарт-карт JaCarta.

Для неавторизованных пользователей защищаемые данные маскируются (представлены в виде произвольных символов), а действия всех авторизованных пользователей персонализируются и протоколируются, что позволяет проводить аудиты и расследовать инциденты безопасности.

Продвинутая ролевая модель и надёжное разграничение прав доступа исключают возможность компрометации защищаемой информации администраторами СУБД. В "Крипто БД" также предусмотрен контроль целостности собственных библиотек, а также модулей СУБД и операционной системы, что позволяет гарантировать невозможность подмены исполняемого кода (как в оперативной памяти, так и на запоминающих устройствах) администратором СУБД.

Возможность выборочного шифрования столбцов таблиц данных позволяет отказаться от тотального шифрования, экономя вычислительные ресурсы серверов и снижая издержки.

Отечественное ПО
Решение "Крипто БД" является полностью отечественной разработкой, включено в Единый реестр отечественного ПО (№№ 509, 518, 4292, 4293) для государственных закупок и поддерживает российские стандарты криптографии ГОСТ 28147-89 и ГОСТ 34.12-2012.

Возможности

Поддержка различных СУБД (Oracle, Microsoft SQL Server, Tibero и PostgreSQL)

Полное или выборочное шифрование информации в таблицах базы данных с применением стойких криптографических алгоритмов

Отложенные процедуры зашифрования/ расшифрования могут проводиться без остановки функционирования информационной системы в целом

Гибкое управление ключами шифрования для создания сложных моделей доступа к защищаемым данным

Двухфакторная аутентификация пользователей с использованием USB-токенов или смарт-карт

Продвинутая ролевая модель с надёжным разделением операций по управлению системой

Мониторинг и аудит действий пользователей

Контроль целостности собственных библиотек, модулей СУБД и ОС, а также среды исполнения

Сферы применения

В силу повсеместного использования СУБД для хранения и обработки конфиденциальной информации, а также широкого распространения угроз компрометации конфиденциальной информации, "Крипто БД" имеет широчайшую сферу применения, распространяющуюся на все без исключения отрасли рынка России.

Основными пользователями "Крипто БД" являются

Органы государственной власти и местного самоуправления, организации различных форм собственности, работающие с конфиденциальной информацией и персональными данными.

Государственные организации, подпадающие под действия ряда требований информационной безопасности, в обязательства которых зачастую включается ответственность за обеспечение конфиденциальности обрабатываемой ими информации.

Коммерческие организации, использующие либо планирующие внедрение информационных систем, обрабатывающих критически важные для их бизнеса данные, кража, модификация или утечка которых может привести к ощутимым потерям.

Преимущества

Повышение уровня информационной безопасности с помощью шифрования баз данных и применения средств аутентификации

Экономия вычислительных ресурсов за счёт выборочного шифрования столбцов таблиц данных

Исключение перехвата трафика между компонентами за счёт применения стойкого шифрования

Защита от администраторов СУБД с помощью продвинутой ролевой модели доступа

Отсутствие необходимости доработки приложений после внедрения решения

Невосстановимость актуальных и удалённых данных при отсутствии ключей шифрования

Обеспечение непрерывности бизнеса с помощью функций отложенной процедуры шифрования

Централизованное управление сервисными операциями и настройками через единую консоль управления

Отслеживание действий сотрудников и администраторов с помощью системы централизованного мониторинга и аудита

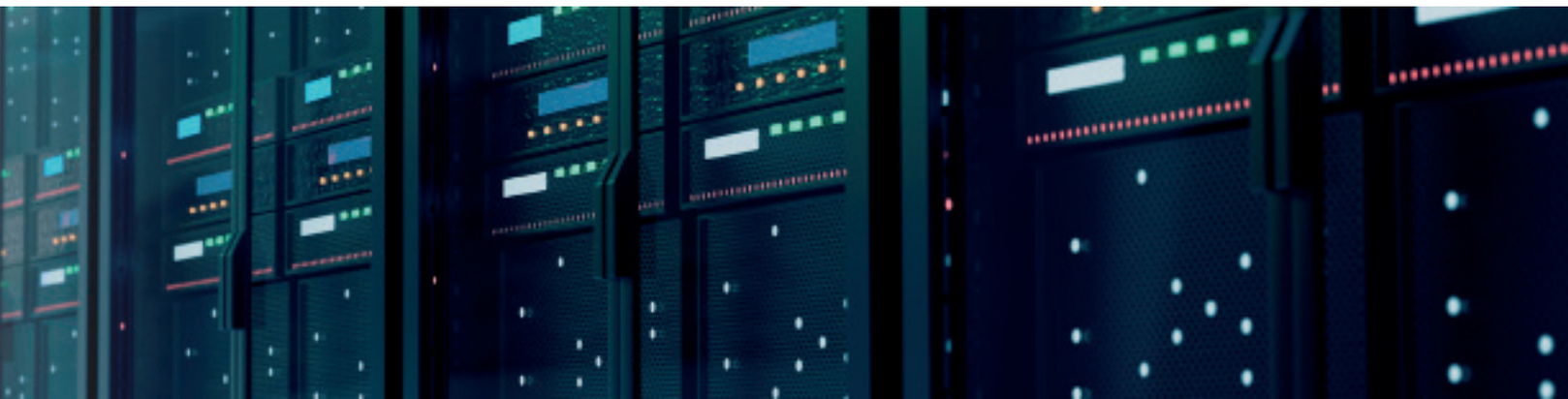
Российский продукт (входит в Единый реестр отечественного ПО)

Сертификаты

Сертифицированная версия "Крипто БД" может быть использована при создании и применении автоматизированных систем до класса защищённости 1Г, а также для защиты информации в ИСПДн до 1 класса включительно.

"Крипто БД" сертифицирована ФСБ России как СКЗИ класса КС1 и КС2 (сертификат соответствия № СФ/124-3249), класса КС3 (сертификат соответствия № СФ/124-3472), что позволяет использовать систему для защиты информации, не содержащей сведений, составляющих государственную тайну.

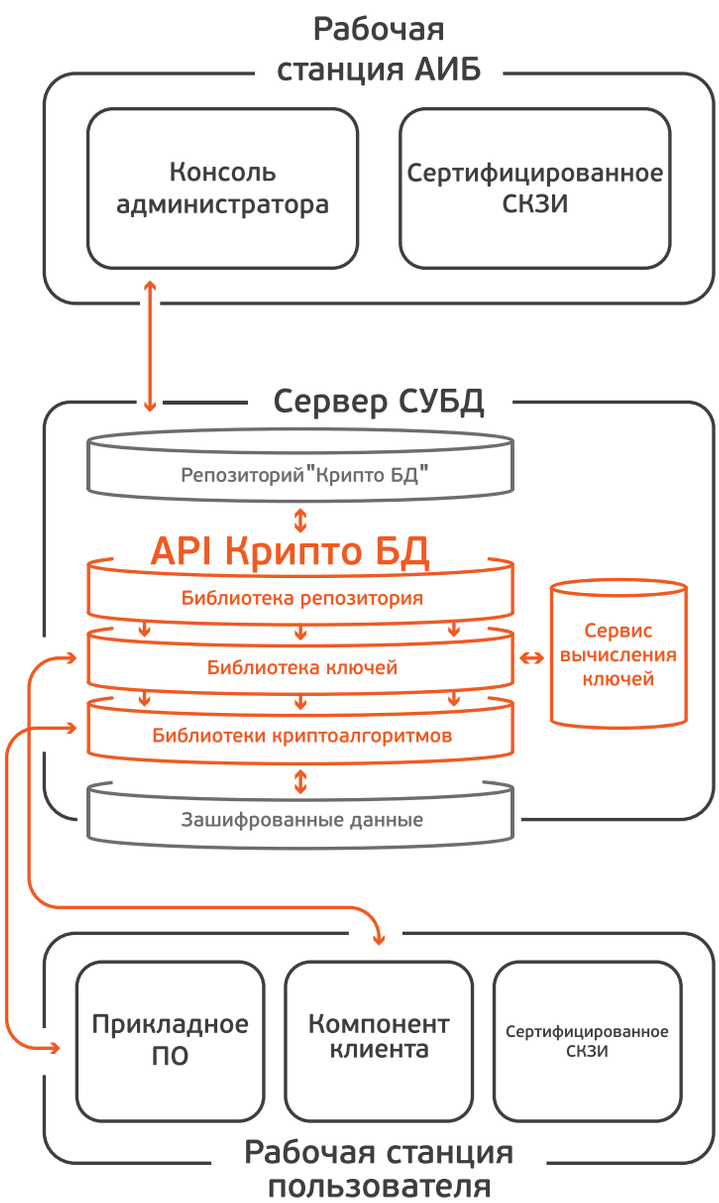
На клиентских рабочих станциях должны использоваться сертифицированные СКЗИ и совместимые ключевые носители.



Технические подробности

Архитектура

Приложение клиента на основании данных в цифровом сертификате получает доступ в определённую БД с соответствующими правами. Если с помощью средства аутентификации (USB-ключ или смарт-карта) будет правильно вычислен ключ шифрования, то зашифрованные данные станут доступны пользователю.



Компоненты "Крипто БД"

- **API** — ядро "Крипто БД", осуществляющее все криптографические операции, включающие шифрование информации, защиту ключей шифрования, безопасную передачу ключей шифрования, а также обеспечение целостности данных, служебного ПО и служебной информации.

- **Репозиторий** — набор информации о зашифрованных таблицах, ключах шифрования, пользователях, настройках аудита и истории изменения указанной информации.

- **Сервис вычисления ключей** — служба, предназначенная для безопасной передачи ключей шифрования между клиентом и сервером.

- **Консоль администрирования** — консоль администратора безопасности, позволяющая выполнять следующие операции:
  - обеспечение жизненного цикла ключей шифрования;
  - шифрование (перешифрование) данных в таблицах БД;
  - управление пользователями (ключами шифрования пользователей);
  - управление аудитом;
  - контроль целостности собственного ПО и объектов пользователей;
  - контроль ошибочных ситуаций.

- **Клиентское ПО** (Клиент "Крипто БД") — интерфейсное ПО для осуществления взаимодействия с СКЗИ для выполнения на сертифицированном СКЗИ криптографических операций.

Лицензирование и поддержка

Продукт состоит из клиентской и серверной частей. Лицензии на клиентскую и серверную части продукта приобретаются по отдельности.

Лицензии "Крипто БД 2.0"

- Серверная часть продукта лицензируется по количеству экземпляров целевой БД, на которых она должна быть установлена, и максимальному объёму данных, защищаемых с помощью продукта.
- Стоимость первого года технической поддержки входит в стоимость серверной лицензии на использование СКЗИ "Крипто БД 2.0". Техническая поддержка включает в себя:
  - доступ к Базе знаний;
  - возможность получения обновлений;
  - возможность размещения кейсов в технической поддержке.
- Стоимость технической поддержки на следующий год составляет 22% от стоимости закупленных серверных лицензий.
- Временный отказ от платной технической поддержки не влечёт каких-либо штрафных санкций при дальнейшем её возобновлении.

Клиентские лицензии "Крипто БД 2.0"

- Продукт лицензируется по числу пользователей, работающих с БД. Это число определяется количеством электронных ключей.
- "Клиент Крипто БД" может быть установлен на любое количество рабочих мест, но использовать его (работать с системой) смогут только пользователи, обладающие электронными ключами.
- Дистрибутив "Клиент Крипто БД" и документация (в электронной форме) поставляются на компакт-диске и входят в состав комплекта документации и ПО.

Базовая техническая поддержка

- Базовая техническая поддержка на первый год эксплуатации предоставляется бесплатно и входит в состав продукта. На все последующие годы планируемой эксплуатации сертификат на базовую техническую поддержку приобретается отдельно. Стоимость годового сертификата рассчитывается как процент от суммарной стоимости всех приобретённых лицензий.
- Оплата базовой технической поддержки не допускает периодов прерывания. При возобновлении требуется оплатить все пропущенные периоды.

Технические подробности

Для достижения оптимальной производительности в работе "Крипто БД" должны быть реализованы следующие технические условия и требования.

Среда функционирования (Сервер базы данных и платформы)	**Microsoft** • Microsoft SQL Server 2016, 2014, 2012, 2008R2, 2008, 2005, 2003 **Oracle** • Oracle Database Server 9i, 10g, 11g, 12c (Personal, Standard, Enterprise editions) ОС на сервере СУБД - Microsoft Windows Server 2008, 2012 (x86-64) - Microsoft Windows Server 2008, 2012 (x86) - Microsoft Windows 2003 Server (x86-64) - Microsoft Windows 2003 Server (x86) - Linux (x86-64), (x86), Itanium - IBM AIX5L - HP-UX PA-RISC - HP Tru64 UNIX - Solaris Operating System (x86), (x86-64), (64-bit SPARC) - IBM z/Linux **Tibero** • Tibero Database Server 5, 6 ОС на сервере СУБД - Microsoft Windows Server 2008, 2012 (x86-64) - Microsoft Windows Server 2008, 2012 (x86) - Microsoft Windows 2003 Server (x86-64) - Microsoft Windows 2003 Server (x86) - Linux (x86-64) - Linux (x86) **PostgreSQL** • PostgreSQL 9.x, PostgresPro 9.x ОС на сервере СУБД - Microsoft Windows Server 2008, 2012 (x86-64) - Microsoft Windows Server 2008, 2012 (x86) - Microsoft Windows 2003 Server (x86-64) - Microsoft Windows 2003 Server (x86) - Linux (x86-64) - Linux (x86)
Поддерживаемые модели USB-токенов и смарт-карт	В качестве носителей закрытых ключей используются USB-токены и смарт-карты, сертифицированные для использования совместно с криптопровайдерами на клиентских рабочих станциях. Состав считывателей и дополнительного ПО конкретизируется в зависимости от используемого сертифицированного СКЗИ и его исполнения. Рекомендованы к использованию смарт-карты и USB-токены JaCarta компании "Аладдин Р.Д.".
Рекомендуемые сертифицированные СКЗИ	• Крипто ПРО (Crypto Pro CSP 3.6 или выше)
Размеры ключей	• Размеры ключей для защиты ключей шифрования: - закрытый ключ — 256 бит; - открытый ключ — 512 бит (ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012). • Размеры ключей шифрования — 256 бит.
Реализуемые алгоритмы криптографического преобразования	Реализованы алгоритмы шифрования ГОСТ 28147-89 и ГОСТ Р 34.12-2015 в следующих режимах (включая режимы выработки и проверки имитовставки): • режим простой замены (ECB); • режим гаммирования (CTR); • режим гаммирования с обратной связью (CFB).

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17
Лицензии ФСБ России № 12632Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации услуг ГОСТ Р (РОСС RU.0001.03ГУ00) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
Сертификат соответствия - № РОСС RU.ФК14.К00011 от 20.07.18
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации "Военный Регистр" (РОСС RU.И1975.04ГШ02) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012
Сертификат соответствия - № ВР 21.1.13537-2019 от 25.04.19