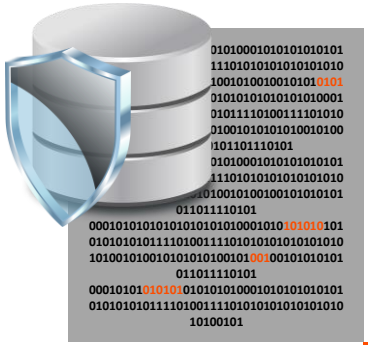
“Крипто БД”

Практические кейсы применения системы защиты СУБД



Денис Суховей
Руководитель департамента развития технологий "Аладдин Р.Д."
d.sukhovey@aladdin.ru

“Крипто БД”

Назначение системы защиты

- **Надёжная защита информации в СУБД**
  - Сертифицированное СКЗИ для защиты данных в базе
  - Зашифровывание таблиц или отдельных столбцов
  - Реализация методов "прозрачного" шифрования
- **Разграничение прав доступа пользователей**
  - В системе реализована двухфакторная аутентификация
- **Аудит и мониторинг действий пользователей**
  - Доступ к данным учитывается в защищенном журнале

ORACLE DATABASE

Microsoft SQL Server

PostgreSQL

TIBERO DataBase

SYBASE

Аладдин

“Крипто БД”

Сертификация и импотозамещение

- **Средство криптографической защиты информации**
- Соответствует требованиям ГОСТ 28147-89 и ГОСТ 34.12-2015 (шифрование "Магма","Кузнечик")
  - Соответствует требованиям к СКЗИ класса **КС1/КС2** (№СФ/124-3249, **КС3** (№СФ/124-3472)
  - Может использоваться для криптографической защиты информации в СУБД
- **Единый реестр отечественного ПО**
  - Решение является **полностью отечественной разработкой**
  - Номера реестровых записей: 509, 518, 4292, 4293

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-1569 от "06" ноября 2010 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-1569 от "06" ноября 2010 г.

Действителен до "06" ноября 2013 г.

Выдан закрытому акционерному обществу «АЛАДДИН Р.Д.»

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «Крипто БД Версия 1.0» (исполнения 1 и 2) в составе согласно формуляру 643.46538383.50.1430.005-01 30 01

соответствует требованиям ГОСТ 28147-89 и требованиям ФСБ России к СКЗИ класса КС1 (для исполнения 1) и КС2 (для исполнения 2) и может использоваться для криптографической защиты (генерация и управление ключевой информацией, шифрование и вычисление имитовставки пользовательских данных) информации, не содержащей сведений, составляющих государственную тайну, хранящейся в таблицах баз данных под управлением СУБД Oracle.

Аладдин

“Крипто БД”

Выполнение нормативных требований

- **Защита КИИ (187-ФЗ)**
  - Защита данных СУБД в информационных системах КИИ
- **Защита ПДн (152-ФЗ)**
  - Разграничение доступа к ПДн
  - Реализация двухфакторной аутентификации в ИСПДН
  - Мониторинг и журналирование событий доступа к ПДн
- **Приказ 17 (защита ГИС)**
  - Аутентификация, авторизация и разграничение прав пользователей
  - Применение ролевой модели разграничения прав
- **Требования PCI DSS (VISA & MasterCard)**
  - Шифрование и маскирование PAN
  - Усечение и использование One-Time-Pad

Аладдин

#1: Предотвращение утечек

Защита информации в СУБД при взломах информационных систем

- **Условная схожесть сценариев атак на СУБД**
  - Поиск и эксплуатация уязвимостей сервера
  - Поиск возможности повышения привилегий
  - Злонамеренное копирование или искажение данных
  - Изменение системных журналов
- **Назначение "Крипто БД"**
  - Обеспечение защиты информации в СУБД
  - Предотвращение утечек информации при любом сценарии атаки

Аладдин

#2: Защита от "админа"

Предотвращение доступа со стороны привилегированных пользователей

- **Почему администратор СУБД важная, но неконтролируемая роль?**
  - Сложность ИС и модели данных в СУБД
  - Загруженность и высокая бизнес-значимость СУБД
  - Малое количество специалистов и их высокая стоимость
- **Последствия**
  - Утечка "катастрофически" больших объемов конфиденциальной информации
  - Отсутствие возможности проведения расследований
- **"Крипто БД" обеспечивает защиту от администратора СУБД**
  - Администратор СУБД не имеет ключей шифрования
  - Все попытки доступа Администратора СУБД к защищаемой информации фиксируются
  - Реализован фундаментальный принцип разделения полномочий и ответственности

Аладдин

#3: Контроль доступа

Разграничение прав доступа пользователей к защищаемой информации

- **Традиционный подход к разработке бизнес-приложений**
  - Разграничение на уровне пользовательских интерфейсов
  - Защита на уровне сервера бизнес-приложений
- **Последствия применения подобного подхода**
  - Низкий уровень надежности защиты
  - Данные в СУБД не защищены
- **"Крипто БД" обеспечивает надежное разграничение пользователей**
  - Гибкие политики группового доступа к защищаемым ресурсам
  - Расширенная ролевая модель, реализующая функции контроля за доступом выделенному сотруднику безопасности

Аладдин

#4: Защита "облаков"

Защита информации при размещении СУБД в "облаке"

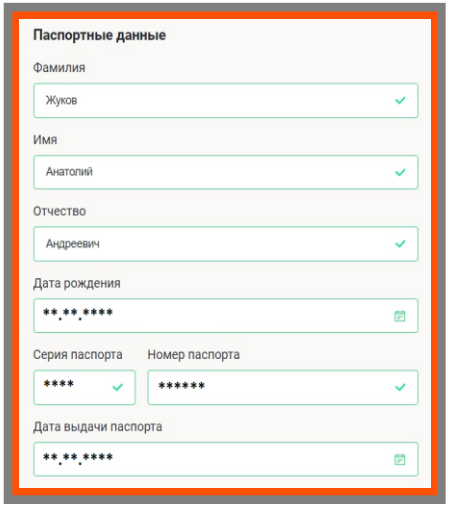
- **Негативные факторы "переезда" СУБД в "облако"**
  - Возможность физического доступа третьих лиц к серверам СУБД
  - Факты неавторизованного доступа к серверам СУБД не контролируются
  - Информация о фактах неавторизованного доступа администраторов не фиксируются
- **Применение "Крипто БД"**
  - Данные надежно защищены за счет шифрования информации
  - Dump/копию СУБД невозможно запустить на альтернативном сервере
  - Факты доступа к защищенной информации фиксируются
  - Управление параметрами защиты на стороне организации

Аладдин

#5: Маскирование данных

Маскирование и деперсонализация информации в СУБД

- **Где используется маскированная информация**
  - Тестовые массивы для сторонних разработчиков ИС
  - Выгрузки данных для сторонних аналитиков и консультантов
  - Непосредственно в бизнес-процессах ИС
- **Требования к реплицированным наборам данных**
  - Наборы данных должны быть актуальными
  - Размер выборки должен быть реалистичным
  - Наборы не должны содержать конфиденциальную информацию
- **Функции маскирования данных в "Крипто БД"**
  - Настраиваемый формат и внешний вид масок
  - Маски могут генерироваться из диапазонов заданных значений
  - Маскируется реальная/актуальная информация (не выгрузка СУБД)



Аладдин

#6: Защита архивов

Защита резервных копий и архивов СУБД

- **Требования к защищенному хранению архивов**
  - Не нарушать процессы резервирования информации
  - При краже/хищении архивов не должно возникать угроз компрометации информации
  - Совместимость с процедурами восстановления
  - При хранении защищенных архивов должно соблюдаться соответствие ряду нормативных требований РФ (например 187-ФЗ, Приказ 21 ФСТЭК России и т.п.)
- **Применение "Крипто БД"**
  - Информация в резервных копиях зашифрована
  - Существующую процедуру архивирования не нужно изменять
  - Хищение зашифрованых архивов не порождает новые угрозы утечки

Аладдин

#7: Независимый аудит

Аудит фактов доступа пользователей к защищаемой информации

- **Условия эффективного расследования инцидентов**
  - Достаточность информации о событиях ИБ
  - Актуальность информации
  - Достоверность собираемых данных
- **Применение в "Крипто БД"**
  - Собственная реализация механизма журналирования событий
  - Фиксация только событий доступа к защищаемой информации
  - Возможность передачи зафиксированной информации внешней системе (например SIEM)
  - Защита процедур логирования от возможных зловредных действий администратора СУБД
  - Криптографическая защита создаваемых журналов событий

Аладдин

#8: Уничтожение данных

Предотвращение возможности восстановления удаленной информации

- **Необходимость надежного уничтожения данных**
  - При выводе из эксплуатации ИС
  - При модернизации ИС или изменении информационной модели
  - При модернизации аппаратных платформ ИС
- **Возникающие проблемы**
  - В СУБД нет функций надежного уничтожения данных
  - Подтверждение надежности уничтожения данных
  - Трудоемкость процесса уничтожения
- **Использование "Крипто БД"**
  - Уничтожаемые конфиденциальные данные зашифрованы
  - Надежность уничтожения обуславливается стойкостью алгоритмов шифрования
  - Нет необходимости использования дополнительных средств

Аладдин

“Крипто БД”

Практические кейсы применения системы защиты СУБД

Предотвращение утечек

- Защита информации в СУБД при взломах информационных систем

Защита от "админа"

- Предотвращение доступа со стороны привилегированных пользователей

Контроль доступа

- Разграничение прав доступа пользователей к защищаемой информации

Защита "облаков"

- Защита информации при размещении СУБД в "облаке"

Маскирование данных

- Маскирование и деперсонализация информации в СУБД

Защита архивов

- Защита резервных копий и архивов СУБД

Независимый аудит

- Аудит фактов доступа пользователей к защищаемой информации

Уничтожение данных

- Предотвращение возможности восстановления удаленной информации

Аладдин

Спасибо!

Будь собой в электронном мире!®

Суховей Денис
Руководитель департамента развития технологий
"Аладдин Р.Д."
+7(916) 550-11-78
d.sukhovey@aladdin.ru
www.aladdin.ru