Аладдин РД
www.aladdin-rd.ru

Защита персональных данных в базах данных

Обеспечение выполнения требований федерального закона о персональных данных № 152-ФЗ в части безопасного доступа и хранения персональных данных.

Справочная информация

для специалистов
по информационной
безопасности и ИТ

Аннотация

Настоящий документ описывает возможности программно-аппаратного решения "Крипто БД" с точки зрения применения в информационных системах, обрабатывающих персональные данные. Рассматриваются технические и технологические методы применения решения для обеспечения выполнения требований федерального закона № 152-ФЗ.

Назначение "Крипто БД"

Средство криптографической защиты "Крипто БД" предназначено для обеспечения конфиденциальности информации с помощью криптографического преобразования. "Крипто БД" позволяет также контролировать целостность информации с помощью выработки и проверки имитовставки.

Основные характеристики

- Шифрование колонок таблиц БД с использованием алгоритма ГОСТ 28147-89 в различных режимах. Существует возможность использования встроенных в СУБД Oracle алгоритмов (DES/TripleDES/AES);
- 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"

СКЗИ "Крипто БД" может быть использовано для защиты информации:

- В клиент-серверных приложениях;
- В многозвенных приложениях;
- В системах, использующих терминальный доступ;
- В системах, использующих автоматические процессы для доступа к данным;
- В облачных системах (IaaS, SaaS).

Сертификация

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

[1] Для использования индексов, в том числе для полнотекстового поиска и поиска по частичному совпадению, возможно применение специальных техник.

[2] Ограничение будет устранено в следующих версиях продукта.

”Крипто БД” и ФЗ 152

“Крипто БД” реализует следующие возможности:

- защита информации от несанкционированного доступа со стороны неуполномоченных пользователей, в том числе привилегированных (администраторы БД, ОС и т. п.);
- надёжная защита ключей шифрования на протяжении их жизненного цикла;
- прозрачное встраивание в готовые информационные системы;
- аудит и мониторинг доступа к защищённым данным;
- централизованное управление функциями безопасности (ключи шифрования, аудит, пользователи и т. п.);
- контроль целостности собственного ПО и служебной информации.

Подобные функциональные возможности позволяют выполнить ряд требований стандарта без какой-либо значительной переделки готовой информационной системы.

В соответствии с федеральным законом о персональных данных Оператор обязан обеспечить безопасность персональных данных в соответствие с отраслевой моделью угроз, разработанной федеральным органом исполнительной власти. На текущий момент отраслевые модели угроз отсутствуют, поэтому в каждом частном случае модель угроз разрабатывается посредством проведения персонального аудита.

В данном документе рассматривается среднестатистическая модель угроз в среднестатистическом случае.

Статья	Пункт	Требование закона	Функциональные возможности “Крипто БД”
6	9	Обработка персональных данных осуществляется … при условии обязательного обезличивания персональных данных*. *Статья 3, п.9: Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.	Обезличивание персональных данных выполняется зашифровыванием той части информации, без которой невозможно однозначно идентифицировать субъекта персональных данных.
7		Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных	Конфиденциальность персональных данных, обрабатываемых оператором, обеспечивается: — шифрованием колонок таблиц баз данных; — защитой копий симметричных ключей шифрования ассиметричными ключами шифрования пользователей и разделением доступа к зашифрованным колонкам по наличию USB-токена или смарт-карты, содержащей закрытые ключи пользователей; — аудитом доступа к зашифрованным данным;
10		Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи	Колонки таблиц баз данных, содержащие персональные данные специальных категорий, зашифровываются.

Статья	Пункт	Требование закона	Функциональные возможности "Крипто БД"
14	7	Субъект персональных данных имеет право на получение информации, касающейся его персональных данных, в том числе содержащей: 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона; 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом; 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;	Данное требование может быть закрыто персонализированным аудитом, настроенным на доступ оператора к зашифрованным данным. Таким образом, личность человека, получавшего доступ к данным, может быть однозначно идентифицирована.
19	1	Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных.	Средствами "Крипто БД" реализуется: — шифрование колонок таблиц баз данных; — защита ключей шифрования; — разделение доступа к зашифрованным колонкам по наличию USB-токена или смарт-карты у пользователей; — аудит доступа к зашифрованным данным;
	2	2) применением … и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, … 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации; 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер; 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня за-	СКЗИ "Крипто БД" имеет сертификат соответствия ФСБ по классам защиты КС1, КС2. Средствами Крипто БД реализуются дискретная или мандатная (16 уровней меток) модель доступа к персональным данным. Критерий доступа - наличие аппаратных USB-токенов или смарт-карт у пользователя с записанным на них ключевым материалом . Собственная система аудита позволяет зафиксировать все факты доступа к защищаемой информации.

Статья	Пункт	Требование закона	Функциональные возможности "Крипто БД"
		щищенности информационных систем персональных данных.	
21	1	В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя … оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту данных или обеспечить их блокирование.	Реализованные в "Крипто БД" модели разделения доступа исключают возможность неправомерной обработки персональных данных субъекта.
	3	В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор ... обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора.	

Аладдин РД

Тел.: +7 (495) 223-0001
E-mail: aladdin@aladdin-rd.ru
Web: www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)
Лицензии ФСБ России № 18229 от 13.10.10, № 9333Р от 03.09.10, №№ 4205П, 4206Х от 22.06.07, № 4898П от 14.12.07
Microsoft Certified Partner, IBM Business Partner, Oracle Business Partner