СРАВНЕНИЕ НАДЕЖНОСТИ ЗАЩИТЫ БАЗ ДАННЫХ МЕТОДАМИ СОВРЕМЕННОЙ КРИПТОГРАФИИ

С.Г. БУЯНОВА
Филиал Белорусский государственный университет информатики и радиоэлектроники «Минский радиотехнический колледж»

Аннотация: в статье рассматриваются вопросы надёжности, удобства использования и технологичности различных методов криптографической защиты баз данных. Особое внимание уделено выбору подхода в зависимости от задач и целей такой защиты. Проведённые сравнения показывают, что криптографические методы, при разумных предположениях о возможностях злоумышленников, обеспечивают максимальную степень защиты с минимальными затратами, не создавая значительных неудобств для пользователей.

Современные криптографические технологии играют ключевую роль в решении задач информационной безопасности. Практически каждая организация, использующая компьютерные системы, сталкивается с необходимостью защиты баз данных. Это обусловлено как требованиями законодательства, так и реальной потребностью в обеспечении безопасности информации. Однако в ряде случаев встроенных возможностей систем управления базами данных (СУБД) и организационных мер оказывается недостаточно. Например, одной из уязвимостей являются файлы-триггеры, которые используются для выполнения запросов. Они часто содержат данные в открытом виде, что делает их доступными для злоумышленников, имеющих физический доступ к серверу [3].

Криптографические методы защиты баз данных можно разделить на два основных направления:

1. Методы, предотвращающие несанкционированное ознакомление с данными путём их шифрования как при хранении, так и при передаче по каналам связи;

2. Методы, обеспечивающие авторизацию доступа и аутентификацию записей базы данных, предотвращающие их подмену или несанкционированные изменения.[1]

Шифрование записей базы данных или их отдельных частей с использованием современных криптографических алгоритмов позволяет эффективно разграничивать доступ к данным. Это снижает необходимость в сложной физической защите носителей информации, так как обеспечивает высокий уровень безопасности на уровне программных решений.

Аутентификация данных посредством электронных подписей предотвращает возможность их подмены. Этот подход позволяет документировать изменения в базе данных с высокой степенью детализации. На сегодняшний день ни один метод защиты, кроме криптографического, не способен гарантировать пользователям столь высокий уровень надёжности и удобства [2].

Однако криптографические методы не лишены недостатков. Один из них связан с тем, что работа с ключами, паролями и процессами шифрования может быть сложной для обычных пользователей. В результате многие пользователи передают управление ключами администраторам, что создаёт риск несанкционированного доступа к данным.

Наиболее надёжным подходом считается использование индивидуальных ключей для шифрования отдельных записей. При этом процесс шифрования и расшифрования выполняется на стороне пользователя, а ключи хранятся в защищённом аппаратном модуле, например, токене. Такая схема исключает доступ администраторов к данным, к которым они не должны иметь доступ.

Интересным решением являются гомоморфные шифры, которые позволяют выполнять операции над зашифрованными данными без их расшифровки. Это значительно снижает риски, связанные с доступом к данным третьих лиц. Однако для широкого применения таких методов необходимо разработать более производительные алгоритмы, которые не будут существенно замедлять работу СУБД.

При выборе методов криптографической защиты баз данных важно учитывать структуру хранимой информации и необходимость её удалённой обработки. Существуют два основных подхода к защите данных на удалённых серверах:

1. Использование единого шифрования для всей базы данных, где операции с данными выполняются на стороне клиента или промежуточного сервера.

2. Применение разных типов шифрования для различных частей базы данных. В этом случае данные шифруются непосредственно на удалённом сервере или в облачной инфраструктуре.

Эффективная защита информационных ресурсов требует соблюдения комплексного подхода, который включает в себя криптографию как один из ключевых элементов. Это позволяет аутентифицировать пользователей, предотвращать просмотр данных посторонними лицами и исключать возможность отказа от совершённых действий (non-repudiation).

Рассмотрим основные криптографические технологии в СУБД. Шифрование данных представляет собой процесс их преобразования в вид, недоступный для понимания без использования ключа. Применяются два основных подхода:

1. Симметричное шифрование. Этот метод использует один ключ для шифрования и дешифрования. Он отличается высокой скоростью работы и подходит для использования в повседневной защите данных. Среди популярных алгоритмов – AES, DES, Triple DES и их вариации.

2. Асимметричное шифрование. Этот метод использует пару ключей: один для шифрования данных, а другой – для их расшифровки. Он обеспечивает более высокий уровень безопасности, но требует больше вычислительных ресурсов. Примером является RSA, который поддерживает ключи длиной до 2048 бит.

Для упрощения управления ключами в асимметричных системах используется инфраструктура открытых ключей (PKI), которая облегчает работу с большим количеством ключей и сертификатов.

Цифровые сертификаты представляют собой асимметричные ключи с дополнительной информацией, такой как срок действия и сведения о центре сертификации, выдавшем сертификат. Они используются для подтверждения личности отправителей и получателей данных. Например, современные версии MS SQL Server автоматически генерируют самоподписанные сертификаты при первом запуске, которые используются для шифрования подключений [1].

Прозрачное шифрование данных (TDE) – это особый случай симметричного шифрования, при котором данные шифруются "на лету", без необходимости изменений в приложении. Этот метод минимизирует вмешательство пользователей в процесс защиты данных.

Криптографические методы защиты баз данных остаются наиболее надёжным и эффективным решением для обеспечения информационной безопасности. Однако их применение требует грамотного управления ключами и учёта специфики базы данных. Ошибки в настройке криптографических механизмов могут свести на нет все преимущества их использования. Поэтому выбор метода защиты должен основываться на структуре базы данных, необходимости удалённой обработки данных и требованиях к безопасности.

Список использованных источников

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / учеб. пособие / В.Ф. Шаньгин. Изд-во Форум, 2021. 416 с.

2. Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М. : Горячая линия – Телеком, 2016. – 175 с.

3. Волк, В.К. Базы данных. Проектирование, программирование, управление и администрирование / В.К. Волк. – СПб.: Лань, 2020. – 244 с