Способ защиты информационного сигнала от несанкционированного доступа в волоконно-оптической линии связи, заключающийся в том, что на передающей стороне волоконно-оптической линии связи формируют информационный сигнал, формируют суммарный сигнал путем смешивания шумового и информационного сигнала, формируют путем модуляции суммарным сигналом подлежащего передаче оптического излучения и вводят в волоконно-оптическую линию связи, а на приемной стороне волоконно-оптической линии связи выводят из нее принимаемое оптическое излучение, из принятого оптического излучения формируют суммарный сигнал из которого выделяют информационный сигнал отличающийся тем, что до формирования суммарного сигнала на приемной стороне формируют исходный и инверсный шумовой сигнал, модулируют исходным шумовым сигналом оптического излучения и вводят в волоконно-оптическую линию связи, а на передающей стороне волоконно-оптической линии связи выводят из нее принимаемое оптическое излучение, из принятого оптического излучения формируют шумовой сигнал который подлежит к смещению информационного сигнала, а выделения информационного сигнала на приемной стороне производят путем смешение задержанного инверсного шумового сигнала к суммарным сигналом причем время задержки инверсного шумового сигнала определяется выражением $t_{зад} = 2L/v$, где: L-длина оптического волокна; *v*-скорость оптического излучения в оптическом волокне.

Литература

1. Хайров И.Е, Румянцев К.Е, Новиков В.В, Троцюк Е.В. Анализ методов съема информации в квантовом канале связи. //Информационное противодействие угрозам терроризма: научн-практ. Журн. /ФГПУ НТЦ , Москва. 2004, №3. С. 71 – 73.]

2. К.Е. Румянцев, И.Е. Хайров, В.В. Новиков, Е.В. Троцюк. Исследование физических принципов осуществления несанкционированного доступа к квантовым каналам связи. //Информационное противодействие угрозам терроризма: научн-практ. Журн. /ФГПУ НТЦ, Москва. 2006, №6. С. 230 – 233.

Р.Р. Мухутдинов, С.А. Бурлов

РАЗРАБОТКА МЕХАНИЗМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ИЗМЕНЕНИЯ В БАЗАХ ДАННЫХ

(Самарский университет)

Введение. Системы управления базами данных являются доминирующим инструментом хранения больших массивов информации. Сколько-нибудь развитые информационные приложения полагаются не на файловые структуры операционных систем, а на многопользовательские СУБД, выполненные в технологии клиент - сервер. В связи с этим обеспечение информационной

безопасности СУБД, и в первую очередь их серверных компонент, приобретает решающее значение для безопасности организации в целом.

В современных СУБД есть средства, которые защищают данные. Однако некоторые законные пользователи могут незаконно изменять информацию, к которой они не должны иметь доступа. Как пример, разработчики баз данных могут использовать подключение к рабочей базе данных напрямую. Тем самым они получают возможность изменять информацию, хранящуюся в базе данных. Что является большой уязвимостью в рабочей информационной системе.

Для обеспечения защиты информации в базе данных от несанкционированного изменения была разработана схема, представленная на рисунке 1. Схема является кроссплатформенной и не зависит от конкретной СУБД, однако существует ряд требований, которым она должна удовлетворять:

- наличие механизма триггеров;
- возможность хранения информации в контексте сессии пользователя;
- иметь интерфейс для работы с сертификатами (криптографические пакеты или библиотеки);
- возможность шифрования таблиц;
- возможность скрытия процедур (обертывание, wrapping);
- возможность динамического формирования запроса (EXECUTE IMMEDIATE, …)

Сертификаты используются для криптографической защиты информации в архитектуре клиент – сервер, а также для проверки подлинности.

Результаты. В данной работе предложена схема для защиты информации в базах данных от несанкционированного изменения.

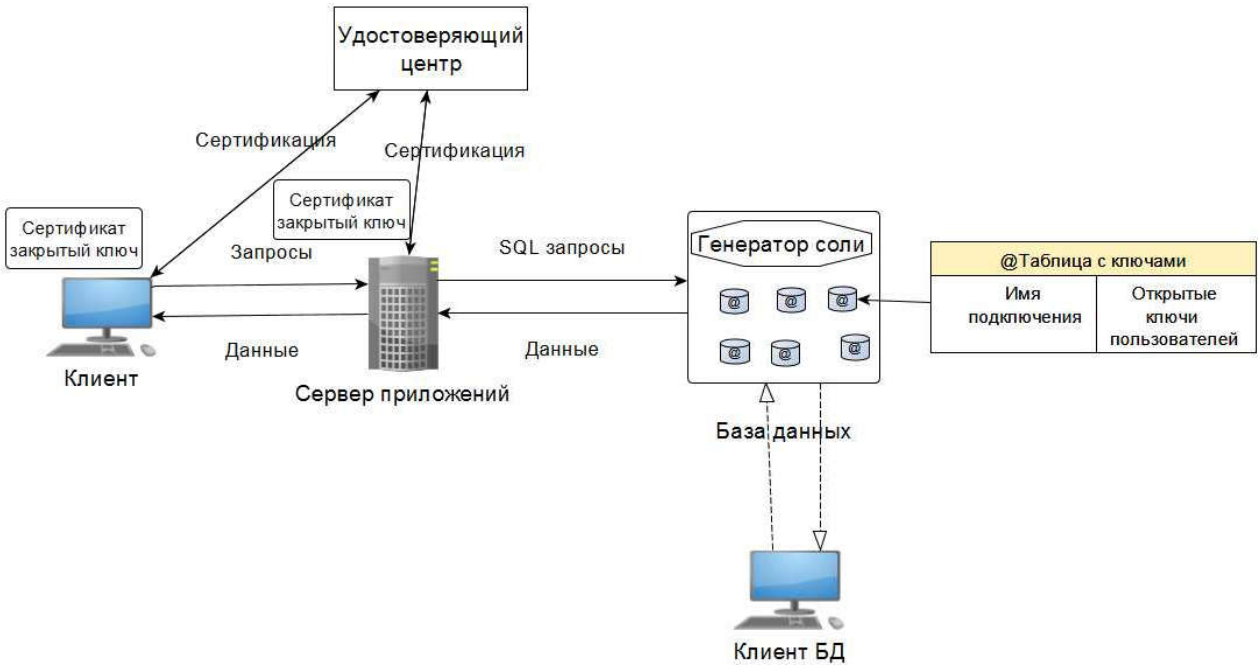

Рис. 1. Схема для защиты информации от несанкционированного изменения

Клиент инициирует запрос на вход в информационную систему. Создается сессия сервера приложений. Затем происходит создание сессии в базе данных на одном из подключений, в сессию помещается информация: зашифрованный хеш-пароля, имя подключения. Механизм базы данных проверяет, включены ли все триггеры, после чего генерирует «соль» и шифрует её открытым ключом сервера приложений. Сгенерированная соль отправляется на сервер приложений и также заносится в сессию базы данных. После чего сервер приложений возвращает пользователю доступный ему интерфейс. После входа в информационную систему клиент может отправлять запросы для работы с данными.

Клиент отправляет запрос на изменение данных. Сервер приложений обрабатывает запрос клиента, формирует *SQL* запрос и передает его СУБД. Ядро СУБД обрабатывает *SQL* запрос, формируется событие на действие. На это событие срабатывает предопределенный триггер. Триггер должен проверить легальность пользователя отправившего запрос на изменение данных.

Проверка происходит с помощью информации, которая находится в сессии БД. В базе данных хранится секретная таблица с открытыми ключами пользователей, она зашифрована средствами базы данных. Из сессии извлекается хеш-пароль пользователя, зашифрованный закрытым ключом пользователя. Хеш-пароль из сессии расшифровывается с помощью открытого ключа хранящегося в секретной таблице базы данных. Проверяется соответствие хешей от пароля, а также наличие в сессии соли сгенерированной БД. Если хеши паролей совпадают и в сессии присутствует сгенерированная соль, то считается, что пользователь прошел проверку и его запрос на изменение данных выполняется, иначе происходит прерывание запроса.

Стоит упомянуть, что данная схема принципиально может быть раскрыта и переработана злоумышленником только при работе под супер привилигированным пользователем (SYS, ROOT, …).

Литература

1. Кайт Томас. Oracle для профессионалов: архитектура, методики программирования и особенности версий 9i, 10g и 11g 2-е издание: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2011. – 848 с..

2. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2012. – 815 с.

3. Эндрю Таненбаум, М. ван Стеен. Распределенные системы. Принципы и парадигмы СПб.: Питер, 2003. — 877 с.

4. Neil Matthew. Beginning Databases with PostgreSQL: From Novice to Professional англ 2005. – 664 с.