**ЗАЩИТА И БЕЗОПАСНОСТЬ БАЗЫ ДАННЫХ**

**Алимжанова Жанна Муратбековна ф.-м.ғ.к., доцент м.а.**

**Балтабекова Аида Ботақызы, магистр, КазНУ им. аль-Фараби**

**Тұрдалы Айдана Дәулетқызы, магистр, КазНУ им. аль-Фараби**

**Аннотация:** Вопросы защиты данных являются критическими при обеспечении безопасности современных корпоративных систем. Статья посвящена сложившейся ситуации в области безопасности данных, находящихся под управлением
систем БД. Сделан обзор существующих работ на указанную тему как отечественных, так и зарубежных авторов. Рассмотрены этапы эволюции систем защиты информации в СУБД. Выделены современные комплексные проблемы в области защиты данных теоретического и практического характера. При анализе проблем безопасности учтены новые направления развития СУБД, такие как in memory и NoSQL-решения. В статье выделены особенности БД с точки зрения информационной безопасности по отношению к другим видам ПО. Предложено базовое деление уязвимостей.

**Ключевые слова:** База данных, защита базы данных.

В настоящее время практически ни одна организация не обходится без использования баз данных в своей деятельности. Поскольку в базах данных может храниться очень деликатная или конфиденциальная информация, касающаяся финансовой документации и клиентской информации, актуален вопрос ее защиты и безопасности.

Под «защитой БД» понимается способ предотвращения несанкционированного доступа к информации, хранимой в таблицах [1]. Долгое время защита баз данных ассоциировалась с защитой локальной сети предприятия от внешних атак хакеров, борьбой с вирусами и т. п. Однако, одним из наиболее слабых мест при обеспечении безопасности данных является большое количество лиц, получающих к ним доступ на самых различных уровнях, т. е. угрозы возникают не только извне, но и изнутри, со стороны легальных пользователей.

Наиболее типичным примером является скачивание базы данных системным администратором перед увольнением, или воровство базы сотрудником, имеющим к ней доступ в связи с должностными обязанностями. Таким образом, возникает проблема защиты конфиденциальной информации от атак злоумышленников. Так каким же образом защитить информацию?

* + основным средствам защиты информации относят следующие:

– парольная защита;

– установление прав доступа к объектам БД;

– защита полей и записей таблиц БД;

– шифрование данных и программ.

Парольная защита представляет простой и эффективный способ защиты БД от несанкционированного

доступа. Пароли устанавливаются конечными пользователями или администраторами БД и хранятся в определенных системных файлах СУБД в зашифрован-ном виде.

* целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта, а также администратор БД имеют все права. Остальные пользователи
* разным объектам могут иметь различные уровни доступа.
	+ данным, имеющимся в таблице, могут применяться меры защиты по отношению к отдельным полям и отдельным записям. В реляционных СУБД отдельные записи специально не защищаются. Применительно к защите данных в полях таблиц можно выделить такие уровни прав доступа, как полный запрет доступа, только чтение, разрешение всех операций (просмотр, ввод новых значений, удаление и изменение).

Более мощным средством защиты данных от про-смотра является их шифрование. Шифрование – это преобразование читаемого текста в нечитаемый с помощью стойкого криптоалгоритма [3]. Для дешифрования информации пользователи, имеющие санкционированный доступ к зашифрованным данным, имеют ключ и алгоритм расшифрования.

Главным объектом атаки являются, как правило, административные полномочия. Их можно получить, узнав в хешированном или символьном виде пароль администратора системы.

**Методы противодействия типовым угрозам**

|  |  |  |
| --- | --- | --- |
| Угроза | Противодействие | Метод |
| Хищение информации из БД неуполномоченным пользователем | Шифрование базы данных и ролевое управление доступом | Установка системы управления доступом по цифровым сертификатам, шифрование критических сегментов базы |
| Хищение информации из БД со стороны легального пользователя (превышение полномочий) | Ролевое управление, подробный аудит  | Аутентификация и дополнительный мониторинг действий пользователя  |
| Хищение или использование чужой учетной записи (из-за отсутствия защиты учетной записи) | Аутентификация по цифровому сертификату | Использование механизма SSL-аутентификации |
| Использование известных паролей, установленных по умолчанию. Хищение пароля. Подбор пароля. Перехват пароля во время передачи по сети | Аутентификация по цифровомуСертификату  | Отказ от использования паролей, пере ход на SSL-аутентификацию с использованием сертификатов |
| Хищение или копирование ключевого контейнера или его резервной копии | Закрытый ключ хранится какне экспортируемый в защищеннойпамяти интеллектуальной смарт карты  | Использование смарт-карт технологий для хранения закрытых для безопасногоключей |
| Перехват закрытого ключа (в момент его использования с помощью специального ПО) | Аппаратная реализация криптографических операций в смарт-карте | Использование смарт-карт технологийдля аппаратного выполнения крипто графических операций (SSL) в процессоре смарт-карты без «выхода» закрытых ключей наружу |
| Дублирование смарт-карты | Доступ к защищенной памяти смарт-карты, в которой хранятсязакрытые ключи, защищен PIN-кодом. Экспорт закрытых ключейиз смарт-карты исключен  | Закрытые ключи, сгенерированныесмарт-картой или импортированныев нее, хранятся в закрытой памятисмарт-карты и не могут быть из нееизвлечены  |
| Перехват передаваемых по сети данных | Шифрование сетевого трафика | Использование SSL-протокола дляШифрования передаваемых по сетиданных с помощью встроенных в Oracleалгоритмов симметричного шифрования  |

Типовые угрозы и технические методы противодействия им с помощью технологий, основанных на применении встроенных в Oracle, приведены в таблице [2].

Итак, для минимизации риска потерь необходима реализация комплекса нормативных, организационных и технических защитных мер, в первую очередь: введение ролевого управления доступом, организация доступа пользователей по предъявлению цифрового сертификата, а в ближайшей перспективе – промышленное решение по выборочному шифрованию и применение алгоритмов ГОСТ для шифрования выбранных сегментов базы.

Для полного решения проблемы защиты данных администратор безопасности должен иметь возможность проводить мониторинг действий пользователей, в том числе с правами администратора. Поскольку штатная система аудита не имеет достаточных средств защиты, необходима независимая система, защищающая корпоративную сеть не только снаружи, но и изнутри [4]. В будущем должны также появиться типовые методики комплексного решения задачи защиты баз данных для предприятий разного масштаба – от мелких до территориально распределенных.

**Библиографические ссылки**

1. Сабанов А. Безопасность баз данных. Что, от кого и как надо защищать. Connect, 2006. № 4.
	1. Увайсова З. М., Билалова И. М. Защита и безопасность баз данных // Студенческий научный форум материалы VII Междунар. студ. электронной науч. конф. [Электронный ресурс]. URL: http://www. scienceforum.ru/ (дата обращения: 14.09.2017).
	2. Лихоносов А. Г. Безопасность баз данных : интернет-курс по дисциплине [Электронный ресурс]. URL: http://www.e-biblio.ru/ (дата обращения: 12.09.2017).
	3. Смирнов С. Н. Безопасность систем баз данных.

М. : Гелиос АРВ, 2007. С. 352–353.