УДК 681.3.067

Д. Р. Утебов, С. В. Белов

Астраханский государственный технический университет

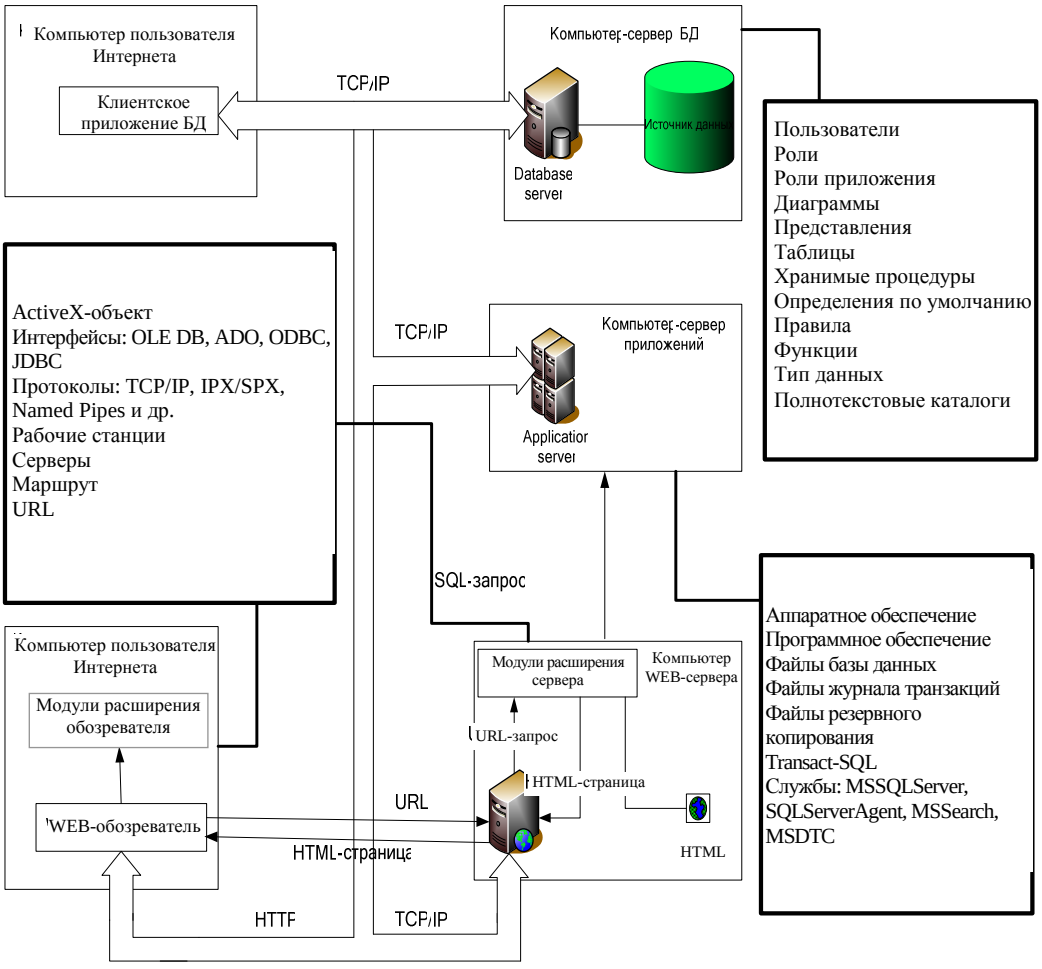
КЛАССИФИКАЦИЯ УГРОЗ В СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Введение

Для того чтобы обеспечить определенный уровень безопасности информационных систем, первоначально необходимо понять природу возникающих угроз. Недостаточный уровень осознания лицами, принимающими решения, природы угроз может привести к неблагоприятным последствиям от реализации угроз. В настоящее время в нормативных документах по защите информации [1, 2] описываются угрозы для баз данных (БД), но данные угрозы носят общий характер для автоматизированных систем, вследствие чего задача классификации угроз для систем управления базами данных (СУБД) является актуальной.

Нами классификация угроз осуществляется на основе обобщенной схемы классификации угроз, предложенной В. А. Герасименко [3]. В данной схеме угрозы по источнику воздействия делятся на внутренние и внешние. Для описания внешних угроз необходимо учитывать объекты воздействия. Под объектами воздействия понимаются объекты, которые могут подвергнуться атакам или могут стать причиной их возникновения. Данные объекты необходимо учитывать на всех уровнях информационной системы. Результатом воздействия внутренних и внешних угроз может быть нарушение целостности, конфиденциальности и доступности информации.

Объекты в СУБД на фоне многоуровневой архитектуры СУБД показаны на рисунке.



Объекты воздействия на фоне многоуровневой архитектуры СУБД

К появлению многоуровневой архитектуры привело развитие архитектуры Web-приложений и технологии «клиент-сервер» [4]. При такой архитектуре клиентский уровень занимает обозреватель, на уровне сервера находится сервер БД, на промежуточном уровне находятся Web-сервер и модули расширения сервера. Модуль расширения сервера выступает преобразователем протоколов между клиент-серверным приложением БД и Web-сервером. Сервер приложений также является промежуточным уровнем, который обеспечивает организацию взаимодействия клиентов и сервера БД. Данная архитектура позволяет решать различные задачи и получать различные преимущества. Но публикация БД в Интернете приводит к увеличению риска безопасности БД. Развитие архитектуры привело к появлению новых объектов, которые могут стать причинами реализации атак. Согласно архитектуре, данные объекты можно разделить на три уровня: уровень сети, уровень операционной системы (ОС) и уровень БД.

Объекты, разделенные по уровням, показаны в таблице.

Объекты воздействия

На уровне сети	Activex-объект Интерфейсы: OLE DB, ADO, ODBC, JDBC Протоколы: TCP/IP, IPX/SPX, Named Pipes, Multiprotocol Рабочие станции Серверы Маршрут URL
На уровне ОС	Аппаратное обеспечение Программное обеспечение Файлы базы данных Файлы журнала транзакций Файлы резервного копирования Transact-SQL, PLSQL Службы: MSSQLServer, SQLServerAgent, TNSListener и т. д.
На уровне БД	Пользователи Роли Роли приложения Диаграммы Представления Таблицы Хранимые процедуры Определения по умолчанию Правила Функции Тип данных Триггеры

Сформируем перечень внешних и внутренних угроз для СУБД. Внешнюю угрозу представляет любой человек, не имеющий санкционированного доступа к системе. Внутреннюю угрозу представляют люди, которые имеют санкционированный доступ к БД. Это могут быть конечные пользователи, администраторы и разработчики приложений.

Внешними дестабилизирующими факторами, создающими угрозы безопасности функционированию СУБД, являются:

– умышленные, деструктивные действия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы, причиной которых являются нарушения информационной безопасности защищаемого объекта;

– искажения в каналах передачи информации, поступающей от внешних источников;

– сбои и отказы в аппаратуре вычислительных средств;

– вирусы и иные деструктивные программные элементы, распространяемые с использованием систем телекоммуникаций, обеспечивающих связь с внешней средой или внутренние коммуникации распределенной СУБД;

– изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы за пределами, проверенными при тестировании или сертификации системы.

Среди внутренних угроз можно выделить следующие атаки:

– атаки со стороны авторизованных пользователей, направленные на повышение привилегий в системе управления базами данных;

– непреднамеренные ошибки сотрудников, которые по какой-либо причине нарушают установленную политику безопасности или применяют неверные методы безопасности;

– целенаправленное изменение или искажение хранимых данных;

– угрозы, возникающие из-за ошибок в программном обеспечении и неверной конфигурации системы;

– угрозы, возникающие из-за ошибок в аппаратном обеспечении и неверной их настройки.

В соответствии с приведенным выше выделением объектов на уровни, атаки на СУБД разделим на атаки на ОС, атаки на уровне сети и атаки на уровне БД.

Атаки на ОС, в которых функционирует СУБД, возникают гораздо чаще, т. к. защитить ОС гораздо сложнее, чем СУБД. Это обусловлено тем, что число различных типов защищаемых объектов в современных ОС может достигать нескольких десятков, а число различных типов защищаемых информационных потоков – нескольких сотен. Возможность практической реализации той или иной атаки на ОС в значительной мере определяется архитектурой и конфигурацией ОС. Тем не менее существуют атаки (перечислены ниже), которые могут быть направлены практически на любые ОС.

1. Кража ключевой информации. Данная атака может реализовываться с использованием следующих методов:

– подсматривание пароля при его вводе пользователем;

– получение пароля из командного файла. Некоторые ОС при сетевой аутентификации (подключении к серверу) допускают ввод пароля из командной строки. Если аутентификация происходит с использованием командного файла, пароль пользователя присутствует в этом файле в явном виде;

– некоторые пользователи, чтобы не забыть свой пароль, записывают его в записные книжки, на бумажки, которые затем приклеивают к нижней части клавиатуры, и т. д. Для злоумышленника узнать такой пароль не составляет никакого труда. Особенно часто такая ситуация имеет место, если администраторы заставляют сотрудников использовать длинные, труднозапоминаемые пароли;

– кража внешнего носителя ключевой информации. Некоторые ОС допускают использование вместо паролей внешних носителей информации (ключевые дискеты, Touch Memory, Smart Card и т. д.). Использование внешних носителей повышает надежность защиты ОС, но в этом случае появляется угроза кражи носителя с ключевой информацией;

– перехват пароля программной закладкой.

2. Подбор пароля. При данной атаке могут использоваться следующие методы:

– неоптимизированный перебор. В этом случае злоумышленник последовательно опробует все возможные варианты пароля. Для паролей длиннее шести символов во многих случаях данный метод может быть признан неэффективным;

– перебор, оптимизированный по статистике встречаемости символов и биграмм. Разные символы встречаются в паролях пользователей с разной вероятностью. Согласно различным исследованиям, статистика встречаемости символов в алфавите паролей близка к статистике встречаемости символов в естественном языке. При практическом применении данного метода злоумышленник вначале опробует пароли, состоящие из наиболее часто встречающих символов, за счет чего время перебора существенно сокращается. Иногда при подборе паролей используется не только статистика встречаемости символов, но и статистика встречаемости биграмм и триграмм – комбинаций двух и трех последовательных символов. Для подбора паролей по данному методу злоумышленник может использовать множество программ, в основном ориентированных на взлом ОС. При этом можно выделить две базовые технологии: явное опробование последовательно генерируемых паролей их подачей на вход подсистемы аутентификации и расчет значения хэш-функции и ее последующего сравнения с известным образом пароля;

– перебор, оптимизированный с использованием словарей вероятных паролей. При использовании данного метода подбора паролей злоумышленник вначале опробует в качестве пароля все слова из словаря, содержащего наиболее вероятные пароли. Если подбираемый пароль отсутствует в словаре, злоумышленник может опробовать всевозможные комбинации слов из словаря, слова из словаря с добавленными к началу или к концу одной или несколькими буквами, цифрами и знаками препинания и т. д.;

– перебор, оптимизированный с использованием знаний о пользователе. В этом случае в первую очередь злоумышленник пробует пароли, использование которых сотрудником представляется наиболее вероятным (имя, фамилия, дата рождения, номер телефона и т. д.);

– перебор, оптимизированный с использованием знаний о подсистеме аутентификации ОС. Если ключевая система ОС допускает существование эквивалентных паролей, при переборе из каждого класса эквивалентности опробуется всего один пароль.

Все перечисленные выше методы злоумышленник может применять в совокупности.

3. Сканирование жестких дисков компьютера. Данная атака заключается в последовательном считывании файлов, хранящихся на жестких дисках компьютера. Если при обращении к некоторому файлу или каталогу злоумышленник получает отказ, он просто продолжает сканирование дальше. Если объем жесткого диска компьютера достаточно велик, можно быть уверенным, что при описании прав доступа к файлам и каталогам этого диска администратор допустил хотя бы одну ошибку. При применении этой атаки все файлы, для которых были допущены такие ошибки, будут прочитаны злоумышленником. Несмотря на примитивность данной атаки, она во многих случаях оказывается весьма эффективной. Для ее реализации злоумышленник должен быть легальным пользователем ОС.

4. Данный метод можно применять не только для сканирования дисков локального компьютера, но и для сканирования разделяемых ресурсов локальной сети.

5. Превышение полномочий. Используя ошибки в программном обеспечении или администрировании ОС, злоумышленник получает в системе полномочия, превышающие предоставленные ему согласно текущей политике безопасности. Превышение полномочий может быть достигнуто следующими способами:

– запуск программы от имени пользователя, обладающего необходимыми полномочиями;

– запуск программы в качестве системной программы (драйвер, сервис, демон и т. д.), выполняющейся от имени ОС;

– подмена динамически подгружаемой библиотеки, используемой системными программами, или несанкционированное изменение переменных среды, описывающих путь к такой библиотеке;

– модификация кода или данных подсистемы защиты ОС.

6. Атаки класса «Отказ в обслуживании». Эти атаки нацелены на полный или частичный вывод ОС из строя. Существуют следующие атаки данного класса:

– захват ресурсов – программа захватывает все ресурсы компьютера, которые может получить. Например, программа присваивает себе наивысший приоритет и уходит в вечный цикл;

– бомбардировка трудновыполнимыми запросами – программа в вечном цикле направляет ОС запросы, выполнение которых требует больших затрат ресурсов компьютера;

– бомбардировка заведомо бессмысленными запросами – программа в вечном цикле направляет ОС заведомо бессмысленные (обычно случайно генерируемые) запросы. Рано или поздно в ОС происходит фатальная ошибка;

– использование известных ошибок в программном обеспечении или администрировании ОС.

Наиболее опасные атаки на СУБД исходят из сетей. Это в первую очередь обусловлено обилием протоколов, которые используются в сетях Интернет, и автономными программами небольшого размера, загруженными в пользовательские компьютерные системы. Эти протоколы и активные элементы могут создать серьезную угрозу для безопасности системы. На уровне сетевого программного обеспечения возможны следующие атаки на СУБД.

1. Прослушивание канала. Данная атака возможна только в сегменте локальной сети. Практически все сетевые карты поддерживают возможность перехвата пакетов, передаваемых по общему каналу локальной сети. При этом рабочая станция может принимать пакеты, адресованные другим компьютерам того же сегмента сети. Таким образом, весь информационный обмен в сегменте сети становится доступным злоумышленнику. Для успешной реализации этой атаки компьютер злоумышленника должен располагаться в том же сегменте локальной сети, что и атакуемый компьютер.

2. Перехват пакетов на маршрутизаторе. Сетевое программное обеспечение маршрутизатора имеет доступ ко всем сетевым пакетам, передаваемым через данный маршрутизатор, что позволяет осуществлять перехват пакетов. Для реализации этой атаки хакер должен иметь привилегированный доступ хотя бы к одному маршрутизатору сети. Поскольку через маршрутизатор обычно передается очень много пакетов, их тотальный перехват практически невозможен. Однако отдельные пакеты вполне могут быть перехвачены и сохранены для последующего анализа хакером. Наиболее эффективен перехват пакетов FTP, содержащих пароли пользователей.

3. Создание ложного маршрутизатора. Злоумышленник отправляет в сеть пакеты определенного вида, в результате чего его компьютер становится маршрутизатором и получает возможность осуществлять предыдущую угрозу. Ложный маршрутизатор необязательно заметен всем компьютерам сети – можно создавать ложные маршрутизаторы для отдельных компьютеров сети и даже для отдельных соединений.

4. Навязывание пакетов. Злоумышленник отправляет в сеть пакеты с ложным обратным адресом. С помощью этой атаки злоумышленник может переключать на свой компьютер соединения, установленные между другими компьютерами и получать необходимые данные от СУБД. При этом права доступа хакера становятся равными правам того пользователя, чье соединение с сервером было переключено на компьютер хакера.

5. Атаки класса «Отказ в обслуживании». Злоумышленник отправляет в сеть пакеты определенного вида, в результате чего один или несколько компьютеров сети полностью или частично выходят из строя.

6. Нелегальное внедрение разрушающих программных средств. Злоумышленник может использовать троянские программы, которые могут быть предназначены для исследования параметров информационной системы, сбора данных, зомбирования компьютера с последующим нецелевым расходованием ресурсов и т. д. Может быть осуществлено также заражение компьютера вирусами с деструктивными функциями.

Классификацию угроз на уровне базы данных проведем по результатам воздействия: угрозы конфиденциальности информации, угрозы целостности информации и угрозы доступности [5].

К угрозам конфиденциальности информации можно отнести следующие.

1. Инъекция SQL. Во многих приложениях используется динамический SQL – формирование SQL – формирование SQL-предложений кодом программы путем конкатенации строк и значений параметров. Зная структуру базы данных, злоумышленник может либо выполнить хранимую программу в запросе, либо закомментировать «легальные» фрагменты SQL-кода, внедрив, например, конструкцию UNION, запрос которой возвращает конфиденциальные данные. В последнее время злоумышленник может использовать специальные программы, автоматизирующие процесс реализации подобных угроз.

2. Логический вывод на основе функциональных зависимостей. Пусть дана схема отношения: $R(A_1, ..., A_n)$. Пусть $U = \{A_1, ..., A_n\}, X, Y$ – подмножества из U. X функционально определяет Y, если в любом отношении r со схемой $R(A_1, ..., A_n)$ не могут содержаться два кортежа с одинаковыми значениями атрибутов из X и с различными из Y. В этом случае имеет место функциональная зависимость, обозначаемая $X \to Y$. В реальных БД при наличии сведений о функциональных зависимостях злоумышленник может вывести конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение.

3. Логический вывод на основе ограничений целостности. Для кортежей отношений в реляционной модели данных можно задать ограничения целостности – логические условия, которым должны удовлетворять атрибуты кортежей. При этом ограничение целостности может быть задано в виде предиката на всем множестве атрибутов кортежа. В случае попытки изменить данные в таблице, СУБД автоматически вычисляет значение этого предиката, и в зависимости от его истинности операция разрешается или отвергается. Многократно изменяя данные и анализируя реакцию системы, злоумышленник может получить те сведения, к которым у него нет непосредственного доступа. К этому виду угроз можно отнести также анализ значений первичных/вторичных ключей.

4. Использование оператора UPDATE для получения конфиденциальной информации. В некоторых стандартах SQL пользователь, не обладая привилегией на выполнение оператора SELECT, мог выполнить оператор UPDATE со сложным логическим условием. Так как после выполнения оператора UPDATE сообщается, сколько строк он обработал, фактически пользователь мог узнать, существуют ли данные, удовлетворяющие этому условию.

Рассмотрим угрозы целостности информации, специфические для СУБД. С помощью SQL-операторов UPDATE, INSERT и DELETE можно изменить данные в СУБД. Опасность заключается в том, что пользователь, обладающий соответствующими привилегиями, может модифицировать все записи в таблице.

К угрозам доступности для СУБД можно отнести следующие.

1. Использование свойств первичных и внешних ключей. В первую очередь отнесем сюда свойство уникальности первичных ключей и наличие ссылочной целостности. В том случае, если используются натуральные, а не генерируемые системой значения первичных ключей, может создаться такая ситуация, когда в таблицу невозможно будет вставить новые записи, т. к. там уже будут записи с такими же значениями первичных ключей. Если в БД поддерживается ссылочная целостность, можно организовать невозможность удаления родительских записей, умышленно создав подчиненные записи.

2. Блокировка записей при изменении. Заблокировав записи или всю таблицу, злоумышленник может на значительное время сделать ее недоступной для обновления.

3. Загрузка системы бессмысленной работой. Злоумышленник может выполнить запрос, содержащий декартовое произведение двух больших отношений. Мощность декартового произведения двух отношений мощности N_1 и N_2 равна $N_1 \cdot N_2$. Это означает, что при выдаче злоумышленником запроса вида SELECT * FROM Tab1, Tab1 ORDER BY 1, где мощность отношения (количество строк в таблице Tab1) N_1 = 10 000, мощность результирующего отношения будет $N = N_1^2 = 10\,000^2$. Вычисление соединения и сортировка результирующего отношения потребуют значительных ресурсов системы и отрицательно скажутся на производительности операций других пользователей.

4. Использование разрушающих программных средств. Например, атака типа «троянский конь» – запуск пользователями программ, содержащих код, выполняющий определенные действия, внедренный туда злоумышленником.

Заключение

Разработка любой системы информационной безопасности должна основываться на определенном перечне потенциальных угроз безопасности и установлении возможных источников их возникновения. Так как если в системе существуют угрозы, для которых непредусмотрены какие-либо меры противодействия, то это может привести к тому, что все усилия, затраченные на возведение системы защиты, к ожидаемому результату не приведут. Поэтому при проектировании конкретной системы безопасности для любого объекта, в том числе и для СУБД, необходимо произвести всесторонний учет угроз и для каждой из них реализовать соответствующий угрозе метод защиты. В данной статье приводится классификация угроз безопасности для СУБД, которая позволяет уточнить угрозы различных классов на всех стадиях жизненного цикла информационной системы, построенной на основе реляционной СУБД.

СПИСОК ЛИТЕРАТУРЫ

1. *ГОСТ* Р ИСО / МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий / http:www.fstec.ru.
2. *Специальные* требования и рекомендации по технической защите конфиденциальной информации. – М.: СИПРИЛ, 2002. – 80 с.
3. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – Кн. 1. – 400 с.
4. *Хомоненко А. Д., Цыганков В. М., Мальцев М. Г.* Базы данных. – СПб.: КОРОНА принт, 2006. – 736 с.
5. *Смирнов С. Н.* Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 382 с.

Статья поступила в редакцию 27.11.2007

CLASSIFICATION OF THREATS IN SYSTEMS OF DATABASE MANAGEMENT

D. R. Utebov, S. V. Belov

The classification of threats in the systems of database management is given. The classification is made on the basis of the generalized scheme of classification of threats offered by V. A. Gerasimenko. The external and internal threats to databases are described. The threats are divided into three levels: the level of the network, the level of the operational system, the level of the database. At a level of operational system threats, characteristic for operational system under control of which the control system of databases works have been described. The classification of threats allows to consider the majority of possible threats to systems of database management on their designing.