МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ (ПРЕЗЕНТАЦИИ К ЛЕКЦИОННЫМ МАТЕРИАЛАМ)

Безопасность систем баз данных

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	специалист
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	10.03.01 «Информационная безопасность автоматизированных систем»
	(код и наименование)
Институт	Кибербезопасности и цифровых технологий
	(полное и краткое наименование)
Кафедра	Информационно-аналитические системы кибербезопасности (КБ-2)
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н., доцент Шукенбаев Айрат Бисенгалеевич
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/2024
(учебный год цифрами)

Проверено и согласовано «____» _____20___г.

_____ А.А. Бакаев
(подпись директора Института/Филиала с расшифровкой)

Москва 2024 г.

Ощущение полной безопасности наиболее опасно.
Илья Нисонович Шевелев
Везде, где есть жизнь, есть и опасность.
Ральф Уолдо Эмерсон

Безопасность систем баз данных.

Тема лекции: **Угрозы информационной безопасности баз данных**

Источники угроз информации баз данных. Классификация угроз информационной безопасности баз данных
Угрозы, специфичные для систем управления базами данных

операторы *GRANT, REVOKE*

КОМАНДА GRANT

Предположим, что пользователь Diane имеет таблицу Заказчиков и хочет позволить пользователю Adrian выполнить запрос к ней. Diane должна в этом случае ввести следующую команду:

GRANT INSERT ON Salespeople TO Adrian;

Когда SQL получает команду GRANT, он проверяет привилегии пользователя подавшего эту команду, чтобы определить допустима ли команда GRANT. Если Adrian - владелец таблицы Продавцов, то он может позволить Diane вводить в нее строки с помощью следующего предложения

GRANT INSERT ON Salespeople TO Diane;

Теперь Diane имеет право помещать нового продавца в таблицу.

КОМАНДА REVOKE

С помощью команды ***REVOKE осуществляется отмена привилегий***, синтаксис команды *REVOKE* аналогичен синтаксису команды *GRANT*.

Пример 1. Отмена привилегии ***CREATE TABLE*** на создание таблиц в базе данных у пользователя *user*

REVOKE CREATE TABLE FROM user;

Методы доступа к данным в БД:

Большинство современных реляционных СУБД поддерживает дискреционную (DAC) и мандатную (MAC) модели разграничения доступа.

Дискреционное управление доступом - это метод ограничения доступа к объектам, который основан на том, что некоторый субъект (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

Дискреционное разграничение доступа к объектам (Discretionary Access Control — DAC) характеризуется следующим набором свойств:

- все субъекты и объекты компьютерной системы должны быть однозначно идентифицированы;
- для любого объекта определен пользователь-владелец;
- владелец объекта обладает правом определения прав доступа к объекту со стороны любых субъектов;
- существует привилегированный пользователь, обладающий правом полного доступа к любому объекту.

К достоинствам дискреционного разграничения доступа относятся относительно простая реализация и хорошая изученность.

Недостатки дискреционного разграничения доступа. Прежде всего, к ним относится статичность разграничения доступа .

Дискреционные — управление доступом субъектов (пользователей или прикладных процессов) к объектам (фрагментам данных, файлам, сегментам БД) на основе списков управления доступом или матрицы доступа (матрицы безопасности). Каждому пользователю (прикладному процессу) предписывается право доступа к каждому фрагменту данных, если право не предоставлено, то его запросы к данному фрагменту данных игнорируются.

Мандатное разграничение доступа (Mandatory Access Control — MAC).

К основным характеристикам этой модели относится следующее:

- все субъекты и объекты должны быть однозначно идентифицированы;
- имеется линейно упорядоченный набор меток конфиденциальности и соответствующих им уровней допуска;
- каждому объекту присвоена метка конфиденциальности;
- каждому субъекту присваивается степень допуска;
- в процессе своего существования каждый субъект имеет свой уровень конфиденциальности, равный максимуму из меток конфиденциальности объектов, к которым данный субъект получил доступ;
- существует привилегированный пользователь, имеющий полномочия на удаление любого объекта системы;
- понизить метку конфиденциальности объекта может только субъект, имеющий доступ к данному объекту и обладающий специальной привилегией;
- право на чтение информации из объекта получает только тот субъект, чья степень допуска не меньше метки конфиденциальности данного объекта;
- право на запись информации в объект получает только тот субъект, чей уровень конфиденциальности не больше метки конфиденциальности данного объекта.

Целью мандатного разграничения доступа к объектам является предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности.

К другим достоинствам мандатного разграничения доступа относятся:

- более высокая надежность работы самой компьютерной системы, так как при разграничении доступа к объектам контролируется и состояние самой системы, а не только соблюдение установленных правил;
- большая простота определения правил разграничения доступа по сравнению с дискреционным разграничением.

Недостатки мандатного разграничения доступа к объектам компьютерной системы:

- сложность программной реализации, что увеличивает вероятность внесения ошибок и появления каналов утечки конфиденциальной информации;
- снижение эффективности работы компьютерной системы, так как проверка прав доступа субъекта к объекту выполняется не только при открытии объекта в процессе субъекта, но и перед выполнением любой операции чтения из объекта или записи в объект;
- создание дополнительных неудобств работе пользователей компьютерной системы, связанных с невозможностью изменения информации в не конфиденциальном объекте, если тот же самый процесс использует информацию из конфиденциального объекта.

Мандатные —разграничение доступа субъектов к объектам, основанное на назначении степени конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такой степени конфиденциальности. Каждому пользователю (прикладному процессу) назначается привилегия доступа (или ограничение на доступ) к каждой степени конфиденциальности, если субъект обращается к данным со степенью конфиденциальности, к которой он не допущен, то его запросы отклоняются.

Ролевые (*role based access control* - ***RBAC***)—развитие методов дискреционного доступа, при этом привилегии субъектов системы на объекты группируются с учётом специфики их применения, образуя роли. Все пользователи (прикладные процессы) объединяются в группы с одинаковым уровнем благонадежности и наследуют привилегии доступа к данным, назначенные для их уровня благонадежности.

Атрибутивные *(attribute based access control* - ***ABAC***) — метод доступа к объектам, основанный на наборе правил для атрибутов объектов или субъектов, возможных операций с ними и окружения, соответствующего запросу. Каждому уровню благонадежности пользователей (прикладных процессов) назначается совокупность привилегий и условий, при которых они реализуются, относительно каждой степени конфиденциальности данных, что позволяет учитывать условия обращения к данным, как дополнительный фактор в принятии решения о доступе.

Под угрозой понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угрозой ИБ АИС назовем возможность воздействия на информацию, обрабатываемую в системе, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты ИС, приводящего к утрате, уничтожению или сбою функционирования носителя информации или средства управления программно-аппаратным комплексом системы

Угроза нарушения конфиденциальности.

Угроза нарушения целостности.

Угроза нарушения доступности.

Первый шаг в анализе угроз – их идентификация.

Источники угроз информации баз данных

Внешними дестабилизирующими факторами являются:

— умышленные, деструктивные действия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы;

— искажения в каналах передачи информации, поступающей от внешних источников, циркулирующих в системе и передаваемой потребителям, а также недопустимые значения и изменения характеристик потоков информации из внешней среды и внутри системы;

— сбои и отказы в аппаратуре вычислительных средств;

— вирусы и иные деструктивные программные элементы;

— изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы за пределы, проверенные при тестировании или сертификации системы.

Внутренними источниками угроз безопасности СБД и СУБД являются:

— системные ошибки при постановке целей и задач проектирования автоматизированных информационных систем и их компонент, допущенные при формулировке требований к функциям и характеристикам средств обеспечения безопасности системы;

— ошибки при определении условий и параметров функционирования внешней среды, в которой предстоит использовать информационную систему;

— ошибки проектирования при разработке и реализации алгоритмов обеспечения безопасности аппаратуры, программных средств и баз данных;

— ошибки и несанкционированные действия пользователей, административного и обслуживающего персонала в процессе эксплуатации системы;

— недостаточная эффективность используемых методов и средств обеспечения информационной безопасности в штатных или особых условиях эксплуатации системы.

Классификация угроз информационной безопасности баз данных

Классификация по цели реализации угрозы:

- Нарушение конфиденциальности информации.
- Нарушение целостности информации.
- Полное или частичное нарушение работоспособности системы.

Классификация по природе возникновения угрозы:

- Естественные угрозы .
- Искусственные угрозы

Классификация по локализации источника угрозы представляется следующим образом:

1. Угрозы, непосредственным источником которых является человек:

— разглашение, передача или утрата атрибутов разграничения доступа;
— подкуп или шантаж обслуживающего персонала или пользователей;
— копирование конфиденциальных данных легальным пользователем системы с целью неправомерного;
— взлом системы защиты с целью выполнения деструктивных действий лицом, не являющимся законным пользователем системы;
— внедрение агентов фирм-конкурентов или преступных организаций в обслуживающий персонал атакуемой ИС.

2. Угрозы, непосредственным источником которых являются штатные программно-аппаратные средства ИС:

— неквалифицированное использование или ошибочный ввод параметров программ;
— неквалифицированное использование или ошибочный ввод параметров программ;
— отказы и сбои в работе операционной системы, СУБД и прикладных программ.

3. Угрозы, непосредственным источником которых являются несанкционированно используемые программно-аппаратные средства:
— нелегальное внедрение и использование программ;
— нелегальное внедрение и использование троянских программ;
— заражение компьютера вирусами с деструктивными функциями;
— работа генераторов шума и подобных источников электромагнитного излучения.
4. Угрозы, непосредственным источником которых является среда обитания:
— внезапное и длительное отключение систем электропитания;
— техногенные и природные катастрофы;
— всплески природных электромагнитных излучений.

Классификация по расположению источника угроз.

1. Угрозы, источник которых расположен вне контролируемой зоны места расположения АИС:
— нарушение нормальной работы или разрушение систем жизнеобеспечения зданий
— блокирование физического доступа на объект размещения автоматизированной системы обслуживающего персонала, пользователей;
— нарушение нормальной работы или разрушение внешних каналов связи
2. Угрозы, источник которых расположен в пределах контролируемой зоны расположения АИС:
— нарушение нормальной работы или разрушение систем электропитания и водоснабжения помещений;
— физическое разрушение линий связи или аппаратуры, обеспечивающей работу информационной системы;
— считывание конфиденциальной информации из аппаратных средств телекоммуникационной или вычислительной техники с использованием перехвата электромагнитных излучений;
— выведения из рабочего состояния обслуживающего персонала.
3. Угрозы, источник которых имеет доступ к терминальным устройствам АИС:
— получение параметров входа в систему и аутентифицирующей информации с использованием видеонаблюдения, клавиатурных закладок и технологий подбора паролей;
— получение параметров входа в систему и аутентифицирующей информации с использованием мошеннических приемов, насилия;
— получение возможности несанкционированного входа в систему в период, когда легальный пользователь покинул рабочее место, не завершив сеанс взаимодействия с системой;
— получение конфиденциальной информации из распечаток результатов выполнения запросов и иных выводимых системой данных.
4. Угрозы, источник которых имеет доступ к помещениям, где расположены серверы АИС:
— физическое разрушение элементов серверов и коммутационной аппаратуры;
— выключение электропитания серверов и коммутационной аппаратуры;
— остановка серверных и иных критически важных для функционирования автоматизированной системы процессов;
— уничтожение или модификация критически важных для функционирования АС файлов операционной системы;
— нарушение штатной работы базовой операционной системы;
— рассылка сообщений, дезорганизующих работу пользователей и обслуживающего персонала системы.

Классификация по способу воздействия на методы и средства хранения данных информационной системы.

1. Угрозы нарушения информационной безопасности данных хранимых на внешних запоминающих устройствах:

— нарушение конфиденциальности, уничтожение или модификация данных, сохраненных средствами создания резервных копий на магнитных носителях, путем незаконного восстановления баз данных с последующей заменой реальной копии или без таковой;

— нарушение конфиденциальности, уничтожение ил модификация данных, созданных штатными средствам ведения журнала изменений баз данных;

— дискредитация криптографических систем защиты информации путем создания копии носителей ключевой информации;

— создание несанкционированных копий файлов операционной системы, содержащих информацию баз данных для проведения последующего анализа с целью доступа к конфиденциальной информации.

2. Угрозы нарушения ИБ данных, хранимых в оперативной памяти серверов и клиентских компьютеров:

— изменение информации в оперативной памяти, используемой СУБД для кэширования данных, организации хранения промежуточных результатов выполнения запросов, констант и переменных процессов обработки данных;

— изменение информации в оперативной памяти, используемой операционной системой для кэширования данных, организации многопользовательского режима работы, констант и переменных процессов обработки данных;

— изменение информации в оперативной памяти, используемой прикладными программами в процессе организации и выполнения сессии взаимодействия с сервером баз данных и прослушивающим процессом.

3. Угрозы нарушения ИБ данных, отображаемой на терминале пользователя или принтере:

— организация имитации процесса установления взаимодействия с сервером с целью получения идентификаторов и аутентифицирующей информации пользователей;

— изменение элементов данных, выводимых на терминал пользователя за счет перехвата потока вывода;

— изменение элементов данных, выводимых на принтер за счет перехвата потока вывода.

Классификация по характеру воздействия на информационную систему (целесообразно выделить два варианта):

— активное воздействие;
— пассивное воздействие.

Математической модели первого приближения уровень обеспечения ИБ некоторой ИС может рассматриваться как многомерный вектор, включающий характеристики нескольких независимых измерений:

— физического;
— технологического;
— логического (процедурного);
— человеческого.

Угрозы, специфичные для систем управления базами данных

Существует несколько оснований для классификации угроз, специфичных для СУБД. Будем использовать упрощенную классификацию угроз по следующим основаниям:

– угрозы конфиденциальности информации;
– угрозы целостности информации;
– угрозы доступности.

Угрозы конфиденциальности информации.

К угрозам такого типа можно отнести:

1. Инъекция SQL (конструкция UNION)

2. Логический вывод на основе функциональных зависимостей.

Пусть дана схема отношения: *R(A1, …, An)*. Пусть *U= (A1, …, An)*, *X, Y* – подмножества из *U*. Говорят, что *X* функционально определяет *Y*, если в любом отношении r со схемой *R(A1, …, An)* не могут содержаться два кортежа с одинаковыми значениями атрибутов из *X* с различными из *Y*. В этом случае имеет место функциональная зависимость, обозначаемая *X* > *Y*.

Логический вывод на основе ограничений целостности

Использование оператора *UPDATE* для получения конфиденциальной информации. Оператор *SELECT*, мог выполнить оператор *UPDATE* со сколь угодно сложным логическим условием.

Угрозы целостности информации, специфические для систем управления базами данных.

Модификация данных в реляционных СУБД возможна с помощью SQL операторов *UPDATE*, *INSERT* и *DELETE* оператором *CHECK*

Специфичными для систем управления базами данных угрозами доступности являются:

1. Использование свойств первичных и внешних ключей

Блокировка записей при изменении

2. Загрузка системы бессмысленной работой. Простейший пример – выполнение запроса, содержащего декартово произведение двух больших отношений. Мощность декартового произведения двух отношений мощности N1 и N2, равна N1 * N2. Т.е. при выдаче злоумышленником запроса вида *SELECT * FROM Tab 1, Tab 1 ORDER BY 1,*

где мощность отношения (количество строк в таблице Tab 1) = 10000,

мощность результирующего отношения будет $N = N1^2 = 10000^2 = 100\ 000\ 000$.

Большинство современных реляционных СУБД поддерживает дискреционную (DAC) и мандатную (MAC) модели разграничения доступа.