Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Н. Ф. Чикунова

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент
доцент кафедры информационной безопасности
института цифровых технологий ФГБОУ ВО «КГТУ»
А. Г. Жестовский

Чикунова, Н. Ф.

Безопасность систем баз данных: учебно-методическое пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / Н. Ф. Чикунова. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. –41 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Безопасность систем баз данных» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». В нем представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, указания к изучению каждой темы. Содержатся требования к текущей и промежуточной аттестации, определены условия получения положительной оценки.

Табл. 1, список лит. – 30 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 14 июня 2022 г., протокол № 09

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала методической комиссией Института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 04

.

ОГЛАВЛЕНИЕ

1. Введение

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», изучающих дисциплину «Безопасность систем баз данных».

Цель освоения дисциплины: формирование у обучаемых компетенций, необходимых для профессиональной деятельности в области обеспечения информационной безопасности систем баз данных, их теоретическая и практическая подготовка по вопросам безопасности систем баз данных, освоение основных положений теории баз данных, методов решения задач, связанных с проблемами обеспечения их информационной безопасности на этапах проектирования и эксплуатации.

В результате освоения дисциплины ожидается, что студенты получат целостное представление о методах абстрагирования данных; характеристиках и типах систем БД; областях применения СУБД; этапах проектирования БД; средствах поддержания целостности; критериях защищенности БД; угрозах безопасности БД; критериях и методах оценивания механизмов защиты; особенностях организации средств защиты в распределенных СУБД.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют «Информатика», «Языки программирования», «Безопасность операционных систем», «Основы информационной безопасности», «Теория информации», «Безопасность сетей электронных вычислительных машин», «Правовое обеспечение информационной безопасности».

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных/практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребует больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе Содержание дисциплины приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

В разделе «Система оценивания» приведен порядок применения традиционной пятибалльной системы контроля успеваемости.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Для обеспечения образовательного процесса по дисциплине необходимо следующее программное обеспечение:

- программное обеспечение Microsoft Desktop Education (операционная система Windows Desktop operating system, офисные приложения: Microsoft Office, включая СУБД MS Access) по соглашению V9002148 Open Value Subscription от 05.07.2018, контракт №03351000161180000073-0484577-02);
- Антивирусное программное обеспечение Kaspersky Total Space Security Russian Edition, лицензия 17EO-171225-104659-470-270, срок использования с 2017-12-26 до 2020-03-13;
- СУБД MS SQL 5.0, DB Designer 4.0, My SQL WorkBench 8.0 12 - лицензия: свободная GNU General Public Licence / проприетарная EULA;
- доступ к ресурсам сети «Интернет».

2. Тематический план

Тематический план изучения дисциплины «Безопасность систем баз данных» представлен в таблице 1.

Таблица 1

Тематический план изучения дисциплины «Безопасность систем баз данных»

№ темы	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч
		Лекции	
1	2	3	4
1.1	Введение в безопасность систем баз данных	Тема 1.1 Введение в дисциплину. Назначение и роль баз данных. Модели данных. История развития вопроса безопасности баз данных. Безопасность систем баз данных. Актуальность проблемы. Основные понятия	4
1.2		Тема 1. 2 Этапы научного формирования проблемы информационной безопасности систем баз данных. Структура свойства информационной безопасности баз данных	4
2.1	СУБД – средства управления данными в БД. Проектирование реляционных баз данных	Тема 2.1. СУБД – средства управления данными в БД. Проектирование баз данных. Инфологическое моделирование предметной области БД.	4
2.2		Тема 2.2. Реляционные базы данных. Обеспечение целостности реляционных БД путем нормализации их отношений	4
2.3		Тема 2.3. Проектирование баз данных. Решение проблем информационной безопасности на различных этапах проектирования	4

Продолжение таблицы 1

1	2	3	4
3.1	Эксплуатация баз данных и организация их защиты	Тема 3.1. Основы безопасности БД. Руководящие материалы	4
3.2		Тема 3.2. Эксплуатация баз данных. Состав и проведение регламентных работ	4
3.3		Тема 3.3. СУБД. Языковые средства описания, манипулирования, запросов. Функции и использование	4
3.4		Тема 3.4. Распределенная обработка данных. Архитектура систем управления базами данных	4
3.5		Тема 3.5. Угрозы информационной безопасности баз данных. Источники угроз. Классификация угроз информационной безопасности баз данных	4
3.6		Тема 3.6 Политика безопасности	4
3.7		Тема 3.7 Средства защиты систем баз данных	4
3.8		Тема 3.8 Обеспечение целостности баз данных. Структурная, языковая, ссылочная целостность. Способы поддержки семантической целостности. Администрирование баз данных.	4
3.9		Тема 3.9. Обеспечение согласованности данных в многопользовательском режиме обработки. Понятие транзакции. Идентификация и аутентификация пользователей	4
3.10		Тема 3.10 Дискреционная защита. Представления	4
3.11		Тема 3.11 Мандатная защита	4
3.12		Тема 3.12 Многоуровневая модель безопасности. Защита данных при статистической обработке	4
ИТОГО			**68**

Продолжение таблицы 1

1	2	3	4
		Практические (лабораторные занятия)	
2.1	СУБД – средства управления данными в БД. Проектирование реляционных баз данных	Инфологическое моделирование предметной области.	2
		Нормализация отношений баз данных	4
		Автоматизация проектирования БД. Моделирование структуры БД в Case-средстве DB Designer	2
		Проектирование баз данных в СУБД MS Access. Сортировка и фильтрация записей	2
		Построение схемы данных. Обеспечение целостности данных как одного из аспектов информационной безопасности БД.	2
		Изучение технологии проектирования запросов в СУБД Access	2
		Проектирование экранных форм в СУБД MS Access. Ввод и анализ данных с помощью форм	2
		Вывод результатов обработки данных в виде отчетов	2
		Технология создания кнопочной формы	2
		Использование пароля для шифрования базы данных в СУБД MS ACCESS	2
3.1	Эксплуатация баз данных и организация их защиты	Создание SQL запросов. Изучение возможностей оператора Select	4
		Операторы языка SQL для манипулирования данными	2

Окончание таблицы 1

1	2	3	4
		Операторы языка SQL для манипулирования таблицами	2
		Организация защиты баз данных в СУБД Access. Шифрование баз данных паролем	2
		Изучение средств защиты баз данных на уровне пользователя	2
		Работа с центром управления безопасностью в СУБД Access по организации защиты БД	2
		Проектирование защищенной БД в СУБД Access. Самостоятельная работа	8
		Проектирование баз данных в СУБД MySQL. Работа с таблицами.	2
		Ввод данных в таблицы СУБД MySQL.	2
		Проектирование запросов в СУБД MySQL.	2
		Редактирование данных в таблицах в СУБД MySQL	2
		Администрирование БД и обеспечение их безопасности в СУБД MySQL. Работа с учетными записями пользователей	2
		Система привилегий доступа в СУБД MySQL. Реализация контроля доступа пользователей	**2**
		Резервирование базы данных в СУБД MySQL	**2**
		Профилактическая проверка таблиц и их восстановление в СУБД MySQL.	**2**
		Просмотр журналов работы в СУБД MySQL.	**2**
		Проектирование базы данных в СУБД MySQL и ее интеграция в Internet. Организация защиты БД. Самостоятельная работа	6
		ИТОГО	**68**

3. Содержание дисциплины и указания к изучению

3.1 Раздел 1. Введение в безопасность систем баз данных

3.1.1 Тема 1.1 Введение в дисциплину. Назначение и роль баз данных. История развития вопроса безопасности баз данных. Безопасность систем баз данных. Актуальность проблемы. Основные понятия.

Перечень изучаемых вопросов:

Предмет и задачи дисциплины.

Общие требования к хранению информации.

Назначение и роль баз данных в составе автоматизированных информационных систем.

Классификация задач, решаемых с использованием технологии баз данных.

Модели данных.

Исторические аспекты формирования проблемы обеспечения информационной безопасности систем баз данных в мировой и отечественной практике.

Актуальность проблемы безопасности систем баз данных.

Аспекты рассмотрения вопросов информационной безопасности систем баз данных.

Уровни информационной системы, на которых должна строиться комплексная система обеспечения информационной безопасности.

Общая характеристика анализа безопасности СУБД.

Модели доступа: дискреционная, мандатная и ролевая.

Понятие роли, представления, триггера.

Шифрование баз данных.

Обеспечение безопасности при взаимодействии с внешними объектами.

Инсайдерские риски при обеспечении безопасности СУБД.

Методические указания к изучению:

Лекция является основной формой обучения в высшем учебном заведении. Записи лекций в конспектах должны быть избирательными, полностью следует записывать определения и основные положения, на которых делается акцент. В конспекте следует применять сокращение слов, что ускоряет запись. Вопросы, возникающие в ходе лекции, рекомендуется записывать на полях и после окончания лекции обратиться за разъяснением к преподавателю.

Студентам рекомендуется активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях. Конспекты лекций следует использовать при подготовке к практическим занятиям, при выполнении самостоятельных заданий и курсовой работы, при подготовке к экзамену.

Для более глубокого изучения материала и расширения кругозора по изучаемой тематике необходимо пользоваться учебной и научной литературой. Для этого следует использовать ссылки на подборку рекомендуемой литературы, достаточной для изучения предлагаемой темы. В конце учебно-методического пособия дисциплины представлены списки основной и дополнительной литературы. Они носят рекомендательный характер, это означает, что всегда есть литература, которая может не входить в данный список, но является необходимой для освоения темы. При этом следует иметь в виду, что нужна литература различных видов: учебники, учебные и учебно-методические пособия; первоисточники, монографии, сборники научных статей, публикации в журналах, любой эмпирический материал; справочная литература – энциклопедии, словари, тематические, терминологические справочники, раскрывающие категориально-понятийный аппарат. Для более глубокого изучения нормативной документации, регламентирующей вопросы обеспечения безопасности систем баз данных, следует пользоваться справочными информационными системами «Консультант Плюс» или «Гарант».

Перечень рекомендуемой литературы по изучаемой тематике приведен в данном разделе ниже. Кроме того, рекомендуется ознакомиться с презентацией по изучаемой теме «Лекция 1», представленной в ЭИОС.

При изучении теоретического материала рекомендуется придерживаться порядка, указанного в перечне изучаемых вопросов. При изучении данной темы следует уяснить, что является предметом дисциплины и каковы ее задачи. В настоящее время информационные ресурсы предприятий и организаций как в сфере государственного управления, экономике, обороне, так и образовании рассматриваются в качестве одного из наиболее ценных активов. По мере увеличения объемов и ценности информации, хранимой в базах, возрастают и общие требования к хранению информации. Студенту необходимо уяснить, какие именно. Обратить внимание, что хранилищем информации в любой информационной системе являются базы данных. Отсюда вытекает важность поиска эффективных методов решения проблемы обеспечения информационной безопасности (ИБ) автоматизированных систем, которые определены в Доктрине ИБ Российской Федерации, утвержденной Указом Президента Российской Федерации 9 сентября 2000 г. и 5 декабря 2016 г.

При изучении темы следует обратить внимание на классификацию задач, решаемых с использованием технологии баз данных. Важным моментом

для дальнейшего изучения технологии проектирования баз данных является знание моделей данных.

Проблемы обеспечения информационной безопасности имеют исторические корни, излагаемые в лекционном материале.

Следует обратить внимание, что вопросы ИБ баз данных целесообразно рассматривать с двух взаимодополняющих позиций: 1) оценочных стандартов, направленных на классификацию информационных систем и средств их защиты по требованиям безопасности; 2) технических спецификаций, регламентирующих различные аспекты реализации средств защиты.

При изучении уровней, на которых строится комплексная система обеспечения информационной безопасности, важное место занимает уровень СУБД, обеспечивающий хранение и обработку данных информационной системы.

Особое внимание следует обратить на общую характеристику анализа безопасности СУБД. Студенты должны ознакомиться с существующими моделями доступа: дискреционной, мандатной и ролевой. Изучить понятия роли, представления, триггера. Получить представление о таком способе защиты, как шифрование баз данных. Кроме того, ознакомиться с вопросами обеспечения безопасности при взаимодействии с внешними объектами. Получить представление об инсайдерских рисках при обеспечении безопасности СУБД.

Литература:

1. [2, с. 6-16].
2. [13, с.8-11].
3. [16, с.29-34].

Контрольные вопросы:

1. Что является предметом изучения дисциплины?
2. Каковы задачи дисциплины «Безопасность систем баз данных»?
3. Назовите требования к хранению информации.
4. Какова роль баз данных в составе автоматизированных информационных систем?
5. Перечислите задачи, решаемые с использованием технологии баз данных.
6. Назовите основные модели данных.
7. Обоснуйте актуальность проблемы безопасности систем баз данных.
8. Назовите, с каких позиций следует рассматривать вопросы информационной безопасности систем баз данных.
9. На каких уровнях информационной системы должна строиться комплексная система обеспечения информационной безопасности?

10. Дайте общую характеристику анализа безопасности СУБД.

11. Перечислите известные Вам модели доступа.

12. Дайте понятие роли, представления, триггера.

13. Как можно обеспечить безопасность при взаимодействии с внешними объектами?

14. Что такое инсайдерские риски при работе с СУБД?

3.1.2 Тема 1.2 Этапы научного формирования проблемы информационной безопасности систем баз данных. Структура свойства информационной безопасности баз данных

Перечень изучаемых вопросов:

Характеристика этапов научного формирования проблемы информационной безопасности систем баз данных.

Документы и стандарты в области формирования защищенных компьютерных систем.

Классификация АИС по уровню защищенности.

Сущность проблемы обеспечения информационной безопасности систем баз данных.

Обеспечение конфиденциальности баз данных.

Обеспечение доступности баз данных.

Обеспечение целостности баз данных.

Методические указания к изучению:

При изучении данной темы следует обратиться к истории вопроса, прежде всего, изучить основные этапы научного формирования проблемы обеспечения ИБ БД. В чем состояли основные концепции и технологии защиты данных в СУБД. Каковы были подходы к анализу защищенных систем.

Особое внимание следует обратить на перечень документов и стандартов в области формирования защищенных компьютерных систем. В результате изучения темы студент должен будет знать, как классифицируются АИС по уровню защищенности.

Для успешного освоения курса необходимо уяснить сущность проблемы обеспечения информационной безопасности систем баз данных. Обратить внимание на проблему обеспечения конфиденциальности баз данных, доступности баз данных, а также целостности баз данных, которые в совокупности обеспечивают их комплексную защиту.

Для студентов, пропустивших лекцию, следует самостоятельно ознакомиться с презентацией «Лекция 2» и изучить рекомендуемую литературу.

Литература*:*
1. [2, с. 17- 23, 28-29, 41-45].

Контрольные вопросы:

1. Назовите основные этапы научного формирования проблемы информационной безопасности систем баз данных и дайте их краткую характеристику.
2. Какое название получил документ «Критерии оценки надежных компьютерных систем» 1983 года выпуска?
3. Какое название получил документ интерпретация «Критериев оценки надежных компьютерных систем» 1991 года выпуска?
4. Какие документы и стандарты в области формирования защищенных компьютерных систем были приняты в Российской Федерации?
5. Приведите классификацию автоматизированных информационных систем по уровню защищенности.
6. В чем заключается сущность проблемы обеспечения информационной безопасности систем баз данных?
7. Какие меры предусматриваются для обеспечения конфиденциальности баз данных?
8. Какие меры предусматриваются для обеспечения доступности баз данных?
9. Что такое целостность? Какие меры предусматриваются для обеспечения целостности баз данных.

3.2 Раздел 2. СУБД – средства управления данными в БД. Проектирование реляционных баз данных

3.2.1 Тема 2.1 СУБД – средства управления данными в БД. Проектирование баз данных. Инфологическое моделирование предметной области БД

Перечень изучаемых вопросов:

Понятие СУБД.

Общие принципы их построения.

Обзор и сравнительный анализ современных СУБД.

Концептуальные основы реляционных БД. Основные понятия СУБД, компоненты, языки. Этапы проектирования реляционных баз данных.

Состав и архитектура СУБД. Информационное, лингвистическое, математическое, аппаратное, организационное, правовое обеспечения СУБД.

Инфологический подход к проектированию БД. Цель инфологического моделирования. Подходы к инфологическому проектированию: функциональный, предметный и метод «сущность – связь». Понятие сущности, атрибутов сущности, ключа и связей сущностей. Характеристика связей и язык моделирование ER-диаграмм.

Методические указания к изучению:

Для успешного освоения дисциплины студентам, прежде всего, необходимо освоить понятийный аппарат баз данных и систем управления базами данных, знать их принципы построения. В настоящее время существует множество различных СУБД, поэтому следует знать их разновидности функциональные возможности. В практике используются следующие типы БД: фактографические, документальные, распределенные, централизованные, реляционные, неструктурированные.

Обсуждение вопроса постановки задачи обеспечения ИБ БД не может не включать анализ архитектуры системы, поскольку СУБД является комплексом взаимодействующих программных компонент. Студентам необходимо уяснить такие понятия, как сервер, сервер баз данных, клиент, в чем состоит «клиент – серверная» технология, сервер приложений, картриджи БД, картриджи серверов приложений, картриджи на клиенте.

Следует внимательно изучить структуру свойства информационной безопасности, поскольку она определяет подходы разработке средств и методов по ее обеспечению.

Одним из важных этапов проектирования базы данных является изучение предметной области, проектируемой БД и построении ее инфологической модели. Поэтому следует уделить внимание изучению инфологического подхода на основе метода «сущность – связь». На эту тему предусмотрено выполнение лабораторной работы.

Литература:

1. [18, с.9-12, 14-19].
2.[2, с. 35-45].

Контрольные вопросы:

1. Дайте определение баз данных. Каковы их общие принципы их построения?
2. Что такое СУБД?

3. Назовите основные функции СУБД.

4. Приведите классификацию СУБД.

5. Перечислите этапы проектирования реляционных баз данных.

6. Каков состав и архитектура СУБД?

7. Приведите определение сервера, клиента.

8. Что такое «клиент – серверная» технология?

9. Дайте понятие сервера базы данных и сервера приложении. Как они взаимодействуют?

10. Что такое сущность, атрибут сущности?

11. Что представляет собой связь сущностей в инфологической модели?

3.2.2 Тема 2.2 Реляционные базы данных. Обеспечение целостности реляционных БД путем нормализации их отношений

Перечень изучаемых вопросов:

Использование нормальных форм при проектировании приложений в реляционных СУБД.

Аномалии при эксплуатации баз данных.

Нормализация отношений.

Разновидности нормальных форм и их характеристика.

Методологии проектирования.

Этапы нормализации отношений.

Методические указания к изучению:

Одной из наиболее сложных для освоения тем является нормализация отношений баз данных. Изучению данной темы следует уделить должное внимание по следующим причинам. В процессе проектирования необходимо соблюдать требования по обеспечению безопасности создаваемой базы данных, одним из которых является обеспечение ее целостности. В свою очередь, задача обеспечения целостности подразумевает комплекс мер по предотвращению непреднамеренного изменения или уничтожения информации, хранящейся в БД. Одной из причин, приводящих к таким негативным ситуациям, является избыточность информации, которая означает дублирование одних и тех же данных в таблицах. Избыточность приводит к аномалиям модификации в базе данных при редактировании, добавлении или удалении записей, увели-

чивает размер базы данных, усложняет выборку информации. Поэтому устранение избыточности входит в комплекс задач по обеспечению целостности проектируемой БД.

Для самостоятельного освоения изучаемого материала рекомендуется проработать материал презентации «Лекция 3». Практические навыки по обеспечению целостности БД будут отработаны на соответствующем лабораторном занятии.

Литература:

1. [13, с. 24-32].
2. [14, с.154-171].

Контрольные вопросы:

1. Дайте определение следующим элементам таблицы БД: поле, ячейка, запись.
2. Что означает понятие «ключ», «ключевое поле»?
3. Какое поле называют первичным ключом, а какое – внешним?
4. В чем состоит процесс нормализации таблиц БД?
5. Назовите известные Вам виды нормальных форм.
6. Что означает, что таблица находится в первой нормальной форме?
7. Что означает, что таблица находится во второй нормальной форме?
8. Что означает, что таблица находится в третьей нормальной форме?

3.2.3. Тема 2.3. Проектирование баз данных. Решение проблем информационной безопасности на различных этапах проектирования

Перечень изучаемых вопросов:

Цели и этапы процесса проектирования БД.

Основные подходы к решению проблем обеспечения информационной безопасности на различных этапах проектирования баз данных.

Методические указания к изучению:

В данной теме необходимо уяснить цели и этапы процесса проектирования БД, знать, что выполняется на каждом этапе проектирования, какие проблемы, связанные с обеспечением безопасности БД, должны решаться на каждом этапе.

Особое внимание следует акцентировать на том, какие требования предъявляются к проекту с точки зрения обеспечения безопасности БД. По

данной теме рекомендуется ознакомиться с презентацией «Лекция 5». Практические навыки по проектированию базы данных с точки зрения обеспечения ее безопасности отрабатываются на лабораторных работах.

Литература:
1. [13, с. 72-75].

Контрольные вопросы:
1. Сформулируйте цели и этапы процесса проектирования базы данных.
2. Охарактеризуйте каждый этап проектирования БД.
3. Сформулируйте требования к проектируемой базе данных с точки зрения ее безопасности.

3.3 Раздел 3 Эксплуатация баз данных и организация их защиты

3.3.1 Тема 3.1 Основы безопасности БД. Руководящие материалы

Перечень изучаемых вопросов:

Актуальность проблемы контроля безопасности баз данных.
Задачи по обеспечению безопасности баз данных.
Обзор основных руководящих документов, регламентирующих вопрос информационной безопасности в части, касающейся безопасности баз данных.

Методические указания к изучению:

Информационная безопасность баз данных (Database security) представляет собой систему мер и средств, направленная на защиту сведений, находящихся БД различного типа. Проблема контроля безопасности баз данных всегда остается актуальной. Информация, содержащаяся в БД, всегда является предметом интереса третьих лиц, и чем больше БД, тем более серьезного уровня защиты она требует.

Следует иметь в виду, что структурированная и систематизированная информация, размещенная в управляемых базах данных (СУБД), находящихся на выделенных серверах, легче поддается обработке и анализу, используется при выстраивании бизнес-процессов. Интерес у злоумышленников она вызывает больший, чем неструктурированная информация в разрозненных файлах и кратковременной памяти. Поэтому основными задачами по обеспечению безопасности становятся:

1. защита информации от несанкционированного доступа (НСД) инсайдеров или внешних заинтересованных лиц;

2. предотвращение уничтожения данных. Механизмы современных DBMS (систем управления СУБД, Database Management System) способны вычислить частично стертую и поврежденную информацию и откорректировать ошибку, поэтому речь идет об обеспечении безопасности от рисков полного уничтожения содержимого базы;

3. защита от программных и аппаратных ошибок, сложностей с доступом к серверу, которые затрудняют или создают невозможность для пользователей обрабатывать информацию, содержащуюся в базах.

Задачи решаются различными способами, выбор средств обеспечения безопасности основывается на понимании угроз, направленных на содержимое БД. Более подробно виды угроз будут рассмотрены ниже.

Поскольку первой задачей по обеспечению безопасности базы данных становится разграничение прав доступа и определение привилегий, позволяющих системным администраторам осуществлять управление, а пользователям получать доступ к данным, студентам следует обратить внимание на эти вопросы. Выделяют два типа привилегий: системные привилегии и привилегии объектов.

Системные позволяют администратору выполнять управленческие действия по отношению к базе и содержащимся в ней информационным объектам.

Объектные привилегии определяют объем прав пользователя при работе с информационными объектами с учетом ограничений, диктуемых безопасностью.

После определения объема привилегий встает вопрос разграничения прав доступа, что позволяет отсечь от информационных массивов пользователей, не имеющих определенного объема прав, например, сотрудников других подразделений компании. Если система управления предприятием сертифицируется по одному из международных стандартов, например, ISO 9001, и в БД содержится информация, используемая для формирования публичной отчетности, обязательной задачей становится разграничение привилегий, при этом третье лицо, не являющееся разработчиком БД, проводит аудит наличия разграничений. Должно быть подтверждение того, что лицу предоставлено наименьшее количество привилегий при работе с базами данных и не предложено избыточных прав на управление программой или изменение информации. Проблема завышенных привилегий отмечается экспертами как одна из основных уязвимостей, характерных для СУБД.

В единых для всей компании базах данных в целях безопасности сведений встает вопрос разграничения прав пользователей на доступ к различным информационным объектам, содержащимся в БД. Этот вопрос безопасности

решается с использованием различных программных средств, позволяющих присвоить маркеры пользователям и объектам. Операции становятся возможными только при совпадении маркеров. В современных СУБД решена задача разграничения доступа не только к элементам БД – файлам, документам, записям, но и к структурным параметрам, таким как элемент, поле, запись, набор данных.

В настоящий момент существует большое количество подходов к обеспечению и управлению информационной безопасностью. Наиболее эффективные из них формализованы в стандарты.

Международные стандарты и методологии в области ИБ и управления ИТ являются ориентиром при построении информационной безопасности, а также помогают в решении связанных с этой деятельностью задач всех уровней, как стратегических и тактических, так и операционных. Поэтому студентам следует разобраться в идеях популярных зарубежных стандартов и в том, как они могут применяться в отечественной практике.

Для расширения кругозора по изучаемой тематике студентам рекомендуется самостоятельно ознакомиться с документами, регламентирующими вопросы информационной безопасности в части, касающееся безопасности баз данных. Прежде всего, следует ознакомиться с перечнем актуальных национальных стандартов в области информационной безопасности, разработанных ТК 362 и принятых Ростехрегулированием (Росстандартом).

Литература:

1. [2, с.19 – 23, 325-333].
2. [34].
3. [35].

Контрольные вопросы:

1. Сформулируйте понятие информационной безопасности баз данных.
2. Почему проблема контроля безопасности БД всегда является актуальной?
3. Перечислите задачи по обеспечению безопасности БД.
4. Что такое привилегии? Какие они бывают?
5. Назовите известные Вам российские и отраслевые стандарты регламентирующие вопросы информационной безопасности в части, касающейся безопасности баз данных.
6. Сформулируйте основную идею международного стандарта ISO/IEC 15408, известного под названием «Общие критерии». Какой российский стандарт был принят на основе его аутентичного текста?

3.3.2 Тема 3.2. Эксплуатация баз данных. Состав и проведение регламентных работ

Перечень изучаемых вопросов:

Состав, порядок планирования и проведения регламентных работ.

Плановое создание резервных копий с последующей проверкой без восстановления.

Плановое восстановление ранее созданных резервных копий с целью полной проверки их работоспособности.

Анализ носителей информации, на которых расположены системные и все необходимые базы данных.

Плановая проверка работы необходимых служб.

Плановая оптимизация производительности системы.

Плановая проверка целостности данных. Плановая проверка корректности данных.

Методические указания к изучению:

Изучение вопросов темы следует проводить в соответствии с указанным выше перечнем. В данной теме необходимо акцентировать внимание на видах основных регламентных работ с БД.

Для изучения материала рекомендуется ознакомиться с презентацией «Лекция 6».

Литература:

1.[4, С. 338-346]

Контрольные вопросы:

1. Назовите известные Вам основные регламентные работы с базой данных.

2. В каком порядке выполняются регламентные работы?

3. Кто отвечает за проведение регламентных работ?

4. Как создать резервную копию и провести ее проверкой без восстановления?

5. Как восстановить ранее созданную резервную копий БД с целью полной проверки их работоспособности?

6. Как осуществляется анализ носителей информации, на которых расположены системные и все необходимые базы данных?

7. Кто осуществляет плановую проверку работы необходимых служб.

8. Как выполнить плановую оптимизацию производительности системы?

9. Как осуществляется плановая проверка целостности данных?

10. Как осуществляется плановая проверка корректности данных?

3.3.3 Тема 3.3. СУБД. Языковые средства описания, манипулирования, запросов. Функции и использование

Перечень изучаемых вопросов:

Назначение языковых средств СУБД, их разновидности и характеристики.

Структурированный язык запросов SQL.

Операторы определения данных.

Операторы манипулирования данными.

Оператор запросов.

Операторы администрирования данными.

Операторы управления курсором.

Операторы управления действиями (транзакциями).

Методические указания к изучению:

В данной теме необходимо ознакомиться с видами языковых средств для работы с СУБД, выяснить их назначение, характеристики и возможности. Одним из наиболее популярных языков средств является универсальный язык запросов SQL. Студентам рекомендуется изучить синтаксис различных операторов по созданию запросов, определению данных и манипулированию ими, операторов по администрированию данными, управлению курсором и операторов управления действиями (транзакциями).

В презентации «Лекция 7» можно подробно ознакомиться с изучаемым материалом. При выполнении лабораторных работ буду отрабатываться навыки использования языка SQL при эксплуатации БД.

Литература:

1. [1, с.5 - 20].
2. [13, с. 183 – 191].
3. [14, с. 98 -107].

Контрольные вопросы:

1. Каково назначение языковых средств СУБД?
2. Назовите разновидности языковых средств СУБД и приведите их характеристики.
3. Охарактеризуйте структурированный язык запросов SQL.
4. Запишите операторы определения данных.
5. Запишите операторы манипулирования данными.
6. Запишите оператор запросов.
7. Запишите операторы администрирования данными.
8. Запишите операторы управления курсором.
9. Запишите операторы управления действиями (транзакциями).

3.3.4 Тема 3.4. Распределенная обработка данных. Архитектура систем управления базами данных

Перечень изучаемых вопросов:

Анализ архитектуры систем управления базами данных.

Понятия сервера, клиента, их функции.

Архитектура «клиент – сервер», назначение, преимущества и недостатки.

Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование СУБД.

Механизмы блокирования и управления доступом в многопользовательской среде.

Методические указания к изучению:

При изучении данной темы студентам необходимо усвоить понятия сервера и клиента, и знать их функции. Далее следует изучить модель архитектуры «клиент – сервер», обратив внимание на ее преимущества и недостатки. Затем изучаются вопросы, связанные с механизмами блокирования и управления доступом в многопользовательской среде.

Ознакомиться с материалов темы можно в презентации «Лекция 8».

Литература:
1. [2, с. 35 - 41].
2. [14, с. 12 - 14].

Контрольные вопросы:

1. Что представляет собой архитектура систем управления базами данных.

2. Дайте понятия сервера, клиента. Каковы их функции?

3. Что означает архитектура с? Каково ее назначение, преимущества и недостатки?

4. Как архитектура «клиент – сервер» влияет на функционирование СУБД?

5. Каковы механизмы блокирования и управления доступом в многопользовательской среде?

3.3.5 Тема 3.5. Угрозы информационной безопасности баз данных. Источники угроз. Классификация угроз информационной безопасности баз данных

Перечень изучаемых вопросов:

Понятие угрозы информационной безопасности баз данных.

Угрозы нарушения конфиденциальности данных.

Угрозы нарушения целостности.

Угрозы нарушения доступности.

Источники угроз безопасности баз данных.

Факторы, создающие угрозы безопасности функционирования СУБД (внешние и внутренние).

Классификация угроз информационной безопасности баз данных.

Методические указания к изучению:

При изучении темы студентам необходимо уяснить, что понимают под угрозой, и что понимают под угрозой ИБ АИС. Следует обратить внимание, что защита информации в реляционных БД имеет свою специфику в связи с тем, что специфичны и угрозы, характерные для функционирования и самой СУБД. Следует внимательно изучить классификацию угроз информационной безопасности баз данных и постараться самостоятельно привести примеры по каждому виду изучаемых угроз.

Литература:

1. [2, с. 46 - 52].

Контрольные вопросы:

1. Что такое угроза?

2. Поясните понятие угрозы информационной безопасности баз данных.

3. Что такое угрозы нарушения конфиденциальности данных. Приведите пример.

4. Что такое Угрозы нарушения целостности. Приведите пример.

5. Что такое Угрозы нарушения доступности. Приведите пример.

6. Перечислите источники угроз безопасности баз данных.

7. Каковы внешние факторы, создающие угрозы безопасности функционирования СУБД?

8. Каковы внутренние факторы, создающие угрозы безопасности функционирования СУБД?

9. Классификация угроз информационной безопасности баз данных.

3.3.6 Тема 3.6. Политика безопасности

Перечень изучаемых вопросов:

Сущность политики безопасности.
Цель формализации политики безопасности.
Разделы описания политики безопасности.
Комплект документов по реализации политики безопасности.
Принципы построения защищенных систем баз данных.

Методические указания к изучению:

При изучении данной темы студенту следует усвоить, что такое политика безопасности, какова ее сущность, какова цель формализации политики безопасности. Политика безопасности включает общие принципы и конкретные правила работы с информационными ресурсами. Поэтому необходимо изучить общие принципы построения защищенных систем БД, а также какие разделы входят в описание политики безопасности. Для дальнейшей профессиональной деятельности студенту необходимо знать состав документов по реализации политики безопасности. С лекционным материалом можно ознакомиться в презентации «Лекция 11».

Литература:
1.[2, С. 71 - 83]

Контрольные вопросы:

1. Сформулируйте определение политики безопасности (ПБ).
2. Какова цель формализации политики безопасности?
3. Для чего необходимо несколько вариантов документов оформления ПБ для различных уровней управления.
4. Сформулируйте примерный перечень разделов документа, описывающий ПБ.
5. Приведите пример, когда отказ или сбой аппаратных средств приводил к раскрытию конфиденциальных данных.
6. Каким образом и кем должна определяться ценность информационного ресурса?
7. Каковы основные характерные черты и области использования оборонительной, наступательной и упреждающей стратегии обеспечения безопасности информационных ресурсов организации?

3.3.7 Тема 3.7. Средства защиты систем баз данных

Перечень изучаемых вопросов:

Основные средства защиты.
Парольная защита.
Шифрование данных.
Установление прав доступа к объектам базы данных.
Защита полей и записей таблиц БД.
Дополнительные средства защиты.
Встроенные средства контроля значений данных в соответствии с типами.
Повышение достоверности вводимых данных.
Обеспечение целостности связей таблиц.
Организация совместного использования объектов БД в сети.
Блокировки.

Методические указания к изучению:

При изучении темы, прежде всего, следует акцентировать внимание, что является целью защиты. Для построения эффективной системы защиты необходимо выявить уязвимые элементы, угрозы для выделенных элементов, сформировать требования к системе защиты, выбрать методы и средства, отвечающие этим требованиям.

Необходимо изучить какие существуют основные и дополнительные средства и методы защиты. При изучении каждого вида средств постараться

привести примеры. С лекционным материалом можно ознакомиться в презентации «Лекция 13». Для практического закрепления темы предусмотрено выполнение ряда лабораторных работ.

Литература:
1. [14, С. 224 - 241]
2. [2, С.224 - 237]

Контрольные вопросы:
1. Охарактеризуйте основные задачи защиты БД.
2. Как классифицируются средства защиты?
3. Какие средства защиты БД относятся к основным?
4. Какие средства защиты БД относятся к дополнительным?
5. Как установить парольную защита БД?
6. Что происходит при шифровании БД паролем?
7. Как установить права доступа к объектам базы данных?
8. Как организовать защиту полей и записей таблиц БД?
9. Перечислите дополнительные средства защиты.
10. Как работают встроенные средства контроля значений данных в соответствии с типами в БД?
11. Как можно повысить достоверность вводимых данных?
12. Как обеспечить целостность связей таблиц?
13. Какова организация совместного использования объектов БД в сети?
14.Что такое блокировки?

3.3.8 Тема 3.8. Обеспечение целостности баз данных. Структурная, языковая, ссылочная целостность. Способы поддержки семантической целостности. Администрирование баз данных.

Перечень изучаемых вопросов:

Проблема целостности.
Поддержка структурной целостности.
Поддержка языковой целостности.
Поддержка ссылочной целостности.
Поддержка семантической целостности декларативным и процедурным способами.
Администрирование баз данных.

Методические указания к изучению:

При изучении темы следует уяснить понятие целостности и ее видов в БД. Внимательно изучить механизмы поддержания структурной, языковой и ссылочной целостности. Затем уяснить понятие семантической целостности и изучить способы ее поддержания.

Особо важным вопросом в данной теме является вопрос администрирования баз данных, поскольку в функции администратора обычно входят вопросы обеспечения безопасности БД. Поэтому следует акцентировать на этом вопросе внимание.

Литература:

1. [18, с. 68 - 89].
2. [14, с. 63-65].

Контрольные вопросы:

1. Приведите понятие целостности.
2. Какие виды целостности вы знаете, охарактеризуйте каждый вид.
3. Каковы способы поддержания семантической целостности?
4. Какие задачи входят в администрирование баз данных?
5. Каким образом администратор решает вопросы безопасности баз данных?

3.3.9 Тема 3.9. Обеспечение согласованности данных в многопользовательском режиме обработки. Понятие транзакции. Идентификация и аутентификация пользователей

Перечень изучаемых вопросов:

Проблемы выполнения операций с единой базой данных в многопользовательском режиме доступа и их решение.

Транзакции, их назначение и свойства.

Источники отказов в процессе эксплуатации БД.

Ведение журнала транзакций.

Использование транзакций для восстановления данных.

Учетные записи пользователей.

Идентификация и аутентификация пользователей (установление подлинности).

Проверка полномочий.

Технология меток (дескрипторов) доступа.

Методические указания к изучению:

При изучении данной темы следует разобраться, каким образом происходит выполнение операций с единой базой данных в многопользовательском режиме доступа. Необходимо уяснить понятие транзакции, как ведутся их журналы, и как с помощью этих журналов можно восстановить данные. Должное внимание следует уделить изучению источников отказов при эксплуатации БД.

Важным является и понятие учетной записи пользователей.

Необходимо изучить понятия идентификации и аутентификации пользователей (установление подлинности), а также как осуществляется проверка полномочий.

В заключение необходимо изучить вопрос использования технология меток (дескрипторов) доступа.

Для освоения работы с журналом транзакций предусмотрено выполнение лабораторной работы.

Литература:

1. [2, с. 255 - 269].
2. [13, с. 247 -248].

Контрольные вопросы:

1. Перечислите проблемы выполнения операций с единой базой данных в многопользовательском режиме доступа и их решение.
2. Что такое транзакции, каковы их назначение и свойства?
3. Назовите источники отказов в процессе эксплуатации БД.
4. Для чего ведется журнала транзакций?
5. Как используется журнал транзакций для восстановления данных?
6. Что такое учетные записи пользователей и как их создать?
7. Что такое идентификация и аутентификация пользователей? Для чего они используются?
8. Для чего используют технология меток (дескрипторов) доступа?

3.3.10 Тема 3.10 Дискреционная защита. Представления

Перечень изучаемых вопросов:

Дискреционная модель управления доступом и ее реализация.

Привилегии доступа и роли, их назначение различным категориям пользователей.

Права конечных, привилегированных пользователей и администраторов баз данных.

Представления, их назначение, работа с представлениями.

Методические указания к изучению:

При изучении темы следует уяснить, что базовым понятием системы разграничения доступа как одного из средств защиты БД являются привилегии. Привилегии могут системными и привилегии доступа к какому-либо объекту БД. Особыми привилегиями обладает администратор БД и ее владелец. Важным является и понятие роли, которые назначаются разным категориям пользователей.

Для освоения работы с привилегиями, ролями и представлениями предусмотрено выполнение лабораторной работы.

Литература:

1. [2, с.136 - 173].
2. [8, с.73 - 80].

Контрольные вопросы:

1. Сформулируйте содержание понятий добровольного и принудительного управления доступом.
2. Сформулируйте содержание принципа наименьших привилегий.
3. Охарактеризуйте дискреционную модель управления доступом, как она реализуется?
4. Что такое привилегии доступа и роли?
5. Как назначить привилегии различным категориям пользователей?
6. Каковы права конечных, привилегированных пользователей и администраторов баз данных?
7. Что такое представления? Каково их назначение?

3.3.11 Тема 3.11 Мандатная защита

Перечень изучаемых запросов:

Мандатная модель управления доступом и ее реализация.

Использование меток конфиденциальности.

Средства аудита.

Уровни доступа к базе данных.

Методические указания к изучению:

При изучении темы следует уяснить основную идею мандатной модели доступа, заключающуюся в приписывании объектам и субъектам доступа меток. Объектами в БД выступают таблицы БД, а субъектами - пользователи и процессы над данными.

Литература:

1. [2, с. 204 – 222, 281 - 299].

Контрольные вопросы:

1. Сформулируйте характерные черты мандатной модели управления доступом.
2. Каковы особенности ее реализация?
3. Что такое метки конфиденциальности и как их используют?
4. Назовите известные Вам средства аудита.
5. Каковы уровни доступа к базе данных?

3.3.12 Тема 3.12 Многоуровневая модель безопасности. Защита данных при статистической обработке

Перечень изучаемых запросов:

Уровни безопасности.

Понятие метки безопасности.

Классы и уровни доступа.

Модель Белла – Ла Падула.

Угрозы информационной безопасности баз данных, возникающие при статистической обработке.

Организация защиты данных при статистической обработке.

Методические указания к изучению:

При изучении темы следует уяснить, что многоуровневая модель означает, что в вычислительной системе хранится информация, относящаяся к разным классам безопасности, а часть пользователей не имеет доступа к инфор-

мации высшего класса безопасности. Важным является знание уровней безопасности, в соответствии с которыми пользователи получают метки доступа. Многоуровневые системы безопасности строятся на модели Белла – Ла Падула.

Далее следует изучить угрозы информационной безопасности баз данных, возникающие при статистической обработке, а также вопросы, связанные с организацией защиты данных.

С материалом лекции можно ознакомиться в презентации «Лекция 17».

Литература:

2. [15, с. 143 - 146].

Контрольные вопросы:

1.Перечислите известные Вам уровни безопасности для правительственных и коммерческих структур.

2. Сформулируйте понятие метки безопасности.

3. Назовите классы и уровни доступа.

4. Для чего предназначена модель Белла – Ла Падула?

5. Какие угрозы информационной безопасности баз данных могут возникнуть при статистической обработке.

6. Охарактеризуйте специфические проблемы защиты данных для процедур статистической обработки.

4.Требования к аттестации по дисциплине

4.1 Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: выполнение и защита лабораторных работ, заключающаяся в представлении в электронном или бумажном виде отчета по лабораторной работе и в ответах на контрольные вопросы.

4.2 Условия получения положительной оценки

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой выполнение и защиту курсовой работы, а также сдачу экзамена.

Курсовая работа на тему «Обеспечение информационной безопасности при проектировании базы данных» выполняется в соответствии с индивидуальными вариантами, определяемыми преподавателем. Работа выполняется студентом в соответствии с методическими указаниями. Пояснительная записка к курсовой работе должна включать перечень обязательных разделов.

Курсовая работа может быть оценена оценкой «отлично», если она выполнена безупречно, т. е. соответствует всем требованиям, предъявляемым к содержанию и форме: выполнена самостоятельно, имеет элементы научного знания, отражает современные подходы в области информационной безопасности систем баз данных, а также их реализацию в разработанной базе данных. Для защиты курсовой работы на оценку «отлично» студент должен продемонстрировать свободное владение материалом, профессиональной терминологией, уметь отвечать на поставленные вопросы.

Курсовая работа может быть оценена оценкой «хорошо», если она в целом отвечает предъявляемым требованиям, но имеет отдельные недостатки. Основанием для снижения оценки могут послужить: использование в недостаточном количестве научных источников, недостаточно четкая формулировка выводов, допущены малосущественные ошибки, несоответствие стандартам оформления сносок, ссылок, списка использованных источников.

Курсовая работа оценивается оценкой «удовлетворительно», если она имеет существенные недостатки, но студент все же проделал определенную работу по ее подготовке. Существенными недостатками курсовой работы являются: неглубокий анализ предметной области, наличие ошибок в отчетных материалах по проектированию базы данных, поверхностная проработка общетехнических и организационных мер по повышению информационной безопасности, отдельные замечания по оформлению курсовой работы, отдельные нарушения требований стандартов при составлении списка использованных источников.

Курсовая работа не допускается к защите и оценивается «неудовлетворительно», если она выполнена не самостоятельно или имеет следующие существенные недостатки: отсутствует анализ предметной области, наличие грубых ошибок в отчетных материалах по проектированию базы данных, отсутствие предложений по общетехническим и организационным мерам по повышению информационной безопасности, небрежное оформление курсовой работы, грубое нарушение требований стандартов при составлении списка использованных источников. Такая работа возвращается студенту для переделки с учетом всех замечаний, высказанных в рецензии преподавателем.

Экзамен проводится в традиционной форме по пятибалльной системе. Допуском к экзамену является успешная защита курсовой работы, выполнение и защита всех лабораторных работ.

Ниже приведены критерии оценивания экзамена по дисциплине (отлично, хорошо, удовлетворительно).

Оценка «отлично» выставляется в случае правильных, полных и четких ответов на теоретические вопросы, с их проецированием и интерпретацией на сегодняшнюю ситуацию. Допускаются непринципиальные погрешности или небольшая незавершенность ответов, диктуемых лимитом времени.

Оценка «хорошо» выставляется в случаях правильных и четких ответов при незначительных замечаниях, неточностях.

Оценка «удовлетворительно» выставляется в случаях ответа на большую часть (не менее 50% основных положений); при правильном ответе на один вопрос или неполных ответах на два вопроса.

Оценка «неудовлетворительно» выставляется при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

В случае успешной работы студента в течение всего семестра, стопроцентной посещаемости, своевременной сдачи лабораторных работ и защиты курсовой работы на оценку «отлично», студенту может быть выставлен «автомат» на экзамене.

4.3 Примерные вопросы к экзамену по дисциплине

1. Базы данных, системы управления базами данных. Основные понятия и определения.
2. Аспекты рассмотрения вопросов информационной безопасности баз данных
3. Уровни информационной системы, на которых должна строиться комплексная система обеспечения информационной безопасности
4. Задачи, решаемые для обеспечения безопасности автоматизированных информационных систем (обеспечение конфиденциальности, целостности, доступности), их характеристика.
5. Понятие роли, представления, триггеров. Их назначение, характеристика использования.
6. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных
7. Модели баз данных
8. Нормализация таблиц баз данных
9. Проектирование связей между таблицами. Правила установления связей. Типы связей.
10. Понятие первичного и внешнего ключей таблицы. Каскадирование. Ограничение. Установление.

11. Проектирование БД, решение проблем информационной безопасности на различных этапах проектирования.

12. Инфологическое моделирование баз данных

13. СУБД. Языковые средства описания, манипулирования, запросов. Функции и использование.

14. Структурированный язык запросов SQL.

15. Архитектура систем управления базами данных.

16. Архитектура «клиент – сервер». Понятие клиента и сервера.

17. Многозвенная архитектура. Понятие сервера баз данных и сервера приложений. Универсальный клиент.

18. Структура свойства информационной безопасности баз данных.

19. Сущность проблемы обеспечения информационной безопасности систем баз данных.

20. Угрозы информационной безопасности баз данных.

21. Источники угроз информации баз данных.

22. Классификация угроз информационной безопасности баз данных.

23. Политика безопасности, ее цели, структура, решаемые задачи по безопасности баз данных, ответственные лица.

24. Цель формализации политики безопасности.

25. Комплект документов, предоставляющий основные решения организации по реализации политики безопасности.

26. Принципы построения защищенных систем баз данных.

27. Стратегия применения средств обеспечения информационной безопасности баз данных.

28. Основные средства защиты баз данных.

29. Дополнительные средства защиты баз данных.

30. Обеспечение целостности данных (поддержка структурной, языковой и ссылочной целостности).

31. Декларативное обеспечение семантической целостности.

32. Процедурное обеспечение семантической целостности. Понятия хранимой процедуры и триггера.

33. Администрирование баз данных. Функции администратора.

34. Обеспечение согласованности данных в многопользовательском режиме обработки. Понятие транзакции

35. Использование транзакций для восстановления после сбоев или отказов системы. Причины отказов.

36. Идентификация и аутентификация пользователей баз данных (установление подлинности)

37. Учетные записи пользователей. Общие сведения

38. Создание учетной записи пользователя, установка пароля, просмотр учетных записей и их удаление.

39. Система привилегий доступа. Общие сведения.

40. Предоставление, просмотр и отмена привилегий доступа пользователей.

41. Резервирование баз данных. Полное резервное копирование базы данных. Ведение двоичных журналов.

42. Восстановление данных в СУБД MY SQL.

43. Профилактическая проверка таблиц и их восстановление в СУБД MY SQL.

44. Журналы работы (журнал ошибок, двоичные журналы, общий журнал запросов, журнал медленных запросов) и их просмотр в СУБД MY SQL.

45. Реализации политики безопасности при эксплуатации БД. Уровни защиты данных.

46. Дискреционная защита и ее реализация.

47. Использование представлений для управления доступом пользователей СУБД

48. Мандатная защита и ее использование для управления доступом пользователей СУБД.

49. Многоуровневая модель безопасности баз данных. Иерархия прав доступа. Метки безопасности

50. Защита баз данных при статистической обработке

5. Заключение

Учебно-методическое пособие по дисциплине «Безопасность систем баз данных» посвящено изложению вопросов безопасности систем баз данных. Оно разработано в помощь студентам, изучающим указанную дисциплину. В пособии нашли отражение все темы курса с перечнем изучаемых вопросов, проработав которые студенты могут ответить на контрольные вопросы, чтобы оценить степень усвоения учебного материала. Для студентов, пропустивших ту или иную лекцию, рекомендуется воспользоваться ссылками на указанную литературу, а также проработать материал презентаций, представленных в ЭИОС. Теоретический материал закрепляется на практике при выполнении лабораторных работ.

6. Список литературы

6.1 Основная литература:

1. СУБД. Язык SQL в примерах и задачах: учебное пособие / И. Ф. Астахова, В. М. Мельников, А. П. Толстобров, В. В. Фертиков. – Москва: Академия, 2007. 168 с.

2. Смирнов, С. Н. Безопасность систем баз данных/ С. Н. Смирнов. – Москва: Гелиос АРВ, 2007. – 352 с.

6.2 Дополнительная литература:

3. Агальцов, В. П. Базы данных. В 2-х кн. [Текст]: учебник / В. П. Агальцов. - Москва: ИД "Форум"; Москва: ИНФРА-М. Кн.1: Локальные базы данных. - 2013. - 352 с.

4. Агальцов, В. П. Базы данных. В 2-х кн. [Текст]: учебник / В. П. Агальцов. - Москва: ИД "Форум"; Москва: ИНФРА-М. Кн.2: Распределенные и удаленные базы данных. - 2013. - 272 с.

5. Администрирование Microsoft SQL Server 2000: учебный курс MCSA/ MCSE, MCDBA: экзамен 70-228: официальное пособие для самоподготовки: пер. с англ. / пер. А. П. Харламов. - 2-е изд., испр. - М.: Русская редакция; Санкт-Петербург: Питер, 2006. - 610 с.: ил. - (Учебный курс Microsoft). - Предм. указ.: с. 588.

6. Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие / Л. Г. Гагарина, Д. В. Киселев, Е. Л. Федотова. - Москва: ИД "Форум", 2009. - 384 с.

7. Гольцман, В. MySQL 5.0: практическое пособие / В. Гольцман. - Санкт-Петербург: Питер, 2009. - 256 с.

8. Дейт, К. Дж. Введение в системы баз данных / К. Дж. Дейт. - Москва: ИД Вильямс, 2002. 1072 с.

9. Информатика. Базовый курс: учебное пособие / ред. С. В. Симонович. - 3-е изд. Стандарт третьего поколения. - Санкт-Петербург : Питер, 2013. - 640 с.

10. Мартишин, С. А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench. Методы и средства проектирования информационных систем и технологий. Инструментальные средства информационных систем: учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. - Москва: ИД "Форум" ; Москва : ИНФРА-М, 2012. - 160 с.

11. Проектирование и реализация баз данных Microsoft SQL Server 2000 : учебный курс MCAD/MCSE, MCDBA: экзамен 70-229: официальное пособие для самоподготовки: пер. с англ. / пер. В. Г. Вшивцев. - 3-е изд. -

Москва : Русская редакция ; Санкт-Петербург : Питер, 2005. - 482 с. : ил. - (Учебный курс Microsoft). - Предм. указ.: с. 468.

12. Суркова, Н. Е. Методология структурного проектирования информационных систем [Электронный ресурс]: монография / Н. Е. Суркова, А. В. Остроух. - Красноярск: Научно-инновационный центр, 2014. - 190 с.

13. Фуфаев, Э. В. Базы данных: учеб. пособие / Э. В. Фуфаев, Д. Э. Фуфаев. - 4-е изд. - Москва : Academia, 2008. - 320 с.

14. Хомоненко, А. Д. Базы данных: учебник / А. Д. Хомоненко, В. М. Цыганков, М. Г. Мальцев. - 6-е изд., доп. - Санкт-Петербург: КОРОНА-Век, 2009. - 736 с.

15. Основы защиты информации: учеб. пособие. / А. А. Шелупанов [и др.]. Изд. 5-е, перераб. и доп.. – Томск: В-Спектр, 2011. – 244 с.

6.3 Учебно-методические пособия по дисциплине:

16. Капустин, В. В. Обеспечение информационной безопасности при проектировании базы данных [Электронный ресурс]: Методические указания по выполнению курсовой работы по дисциплине «Безопасность систем баз данных» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / В. В. Капустин, Н. Ф. Чикунова. - Калининград: Изд-во БГАРФ, 2019. - 62 с.

17. Основы защиты информации: учеб. пособие для студентов специальности 090105.65 «Комплексное обеспечение информационной безопасности автоматизированных систем» / А. В. Кузнецов [и др.] - Калининград: Изд-во БГАРФ, 2014. - 179 с.

18. Чикунова, Н. Ф. Проектирование баз данных и организация их защиты в СУБД Access. Часть 1: учеб. пособие / Н. Ф. Чикунова. – Калининград: Изд-во БГАРФ, 2019. – 106 с.

19. Чикунова, Н. Ф. Проектирование баз данных и организация их защиты в СУБД MySQL. Часть 2: учеб. пособие / Н. Ф. Чикунова. – Калининград: Изд-во БГАРФ, 2020. – 92 с.

20. Чикунова, Н. Ф. Нормализация баз данных: методические указания по выполнению лабораторной работы по дисциплине «Безопасность систем баз данных» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / Н. Ф. Чикунова. - Калининград: Изд-во БГАРФ, 2021. - 24 с.

6.4. Интернет-ресурсы:

21. http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/ - электронный каталог библиотеки БГАРФ

22. https://www.it.ru - Официальный сайт компании АйТи

23. http://elibrary.ru - электронная библиотека Elibrary

24. http://elibrary.ru/projects/subscription/rus_titles_open.asp - БД российских научных журналов на Elibrary.ru (РУНЭБ)

25. http://rugost.com – электронный каталог ГОСТов

26. https://fstec.ru/component/attachments/download/2018

27. САБ Ирбис 64-2018.1 – лицензия № 698/1 от 11.07.2016 с ежегодным обновлением

28. Интернет- версия «Гарант» -Договор № 04/19АО от 29.01.2019

29. НЭБ РФ - Национальная электронная библиотека НЭБ – договор 101/НЭБ/2366 от 19.08.2017для всего университетского комплекса

30. ЭБС «Университетская библиотека онлайн» Контракт №06 от 11.03.2019

31. ЭБС IPRbooks ООО «Ай Пи Эр Медиа» Контракт №4228/18 от 04.06.2018 - 15.07.2019

Учебное издание

Наталья Федоровна Чикунова

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

Редактор Г. А. Смирнова

Уч.-изд. л 2,8. Печ. л. 2,5

Издательство федерального государственного бюджетного образовательного учреждения высшего образования «калининградский государственный технический университет»
236022, Калининград, Советский проспект, 1