Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

«Основы построения защищенных баз данных»

для студентов специалитета по специальности
10.05.01 Компьютерная безопасность,

Ульяновск, 2021

Методические указания для выполнения лабораторных работ и самостоятельной работы студентов по дисциплине «Основы построения защищенных баз данных» для студентов специальности 10.05.01 «Компьютерная безопасность» / составитель: Клочков А.Е. - Ульяновск: УлГУ, 2021.

Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.01 «Компьютерная безопасность», изучающих дисциплину «Основы построения защищенных баз данных». В работе приведены рекомендуемая литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, указания по выполнению лабораторных работ.

Студентам следует использовать данные методические указания при выполнении лабораторных работ, при подготовке к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 4/21 от 18 мая 2021 г.)

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

1. Гусева, Л. Л. Основы построения защищенных баз данных: учебное пособие (лабораторный практикум) / Л. Л. Гусева. — Ставрополь: Северо-Кавказский федеральный университет, 2018. — 120 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: https://www.iprbookshop.ru/92575.html. — Режим доступа: для авторизир. пользователей
2. Космачева, И. М. Проектирование защищенных баз данных : учебное пособие / И. М. Космачева, Н. В. Давидюк ; под редакцией Т. С. Кулаковой. — Санкт-Петербург : Интермедия, 2020. — 144 с. — ISBN 978-5-4383-0191-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/95265.html — Режим доступа: для авторизир. пользователей
3. Базы данных : учебное пособие / . — Саратов : Научная книга, 2012. — 158 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/6261.html — Режим доступа: для авторизир. пользователей.
4. Безопасность систем баз данных : учебное пособие / А. В. Скрыпников, С. В. Родин, Г. В. Перминов, Е. В. Чернышова ; под редакцией С. В. Белокуров. — Воронеж : Воронежский государственный университет инженерных технологий, 2015. — 144 с. — ISBN 978-5-00032-122-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/50628.html — Режим доступа: для авторизир. пользователей
5. Стружкин, Н. П. Базы данных: проектирование : учебник для вузов / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2021. — 477 с. — (Высшее образование). — ISBN 978-5-534-00229-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469021
6. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для вузов / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2021. — 291 с. — (Высшее образование). — ISBN 978-5-534-00739-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470023.
7. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2.
8. http://www.securitylab.ru – российский портал по компьютерной безопасности.
9. http://www.pgpru.com – русскоязычный сайт, посвященный криптографическому стандарту PGP.
10. http://www.docload.spb.ru/Basesdoc/45/45674/index.htm – основные термины и определения в области технической защиты информации (согласно Приказу Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст)

Базы данных, информационно-справочные и поисковые системы

1. http://www.sql.ru (Форум SQL.RU)

2. http://asktom.oracle.com (Интернет-ресурс «Ask Tom Oracle»)

3. http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и

преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)

4. http://www.infosecurity.report.ru/ (портал по информационной безопасности)

5. http://www.void.ru/ (портал по информационной безопасности)

6. http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)

7. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Теоретические основы безопасности в БД

Тема 1. Безопасность БД, угрозы, защита

Основные вопросы темы:

Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. История развития, назначение и роль баз данных. Модели данных. Математические основы построения реляционных СУБД.

Тема 2. Критерии защищенности БД

Основные вопросы темы:

Критерии оценки надежных компьютерных систем (TCSEC). Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI). Оценка надежности СУБД как компоненты вычислительной системы.

Тема 3. Модели безопасности в СУБД

Основные вопросы темы:

Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД.

Раздел 2. Средства и методы обеспечения целостности БД

Тема 4. Средства идентификации и аутентификации

Основные вопросы темы:

Общие сведения. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.

Тема 5. Средства управления доступом

Основные вопросы темы:

Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Использование представлений для обеспечения конфиденциальности информации в СУБД. Средства реализации мандатной политики безопасности в СУБД.

Тема 6. Целостность БД и способы ее обеспечения

Основные вопросы темы:

Основные виды и причины возникновения угроз целостности. Способы

противодействия. Цели использования триггеров. Способы задания, моменты выполнения. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности.

Раздел 3. Средства и методы обеспечения конфиденциальности и доступности БД

Тема 7. Классификация угроз конфиденциальности СУБД

Основные вопросы темы:

Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов.

Тема 8. Аудит и подотчетность

Основные вопросы темы:

Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

Тема 9. Транзакции и блокировки

Основные вопросы темы:

Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Цель. Лабораторный практикум по дисциплине направлен на изучение студентами всех современных подходов для обеспечения информационной безопасности современных баз данных.

Методология основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Все работы созданы на основе стандартных практических задач современного предприятия. Поиск технической информации, а также подбор необходимого решения производиться самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и процессе демонстрации полученного решения.

Результат. Полученные решения демонстрируются студентом для каждого из типа операционных систем. При необходимости демонстрируется ход выполнения работы.

Требования к оборудованию. Для выполнения работ студенты используют среду разработки на языках C#, C++, Java, системы управления базами данных: MS SQL Server 2008-2012, Oracle 10g – Oracle 11g, MS Office Visio.

Лабораторная работа № 1.
Тема: Модели данных. Создание и модификация баз данных. Управление доступом к СУБД
Задание и указания по выполнению лабораторной работы см. в [1, с.6-15]

Лабораторная работа № 2.
Тема: Нормализация. Связывание таблиц. Внешние ключи.

Задание и указания по выполнению лабораторной работы см. в [1, с. 16-24]

Лабораторная работа № 3.
Тема: Проектирование БД.
Задание и указания по выполнению лабораторной работы см. в [1, с.25-39]

Лабораторная работа № 4.
Тема: Транзакции в СУБД
Задание и указания по выполнению лабораторной работы см. в [1, с.40-44]

Лабораторная работа № 5.
Тема: Репликация БД. Резервирование и распределение
Задание и указания по выполнению лабораторной работы см. в [1, с.65-70]

Лабораторная работа № 6.
Тема: Криптографические методы защиты в БД
Задание и указания по выполнению лабораторной работы см. в [1, с.71-75]

Лабораторная работа № 7.
Тема: Защита от атак типа внедрение
Задание и указания по выполнению лабораторной работы см. в [1, с.76-84]

Лабораторная работа № 8.
Тема: Резервное копирование и восстановление
Задание и указания по выполнению лабораторной работы см. в [1, с.85-95]

Лабораторная работа № 9.
Тема: Шифрование соединения между СУБД и серверным приложением
Задание и указания по выполнению лабораторной работы см. в [1, с.109-112]

Методические указания для обучающихся по освоению дисциплины

Организуя свою учебную работу, студенты должны:

Во-первых, выявить рекомендуемый режим и характер учебной работы по изучению теоретического курса, практическому применению изученного материала, по выполнению заданий для самостоятельной работы, по использованию информационных технологий и т.д.

Во-вторых, ознакомиться с указанным в методическом материале по дисциплине (модулю) перечнем учебно-методических изданий, рекомендуемых студентам для подготовки к занятиям и выполнения самостоятельной работы, а также с методическими материалами на бумажных и/или электронных носителях, выпущенных кафедрой своими силами и предоставляемые студентам во время занятий.

Самостоятельная работа студентов, предусмотренная учебным планом, должна соответствовать более глубокому усвоению изучаемого курса, формировать навыки исследовательской работы и ориентировать студентов на умение применять теоретические знания на практике.

Самостоятельная работа обучающихся направлена на освоение учебного материала и развитие практических умений. Самостоятельная работа включает следующие виды самостоятельной работы студентов

– работа с рекомендованной учебной литературой;

– выполнение заданий по лабораторным работам;

– подготовка к экзамену.

1. Работа с учебными пособиями. Для полноценного усвоения курса студент должен, прежде всего, овладеть основными понятиями этой дисциплины. Необходимо усвоить определения и понятия, уметь приводить их точные формулировки, приводить примеры объектов, удовлетворяющих этому определению. Кроме того, необходимо знать круг фактов, связанных с данным понятием. Требуется также знать связи между понятиями, уметь устанавливать соотношения между классами объектов, описываемых различными понятиями.

2. Самостоятельное изучение тем. Самостоятельная работа студента является важным видом деятельности, позволяющим хорошо усвоить изучаемый предмет и одним из условий достижения необходимого качества подготовки и профессиональной переподготовки специалистов. Она предполагает самостоятельное изучение студентом рекомендованной учебно-методической литературы, различных справочных материалов, подготовку к экзамену.

3. Выполнение лабораторных работ

Особое внимание уделено освоению студентами практических умений управления защитой современных СУБД.

Основной упор в методике проведения лабораторных занятий сделан на отработке и закреплении учебного материала в процессе выполнения заданий с применением вычислительной техники в компьютерном классе.

Текущий контроль усвоения знаний осуществляется путем подготовки и сдачи отчетов по итогам выполнения лабораторных работ, опросов на лабораторных занятиях.

Курс имеет практическую направленность, поэтому основное внимание уделяется выработке практических навыков и умений по организации защиты баз данных. При этом большое значение имеет практическое выполнение студентами всех заданий и упражнений в дисплейном классе. Исходя из объема часов, выделяемых на изучение дисциплины, обращается особое внимание на организацию самостоятельной работы. Детальная проработка материала, связанного с разработкой программного обеспечения, остается на самостоятельное изучение.

Лабораторные занятия по дисциплине служат для получения практических навыков по применению теоретических знаний, полученных студентами на лекциях, для решения конкретных задач в профессиональной сфере специалистов.

4. Подготовка к экзамену. При подготовке к экзамену студенты должны использовать как самостоятельно подготовленные конспекты, так и материалы, полученные в ходе лекций.

ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные.
2. Понятие политики безопасности. Сущность политики безопасности. Цели формализации политики безопасности. Принципы построения защищенных систем.
3. Дискреционные модели безопасности СУБД. Реализация ролевой модели политикибезопасности в СУБД Oracle.
4. Мандатная модель политики безопасности.
5. БД с многоуровневой секретностью (MLS). Многозначность. Реализация модели MLS. Авторизация меток пользователя. Специальные привилегии доступа. Меточные функции. Опции ограничения.
6. Метаданные и словарь данных. Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представления словаря.

7. Понятие транзакции. Фиксация транзакции. Прокрутки вперед и назад. Контрольная точка. Откат. Транзакции как средство изолированности пользователей. Сериализация транзакций.
8. Блокировки. Режимы блокирования. Правила согласования блокировок.
9. Двухфазный протокол синхронизационных блокировок. Взаимоблокировки, их распознавание и разрушение.
10. Целостность кода приложения. SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции.
11. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя.
12. Управление набором регистрируемых событий. Анализ регистрационной информации.