

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Безопасность систем баз данных

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем (в сфере информационных технологий)»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Целью дисциплины «Безопасность систем баз данных» является обучение студентов принципам обеспечения безопасности информации в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД), навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты.

Задачи дисциплины:

- приобретение системного подхода к проблеме защиты информации в СУБД;
- изучение моделей и механизмов защиты в СУБД;
- приобретение практических навыков организации защиты БД.

Данный курс, позволяет путем изучения уязвимостей информационных систем и особенностей обеспечения безопасности баз данных, выработать у студентов убежденность в необходимости принятия адекватных угрозам безопасности мер защиты российских объектов информатизации, предоставляет достаточные знания и навыки, требуемые для этого.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» - работа с программными средствами общего назначения;

«Языки программирования» - знание одного из языков программирования высокого уровня;

«Основы информационной безопасности» - знание основных угроз безопасности информации и модели нарушителя в компьютерной системе;

«Администрирование средств защиты информации в компьютерных системах и сетях» - знание формальных моделей безопасности; политик безопасности; знание критериев и классов защищенности средств вычислительной техники и автоматизированных информационных систем; знание стандартов по оценке защищенных систем; умение исследования корректности систем защиты; владеть методологией обследования и проектирования защиты;

«Криптографические методы защиты информации» - знание принципов построения криптографических алгоритмов с симметричными и несимметричными ключами; программные реализации шифров; знание криптографических протоколов; криптографических хеш-функций, электронной цифровой подписи; криптографических стандартов;

«Безопасность компьютерных сетей» - знание принципов и особенностей организации защиты информационных систем средствами сетевой безопасности;

«Безопасность операционных систем» - знание принципов и особенностей организации защиты информационных систем средствами защиты операционных систем;

«Системы управления базами данных» - знание общих принципов построения баз данных; знание особенностей средств управления в реализациях реляционных СУБД, знание проблем оптимизации доступа к базам данных;

Дисциплина «Безопасность систем баз данных» используются студентами при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретение следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции		
ОПК-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	И-ОПК-1.3.1. Знает методы защиты информации в системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации	Знать: - перечень утилит, необходимый для проведения анализа АИС на предмет выявления уязвимостей. - теоретические основы построения защищённых БД. Уметь: - поэтапно проводить тестирование АИС на предмет выявления уязвимостей. - пользоваться средствами языков программирования для реализации сохранения целостности данных в БД. Владеть навыками: распознавания уязвимостей и слабых мест в АИС по итогам проведённого тестирования.
	И-ОПК-1.3.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации систем передачи информации	Знать: - информационные ресурсы, на которых публикуются актуальные сведения об известных уязвимостях различных СУБД. Уметь: - проводить анализ АИС на предмет выявления уязвимостей. - пользоваться средствами СУБД для реализации механизма разграничения доступа к данным, а также обеспечения высокой степени безотказности БД. Владеть навыками: - разработки проектов нормативных правовых актов и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем.
Профессиональные компетенции		
ПК-3 Способен обеспечивать контроль над соблюдением требований по защите информации	И-ПК-3.1 Знает и понимает нормативные требования по защите информации И-ПК-3.2 Умеет осуществлять оценку и контроль исполнения требований по защите информации И-ПК-3.3 Владеет навыками осуществления контроля над соблюдением требований по защите информации	Знает: нормативные требования по защите информации Умеет: осуществлять оценку и контроль исполнения требований по защите информации Владеет навыками: осуществления контроля над соблюдением требований по защите информации

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетных единиц, **108** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационны е испытания		
1	Теоретические основы безопасности в СУБД	7	7			1		4	
2	Механизмы обеспечения целостности СУБД	7	6	4		1		12	Опрос по заданиям для самостоятельной работы
3	Механизмы обеспечения конфиденциальности в СУБД	7	10	8		2		14	Опрос по заданиям для самостоятельной работы
4	Механизмы, поддерживающие высокую готовность	7	4	2		1		10	Опрос по заданиям для самостоятельной работы
5	Защита данных в распределенных системах	7	5	2		1		10	Опрос по заданиям для самостоятельной работы
							0,3	3,7	Зачет
	ИТОГО		32	16		6	0,3	53,7	

Содержание разделов дисциплины.

Тема 1. Теоретические основы безопасности в СУБД

1.1. Угрозы безопасности БД: общие и специфичные. Понятие безопасности БД. Требования безопасности БД. Целостность БД. Аудит.

1.2. Средства обеспечения защиты информации в СУБД и многоуровневая защита. Типы контролей безопасности: потоковый, контроль вывода, контроль доступа.

1.3. Политика безопасности в СУБД. Понятие политики безопасности. Сущность политики безопасности. Цели формализации политики безопасности. Принципы построения защищенных систем. Модели безопасности в СУБД. Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД. Модели RBAC. Мандатные модели: BellLaPadula, Biba. СУБД с многоуровневой секретностью (MLS).

1.4. Роль положений национальных стандартов семейства «Общие критерии доверия и безопасности информационных систем» (ГОСТ Р ИСО/МЭК 15408-2012-1, ГОСТ Р ИСО/МЭК 15408-2013-2, ГОСТ Р ИСО/МЭК 15408-2013-3) и ГОСТа Р ИСО/МЭК 18045-2012 «Методология оценки безопасности информационных технологий» для анализа проектных решений подсистем информационной безопасности баз данных и обеспечения защищенности компьютерных систем в целом.

Тема 2. Механизмы обеспечения целостности СУБД

- 2.1. Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия.
- 2.2. Понятие транзакции. Фиксация транзакции. Прокрутки вперед и назад. Контрольная точка. Откат. Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. Блокировки. Режимы блокирования. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок.
- 2.3. Тупиковые ситуации, их распознавание и разрушение. Ссылочная целостность. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности. Правила (триггеры). Цели использования правил. Способы задания, моменты выполнения. Событийная реализация правил безопасности.

Тема 3. Механизмы обеспечения конфиденциальности в СУБД

- 3.1. Классификация угроз конфиденциальности СУБД. Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия.
- 3.2. Роль положений национальных стандартов ГОСТ Р ИСО/МЭК 56545-2015 «Защита информации. Уязвимость информационных систем. Правила описания уязвимостей», ГОСТ Р ИСО/МЭК 56546-2015 «Защита информации. Уязвимость информационных систем. Классификация уязвимостей информационных систем» и федерального банка данных угроз безопасности, ведущегося на сайте ФСТЭК России в разделе «Техническая защита информации» (<https://bdu.fstec.ru>) в идентификации угроз безопасности информационных систем.
- 3.3. Средства идентификации и аутентификации. Общие сведения. Методы аутентификации пользователей СУБД. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. Преимущества и недостатки встроенных средств аутентификации. Внешняя и сквозная аутентификация. Технология Single-Sign-On (SSO).
- 3.4. Средства управления доступом. 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. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации в СУБД. Механизмы тщательного контроля доступа.
- 3.5. Аудит и подотчетность. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.
- 3.6. Криптографические методы защиты баз данных. Особенности применения криптографических методов. Прозрачное шифрование и шифрование по требованию. Особенности хранения ключевой информации в БД.
- 3.7. Роль положений национальных стандартов ГОСТ Р ИСО/МЭК 53113-1-2008 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 1. Общие положения», ГОСТ Р ИСО/МЭК 53113-2-2009 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 2. Рекомендации по защите информации, информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов» и Руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» для обеспечения защищенности компьютерных систем с базами данных от несанкционированного доступа.

Тема 4. Механизмы, поддерживающие высокую готовность

4.1. Средства, поддерживающие высокую готовность. Аппаратная и программная поддержки. Кластерная организация серверов баз данных. Параметры настройки СУБД. Сохранение и восстановление БД. Оперативное администрирование. Задачи, средства и режимы администрирования.

4.2. Мониторинг серверов СУБД. Функциональная насыщенность СУБД. Формы избыточности. Аппаратная избыточность. Избыточность данных. Программное зеркалирование. Тиражирование данных.

Тема 5. Защита данных в распределенных системах

5.1. Распределенные вычислительные среды. Распределенная обработка информации в среде клиент-сервер. Распределенные базы данных в сетях ЭВМ. Угрозы безопасности распределенных СУБД. Угрозы доступности, целостности и конфиденциальности данных. Механизмы противодействия.

5.2. Распределенная обработка данных. Понятие распределенной транзакции. Модель обработки транзакций. Мониторы обработки транзакций. Протоколы фиксации транзакций. Тиражирование данных. Обзор средств тиражирования (репликации) данных. Эффективные алгоритмы тиражирования. Сравнение подходов к тиражированию БД.

5.3. Положения национального стандарта ГОСТ Р ИСО/МЭК 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении», регламентирующего построение защищенных информационных систем на основе защищенных баз данных.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Virtual Box (свободно распространяемое ПО);
- Ubuntu (свободно распространяемое ПО);

- Oracle Express 11g (свободно распространяемое ПО);
- Kali Linux (свободно распространяемое ПО);
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используется:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Поляков, А. М. Безопасность Oracle глазами аудитора : нападение и защита / А. М. Поляков. - Москва : ДМК Пресс, 2017. - 336 с. - ISBN 978-5-97060-469-4. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785970604694.html>
2. Скрыпников А. В., Родин С. В., Перминов Г. В., Чернышова Е. В. Безопасность систем баз данных: учеб. пособие - Воронеж: ВГУИТ, 2015. <https://www.studentlibrary.ru/ru/doc/ISBN9785000321225-SCN0000/000.html>
3. Баранчиков А. И., Баранчиков П. А., Пылькин А. Н. Алгоритмы и модели ограничения доступа к записям БД - Москва : Горячая линия - Телеком, 2011. <https://www.studentlibrary.ru/ru/doc/ISBN9785991202039-SCN0000/000.html>
4. ГОСТ Р ИСО/МЭК 51583 - 2014 года, «Порядок создания автоматизированных систем в защищенном исполнении», Федеральное агентство по техническому регулированию и метрологии («Росстандарт»), М.: 2014. <https://ohranatruda.ru/upload/iblock/44b/4293772843.pdf>

б) дополнительная литература

1. ГОСТ Р ИСО/МЭК 15408 «Общие критерии доверия и безопасности информационных систем», Росстандарт России.
Часть 1 - 2012г: <https://ohranatruda.ru/upload/iblock/857/4293781374.pdf?ysclid=lj48m4r0xz335393767>
Часть 2 – 2013г: <http://data.1000gost.ru/catalog/Data/554/55439.pdf>
Часть 3 - 2013г: <http://gost.gtsever.ru/Data/554/55440.pdf?ysclid=lj48qz60cw360426998>
2. Проскурин В. Г. Защита программ и данных: учебное пособие для вузов. - М.: Академия, 2012.
3. Власова О.В. Системы управления базами данных: лабораторный практикум – Ярославль: ЯрГУ, 2010. <http://www.lib.uniyar.ac.ru/edocs/iuni/20100201.pdf>
4. Власова О.В. SQL: Учебное пособие – Ярославль: ЯрГУ, 2011. <http://www.lib.uniyar.ac.ru/edocs/iuni/20110206.pdf>

5. Пржиялковский В. В. Введение в Oracle SQL - М: Национальный Открытый Университет "ИНТУИТ", 2016. https://www.studentlibrary.ru/ru/doc/intuit_047-SCN0000/000.html
6. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов - М: Горячая линия - Телеком, 2012. <https://www.studentlibrary.ru/ru/doc/ISBN9785991201476-SCN0000/000.html>
7. Руководящий документ ФСТЭК России (бывш. Гостехкомиссия) «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей». (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г., № 114). <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114?ysclid=lj48ywrh6a506906471>

в) ресурсы сети «Интернет» (при необходимости)

1. Новости в сфере угроз безопасности и защиты компьютерной информации российских журнала «Хакер»: <https://haker.ru/tag/news> и журнала «Информационная безопасность»: <http://itsec.ru/main.php>.
2. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»: <http://www.kaspersky.ru/internet-security-center>.
3. Материалы ежегодного (с 27 по 30 декабря) всемирного конгресса хакеров «Chaos Communication Congress» (CCC) в Гамбурге, где рассказывается о новых выявленных уязвимостях в аппаратных решениях и программном обеспечении (на английском языке): https://events.ccc.de/congress/2015/wiki/Static:Main_Page, видеоматериалы с субтитрами конгресса CCC: <https://www.youtube.com/user/CCCEn/videos>.
4. Интерактивные учебники по SQL: <http://www.sql-tutorial.ru/>, <http://www.sql.ru/>.
5. Портал разработчиков клиент-серверных приложений Microsoft Developer Network (MSDN) <https://msdn.microsoft.com/ru-ru/>.
6. Федеральный банк данных угроз безопасности, ведущийся в разделе «Техническая защита информации» официального сайта ФСТЭК России: <https://bdu.fstec.ru>.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа, оборудованная персональной компьютерной техникой с установленными средствами визуализации текстов в формате DOC/DOCX, PDF, F2B, файлов изображений, презентаций, видео и других мультимедийных файлов, а также - видеопроектором и жалюзи на окнах, или компьютерной техникой и интерактивной компьютерной доской;
- учебные аудитории для проведения практических занятий: лаборатории информационных технологий и программно-аппаратных средств обеспечения информационной безопасности (Virtual Box, операционные системы Microsoft Windows и Kali Linux, СУБД Microsoft SQL Server не ниже версии 2010, СУБД Oracle версии не ниже 11g);
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;

- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Автор(ы):

Доцент кафедры КБ и ММОИ

Козырев И.

**Приложение № 1 к рабочей программе дисциплины
«Безопасность систем баз данных»**

**Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости**

Перечень заданий для самостоятельной работы студентов:

1. На основе сопоставления положений международных и российских стандартов безопасности из перечня основной и дополнительной литературы рабочей программы дисциплины сформулируйте чем отличаются зарубежные и российские определения и понятия угроз безопасности? Обоснуйте ответ.
2. На основе знакомства с национальными стандартами по уязвимостям (ГОСТ Р ИСО/МЭК 56545-2015 «Защита информации. Уязвимость информационных систем. Правила описания уязвимостей» и ГОСТ Р ИСО/МЭК 56546-2015 «Защита информации. Уязвимость информационных систем. Классификация уязвимостей информационных систем») и банка данных угроз безопасности, ведущегося на сайте ФСТЭК России (<https://fstec.ru>) в разделе «Техническая защита информации» (<https://bdu.fstec.ru>) отберите угрозы, представляющие наибольшую опасность для информационных систем на основе баз данных. Обоснуйте ответ.
3. В чем заключается суть и назначение пакета DBMS_CRYPTO для шифрования в БД. Обоснуйте ответ.
4. На основе учебной литературы выясните преимущества и недостатки средств аутентификации, встроенных в СУБД Oracle. Обоснуйте ответ.
5. На основе учебной литературы выясните сходство и различия в ролях и привилегиях пользователей СУБД и операционных систем. Обоснуйте ответ.
6. На основе учебной литературы выясните и охарактеризуйте системные и объектные виды привилегий для пользователей СУБД. Обоснуйте ответ.
7. На основе учебной литературы выясните и охарактеризуйте использование представлений для Управление доступом к БД и обеспечения конфиденциальности информации в СУБД. Обоснуйте ответ.
8. На основе учебной литературы выясните и охарактеризуйте методы поддержания декларативной и процедурной целостности в СУБД. Обоснуйте ответ.
9. На основе учебной литературы выясните в чем состоят особенности ссылочной целостности в СУБД и ее поддержания. Обоснуйте ответ.
10. На основе учебной литературы выясните в чем заключаются цели использования триггеров и чем они отличаются от хранимых процедур? Обоснуйте ответ.
11. На основе учебной литературы выясните и обоснуйте фундаментальный для безопасности БД смысл понятия транзакций и контрольных точек. Обоснуйте ответ.
12. Каковы роль и возможности методы сериализации транзакций как средства изолированности пользователей БД. Обоснуйте ответ.
13. На основе учебной литературы выясните и обоснуйте значение для безопасности БД режимов блокирования. Обоснуйте ответ.
14. На основе учебной литературы выясните и охарактеризуйте правила согласования блокировок. Обоснуйте ответ.

15. В чем состоит методологическая роль положений национальных стандартов семейства «Общие критерии доверия и безопасности информационных систем» (ГОСТ Р ИСО/МЭК 15408-2012-1, ГОСТ Р ИСО/МЭК 15408-2013-2, ГОСТ Р ИСО/МЭК 15408-2013-3) в разработке подсистемы информационной безопасности баз данных и рамках создания безопасной информационной системы на их основе?
16. В чем состоит роль положений семейства национальных стандартов ГОСТ Р ИСО/МЭК 53113-1-2008, ГОСТ Р ИСО/МЭК 53113-2-2009 и руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» для обеспечения защищенности компьютерных систем с базами данных от несанкционированного доступа? Обоснуйте ответ.
17. На основе учебной литературы выясните разницу и общие черты аудита в базах данных и операционных системах. Обоснуйте ответ.
18. На основе учебной литературы национальных стандартов безопасности выясните и сформулируйте правила резервирования и восстановления баз данных после сбоев, нештатных режимов работы и других инцидентов безопасности. Обоснуйте ответ.
19. На основе учебной литературы национальных стандартов безопасности сформулируйте содержание и этапы формирования задания по безопасности и профиля защиты при проектировании БД.
20. На основе учебной литературы и положений национального стандарта ГОСТ Р ИСО/МЭК 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении», обобщите и сформулируйте порядок и этапы построения защищенных информационных систем на основе защищенных баз данных.

Перечень вопросов для опроса на практических занятиях:

1. Сформулируйте и обоснуйте понятия угроз безопасности БД - общие и специфичные.
2. На основе учебной литературы выясните в чем состоит понятие, сущность и цели политики безопасности БД. Обоснуйте ответ.
3. На основе учебной литературы национальных стандартов безопасности семейства ГОСТ Р ИСО/МЭК 15408-2012-2013 обобщите и сформулируйте принципы построения защищенных информационных систем на основе БД.
4. На основе учебной литературы выясните в чем заключается разница между дискреционными и мандатными моделями безопасности СУБД. Обоснуйте ответ.
5. На основе учебной литературы выясните в чем заключается разница между метками пользователя, специальными привилегиями доступа в БД и маркерами безопасности и правами и привилегиями доступа в ОС. Обоснуйте ответ.
6. На основе учебной литературы выясните назначение и состав словаря данных для целей обеспечения безопасности в БД. Обоснуйте ответ.
7. На основе учебной литературы выясните значение представлений словаря для обеспечения целостности данных и разграничения доступа в БД. Обоснуйте ответ.
8. На основе учебной литературы выясните значение транзакций для целей обеспечения безопасности в БД. Обоснуйте ответ.
9. На основе учебной литературы выясните значение для обеспечения безопасности БД режимов блокирования и правил согласования блокировок, а также взаимоблокировок, их распознавания и разрушения.
10. В чем состоит ценность для целей обеспечения безопасности в БД Oracle утилиты WRAP? Обоснуйте ответ.
11. В чем состоит ценность для целей обеспечения безопасности в БД применения технологии FLASHBACK для получения ретроспективных состояний БД (Query, Version Query, Transaction Query, Table, Drop, Database). Обоснуйте ответ.

12. Каковы роль и возможности национальных стандартов семейства ГОСТ Р ИСО/МЭК 53113-1-2008, ГОСТ Р ИСО/МЭК 53113-2-2009 и руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» для обеспечения защищенности компьютерных систем с базами данных от несанкционированного доступа?

13. В чем состоит роль положений национального стандарта ГОСТа Р ИСО/МЭК 18045-2012 «Методология оценки безопасности информационных технологий» для анализа проектных решений подсистем информационной безопасности баз данных и обеспечения защищенности компьютерных систем в целом.

14. На основе национальных стандартов семейства ГОСТ Р ИСО/МЭК 15408-2012-2013 «Общие критерии доверия и безопасности информационных систем» сформулируйте содержание и этапы формирования задания по безопасности и профиля защиты при проектировании БД.

15. На основе национальных стандартов семейства ГОСТ Р ИСО/МЭК 53113-1-2008 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 1. Общие положения» и ГОСТ Р ИСО/МЭК 53113-2-2009 «Информационные технологии. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов. Часть 2. Рекомендации по защите информации, информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с помощью скрытых каналов» обобщенно сформулируйте принципы разработки подсистемы безопасности от несанкционированного доступа к ИС на основе БД.

16. На основе положений национальных стандартов безопасности ИС выясните и сформулируйте правила резервирования и восстановления баз данных после сбоев, нештатных режимов работы и других инцидентов безопасности, их место и роль в политике безопасности информационной системы.

Примеры заданий для самостоятельной практической работы студентов:

1. Составить и презентовать доклад о недавно закрытой уязвимости в любой БД.

Критерии выполнения задания:

- теоретическое описание уязвимости с указанием конкретных версий СУБД, для которых она воспроизводится;
- описание реализованных методов защиты от этой уязвимости;
- практическое представление механизмов атаки и защиты (возможность демонстрации онлайн преподавателю).

2. Написать программу для защиты СУБД.

Программа должна уметь следить за текущим состоянием защищённости системы (например, с помощью журналов логирования и аудита). В случае обнаружения выполненной атаки необходимо внедрить меры, обеспечивающие защиту от подобных атак в будущем и постараться нейтрализовать нанесённый ущерб, при этом обязательно оповестить администратора о применённых мерах. Например, если появилось предположение о краже пароля, необходимо применить настройку для защиты от конкретной атаки, поменять пароль и сообщить об этих действиях пользователю.

Критерии выполнения задания:

- реализована защита как минимум от трёх различных атак;
- программа должна уметь распознавать именно атаки, а не внедрять превентивные меры для устранения возможных угроз;
- проведена демонстрация атак (можно вручную, а можно автоматизировать и эту часть);
- проведена демонстрация работы программы;

– проведена демонстрация кода программы (можно на github.com).

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету:

1. Угрозы безопасности БД, общие и специфичные.
2. Парадигма безопасности БД (ИС) в соответствии с ГОСТ Р ИСО/МЭК 15408-2012-2013.
3. Защита от несанкционированного доступа. Классификация АС (БД) и требования по защите информации в соответствии с действующими руководящими документами ФСТЭК России.
4. Типовые модели ограничения доступа.
5. Способы организации разграничения доступа.
6. Ограничение доступа к записям таблиц БД.
7. Изменение доступа к записи.
8. Ограничение доступа при использовании кластеризационной модели.
9. Ограничение доступа при использовании мандатной модели.
10. Изменения в дочерних отношениях доступа.
11. Ограничение доступа при использовании дискреционно-ролевой модели доступа.
12. Хранение привилегий в защищаемом отношении.
13. Хранение привилегий в отдельном отношении.
14. Ограничение доступа при функциональной модели доступа
15. Маскировка атрибутов и организация их хранения.
16. Реализация предиката определения и использование побитной карты.
17. Назначение, структура и состав словаря данных БД.
18. Транзакции требования к ним. Фиксация транзакции в БД. Контрольные точки.
19. Триггеры.
20. Понятие целостности данных, декларативная и процедурная ссылочные целостности БД.
21. Ссылочные операции обеспечения ссылочной целостности.
22. Триггерные процедуры в обеспечении ссылочной целостности.
23. Обеспечение целостности базы данных на примере Oracle.
24. Ссылочные ограничения и реляционные ограничения DB2
25. Организация взаимодействия СУБД (на примере Oracle) и базовой ОС.
26. Соотношение прав доступа, определяемых ОС и СУБД (на примере Oracle), совместное использование файлов с другими установками, настройка маски (umask).
27. Модель полномочий на файлы от Oracle.
28. Альтернативные модели полномочий на файлы, безопасность исходных устройств, Использование безопасного временного каталога. Файлы Oracle с установленным битом SUID.
29. Субъекты и объекты, группы пользователей, привилегии, роли и представления.
30. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей.
31. Распознавание и разрушение тупиковых ситуаций в БД путем блокировок, классификация блокировок.
32. Блокировки и режимы доступа к данным в БД.
33. Уровни изоляции в SQL.
34. Блокировки в Oracle.
35. Блокировки в MySQL
36. Уязвимости, как условия существенно облегчающие нарушения конфиденциальности в БД.
37. Фазы проектирования безопасных БД. Предварительный анализ.
38. Роль обеспечения высокой готовности БД в структуре обеспечения их безопасности.

39. Получение несанкционированного доступа к конфиденциальной информации в БД путем логических выводов.
40. Методы противодействия несанкционированному доступу. Метки безопасности в БД. Использование представлений для обеспечения конфиденциальности информации в СУБД.
41. Подотчетность действий пользователя и аудит связанных с безопасностью событий в БД Oracle (опции аудита, включение и выключение опций, работа с журналом аудита, аудит с помощью триггеров и защита журнала).
42. Методы аутентификации пользователей в Oracle.
43. Модели безопасности БД (цели безопасности, роль модели безопасности в политике безопасности, простейшая модель безопасности баз данных, проверка полномочий, проверка подлинности).
44. Дискреционные (избирательные) модели безопасности БД, дискреционная политика.
45. Мандатные (полномочные) модели безопасности БД.
46. Многоуровневые модели безопасности БД. Модель Белла-Лападула.
47. Использование SQL-инъекций для нештатного использования процедур и функций.
48. Метаданные и словарь данных БД.
49. Тупиковые ситуации, их распознавание и разрушение.
50. Понятие Блокировки. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок.
51. Роль положений национальных стандартов семейства «Общие критерии доверия и безопасности информационных систем» (ГОСТ Р ИСО/МЭК 15408-2012-1, ГОСТ Р ИСО/МЭК 15408-2013-2, ГОСТ Р ИСО/МЭК 15408-2013-3) и ГОСТа Р ИСО/МЭК 18045-2012 «Методология оценки безопасности информационных технологий» для анализа проектных решений подсистем информационной безопасности баз данных и обеспечения защищенности компьютерных систем в целом.
52. Роль положений национальных стандартов ГОСТ Р ИСО/МЭК 56545-2015 «Защита информации. Уязвимость информационных систем. Правила описания уязвимостей», ГОСТ Р ИСО/МЭК 56546-2015 «Защита информации. Уязвимость информационных систем. Классификация уязвимостей информационных систем» и федерального банка данных угроз безопасности, ведущегося на сайте ФСТЭК России в разделе «Техническая защита информации» (<https://bdu.fstec.ru>) в идентификации угроз безопасности информационных систем.
53. Роль положений национальных стандартов ГОСТ Р ИСО/МЭК 53113-1-2008, ГОСТ Р ИСО/МЭК 53113-2-2009 и руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» для обеспечения защищенности компьютерных систем с базами данных от несанкционированного доступа.
54. Положения национального стандарта ГОСТ Р ИСО/МЭК 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении», регламентирующего построение защищенных информационных систем на основе защищенных баз данных.

Зачет выставляется по итогам устного опроса и отчетам по практическим работам.

Приложение № 2 к рабочей программе дисциплины «Безопасность систем баз данных»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Основы построения защищённых баз данных» являются лекции, что связано, прежде всего, с новизной материала для обучающихся. По большинству тем предусмотрены практические занятия, целью которых является закрепление лекционного материала путем решения специальным образом подобранных практических задач.

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала и решение практических задач, как в аудитории, так и самостоятельно в качестве самостоятельной работы. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения практических задач – выработать навыки построения защищённых баз данных, а также анализа информационных систем на предмет слабых мест и уязвимостей, связанных с системами управления базами данных. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

Большое внимание должно быть уделено самостоятельной работе. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или схожие с ними.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде тестирований. Также проводятся консультации (при необходимости) по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

В конце изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса и одну практическую задачу. На самостоятельную подготовку к экзамену выделяется 3 дня, в это время предусмотрена и групповая консультация.