МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«__15__» ____июня____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы построения защищённых баз данных

Направление подготовки 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс ___5___ семестр ___9____
лекции _36_ час.
практические занятия ___36__час.
лабораторные работы ____00__час.
в том числе с использованием МАО лек. __9___/пр.__12__/лаб.__00___ час.
в том числе в электронной форме лек. ___00__/пр.__00___/лаб.___00__ час.
всего часов аудиторной нагрузки___72___ час.
в том числе с использованием МАО __21__ час.
самостоятельная работа ___36____час.
в том числе на подготовку к экзамену ____00__ час.
курсовая работа / курсовой проект _____не предусмотрены
зачет ____9_____ семестр
экзамен ___не предусмотрен__

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель: Власов А.А.

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины
«Основы построения защищённых баз данных»

Рабочая программа дисциплины «Основы построения защищенных баз данных» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.35.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (36 час.), самостоятельная работа студентов (36 час.). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – зачёт.

Дисциплина логически и содержательно связана с такими курсами, как «Языки программирования», «Системы управления базами данных», «Основы информационной безопасности».

Дисциплина является базовой для изучения курсов по телекомуникационным сетям. Знания, умения и практические навыки, полученные в результате изучения дисциплины «Основы построения защищенных баз данных», позволят студентам основывать свою профессиональную деятельность на построении, проектировании и эксплуатации программно-аппаратных технологий защиты передачи информации.

Цель - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных, а также связанных с обеспечением безопасности информации в автоматизированных информационных системах, основу которых составляют базы данных, навыкам работы со встроенными в системы управления базами данных средствами защиты.

Задачи:

- обучить студентов принципам работы современных систем управления базами данных;
- привить студентам навыки проектирования и реализации баз данных;
- приобретение системного подхода к проблеме защиты информации в СУБД;
- изучение моделей и механизмов защиты в СУБД;
- приобретение практических навыков организации защиты БД;
- обучить студентов проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;
- обучить студентов формализовать поставленную задачу по обеспечению защиты БД;
- обучить студентов применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- привить студентам навыки разработки нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации в СУБД;

Для успешного изучения дисциплины «Основы построения защищенных баз данных» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5)

- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);

- способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

- способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-10).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-8 способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	интернет-технологии для поиска информации
	Умеет	использовать пакеты прикладных программ для решения задач профессиональной деятельности
	Владеет	навыками работы с прикладными программами; навыками анализа эффективности используемых прикладных программ
ПК-17 способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое	Знает	методы сбора и анализа данных при проектировании системы защиты компьютерной сети
	Умеет	производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение

программное обеспечение	Владеет	навыком выявления различных типов проблемных ситуаций; навыками анализа и составления отчетных документов

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы построения защищенных компьютерных сетей» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Теоретические основы безопасности БД (6 час.)

Тема 1. Безопасность БД, угрозы, защита (2 час.)

Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД.

Тема 2. Критерии защищенности БД (2 час.)

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 (2 час.)

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

Раздел II. Средства и методы обеспечения безопасности БД (26 час.)

Тема 1. Целостность БД и способы ее обеспечения (2 час.)

Основные виды и причины возникновения угроз целостности. Способы противодействия.

Тема 2. Метаданные и словарь данных. Транзакции и блокировки (2 час.)

Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представления словаря. 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.

Тема 3. Ссылочная целостность (2 час.)

Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности.

Тема 4. Триггеры (2 час.)

Цели использования триггеров. Способы задания, моменты выполнения.

Тема 5. Классификация угроз конфиденциальности СУБД (4 час.)

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 6. Целостность кода приложения (2 час.)

SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции.

Тема 7. Средства идентификации и аутентификации (2 час.)

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

Тема 8. Средства управления доступом (4 час.)

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 9. Аудит и подотчетность (2 час.)

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

Тема 10. Средства, поддерживающие высокую готовность (2 час.)

Аппаратная и программная поддержки. Кластерная организация серверов баз данных. Сохранение и восстановление БД

Тема 11. Распознавание вторжений в БД. (2 час.)

Определение понятия распознавания вторжений. Цели выявления злоупотреблений. Место процедуры распознавания вторжений в общей системе защиты. Типы моделей систем распознавания вторжений (ID-систем). Общая структура ID-систем. Шаблоны классов пользователей. Модели известных атак.

Раздел III. Проектирование безопасных БД (4 час.)

Тема 1. Основные понятия проектирования безопасных БД (2 час.)

Безопасное программное обеспечение. Правила безопасности. Отличия в проектировании безопасных ОС и СУБД. Независимые принципы целостности данных. Модель авторизации в System R. Архитектура безопасной СУБД. Архитектура SeaView и ASD.

Тема 2. Методология проектирования (2 час.)

Фазы проектирования безопасных БД (по DoD). Предварительный анализ. Требования и политики безопасности. Концептуальное проектирование. Логическое проектирование. Физическое проектирование.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Занятие 1. Основы построения и эксплуатации баз данных (4 час.)

1. Построение реляционных СУБД.
2. Эксплуатация баз данных.
3. Автоматизированное проектирование баз данных.

Занятие 2. Безопасность БД, угрозы, защита (4 час.)

1. Угрозы безопасности БД: общие и специфичные.
2. Требования безопасности БД.

Занятие 3. Модели безопасности в СУБД (4 час.)

1. Дискреционная (избирательная) и мандатная (полномочная) модели безопасности.
2. Классификация моделей.
3. Исследование моделей безопасности. Применение моделей безопасности в СУБД.

Занятие 4. Средства идентификации и аутентификации (4 час.)

1. Применение средств идентификации и аутентификации, встроенных в СУБД
2. Применение средств идентификации и аутентификации, встроенных в ОС.

Занятие 5. Средства управления доступом (4 час.)

1. Использование ролей и привилегий пользователей.
2. Использование представлений для обеспечения конфиденциальности информации в СУБД.
3. Использование средств реализации политик безопасности в СУБД.

Занятие 6. Целостность БД и способы ее обеспечения (4 час.)

1. Способы обеспечения целостности БД.
2. Использование триггеров.
3. Применение декларативной и процедурной ссылочные целостности.
4. Резервное копирование и восстановление базы данных.

Занятие 7. Классификация угроз конфиденциальности СУБД (4 час.)

1. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.
2. Методы противодействия.
3. Применение криптографических методов.

Занятие 8. Аудит и подотчетность (4 час.)

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

Занятие 9. Транзакции и блокировки (4 час.)

1. Применение транзакций как средства изолированности пользователей.
2. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок.
3. Тупиковые ситуации, их распознавание и разрушение.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы построения защищённых баз данных» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Теоретические основы безопасности БД	ОПК-8	знает	конспект (ПР-7)	1-5
			умеет	ОУ-1	1-5
			владеет	ОУ-2	1-5
2	Раздел II. Средства и методы обеспечения безопасности БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	6-28
			умеет	ОУ-1	6-28
			владеет	ОУ-2	6-28
3	Раздел III. Проектирование безопасных БД	ПК-17	знает	конспект (ПР-7)	29-33
			умеет	ОУ-1	29-33
			владеет	ОУ-2	29-33

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений,

навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Грошев, А.С. Основы работы с базами данных [Электронный ресурс]/ А.С. Грошев — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 255 с.— Режим доступа: http://www.iprbookshop.ru/73653.html. — ЭБС «IPRbooks»

2. Сысоев, Э.В. Особенности построения баз данных [Электронный ресурс]: учебное пособие/ Э.В. Сысоев, А.В. Селезнев— Электрон. текстовые данные. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2012. — 81 с. — Режим доступа: http://www.iprbookshop.ru/64157.html — ЭБС «IPRbooks»

3. Тарасов, С.В. СУБД для программиста. Базы данных изнутри [Электронный ресурс]: Практическое пособие / С.В. Тарасов. — Электрон. дан. — М.: СОЛОН-Пр., 2015. — 320 с. — Режим доступа: http://znanium.com/catalog/product/858603 — ЭБС «Znanium.com»

Дополнительная литература

(печатные и электронные издания)

1. Агальцов, В.П. Базы данных. В 2-х кн. Кн. 1. Локальные базы данных: учебник / В.П. Агальцов. — 2-е изд., перераб. — М.: ИД ФОРУМ: ИНФРА-М, 2012. — 352 с.: ил.; — Режим доступа: http://znanium.com/catalog/product/326451 — ЭБС «Znanium.com»

2. Агальцов, В.П. Базы данных. В 2-х кн. Кн. 2. Распределенные и удаленные базы данных: учебник / В.П. Агальцов. — 2-е изд., перераб. — М.: ИД ФОРУМ: ИНФРА-М, 2013. — 272 с.: ил.; — Режим доступа: http://znanium.com/catalog/product/326451 — ЭБС «Znanium.com»

3. Поляков, А.М. Безопасность Oracle глазами аудитора: нападение и защита [Электронный ресурс]: учебник / А.М. Поляков — М.: ДМК Пресс, 2010. — 336 с.: ил. — Режим доступа:

http://www.studentlibrary.ru/book/ISBN9785940745174.html — ЭБС «Консультант студента»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Интернет-курс по дисциплине «Безопасность баз данных» [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.e-biblio.ru/book/bib/01_informatika/b_baz_dan/sg.html
2. Базу данных не стащить: правильные способы защитить данные в таблицах БД [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://xakep.ru/2009/06/02/48406/
3. Защищённые системы: общие принципы [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://crypto.pp.ua/2010/06/319/
4. Безопасность баз данных: проблемы и перспективы [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.swsys.ru/index.php?page=article&id=4175&lang

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 450, специализированная лаборатория кафедры КС: Лаборатория администрирования информационных систем, компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	"1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015.

	Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019." 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Основы построения защищённых баз данных», составляет 108 часов. На самостоятельную работу студента отведено 36 часов.

Аудиторная нагрузка состоит из 36 часов лекционных занятий и 36 часов практических занятий. На лекционных занятиях обучающийся получает базовые теоретические знания, углубляя их в ходе самостоятельной работы и на практических занятиях. Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю. При подготовке к практическим занятиям также необходимо повторить теоретический материал. На практических занятиях обучающимся предлагаются задания различного типа, направленные на получение углубленных знаний по теме.

Данная дисциплина реализуется в 9 семестре. Курс занятий предусмотрен завершается зачётом.

Вопросы к зачёту соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к зачёту студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

Для получения «зачтено» на зачёте необходимо отчитаться о выполнении всех практических заданий.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 450, специализированная лаборатория кафедры КС: Лаборатория администрирования информационных систем, компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30) Оборудование: 11 компьютеров (системный блок модель - 30AGCT01WW P3+монитором AOC 28" LI2868POU) , доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Основы построения защищённых баз данных»
Направление подготовки 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-17 недели обучения	Подготовка к практическим занятиям №1-№9	27	Собеседование (УО-1), коллоквиум (УО-2)
2	18 неделя обучения	Подготовка к зачёту	9	Зачёт

Рекомендации по самостоятельной работе студентов

Формой контроля является зачёт, сдача практических заданий необходима для выставления зачёта.

Подготовка к практическим занятиям предполагает повторение лекционного материала и выполнение заданий по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовиться к ответу на практическом занятии. При подготовке необходимо использовать как основные, так и дополнительные материалы для более глубокого понимания предмета. По результатам работы на занятии оценивается активность студента. При условии посещения и активной работы на всех занятиях, студент получает «зачтено». В случае пропуска занятий и/или недостаточной работы, студент получает возможность сдать недостающие задания на зачёте.

Самостоятельная работа при подготовке к зачёту включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Основы построения защищённых баз данных»
Направление подготовки 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-8 способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знает	интернет-технологии для поиска информации
	Умеет	использовать пакеты прикладных программ для решения задач профессиональной деятельности
	Владеет	навыками работы с прикладными программами; навыками анализа эффективности используемых прикладных программ
ПК-17 способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Знает	методы сбора и анализа данных при проектировании системы защиты компьютерной сети
	Умеет	производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение
	Владеет	навыком выявления различных типов проблемных ситуаций; навыками анализа и составления отчетных документов

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Теоретические основы безопасности БД	ОПК-8	знает	конспект (ПР-7)	1-5
			умеет	ОУ-1	1-5
			владеет	ОУ-2	1-5
2	Раздел II. Средства и методы обеспечения безопасности БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	6-28
			умеет	ОУ-1	6-28
			владеет	ОУ-2	6-28
3	Раздел III. Проектирование безопасных БД	ПК-17	знает	конспект (ПР-7)	29-33
			умеет	ОУ-1	29-33
			владеет	ОУ-2	29-33

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачёт.

Зачёт проводится в форме собеседования, вопросы к зачёту соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на экзамене обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

Оценочные средства для промежуточной аттестации

Список вопросов к зачёту:

1. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД.
2. Критерии оценки надежных компьютерных систем (TCSEC). Интерпретация TCSEC для надежных СУБД (TDI).
3. Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели.
4. Дискреционная (избирательная) и мандатная (полномочная) модели безопасности.
5. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД.
6. Основные виды и причины возникновения угроз целостности. Способы противодействия.
7. Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представления словаря.
8. Транзакции как средство изолированности пользователей.

9. Сериализация транзакций. Методы сериализации транзакций.

10. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок.

11. Тупиковые ситуации, их распознавание и разрушение.

12. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности.

13. Цели использования триггеров. Способы задания, моменты выполнения.

14. Причины, виды, основные методы нарушения конфиденциальности.

15. Типы утечки конфиденциальной информации из СУБД, частичное разглашение.

16. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.

17. Методы противодействия. Особенности применения криптографических методов.

18. SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции.

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

20. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления.

21. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей.

22. Соотношение прав доступа, определяемых ОС и СУБД.

23. Использование представлений для обеспечения конфиденциальности информации в СУБД.

24. Средства реализации мандатной политики безопасности в СУБД.

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

26. Аппаратная и программная поддержки. Кластерная организация серверов баз данных. Сохранение и восстановление БД

27. Определение понятия распознавания вторжений. Цели выявления злоупотреблений. Место процедуры распознавания вторжений в общей системе защиты.

28. Типы моделей систем распознавания вторжений (ID-систем). Общая структура ID-систем. Шаблоны классов пользователей. Модели известных атак.

29. Безопасное программное обеспечение. Правила безопасности.

30. Отличия в проектировании безопасных ОС и СУБД.

31. Независимые принципы целостности данных. Модель авторизации в System R.

32. Архитектура безопасной СУБД. Архитектура SeaView и ASD.

33. Фазы проектирования безопасных БД (по DoD). Предварительный анализ. Требования и политики безопасности. Концептуальное проектирование. Логическое проектирование. Физическое проектирование.

На зачёте студенту задаются два вопроса из списка выше. По результатам ответа студент получает «зачтено» либо «незачтено». В зачетную книжку заносится только «зачтено».

При оценке ответа на зачёте учитываются:

- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет.

Для получения «зачтено» ответ студента должен соответствовать следующим минимальным требованиям: полный ответ на 1 вопрос или частичный ответ на 2 вопроса; допускаются нарушения в последовательности изложения; демонстрируются поверхностные знания вопроса; имеются затруднения с выводами; допускаются нарушения норм литературной речи.

Оценка **«незачтено»** выставляется в случае если: обучающийся не ответил полно ни на один вопрос; материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине; имеются заметные нарушения норм литературной речи.

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются коллоквиум (УО-2) и конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся коллоквиумы. Темы коллоквиумов соответствуют темам практических занятий из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание ответа
Отлично	Полные и точные ответы на все вопросы по теме занятия; Свободное владение основными терминами и понятиями курса; Последовательное и логичное изложение материала курса; Законченные выводы и обобщения по теме вопросов; Соблюдаются нормы литературной речи.
Хорошо	Полные и точные ответы на все вопросы по теме занятия; Знание основных терминов и понятий курса; Последовательное изложение материала курса; Умение формулировать некоторые обобщения по теме вопросов;

	Соблюдаются нормы литературной речи.
Удовлетворительно	Полные и точные ответы на часть вопросов; Удовлетворительное знание основных терминов и понятий курса; Удовлетворительное знание и владение методами и средствами решения поставленных задач; Недостаточно последовательное изложение материала курса; Умение формулировать отдельные выводы и обобщения по теме вопросов.
Неудовлетворительно	Полные и точные ответы на часть вопросов; Материал излагается непоследовательно, сбивчиво; Имеются заметные нарушения норм литературной речи.