



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

Специальность 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 72 час.
в том числе на подготовку к экзамену 27 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 9 семестр

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)

ABSTRACT

Specialist's degree in 10.05.01 Computer Security

Specialization "Mathematical Methods for Information Security"

Course title: Basics of building secure databases

Basic part of Block, 3 credits

Instructor: Vlasov A.A.

At the beginning of the course a student should be able to:

- • ability to apply scientific research methods in professional activities, including work on interdisciplinary and innovative projects (OPK-4);
- • the ability to develop formal models of security policies, access control and information flow policies in computer systems, taking into account information security threats (OPK-9);

Learning outcomes:

- OPK-8 ability to use programming languages and systems, tools for solving professional, research and applied tasks
- PC-17 with the ability to install, adjust, test and maintain modern general and special software, including operating systems, database management systems, network software

Course description:

Discipline is basic for studying courses on telecommunication networks. Knowledge, skills and practical skills obtained as a result of studying the discipline "Basics of building secure databases" will allow students to base their professional activities on building, designing and operating software and hardware technologies for protecting information transfer.

Main course literature:

1. Шмырев В.И., Шмырев Д.В. Анализ зарубежного опыта по защите операционных систем и систем управления базами данных / В.И . Шмырев, Д.В. Шмырев – Москва : Российский государственный социальный университет 2011. – 314 с. – Режим доступа: <https://elibrary.ru/item.asp?id=24438209>

2. Сенченко П.В. Организация баз данных [Электронный ресурс]: учебное пособие/ Сенченко П.В.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 170 с.— Режим доступа: <http://www.iprbookshop.ru/72147.html>

Form of final control: exam.

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

Рабочая программа учебной дисциплины «Основы построения защищённых баз данных» разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» в базовую часть дисциплин учебного плана Б1.Б.6.9.

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 – зачет в 9 семестре.

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

Содержание дисциплины охватывает следующий круг вопросов: администрирование Систем управления баз данных, механизмов защиты как внешних, так и встроенных. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных. Кластерная организация серверов баз данных.

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

Дисциплина направлена на формирование общекультурных, общепрофессиональных и профессиональных компетенций выпускника.

Цель дисциплины: 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:

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

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

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, 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	интернет-технологии для поиска информации
Знает	использовать пакеты прикладных программ для решения задач профессиональной деятельности
Умеет	навыками работы с прикладными программами;
Владеет	навыками анализа эффективности используемых прикладных программ
ПК-17 способностью производить установку, наладку, тестирование и обслуживание современного общего и специального	методы сбора и анализа данных при проектировании системы защиты компьютерной сети
Знает	

программного
обеспечения, включая
операционные системы,
системы управления
базами данных, сетевое
программное обеспечение

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

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы построения защищенных баз данных» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах, проведение и сдача лабораторных работ. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Теоретические основы безопасности БД (8 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 (4 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 (20 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 (1 час.)

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

Тема 4. Триггеры (1 час.)

Цели использования триггеров. Способы задания, моменты выполнения.

Тема 5. Классификация угроз конфиденциальности СУБД (2 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 (2 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 (8 час.)

Тема 1. Основные понятия проектирования безопасных БД (4 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 (4 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 ПК-17	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	1-5
			умеет	лабораторные работы (ПР-6),	1-5
			владеет	конспект (ПР-7)	1-5
2	Раздел II. Средства и методы обеспечения безопасности БД	ОПК-8 ПК-17	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	6-28
			умеет	лабораторные работы (ПР-6),	6-28
			владеет	конспект (ПР-7)	6-28
3	Раздел III. Проектирование безопасных БД	ОПК-8 ПК-17	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	29-33
			умеет	лабораторные работы (ПР-6),	29-33
			владеет	конспект (ПР-7)	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. Шмырев В.И., Шмырев Д.В. Анализ зарубежного опыта по защите операционных систем и систем управления базами данных / В.И. Шмырев, Д.В. Шмырев – Москва : Российский государственный социальный университет 2011. – 314 с. – Режим доступа: <https://elibrary.ru/item.asp?id=24438209>

2. Сенченко П.В. Организация баз данных [Электронный ресурс]: учебное пособие/ Сенченко П.В.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 170 с.— Режим доступа: <http://www.iprbookshop.ru/72147.html>

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>

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>

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>

3. Варлатая С.К., Шаханова М.В. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс для вузов - Владивосток : Изд-во Дальневосточного технического университета, 2008. – 216 с. - <http://lib.dvfu.ru:8080/lib/item?id=chamo:384163&theme=FEFUпр>

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 566, Учебная 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
---	--

	<p>Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно.</p> <p>4) MathCad Education University Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно.</p> <p>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.</p> <p>6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.</p>
--	---

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 54 часа.

Аудиторная нагрузка состоит из 27 часов лекционных занятий и 27 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**

<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 566, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 50) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт</p>
--	---



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

**УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ
РАБОТЫ ОБУЧАЮЩИХСЯ**
по дисциплине «Основы построения защищённых баз данных»
Специальность 10.05.01 Компьютерная безопасность
специализация «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	34	Собеседование (УО-1), коллоквиум (УО-2)
2	18 неделя обучения	Подготовка к зачёту	2	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.



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Основы построения защищённых баз данных»
Специальность 10.05.01 Компьютерная безопасность
специализация «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

Умеет

Владеет

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

Умеет

интернет-технологии для поиска информации

использовать пакеты прикладных программ для
решения задач профессиональной деятельности

навыками работы с прикладными программами;

навыками анализа эффективности используемых
прикладных программ

методы сбора и анализа данных при
проектировании системы защиты компьютерной
сети

производить установку, наладку, тестирование и
обслуживание современного общего и
специального программного обеспечения, включая
операционные системы, системы управления

базами данных, сетевое программное обеспечение
 навыком выявления различных типов проблемных
 ситуаций;
 Владеет
 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 ПК-17	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	1-5
			умеет	лабораторные работы (ПР-6),	1-5
			владеет	конспект (ПР-7)	1-5
2	Раздел II. Средства и методы обеспечения безопасности БД	ОПК-8 ПК-17	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	6-28
			умеет	лабораторные работы (ПР-6),	6-28
			владеет	конспект (ПР-7)	6-28
3	Раздел III. Проектирование безопасных БД	ОПК-8 ПК-17	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	29-33
			умеет	лабораторные работы (ПР-6),	29-33
			владеет	конспект (ПР-7)	29-33

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	Этапы формирования компетенции	критерии	показатели
ОПК-8 способностью использовать языки и	Знает	Методы сбора и анализа данных при проектировании системы защиты	полнота и системность знаний изложение полученных знаний полное, в соответствии

системы программирования, инструментальные средства для решения различных профессиональных, исследовательских и прикладных задач		компьютерной сети.		с требованиями учебной программы; ошибки отсутствуют или несут незначительный характер, обучающийся способен самостоятельно исправить.
	Умеет	Использовать пакеты прикладных программ для решения задач профессиональной деятельности.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	Навыком выявления различных типов проблемных ситуаций. Навыками анализа и составления отчетных документов.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных

			цели, проводить самоанализ и самооценку.	задач.
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	Общие принципы построения охраны и защиты объектов	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
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	Умеет	Производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.

		программное обеспечение.		
	Владеет	Навыками работы с прикладными программами. Навыками анализа эффективности и используемых прикладных программ.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.

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	<p>Полные и точные ответы на все вопросы по теме занятия;</p> <p>Свободное владение основными терминами и понятиями курса;</p> <p>Последовательное и логичное изложение материала курса;</p> <p>Законченные выводы и обобщения по теме вопросов;</p> <p>Соблюдаются нормы литературной речи.</p>
Хорошо	<p>Полные и точные ответы на все вопросы по теме занятия;</p> <p>Знание основных терминов и понятий курса;</p> <p>Последовательное изложение материала курса;</p> <p>Умение формулировать некоторые обобщения по теме вопросов;</p> <p>Соблюдаются нормы литературной речи.</p>
Удовлетворительно	<p>Полные и точные ответы на часть вопросов;</p> <p>Удовлетворительное знание основных терминов и понятий курса;</p> <p>Удовлетворительное знание и владение методами и средствами решения поставленных задач;</p> <p>Недостаточно последовательное изложение материала курса;</p> <p>Умение формулировать отдельные выводы и обобщения по теме вопросов.</p>
Неудовлетворительно	<p>Полные и точные ответы на часть вопросов;</p> <p>Материал излагается непоследовательно, сбивчиво;</p> <p>Имеются заметные нарушения норм литературной речи.</p>