



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 защищенных 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.

в том числе в электронной форме 00 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 (ли): Москаленко Ю.С. К.т.н., доцент, с.н.с. Профессор

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

Bachelor's degree in *Computer security (10.05.01)*

Specialization “*Mathematical methods of information protection*”

Course title: *Basics of building secure databases*

Basic part of Block, 3 credits

Instructor: *Moskalenko Yu.S.*

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. *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»*

Form of final control: *pass-fail exam.*

Аннотация к рабочей программе дисциплины «Основы построения защищенных 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 базовую часть учебного плана Б1.Б.35.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов (лекции – 36 часов, практические занятия – 36 часов, самостоятельная работа – 36 часов). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – зачет.

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 телекоммуникационным 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 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	<p>Знает Интернет-технологии для поиска информации.</p> <p>Умеет Использовать пакеты прикладных программ для решения задач профессиональной деятельности.</p> <p>Владеет Навыками работы с прикладными программами. Навыками анализа эффективности используемых прикладных программ.</p>
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	<p>Знает Методы сбора и анализа данных при проектировании системы защиты компьютерной сети.</p> <p>Умеет Производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение.</p> <p>Владеет Навыком выявления различных типов проблемных ситуаций. Навыками анализа и составления отчетных документов.</p>

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. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).

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

№	Контролируемые	Коды и этапы	Оценочные средства
---	----------------	--------------	--------------------

п/п	разделы / темы дисциплины	формирования компетенций	текущий контроль	промежуточная аттестация	
1	Раздел I. Теоретические основы безопасности БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	1-5
			умеет	коллоквиум (УО-2)	1-5
			владеет	коллоквиум (УО-2)	1-5
2	Раздел II. Средства и методы обеспечения безопасности БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	6-28
			умеет	коллоквиум (УО-2)	6-28
			владеет	коллоквиум (УО-2)	6-28
3	Раздел III. Проектирование безопасных БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	29-33
			умеет	коллоквиум (УО-2)	29-33
			владеет	коллоквиум (УО-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

Для работы с литературой из списка необходимо наличие у студента аккаунтов в указанных электронно-библиотечных системах: «IPRbooks» (<http://www.iprbookshop.ru/>), «Znanium.com» (<http://znanium.com/>), «Консультант студента» (<http://www.studentlibrary.ru>).

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. Учебная аудитория для проведения занятий	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30) Оборудование: 11 компьютеров (системный блок модель - 30AGCT01WW P3+монитором AOC 28" LI2868POU) Доска аудиторная
--	---

лекционного, практического семинарского групповых индивидуальных консультаций, контроля промежуточной аттестации.	и типа, и текущего и
---	----------------------------------



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

**УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ
РАБОТЫ ОБУЧАЮЩИХСЯ**
по дисциплине «Основы построения защищённых баз данных»
Направление подготовки 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 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	30	Отчет о выполнении практического задания
2	18 неделя обучения	Подготовка и сдача зачета	6	Зачет

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения «зачтено» отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка «незачтено» выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.



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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

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

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции

Этапы формирования компетенции

<p>ОПК-8 способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач</p>	<p>Знает</p> <p>Умеет</p> <p>Владеет</p>	<p>Интернет-технологии для поиска информации.</p> <p>Использовать пакеты прикладных программ для решения задач профессиональной деятельности.</p> <p>Навыками работы с прикладными программами.</p> <p>Навыками анализа эффективности используемых прикладных программ.</p>
<p>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</p>	<p>Знает</p> <p>Умеет</p> <p>Владеет</p>	<p>Методы сбора и анализа данных при проектировании системы защиты компьютерной сети.</p> <p>Производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение.</p> <p>Навыком выявления различных типов проблемных ситуаций. Навыками анализа и составления отчетных документов.</p>

№ 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	конспект (ПР-7)	1-5
			умеет	коллоквиум (УО-2)	1-5
			владеет	коллоквиум (УО-2)	1-5
2	Раздел II. Средства и методы обеспечения безопасности БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	6-28
			умеет	коллоквиум (УО-2)	6-28
			владеет	коллоквиум (УО-2)	6-28
3	Раздел III. Проектирование безопасных БД	ОПК-8, ПК-17	знает	конспект (ПР-7)	29-33
			умеет	коллоквиум (УО-2)	29-33
			владеет	коллоквиум (УО-2)	29-33

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.

Критерии выставления оценки на зачет

Оценка	Требования к сформированным компетенциям
«зачтено»	Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их

	выполнения.
«не зачтено»	Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины