

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю

Зам. директора по УР

Н.А. Андреева

«28» _____ 2026 г.

Рабочая программа дисциплины

Б1.О.36.04 Безопасность систем баз данных

Кафедра: **Информационная безопасность**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	Часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/7
Контактная работа, в том числе (по семестрам, курсам):		68/7
Лекции		34/7
Лабораторных работ		18/7
Практических занятий		16/7
Семинаров		
Самостоятельная работа		40/7
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/7
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

Профессор кафедры ИБ, д.пол.н., к.т.н., доцент Жуковский А.Г.

Рабочая программа дисциплины
«Безопасность систем баз данных»

Разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427

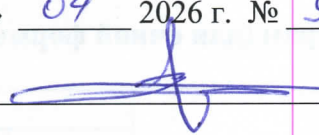
.

Составлена на основании учебного плана

направления 10.03.01 Информационная безопасность, профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03. 2026 г., и утвержденного директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационная безопасность

Протокол от «28» 04 2026 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины «Безопасность систем баз данных» является формирование у обучаемых знаний в области информационной безопасности СУБД и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в базах данных.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности:

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ОПК-1.3: Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям
Знать:
- принципы администрирования средств защиты информации при работе с базами данных в соответствии с требованиями по защите информации.
Уметь:
- использовать средства администрирования различных баз данных, web-ресурсов и проводить оценку угроз их информационной безопасности.
Владеть:
- навыками администрирования различных систем управления базами данных в соответствии с требованиями по защите информации, создания защищенных баз данных для получения, обработки, хранения и использования информации веб-ресурсов.
ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
Знать:
- принципы построения и контроля ИТ-инфраструктуры организации; - основные аспекты информационной безопасности; - методы защиты объектов от несанкционированного доступа физических лиц и основные направления противодействия техническим средствам разведки; - механизмы, используемые для защиты информации, циркулирующей в различных системах;
Уметь:
- моделировать типовые и специализированные информационные системы; - применять на практике технические методы защиты информации, пользоваться стандартной терминологией и определениями; - формулировать и решать задачи проектирования профессионально-ориентированных подсистем и средств обеспечения защиты информации с использованием различных методов и решений.
Владеть:
- навыками мониторинга событий информационной безопасности, расследования инцидентов информационной безопасности; - навыками выявления и нейтрализации компьютерных атак, оценки защищенности элементов информационных сетей; - способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики; - методами и средствами инженерной защиты и технической охраны объектов; - навыками подготовки технического задания на разработку подсистем защиты информации.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.27 Основы информационной безопасности
2	Б1.О.33 Программно-аппаратные средства защиты информации
3	Б1.О.40 Базы данных
4	Б1.В.03 Защита информации от вредоносного программного обеспечения
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.30 Моделирование систем защиты информации
2	Б1.В.02 Комплексное обеспечение защиты информации объекта информатизации
3	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях
4	Б2.В.03(Пд) Производственная (преддипломная) практика

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 68 аудиторных часов – 34 лек + 18 лр + 16 пз + 40 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИ О
Курс 4, Семестр 7					
Модуль 1. Проектирование безопасных СУБД. (18л+20лр+20) часов					
1.1	Лекция 1. Введение в дисциплину. Назначение и роль баз данных. Модели данных. История развития вопроса безопасности баз данных. Безопасность систем баз данных. Актуальность проблемы. Основные понятия.	Лек. 1	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Этапы научного формирования проблемы информационной безопасности систем баз данных. Структура свойства информационной безопасности баз данных	Лек. 2	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. СУБД – средства управления данными в БД. Проектирование баз данных. Инфологическое моделирование предметной области БД.	Лек. 3	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.4	Лекция 4. Реляционные базы данных. Обеспечение целостности реляционных БД путем нормализации их отношений	Лек. 4	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.5	Лекция 5. Проектирование баз данных. Решение проблем информационной безопасности на различных этапах	Лек. 5	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3

	проектирования				
1.6	Лекция 6. Основы безопасности БД. Руководящие документы.	Лек 6	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.7	Лекция 7. Эксплуатация баз данных. Состав и проведение регламентных работ	Лек 7	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.8	Лекция 8. СУБД. Языковые средства описания, манипулирования, запросов. Функции и использование	Лек 8	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.9	Лекция 9 Распределенная обработка данных. Архитектура систем управления базами данных	Лек 9	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
1.10	Установка POSTGRESQL для WINDOWS	ЛР1	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.11	Установка POSTGRESQL для LINUX	ЛР2	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.12	Подключение к серверу PostgreSQL	ЛР3	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.13	Утилита pgAdmin III — графическое средство для администрирования СУБД PostgreSQL	ЛР4	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.14	Утилита psql – интерактивный терминал для администрирования СУБД PostgreSQL	ЛР5	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.15	Расположение файлов сервера базы данных	ЛР6	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.16	Расположение файлов сервера базы данных. Таблицы в базе данных	ЛР7	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.17	Создание тестовой базы данных. Создание таблиц. Создание последовательностей. Ввод данных. Чтение данных из таблиц	ЛР8	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.18	Сортировка результатов. Чтение данных из нескольких таблиц с применением вложенных запросов. Транзакции	ЛР9	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.2
1.19	Основные принципы обеспечения безопасности Управление привилегиями Секционирование. Сегментирование	СРС	20	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3

	Факторы планирования резервного копирования				
Модуль 2. Угрозы информационной безопасности баз данных. Средства защиты и обеспечение целостности БД (16+14+20) часов					
2.1	Лекция 9. Угрозы информационной безопасности. Источники угроз. Классификация угроз информационной безопасности баз данных	Лек. 10	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.2	Лекция 10. Политика безопасности	Лек. 11	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.3	Лекция 11. Средства защиты систем баз данных	Лек. 12	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.4	Лекция 12 Обеспечение целостности баз данных. Структурная, языковая, ссылочная целостность. Способы поддержки семантической целостности. Администрирование баз данных.	Лек 13	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.5	Лекция 13. Обеспечение согласованности данных в многопользовательском режиме обработки. Понятие транзакции. Идентификация и аутентификация пользователей	Лек 14	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.6	Лекция 14. Дискреционная защита. Представления	Лек 15	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.7	Лекция 15 Мандатная защита	Лек 16	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3
2.8	Лекция 16 Многоуровневая модель безопасности. Защита данных при статистической обработке	Лек 17	2	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3Л 3.2
2.9	Аутентификация в PostgreSQL	ПЗ1	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.1
2.10	Резервное копирование в PostgreSQL Основные понятия. Типы резервного копирования.	ПЗ2	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.1
2.11	Аудит в БД. Возможности аудита в PostgreSQL	ПЗ3	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.1
2.12	Мониторинг инфраструктуры БД. Мониторинг в PostgreSQL	ПЗ 4	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 Л3.1
2.13	Zabbix – свободно-распространяемая система мониторинга статусов различных сервисов компьютерной сети, серверов и сетевого	ПЗ5	4	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3

	оборудования.				ЛЗ.1
2.14	Защита данных встроенными средствами СУБД. Триггеры	ПЗ6	2	ОПК-1.3 ОПК-12	Л2.1 Л2.2 Л2.3 ЛЗ.1
2.15	Механизмы репликации в PostgreSQL Виды шифрования БД. Шифрование в PostgreSQL Противодействие SQL-инъекциям	СРС	20	ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3 Л2.1
3	Зачет			ОПК-1.3 ОПК-12	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 ЛЗ.1 ЛЗ.2
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛП.1	А. В. Скрыпников, С. В. Родин, Г. В. Перминов, Е. В. Чернышова ; под редакцией С. В. Белокуров	Безопасность систем баз данных. Учебное пособие	Воронеж : Воронежский государственный университет инженерных технологий, 2015. — 144 с.	Э1
ЛП.2	Гулятьева, Т. А.	Основы информационной безопасности : учебное пособие	Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с.	Э2
ЛП.3	Гутман, Г. Н.	Объектно-реляционная СУБД PostgreSQL : учебное пособие	Самара : Самарский государственный технический университет, ЭБС АСВ, 2016. — 125 с.	Э3
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛП.1	Малков, О. Б.	Работа с СУБД PostgreSQL : учебное пособие	Омск : Омский государственный технический университет, 2023. — 175 с.	Э4
ЛП.2	А. М. Наместников, А. А. Филиппов	Базы данных. Практический курс. В 2 частях. Ч.1. Объектно-реляционные базы данных на примере PostgreSQL 9.5 : учебное пособие	Ульяновск : Ульяновский государственный технический университет, 2017	Э5
ЛП.3	Бурцева Е.В., Рак И.П.,	Базы данных. Учебное пособие	Тамбовский государственный технический университет, ЭБС	Э6

	Платенкин А.В.		АСВ 2023	
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	Осин А.В., Хализев К.А.	Безопасность систем баз данных. Практические примеры настройки базовых функций безопасности баз данных: Учебно-методическое пособие для выполнения практических работ для бакалавров. Направление подготовки 10.03.01	Москва: МТУСИ, 2025. – 18с.	Э7
ЛЗ.2	Осин А.В., Ванюшина А.В., Васильев Р.А.	Безопасность систем баз данных: Практикум по выполнению лабораторных работ для бакалавров. Направление подготовки: 10.03.01	Москва: МТУИ, 2023. – 55 с.	Э8
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/50628.html			
Э2	https://www.iprbookshop.ru/91640.html			
Э3	https://www.iprbookshop.ru/90660.html			
Э4	https://www.iprbookshop.ru/140858.html			
Э5	https://www.iprbookshop.ru/106085.html			
Э6	https://www.iprbookshop.ru/141031.html			
Э7	https://elib.mtuci.ru/view.php?book_id=34640			
Э8	https://elib.mtuci.ru/view.php?book_id=3068			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Сборник нормативных документов «Регламент» – https://reglament.pro/index.php/entrance (неограниченный доступ для авторизованных пользователей)			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Электронный ресурс http://www.securitylab.ru/			
5.3.5	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.6	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	PostgreSQL			
П.2	Утилита pgAdmin III			
П.3	Утилита psql			
П.4	Zabbix – свободно-распространяемая система мониторинга статусов различных сервисов			
П.5	MS Word – лицензионное ПО			
П.6	ОС Linux – свободное ПО			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации
2	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.
--

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала

(понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Безопасность систем баз данных Б1.О.36.04» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____

(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

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

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной

		литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	--

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-1.3: Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям; ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений		
Знать:		
ОПК-1.3 - принципы администрирования средств защиты информации при работе с базами данных в соответствии с требованиями по защите информации; ОПК-12 – принципы построения и контроля ИТ-инфраструктуры организации; основные аспекты информационной безопасности; методы защиты объектов от несанкционированного доступа физических лиц и основные направления противодействия техническим средствам разведки; механизмы, используемые для защиты информации, циркулирующей в различных системах	Контрольная работа Лекции 1-9	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
	Контрольная работа Лекции 10-17	Модуль 2 0÷11 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-11
Уметь		
ОПК-1.3 - использовать средства администрирования различных баз данных, web-ресурсов и проводить оценку угроз их информационной безопасности; ОПК-12 – моделировать типовые и специализированные информационные системы; применять на практике технические методы защиты информации, пользоваться стандартной терминологией и определениями; формулировать и решать задачи	Лабораторные работы 1-5	Модуль 1 0÷4 за каждую ЛР «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4
	Практические занятия 1-3	Модуль 2 0÷6 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3-4 «Отлично» - 5-6

проектирования профессионально-ориентированных подсистем и средств обеспечения защиты информации с использованием различных методов и решений.		
Владеть		
ОПК-1.3 - навыками администрирования различных систем управления базами данных в соответствии с требованиями по защите информации, создания защищенных баз данных для получения, обработки, хранения и использования информации веб-ресурсов; ОПК-12 — навыками мониторинга событий информационной безопасности, расследования инцидентов информационной безопасности; навыками выявления и нейтрализации компьютерных атак, оценки защищённости элементов информационных сетей; способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики; методами и средствами инженерной защиты и технической охраны объектов; навыками подготовки технического задания на разработку подсистем защиты информации.	Лабораторные работы 6-9	Модуль 1 0÷5 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практические занятия 4-6	Модуль 2 0÷7 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 4-5 «Отлично» - 6-7
	Зачет	0-100 баллов: «Не зачтено» - 0-40 «Зачтено» - 41-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 9 лекционных занятия и 9 лабораторных работ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные лабораторные работы обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-1.3 ОПК-12):

1. Назначение и роль баз данных.
2. Модели данных.
3. Безопасность систем баз данных.
4. Этапы научного формирования проблемы информационной безопасности систем баз данных.
5. Структура свойства информационной безопасности баз данных
6. СУБД – средства управления данными в БД.
7. Проектирование баз данных.
8. Инфологическое моделирование предметной области БД.
9. Реляционные базы данных.
10. Обеспечение целостности реляционных БД путем нормализации их отношений
11. Проектирование баз данных.
12. Решение проблем информационной безопасности на различных этапах проектирования
13. Основы безопасности БД. Руководящие документы.
14. Эксплуатация баз данных. Состав и проведение регламентных работ
15. СУБД. Основные понятия.
16. Языковые средства описания, манипулирования, запросов.
17. Функции и использование СУБД.
18. Распределенная обработка данных.
19. Архитектура систем управления базами данных

Лабораторная работа 1. Установка PostgreSQL для WINDOWS**Лабораторная работа 2. Установка PostgreSQL для LINUX****Лабораторная работа 3. Подключение к серверу PostgreSQL****Лабораторная работа 4. Утилита pgAdmin III — графическое средство для администрирования СУБД PostgreSQL****Лабораторная работа 5. Утилита psql – интерактивный терминал для администрирования СУБД PostgreSQL****Лабораторная работа 6. Расположение файлов сервера базы данных****Лабораторная работа 7. Расположение файлов сервера базы данных. Таблицы в базе данных****Лабораторная работа 8. Создание тестовой базы данных. Создание таблиц. Создание последовательностей. Ввод данных. Чтение данных из таблиц****Лабораторная работа 9. Сортировка результатов. Чтение данных из нескольких таблиц с применением вложенных запросов. Транзакции.****Модуль 2: (50 баллов):**

Модуль содержит 8 лекционных занятий и 6 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 11. За выполненные и защищенные практические работы обучающийся получает максимум 39 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-1.3, ОПК-12):

1. Угрозы информационной безопасности.
2. Источники угроз.
3. Классификация угроз информационной безопасности баз данных
4. Политика безопасности

5. Средства защиты систем баз данных
6. Обеспечение целостности баз данных.
7. Структурная, языковая, ссылочная целостность.
8. Способы поддержки семантической целостности.
9. Администрирование баз данных.
10. Обеспечение согласованности данных в многопользовательском режиме обработки.
11. Понятие транзакции.
12. Идентификация и аутентификация пользователей
13. Дискреционная защита. Представления
14. Мандатная защита
15. Многоуровневая модель безопасности. Защита данных при статистической обработке

Практическое занятие 1. Аутентификация в PostgreSQL

Практическое занятие 2. Резервное копирование в PostgreSQL. Основные понятия.

Типы резервного копирования.

Практическое занятие 3. Аудит в БД. Возможности аудита в PostgreSQL

Практическое занятие 4. Мониторинг инфраструктуры БД. Мониторинг в PostgreSQL

Практическое занятие 5. Zabbix – свободно-распространяемая система мониторинга статусов различных сервисов компьютерной сети, серверов и сетевого оборудования.

Практическое занятие 6. Защита данных встроенными средствами СУБД. Триггеры.

1.3.2. Вопросы, выносимые на зачет по дисциплине «Безопасность систем баз данных» (ОПК-1.3, ОПК-12) (промежуточная аттестация):

1. Назначение и роль баз данных.
2. Модели данных.
3. Безопасность систем баз данных.
4. Этапы научного формирования проблемы информационной безопасности систем баз данных.
5. Структура свойства информационной безопасности баз данных
6. СУБД – средства управления данными в БД.
7. Проектирование баз данных.
8. Инфологическое моделирование предметной области БД.
9. Реляционные базы данных.
10. Обеспечение целостности реляционных БД путем нормализации их отношений
11. Проектирование баз данных.
12. Решение проблем информационной безопасности на различных этапах проектирования
13. Основы безопасности БД. Руководящие документы.
14. Эксплуатация баз данных. Состав и проведение регламентных работ
15. СУБД. Основные понятия.
16. Языковые средства описания, манипулирования, запросов.
17. Функции и использование СУБД.
18. Распределенная обработка данных.
19. Архитектура систем управления базами данных
20. Угрозы информационной безопасности.
21. Источники угроз.
22. Классификация угроз информационной безопасности баз данных

23. Политика безопасности
24. Средства защиты систем баз данных
25. Обеспечение целостности баз данных.
26. Структурная, языковая, ссылочная целостность.
27. Способы поддержки семантической целостности.
28. Администрирование баз данных.
29. Обеспечение согласованности данных в многопользовательском режиме обработки.
30. Понятие транзакции.
32. Идентификация и аутентификация пользователей
32. Дискреционная защита. Представления
33. Мандатная защита
34. Многоуровневая модель безопасности.
35. Защита данных при статистической обработке.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения промежуточных и итоговой аттестаций

Предусмотрены следующие виды контроля:

- промежуточный контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- промежуточный контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- итоговый контроль по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы в рамках текущего контроля переводятся в оценку на зачете в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Безопасность систем баз данных»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	11	39
Зачет	100	100	

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На зачете производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю И.о.зав. кафедрой «ИБ» _____ А.Г. Жуковский «___» _____ 20__ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 4 Дисциплина: Безопасность систем баз данных		
Билет №1 1. Структура свойства информационной безопасности баз данных. 2. . Классификация угроз информационной безопасности баз данных. «___» _____ 20__ г. И.о.зав.кафедрой ИБ, д.пол.н., к.т.н., доцент _____ Жуковский А.Г.		

Один комплект отпечатанных билетов к зачету, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания по дисциплине «Безопасность систем баз данных»

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций:

ОПК-1.3: Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.

ОПК-2 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой из компетенций равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ОПК-1.3: Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Одним из средств обеспечения конфиденциальности информации является: 1. Кодирование 2. Шифрование 3. Утечка 4. Наблюдение
2	Угрозами нарушения конфиденциальности данных могут быть: 1. Несанкционированный доступ к данным 2. Случайная ошибка программиста 3. Неквалифицированные действия оператора 4. Установка обновлений ОС
3	Системы БД отличаются от остальных видов прикладного программного обеспечения (ПО): 1. Спецификой запуска 2. Объемом программного кода. 3. Двойственной природой (БД и СУБД)
4	Администрирования СУБД включает: 1. Аутентификация и авторизация пользователя; 2. Криптографическая защита БД; 3. Резервное копирование данных; 4. Аудит событий безопасности БД; 5. Списание устаревшего оборудования.

№ задания	Тексты заданий
5	Целью управления доступом является: 1. Ограничение действий или операций, которые может выполнять легальный пользователь; 2. Ограничение действий или операций, которые может выполнять несанкционированный пользователь; 3. Улучшение эффективности работы информационной системы. 1.
6	Резервное копирование необходимо для: 1. Аварийного восстановления данных; 2. Устранения ошибок пользователей; 3. Необходимости получения данных или схемы базы данных в некоторый момент времени в прошлом; 4. Ускорения работы информационной системы.
7	Резервное копирование может быть: 1. Полным; 2. Дифференциальным; 3. Инкрементным; 4. Закрытым.
8	По способу создания резервное копирование может быть: 1. Физическим; 2. Логическим; 3. Патологическим.
9	Существуют следующие базовые стратегии резервного копирования 1. Простая; 2. Сбалансированная; 3. Сложная.
10	Различают следующие типы репликаций: 1. Синхронная репликация; 2. Асинхронная репликация; 3. Полусинхронная репликация; 4. Сверхсинхронная репликация; 5. Отсутствующая репликация;

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие Пользователь, который имеет неограниченные привилегии. 1. В MySQL; 2. В PostgreSQL; 3. В MongoDB. А. «root», Б. «postgres»; В. «userAdminAnyDatabase» А,Б,В.
12	Установите соответствие команд их описанию параметров 1. SUPERUSER NOSUPERUSER 2. CREATEDB NOCREATEDB 3. CREATEROLE NOCREATEROLE 4. CONNECTION LIMIT А. Определяют, будет ли эта роль «суперпользователем», который может переопределить все ограничения доступа. Б. Определяют, сможет ли роль создавать базы данных. В. Определяют, сможет ли роль создавать (изменять, удалять) другие роли. Г. Определяет, сколько параллельных подключений может установить роль. АБВГ
13	Установите соответствие 1. BACKUP COPY;

№ задания	Тексты заданий
	2. RECOVERY POINT OBJECTIVE; 3. RECOVERY TIME OBJECTIVE. А. Процедура или операция создания копии данных, размещённой отдельно от оригинала, обычно на отдельных носителях информации. Б. Максимальный период времени, за который могут быть потеряны данные в результате инцидента. В. Промежуток времени, в течение которого система может оставаться недоступной в случае аварии. АБВ
14	Установите соответствие видов топологии репликации БД: 1. При репликации с одним ведущим сервером; 2. При репликации с несколькими ведущими серверами; 3. При репликации без ведущих серверов; А. Данные всегда отправляются на один конкретный узел; Б. Может существовать несколько узлов, играющих роль ведущих, и каждый ведущий узел должен сохранять данные в кластере; В. Все узлы могут принимать данные при записи. АБВ

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Перечислите 3 вида классических SQL-инъекций 1. SQL-инъекции на основе объединения; 2. SQL-инъекции на основе последовательных запросов; 3. SQL-инъекции на основе возвращаемых ошибок.
16	Перечислите 3 вида слепых SQL-инъекций 1. SQL-инъекции на основе содержимого; 3. SQL-инъекции на основе возвращаемых ошибок; 4. SQL-инъекции на основе времени исполнения запроса.
17	Транзакция – это выполняемая от имени определенного пользователя или процесса последовательность операторов манипулирования данными, переводящая базу данных из одного целостного состояния в другое целостное состояние. Транзакциям присущи следующие свойства, известные как ACID. Расставьте соответствующую последовательность свойств в нужном порядке 1. durability – долговечность; 2. isolation – изолированность; 3. consistency – согласованность; 4. atomicity – атомарность. 4321

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите ответ

№ задания	Тексты заданий
18	Добавить недостающие слова в определение доступа к информации: Безопасность данных – это состояние защищенности, при котором обеспечиваются конфиденциальность, доступность и _____ данных.
19	Закончить определение Процесс подтверждения заявленной идентичности посредством предоставления доказательств - это _____
20	Завершите определения Копия данных, которая может использоваться для восстановления данных в случае возникновения ошибки или для восстановления БД на другом сервере называют _____

**Система оценивания выполнения тестовых заданий по компетенции ОПК-1.3,
формируемой дисциплиной «Безопасность систем баз данных»**

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Источниками угроз для баз данных могут быть: 1. Системный администратор 2. Программист 3. Пользователь 4. Неисправность жесткого диска. 5. Слабый процессор сервера
2	Принципы, на которых основаны политики, следующие: 1. Принцип минимальных или максимальных привилегий; 2. Принцип открытой или закрытой системы; 3. Принцип централизованного и децентрализованного администрирования; 4. Принцип неприкосновенности.
3	В PostgreSQL метод аутентификации конкретного клиентского соединения может основываться: 1. На адресе компьютера клиента, 2. На имени базы данных, 3. На имени пользователя. 4. На понятиях и правилах. 1,2,3
4	В PostgreSQL поддерживаются несколько типов аутентификации: 1. Простая аутентификация; 2. Аутентификация по паролю; 3. Внешние системы аутентификации; 4. Сложная аутентификация. 1,2,3.
5	В PostgreSQL существует множество типов прав. К ним относятся: 1. DELETE, 2. CREATE, 3. USAGE, 4. DESERT 5. SELECT,
6	Выберите три разных подхода к резервному копированию данных в PostgreSQL: 1. Долгое копирование; 2. Ассимиляционное копирование. 3. Логическое копирование – выгрузка в SQL; 4. Физическое копирование на уровне файлов; 5. Непрерывное архивирование;
7	Использование репликации позволяет осуществить ряд практических задач: 1. Повышение производительности системы; 2. Обеспечение отказоустойчивости; 3. Резервирование данных; 4. Автоматическое выключение. 5. Увеличить количество ошибок.
8	В модели репликации PostgreSQL для репликации используются следующие физические компоненты: 1. Ведущий сервер – сервер, предоставляющий данные; 2. Подчиненный сервер – сервер, копирующий себе данные, предоставляемые ведущим сервером. 3. Рабочие станция, предназначенные для пользователей.
9	Параметры мониторинга БД включают следующие группы 1. мониторинг на уровне соединения с хранилищем данных; 2. контроль процессов внутри базы данных; 3. мониторинг объектов базы данных; 4. мониторинг запросов к базе. 5. мониторинг операционной системы.

№ задания	Тексты заданий
10	Шифрование баз данных может быть осуществлено 1. На высоком уровне; 2. На уровне хранилища; 3. На уровне базы данных; 4. На уровне приложения.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие 1. Секционирование; 2. Сегментирование; А. Разделение хранимых объектов баз данных (таких как таблицы, индексы, материализованные представления) на отдельные части с отдельными параметрами физического хранения. Б. разделение баз данных, отдельных её объектов или индексов поисковых систем на независимые части, каждая из которых управляется отдельным экземпляром сервера базы данных, размещаемым, как правило, на отдельном вычислительном узле.
12	Установите соответствие задач мониторинга инфраструктуры: 1. отладка и послеаварийный анализ 2. бизнес-анализ 3. исправления и изменения 4. анализ производительности и поведения 5. планирование мощностей А. для определения когда что-то повреждено или скоро будет повреждено, чтобы вовремя это исправить Б. Для понимания того, как влияет использование новых функций и оптимизация. В. Для предотвращения нехватки ресурсов в критический момент Г. Для быстрого нахождения точки сбоя и точки оптимизации, позволяющих снизить риск в будущем Д. Для наблюдения, как пользователи используют функции системы и как это влияет на соотношение стоимости разработки и эффективности.
13	Установите соответствие в определениях 1. Шифрование 2. Шифрование БД 3. Шифрование подвижных данных А. Использование технологии сокрытия информации Б. Использование технологии шифрования для преобразования информации, хранящейся в базе данных, в шифротекст В. Шифрование обмена данными между БД и любыми клиентами или приложениями, которым требуется доступ к базе данных
14	Установите соответствие командам шифрования и дешифрования в PostgreSQL 1. pgp_sym_encrypt 2. pgp_pub_encrypt 3. pgp_sym_decrypt 4. pgp_pub_decrypt А. зашифровывает данные открытым ключом PGP Б. шифрует данные симметричным ключом PGP В. расшифровывает сообщение, зашифрованное открытым ключом. Г. расшифровывает сообщение, зашифрованное симметричным ключом PGP.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в порядке уровни системы мониторинга БД 1. настройка оповещений для системы мониторинга, 2. уровень инфраструктуры 3. мониторинг приложения как инженерного продукта 4. уровень приложения
16	Установите правильный порядок уровней иерархии системы мониторинга 1. Проверка доступности базы данных. 2. Мониторинг общих показателей задержек/ошибок и сквозной мониторинг работоспособности. 3. Мониторинг прикладного уровня для измерения задержек/ошибок для каждого вызова базы данных. 4. Сбор как можно большего количества показателей, относящихся к уровням системы, хранилища, базы данных и приложений. 5. Специальные проверки для отдельных известных проблем.
17	Перечислите 5 компонентов программы мониторинга БД Zabbix:

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите ответ

№ задания	Тексты заданий
18	Завершите определение: Лицо или процесс, действия которого регламентируются правилами разграничения доступа – это _____ Единица информации автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа это _____
19	Завершите определение _____ событий безопасности БД представляет собой процесс получения и анализа данных о происходящих в системе событиях
20	При использовании _____ необходимо отслеживать следующие 4 события: - попытки неудачной аутентификации; - изменения в системе безопасности; - выполнение резервного копирования; - действия привилегированных пользователей.

Система оценивания выполнения тестовых заданий по компетенции ОПК-12, формируемой дисциплиной «Безопасность систем баз данных»

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий, учебно-методических материалов, образцов техники
- содержать материал, углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 40	Неделя
Модуль 1 – 20 часов			
1	Основные принципы обеспечения безопасности	5	1-2
2	Управление привилегиями	5	3-4
3	Секционирование. Сегментирование	5	5-6
4	Факторы планирования резервного копирования;	5	7-8
Модуль 2 – 20 часов			
9	Механизмы репликации в PostgreSQL.	6	9-11
10	Виды шифрования БД. Шифрование в PostgreSQL.	8	12-14
11	Противодействие SQL-инъекциям.	6	15-17

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.