Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

**Рабочая программа дисциплины**
**Средства и методы защиты хранилищ и баз данных**

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2021 года

Квалификация
Бакалавр

КАФЕДРА **Информационные технологии и программирование**

**Распределение часов дисциплины по семестрам**

| Семестр (<Курс>.<Семестр на курсе>) | **3 (2.1)** | | Итого | |
|---|---|---|---|---|
| Недель | 16 | | | |
| Вид занятий | УП | РП | УП | РП |
| Лекции | 48 | 48 | 48 | 48 |
| Лабораторные | 48 | 48 | 48 | 48 |
| Итого ауд. | 96 | 96 | 96 | 96 |
| Контактная работа | 96 | 96 | 96 | 96 |
| Сам. работа | 12 | 12 | 12 | 12 |
| Итого | 108 | 108 | 108 | 108 |

## ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): доцент, Прохоров А.И.

Зав. кафедрой: к.э.к., доц. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| | |
|---|---|
| 1.1 | Изучение принципов и методов построения защиты хранилищ и баз данных |

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

**В результате освоения дисциплины обучающийся должен:**

**Знать:**

Знать основы системного администрирования и программирования, методы и архитектуры обеспечения отказоустойчивости (соотнесено с индикатором ОПК-12.1)

**Уметь:**

Уметь разрабатывать и реализовывать отказоустойчивые приложения, настраивать и обслуживать программное и аппаратное обеспечение, анализировать и диагностировать проблемы системы, проводить тестирование на отказ и мониторинг производительности.(соотнесено с индикатором ОПК-12.2)

**Владеть:**

Владеть системами управления версиями, СУБД и консольными утилитами для разработки и тестирования, инструментами мониторинга и логирования. (соотнесено с индикатором ОПК-12.3)

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### Раздел 1. Основы защиты баз данных

| № | Наименование темы / Вид занятия | Семестр / Курс | Часов | Компетен-ции | Литература |
|---|---|---|---|---|---|
| 1.1 | Основы хранилищ и баз данных, термины и нормативные документы / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.2 | Средства защиты баз данных. Рассматриваются основные угрозы безопасности, методы защиты и практические рекомендации для повышения устойчивости систем / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.3 | Рекомендации по разработке безопасных приложений для работы с базами данных. Систематизированный обзор ключевых рекомендаций по обеспечению безопасности приложений, работающих с базами данных / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.4 | Многоуровневая защита хранилищ данных / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.5 | Настройка прав доступа в СУБД с применением PostgreSQL и Firebird / Лаб / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.6 | Реализация многоуровневой защиты хранилищ с применением PostgreSQL. Построение комплексный подхода, объединяющий аппаратные, программные и организационные меры безопасности / Лаб / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.7 | Современные подходы к защите баз данных. Рассмотрение передовых тактик и стратегий построений защищенных баз данных / Ср / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 1.8 | Методы и инструменты для мониторинга активности в базах данных / Ср / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |

### Раздел 2. Криптография и безопасность данных

| № | Наименование темы / Вид занятия | Семестр / Курс | Часов | Компетен-ции | Литература |
|---|---|---|---|---|---|
| 2.1 | Криптография в защите данных. рассмотрение способов применения криптографических технологий для защиты баз данных / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 2.2 | Использование средств контроля целостности данных. Рассмотрение наборов средств для контроля целостности | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, |

| | | | | | |
|---|---|---|---|---|---|
| | данных / Лек / | | | | Л2.4 |
| 2.3 | Рекомендации по разработке безопасных приложений для работы с базами данных. Рассмотрение примеров безопасных приложений и приложений имеющих уязвимости / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 2.4 | Зависимость защиты данных от использования искусственного интеллекта (ИИ). Применение ИИ в системах с использованием СУБД / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 2.5 | Шифрование данных в базах данных с применением PostgreSQL. Настройка шифрования баз данных / Лаб / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 2.6 | Аудит доступа к базам данных с применением PostgreSQL. Рассмотрениеключевых аспектов обеспечения безопасности, надежности и производительности информационных систем / Лаб / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 2.7 | Лучшие практики применения криптографии в базах данных / Ср / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 2.8 | Управление уязвимостями в системах с базами данных / Ср / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |

**Раздел 3. Безопасность сетевого взаимодействия и аудит баз данных**

| № | Наименование темы / Вид занятия | Семестр / Курс | Часов | Компетен-ции | Литература |
|---|---|---|---|---|---|
| 3.1 | Безопасность сетевого взаимодействия с базами данных. Общие угрозы безопасности при сетевом взаимодействии / Лек / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 3.2 | Аудит и мониторинг баз данных. Способы выявления аномалий по системам логирования / Лек / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 3.3 | Анализ и интерпретация журналов аудита. Повышение безопасности СУБД, способы интерпретации журналов / Лек / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 3.4 | Проведение аудита и оценка рисков в управлении базами данных. Рассмотрение рекомендаций ФСТЭК по проведению аудита ИС / Лек / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 3.5 | Анализ уязвимостей баз данных с применением sqlmap и PostgreSQL. Поиск и выявление уязвимостей в лабораторных условиях / Лаб / | 3 | 8 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 3.6 | Аудит доступа к базам данных с применением PostgreSQL. Настройка аудита доступа в лабораторных условиях / Лаб / | 3 | 8 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 3.7 | Методы и инструменты для мониторинга активности в базах данных / Ср / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |

**Раздел 4. Резервное копирование и современные угрозы**

| № | Наименование темы / Вид занятия | Семестр / Курс | Часов | Компетен-ции | Литература |
|---|---|---|---|---|---|
| 4.1 | Резервное копирование и восстановление. Рассмотрение подходов к резервному копированию и восстановлению для баз данных / Лек / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 4.2 | Новые тренды в резервном копировании и восстановлении данных. Перспективные способы и подходы к резервному копированию и восстановлению для баз данных / Лек / | 3 | 4 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 4.3 | Безопасность облачных хранилищ данных. Рассмотрение подходов к резервному копированию и восстановлению для облачных баз данных / Лек / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 4.4 | Резервное копирование и восстановление баз данных с применением PostgreSQL. Настройка резервного копирования в лабораторных условиях / Лаб / | 3 | 8 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 4.5 | Тестирование на SQL-инъекции с применением PostgreSQL. Защита от SQL-инъекций в лабораторных условиях / Лаб / | 3 | 8 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |

| | | | | | |
|---|---|---|---|---|---|
| 4.6 | Управление уязвимостями в системах с базами данных / Ср / | 3 | 2 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |
| 4.7 | / Зачёт / | 3 | 0 | ОПК-12 | Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л2.4 |

## 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература

| | Авторы, | Заглавие | Издательство, год | Колич-во |
|---|---|---|---|---|
| Л1.1 | Завгородний В. И. | Комплексная защита информации в компьютерных системах: Учеб. пособие | М.: Логос, 2001 | 49 |
| Л1.2 | Артемов А. В. | Информационная безопасность: курс лекций: курс лекций | Орел: Межрегиональная академия безопасности и выживания, 2014 | https://biblioclub.ru/index.php?page=book&id=428605 неограниченный доступ для зарегистрированных пользователей |
| Л1.3 | Парфенов, Ю. П. | Постреляционные хранилища данных: учебное пособие | Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2016 | https://www.iprbookshop.ru/68372.html неограниченный доступ для зарегистрированных пользователей |

### 5.2. Дополнительная литература

| | Авторы, | Заглавие | Издательство, год | Колич-во |
|---|---|---|---|---|
| Л2.1 | Тищенко Е. Н. | Основы информационной безопасности: учеб.-метод. разраб. | Ростов н/Д: Изд-во РГЭУ (РИНХ), 2012 | 10 |
| Л2.2 | Хорев П. Б. | Программно-аппаратная защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. "Информ. безопасность" | М.: ФОРУМ, 2015 | 25 |
| Л2.3 | Рытенкова О. | Информационная безопасность: журнал | Москва: ГРОТЕК, 2014 | https://biblioclub.ru/index.php?page=book&id=238446 неограниченный доступ для зарегистрированных пользователей |
| Л2.4 | Прохорова О. В. | Информационная безопасность и защита информации: учебник | Самара: Самарский государственный архитектурно-строительный университет, 2014 | https://biblioclub.ru/index.php?page=book&id=438331 неограниченный доступ для зарегистрированных пользователей |

### 5.3 Профессиональные базы данных и информационные справочные системы

Консультант Плюс

### 5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Libreoffice (свободно распространяемое ПО)
postgresql (свободно распространяемое ПО)
sqlmap (свободно распространяемое ПО)

**5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья**

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и свободно распространяемыми программными средствами и выходом в Интернет.

## 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

**Приложение 1**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## 1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

| ЗУН, составляющие компетенцию | Показатели оценивания | Критерии оценивания | Средства оценивания |
|---|---|---|---|
| ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; | | | |
| Знать основы системного администрирования и программирования, методы и архитектуры обеспечения отказоустойчивости | Описывает способы решения стандартных задач профессиональной деятельности в области информационной безопасности | Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное | Опрос (вопросы 1-50)<br><br>Вопросы к зачету (вопросы 1-50) |
| Уметь разрабатывать и реализовывать отказоустойчивые приложения, настраивать и обслуживать программное и аппаратное обеспечение, анализировать и диагностировать проблемы системы, проводить тестирование на отказ и мониторинг производительности. | Анализирует состояние информационной системы, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания | Полнота и правильность решения практико-ориентированного задания или практического задания | Лабораторные работы (задания 1-7)<br><br>Практико-ориентированные задания к зачету (задания 1-10) |
| Владеть системами управления версиями, СУБД и консольными утилитами для разработки и тестирования, инструментами мониторинга и логирования. | Использует методы и средствами управления программного обеспечения в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания | Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного и практического задания | Лабораторные работы (задания 1-7)<br><br>Практико-ориентированные задания к зачету (задания 1-10) |

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов (зачтено)

0-49 баллов (не зачтено)

## 2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

### Вопросы к зачету

1. Как создать роль в PostgreSQL?
2. Какие привилегии можно назначить ролям?
3. Как использовать группы пользователей для упрощения управления доступом?
4. Что такое наследование привилегий в СУБД?
5. Как проверить текущие роли и привилегии пользователя?
6. Что представляет собой принцип наименьших привилегий?
7. Как реализовать этот принцип в базе данных?
8. Как это помогает минимизировать риски безопасности?
9. Какие метрики можно использовать для оценки реализации этого принципа?
10. Каковы лучшие практики для управления правами доступа?
11. Какие существуют методы шифрования данных в СУБД?
12. Когда следует использовать шифрование данных?
13. Как осуществляется шифрование на уровне столбца и таблицы?
14. Как обеспечить безопасность ключей шифрования?
15. В чем разница между Transparent Data Encryption и раздельным шифрованием?
16. Какие встроенные средства шифрования доступны в PostgreSQL?
17. Как настроить встроенное шифрование данных?
18. Как хорошо встроенные средства шифрования работают с производительностью?
19. Как проверять, что данные зашифрованы правильно?
20. Какие аспекты безопасности необходимо учесть при использовании встроенных средств?
21. Как внедрить внешние криптографические модули в СУБД?
22. Каковы преимущества использования внешнего шифрования?
23. Как осуществляется интеграция внешних модулей с базой данных?
24. Как проверить корректность работы внешних криптографических модулей?
25. Какие существуют известные модули для шифрования данных?
26. Как настроить автоматизированное резервное копирование в PostgreSQL?
27. Какие параметры следует учитывать при настройке расписания?
28. Каковы лучшие практики для управления расписанием резервного копирования?
29. Что такое инкрементальное и полное резервное копирование?
30. Как гарантировать целостность резервных копий?
31. Как тестирование процедур восстановления помогает обеспечить безопасность?
32. Как часто следует проводить тестирование восстановления?
33. Каковы стандартные процедуры для восстановления из резервных копий?
34. Как оценить эффективность тестов на восстановление?
35. Что включается в документирование процедур восстановления?
36. Что такое аудит доступа и зачем он нужен?
37. Как настроить аудит доступа к базе данных?
38. Какие действия должны отслеживаться в аудите?
39. Каковы цели анализа журнала аудита?

40. Как использовать аудиторские данные для повышения безопасности?
41. Как настроить аудит в PostgreSQL?
42. Какие существуют инструменты для ведения журнала аудита?
43. Как анализировать результаты аудита для выявления уязвимостей?
44. Как организовать хранение журналов аудита?
45. Как проводить регулярные проверки аудиторских записей?
46. Как интерпретировать журналы аудита?
47. Какие инструменты могут помочь в анализе журналов?
48. Как выявить подозрительные действия в журналах аудита?
49. Какова роль анализаторов в процессе повышения безопасности?
50. Как использовать результаты анализа для улучшения политики безопасности?

## Практико-ориентированные задания к зачету

Задание 1
Настройка прав доступа

Создайте новую роль в PostgreSQL с ограниченными правами. Назначьте ей доступ только для чтения к таблицам в тестовой базе данных. Проверьте, что роль не может изменять данные.

Задание 2
Аудит доступа к базе данных

Настройте аудит в PostgreSQL для отслеживания действий пользователей в тестовой базе данных. Введите несколько операций с данными и проанализируйте журналы аудита на предмет зарегистрированных действий.

Задание 3
Защита от SQL-инъекций

Создайте веб-приложение с использованием PHP, в котором есть форма для ввода данных. Реализуйте SQL-запросы без подготовки и протестируйте приложение на уязвимость к SQL-инъекциям. Затем исправьте уязвимости, используя подготовленные запросы.

Задание 4
Резервное копирование и восстановление

Настройте автоматизированное резервное копирование базы данных PostgreSQL. Реализуйте процедуру восстановления из резервной копии и протестируйте процесс, убедившись, что все данные восстановлены правильно.

Задание 5
Шифрование данных

Создайте таблицу в базе данных и реализуйте шифрование одного из полей с помощью встроенных средств шифрования PostgreSQL. Проверьте, как шифрование влияет на производительность.

Задание 6
Использование внешних криптографических модулей

Интегрируйте внешний криптографический модуль с вашей базой данных. Используйте его для шифрования и дешифрования данных, хранящихся в таблице.

Задание 7
Мониторинг активности базы данных

Настройте инструмент мониторинга для отслеживания активности в вашей базе данных PostgreSQL. Создайте отчет, в котором указаны активные соединения и выполненные запросы за определенный период.

Задание 8
Тестирование на уязвимости

Используйте инструмент для тестирования на уязвимости (например, SQLMap) и прогоните его через ваше веб-приложение, чтобы выявить потенциальные уязвимости. Составьте отчет с рекомендациями по улучшению безопасности.

Задание 9
Настройка защищённого соединения

Настройте SSL-соединение для вашей базы данных PostgreSQL. Проверьте, что данные передаются по защищенному каналу и настройте клиентское приложение для работы с SSL.

Задание 10
Разработка безопасного приложения

Создайте простое веб-приложение для управления пользователями, включая функции регистрации и входа. Реализуйте безопасные методы ввода данных, проверку на уровне сервера, и обеспечьте защиту паролей с помощью хэширования.

**Критерии оценивания:**
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

*Критерии оценивания одного теоретического вопроса:*
- 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
- 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

*Критерии оценивания практико-ориентированного задания:*
- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
- 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
- 11-24 балла выставляется, если задание решено частично.

– 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:

- 50-100 баллов (зачтено);
- 0-49 баллов (не зачтено).

## Опрос

Вопросы для опроса:

1. Что такое базовая концепция защиты данных?
2. Каковы основные угрозы для баз данных?
3. В чем разница между конфиденциальностью, целостностью и доступностью данных?
4. Какова роль шифрования в защите баз данных?
5. Какие существуют методы аутентификации пользователей?
6. Какие средства используются для защиты баз данных?
7. Как работает межсетевой экран для защиты баз данных?
8. Какие существуют типы шифрования данных в СУБД?
9. Как настроить резервное копирование баз данных для защиты от потери данных?
10. Какие меры по защите от физической угрозы существуют?
11. Какова основная роль криптографии в безопасности данных?
12. В чем разница между симметричным и асимметричным шифрованием?
13. Какие алгоритмы шифрования используются для защиты данных в базах данных?
14. Как проверяются подлинность и целостность данных с использованием криптографии?
15. Что такое хэширование и как оно применяется в безопасности данных?
16. Как обеспечить безопасное соединение с базой данных через интернет?
17. Какова роль SSL/TLS в защите сетевого взаимодействия?
18. Какие меры принимаются для предотвращения MITM-атак на соединениях с БД?
19. Какова важность сегментации сети для безопасности баз данных?
20. Как настроить доступ к базе данных через VPN?
21. Что такое аудит базы данных и зачем он нужен?
22. Каковы основные действия, которые должны отслеживаться в процессе аудита?
23. Как использовать журналы аудита для повышения безопасности?
24. Какие существуют инструменты для мониторинга активности в базах данных?
25. Как интерпретировать журналы аудита для обнаружения аномалий?
26. Что такое SQL-инъекция и как она происходит?
27. Какие меры можно принять для предотвращения SQL-инъекций?
28. Каковы лучшие практики для работы с пользовательским вводом в SQL-запросах?
29. Как работают подготовленные запросы для защиты от SQL-инъекций?
30. Какие инструменты могут помочь в тестировании на уязвимости SQL-инъекций?
31. Какие основные риски связаны с облачными хранилищами данных?
32. Как обеспечить безопасность данных в облаке?
33. Как происходит управление доступом в облачных БД?
34. Какие стандарты безопасности данных существуют для облачных хранилищ?
35. Как обеспечить шифрование данных в облачных хранилищах?
36. Каково значение резервного копирования баз данных?
37. Какие существуют стратегии резервного копирования?
38. Каковы методы восстановления данных после сбоя?
39. Что такое тестирование процедур восстановления?
40. Как настроить автоматизированное резервное копирование?
41. Как искусственный интеллект может улучшить безопасность данных?
42. Какие потенциальные уязвимости существуют в системах с ИИ?
43. Как алгоритмы ИИ могут быть использованы для обнаружения аномалий?

44. Как обеспечить безопасный доступ к данным для ИИ-систем?
45. Как обеспечить защиту данных, используемых для обучения ИИ?
46. Каковы основные принципы управления доступом в СУБД?
47. Как назначить права доступа пользователям в PostgreSQL?
48. Как работают роли и привилегии в СУБД?
49. Как реализовать принцип наименьших привилегий?
50. Какие инструменты можно использовать для управления правами доступа?

**Критерии оценивания*:***
Максимальное количество баллов, которые обучающийся может набрать – 30 баллов (за 30 ответов).
Ответ на вопрос оценивается:

- 1 балл – правильный и полный ответ;
- 0 баллов – неправильный ответ или ответ не представлен.

## Лабораторные работы

1. Анализ уязвимостей баз данных с применением sqlmap и postgresql
2. Настройка прав доступа в СУБД с применением postgresql
3. Шифрование данных в базах данных с применением postgresql
4. Резервное копирование и восстановление баз данных с применением postgresql
5. Аудит доступа к базам данных с применением postgresql
6. Тестирование на SQL-инъекции с применением postgresql
7. Реализация многоуровневой защиты хранилищ с применением postgresql

**Критерии оценивания:**
Максимальное количество баллов, которые обучающийся может набрать – 70 баллов (за 7 работ).
Каждое задание оценивается:

- 10 баллов. – задание выполнено верно;
- 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 6-3 баллов. – при выполнении задания были допущены ошибки;
- 2- 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

**Текущий контроль** успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

**Промежуточная аттестация** проводится в форме зачета.

Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

**Приложение 2**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные работы

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовки к практическим занятиям.

В ходе лабораторных работ углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием практической работы;
- подготовить ответы на контрольные вопросы по изучаемой теме.

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.