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
Методы отказоустойчивого программирования

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 2024 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
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.н., доц. Радченко Ю.В.

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Изучение принципов и методов разработки защищенных систем и программного обеспечения

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и защищенных технических средств обработки информации

В результате освоения дисциплины обучающийся должен:

Знать:

основы системного администрирования и программирования, методы и архитектуры обеспечения отказоустойчивости (соотнесено с индикатором ПК-1.1)

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 ПК-1.2)

Владеть:

системами управления версиями и консольными утилитами для разработки и тестирования, инструментами мониторинга и логирования. (соотнесено с индикатором ПК-1.2)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основы отказоустойчивости и надежности ПО

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Введение в отказоустойчивое программирование Основные принципы и концепции отказоустойчивости, их значение для разработки программного обеспечения. / Лек /	4	2	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.2	Методы тестирования и проверки надежности программного обеспечения Обзор методов тестирования, таких как юнит-тесты, интеграционные и нагрузочные тесты, а также методы, обеспечивающие надежность работы ПО. / Лек /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.3	Архитектуры с высокой доступностью (High Availability) и устойчивостью к сбоям Примеры и особенности архитектур с высокой доступностью, использование кластеров и репликаций. / Лек /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.4	Использование избыточности и дублирования в отказоустойчивых системах Методы репликации данных и дублирования процессов для обеспечения стабильной работы в случае отказа. / Лек /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.5	Системы обнаружения и устранения ошибок Обзор механизмов обнаружения и исправления ошибок, таких как контрольные суммы и алгоритмы самовосстановления. / Лек /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.6	естирование надежности программного обеспечения Ознакомиться с методами юнит-тестирования и интеграционного тестирования для проверки надежности ПО. / Лаб /	4	8	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.7	Создание системы с высокой доступностью. Научиться применять принципы архитектуры с высокой доступностью и устойчивостью к сбоям. / Лаб /	4	8	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.8	Методологии обеспечения отказоустойчивости в различных сферах ИТ Изучение различных подходов к отказоустойчивости в веб-приложениях, мобильных платформах, промышленных системах и облачных сервисах. / Ср /	4	6	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.9	Метрики надежности программного обеспечения Ключевые показатели надежности: MTBF (среднее время между отказами), MTTR (среднее время восстановления) и их роль в оценке стабильности системы. / Ср /	4	6	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.10	Примеры реальных систем с высокой доступностью Исследование архитектур Amazon, Google, Netflix и других	4	6	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4

	компаний, нацеленных на обеспечение высокой доступности. / Ср /				
1.11	Кластеры и балансировка нагрузки Принципы организации кластерных систем и балансировки нагрузки для устойчивости к пиковым нагрузкам и сбоям. / Ср /	4	6	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
1.12	Методы обнаружения и исправления сбоев в реальном времени Примеры использования мониторинга и автоматических систем обнаружения отказов для предотвращения и устранения проблем. / Ср /	4	6	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4

Раздел 2. Методы обеспечения целостности и безопасности в отказоустойчивых системах

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Исключения и обработка ошибок в отказоустойчивом программировании Принципы обработки ошибок, структурирование исключений и создание самовосстанавливающихся процессов. / Лек /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.2	Техника резервного копирования и восстановления Резервное копирование данных, стратегии восстановления после отказа и их автоматизация. / Лек /	4	2	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.3	Методы обеспечения целостности данных Проверка целостности данных, коды Хэмминга, CRC и другие подходы к защите данных от ошибок. / Лек /	4	2	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.4	Непрерывное развертывание и мониторинг отказоустойчивых систем Автоматизация развертывания, мониторинг и анализ поведения системы в реальном времени для своевременного реагирования на сбои. / Лек /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.5	Безопасность и отказоустойчивость программного обеспечения Методы защиты данных и систем от атак, механизмы предотвращения и реагирования на инциденты, обеспечивающие отказоустойчивость. / Лек /	4	2	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.6	Обработка исключений и восстановление после ошибок. Изучить механизмы обработки исключений и способы восстановления ПО после сбоев. / Лаб /	4	8	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.7	Резервное копирование и восстановление данных. Изучить стратегии резервного копирования и восстановления данных. / Лаб /	4	8	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.8	Методы кодирования для обеспечения целостности данных Изучение кодов Хэмминга, CRC и других методов кодирования для предотвращения потери и искажения данных. / Ср /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.9	Алгоритмы самовосстановления и самовосстанавливающиеся системы Примеры использования алгоритмов самовосстановления, таких как системные «watchdogs» и службы автоматического перезапуска. / Ср /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.10	Основы кибербезопасности для отказоустойчивых систем Изучение угроз и методов защиты отказоустойчивых систем от атак и вредоносного ПО. / Ср /	4	4	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.11	Самостоятельная работа в libreoffice. / Ср /	4	2	ПК-1	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4
2.12	/ Зачёт /	4	0	ПК-1	Л1.1, Л1.2, 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

	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	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)

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
ПК-1: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и защищенных технических средств обработки информации			
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) 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 задания (задания 1-7) Практико-ориентированные задания к зачету (задания 1-10)
Владеть системами управления версиями 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 задания (задания 1-7) 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. Что такое отказоустойчивость программного обеспечения и зачем она нужна?
2. Какие основные принципы отказоустойчивого программирования вы знаете?
3. В чем разница между отказоустойчивостью и восстановлением после отказа?
4. Какие существуют типы отказов в программном обеспечении?
5. Как тестирование помогает обеспечивать надежность программного обеспечения?
6. Какие виды тестирования используются для повышения надежности?
7. Что такое юнит-тестирование и как оно способствует отказоустойчивости?
8. В чем заключается суть нагрузочного тестирования и в каких случаях оно применяется?
9. Что такое архитектура с высокой доступностью (High Availability)?
10. Каковы ключевые особенности кластерных систем?
11. Какие подходы используются для повышения отказоустойчивости в архитектуре приложений?

12. В чем заключается роль дублирования данных в отказоустойчивых системах?
13. Какие существуют виды репликации данных?
14. В чем разница между активной и пассивной репликацией?
15. Как можно обеспечить отказоустойчивость при помощи кластеров?
16. Что такое система обнаружения и устранения ошибок?
17. Какие методы автоматического обнаружения отказов применяются в современных системах?
18. В чем заключается роль контрольных сумм в отказоустойчивом программировании?
19. Какие существуют алгоритмы для проверки целостности данных?
20. Что такое код Хэмминга и как он используется в отказоустойчивом программировании?
21. Как работает балансировка нагрузки в отказоустойчивых системах?
22. Какие метрики надежности программного обеспечения применяются для оценки отказоустойчивости?
23. Как рассчитывается MTBF и MTTR?
24. Какие архитектуры и технологии используются для повышения отказоустойчивости в облачных системах?
25. Какие компании и системы можно считать образцовыми примерами по отказоустойчивости?
26. Что такое обработка исключений и как она помогает в создании отказоустойчивых систем?
27. Какую роль играет механизм обработки исключений в защите системы от сбоев?
28. Как работает механизм самовосстановления в отказоустойчивых системах?
29. Какие существуют принципы построения самовосстанавливающихся программных систем?
30. Что такое резервное копирование и зачем оно необходимо?
31. Какие стратегии резервного копирования данных применяются в отказоустойчивых системах?
32. Какова роль восстановления данных в отказоустойчивом программировании?
33. В чем разница между полным и инкрементным резервным копированием?
34. Какие существуют методы восстановления данных после сбоя?
35. В чем заключается значимость обеспечения целостности данных?
36. Как применяется алгоритм CRC в защите целостности данных?
37. Какие механизмы применяются для защиты целостности данных в системах с высокой отказоустойчивостью?
38. Какие алгоритмы самовосстановления применяются в современных системах?
39. Какие инструменты используются для мониторинга отказоустойчивых систем?
40. Какие метрики мониторинга помогают своевременно обнаружить отказ в системе?
41. Какую роль играет логирование в обеспечении надежности ПО?
42. Что такое Prometheus и Grafana, и как они помогают в мониторинге систем?
43. Какова роль кибербезопасности в обеспечении отказоустойчивости систем?
44. Какие методы защиты отказоустойчивых систем от атак существуют?
45. В чем заключаются основные принципы кибербезопасности для отказоустойчивых систем?
46. Как организуется резервное копирование данных в облачных хранилищах?
47. Какую роль играют облачные технологии в обеспечении надежности и безопасности данных?
48. Какие методы предотвращения инцидентов используются в отказоустойчивых системах?
49. Как методы отказоустойчивого программирования могут помочь при внешних атаках на систему?
50. В чем заключаются основные преимущества отказоустойчивого программирования для современного бизнеса?

Практико-ориентированные задания к зачету

1. Разработать программу, которая обрабатывает различные исключения (например, деление на ноль, неверный ввод данных). Реализовать механизм логирования всех ошибок и предусмотреть самовосстановление программы после каждого сбоя.
2. Написать скрипт для создания регулярных резервных копий файловой системы. Программа должна сохранять копии в указанную директорию и уведомлять пользователя об успешном завершении или ошибках копирования.

3. Настроить кластер из нескольких виртуальных машин с балансировщиком нагрузки. Проверить распределение запросов и протестировать работу системы при отказе одного из узлов.
4. Создать простую базу данных, внести данные и выполнить «случайное» удаление данных. Затем использовать резервную копию для восстановления информации и подготовить отчёт о ходе восстановления.
5. Настроить мониторинг для отслеживания загрузки CPU и памяти сервера. Сконфигурировать систему так, чтобы она отправляла уведомления при достижении критических значений.
6. Используя Docker, создать несколько контейнеров с приложением и запустить их в системе оркестрации (например, Docker Swarm или Kubernetes). Проверить распределение нагрузки и поведение системы при отказе одного из контейнеров.
7. Написать скрипт или настроить систему, которая автоматически перезапускает приложение, если оно завершает работу с ошибкой. Проверить, что приложение возобновляет работу после сбоев.
8. Написать программу, которая создает контрольную сумму для файла, а затем проверяет ее при каждом запуске программы, чтобы гарантировать отсутствие изменений в файле.
9. Настроить базу данных с репликацией данных между двумя узлами. Протестировать синхронизацию данных между узлами и восстановление работы системы после отказа одного из узлов.
10. С помощью средств нагрузочного тестирования (например, Apache JMeter или Locust) создать сценарии для проверки устойчивости системы к нагрузкам. Провести тестирование и оценить, как система справляется с резким увеличением числа запросов.

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

1. Чем отказоустойчивое программирование отличается от стандартного подхода к разработке?
2. Как отказоустойчивость влияет на пользовательский опыт?
3. Какие элементы архитектуры могут стать точками отказа?
4. Как определяется уровень отказоустойчивости для конкретной системы?
5. Какие инструменты могут помочь в проектировании отказоустойчивых систем?
6. Каковы основные причины сбоев в программных системах?
7. Как правильное проектирование API помогает улучшить отказоустойчивость?
8. Какие проблемы могут возникать при добавлении отказоустойчивости в существующую систему?
9. В чем разница между планируемым и непланируемым простоем системы?
10. Как нагрузочные тесты помогают выявить потенциальные проблемы отказоустойчивости?
11. Какова роль DevOps-практик в создании отказоустойчивых систем?
12. Как CI/CD-процессы способствуют надежности и отказоустойчивости?
13. Какие существуют подходы к модульному тестированию в целях повышения отказоустойчивости?
14. Какие типы нагрузок наиболее опасны для отказоустойчивости?
15. Как горизонтальное и вертикальное масштабирование влияют на отказоустойчивость?
16. Что такое отказоустойчивость к "сплит-мозгу" в кластерных системах?
17. В чем особенности избыточности данных для файловых систем и баз данных?
18. Как проверяется надёжность резервных копий?
19. Почему обработка ошибок важна в распределённых системах?
20. Какие инструменты используют для имитации сбоев при тестировании?
21. Как происходит миграция данных в отказоустойчивых системах?
22. Как проверяется целостность данных при репликации?
23. В чем заключается принцип "принятия отказов" (failure acceptance)?
24. Что такое «горячее» и «холодное» резервное копирование?
25. Какие риски несет использование устаревшего оборудования для отказоустойчивых систем?
26. Как обеспечить целостность данных в условиях постоянного обновления?
27. Какие методы применяются для защиты данных от случайной потери или порчи?
28. Как действует метод двойной записи данных?
29. Как обеспечивается устойчивость базы данных при внезапных отключениях?
30. Какие угрозы целостности данных можно предотвратить с помощью кодирования?
31. Что такое контроль целостности на основе хешей и как его применяют?
32. Как работают избыточные блоки данных в отказоустойчивых файловых системах?
33. Что такое управление версиями и как оно помогает в восстановлении данных?
34. Как конфиденциальность и отказоустойчивость связаны между собой?
35. Какие методы мониторинга данных помогают обнаружить сбои?
36. Как анализ логов помогает в улучшении отказоустойчивости?
37. Какие механизмы резервного копирования наиболее эффективны для минимизации потерь?
38. Почему важно тестировать процесс восстановления данных?
39. Какова роль самовосстанавливающихся алгоритмов в кибербезопасности?
40. Как работает система автоматического перезапуска процессов при сбоях?
41. Почему необходимо постоянно обновлять системы мониторинга?
42. Какие бывают уровни защиты целостности данных?
43. Какова разница между самовосстанавливающейся системой и системой с отказоустойчивостью?
44. Какие риски несет высокая сложность архитектуры системы в плане отказоустойчивости?
45. В чем разница между высокой доступностью и аварийным восстановлением?
46. Что такое failover и как он применяется в отказоустойчивых системах?
47. Какие ограничения существуют для архитектур с высокой доступностью?
48. Как отказоустойчивость влияет на требования к масштабированию системы?
49. В чем преимущества контейнеризации для отказоустойчивых систем?
50. Какие параметры системы наиболее важны для обеспечения отказоустойчивости?

Критерии оценивания*:*

Максимальное количество баллов, которые обучающийся может набрать – 20 баллов (за 20 ответов).
Ответ на вопрос оценивается:
– 1 балл – правильный и полный ответ;
– 0 баллов – неправильный ответ или ответ не представлен.

Лабораторные задания

Лабораторная работа 1: Тестирование надежности программного обеспечения
Цель: Ознакомиться с методами юнит-тестирования и интеграционного тестирования для проверки надежности ПО.
Описание: Студенты разрабатывают тесты для базовых функций программного модуля и анализируют результаты с целью выявления слабых мест, которые могут привести к отказам.

Лабораторная работа 2: Создание системы с высокой доступностью
Цель: Научиться применять принципы архитектуры с высокой доступностью и устойчивостью к сбоям.
Описание: Студенты настраивают кластеры с дублированием баз данных или файловых систем и тестируют их поведение при симуляции сбоев.

Лабораторная работа 3: Обработка исключений и восстановление после ошибок
Цель: Изучить механизмы обработки исключений и способы восстановления ПО после сбоев.
Описание: Студенты пишут программу, содержащую несколько типов ошибок, и добавляют обработку исключений для минимизации последствий отказов. Также проводится симуляция самовосстановления.

Лабораторная работа 4: Резервное копирование и восстановление данных
Цель: Изучить стратегии резервного копирования и восстановления данных.
Описание: Студенты реализуют сценарий создания резервных копий базы данных, тестируют процесс восстановления и оценивают его скорость и эффективность.

Критерии оценивания:
Максимальное количество баллов, которые обучающийся может набрать – 80 баллов (за 4 заданий).
Каждое задание оценивается:
– 20 баллов. – задание выполнено верно;
– 19-11 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
– 10-6 баллов. – при выполнении задания были допущены ошибки;
– 5- 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 лабораторной работы;

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.