МИНОБРНАУКИ РОССИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ВГУ»)**

**УТВЕРЖДАЮ**

И.о. заведующего кафедрой
математического анализа
Шабров С.А.

01.07.2021

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.04 Анализ защищенности информационных систем

**1. Код и наименование направления подготовки/специальности:**

10.05.04 Информационно-аналитические системы безопасности

**2. Профиль подготовки/специализация:** "Автоматизация информационно-аналитической деятельности", "Информационная безопасность финансовых и экономических структур"

**3. Квалификация выпускника:** специалист по защите информации

**4. Форма обучения:** очная

**5. Кафедра, отвечающая за реализацию дисциплины:** математического анализа

**6. Составители программы:** Бахтина Ж.И., к. ф.-м. н, доцент

---

**7. Рекомендована:** Научно-методическим советом математического факультета
протокол от 29.06.2021 № 0500-07

**8. Учебный год:** 2024-2025 **Семестр(ы):** 8

**9.Цели и задачи учебной дисциплины**

Целями изучения дисциплины «Анализ защищенности информационных систем» являются формирование у обучаемых знаний, умений и навыков (уровня сформированности соответствующих компетенций) в результате последовательного

изучения содержательно связанных между собой разделов (тем) учебных занятий, а также изучение теоретических основ и методов оценки и анализа надежности и безопасности информационных систем с учетом их специфики при управлении их деятельностью.
Задачами изучения дисциплины «Анализ защищенности информационных систем» является ознакомление студентов с приемами и инструментами, применяемыми при защите информационных систем.

## 10. Место учебной дисциплины в структуре ООП:

Для успешного освоения дисциплины необходимы знания по курсам математического анализа, информатики, основ информационной безопасности, баз данных, методов анализа данных, экономической безопасности, макростатистического анализа.

Данная дисциплина является предшествующей для дисциплин: Безопасность программного обеспечения, Специальные технологии баз данных и информационных систем, Основы финансового расследования, Расследование инцидентов информационной безопасности и правонарушений в компьютерной сфере.

## 11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

| Код | Название компетенции | Код(ы) | Индикатор(ы) | Планируемые результаты обучения |
|---|---|---|---|---|
| ПК-2.1 | Способен анализировать безопасность информации с помощью формальных моделей | | Может анализировать безопасность информации с помощью формальных моделей | Знать: основы информационной безопасности и защиты информации;<br>Уметь: осуществлять математическую и информационную постановку задач по обработке информации, использовать алгоритмы обработки информации для различных приложений; проводить предпроектное обследование объекта проектирования, системный анализ предметной области, их взаимосвязей, проводить выбор исходных данных для проектирования ИС и БД,<br>Владеть: методами и средствами представления данных и знаний о предметной области, методами и средствами анализа информационных систем, технологиями реализации, внедрения проекта информационной системы; методами и средствами проектирования, модернизации и модификации информационных систем; |
| ПК-2.3 | Способен анализировать защищенность информационных систем | | Может анализировать защищенность информационных систем | Знать: типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; основные понятия надежности информационных систем; количественные характеристики надежности невосстанавливаемых и восстанавливаемых изделий; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; основные понятия надежности информационных систем; количественные характеристики надежности невосстанавливаемых и восстанавливаемых изделий; законы распределения, |

| | | | | |
|---|---|---|---|---|
| | | | | используемые в исследованиях и расчетах надежности; методы статистической оценки надежности изделий в условиях эксплуатации; методику построения структурных моделей надежности и ее расчета; методику разработки требований к надежности ИС и БД;<br>Уметь: адаптировать приложения к изменяющимся условиям функционирования; реализовывать основные этапы построения ИС, БД и сетей на основе принципов создания надежных и безопасных систем;<br>Владеть: навыками решения конкретных задач по расчетам надежности ИС и БД |

**12. Объем дисциплины в зачетных единицах/час.**(*в соответствии с учебным планом)* — 5/180.

**Форма промежуточной аттестации***(зачет/экзамен)* экзамен

## 13. Трудоемкость по видам учебной работы

| Вид учебной работы | | Трудоемкость | | | |
|---|---|---|---|---|---|
| | | Всего | По семестрам | | |
| | | | 8 | № семестра | … |
| Аудиторные занятия | | 96 | 96 | | |
| в том числе: | лекции | 48 | 48 | | |
| | практические | | | | |
| | лабораторные | 48 | 48 | | |
| Самостоятельная работа | | 48 | 48 | | |
| в том числе: курсовая работа (проект) | | | | | |
| Форма промежуточной аттестации *(экзамен – __час.)* | | 36 | 36 | | |
| Итого: | | 180 | 180 | | |

### 13.1. Содержание дисциплины

| п/п | Наименование раздела дисциплины | Содержание раздела дисциплины | Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК * |
|---|---|---|---|
| **1. Лекции** | | | |
| 1.1 | Понятие защищенности ИС | Понятие защищенности автоматизированной системы. Нормативная база. Методика анализа защищенности. Исходные данные обследуемой ИС. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности. Средства анализа параметров защиты. Классификация методов анализа параметров защиты (Security Benchmarks). Спецификации Security Benchmarks. Спецификации первого уровня для базового (минимального) уровня защиты. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности. | |
| 1.2 | Средства анализа защищенности | Уязвимости уровня операционной системы. Методика поиска уязвимостей | |

| | | | |
|---|---|---|---|
| | операционных систем и приложений. | проектирования программного обеспечения: неустановленные обновления (patch'и и hotfix'ы) операционной системы, уязвимые сервисы и незащищенные конфигурации по умолчанию. Методика поиска уязвимостей, связанных с действиями администратора: неправильно используемые настройки и функции системы, не отвечающие политике безопасности требования, несанкционированные изменения в конфигурации системы. Методика поиска уязвимостей, связанных с деятельностью пользователя | |
| 1.3 | Средства анализа защищенности сетевых сервисов | Уязвимости сетевых протоколов, служб, сервисов. Классификация средств анализа защищенности сетевых сервисов. Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС. Функции, методика использования. ТСредства анализа защищённости СУБД. Анализ уязвимостей СУБД. Классификация систем анализа защищенности СУБД. Система Database Scanner. Средство SQLMap. | |
| 1.4 | Средства анализа защищенности web-приложений | Анализ и классификация уязвимостей web-приложений. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC). Комплексная оценка защищенности web приложения. Принцип «черного ящика» Принцип «серого ящика». Принцип «белого ящика». Инструментальные средства анализа защищенности web-приложения. | |
| **2. Лабораторные занятия** | | | |
| 2.1 | Понятие информационной безопасности. | Основные составляющие. Важность проблемы. Наиболее распространенные угрозы. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности. | |
| 2.2 | Надежность информационных систем. | Создание проекта надежной ИС. | |
| 2.3 | Надежность информационных систем. | Проектирование надежного ПО. | |
| 2.4 | Надежность информационных систем. | Устойчивость к ошибкам. | |
| 2.5 | Надежность информационных систем. | Надежность при предаче данных. | |
| 2.6 | Надежность информационных систем. | Надежность при хранении данных. | |
| 2.7 | Надежность информационных систем. | Проверка на надежность ИС. | |
| 2.8 | Распространение объектно-ориентированного подхода на информационную безопасность. Административный уровень информационной безопасности. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности. | Распространение объектно-ориентированного подхода на информационную безопасность. Административный уровень информационной безопасности. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности. | |
| 2.9 | Идентификация и аутентификация, | Идентификация и аутентификация, управление доступом. Протоколирование и аудит, | |

| | | | |
|---|---|---|---|
| | управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление. | шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление. | |
| 2.10 | Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире. Модель угроз и принципы обеспечения безопасности программного обеспечения. | Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире. Модель угроз и принципы обеспечения безопасности программного обеспечения. | |
| 2.11 | Обеспечение технологической безопасности программного обеспечения. Обеспечение эксплуатационной безопасности программного обеспечения. | Обеспечение технологической безопасности программного обеспечения. Обеспечение эксплуатационной безопасности программного обеспечения. | |
| 2.12 | Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Безопасность программного обеспечения и человеческий фактор. Психология программирования. | Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Безопасность программного обеспечения и человеческий фактор. Психология программирования. | |

### 13.2. Темы (разделы) дисциплины и виды занятий

| № п/п | Наименование темы (раздела) дисциплины | Виды занятий (количество часов) | | | | |
|---|---|---|---|---|---|---|
| | | Лекции | Практические | Лабораторные | Самостоятельная работа | Всего |
| 1 | Понятие защищенности ИС | 6 | | | 2 | 8 |
| 2 | Средства анализа защищенности операционных систем и приложений. | 12 | | | 2 | 14 |
| 3 | Средства анализа защищенности сетевых сервисов | 14 | | | 2 | 16 |
| 4 | Средства анализа защищенности web-приложений | 16 | | | 2 | 18 |
| 5 | Понятие | | | 2 | 4 | 6 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | информационной безопасности. | | | | | |
| 6 | Надежность информационных систем. | | | 24 | 12 | 36 |
| 7 | Распространение объектно-ориентированного подхода на информационную безопасность. Административный уровень информационной безопасности. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности. | | | 4 | 4 | 8 |
| 8 | Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление. | | | 4 | 4 | 4 |
| 9 | Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире. Модель угроз и принципы обеспечения безопасности программного обеспечения. | | | 4 | 4 | 4 |
| 10 | Обеспечение технологической безопасности программного обеспечения. Обеспечение эксплуатационной безопасности программного обеспечения. | | | 6 | 8 | 14 |
| 11 | Стандарты и другие нормативные документы, регламентирующие защищенность программного | | | 4 | 4 | 8 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | обеспечения и обрабатываемой информации. Безопасность программного обеспечения и человеческий фактор. Психология программирования. | | | | | |
| | Итого: | | 48 | 48 | 48 | 144 |

**14. Методические указания для обучающихся по освоению дисциплины**

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся.

*Методические указания к лекционным занятиям*

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

*Методические рекомендации студентам к лабораторным занятиям*

Важной составной частью учебного процесса в вузе являются лабораторные занятия. Они требуют помимо знаний теоретического материала еще и навыков решения практических задач, и помогают студентам глубже усвоить учебный материал, приобрести практические навыки и навыки творческой работы над учебной и научной литературой.

В начале лабораторного занятия происходит обсуждение задач, решенных студентами самостоятельно дома. Это возможность для студентов еще раз обратить внимание на не непонятные до сих пор моменты и окончательно разобрать их. Преподаватель может (выборочно) проверить записи с самостоятельно решенными задачами.

Затем начинается опрос по теме, обозначенной для данного занятия. В процессе этого опроса студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия.

Затем приступают к выполнению лабораторных работ, используя изученные теоретические положения.

*Методические рекомендации студентам к самостоятельной работе*

Среди основных видов самостоятельной работы студентов выделяют следующие: подготовка к лекциям, семинарским и практическим занятиям, зачетам и экзаменам, презентациям и докладам; написание рефератов, выполнение лабораторных и контрольных работ, участие в научной работе. Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности и уровня умений студентов.

Студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому

усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

Курс дисциплины построен таким образом, чтобы позволить студентам максимально проявить способность к самостоятельной работе. Для успешной самостоятельной работы предполагается тесный контакт с преподавателем.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

| № п/п | Источник |
|---|---|
| 1 | Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с. https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| 2 | Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099 |
| 3 | Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 |
| 4 | Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов. Москва: УМЦ по образован ию на железнодорожном транспорте, 2014 https://docplayer.com/59774640-Informacionnaya-bezopasnost-i-zashchita-informacii-na-zheleznodorozhnom-transporte.html |
| 5 | Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 2. Программно- аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов. Москва: УМЦ по образованию на железнодорожном транспорте, 2014 https://docplayer.com/59717425-Informacionnaya-bezopasnost-i-zashchita-informacii-na-zheleznodorozhnom-transporte.html |

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

| № п/п | Ресурс |
|---|---|
| 1. | http://www.lib.vsu.ru –официальный сайт библиотеки ВГУ |
| 2. | http://www.math.vsu.ru – официальный сайт математического факультета ВГУ |
| 3. | База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru |
| 4. | База данных «Библиотека программиста» https://proglib.io/ |
| 5. | База данных «Отраслевой портал специалистов» http://www.connect-wit.ru/ |
| 6. | База данных «Техническая литература» http://booktech.ru/journals/vestnik-mashinostroeniya |

## 16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных), курсовых работ и др.)*

| № п/п | Источник |
|---|---|
| 1 | Учебное пособие Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов на Дону: Феникс, 2010. - 324 с. |

| | |
|---|---|
| | http://library.lgaki.info:404/2017/%D0%93%D0%B0%D1%84%D0%BD%D0%B5%D1%80%20%D0%92_%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD_pdf.pdf |

**17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):**

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ».

**18. Материально-техническое обеспечение дисциплины:**

1. Учебные аудитории для проведения занятий лекционного типа, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование для предоставления учебной информации большой аудитории и/или звукоусиливающее оборудование (стационарное или переносное).
2. Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование и/или звукоусиливающее оборудование (стационарное или переносное)
3. Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.
4. Помещения для хранения и профилактического обслуживания учебного оборудования.

**19. Оценочные средства для проведения текущей и промежуточной аттестаций**

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

| № п/п | Наименование раздела дисциплины (модуля) | Компетенция(и) | Индикатор(ы) достижения компетенции | Оценочные средства |
|---|---|---|---|---|
| 1 | Понятие защищенности ИС | ПК 2.1, ПК 2.3 | Может анализировать безопасность информации с помощью формальных моделей<br><br>Может анализировать защищенность информационных систем | Лабораторные работы |
| 2 | Средства анализа защищенности операционных систем и приложений. | | | |
| 3 | Средства анализа защищенности сетевых сервисов. | | | |
| 4 | Средства анализа защищенности web-приложений | | | |
| 5 | Понятие информационной безопасности. | | | |
| 6 | Надежность информационных систем. | | | |
| 7 | Распространение объектно- | | | |

| № п/п | Наименование раздела дисциплины (модуля) | Компетенция(и) | Индикатор(ы) достижения компетенции | Оценочные средства |
|---|---|---|---|---|
| | ориентированного подхода на информационную безопасность. Административный уровень информационной безопасности. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности. | | | |
| 8 | Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление. | | | |
| 9 | Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире. Модель угроз и принципы обеспечения безопасности программного обеспечения. | | | |
| 10 | Обеспечение технологической безопасности программного обеспечения. Обеспечение эксплуатационной безопасности программного обеспечения. | | | |
| 11 | Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. | | | |

| № п/п | Наименование раздела дисциплины (модуля) | Компетенция(и) | Индикатор(ы) достижения компетенции | Оценочные средства |
|---|---|---|---|---|
| | Безопасность программного обеспечения и человеческий фактор. Психология программирования. | | | |
| Промежуточная аттестация форма контроля - экзамен | | | | Комплект КИМ |

## 20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

### 20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: Лабораторные работы.

Лабораторные работы по учебной дисциплине имеют своей целью:

- закрепление, углубление и расширение теоретических знаний студентов в процессе решения конкретных задач по расчетам надежности ИС;
- развитие у студентов профессиональных навыков, а также практическое овладение методами расчета надежности сложных информационных систем;
- закрепление умений и навыков использования систем автоматизированного решения математических задач.

Выполнению работы предшествует опрос по теории работы и устное собеседование по методике ее выполнения.

Каждая работа оформляется студентом в виде отчета, который обязательно включает раздел, где анализируется и объясняется вся полученная информация.

Итогом работы является ее защита. Защита проводится устно, но обязательно индивидуально.

Пример лабораторной работы по теме «Надежность информационных систем»

Расчет надежности ИС с использованием аналитической модели с дискретным увеличением времени наработки на отказ.

**Цель работы**: практическое освоение метода расчета надежности на основе использования модели с дискретным увеличением времени наработки на отказ.

**Предмет и содержание работы**. Модель надежности программ с дискретным увеличением времени наработки на отказ основана на предположении, что устранение ошибки приводит к увеличению времени наработки на отказ на некоторую случайную величину.

$$T_m = \frac{m(m+1)}{2} M[\Delta T],$$

где $T_m$ – время наработки на отказ до возникновения $m$-го отказа;

$M[\Delta T]$ – математическое ожидание времени между двумя отказами;

$$M[\Delta T] = \sum_{i=1}^{m} t_i \Big/ m \quad .$$

Для того чтобы подсчитать, какое время тестирования необходимо для обеспечения некоторой наработки на отказ, нужно сначала определить математическое ожидание времени между двумя отказами по существующим данным. Далее надо

последовательно высчитывать по формуле время наработки на отказ до тех пор, пока оно не достигнет нужного значения. Просчитанные данные лучше заносить в таблицу. После достижения нужного значения все времена нужно сложить, получив в результате искомое время тестирования.

**Задание**: определить время тестирования, необходимое для достижения указанного времени наработки на отказ. Исходные данные: время первого отказа, время второго отказа, время наработки на отказ.

**Оборудование, технические средства, инструмент**: рабочая станция с установленной ОС, подключенная к Интернету, обозреватель Интернета (для доступа к Wolfram Alpfa), MicroSoft Word (текстовый процессор Open Office). В случае отсутствия доступа в Интернет задача может быть решена непосредственно на рабочей станции путем использования возможностей доступной на ней системы программирования.

**Порядок (последовательность) выполнения работы:** включение рабочей станции; проверка наличия связи с Интернетом; установление связи с Wolfram Alpfa, выбор исходных данных для решения задачи, разработка алгоритма решения задачи, решение поставленной задачи, подготовка данных для отчета, сохранение этих данных, выключение компьютера.

**Контрольные вопросы**

1. Понятие надежности ИС.
2. Краткая характеристика аналитических моделей надежности.
3. Особенности аналитической модели с дискретным увеличением времени наработкина отказ.

**Задания**

1. Изучить свойства надежности ИС.
2. Изучить классификацию моделей надежности ИС.
3. Изучить особенности модели надежности программ с дискретным увеличением времени наработки на отказ.
4. Определить время тестирования, необходимое для достижения указанного времени наработки на отказ. Исходные данные: время первого отказа, время второго отказа, время наработки на отказ.
5. Подготовить данные для отчета.

Оценка «отлично»: правильно выполнены все задания лабораторной работы, правильно даны ответы на все вопросы, работа выполнена своевременно.
Оценка «хорошо»: правильно выполнены все задания работы, правильно даны ответы на большую часть вопросов, работа выполнена своевременно, либо в случае своевременно выполненной работы, но с наличием несущественных ошибок в выполнении заданий и/или ответах на вопросы, не противоречащих основным понятиям дисциплины.
Оценка «удовлетворительно»: выполнены не все, но более 50% заданий работы, дан ответ на часть вопросов, имеются несущественные ошибки в выполнении заданий и/или ответах на вопросы, не противоречащие основным понятиям дисциплины, несвоевременно выполнена работа.
Оценка «неудовлетворительно»: выполнено менее 50% заданий практической части работы, не даны ответы на вопросы, имеются грубые ошибки в выполнении заданий и/или ответах на вопросы, противоречащие или искажающие основные понятия дисциплины, отчет о выполнении работы не предоставлен.

### 20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: Собеседование по экзаменационным билетам.

Перечень вопросов к экзамену:

1. Понятие защищенности ИС
2. Средства анализа защищенности операционных систем и приложений.
3. Средства анализа защищенности сетевых сервисов.
4. Средства анализа защищенности web-приложений
5. Понятие информационной безопасности.
6. Надежность информационных систем.
7. Распространение объектно-ориентированного подхода на информационную безопасность. Административный уровень информационной безопасности.
8. Законодательный уровень информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Идентификация и аутентификация, управление доступом.
11. Протоколирование и аудит, шифрование, контроль целостности.
12. Экранирование, анализ защищенности.
13. Обеспечение высокой доступности.
14. Туннелирование и управление.
15. Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире.
16. Модель угроз и принципы обеспечения безопасности программного обеспечения.
17. Обеспечение технологической безопасности программного обеспечения.
18. Обеспечение эксплуатационной безопасности программного обеспечения.
19. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.
20. Безопасность программного обеспечения и человеческий фактор.
21. Психология программирования.

Примеры задач:

1. Вероятность безотказной работы автоматической линии изготовления цилиндров автомобильного двигателя в течении 120 часов равна 0.9. Предполагается, что справедлив экспоненциальный закон надежности. Требуется рассчитать интенсивность отказов и частоту отказов линии для момента времени t =120 часов, а также среднее время безотказной работы.

2. Среднее время безотказной работы автоматической системы управления равно 640 час. Предполагается, что справедлив экспоненциальный закон надежности. Необходимо определить вероятность безотказной работы в течение 120 час., частоту отказов для момента времени t=120 часов и интенсивность отказов.

3. Невосстанавливаемая в процессе работы электронная машина состоит из 200000 элементов, средняя интенсивность отказов которых $\lambda ср = 0{,}2 \cdot 10^{-6}$ 1/час. Требуется определить вероятность безотказной работы электронной машины в течении t = 24 часа и среднее время безотказной работы электронной машины.