**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**
**(РУТ (МИИТ)**

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Обеспечение надёжности и безопасности информационных систем

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Автоматизированные системы обработки информации и управления

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 5665
Подписал: заведующий кафедрой Нутович Вероника Евгеньевна
Дата: 02.06.2021

1. Общие сведения о дисциплине (модуле).

Проблема дисциплины "Обеспечение надёжности и безопасности информационных систем" является комплексной, системотехнической. Производственный опыт и теоретические исследования свидетельствуют, что нельзя добиться значительного увеличения надёжности отдельными разрозненными мероприятиями. Совместное проведение многих мероприятий объединенных в систему не только увеличивает эффективность каждого из них, но и даёт возможность получить качественно новые результаты.

Надёжность ИС определяется надёжностью её элементов и аппаратуры, надёжностью программного обеспечения, управляющего выполнением вычислительного процесса, а также использованием средств контроля и восстановления системы. Пользователя компьютерной техники интересует только получение правильных результатов вычислений за заданное время. Для достижения этой цели необходимо, чтобы все названные составляющие обладали необходимой надёжностью. Для разработки эффективной системы мероприятий по обеспечению надёжности ИС нужно ясное понимание студентами идей, лежащих в основе многих различных методов оценки и повышения надёжности, позволяющее им оценить возможности и особенности применения этих методов.

Цель дисциплины «Обеспечение надёжности и безопасности информационных систем» – освещение вопросов, связанных с обеспечением высокой надёжности и эффективной безопасности информационных систем. В лекциях изложены вопросы оценки и расчёта надёжности аппаратурных и программных средств ИС на основе статистических, структурных и эксплуатационных моделей, вопросы надёжности ПО, надежность ОУС, задачи оптимального резервирования ИС, ознакомление с основными типами угроз и атак, изучение механизмов защиты административного интерфейса и разграничения прав доступа, изучение технологии и принципов AAA, изучение способов защиты информации в сетях, изучение принципов построения виртуальных частных сетей.

Данный курс базируется на знаниях общих и профилирующих дисциплин: математическая логика позволяет представить сложные логические зависимости между состояниями системы и её комплектующих частей, теория вероятностей, математическая статистика и теория вероятностных процессов дают возможность учитывать случайный характер возникающих в системе событий и процессов, формировать математические основы теории надёжности, теория графов, исследования операций, теория информации, техническая диагностика, теория моделирования, основы

проектирования систем и технологических процессов позволяют обоснованно решать задачи надёжности.

Основной целью изучения учебной дисциплины "Обеспечение надёжности и безопасности информационных систем" является формирование у обучающегося компетенций в области основ теории надежности и безопасности ИС, в применении к информационным системам и информационным услугам, для научно-исследовательской и проектной деятельности.

Основной целью изучения учебной дисциплины является формирование у обучающегося компетенций в области надежности информационных систем и защиты информации, необходимых при эксплуатации, техническом обслуживании, проектировании, производстве, испытаниях, модернизации технических и программных средств железнодорожного транспорта для следующих видов деятельности:

- научно-исследовательской;

-проектно-конструкторской.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

проектно-конструкторская деятельность:

- разработки технических требований, технических заданий и технических условий на проекты систем защиты информации с использованием средств автоматизации и информационных технологий;

- создание (модификация) и сопровождение информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы в организациях различных форм собственности с целью повышения эффективности деятельности организаций и пользователей информационных систем.

научно-исследовательская деятельность:

- научных исследований в области эксплуатации и производства систем информационной безопасности железнодорожного транспорта, интерпретации и вероятностного моделирования отказов систем защиты с формулировкой аргументированных умозаключений и выводов; поиска и проверки новых технических и программных решений по совершенствованию этих систем; разработки планов, программ и методик проведения исследований уровня защищенности, анализ их результатов.

## 2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

**ОПК-1** - Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;

**ОПК-3** - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

**ПК-5** - Способен оценивать показатели качества автоматизированной системы в целом, в том числе путем проведения тестирования и исследование результатов;

**ПК-8** - Способен проводить предпроектное обследование объекта проектирования, системный анализ предметной области, формировать требования к объекту проектирования.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

**Уметь:**

-корректно применять математические методы и модели расчета показателей надежности;

-обосновывать выбор показателей надежности для конкретных объектов и моделей для их расчета;

-корректно применять математические методы и модели расчета показателей надежности;

-устанавливать права доступа к файлам и папкам; анализировать входные данные.

**Знать:**

-основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основы системного администрирования;

-устройство и функционирование современных информационных систем;

-современные стандарты информационного взаимодействия систем;

-программные средства и платформы инфраструктуры информационных технологий организаций; основы информационной безопасности организации.

**Владеть:**

-основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации; - определением базовых элементов конфигурации информаионных систем;

планированием аудитов конфигураций информаионных систем.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

| Тип учебных занятий | Количество часов | | |
|---|---|---|---|
| | Всего | Семестр | |
| | | №6 | №7 |
| Контактная работа при проведении учебных занятий (всего): | 120 | 56 | 64 |
| В том числе: | | | |
| Занятия лекционного типа | 60 | 28 | 32 |
| Занятия семинарского типа | 60 | 28 | 32 |

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 96 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| 1 | Основные понятия надежности информационных систем (ИС) и пути её обеспечения.<br>Основные понятия надежности информационных систем (ИС) и пути её обеспечения.<br>Показатели надежности невосстанавливаемых ИС.<br>Показатели надежности восстанавливаемых устройств технических объектов ИС. Зависимость надёжности от времени. |
| 2 | Показатели надежности невосстанавливаемых ИС.<br>Методика оценки безотказности нерезервированных систем.<br>Надежность невосстанавливаемых и нерезервированных ИС.<br>Структурное резервирование и его виды. |
| 3 | Показатели надежности восстанавливаемых устройств технических объектов ИС. Зависимость надёжности от времени.<br>Расчет характеристик надежности невосстанавливаемых резервированных систем.<br>Надежность резервированных устройств с последовательно-параллельной структурой (метод свертки). |
| 4 | Методика оценки безотказности нерезервированных систем. |
| 5 | Надежность невосстанавливаемых и нерезервированных ИС. |
| 6 | Структурное резервирование и его виды. |
| 7 | Расчет характеристик надежности невосстанавливаемых резервированных систем. |
| 8 | Надежность резервированных устройств с последовательно-параллельной структурой (метод свертки). |
| 9 | Оценка надежности методом путей и сечений. Логико-вероятностные методы анализа сложных систем. |
| 10 | Расчет надежности восстанавливаемых систем (метод дифференциальных уравнений). Расчет надежности восстанавливаемых систем (метод дифференциальных уравнений). |
| 11 | Марковские модели для оценки надежности резервированных восстанавливаемых ИС. |
| 12 | Приближенные методы расчета ИС. |
| 13 | Надежность программного обеспечения ИС. |
| 14 | Методы введения структурной избыточности в программы. |
| 15 | Модели надежности программ. |
| 16 | Надежность отказоустойчивых систем (ОУС). Назначение и свойства ОУС, примеры реализации. |
| 17 | Методы и алгоритмы автоматического восстановления ИС. |
| 18 | Задачи оптимального резервирования ИС. |
| 19 | Основные принципы защиты информации в информационных системах.<br>Основные направления действия системы защиты информации и принципы ее организации. |
| 20 | Политика защиты и сетевая безопасность.<br>Вопросы безопасности сети предприятия, направления действия политики защиты. Примерные варианты реализации политик защиты. Анализ угроз безопасности.<br>Описание типов угроз и общие рекомендации по борьбе с ними. Вирусы.<br>Типы вирусов, среда обитания, способы заражения, вредоносное воздействие. |
| 21 | Защита сети.<br>Защита административного доступа к сетевым устройствам. Вопросы защиты доступа к |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | административным интерфейсам. Методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами.<br>Методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты и принципы AAA.<br>Методы аутентификации и авторизации, технология защиты AAA, принципы ее работы и конфигурирования. |
| 22 | Защита сетевых соединений.<br>Модели обороны. Существующие модели обороны, их преимущества и недостатки.<br>Защита периметра сети.<br>Зонная архитектура защиты сети и ее компоненты.<br>Контроль сервисов TCP/IP.<br>Средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Контроль доступа.<br>Средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, а также настройка средств защиты от синхронных атак. |
| 23 | Шифрование и криптография.<br>Механизмы шифрования.Блочное шифрование и цифровая подпись.<br>Шифрование на сетевом уровне. Носители секретной информации. |
| 24 | Построение виртуальных частных сетей (VPN).<br>Обзор технологии виртуальных частных сетей. Обзор технологии виртуальных частных сетей, их топологий и средств поддержки.<br>Механизмы IPSec.Принципы работы и настройки механизмов IPSec с использованием IKE.<br>Настройка IPSec VPN. |

## 4.2. Занятия семинарского типа.

### Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | КОЛИЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ НАДЕЖНОСТИ.<br>КОЛИЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ НАДЕЖНОСТИ.<br>Показатели и количественные характеристики надежности. |
| 2 | РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ НЕРЕЗЕРВИРОВАННЫХ СИСТЕМ.<br>РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ НЕРЕЗЕРВИРОВАННЫХ СИСТЕМ.<br>Прикидочный расчет показателей надежности.<br>Окончательный (полный) расчет показателей надежности.<br>Ориентировочный расчет показателей надежности. |
| 3 | РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ РЕЗЕРВИРОВАННЫХ СИСТЕМ.<br>РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ РЕЗЕРВИРОВАННЫХ СИСТЕМ.<br>Виды структурного резервирования. |
| 4 | РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ ВОССТАНАВЛИВАЕМЫХ СИСТЕМ.<br>РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ ВОССТАНАВЛИВАЕМЫХ СИСТЕМ.<br>Метод, основанный на использовании классической теории вероятностей.<br>Метод, основанный на использовании теории графов. |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| | Метод преобразованных сетей. |
| 5 | Защита информации в персональном компьютере с помощью стандартных средств ОС Windows 7 и пакета Microsoft Office. |
| 6 | Разработка пользовательского приложения, обеспечивающего авторизацию пользователя. |
| 7 | Шифрование данных путем замены и перестановок. |
| 8 | Шифрование с закрытым ключом. |
| 9 | Алгоритмы шифрования с открытым ключом. |
| 10 | Криптографические методы защиты информации. Электронная цифровая подпись. |
| 11 | ЗИ в телекоммуникационных сетях. Защита периметра сети. |
| 12 | Законодательство в области ИБ. Обеспечение безопасности данных. |
| 13 | Законодательство в области ИБ. Итоговое занятие. |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | Подготовка к практическому занятию: «КОЛИЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ НАДЕЖНОСТИ». |
| 2 | Подготовка к практическому занятию: «РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ НЕРЕЗЕРВИРОВАННЫХ СИСТЕМ». |
| 3 | Подготовка к практическому занятию: «РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ РЕЗЕРВИРОВАННЫХ СИСТЕМ». |
| 4 | Подготовка к практическому занятию: «РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ ВОССТАНАВЛИВАЕМЫХ СИСТЕМ». |
| 5 | Подготовка к промежуточной аттестации (контрольная работа, экзамен). |
| 6 | Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС). Подготовка к контрольной работе. Проработка учебного материала по литературе. |
| 7 | Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз. Проработка учебного материала по литературе. |
| 8 | Криптографические методы защиты информации. . Подготовка к промежуточному контролю по тесту ПК 1. Проработка учебного материала по литературе. |
| 9 | Защищенные виртуальные сети. Проработка учебного материала по литературе. |
| 10 | Подготовка к промежуточной аттестации. |
| 11 | Подготовка к текущему контролю. |

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Управление развитием информационных систем: учебник Васильев Р.Б. Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа , 2020 | Электронно-библиотечная система IPR BOOKS - URL: http://www.iprbookshop.ru/94864.html — Режим доступа: для авторизир. пользователей |
| 2 | Экономика и менеджмент информационных систем: учебник Галиева Н.В. Москва: Издательский Дом МИСиС , 2018 | Электронно-библиотечная система IPR BOOKS -URL: http://www.iprbookshop.ru/84430.html — Режим доступа: для авторизир. пользователей |
| 3 | Управление качеством информационных систем Исаев Г.Н Москва: Инфра-М , 2016 | URL: https://ibooks.ru/bookshelf/361670/reading |
| 4 | Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Издательский центр "Академия", , 2011 | ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ) |
| 5 | Защита программ и данных В.Г. Проскурин Москва Академия 004 П 82 , 2011 | НТБ МИИТ |
| 6 | ГОСТ Р 50922-96 Защита информации. Основные термины и определения http://standartgost.ru/ | НТБ МИИТ |

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

• Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

• Единая коллекция цифровых образовательных ресурсов (http://window.edu.ru);

• Электронно-библиотечная система "Лань" (https://e.lanbook.com);

• Электронно-библиотечная система ibooks.ru (https://ibooks.ru);

• Научно-техническая библиотека РУТ (МИИТ) (http://library.miit.ru).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

• Windows 7, 10 – лицензионное ПО;

• Foxit Reader или Adobe Reader– свободно распространяемое ПО;

• Microsoft Teams - лицензионное ПО;
• Microsoft Office Word, Excel, PowerPoint – лицензионное ПО.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий и самостоятельной работы требуется:

1) рабочее место преподавателя с персональным компьютером.

2) специализированная лекционная аудитория с экраном и компьютером преподавателя, подключенным к проектору.

3) рабочие места студентов в компьютерном классе должны быть оснащены компьютерами, подключёнными к сети Internet и имеющими характеристики не ниже следующих: Intel(R) Core(TM) i3-10100, ОЗУ 8 ГБ, HDD SPCC M.2 PCIe SSD, USB 3.0.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 6 семестре.
Экзамен в 7 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы

| | |
|---|---|
| Профессор, старший научный сотрудник, д.н. кафедры «Системы управления транспортной инфраструктурой» | Ридель Валерий Вольдемарович |
| Доцент, доцент, к.н. кафедры «Цифровые технологии управления транспортными процессами» | Иконников Сергей Евгеньевич |


Лист согласования

| | |
|---|---|
| Заведующий кафедрой ЦТУТП | В.Е. Нутович |
| Председатель учебно-методической комиссии | Н.А. Клычева |