МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Администрирование операционных систем»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 8 зачетных единиц, 288 академических часов.

Форма промежуточной аттестации: зачет (5 семестр), экзамен (6 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Администрирование операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Администрирование операционных систем» является изложение основополагающих принципов администрирования операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Администрирование операционных систем»:

- дать представление об основных задачах администрирования ОС и методах их решения;
- научить использовать встроенные средства ОС для решения задач администрирования ОС.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1.1: способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;

В результате изучения дисциплины студент должен:

знать:

- основные задачи и функции администратора ОС;
- знать типы, версии и редакции ОС Windows, Linux, Unix;
- основные инструментальные средства, применяемые при администрировании ОС Windows, Linux, Unix, включая средства обеспечения безопасности;
- знать основные команды, применяемые при администрировании ОС Windows, Linux, Unix;
- основы разработки сценариев;
- базовые задачи по обеспечению защиты ОС, вычислительных ресурсов ЭВМ и данных.

уметь:

- выполнять установку и конфигурирование ОС Windows, Linux, Unix;
- выполнять задачи по управлению пользователями в ОС Windows, Linux, Unix;
- выполнять задачи по управлению запоминающими устройствами в ОС Windows, Linux, Unix;
- выполнять задачи по ограничению доступа к объектам файловой системы в ОС Windows, Linux, Unix;
- конфигурировать и администрировать основные сетевые службы в ОС Windows, Linux, Unix;
- выполнять резервное копирование и восстановление данных в ОС Windows, Linux, Unix;
- конфигурировать и обслуживать основные сервисы безопасности ОС;
- определять ресурсы, подлежащие защите.

владеть:

- навыками базового администрирования ОС Windows, Linux, Unix;
- навыками работы в командной строке;
- навыками написания и выполнение административных сценариев.

Краткое содержание дисциплины (модуля) Тема
1. Введение в администрирование ОС.
Тема 2. Базовые инструменты администрирования ОС Windows.
Тема 3. Управление локальными пользователями в ОС Windows.
Тема 4. Управление дисковыми ресурсами.
Тема 5. Сетевые параметры в ОС Windows.
Тема 6. Система доменных имен.
Тема 7. Протокол динамической конфигурации хоста.
Тема 8. Настройка файлового сервера под управлением ОС Windows.
Тема 9. Администрирование доменов в сетях Windows.
Тема 10. Настройка удаленного доступа в Windows.
Тема 11. Резервное копирование данных.
Тема 12. Мониторинг работы и контроль производительности ОС Windows.
Тема 13. Автоматизация задач администрирования в ОС Windows. PowerShell.
Тема 14. Общий обзор Unix-like систем. ОС FreeBSD.
Тема 15. Командная строка FreeBSD.
Тема 16. Управление локальными пользователями в ОС FreeBSD.
Тема 17. Управление дисковыми ресурсами, ФС UFS.
Тема 18. Ограничение доступа к файлам и каталогам.
Тема 19. Сетевые параметры в ОС FreeBSD.
Тема 20. Загрузка ОС FreeBSD. Сборка ядра, обновление системы.
Тема 21. Установка программного обеспечения в ОС FreeBSD.
Тема 22. Сервер имен под управлением ОС FreeBSD.
Тема 23. DHCP-сервера под управлением ОС FreeBSD.
Тема 24. Файловый сервер под управлением ОС FreeBSD.
Тема 25. Организация удаленного доступа к серверу под управлением ОС FreeBSD.
Тема 26. Организация резервного копирования и восстановления данных в ОС FreeBSD.
Тема 27. Мониторинг работы и контроль производительности ОС FreeBSD.
Тема 28. Обеспечение отказоустойчивости ОС FreeBSD.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Методы и средства криптографической защиты информации»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 9 зачетных единиц, 324 академических часов.

Форма промежуточной аттестации: экзамен (5, 6 семестр).

Цели и задачи освоения дисциплины (модуля)
Программа дисциплины ориентирована на достижение следующих целей: · приобретение основных знаний о методах криптографических преобразований информации и методах криптоанализа современных шифров; овладение умением чтения российских и зарубежных криптографических стандартов; · воспитание ответственности к профессиональной деятельности, воспитание самообразования; · развитие навыков программной реализации криптографических алгоритмов; · формирование готовности использовать приобретенные знания в профессиональной деятельности.
Исходя из целей, в программе дисциплины «Методы и средства криптографической защиты информации» предусматриваются задачи: · сформировать у обучающегося необходимый объем знаний о принципах разработки шифров и методах их криптоанализа; · научить читать базовые российские и зарубежные криптографические стандарты; · развить навыки программной реализации криптографических алгоритмов; · сформировать умения применять знания о математических методах построения криптографических средств защиты информации на практике.
Планируемые результаты освоения
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОПК-3 - способен использовать необходимые математические методы для решения задач профессиональной деятельности;
ОПК-9 - способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

В результате изучения дисциплины студент должен:
Знать:
- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования;
- основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности;
- внутреннюю структуру криптографических алгоритмов, их область применения и свойства; внутреннее содержание отечественных криптографических стандартов, их характеристики по сравнению с зарубежными.

Уметь:
- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
- читать базовые криптографические стандарты и осуществлять программную реализацию алгоритма;

- самостоятельно реализовать стандартный криптографический алгоритм; применять на практике отечественные и зарубежные стандарты.

Краткое содержание дисциплины (модуля) Дисциплина
включает 10 тем:
Тема 1. Введение в криптографию
Тема 2. История криптографии. Исторические шифры.
Тема 3. Математическая модель шифра. Теория секретности Шеннона.
Тема 4. Блочные шифры
Тема 5. Псевдослучайные последовательности и поточные шифры.
Тема 6. Теория имитостойкости Симмонса и криптографические хэш-функции.
Тема 7. Асимметричные (с открытым ключом) шифры.
Тема 8. Схемы цифровой подписи
Тема 9. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе.
Тема 10. Введение в криптографические протоколы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Научно-проектный (исследовательский) семинар»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 2 зачетных единицы, 72 акад.час.

Форма промежуточной аттестации: зачет (6, 8 семестры).

Цели и задачи освоения дисциплины (модуля)

Основной целью дисциплины является развитие навыков студента для проведения самостоятельной научно-исследовательской работы.

Задачи дисциплины:

- развить навыки поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности;
- научить правилам оформления списка литературных источников;
- навыками проведения научно-исследовательской работы и применения методов научных исследований в профессиональной деятельности;
- развить навыки разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ;
- дать опыт публичной защиты собственного научного труда.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

В результате изучения дисциплины студент должен:

Знать:

- основные научные проблемы в области ИБ;
- правила оформления отчета по курсовой работе;
- правила оформления списка литературы.

Уметь:

- применять методы научных исследований в профессиональной деятельности;
- применять навыки проведения научно-исследовательской работы;
- осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности;
- применять навыки разработки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ.

Краткое содержание дисциплины (модуля) Дисциплина включает 9 тем:
Тема 1. Безопасность БД, угрозы, защита.
Тема 2. Критерии защищенности БД.
Тема 3. Модели безопасности в СУБД.
Тема 4. Средства идентификации и аутентификации.
Тема 5. Средства управления доступом.
Тема 6. Целостность БД и способы ее обеспечения.
Тема 7. Классификация угроз конфиденциальности СУБД.
Тема 8. Аудит и подотчетность.
Тема 9. Транзакции и блокировки.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Операционные системы»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единиц, 144 академических часов.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины

Основной целью дисциплины «Операционные системы» является дать целостное представление об архитектуре современных операционных систем (ОС). Задачи дисциплины «Операционные системы»:

- познакомить с историей развития ОС;
- дать представление об основных функциях, принципах построения и видах ОС;
- дать представление о методах управления основными вычислительными ресурсами ЭВМ;
- дать представление об управлении устройствами вода-вывода;
- познакомить с общими подходами к реализации файловых систем и организацией популярных файловых систем;
- познакомить с архитектурой современных ОС.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-2: способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

В результате изучения дисциплины студент должен:

знать:

- историю развития ОС;
- основные функции ОС, принципы построения ОС, основные архитектурные решения, применяемые при разработке ОС;
- основные подсистемы современных ОС и их назначение;
- принципы управления основными вычислительными ресурсами ЭВМ;
- принципы управления процессами и потоками;
- технологии управления памятью;
- принципы организации ввода-вывода;
- структуру современных файловых систем и технологии распределения дискового пространства;
- принципы организации взаимодействия прикладного ПО с ОС и аппаратным обеспечением;
- архитектуру современных ОС;

уметь:

- применять полученные знания при разработке программного обеспечения (организация взаимоисключающего доступа к критическим ресурсам, методы борьбы с тупиками и пр.);
- получать системную информацию о ресурсах ЭВМ;
- применять полученные знания при администрировании и защите ОС;
- использовать программные методы синхронизации процессов;
- использовать программные методы работы с памятью;
- применять полученные знания к различным предметным областям; владеть:
- базовыми навыками разработки многопоточных приложений;
- приемами программирования, исключающими проблемы синхронизации потоков, взаимоблокировок;
- использования различных механизмов управления памятью при разработке приложений;
- навыками разработки приложений с использованием функций интерфейса прикладного программирования.

Краткое содержание дисциплины

Тема 1. Введение в ОС. Архитектура, функции, принципы построения, классификация ОС.
Тема 2. Управление процессами, алгоритмы планирования.
Тема 3. Синхронизация процессов. Тупики.
Тема 4. Управление памятью.
Тема 5. Организация ввода -вывода в ОС.
Тема 6. Файловая система. Общие положения.
Тема 7. Обзор современных файловых систем.
Тема 8 .ОС семейства Windows NT. Общий обзор, архитектура.
Тема 9. Unix-like системы. Общий обзор, архитектура.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Организационное и правовое обеспечение информационной безопасности»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 3 зачетных единицы, 108 академических часа.

Форма промежуточной аттестации: экзамен (4 семестр).

Цели и задачи освоения дисциплины (модуля)

Целью преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» является раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы.

Задачи дисциплины– дать основы:

- информационного законодательства Российской Федерации;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях;
- построения систем организационной защиты объектов информатизации

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1.4: способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

ОПК-13: способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма

В результате изучения дисциплины студент должен:

знать:

- нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных, их содержание, предмет регулирования и сферу применения;
- основные понятия, термины и определения в области обработки и защиты персональных данных;
- основные угрозы безопасности информации;
- этапы создания системы защиты информации;
- виды защищаемой информации и информационных систем, требования по их защите;
- порядок проведения аттестации объекта информатизации;
- правила разработки технического задания на создание АС в защищенном исполнении;
- правила разработки технического проекта на создание системы защиты информации;
- необходимые для написания документов НПА и ГОСТы;

- порядок внедрения режима коммерческой тайны;
- порядок отнесения сведений к гостайне;
- грифы секретности и уровни допуска к гостайне;
- состав и принципы написания организационно-распорядительной документации по защите информации;
- способы использования и обозначения требований по защите информации в организационно-распорядительной документации;
- существующие базы знаний и информационные системы нормативных правовых актов РФ;
- дополнительные источники получения информации по НПА и защите информации;
- отечественные нормативно-правовые акты, методические документы и стандарты в области защиты информации и защиты информации;
- основные угрозы безопасности информации;
- нормативные и методические документы ФСТЭК России и ФСБ России по моделированию нарушителя и угроз безопасности информации;
- основные угрозы безопасности информации;
- нормативные и методические документы ФСТЭК России и ФСБ России по моделированию нарушителя и угроз безопасности информации;
- основные этапы защиты информации;
- правила формирования политики информационной безопасности; уметь:
- применять нормативные правовые акты Российской Федерации в области обработки и защиты персональных данных для конкретных задач и ситуаций в области защиты информации;
- сформировать перечень требований по защите информационной системы;
- разрабатывать проекты документов Техническое задание и Технический проект на создание системы защиты информации;
- определять порядок и состав действий по внедрению коммерческой тайны;
- разрабатывать проекты организационно-распорядительной документации по защите персональных данных;
- использовать специальные информационные системы, базы знаний и электронные библиотеки для поиска и работы с нормативными правовыми документами;
- использовать средства поиска информации в сети Интернет;
- осуществлять подбор и анализ нормативных правовых документов и информации необходимых для решения конкретных задач по обработке и защите информации;
- построить модель нарушителя и модель угроз информационной безопасности информации;
- определить и спланировать процесс оценки эффективности системы защиты информации;

Краткое содержание дисциплины (модуля)

Тема 1. Законодательство РФ в сфере информационной безопасности
Тема 2. Практика правонарушений в области ИБ
Тема 3. Государственная система защиты информации РФ
Тема 4. Организация режима коммерческой тайны
Тема 5. Защита государственной тайны
Тема 6. Документация в области ИБ
Тема 7. Лицензируемая деятельность в области ИБ
Тема 8. Проектирование системы защиты информации
Тема 9. Аттестация объектов информатизации

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Организация электронно-вычислительных машин и вычислительных систем» Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е., 144 час.
Форма промежуточной аттестации: зачет (3 семестр).
Цели и задачи освоения дисциплины
Цель дисциплины — обучить студентов общим принципам построения и эксплуатации аппаратных средств вычислительной техники и методов ее функционирования в локальных и глобальных вычислительных сетях.
Задачи дисциплины:

- обучение систематизированным представлениям о принципах построения и архитектурных особенностях различных классов электронно-вычислительных машин (ЭВМ);
- изложение основных концепций, представления, хранения и обработки данных в ЭВМ; изучение принципов работы микропроцессорных систем.

Планируемые результаты освоения
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОПК-4: способен применять необходимые физические законы и модели для решения задач профессиональной деятельности.

В результате изучения дисциплины студент должен:
знать:

- основные этапы создания и развития ЭВМ;
- существующие виды архитектур ЭВМ, назначение и функции ее элементов;
- 2-х, 8-ми, 10-ти, 16-ти -ричную арифметики;
- основы теории кодирования данных;
- основы теории построения логических схем;
- организацию и структуру центрального процессора, памяти, системы прерывания, системы ввода вывода;
- организацию системной магистрали, способы подключения дополнительных устройств;
- физические основы и принципы действия периферийных устройств, интерфейсы периферийных устройств;
- основы языка низкого уровня.

уметь:

- формализовать поставленную задачу;
- осуществлять программную реализацию алгоритма;
- разбираться в устройстве рабочих станций, ноутбуков, серверов;

– применять полученные знания к различным предметным областям.

владеть навыками:

изучения компонентов компьютера с помощью инструкций на языке ассемблера; оценки конфигурации вычислительной системы с точки зрения требуемых функциональных возможностей;

оценки программно-аппаратной конфигурации вычислительной системы с точки зрения компьютерной безопасности.

Краткое содержание дисциплины

Дисциплина включает 18 тем

1. История вычислительной техники, поколения и архитектуры ВТ
2. Архитектура и структура ЭВМ
3. Основные элементы и периферийные узлы ЭВМ.
4. Представление данных в ЭВМ.
5. Кодирование данных.
6. Логические основы функционирования ЭВМ.
7. Основы построения цифровых логических цепей, принципы организации памяти
8. Организация микропроцессорной техники.
9. Основы языка ассемблера.
10. Основы операционных и файловых систем семейства Windows.
11. Основы операционных и файловых систем семейства Unix/Linux.
12. Носители и накопители данных. Принципы восстановления данных.
13. Организация и компоненты системной платы ПК. Шины расширения. Интерфейсы.
14. Видео и аудио подсистемы.
15. Стандарты электропитания компьютера.
16. Периферийные устройства ввода/вывода. Сканеры, принтеры, коммуникационные устройства.
17. Ноутбуки и современные мобильные платформы.
18. Сервера, блэйд-системы, системы хранения данных. Многопроцессорные комплексы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Основы информационной безопасности»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 5 зачетных единицы, 180 академических часа.

Форма промежуточной аттестации: экзамен (1 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Основы информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью дисциплины «Основы информационной безопасности» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение основам информационной безопасности, принципам и методам защиты информации в информационных системах.

Задачи дисциплины «Основы информационной безопасности»:

- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в информационных системах;
- изучение типовых угроз безопасности информации при её обработке в информационных системах;
- изучение основных принципов обеспечения информационной безопасности; ● изучение основ построения модели угроз и политики безопасности; ● изучение основных моделей доступа.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1: способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства В результате изучения дисциплины студент должен:

знать:

- основные понятия информационной безопасности;
- важность и необходимость информационной безопасности на человека, организации и государства;
- уровни обеспечения информационной безопасности РФ;
- ответственность за преступления в информационной сфере в соответствии с законодательством РФ;
- основные регуляторы в области информационной безопасности;
- основные термины и определения в области теории информации, информационных технологий и защиты информации;
- основные угрозы информационной безопасности;
- основные методы обеспечения безопасности информационных систем;
- основные методы поиска информации из открытых источников;

- нормативные правовые акты Российской Федерации в области защиты информации, их содержание, предмет регулирования и сферу применения;
- основные методы обеспечения безопасности информационных систем.

уметь:

- оценить возможные последствия противоправных действий в области информационных технологий;
- классифицировать информационные системы;
- классифицировать угрозы безопасности информации;
- применять нормативные правовые акты Российской Федерации в области защиты информации для конкретных задач и ситуаций;
- проводить аудит информационной безопасности;
- использовать результаты аудита для принятия решений в области информационной безопасности.

Краткое содержание дисциплины (модуля)

Тема 1. Основные понятия теории информационной безопасности
Тема 2. Классификация угроз информационной безопасности
Тема 3. Основные механизмы обеспечения информационной безопасности
Тема 4. Теоретический подход к обеспечению информационной безопасности
Тема 5. Нормативно-правовой подход к обеспечению информационной безопасности
Тема 6. Практический (экспериментальный) подход к обеспечению информационной безопасности
Тема 7. Построение модели угроз
Тема 8. Определение и разработка политики безопасности
Тема 9. Аудит информационной безопасности

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Основы построения защищенных баз данных»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единицы, 144 акад.час.

Форма промежуточной аттестации: экзамен (7 семестр).

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Основы построения защищенных баз данных» - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных (СУБД), а также связанных с обеспечением безопасности информации в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД), навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты. Знания, умения и практические навыки, полученные в результате изучения дисциплины «Основы построения защищенных баз данных», используются студентами при разработке курсовых и дипломных работ.

Задачи курса:

- обучить студентов принципам работы современных систем управления базами данных;
- привить студентам навыки проектирования и реализации баз данных;
- приобретение системного подхода к проблеме защиты информации в СУБД;
- изучение моделей и механизмов защиты в СУБД;
- приобретение практических навыков организации защиты БД;
- обучить студентов проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;
- обучить студентов формализовать поставленную задачу по обеспечению защиты БД;
- обучить студентов применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- привить студентам навыки разработки нормативных и организационнораспорядительных документов, регламентирующих работу по защите информации в СУБД.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

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

В результате изучения дисциплины студент должен:

Знать:

- содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;
- нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД;
- основные средства и способы обеспечения информационной безопасности, предоставляемые системами управления базами данных; - принципы построения систем защиты информации.

Уметь:
- самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
- формализовать поставленную задачу;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять действующую законодательную базу в области обеспечения безопасности систем баз данных;
- применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;
- использовать средства защиты, предоставляемые системами управления базами данных;
- проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований.

Краткое содержание дисциплины (модуля) Дисциплина включает 9 тем:
Тема 1. Безопасность БД, угрозы, защита.
Тема 2. Критерии защищенности БД.
Тема 3. Модели безопасности в СУБД.
Тема 4. Средства идентификации и аутентификации.
Тема 5. Средства управления доступом.
Тема 6. Целостность БД и способы ее обеспечения.
Тема 7. Классификация угроз конфиденциальности СУБД.
Тема 8. Аудит и подотчетность.
Тема 9. Транзакции и блокировки.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

«Основы построения защищенных компьютерных сетей»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единицы, 144 акад.час.

Форма промежуточной аттестации: экзамен (7 семестр).

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины "Основы построения защищенных компьютерных сетей" - является изложение основополагающих принципов разработки сетевого программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

Задачи курса - изучение:

- основных принципов разработки сетевых протоколов;
- основных принципов анализа сетевых протоколов;
- принципов разработки сетевых программ и выбора технологии и протокола передачи данных.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях.

В результате изучения дисциплины студент должен:

Знать:

- принципы функционирования протоколов FTP, HTTP, SMTP и POP3, стандартные - команды протоколов;
- назначение, преимущества и недостатки протоколов FTP, HTTP, SMTP и POP3;
- протоколы FTP, HTTP, SMTP и POP3;
- Basic, Digest, NTLM и авторизацию с помощью форм.

Уметь:

- производить основные действия с протоколами FTP, HTTP, SMTP или POP3 программно;
- производить проверку безопасности реализации протоколов FTP, HTTP, SMTP и POP3;
- разрабатывать положения, инструкции и других организационно- распорядительные документы необходимые для обеспечения ИБ при использовании протоколов FTP, HTTP, SMTP и POP3;
- настраивать Basic, Digest, NTLM и авторизацию с помощью форм.

Краткое содержание дисциплины (модуля) Дисциплина включает 9 тем:

Тема 1. Основные понятия.

Тема 2. Протокол HTTP.

Тема 3. Протокол FTP.
Тема 4. Протокол POP3.
Тема 5. Протокол SMTP.
Тема 6. Уязвимости сетевых протоколов.
Тема 7. Обзор современных сетевых протоколов.
Тема 8. Разработка сетевых приложений на базе протокола TCP.
Тема 9. Анонимные и именованные каналы связи.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

«Основы управления информационной безопасностью»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 5 зачетных единицы, 180 академических часа.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Основы управления информационной безопасностью обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель дисциплины «Основы управления информационной безопасностью» - является изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

Задачи дисциплины:

- Формирование требований к системе управления ИБ конкретного объекта.
- Проектирование системы управления ИБ конкретного объекта.
- Эффективное управление ИБ конкретного объекта.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1.4: способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

ОПК-5: способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-10: способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

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

В результате изучения дисциплины студент должен:

знать:

- основные стандарты, регламентирующие управление ИБ;
- основные понятия информационной безопасности;
- принципы разработки процессов управления ИБ;
- подходы к интеграции системы управления ИБ в общую систему управления предприятием;
- основные понятия аппаратных средств вычислительной техники;

- основы операционных систем;
- основы Интернет-технологий;
- основы локально вычислительных сетей;

уметь:

- анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессами управления ИБ;
- определять цели и задачи, решаемые разрабатываемым процессам управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- разрабатывать процессы управления ИБ, учитывающие особенности функционирование предприятия и решаемых им задач, и оценивать их эффективность;
- решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять систему управления ИБ и оценивать ее эффективность;
- формализовать поставленную задачу;
- осуществлять аппаратную реализации состава системы;
- проводить оценку рисков.

Краткое содержание дисциплины (модуля)

Тема 1. Введение. Базовые вопросы управления ИБ. Процессный подход Тема 2. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ.
Тема 3. Рискология ИБ.
Тема 4. Основные процессы СУИБ. Обязательная документация СУИБ Тема 5. Эксплуатация и независимый аудит СУИБ.
Тема 6. Внедрение разработанных процессов. Документ «Положение о применимости» Тема 7. Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведениябизнеса»
Тема 8. Обеспечение соответствия требованиям законодательства РФ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Программно-аппаратные средства защиты информации»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 3 зачетных единиц, 108 академических часа.

Форма промежуточной аттестации: экзамен (7 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Программно-аппаратные средства защиты информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Программно-аппаратные средства защиты информации» является теоретическая и практическая подготовка работе с современными отечественными средствами защиты информации и внедрение их в систему защиты информации.

Для достижения поставленной цели предусмотрены следующие задачи:

- изучить типы и виды средств защиты информации;
- дать представление о существующих отечественных и зарубежных средствах защиты информации;
- научить устанавливать, настраивать и администрировать средства защиты информации;
- научить делать обоснованный выбор средства защиты информации при проектировании системы защиты информации.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-6: способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате изучения дисциплины студент должен:

знать:

- дополнительные источники получения информации по администрированию средств защиты;
- основные угрозы безопасности информации;
- требования к обеспечению ИБ различными техническими мерами;
- принципы работы и основной функционал средств защиты информации;
- порядок сертификации средств защиты информации в РФ;
- варианты и формы сертификации средств защиты информации в РФ;
- виды сертифицируемых средств защиты информации и предъявляемые им требования по безопасности;
- основные типы и виды средств защиты информации, принципы их действия;
- основные модули и функциональные возможности средств защиты информации;
- требования к среде функционирования средства защиты информации;
- принципы функционирования модулей средств защиты информации;

- способы влияния средств защиты информации на программное окружение;
- варианты зависимости работоспособности средств защиты информации от программного окружения;
- основные виды и типы средств защиты информации;
- основной функционал различных видов средств защиты информации;
- требования по обеспечению ИБ для различных ИС;
- правила выбора средств защиты информации в различных ИС;
- отечественные средства защиты информации; уметь:
- находить необходимую дополнительную информацию по средству защиты на сайте компании-производителя;
- сопоставлять реализуемый средствами защиты информации функционал с предъявляемыми требованиями по ИБ;
- определять нейтрализуемые средствами защиты информации угрозы;
- формулировать требования к конфигурированию средств защиты информации;
- выбрать необходимый способ сертификации средства защиты информации;
- составить план сертификации средства безопасности;
- определить состав требований, предъявляемых к сертифицируемому средству защиты информации и к компании-заявителю;
- настраивать среду функционирования перед установкой средств защиты информации;
- устанавливать, настраивать и удалять средства защиты информации;
- применять различные конфигурации средств защиты информации в зависимости от параметров информационной системы;
- проводить проверку работоспособности средств защиты информации
- анализировать журнал событий средств защиты информации;
- осуществлять сохранение настроек средства защиты информации и их восстановление;
- поиск причин нарушения работоспособности средства защиты информации;
- определить виды средств защиты информации в зависимости от предъявляемых требований;
- обоснованно подобрать необходимые модели и марки средств защиты информации;

Краткое содержание дисциплины (модуля)

Тема 1.Классификация и виды средств защиты информации.
Тема 2. Система сертификации средства защиты информации в РФ.
Тема 3. Средства доверенной загрузки.
Тема 4. Средства защиты от несанкционированного доступа.
Тема 5. Средства криптографической защиты информации.
Тема 6. Выбор технических мер при проектировании системы защиты информации.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Сети и системы передачи информации»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 8 зачетных единиц, 288 академических часа.

Форма промежуточной аттестации: 3 семестр – зачет, 4 семестр – экзамен.

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Сети и системы передачи информации» – изучение методов и средств построения и эксплуатации программно-аппаратных технологий, изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий передачи информации.

Задачи курса – изучение:

− принципов построения, функционирования и применения аппаратных средств современной вычислительной техники;

− основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1.2 – способен администрировать средства защиты информации в компьютерных системах и сетях;

ОПК-1.4 – способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

В результате изучения дисциплины студент должен:

Знать:

− способы аппаратной защиты беспроводной передачи информации;
− способы программной защиты беспроводной передачи информации;
− назначение и функции элементов аппаратной технологии защиты;
− организацию и структуру программной технологии защиты
− протоколы передачи информации;
− возможные угрозы при беспроводной передаче информации;
− организацию системной магистрали, способы подключения дополнительных устройств.

Уметь:

− формализовать поставленную задачу;
− настраивать беспроводные средства передачи информации;
− разбираться в устройствах рабочих станций и серверов;
− разбираться в телекоммуникационных устройствах передачи данных
− осуществлять обоснованный выбор стандартного периферийного оборудования; − применять полученные знания к различным предметным областям.

Краткое содержание дисциплины (модуля)

Дисциплина включает 18 тем:

Тема 1. Введение.
Тема 2. Коммуникации с помощью сетей.
Тема 3. Модель OSI. Уровень приложений и транспортный уровень.
Тема 4. Сетевой уровень модели OSI.
Тема 5. Адресация в сети – IPv4.
Тема 6. Канальный и физический уровни модели OSI.
Тема 7. Ethernet.
Тема 8. Планирование и монтаж сети.
Тема 9. Конфигурирование и тестирование сети.
Тема 10. Статическая маршрутизация.
Тема 11. Динамическая маршрутизация.
Тема 12. Дистанционно-векторные протоколы маршрутизации.
Тема 13. RIP, VLSM и CIDR.
Тема 14. RIPv2.
Тема 15. Таблицы маршрутизации.
Тема 16. EIGRP.
Тема 17. Протоколы маршрутизации по состоянию канала.
Тема 18. OSPF.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Системы управления базами данных»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 9 зачетных единицы, 324 академических часа.

Форма промежуточной аттестации: зачет (5 семестр), экзамен (6 семестр).

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Системы управления базами данных» - формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с проектированием и реализацией прикладных защищенных решений и баз данных под управлением современных систем управления базами данных (СУБД).

Задачи курса:

- обучить студентов принципам работы современных систем управления базами данных;
- привить студентам навыки проектирования и реализации баз данных;
- дать студентам представление о проектировании и эксплуатации реляционных баз данных.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

В результате изучения дисциплины студент должен:

Знать:

- области применения систем управления базами данных;
- особенности управления данными в системах распределенной обработки;
- работы с системами управления базами данных на различных платформах;

Уметь:

- разрабатывать программы на высокоуровневых языках программирования;
- применять навыки разработчика и администратора баз данных.

Краткое содержание дисциплины (модуля)

Дисциплина включает 12 тем:

Тема 1. История развития, назначение и роль баз данных
Тема 2. Общие принципы построения БД. Модели данных
Тема 3. Основы построения реляционных БД
Тема 4. Физическая организация баз данных
Тема 5. Нормализация базы данных
Тема 6. Языковые средства СУБД для различных моделей данных. Язык SQL
Тема 7. Планирование, проектирование и администрирование БД
Тема 8. Сервисные средства СУБД; средства автоматизации проектирования баз данных
Тема 9. Средства поддержания целостности базы данных
Тема 10. Эксплуатация баз данных

Тема 11. Технология и модели архитектуры клиент/сервер. Серверы баз данных
Тема 12. Типология БД

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Электроника и схемотехника»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е. (144 часов)

Форма промежуточной аттестации: экзамен (6 семестр).

Цели и задачи освоения дисциплины

Целью дисциплины «Электроника и схемотехника» является изучение основ электроники, элементов теории сигналов и схемотехники преобразовательных, усилительных и генераторных элементов в информационных системах, системах автоматизации.

Задачами дисциплины являются:

- ознакомление студентов с основами преобразования электрических сигналов в линейных и нелинейных аналоговых и цифровых цепях;
- ознакомление с элементной базой электротехнических и электронных цепей;
- ознакомление с основными принципами преобразования электромагнитной энергии в устройствах усиления, выпрямления и генерации;
- ознакомление со схемотехникой аналоговых и цифровых устройств;
- получение практических навыков исследования радиоэлектронных устройств.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-4: способен применять необходимые физические законы и модели для решения задач профессиональной деятельности.

В результате изучения дисциплины студент должен:

знать:

- основные физические принципы работы базовых аналоговых и цифровых функциональных элементов электроники;
- основные принципы работы и проектирования электронных систем; особенности применения аналоговых и цифровых радиоэлектронных устройств;
- основные возможности и особенности существующих программных средств системного, прикладного и специального назначения, используемых в области защиты информации;
- терминологию и символику, используемую в электронике, методы составления и чтения основных видов электрических схем;
- основные физические понятия и принципы функционирования базовых электронных полупроводниковых компонентов в аналоговых и цифровых системах;
- основные параметры и принципы работы базовых функциональных элементов радиоэлектроники (усилителей, генераторов и т.п.);

уметь:

- анализировать физические явления и процессы для решения профессиональных задач;
- применять положения электроники и схемотехники для решения профессиональных задач;
- использовать инструментальные средства, языки и системы программирования для решения профессиональных задач;
- проводить контрольные проверки работоспособности и эффективности применяемых технических средств защиты информации;
- проводить базовые теоретические и экспериментальные исследования электронного оборудования и систем;
- оценивать степень достоверности результатов, полученных с помощью экспериментальных и теоретических методов исследований;
- рассчитывать простые аналоговые и цифровые радиоэлектронные устройства.

Краткое содержание дисциплины

Темы лекционных занятий:
Тема 1. Полупроводниковые приборы.
Тема 2. Биполярные транзисторы.
Тема 3. Усилители электрических сигналов.
Тема 4. Дифференциальный каскад.
Тема 5. Генераторы электрических колебаний.
Тема 6. Элементы цифровой электроники.
Тема 7. Сигналы и их классификация.
Тема 8. Прохождение гармонического сигнала через нелинейную цепь.

Темы лабораторных занятий:
Лабораторная работа №1. Исследование диодов.
Лабораторная работа №2. Исследование биполярного транзистора.
Лабораторная работа №3. Исследование инвертирующего и неинвертирующего усилителя на операционном усилителе.
Лабораторная работа №4. Исследование логических элементов цифровых интегральных микросхем.
Лабораторная работа №5. Исследование JK-триггера и счетчика.
Лабораторная работа №6. Исследование параметрического стабилизатора напряжения.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Языки программирования»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 8 *з.е.,* **288** академических часов.

Форма промежуточной аттестации: зачет (1 семестр), экзамен (2 семестр).

Цели и задачи освоения дисциплины (модуля):
Цель дисциплины: освоение базовых конструкция языка программирования высокого уровня; изучение стандартных типов данных языка программирования высокого уровня; овладение умением конструирования пользовательских типов данных; получение знаний о приёмах алгоритмизации, о формальной постановке задачи, об основных этапах реализации программ на компьютере; формирование готовности использовать приобретенные знания в профессиональной деятельности.

Задачи дисциплины:
- получение знаний, составляющих основу научных представлений об информации, информационных процессах, системах, технологиях и моделях; приобретении практических навыков работы с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий;
- обучение студентов основным подходам к проектированию, разработке и использованию программ;
- дать обучающимся знание технологий разработки программного обеспечения с использованием универсальных языков программирования.

Планируемые результаты освоения
Освоение дисциплины способствует формированию у обучающихся следующих компетенций:
ОПК-7: способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен:
Знает:
- основные направления развития технологий программирования, виды основных структур данных, их особенности, основные методы решения типовых численных задач, методы решения профессиональных, исследовательских и прикладных задач: основные концептуальные положения процедурного программирования, основные методы реализации соответствующих алгоритмов с помощью ЭВМ;
- алгоритмы и технологии программирования для разработки приложений, осуществляющих решение профессиональных задач.

Умеет:
- формализовать вычислительную задачу и выбрать необходимый типовой алгоритм для ее решения;
- выявить типовые, а также нестандартные задачи, разработать метод решения поставленной задачи с использованием типовых алгоритмов;

- разрабатывать специализированные программы для решения задач, тестировать и отлаживать программы в интегрированной среде разработки;
- опираясь на знания теоретических основ программирования, оптимизировать исходный код.

Краткое содержание дисциплины (модуля)

Освоение дисциплины предполагает последовательное освоение следующих тем:

1. Введение в C#. Система типов языка C#. Выражения и операторы. Управление действиями с данными. Массивы.
2. Основные принципы и этапы ООП. Классы и объекты. Элементы класса. Поля и методы. Свойства объектов.
3. Наследование в C#.
4. Виртуальные и динамические методы. Полиморфизм.
5. Абстрактные классы. Интерфейсы. Исключения. Делегаты и события
6. Основы визуального программирования на языке C#.
7. Использование стандартных компонент пользовательского интерфейса
8. Разработка многооконных приложений. Стандартные окна диалога. Файловые типы данных.
9. Организация механизма Drag&Drop.
10. Построение графических изображений.
11. Организация многопоточных приложений.
12. Основы языка Python.
13. Организация работы с файлами в Python.
14. Функции в Python.
15. Основы ООП в Python.
16. Технологии доступа к данным.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Введение в теорию вероятностей и математическую статистику»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Трудоемкость дисциплины: 4 зачетных единиц, 144 академических часов.

Форма промежуточной аттестации: экзамен (4 семестр).

Цели и задачи освоения дисциплины

Целью изучения данной дисциплины является знакомство студентов с основными понятиями, методами и результатами теории вероятностей и математической статистики. Объектами изучения в данной дисциплине являются случайные события и случайные величины. С их помощью могут быть сформулированы как законы природы, так и разнообразные процессы, происходящие в экономике, природе, технике. Отсюда объективная важность теории вероятностей и математической статистики как средства изучения случайных явлений и процессов. Задачами является изучение различных вероятностных моделей случайных событий, свойств распределений случайных величин, предельных теорем, основных задач математической статистики. Большое внимание уделяется вопросам построения математических моделей случайных экспериментов, проверке статистических гипотез, выявлению взаимосвязей между исследуемыми признаками и выработке навыков применения изученных методов при решении практических задач.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОПК-3: способен использовать необходимые математические методы для решения задач профессиональной деятельности.

В результате изучения дисциплины студент должен:
знать:

- основные понятия, теоремы и методы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла;
- методы проведения экспериментов, способы обработки результатов, способы оценки погрешностей и достоверности результатов;

уметь:

- использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач; пользоваться источниками для самостоятельного изучения специальной литературы;
- самостоятельно проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;

владеть:

- методами решения алгебраических уравнений и других задач элементарной и прикладной алгебры, геометрии, дискретной математики, математического анализа,

теории вероятностей, математической статистики, математической логики, теории алгоритмов, в том числе с использованием вычислительной техники; методами построения математических моделей для задач, возникающих на практике и численными методами их решения; математическим аппаратом, необходимым для изучения других фундаментальных и профессиональных дисциплин, работы с современной научно-технической литературой при решении прикладных задач в области профессиональной деятельности;

- способностью качественно проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

Краткое содержание дисциплины

Введение в теорию вероятностей и математическую статистику. Основные понятия теории вероятностей. Случайные события. Классическое, геометрическое, статистическое и аксиоматическое определения вероятности события. Условная вероятность. Теоремы сложения и умножения вероятностей. Формула полной вероятности. Формула Байеса. Схема Бернулли. Случайные величины. Дискретные случайные величины. Непрерывные случайные величины. Примеры распределений известных случайных величин.

Законы распределения. Числовые характеристики случайных величин. Закон больших чисел. Центральная предельная теорема. Генеральная совокупность. Выборки. Основные выборочные характеристики. Статистические оценки. Методы статистическогооценивания. Статистическая проверка гипотез.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Высшая математика»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объём дисциплины (модуля): 8 зачётных единиц, 288 академических часов

Форма промежуточной аттестации: экзамен (2, 3 семестры)

Цели и задачи дисциплины.

Целями преподавания дисциплины являются:

- формирование и развитие навыков математического мышления, навыков использования математических методов и основ математического моделирования, математической культуры у обучающихся;
- обеспечение высокого уровня фундаментальной математической подготовки студентов, необходимого для дальнейшего обучения и успешного усвоения специальных дисциплин;
- приобретение навыков самостоятельного изучения отдельных тем дисциплины и решения типовых задач;
- усвоение полученных знаний студентами, а также формирование у них мотивации к самообразованию за счет активизации их познавательной деятельности.

Задачи изучения дисциплины:

- формирование у студентов базовых знаний об основных математических объектах и структурах,
- освоение методов работы с указанными объектами;
- изучение алгоритмов решения типовых задач;
- обзор возможностей применения изученных моделей и методов к решению различных задач.

Планируемые результаты освоения дисциплины.

В результате освоения ОП выпускник должен обладать следующими компетенциями:

ОПК-3: Способен использовать необходимые математические методы для решения задач профессиональной деятельности.

Перечень планируемых результатов обучения по дисциплине (модулю).

В результате изучения дисциплины студент должен:

знать:

- основные понятия, теоремы и методы алгебры, геометрии, математической логики, теории алгоритмов, теории информации, использующихся при изучении общетеоретических и специальных дисциплин учебного цикла;

уметь:

- использовать знания фундаментальных основ, подходы и методы математики при решении прикладных задач;
- пользоваться источниками для самостоятельного изучения специальной литературы;

владеть:

- методами решения алгебраических уравнений и других задач элементарной и прикладной алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, в том числе с использованием вычислительной техники;
- методами построения математических моделей для задач, возникающих на практике и численными методами их решения;
- математическим аппаратом, необходимым для изучения других фундаментальных и профессиональных дисциплин, работы с современной научно-технической литературой при решении прикладных задач в области профессиональной деятельности.

Содержание дисциплины.

1 семестр.

Тема 1.1. Матрицы и определители.

Размещения, перестановки, сочетания. Связи между ними. Основной комбинаторный принцип. Выборки с возвращением. Выборки без возвращения. Выборки элементов, некоторые из которых повторяются. Множество. Пустое множество. Подмножество. Собственные и несобственные подмножества множества. Равенство множеств. Внутренние бинарные операции на множестве. Объединение множеств. Пересечение множеств. Дополнение одного множества до другого. Декартово произведение множеств. Матрица размера m n. Квадратная матрица порядка n. Диагональная матрица. Единичная матрица порядка n. Нулевая матрица размера m n. Вектор-строка. Вектор-столбец. Равенство матриц. Операции над матрицами. Сложение матриц одинакового размера. Умножение матрицы на число. Транспонирование матрицы. Произведение матриц. Свойства операций над матрицами. Элементарные преобразования матриц. Определитель квадратной матрицы. Миноры и алгебраические дополнения. Теорема Лапласа. Разложение определителя по строке. Свойства определителя. Вырожденные и невырожденные матрицы. Определитель квазитреугольной матрицы. Обратная матрица. Свойства обратной матрицы.

Тема 1.2. Системы линейных уравнений и неравенств.

Линейное пространство. Примеры линейных пространств: пространство геометрических векторов, арифметическое пространство Rn. Подпространство линейного пространства. Линейная оболочка. Сумма подпространств. Пересечение подпространств. Изоморфизм линейных пространств. Линейная зависимость векторов и ее геометрический смысл. Базис линейного пространства. Размерность линейного пространства. Координаты вектора. Ранг матрицы над полем. Ранг матрицы и линейная зависимость. Инвариантность ранга матрицы относительно ее элементарных преобразований. Вычисление ранга. Эквивалентные матрицы. Переход к новому базису. Матрица перехода к новому базису. Преобразование координат вектора при переходе к новому базису. Система линейных уравнений над полем. Определение решения системы линейных уравнений. Эквивалентность систем линейных уравнений. Совместность системы линейных уравнений. Теорема Кронекера — Капелли. Однородная система линейных уравнений. Неоднородная система линейных уравнений. Система линейных уравнений с квадратной невырожденной матрицей. Правило Крамера. Исследование и решение системы линейных уравнений методом Жордана — Гаусса. Частные решения системы линейных уравнений. Элементарные преобразования системы линейных уравнений. Геометрические свойства решений системы линейных уравнений: фундаментальная система решений однородной системы линейных уравнений, линейное подпространство решений однородной системы линейных уравнений. Поиск неотрицательных базисных решений системы линейных уравнений. Симплексные преобразования. Системы линейных алгебраических неравенств.

Тема 2.1. Основные алгебраические структуры.

Полугруппы, группы, кольца, поля и их простейшие свойства.

Тема 2.2. Кольцо целых чисел. Кольца вычетов.

Делимость и деление с остатком в кольце целых чисел. Основная теорема арифметики. Уравнения в кольце вычетов и сравнения. Системы линейных уравнений над кольцом вычетов.

Тема 3.1. Поле комплексных чисел.

Комплексное число. Алгебраическая форма комплексного числа. Комплексная плоскость. Тригонометрическая форма комплексного числа. Возведение комплексного числа в натуральную

степень. Формула Муавра. Извлечение корня натуральной степени из комплексного числа. Геометрическая интерпретация корней. Возведение комплексного числа в рациональную степень.

Тема 3.2. Кольцо многочленов.

Многочлен над полем. Сумма многочленов. Произведение многочленов. Кольцо многочленов. Деление многочленов. Теорема о делении многочлена на многочлен с остатком. Теорема о наибольшем общем делителе многочленов. Корни многочлена. Теорема Безу. Многочлены над полем комплексных чисел. Основная теорема алгебры. Каноническое разложение многочлена над полем комплексныхчисел. Теорема о равенстве многочленов. Формулы Виета. Многочлены над полем вещественных чисел. Каноническое разложение многочлена над полем вещественных чисел. Возведение матрицы в натуральную степень. Многочлен от матрицы.

2 семестр.

Тема 1.1. Евклидовы и унитарные пространства.

Линейное пространство над произвольным полем. Свойства линейного пространства над произвольным полем. Линейная зависимость. Ранг и база системы векторов. Критерий базы. Базис и размерность линейного пространства. Изоморфизм линейных пространств. Критерий изоморфизма. Линейные подпространства. Линейная оболочка системы векторов. Сумма и пересечение линейных подпространств. Прямая сумма подпространств. Критерий прямой суммы. Дополнительное подпространство. Скалярное произведение. Неравенство Коши — Буняковского. Евклидово пространство. Унитарное пространство. Длина вектора в евклидовом (унитарном) пространстве. Неравенства треугольника. Ортогональные векторы. Ортогональный базис линейного пространства. Ортонормированный базис линейного пространства. Процесс ортогонализации Грама — Шмидта. Матрица Грама. Определитель Грама. Эрмитова матрица. Симметричная матрица. Свойства матрицы Грама и определителя Грама. Ортогональное дополнение. Задача о перпендикуляре. Теорема Пифагора. Линейные многообразия в евклидовом (унитарном) пространстве. Расстояние от вектора до линейного подпространства.

Тема 1.2. Линейные операторы.

Линейный оператор. Примеры линейных операторов: оператор проектирования, оператор отражения, нулевой оператор, единичный оператор. Свойства линейного оператора. Матрица линейного оператора. Граф линейного оператора. Координаты вектора и его образа. Матрицы оператора в различных базисах. Подобные матрицы. Линейное пространство операторов. Образ и ядро линейного оператора. Ранг и дефект линейного оператора. Теорема о ранге матрицы линейного оператора в произвольном базисе. Теорема о ранге и дефекте линейного оператора. Инвариантное подпространство относительно линейного оператора. Собственные значения и собственные векторы линейного оператора. Линейная независимость собственных векторов, отвечающих различным собственным значениям. Собственные значения и собственные векторы матрицы. Характеристический многочлен матрицы. Характеристический многочлен линейного оператора. Способ определения собственных векторов.

Тема 2.1. Жорданова нормальная форма матрицы.

Жорданова клетка. Треугольная форма матрицы линейного оператора. Нильпотентный оператор. Индекс нильпотентности. Прямая сумма операторов. Теорема о разложении произвольного линейного оператора в прямую сумму нильпотентного и невырожденного линейных операторов. Теорема о расщеплении линейного оператора. Корневые векторы. Корневые подпространства. Канонический базис корневого подпространства. Матрица линейного оператора в каноническом базисе. Жорданова форма матрицы линейного оператора в комплексном пространстве. Теорема Гамильтона — Кэли.

Тема 2.2. Линейные операторы в пространствах.

Сопряженный оператор. Нормальный оператор. Теорема Шура. Критерий нормальности. Унитарно подобные матрицы. Унитарный (ортогональный) оператор. Критерий унитарности. Спектральная характеристика унитарного оператора. Каноническая форма матрицы ортогонального оператора. Самосопряженный оператор. Знакоопределенные операторы. Идемпотентный оператор. Разложения линейного оператора.

Тема 3.1. Квадратичные формы.

Билинейная форма. Квадратичная форма и ее канонический вид. Приведение квадратичной формы к каноническому виду методом Лагранжа. Критерий Сильвестра положительной определенности квадратичной формы. Квадратичные формы в вещественном пространстве. Закон инерции квадратичных форм. Знакоопределенные квадратичные формы. Квадратичные формы в комплексном пространстве.

Полуторалинейные и эрмитовы формы. Квадратичные формы в евклидовом (унитарном) пространстве.

Тема 3.2. Группы. Кольца. Поля.

Свойства элементов группы. Подгруппы группы. Гомоморфизм групп. Циклические группы. Теорема Кэли. Разложение группы в смежные классы и классы сопряжённых элементов. Критерий равенства смежных классов. Произведение подгрупп. Нормальные делители группы. Конечные абелевы группы. Теорема Прюфера. Группа подстановок. Свойства групп подстановок, связанные с транзитивностью. Основные свойства элементов кольца. Подкольца и идеалы кольца. Простые и главные идеалы. Евклидовы кольца. Прямые суммы колец и идеалов. Кольца многочленов. Симметрические многочлены. Классификация расширений полей. Простые поля. Теорема о простых полях. Теорема о степенях. Поле разложения многочлена. Конечные и совершенные поля. Многочлены над конечными полями. Линейные рекуррентные последовательности над полем.

3 семестр.

Тема 1.1. Булевы функции и логика высказываний.

Функции алгебры логики. Существенные и несущественные переменные. Формулы. Представление функций формулами. Операция суперпозиции. Операция введения несущественной переменной. Замыкание множества функций. Замкнутые классы. Равенство функций. Эквивалентность формул. Элементарные функции и их свойства. Совершенная дизъюнктивная нормальная форма. Совершенная конъюнктивная нормальная форма. Полные системы функций. Достаточное условие полноты. Примеры полных систем. Полиномы Жегалкина. Представление булевых функций полиномами. Линейные функции и их свойства. Функции, сохраняющие константы. Самодвойственные функции и их свойства. Монотонные функции и их свойства. Теорема Поста о полноте системы булевых функций. Возможность выделить из каждой полной системы полную подсистему, состоящую не более чем из 4-х функций. Базисы замкнутых классов. Примеры базисов в P_2. Предполные классы. Свойства предполных классов в P_2. Теорема Поста о конечной порожденности замкнутых классов булевых функций.

Тема 1.2. Исчисление высказываний.

Высказывания и операции над ними. Аксиомы классического исчисления высказываний. Схемы аксиом. Правила вывода. Вывод. Выводимые формулы. Вывод из системы гипотез. Простые свойства выводимости. Примеры вывода. Вывод формулы $A \to A$. Теорема о дедукции. Тождественная истинность выводимых формул. Непротиворечивость классического исчисления высказываний. Теорема о полноте. Независимость схем аксиом исчисления высказываний. Теорема о независимости схем аксиом исчисления высказываний.

Тема 2.1. Логика предикатов.

Понятие предиката. Примеры. Логические операции над предикатами; кванторы. Теоретикомножественный смысл операций над предикатами. Условия полноты системы предикатов на конечном множестве. Формулы; свободные и связанные переменные. Модель, сигнатура модели. Значение формулы в модели. Формула, истинная в модели. Формула, истинная на множестве. Тождественно истинная формула. Правила эквивалентных преобразований формул логики предикатов. Нормальная форма. Приведение формул к нормальной форме.

Тема 2.2. Исчисление предикатов.

Фильтры, максимальные фильтры. Теорема о вложении фильтров. Теорема об ультрафильтрах. Фильтрованные произведения, ультрапроизведения. Теорема об ультрапроизведениях. Теорема компактности. Предложение о бесконечных моделях. Нестандартные арифметики. Теорема о нестандартных арифметиках.

Аксиомы классического исчисления предикатов. Правила вывода. Выводимые формулы. Примеры вывода. Специальный вывод из системы гипотез, теорема о дедукции. Тождественная

истинность выводимых формул. Непротиворечивость классического исчисления предикатов. Теорема Гёделя о полноте.

Тема 3.1. Частично рекурсивные функции.

Частичные числовые функции. Простейшие функции. Операции суперпозиции и примитивной рекурсии. Примитивно рекурсивные функции. Операция минимизации. Частично рекурсивные функции, общерекурсивные функции. Тезис Чёрча. Теорема о совпадении класса частично рекурсивных функций и класса частичных числовых функций, вычислимых по Тьюрингу. Рекурсивные множества, разрешимые предикаты, рекурсивно перечислимые множества, частично разрешимые предикаты. Теорема Райса.

Нормальные алгоритмы Маркова. Принцип нормализации.

Тема 3.2. Машина Тьюринга.

Машина Тьюринга и универсальные функции. Машина Поста. Сводимости и степени. Сводимость по Тьюрингу, степени неразрешимости.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

«Дополнительные главы математического анализа»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Трудоемкость дисциплины (модуля): 4 зачетных единиц, 144 академических часа.

Форма промежуточной аттестации: зачет (4 семестр).

Цели и задачи освоения дисциплины (модуля)

Цель изучения дисциплины: создание у студентов целостного представления о современном математическом анализе.

Задачами изучения данного курса являются:

-овладение знаниями, умениями и навыками из разделов математического анализа, необходимыми для изучения последующих математических и естественнонаучных дисциплин на базовом и продвинутом уровне, для получения образования в областях, не требующих углубленной математической подготовки;

-развитие алгоритмической культуры, логического и критического мышления на уровне, необходимом для будущей профессиональной деятельности студентов или последующего обучения в вузе;

-воспитание средствами математики культуры личности, понимания значимости математики для научно-технического прогресса, отношения к математике как к части общечеловеческой культуры.

Основу данного курса составляют дифференциальное и интегральное исчисление функций одной и многих действительных переменных, элементы дифференциальных уравнений.

Теоретический материал дается в достаточно кратком изложении, в связи с чем, на самостоятельное изучение студентам предлагаются доказательства некоторых основных утверждений и теорем. На практических занятиях внимание уделяется стандартным задачам и задачам повышенной сложности данной дисциплины.

Знать: основные понятия, определения и свойства объектов математического анализа, формулировки и доказательства утверждений, методы их доказательства, возможные сферы их связи и приложения в других областях математического знания и дисциплинах естественнонаучного содержания.

Уметь: доказывать утверждения математического анализа, решать задачи математического анализа, уметь применять полученные навыки в других областях математического знания и дисциплинах естественнонаучного содержания.

Планируемые результаты освоения

В результате освоения дисциплины формируется профессиональных задач:

ОПК-3 – способен использовать необходимые математические методы для решения задач профессиональной деятельности.

Краткое содержание дисциплины

Элементы теории множеств.
Последовательности.
Числовые функции.
Непрерывность функции.
Дифференциальное исчисление функций одной переменной.
Приложение дифференциального исчисления к исследованию свойств функций.

Дифференциальное исчисление функций многих переменных.
Экстремумы функции многих переменных.
Первообразная и неопределенный интеграл. Методы вычисления неопределенного интеграла.
Определенный интеграл. Геометрические и физические приложения определенного интеграла.
Дифференциальные уравнения первого порядка.
Дифференциальные уравнения второго порядка.
Числовые ряды.
Функциональные ряды.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

«Защита в операционных системах»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единиц, 144 академических часа.

Форма промежуточной аттестации: экзамен (7 семестр).

Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Безопасность операционных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Безопасность операционных систем» является изложение основополагающих принципов защиты операционных систем (ОС) и примеров реализации подобных методов на практике.

Задачи дисциплины «Безопасность операционных систем»:

- дать представление об основных угрозах ИБ для современных ОС;
- научить оценивать уровень защищенности ОС с учетом актуальных моделей угроз и требований руководящих документов;
- дать основы системного подхода к обеспечению безопасности в современных ОС;
- изучить сервисы безопасности современных ОС и научить использовать их для защиты ОС.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-1.1: способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;

В результате изучения дисциплины студент должен:

В результате изучения этих дисциплин студент должен:

знать:

- основные понятия и положения защиты информации в ОС;
- основные угрозы ИБ в ОС;
- ресурсы, подлежащие защите;
- основные понятия программно-технического уровня ИБ;
- требования к обеспечению ИБ в ОС;
- основные сервисы безопасности ОС, принципы их организации и структуру;
- методы обеспечения ИБ в ОС;
- перечень программно-технических мер ИБ в ОС;
- основные ресурсы для поиска информации об уязвимостях ОС;

уметь:

- проводить анализ угроз информационной безопасности в ОС;
- проводить классификацию возможных угроз ИБ в ОС;
- оценивать эффективность и надежность защиты ОС;
- находить информацию об актуальных угрозах ОС, уязвимостях ОС;
- выявлять слабые места в защите ОС;

- конфигурировать встроенные сервисы безопасности ОС;
- проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- проводить инструментальный контроль защищенности ОС; владеть:
- навыками поиска и анализа информации об уязвимостях ОС;
- навыками анализ угроз информационной безопасности в ОС;
- навыками безопасного администрирования ОС;
- навыками оценки уровня безопасности ОС;
- навыками использования средств инструментального контроля защищенности ОС.

Краткое содержание дисциплины (модуля)

Тема 1. Основные понятия и положения защиты информации в АС.
Тема 2. Угрозы ИБ: определения, анализ и классификация.
Тема 3. Основные направления и методы реализации угроз ИБ.
Тема 4. Программно-технические меры ИБ, сервисы ИБ.
Тема 5. Требования безопасности информации к операционным системам
Тема 6. Модели безопасности основных операционных систем.
Тема 7. Базовые сервисы безопасности ОС Windows. Реализация, конфигурирование, уязвимости, компрометация, защита.
Тема 8. Дополнительные механизмы защиты в ОС Windows.
Тема 9. Организация защищенного удаленного доступа в ОС Windows.
Тема 10. Сетевая безопасность в ОС Windows.
Тема 11. Аудит безопасности в ОС Windows.
Тема 12. Базовые сервисы безопасности в Unix-like систем. Реализация, конфигурирование, уязвимости, компрометация, защита.
Тема 13. Дополнительные механизмы защиты объектов ФС в Unix-like системах.
Тема 14. Шифрование, контроль целостности в Unix-like системах.
Тема 15. Мандатная модель управления доступом в Unix-like системах.
Тема 16. Подключаемые модули аутентификации.
Тема 17. Организация защищенного удаленного доступа в Unix-like системах.
Тема 18. Сетевая безопасность в Unix-like системах.
Тема 19. Аудит безопасности в Unix-like системах.
Тема 20. Общие рекомендации по защите ОС.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Компьютерные сети»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 4 зачетных единиц, 144 акад.час.

Форма промежуточной аттестации: экзамен.

Цели и задачи освоения дисциплины (модуля)

Цель дисциплины «Компьютерные сети» - является изложение истории развития мировой и отечественной мысли в области коммуникаций, а также истории защиты информации в средствах коммуникации.

Задачи курса - изучение:

- основных этапов истории развития коммуникаций терминологии;
- истории аналоговой коммуникации;
- истории и тенденции развития цифровых коммуникаций;
- основных технологий цифровых коммуникаций и их защищенность.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-2: способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

В результате изучения дисциплины студент должен:

Знать:

- свойства информации, подлежащие закрытию;
- этапы развития средств и технологий коммуникаций;
- историю развития информационного противоборства в России и мире
- основные технологии передачи цифровой информации;
- назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих передачу цифровой информации.
- основные стандарты, используемые при передаче цифровой информации; - основные технологии защиты информации.

Уметь:

- создавать и настраивать LAN сети.
- ориентироваться в истории технологий передачи информации, методах защиты информации в контексте исторического развития.
- создавать, безопасное подключение LAN к Интернет.

Краткое содержание дисциплины (модуля) Дисциплина включает 9 тем:

Тема 1. Введение в технологии защищенных коммуникаций
Тема 2. 3 этапа развития защищенных коммуникаций
Тема 3. Локальные, корпоративные и глобальные сети

Тема 4. Сетевая адресация. IP адреса и маска подсети
Тема 5. Сетевые службы
Тема 6. Беспроводные технологии
Тема 7. Основы безопасности цифровых коммуникаций
Тема 8. Структура, адресация и настройка сети. Маршрутизация
Тема 9. Коммутируемая архитектура. Корпоративные сети.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Разработка и защита web-приложений»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 5 зачетных единиц, 180 академических часов.

Форма промежуточной аттестации: зачет.

Цели и задачи освоения дисциплины (модуля)

Целью дисциплины «Разработка и защита web-приложений» является обучение студентов основам создания веб приложений, ознакомиться с современным серверным и сетевым оборудованием, изучить методики и способы защиты веб приложений и сетевого оборудования.

Задачи дисциплины «Разработка и защита web-приложений»:

- изучить устройство сети Интернет;
- изучить языки разметки документов;
- изучить протоколы http, https, ftp;
- изучить принцип работы веб сервера;
- принципы функционирования веб приложений;
- изучить средства разработки веб приложений;
- изучить наиболее распространённые веб серверы, их возможности и функционал;
- научиться создавать простейшие веб страницы;
- научиться использовать основные и дополнительные метатеги;
- изучить способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов;
- изучить методы проверки и тестирования законченных сайтов.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-2 – способен администрировать средства защиты информации в компьютерных системах и сетях.

ПК-3 – способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации.

ПК-4 – способен организовывать и проводить работы по технической защите информации.

В результате изучения дисциплины студент должен:

Знать:

− устройство сети Интернет;
− языки разметки документов;
− протоколы http, https, ftp;
− принцип работы веб сервера;
− принципы функционирования веб приложений; −
средства разработки веб приложений;
− наиболее распространённые веб серверы, их возможности и функционал;
− способы создания простейших веб страниц;
− основные и дополнительные метатеги;

- способы создания и настройки дополнительных инструментариев, позволяющие увеличивать посещаемость сайтов.

Уметь:

- использовать средства разработки веб приложений;
- разрабатывать простые веб страницы на языке html;
- использовать основные и дополнительные метатеги;
- использовать дополнительный инструментарий, позволяющий увеличивать число посетителей и продвигать сайт в поисковых системах.
-

Краткое содержание дисциплины (модуля)

Тема 1. Введение. Устройство сети Интернет. Обзор современных веб технологий.

Тема 2. DNS сервер и его роль в организации работы сайта.

Тема 3. DNS записи, маршрутизация и обзор современных DNS серверов.

Тема 4. Языки разметки документов. Гипертекстовая разметка XML.

Тема 5. Средства разработки веб приложений. CMS – Системы управления контентом веб-сайтов.

Тема 6. Протокол HTTP, веб сервер и веб клиент, прокси сервер.

Тема 7. Создание простой web-страницы. Форматирование.

Тема 8. Каскадные таблицы стилей (CSS).

Тема 9. Метатеги основные и дополнительные.

Тема 10. Системы индексации сайтов. Файл robots.txt и sitemap.xml. **Тема 11.** Веб-аналитика. Счетчики.

Тема 12. JavaScript для WEB.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Технологии и методы программирования»
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины (модуля): 8 зачетных единиц, 288 академических часов.
Форма промежуточной аттестации: зачет (3 семестр), экзамен (4 семестр).
Цели и задачи освоения дисциплины (модуля)

Учебная дисциплина «Технологии и методы программирования» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом.

Основной целью дисциплины «Технологии и методы программирования» является изложение основополагающих принципов разработки программного обеспечения в различных средах с использованием различных информационных технологий при решении разнообразных прикладных задач.

Задачи дисциплины «Технологии и методы программирования»

- дать представление о компьютерных технологиях и методах программирования;
- научить использовать компьютерные технологии и методы программирования для решения разнообразных прикладных задач.

Планируемые результаты освоения

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ПК-1 - способен выполнять комплекс мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД.

В результате изучения дисциплины студент должен:
знать:

- значение информации в развитии современного общества;
- основные языки и системы программирования, среды разработки и компьютерные технологии.

уметь:

- применять информационные технологии для поиска и обработки информации;
- применять основные языки и системы программирования, среды разработки и компьютерные технологии для решения профессиональных задач.

Краткое содержание дисциплины (модуля)

1. Введение в дисциплину
2. Разработка с использованием скриптовых языков программирования.
3. Разработка Win32 приложений и библиотек
4. Разработка консольных приложений
5. Разработка оконных приложений
6. Параллельное программирование
7. Разработка и использование COM объектов
8. Разработка и использование ActiveX объектов
9. Разработка сетевых приложений
10. Разработка сервисных приложений

11. Разработка .NET-приложений
12. Разработка внешних хранимых процедур для серверов баз данных
13. VBA приложения
14. Web приложения

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации от утечки по техническим каналам
Направление подготовки: 10.03.01 «Информационная безопасность»
профиль: «Безопасность компьютерных систем»
(связь, информационные и коммуникационные технологии)
форма обучения очная

Объем дисциплины: 4 з.е.

Форма промежуточной аттестации: экзамен (7 семестр)

Планируемые результаты освоения:

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-6 - способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами.

В результате изучения дисциплины студент должен:

знать:

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области.

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю оценки защищенности компьютерных систем;
- анализировать и оценивать угрозы информационной безопасности объекта;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.

Краткое содержание дисциплины (модуля)

Тема 1.1. Введение. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке.

Тема 1.2. Свойства и виды информации. Виды, источники и носители защищаемой информации.

Тема 1.3. Демаскирующие признаки объектов наблюдения и сигналов. Опасные сигналы и их источники.
Тема 1.4. История развития разведки и съема информации. Средства и методы технической разведки. Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
Тема 1.5. Способы и средства перехвата сигналов. Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации.
Тема 2.1. Технические каналы утечки информации. Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации.
Тема 2.2. Оптические и радиоэлектронные каналы утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации. Электромагнитные каналы утечки информации. Канал ПЭМИН. 10.
Тема 2.3. Акустические и виброакустические каналы утечки информации. Материальновещественные каналы утечки информации. Комплексное использование каналов утечки информации.
Тема 2.4. Средства обнаружения технических каналов утечки информации. Средства обнаружения и локализации закладных устройств. Нелинейные локаторы. Сканирующие приёмники. Детекторы электромагнитного поля. Программно-аппаратные автоматизированные комплексы. Досмотровая техника.
Тема 2.5. Мероприятия по выявлению средств технической разведки. Специальные проверки, специальные обследования, и специальные исследования.
Тема 3.1. Методы и средства защиты информации от утечки по техническим каналам. Пассивные и активные методы защиты.
Тема 3.2. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов.
Тема 3.3. Обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов.
Тема 3.4. Концепция и методы инженерно-технической защиты информации. Методы и средства инженерной защиты и технической охраны объектов.
Тема 3.5. Виды контроля и расчёта эффективности защиты информации. Физические принципы контроля защиты информации; основные положения методологии инженерно-технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации. Средства измерения при инструментальном контроле.