Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

КАФЕДРА ФИНАНСОВОГО МОНИТОРИНГА

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2/1

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

АДМИНИСТРИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Направление подготовки (специальность) [1] 10.03.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
7	3-4	108-144	16	32	0		6-42	0	Э
Итого	3-4	108-144	16	32	0	0	6-42	0	

АННОТАЦИЯ

Дисциплина направлена на формирование у студентов представления об общих и специфических особенностях функционирования компьютерных сетей, систем, протоколов, технологий различного типа и отдельных их составляющих, а также навыков администрирования средств защиты информации в компьютерных системах и сетях.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основная цель курса заключается в формировании у студентов представлений о принципах построения вычислительных сетей, спецификациях типовых протоколов, разработанных в соответствии с существующими стандартами в области компьютерных сетей, а также в формировании первичных навыков работы с сетевым оборудованием и средствами защиты в компьютерных системах и сетях.

В процессе изучения предмета студенты получают знания о базовых технологиях и процессах, связанных с формированием и передачей сигналов различного типа.

Овладев предложенной в рамках курса информацией, обучающиеся должны иметь представление об общих и специфических особенностях функционирования компьютерных сетей, систем, протоколов, технологий различного типа и отдельных их составляющих, знать о возможностях применения в конкретных областях.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина опирается на компетенции, знания и навыки, полученные студентами при изучении таких дисциплин, как «Информатика (основы программирования)», «ЭВМ и периферийные устройства», «Программирование (алгоритмы и структуры данных)», «Программирование (объектно-ориентированное программирование)», «Основы информационной безопасности», «Низкоуровневое программирование», «Техническая защита информации», «Защита информации от несанкционированного доступа», «Защита программного обеспечения и безопасность веб-приложений», «Базы данных и экспертные системы», «Комплексная защита объектов информатизации», «Стеганография», «Сети и телекоммуникации / Networks and Telecommunications», «Методы и средства криптографической защиты информации», «Моделирование процессов и проектирование систем защиты информации», «Программно-аппаратные средства защиты информации». В свою очередь, знание основ администрирования средств защиты информации в компьютерных системах и сетях необходимо при изучении таких дисциплин, как «Принципы построения, проектирования и эксплуатации информационных и аналитических систем», «Безопасность электронного документооборота», «Основы управления информационной безопасностью», «Защита информации от утечки по скрытым каналам / Covert Channels Protection», «Безопасность информационных и аналитических систем», при выполнении учебно-исследовательской работы, при прохождении производственной практики (преддипломной), а также для подготовки выпускной квалификационной работы (ВКР).

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-6.2 [1] – Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур, для информационно-аналитического обеспечения финансового мониторинга	З-ОПК-6.2 [1] – знать особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур У-ОПК-6.2 [1] – уметь проводить финансового мониторинг с учетом особенностей информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур В-ОПК-6.2 [1] – владеть принципами проведения финансового мониторинга
ОПК-6.3 [1] – Способен осуществлять эксплуатацию и проводить техническое обслуживание информационно-аналитических систем финансового мониторинга	З-ОПК-6.3 [1] – знать комплекс мероприятий по эксплуатации и техническому обслуживанию информационно-аналитических систем финансового мониторинга У-ОПК-6.3 [1] – уметь осуществлять эксплуатацию и проводить техническое обслуживание информационно-аналитических систем финансового мониторинга В-ОПК-6.3 [1] – владеть принципами проведения технического обслуживания информационно-аналитических систем финансового мониторинга
ОПК-6.4 [1] – Способен реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	З-ОПК-6.4 [1] – знать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур У-ОПК-6.4 [1] – уметь организовать защиту информации в автоматизированных системах финансовых и экономических структур В-ОПК-6.4 [1] – владеть принципами организации защиты информации в автоматизированных системах финансовых и экономических структур

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
эксплуатационный			
Решение информационно-аналитических задач в сфере	Система обеспечения информационной безопасности и	ПК-1 [1] - способен устанавливать, настраивать и проводить техническое	З-ПК-1[1] - знать требования к проведению технического

профессиональной деятельности с использованием специальных ИАС	информационно-аналитического обеспечения финансового мониторинга	обслуживание средств защиты информации *Основание:* Профессиональный стандарт: 06.033	обслуживания средств защиты информации ; У-ПК-1[1] - уметь устанавливать, настраивать и проводить техническое обслуживание средств защиты информации; В-ПК-1[1] - владеть навыками проведения технического обслуживания средств защиты информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры финансовой безопасности (В44)	1.Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков финансовой безопасности через изучение типологий финансовых махинаций, освоение механизмов обеспечения кибербезопасности в кредитно-финансовой сфере в соответствии с нормативными документами ЦБ РФ, изучение рисков и угроз в рамках процедур кредитования, инвестирования и других механизмов экономической деятельности. 2.Использование воспитательного потенциала дисциплин профессионального модуля для развития коммуникативных компетенций, навыков делового общения, работы в гибких командах в условиях быстроменяющихся внешних факторов за счет изучения учащимися возможностей, методов получения информации, ее обработки и принятии решения в условиях оценки многофакторных ситуаций, решения кейсов в области межличностной коммуникации и делового общения. 3.Использование воспитательного потенциала дисциплин профессионального модуля для формирования нравственных и

		правовых норм.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	7 Семестр						
1	Распределенная обработка и хранение данных. Коммуникационная инфраструктура	1-8	8/16/0	Т-7 (25)	25	КИ-8	З-ОПК-6.2, У-ОПК-6.2, В-ОПК-6.2, З-ОПК-6.3, У-ОПК-6.3, В-ОПК-6.3, З-ОПК-6.4, У-ОПК-6.4, В-ОПК-6.4, З-ПК-1, У-ПК-1, В-ПК-1
2	Средства защиты открытых информационных систем	9-16	8/16/0	Т-15 (25)	25	КИ-16	З-ОПК-6.2, У-ОПК-6.2, В-ОПК-6.2, З-ОПК-6.3, У-ОПК-6.3, В-ОПК-6.3, З-ОПК-6.4, У-ОПК-6.4, В-ОПК-6.4, З-ПК-1, У-ПК-1, В-ПК-1
	Итого за 7 Семестр		16/32/0		50		
	Контрольные мероприятия за 7 Семестр				50	Э	З-ОПК-6.2, У-ОПК-6.2, В-ОПК-6.2, З-ОПК-6.3, У-ОПК-6.3, В-ОПК-6.3, З-ОПК-6.4, У-ОПК-6.4, В-ОПК-6.4,

							З-ПК-1, У-ПК-1, В-ПК-1

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
Т	Тестирование
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	7 Семестр	16	32	0
1-8	**Распределенная обработка и хранение данных. Коммуникационная инфраструктура**	8	16	0
1 - 2	**Концепция ОИС. Модельное представление ОИС. Основные аспекты совместимости ОИС.** Концепция ОИС Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем. Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Системообразующие стандарты ISO/IEC. Модельное представление ОИС Формы логической организации стандартов. Классификация моделей. Модель ISO OSI. Профили на базе модели ISO OSI. Спецификация POSIX и её развитие. Модель OSE/RM. Тестирование соответствия профилям. Эволюция моделей открытых систем. Модели распределённых вычислений. Модель TOGAF – современная концепция описания компьютерных систем: метод синтеза архитектуры системы, нормативная техническая модель, описание сложной системы специалистами различных предметных областей, информационная база стандартов. Основные аспекты совместимости ОИС Базовая модель информационной системы (ИС), её основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы.	Всего аудиторных часов 2 Онлайн 0	4 0	0 0
3 - 4	**Распределенная обработка и хранение данных** Уровни распределения обработки данных в архитектуре	Всего аудиторных часов 2	4	0

	открытой системы. Модель RM-ODP. Модели организации распределённых вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки: диспетчеризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок. Архитектура распределённого хранения данных. Сети хранения данных (SAN – Storage Area Networks). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN.	Онлайн 0	0	0
5 - 6	**Глобальная коммуникационная инфраструктура** Концепция глобальной коммуникационной инфраструктуры. Физические способы реализации инфраструктуры. Проводные, оптические, радиоканалы. Транспортные задачи коммуникационной инфраструктуры. Эффективное кодирование, помехоустойчивость, управление линией передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay.	Всего аудиторных часов 2 Онлайн 0	4 0	0 0
7 - 8	**Управление криптографическими ключами. Концепция инфраструктуры открытых ключей (PKI).** Управление криптографическими ключами Жизненный цикл ключей. Стандарт ISO/IEC 11770. Модели управления ключами: централизованная и децентрализованная. Типовая структура ключевой системы. Концепция инфраструктуры открытых ключей (PKI) Основные модели, стандарты и рекомендации. Управление ключами в многодоменных ИС.	Всего аудиторных часов 2 Онлайн 0	4 0	0 0
9-16	**Средства защиты открытых информационных систем**	8	16	0
9 - 10	**Интранет, экстранет, портал** Понятие интранет как примера открытой системы и задачи ее защиты. Структура интранет. Эталонная модель интранет. Экстранет. Порталы: виды порталов, схема, компоненты, базовые сервисы. Корпоративные порталы.	Всего аудиторных часов 2 Онлайн 0	4 0	0 0
11 - 12	**Модели угроз и нарушителей ИБ** Модели угроз и нарушителей ИБ Основные понятия: уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ. Информационная инфрастуктура.	Всего аудиторных часов 2 Онлайн 0	4 0	0 0

	Причины уязвимости ИС. Уязвимость архитектуры клиент-сервер: конфигурация системы, уязвимость операционных систем, уязвимость серверов (уязвимость систем управления базами данных, уязвимость систем электронного документооборота), уязвимость рабочих станций, уязвимость каналов связи (перехват паролей, перехват незащищенного трафика, недостатки протоколов, уязвимости каналообразующего оборудования). Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении. Сетевые вирусы. Виды угроз ресурсам интранета и Интернета. Виды источников угроз ИБ.			
13 - 14	**Специфика защиты ресурсов открытых ИС. Политика ИБ для открытых ИС.** Специфика защиты ресурсов открытых ИС Комплексный и фрагментарный подходы к защите ИС. Эшелонированная защита. Четырехуровневая модель открытой системы. Руководящие документы и стандарты по защите открытых сетей. Топология сети: физическая изоляция; изоляция протокола; выделенные каналы. Политика ИБ для открытых ИС Разновидности политик ИБ. Модели доверия. Основные положения политики ИБ. Процесс выработки политики ИБ, ее реализация и модификация.	Всего аудиторных часов		
		2	4	0
		Онлайн		
		0	0	0
15 - 16	**Средства защиты открытых ИС** Сервисы безопасности. Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры. Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Дополнительная информация и итоговые рекомендации по защите открытых ИС.	Всего аудиторных часов		
		2	4	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	Темы занятий / Содержание
	7 Семестр
1 - 4	**Знакомство с организацией и работой открытых сетей (на примере Интернета), их протоколами и сервисами и их уязвимостями** Изучение уязвимостей некоторых сервисов и протоколов. Поиск информации по уязвимостям в Интернете. Основные сетевые утилиты ОС Linux, используемые для сбора информации об атакуемой системе. Программа для сканирования и исследования сетевой безопасности nmap.
5 - 8	**Изучение функционирования и настройки межсетевых экранов на примере netfiler/iptables** Изучение функционирования и настройки межсетевых экранов на примере netfiler/iptables
9 - 11	**Изучение и практическое применение шифрованной файловой системы LUKS и протокола удалённого управления ОС SSH.** Изучение и практическое применение шифрованной файловой системы LUKS и протокола удалённого управления ОС SSH.
12 - 15	**Изучение и практическое применение методов аутентификации (PAM), системы аудита auditd и протокола syslog в ОС Linux.** Изучение и практическое применение методов аутентификации (PAM), системы аудита auditd и протокола syslog в ОС Linux.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: лабораторные работы и доклады и презентации с их обсуждением в сочетании с внеаудиторной работой. В соответствии со спецификой ВУЗа в процессе преподавания дисциплины методически целесообразно в каждом разделе выделить наиболее важные темы и акцентировать на них внимание обучаемых.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	Индикаторы освоения	Аттестационное мероприятие (КП 1)
ОПК-6.2	З-ОПК-6.2	Э, КИ-8, КИ-16, Т-7, Т-15
	У-ОПК-6.2	Э, КИ-8, КИ-16, Т-7, Т-15
	В-ОПК-6.2	Э, КИ-8, КИ-16, Т-7, Т-15
ОПК-6.3	З-ОПК-6.3	Э, КИ-8, КИ-16, Т-7, Т-15
	У-ОПК-6.3	Э, КИ-8, КИ-16, Т-7, Т-15
	В-ОПК-6.3	Э, КИ-8, КИ-16, Т-7, Т-15

ОПК-6.4	З-ОПК-6.4	Э, КИ-8, КИ-16, Т-7, Т-15
	У-ОПК-6.4	Э, КИ-8, КИ-16, Т-7, Т-15
	В-ОПК-6.4	Э, КИ-8, КИ-16, Т-7, Т-15
ПК-1	З-ПК-1	Э, КИ-8, КИ-16, Т-7, Т-15
	У-ПК-1	Э, КИ-8, КИ-16, Т-7, Т-15
	В-ПК-1	Э, КИ-8, КИ-16, Т-7, Т-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.</td></tr>
</table>

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Б 73 Информационные системы и технологии. Теория надежности : учебное пособие для вузов, Богатырев В. А., Москва: Юрайт, 2022

2. ЭИ Н 62 Методы защиты информации. Защищенные сети : учебное пособие, Никифоров С. Н., Санкт-Петербург: Лань, 2021

3. ЭИ С 32 Основы локальных компьютерных сетей : , Сергеев А. Н., Санкт-Петербург: Лань, 2022

4. ЭИ Д 44 Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов, Дибров М. В., Москва: Юрайт, 2022

5. ЭИ Д 44 Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов, Дибров М. В., Москва: Юрайт, 2022

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ П 12 Администрирование сетей Cisco: освоение за месяц : , Пайпер Б. , Москва: ДМК Пресс, 2018

2. ЭИ В 34 Администрирование системы защиты SELinux : , Вермейлен С., Москва: ДМК Пресс, 2020

3. ЭИ Г96 Вычислительные системы, сети и телекоммуникации : , Гусева А.И., Киреев В.С., Цыплаков А.С., [Москва]: [МИФИ], 2008

4. ЭИ Б 64 Информационная безопасность: защита и нападение : , Бирюков А. А., Москва: ДМК Пресс, 2017

5. 004 О-54 Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие, Олифер Н., Олифер В., Москва [и др.]: Питер, 2017

6. ЭИ К 14 Надежность и безопасность программного обеспечения : учебное пособие для вузов, Казарин О. В., Москва: Юрайт, 2021

7. ЭИ М60 Сетевые атаки на открытые системы на примере Интранета : учебное пособие для вузов, Милославская Н.Г., Москва: НИЯУ МИФИ, 2012

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Перед началом занятий студентам следует ознакомиться с учебным планом и списком рекомендованной литературы.

Перед посещением очередной лекции освежить в памяти основные концепции пройденного ранее материала. Подготовить при необходимости вопросы преподавателю. На каждой лекции следует задавать вопросы как по материалу текущей лекции, так и по ранее прочитанным лекциям.

При изучении лекционного материала обязательно следует сопоставлять его с материалом семинарских и лабораторных занятий.

Для более подробного изучения курса следует работать с рекомендованными литературными источниками и Интернет-источниками.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Цель учебного курса

Основная цель курса заключается в предоставлении обучающимся начальных сведений о построении вычислительных сетей, спецификациях типовых протоколов, разработанных в соответствии с существующими стандартами в области вычислительных сетей, а также предоставление первичных навыков работы с сетевым оборудованием и программным обеспечением, предназначенным для построения безопасных вычислительных сетей. В процессе изучения предмета предполагается предоставление сведений о базовых технологиях, детализация сведений о процессах, связанных с формированием и передачей сигналов различного типа. Овладев предложенной в рамках курса информацией, обучающиеся должны иметь представление об общих и специфических особенностях функционирования вычислительны сетей, протоколов, технологий различного типа и отдельных их составляющих, знать о возможностях применения в конкретных областях. Помимо этого, основываясь на знаниях базовых принципов построения безопасных вычислительных сетей, студенты, прошедшие курс обучения могут применять полученные знания для выбора соответствующего оборудования при решении поставленных производственных задач. Знания, полученные в процессе изучения рассматриваемой тематики, могут также пригодиться для принятия решений, например, о внедрении той, или иной технологии с соответствующим обоснованием решения при проектировании различных информационных систем.

Задачи курса заключаются в создании у студентов навыков применения полученных сведений для решения исследовательских и практических задач при проектировании безопасных вычислительных сетей различного назначения. Приобретенные знания помогут в разработке собственно безопасных вычислительных сетей, их эксплуатации и перспективном планировании.

Для приступающих к ознакомлению с учебным курсом есть определенные требования по предварительной подготовке, а именно следует знать:

- курс физики в объеме базового курса, полученного в НИЯУ МИФИ или другом институте соответствующего профиля;

- основы электротехники в рамках общеобразовательного курса;

- основы радиотехники, связанные с передачей радиотехнических сигналов;

- основы математической логики;

- курс дискретной математики.

После изучения данного курса обучающиеся должны владеть умением постановки задач для проектирования безопасных вычислительных сетей, исходя из требований к обеспечению информационного процесса на каждом конкретном предприятии.

Для этого студенты, изучившие дисциплину, должны иметь представление:

- об особенности архитектуры систем, рассматриваемых в рамках предлагаемого курса;

- об основных тенденциях развития систем радиосвязи и электросвязи;

- об основных принципах работы систем передачи информации;

- особенности проектирования и эксплуатации безопасных вычислительных сетей;

- о специфике применения рассматриваемых в рамках данного курса средств и систем в хозяйственной, производственной и научной сферах.

Знать:

- основные стандарты построения и взаимодействия безопасных вычислительных сетей;

- принципы работы сетевых протоколов и технологий передачи данных в

безопасных вычислительных сетях;

- основы организации и функционирования безопасных вычислительных сетей, их стандарты,

протоколы и предоставляемые сервисы;

Уметь:

- проектировать безопасные вычислительные сети различной степени сложности;

- производить оценку применения различных средств связи и систем в зависимости от специфики проектируемых или находящихся в эксплуатации

безопасных вычислительных сетей;

- осуществлять управление ИБ в открытых системах.

- прогнозировать возможность применения новых разработок изучаемых средств при необходимости модернизации сетей или систем.

Владеть:

- терминологией и системным подходом построения безопасных вычислительных сетей связи различных типов.

Взаимосвязь данного учебного курса с другими дисциплинами

Основная цель, которую призван решить данный учебный курс, – это предоставить обучающимся систематизированный подход к проблеме использования безопасных вычислительных сетей передачи информации на основе предоставленных базовых сведений.

Курс занимает заметное место в общей системе подготовки специалистов, способных решать практические задачи в обеспечении работоспособности, проектирования и эксплуатации безопасных вычислительных сетей. Полученные студентами знания могут быть полезны в дипломном проектировании или в дальнейшей производственной деятельности.

Средства обеспечения освоения учебного курса

При изучении дисциплины рекомендуется использовать следующие средства обучения:

- программу учебного курса:

- рекомендуемую основную и дополнительную литературу;
- методические указания, пособия и учебники (в бумажном виде);
- задания для самостоятельной работы для закрепления теоретического материала;
- электронное учебное пособие;
- описания лабораторных работ и контрольные вопросы к ним;
- методическое обеспечение текущего и итогового контроля знаний.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы и самостоятельной работе.

Принципы отбора содержания и организации учебного материала дисциплины

Учебный курс включает в себя теоретические знания, приобретаемые в ходе лекционных занятий.

Дисциплина выполняет функции теоретической подготовки студентов. Лекционный курс содержит достаточно большой объем сведений, касающихся как теоретических проблем, так и особенностей структур различных сетей, а также в отдельных случаях – и деталей наиболее важных процессов приема, передачи и обработки разнообразной информации. При изучении курса самостоятельная работа включает ознакомление студентов с теоретическим материалом, представленным в электронном учебном пособии и самостоятельное изучение тем учебной программы.

Порядок оценивания промежуточных и итоговых результатов усвоения учебного материала по курсу

Текущий контроль качества усвоения учебного материала по курсу.

Проверка качества усвоения знаний в течение семестра (промежуточный контроль знаний) может осуществляться в виде

1. В виде индивидуального программированного опроса;
2. В виде собеседования.

Итоговая аттестация по дисциплине осуществляется в форме экзамена по дисциплине.

После изучения теоретической части курса студент должен сдать зачет в форме компьютерного тестирования или на основе последовательного ответа на предлагаемые вопросы индивидуально сформированного теста из разных частей курса. Тест формируется преподавателем курса, для чего определяются следующие параметры: число вопросов в тесте, пропорционально объему каждой темы курса, время тестирования, число попыток запуска теста, критерии оценки по пятибалльной оценке или «зачет-незачет», сложность вопросов и т.п. Далее эти параметры вводятся в систему компьютерного тестирования, которая автоматически составляет тест – индивидуальный для каждого студента, на основе произвольного выбора вопросов из имеющейся базы со случайным порядком вывода на экран ответов для выбора. После завершения тестирования на экран выводится результат тестирования. Преподаватель может посмотреть протокол тестирования отдельного студента и подготовить общую ведомость по тестированию одной учебной группы.

Зачет по дисциплине проводится с учетом оценки результатов тестирования. В случае получения высшей оценки, соответствующей 75% правильным ответам на вопросы каждого из тестов, по решению руководства кафедры студенту может быть поставлена отметка «отлично».

Кроме того, оценка может быть получена на основе анализа знаний студента, проводимого в следующих формах.

1) в устной форме, путем обсуждения проблем в конце изучения каждой темы курса или в виде деловых игр;

2) в письменной форме, путем выполнения студентами разных по форме и содержанию работ и заданий, связанных с теоретическим и практическим освоением дисциплины.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

- самостоятельное ознакомление студентов с теоретическим материалом, представленным в электронном учебном пособии;
- самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

В качестве методической помощи преподавателям рекомендуется перечень вопросов и заданий для самостоятельной работы, к промежуточному контролю знаний и экзамену.

Автор(ы):

Рычков Вадим Александрович