МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

(КГУ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Телекоммуникационные технологии и информационная безопасность

Направление подготовки – **01.04.02 «Прикладная математика и информатика»**

Направленность **«Математическое моделирование и программирование»**

Квалификация (степень) выпускника: магистр

Кострома
2024

Рабочая программа дисциплины Телекоммуникационные технологии и информационная безопасность по направлению подготовки *01.04.02 Прикладная математика и информатика*, направленность *Математическое моделирование и программирование* разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 01.04.02 Прикладная математика и информатика, *приказ №13 от 10 января 2018 г.*

Разработал: _____ Сухов Андрей Константинович, доцент, к.ф.-м.н., доцент

Рецензент: _____ Козырев Сергей Борисович, доцент, к.ф.-м.н., доцент

УТВЕРЖДЕНО:

На заседании кафедры прикладной математики и информационных технологий

Протокол заседания кафедры №12 от 22 мая 2019 г.

Заведующий кафедрой прикладной математики и информационных технологий

_____ Секованов Валерий Сергеевич, профессор, д.п.н., к.ф.-м.н.

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры прикладной математики и информационных технологий

Протокол заседания кафедры №_6__ от __14.05.2024 г.

Заведующий кафедрой прикладной математики и информационных технологий

_Ивков В.А._____ _к.э.н., доцент_(ФИО), ученая степень, ученое звание

подпись

1. Цели и задачи освоения дисциплины

Цель дисциплины:

Развить у студентов способность работать с современными телекоммуникационными технологиям, моделями, методами и средствами обеспечения информационной безопасности.

Задачи дисциплины:

– рассмотрение перспектив использования телекоммуникационных технологий в условиях перехода к информационному обществу.

– дать развернутое представление о проблеме вирусной угрозы в сетях, методах борьбы с вирусами и комплексные системы антивирусной защиты.

– научить решать задачи, связанные с обеспечением информационной безопасности при эксплуатации информационных систем.

2. Перечень планируемых результатов обучения по дисциплине

Студенты, завершившие изучение дисциплины «Телекоммуникационные технологии и информационная безопасность», должны **освоить компетенцию:**

ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

Код и содержание индикаторов компетенции:

ОПК-4.1.

Знать: принципы, методы и средства решения профессиональных задач с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности

ОПК-4.2.

Уметь: решать прикладные задачи в области профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности

ОПК-4.3.

Иметь навыки: применения информационно-коммуникационных технологий в области профессиональной деятельности с учетом требований информационной безопасности

знать:

- основы построения и функционирования сетей передачи данных;
- систему управления сети передачи данных; систему управления безопасностью сети;
- аппаратурный состав коммуникационного оборудования сети, виды угроз информационной безопасности;
- методы и средства борьбы с угрозами информационной безопасности;
- существующие стандарты информационной безопасности;

– нормативные руководящие документы, касающиеся государственной тайны;

уметь:

– анализировать процессы обработки данных,

– интерпретировать получаемые результаты с целью выработки предложений по совершенствованию технологии функционирования сетей,

– выполнять анализ способов нарушений информационной безопасности; использовать методы и средства защиты данных;

– использовать методы и средства защиты данных.

владеть:

– сетевыми технологиями, используемыми в современных телекоммуникационных системах,

– методами криптографической защиты от всех видов компьютерных вирусах;

– концепциями информационной безопасности.

3. Место дисциплины в структуре ОП ВО

Дисциплина «Телекоммуникационные технологии и информационная безопасность» относится к обязательной части учебного плана; изучается в 1-м семестре обучения.

Она служит теоретическим и практическим фундаментом для последующего курса: «Методика обучения web-программированию».

Она также является необходимым этапом для изучения дисциплины «Методика разработки онлайн-курса»; может быть использована при прохождении практик и написании курсовой и дипломной работ.

4. Объём дисциплины «Телекоммуникационные технологии и информационная безопасность»

4.1. Объём дисциплины в зачётных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	4
Общая трудоемкость в часах	144
Аудиторные занятия в часах, в том числе:	46
Лекции	16
Практические занятия	–
Лабораторные занятия	30
Самостоятельная работа в часах	62
Контроль	36
Форма промежуточной аттестации	Экзамен

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	16
Практические занятия	–
Лабораторные занятий	30
Консультации	2
Зачёт/зачёты	–
Экзамен/экзамены	0,66
Контроль	3
Курсовые проекты	-
Всего	51,66

5.Содержание дисциплины «Телекоммуникационные технологии и информационная безопасность», структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия			Самос.
			Всего	Лекции	Лабор.	
1	История и тенденции развития и основные понятия сетевых технологий	0,5/18	8	4	4	10
2	Средства управление сетями	0,33/12	4	2	2	8
3	Особенности построения сетей передачи данных	0,33/12	4	2	2	8
4	Понятие информационной безопасности и защищенной системы	0,33/12	4	2	2	8
5	Угрозы информационной безопасности	0,5/18	6	2	4	12
6	Защита информации	0,5/18	10	2	8	8
7	Криптографические и организационные методы защиты информации.	0,5/18	10	2	8	8
	ИТОГО:	3/108	46	16	30	60

5.2. Содержание:

Тема 1. История и тенденции развития и основные понятия сетевых технологий. Краткая историческая справка о развитии сетевых технологий. Основные термины и определения. Значение современных сетевых технологий для создания вооружений и военной техники. Классификация сетей; интеграция информационного сервиса пользователей; концепция архитектуры открытых систем как основа построения цифровых сетей интегрального обслуживания (ISDN). Базовые сетевые технологии. Основные этапы построения сетей. Модели процессов в сетях. Технология Ethernet. Технология Token Ring. Технология FDDI. Перспективные сетевые технологии. Технология Frame Relay; стек протоколов, перспективы использования сетей Frame Relay. ATM-технология; анализ и синтез топологической структуры магистральной и локальной сети. ISDN – цифровые сети интегрального обслуживания.

Архитектура узлов управления и коммутации ISDN; пакеты в ISDN. оценка эффективности сетей; перспективы развития ISDN; широкополосные B-ISDN.

Тема 2. Средства управление сетями. Административное и оперативное управление сетью; управление режимами коммутации; адаптивная коммутация; управление обменом информации в сетях; адаптивная маршрутизация.

Тема 3. Особенности построения сетей передачи данных. Идеология построения транспортной сети. Топологии сетей передачи данных, используемых в корпорациях и банках. Адресный план, архитектура построения и сетевые технологии. Функциональное назначение, возможности и технические характеристики составных элементов сети. Перспективные направления развития сетевых технологий.

Тема 4. Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

Тема 5. Угрозы информационной безопасности. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Тема 6. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации. Основные понятия теории информационной безопасности. Основные положения теории информационной безопасности информационных систем. Анализ способов нарушений безопасности. Классификация компьютерных вирусов и борьба сними. Среди всего разнообразия вирусов можно выделить следующие основные группы: загрузочные (бутовые) вирусы, файловые вирусы, загрузочно-файловые вирусы, основные свойства компьютерных вирусов, стелс–вирусы, полиморфные вирусы, макровирусы и др.

Тема 7. Криптографические и организационные методы защиты информации. Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Организационно-правовые методы информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и

стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

6. Методические материалы для обучающихся по освоению дисциплины «Телекоммуникационные технологии и информационная безопасность»

6.1. Самостоятельная работа обучающихся по дисциплине

№	Раздел (тема) дисциплины	Задание	Часы	Методические рекомендации	Формы контроля
	История и тенденции развития и основные понятия сетевых технологий	Написание реферата	10	Используйте литературу [2], [4]	Проверка реферата
	Средства управление сетями	Написание реферата	8	Используйте литературу [2], [4]	Проверка реферата
	Особенности построения сетей передачи данных	Изучение литературы	8	Используйте литературу [1], [5]	Устный опрос
	Понятие информационной безопасности и защищенной системы	Изучение литературы и Интернет-источников	8	Используйте литературу [1], [6]	Тестирование
	Угрозы информационной безопасности	Написание реферата	12	Используйте литературу [1], [4]	Проверка реферата
	Защита информации	Изучение литературы	8	Используйте литературу [2], [4]	Мониторинг
	Криптографические и организационные методы защиты информации.	Изучение литературы и Интернет-источников	8	Используйте литературу [1], [5]	Тестирование

6.3. Тематика и задания для лабораторных занятий

1-2. Составить программу в визуальной среде, реализующую шифр замены (код Цезаря).

3-4. Составить таблицы относительных частот букв русского и английского алфавитов на основе текстов, представленных в виде текстовых файлов.

5-6. Составить таблицы относительных частот пар букв русского и

английского алфавитов на основе текстов, представленных в виде текстовых файлов.

7-8. Реализовать кодирование/декодирование сохраненного в файле сообщения шифром подстановки (квадрат Полибия), как на русском, так и на английском языке, на основе матрицы-ключа.

9-10. Реализовать кодирование/декодирование сохраненного в файле сообщения многобуквенной системой шифрования (Таблица Вижинера), как на русском, так и на английском языке, на основе слова-ключа.

11-12. Реализовать кодирование/декодирование сохраненного в файле сообщения шифром Цезаря с ключом, как на русском, так и на английском языке, на основе слова-ключа.

13-14. Реализовать кодирование/декодирование сохраненного в файле сообщения парным шифром, как на русском, так и на английском языке, на основе слова-ключа.

15. Реализовать кодирование/декодирование сохраненного в файле сообщения XOR-кодированием (Схема С.Г. Вернам), как на русском, так и на английском языке, на основе слова-ключа.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины «Телекоммуникационные технологии и информационная безопасность»

а) основная:

1. Информатика : базовый курс / под ред. *С. В. Симоновича*. - 2-е изд. - СПб. : Питер, 2009. - 640 с. – 46 шт
2. Информационные системы и технологии в экономике и управлении : учебник для бакалавров / под ред. *В. В. Трофимова* ; Санкт-Петербургский гос. ун-т экономики и финансов (СПбГУЭФ). - 3-е изд., перераб. и доп. - М. : Юрайт, 2012. - 521, [1] с. – 2 шт
3. *Коноплева, Ирина Аполлоновна.* Управление безопасностью и безопасность бизнеса : учеб. пособие : допущено Минобрнауки / [под ред. И. А. Коноплевой]. - М. : ИНФРА-М, 2010. - 446, [2] с. – 2 шт

б) дополнительная:

4. *Пятибратов, Александр Петрович.* Вычислительные системы, сети и телекоммуникации : [учеб. пособие для студ. вузов] / под ред. А. П. Пятибратова. - М. : КНОРУС, 2013 . - 372 с. – 1 шт
5. *Бройдо, Владимир Львович.* Вычислительные системы, сети и телекоммуникации : [учеб. пособие для студ. высш. учеб. заведений]. - 4-е изд. - СПб. : Питер, 2011. - 554, [1] с. – 1 шт
6. *Гордукалова, Г. Ф.* Анализ информации: технологии, методы, организация : учеб.-практ. пособие. - СПб. : Профессия, 2009. - 508, [1] с. – 1 шт
7. Сети следующего поколения NGN / под ред. *А. В. Рослякова*. - М. : Эко-Трендз, 2008. - 424 с. – 1 шт

8. Стохастические методы и средства защиты информации в компьютерных системах и сетях / под ред. *И. Ю. Жукова*. - М. : КУДИЦ-ПРЕСС, 2009. - 512 с. – 1 шт
9. http://www.osp.ru (Издат. Открытые системы, новости по современным сетевым технологиям)
10. http://www.compres.ru (Журнал Компьютер-пресс)
11. http://www.ibxt.ru (Новости вычислительной техники)
12. http://www.infosecurity.report.ru
13. http://www.infosec.ru
14. http://www.intuit.ru/department/security/antiviruskasp/1/
15. http://support.kaspersky.ru/viruses/common?qid=180593219
16. http://av-school.ru/news
17. http://support.kaspersky.ru/viruses

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Информационно-образовательные ресурсы:

1. Библиотека ГОСТов. Все ГОСТы, [Электронный ресурс], URL:http://vsegost.com/

Электронные библиотечные системы:

1. ЭБС Университетская библиотека онлайн - http://biblioclub.ru
2. ЭБС «Лань» https://e.lanbook.com
3. ЭБС «ZNANIUM.COM» http://znanium.com

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория *228Е* для лекционных, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оборудование: посадочные места 16, рабочее место преподавателя. Имеется мультимедиа – компьютер (переносной) с проектором. Установлено 16 компьютеров.

Аудитория *227Е* для лекционных, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оборудование: посадочные места 15, рабочее место преподавателя. Имеется мультимедиа – компьютер (переносной) с проектором. Установлено 15 компьютеров.

Лицензионное программное обеспечение:

Windows 7 Pro лицензия 00180-912-906-507 постоянная-1шт.; LibreOffice 5.0, лицензия GNU LGPL; Microsoft Visual Studio 2013, лицензия;

Свободно распространяемое программное обеспечение:

– офисный пакет.