МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра интеллектуальных информационных радиофизических систем

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Защита информации в беспроводных сетях

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 17 апреля 2023 г., протокол № 8

Программа одобрена НМК
физического факультета
протокол № 5 от 25 апреля 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью преподавания дисциплины «Защита информации в беспроводных сетях» является изучение методов и средств построения защищенных беспроводных сетей передачи данных, а также ознакомление с основными принципами безопасности беспроводной передачи данных на физическом уровне.

2. Место дисциплины в структуре ОП магистратуры

Данная дисциплина относится к обязательной части Блока 1.

Полученные при изучении дисциплины знания создают необходимую базу для успешного выполнения научных исследований и написания выпускной квалификационной работы, а также в дальнейшей профессиональной деятельности для эффективного построения и эксплуатации программно-аппаратных технологий защиты передачи информации в беспроводных сетях связи.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП магистратуры

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД_УК-1.1 Осуществляет системный анализ задачи, выделяя ее базовые составляющие	**Знать:** – основные технологии и стандарты беспроводной передачи информации.; **Уметь:** – использовать основные метрики безопасности сеанса связи на физическом уровне; **Владеть навыками:** – обоснованного выбора модели беспроводного канала связи для конкретного практического сценария;

Общепрофессиональные компетенции		
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИД_ОПК-1.1 Способен на основе анализа информации о потенциальных рисках и угрозах, видах и возможностей нарушителей, целей и задач защиты, разработать и обосновать требования к системе обеспечения информационной безопасности	**Знать:** –технические характеристики основных беспроводных систем связи, сигналов и протоколов, применяемых для передачи различных видов данных; **Уметь:** **–** рассчитывать основные метрики безопасности сеанса связи на физическом уровне**;** **Владеть навыками:** **–** качественного и количественного сравнения безопасности сеанса связи на физическом уровне в условиях многолучевого распространения и замираний.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 акад. часа.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**						**Формы текущего контроля успеваемости** **Форма промежуточной аттестации** ***(по семестрам)***
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Основы построения и функционирования беспроводных сетей	1	8	2		2		4	Фронтальные опрос
2	Беспроводные каналы передачи информации	1	12	6		2		5	Коллоквиум, расчётное задание
3	Обеспечение безопасности на физическом уровне	1	12	8		2		8,7	Фронтальные опрос, коллоквиум, расчётное задание
	Всего		**32**	**16**	**0**	**6**	**0,3**	**17,7**	
		1					0,3		Зачет
	Всего с зачетом		**32**	**16**	**0**	**6**	**0,3**	**17,7**	

Содержание разделов (тем) дисциплины

Раздел 1

Основы построения и функционирования беспроводных сетей

Основные этапы развития радиоустройств: аппаратное, программное, когнитивное радио. Основы построения беспроводных сетей обработки данных. История развития. Используемые технологии и стандарты. Сети сотовой связи. Протоколы передачи данных в беспроводных сетях. Временной, частотный, кодовый, пространственный способы разделения доступа в беспроводных сетях. Организация физического и канального уровней. Методы модуляции BPSK, QPSK, DBPSK, DQPSK, QAM и представление данных на сигнальном созвездии.

Раздел 2

Беспроводные каналы передачи информации

Классификация моделей беспроводных каналов связи. Лучевые/детерминированные модели каналов связи. Статистические модели каналов связи. Примеры: Рэлеевский и Райсовский каналы. Понятие замираний в канале связи. Классификация замираний, их связь с физическими эффектами. Гибридные модели. Общее сравнение моделей. MIMO системы, особенности описания.

Раздел 3

Обеспечение безопасности на физическом уровне

Основные положения обеспечения безопасности на физическом уровне. Метрики безопасности физического уровня: общие сведение. Пропускная способность безопасного сеанса связи. Эргодическая пропускная способность безопасного сеанса связи. Вероятность прерывания безопасного сеанса связи. Снижение уровня безопасного сеанса связи безопасного сеанса связи. Классическая модель Вайнера канала с пассивной утечкой информации: общие положения. Классическая модель Вайнера канала с пассивной утечкой информации: возможные модификации и их виды. Критерии надежности передачи информации. Модель Вайнера канала с пассивной утечкой информации в условиях замираний: общее описание, постановка задачи оценки безопасной пропускной способности, качественные и количественные эффекты.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения проводятся лекции, практические и лабораторные занятия, в ходе которых используются следующие типы занятий и образовательные технологии.

Вводная лекция - ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Защита информации в беспроводных сетях» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты/видеозаписи лекций по отдельным темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- Microsoft Windows;
- программы Microsoft Office;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература:

1. Томаси, У. Электронные системы связи : руководство / У. Томаси. — Москва : Техносфера, 2016. — 1360 с. — ISBN 978-5-94836-125-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/89821 (дата обращения: 25.01.2022). — Режим доступа: для авториз. пользователей.

2. Пролубников, А. В. Сети передачи данных : учебное пособие : в 2 частях / А. В. Пролубников. — Омск : ОмГУ, 2020 — Часть 1 — 2020. — 116 с. — ISBN 978-5-7779-2466-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/142455 (дата обращения: 25.01.2022). — Режим доступа: для авториз. пользователей.
3. Белов В.М., Новиков С.Н., Солонска О.И. Теория информации. Курс лекций: учебное пособие для вузов. – М.: Горячая линия - Телеком, 2012. – 143с. URL: https://www.studentlibrary.ru/book/ISBN9785991202374.html

б) дополнительная литература

1. Hyadi A., Rezki Z., Alouini M. S. An overview of physical layer security in wireless communication systems with CSIT uncertainty //IEEE Access. – 2016. – Vol. 4. – P. 6121-6132.
2. Zou Y. et al. A survey on wireless security: Technical challenges, recent advances, and future trends //Proceedings of the IEEE. – 2016. – Vol. 104. – №. 9. – Pp. 1727-1765.
3. Nikoukar A. et al. Low-power wireless for the Internet of Things: Standards and applications //IEEE Access. – 2018. – Vol. 6. – Pp. 67893-67926.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);
- учебные аудитории для проведения лабораторных работ;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочим программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.группа обучающихся делится на две подгруппы).

Учебно-методическое обеспечение, необходимое для осуществления образовательного процесса по дисциплине включает в свой состав:

Автор:
Доцент кафедры инфокоммуникаций и радиофизики, к.ф.-м.н. А.С. Гвоздарёв

Приложение №1 к рабочей программе дисциплины
«Защита информации в беспроводных сетях»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1.1 Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

(данные задания выполняются студентом самостоятельно
и преподавателем в обязательном порядке не проверяются)

- Изучить историю развития беспроводных сетей.
- Определить основные тренды развития современных беспроводных сетей.
- Выделить ключевые плюсы и минусы использования временного, частотного, кодового и пространственного способов разделения сигналов.
- Изучить историю эволюции безопасности в беспроводных сетях.
- Ознакомиться с возможностями языка Ассемблера для написания вирусов, червей и троянов.
- Изучить современные антивирусные программы для абонентских терминалов сотовых сетей.
- Эволюция и современное состояние сетей сотовой связи.
- Криптографические алгоритмы, применяемые в сетях сотовой связи.
- Реализация генератора псевдослучайных чисел программным путем.

Примерные расчётные задания:

- Для модели канала с пассивной утечкой информации в условиях замираний доказать существование ненулевой пропускной способности безопасного сеанса связи.
- Для модели канала с пассивной утечкой информации в условиях замираний рассчитать безопасную пропускную способность как функцию соотношения сигнал шум устройства «прослушки».
- Для квазистатического Рэлеевского канала построить зависимость вероятности прерывания безопасного сеанса связи, как функцию соотношения сигнал шум устройства законного приёмника.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету:

1. Основы построения беспроводных сетей и история развития.
2. Технологии и стандарты современных беспроводных сетей.
3. Протоколы передачи данных в беспроводных сетях.
4. Временной, частотный, кодовый, пространственный способы разделения сигналов. Организация физического и канального уровней.
5. Методы модуляции BPSK, QPSK, DBPSK, DQPSK, QAM.
6. Классификация моделей беспроводных каналов связи.

7. Лучевые/детерминированные модели каналов связи.
8. Статистические модели каналов связи. Примеры: Рэлеевский и Райсовский каналы.
9. Понятие замираний в канале связи. Классификация замираний. Связь с физическими эффектами.
10. Гибридные модели. Общее сравнение моделей.
11. MIMO системы. Особенности описания.
12. Основные положения обеспечения безопасности на физическом уровне.
13. Метрики безопасности физического уровня: общие сведение.
14. Пропускная способность безопасного сеанса связи.
15. Эргодическая пропускная способность безопасного сеанса связи.
16. Вероятность прерывания безопасного сеанса связи.
17. Снижение уровня безопасного сеанса связи безопасного сеанса связи.
18. Классическая модель Вайнера канала с пассивной утечкой информации: общие положения.
19. Классическая модель Вайнера канала с пассивной утечкой информации: возможные модификации и их виды.
20. Классическая модель Вайнера канала с пассивной утечкой информации: критерии надежности передачи информации.
21. Модель Вайнера канала с пассивной утечкой информации в условиях замираний: общее описание, постановка задачи оценки безопасной пропускной способности.
22. Модель Вайнера канала с пассивной утечкой информации в условиях многолучевого распространения: качественные и количественные эффекты.

Правила выставления оценки на зачете.

Изучение дисциплины заканчивается зачетом. Во время подготовки к зачету предусмотрена групповая консультация.

Билет для зачета состоит из двух теоретических вопросов по материалам курса.

1. Теоретический вопрос в билете оценивается в 3 балла:

– 3 балла, если вопрос раскрыт более чем на 90% от требуемого объёма. При этом студент демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом; осуществляет межпредметные связи; умеет связывать теорию с практикой. Дает развернутые, полные и четкие ответы на вопрос билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.
– 2 балла, если вопрос раскрыт более чем на 70%, но менее, чем на 90% от требуемого объёма. При этом ответ в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.
– 1 балл, если вопрос раскрыт более чем на 50%, но менее чем на 70% от требуемого объёма. При этом студент демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагается в терминологически корректно, но допускаются ошибки в определениях и раскрытии некоторых основных понятий, формулировке положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Итоговая оценка высчитывается исходя из суммарного балла за оба вопроса билета.

В результате для получения оценки «зачтено» необходимо, чтобы суммарный балл был не ниже 4.

Приложение №2 к рабочей программе дисциплины
«Защита информации в беспроводных сетях»

Методические указания для студентов по освоению дисциплины

Основной формой занятий по дисциплине «Защита информации в беспроводных сетях» являются лекции и практические занятия. На лекциях излагается необходимый минимум теоретических сведений, ставятся вопросы, на которые надо найти ответ самостоятельно, даются рекомендации по побору литературы, даются отсылки к нормативной базе. Теоретический материал представляет собой компиляцию из огромного количества источников, поэтому материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и дополнять информацией, полученной из учебной и научной литературы.

На практических занятиях отрабатываются полученные знания, разбираются практические ситуации, приобретаются практические знания по работе с реальным оборудованием.

Для успешного освоения дисциплины обязательно выполнение всех домашних заданий, они являются формой текущей аттестации. В качестве заданий для самостоятельной работы дома предлагаются задания, аналогичные разобранным на практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых заданий. Некоторые задания относятся к категории заданий повышенной сложности, они подразумевают применение вычислительной техники с математическими пакетами, например, Matematica, MathCad, MATLAB, R, Stetistica или их бесплатных, свободно распространяемых аналогов, например, Octave, SciLAB, FreeMat и других или онлайн-вычислений (пользуйтесь любым удобным Вам способом). По окончании практического курса проводится контрольная работа, включающая в себя задания, интегрирующие множество мелких освоенных задач в один расчётный проект.