Компонент ОПОП 11.05.01 Радиоэлектронные системы и комплексы
Направленность (профиль) Инфокоммуникационные технологии и радиотехнические системы
наименование ОПОП

Б1.О.38
шифр дисциплины

РАБОЧАЯ ПРОГРАММА

Дисциплины (модуля) **Основы защиты информационных систем**

Разработчик (и):
Шульженко А.Е.
ФИО
старший преподаватель
должность

Утверждено на заседании кафедры
радиотехники и связи
наименование кафедры
протокол № 7 от 04.03.2025 года

И.о. заведующего кафедрой РТиС

А.Е. Шульженко

Мурманск
2025

Пояснительная записка

Объем дисциплины 3 з. е.

1. **Результаты обучения по дисциплине (модулю)**, соотнесенные с индикаторами достижения компетенций, установленными образовательной программой

Компетенции	Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ОПК – 7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИД-1 ОПК-7 решает стандартные задачи профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий; ИД-2 ОПК-7 решает задачи профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий**;** ИД-3 ОПК-7 владеет приёмами решения стандартных задач профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий	**знать:** - современные стандарты и средства управления сетями; принципы построения современных сетей связи - принципы работы современных информационных технологий **уметь:** проектировать и разрабатывать современные системы связи **владеть**: технологиями работы с современными сетями связи с применением принципов работы современных информационных технологий и использования их для решения задач профессиональной деятельности

2. **Содержание дисциплины (модуля)**

Тема 1. Законодательная база технической защиты информации в РФ

Основные нормативные правовые акты РФ определяющие область деятельности руководителей и ответственность должностных лиц за организацию защиты информации

Тема 2. Основные виды угроз безопасности информации. Основные свойства информации как объекта защиты. Демаскирующие признаки объектов защиты. Технические каналы утечки информации. Причины образования технических каналов утечки информации. Технические возможности перехвата информации. Возможные угрозы информационной безопасности

Тема 3. Защита автоматизированных система от несанкционированного доступа Концепция защиты АС от НСД к информации. Место защиты информации от НСД в рамках ЗИ. Основные способы НСД. Основные направления обеспечения защиты от НСД. Классы защищенности АС. Требования к показателям защищенности. Средства защиты АС от НСД и их возможности. Защита информации от НСД в ОС Windows

Тема 4. Основы криптографической защиты информации.

Криптосистемы: симметричные и ассиметричные. Требования к криптографическим системам. Криптоатаки. Базовые симметричные криптосистемы. Ассиметричные алгоритмы. Функции хэширования.

Тема 5. Сетевая безопасность. Межсетевые экраны. Антивирусная защита информации. Архитектура безопасности сети предприятия. Политика сетевой безопасности. Межсетевые экраны: виды и выполняемые задачи. Фильтрация трафика. Фильтрация трафика. Вредоносные программы. Технологии обнаружения вирусов. Режимы работы антивирусов. Комплексная система антивирусной защиты

3. Перечень учебно-методического обеспечения дисциплины (модуля)

- мультимедийные презентационные материалы по дисциплине (модулю) представлены в электронном курсе в ЭИОС МАУ;
- методические указания к выполнению практических и контрольных работ представлены в электронном курсе в ЭИОС МАУ;

4. Фонд оценочных средств по дисциплине (модулю)

Является отдельным компонентом образовательной программы, разработан в форме отдельного документа, представлен на официальном сайте МАУ в разделе «Информация по образовательным программам, в том числе адаптированным». ФОС включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля);
- задания текущего контроля;
- задания промежуточной аттестации;
- задания внутренней оценки качества образования.

5. Перечень основной и дополнительной учебной литературы (печатные издания, электронные учебные издания и (или) ресурсы электронно-библиотечных систем)

Основная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»
2. Горев, А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс]: учебно-практическое пособие/ А. И. Горев, А. А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016.— 88 с.— Режим доступа: http://www.iprbookshop.ru/72856.html.— ЭБС «IPRbooks»
3. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н. А. Руденков [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 368 с.— Режим доступа: http://www.iprbookshop.ru/73732.html.— ЭБС «IPRbooks»

Дополнительная литература

1. Лабораторный практикум по дисциплине Методы и средства защиты информации в компьютерных сетях [Электронный ресурс]/ — Электрон. текстовые

данные.— М.: Московский технический университет связи и информатики, 2015.— 58 с.— Режим доступа: http://www.iprbookshop.ru/61742.html.— ЭБС «IPRbooks»

2. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс]: учебное пособие для вузов/ В. И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 224 с.— Режим доступа: http://www.iprbookshop.ru/7007.html.— ЭБС «IPRbooks»

6. Профессиональные базы данных и информационные справочные системы

1) *Информационная система «Единое окно доступа к образовательным ресурсам»_- URL: http://window.edu.ru*
2) *«Документация к ПО MatLab» URL https://docs.exponenta.ru/*

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1) *Офисный пакет Microsoft Office 2007*
2) MatLab 2010

8. Обеспечение освоения дисциплины лиц с инвалидностью и ОВЗ

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

9. Материально-техническое обеспечение дисциплины (модуля) представлено в приложении к ОПОП «Материально-технические условия реализации образовательной программы» и включает:

- учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде МАУ;

Допускается замена оборудования его виртуальными аналогами.

10. Распределение трудоемкости по видам учебной деятельности

Таблица 1 - Распределение трудоемкости

Вид учебной деятельности	Распределение трудоемкости дисциплины (модуля) по формам обучения											
	Очная				Очно-заочная				Заочная			
	Семестр			Всего часов	Семестр			Всего часов	Семестр/Курс			Всего часов
	5								5			
Лекции	10			10								
Практические занятия												
Лабораторные работы	10			10								
Самостоятельная работа	52			52								

Подготовка к промежуточной аттестации	36			36								
Всего часов по дисциплине / из них в форме практической подготовки				**108**								
				10								

Формы промежуточной аттестации и текущего контроля

Экзамен	+											
Зачет/ зачет с оценкой	-											
Курсовая работа (проект)	-											
Количество расчетно-графических работ	1											
Количество контрольных работ	-											

Перечень лабораторных работ по формам обучения

№ п\п	**Темы лабораторных работ**
1	**2**
	Очная форма
1.	Правовые и методические основы ТЗИ в РФ
2.	Настройка безопасности в операционной системе Windows
3.	Разработка дискреционной матрицы доступа в АС
4.	Применение блочного метода шифрования «сеть Фейстеля»
5.	Исследование межсетевого экрана ОС Windows