

**Компонент ОПОП 25.05.03 Техническая эксплуатация транспортного радиооборудования**  
**Специализация Информационно-телекоммуникационные системы на транспорте**  
**и их информационная защита**  
наименование ОПОП

**Б1.В.14**  
шифр дисциплины

**РАБОЧАЯ ПРОГРАММА**

**Дисциплины**  
**(модуля)**

**Кибербезопасность компьютеризированных систем**

Разработчик (и):

Шульженко А.Е.

ФИО

старший преподаватель

должность

Утверждено на заседании кафедры

радиотехники и связи

наименование кафедры

протокол № 8 от 06.03.2024 года

Заведующий кафедрой радиотехники и связи



Борисова Л.Ф.

**Мурманск**  
**2024**

## Пояснительная записка

Объем дисциплины 4 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)
<b>ПК-3</b> Способен осуществлять обнаружение, анализ и диагностику неисправностей	ИД-1 ПК-3 знает основные законодательные акты и нормативные документы, применяемые при построении систем защиты информации ИД-2 ПК-3 применяет статьи законодательных актов в области технической защиты информации ИД-3 ПК-3 разрабатывает комплексные мероприятия по анализу и диагностике систем защиты информации	<b>знать:</b> Основные законодательные акты и нормативные документы, применяемые при построении систем защиты информации <b>уметь:</b> Применять статьи законодательных актов в области технической защиты информации <b>владеть:</b> навыками построения системы безопасности информации

2. **Содержание дисциплины (модуля)**

**Тема 1. Законодательная база технической защиты информации в РФ.** Актуальность проблемы обеспечения безопасности информации. Основные законодательные акты РФ и нормативно-методические рекомендации ФСТЭК РФ.

**Тема 2. Построение комплексной системы защиты информации на предприятии.** Виды мер обеспечения информационной безопасности. Основные принципы построения систем защиты информации. Системно-концептуальный подход к защите информации, Основные проблемы реализации систем защиты информации

**Тема 3. Защита автоматизированных систем от несанкционированного доступа к информации.** Концепция защиты АС от НСД к информации. Модель нарушителя. Направления ЗИ. Защита АС от НСД к информации. Классификация АС. Требования к классам защищенности. Системы защиты информации от НСД.

**Тема 4. Системы криптографической защиты информации. Хэш функции.** Криптографические системы с открытым и закрытым ключом: 4 базовых класса моно- и многоалфавитные подстановки, перестановки, блочные шифры, гуммированные требования к криптографическим системам. Свойства хэш - функций

**Тема 5. Технические каналы утечки информации.** Классификация и краткая характеристика технических каналов утечки информации. СЗИ от утечки по техническим каналам.

**Тема 6. Аттестация объектов информатизации.** Нормативные документы по аттестации объектов информатизации. Порядок аттестации объектов информатизации по требованиям безопасности информации. Типовое содержание программы аттестационных испытаний.

**Тема 7. Антивирусная защита.** Классификация компьютерных вирусов. Технологии обнаружения вирусов. Режимы работы антивирусов

**Тема 8. Защита информации в локальных сетях.** Межсетевые экраны. Классификация МЭ. Требования к классам защищенности.

### **3. Перечень учебно-методического обеспечения дисциплины (модуля)**

- мультимедийные презентационные материалы по дисциплине (модулю) представлены в электронном курсе в ЭИОС МАУ;
- методические указания к выполнению лабораторных 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/ Горев А.И., Симаков А.А.— 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;
- лаборатория 506В

**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	
	7								9			
Лекции	30			30					6			6
Практические занятия												
Лабораторные работы	18			18					8			8
Самостоятельная работа				96								126
Подготовка к промежуточной аттестации												4
<b>Всего часов по дисциплине</b>				<b>144</b>								<b>144</b>
/ из них в форме практической подготовки				18								8

**Формы промежуточной аттестации и текущего контроля**

Экзамен	-								-			
Зачет/зачет оценкой	с	+							+			-

Курсовая работа (проект)	-									-				-
Количество расчетно-графических работ	1									1				
Количество контрольных работ	-													-
Количество рефератов	-													-
Количество эссе	-													-

### Перечень лабораторных работ по формам обучения

№ п\п	Темы лабораторных работ
<b>1</b>	<b>2</b>
	<b>Очная форма</b>
1.	Настройки безопасности в ОС windows
2.	Разработка дискреционной матрицы доступа
3.	Настройка прав доступа к информационным ресурсам в ОС Linux
4.	Применение блочного метода шифрования «Сеть Фейстеля»
5.	Вычисление хэш-функции по алгоритму Эль-Гамалья
6.	Измерение ПЭМИ АРМ на базе ПЭВМ
7.	Анализ параметров информационного сигнала н входе средства перехвата
	<b>Заочная форма</b>
1.	Настройки безопасности в операционной системе windows
2.	Применение блочного метода шифрования «Сеть Фейстеля»
3.	Вычисление хэш-функции по алгоритму Эль-Гамалья
4.	Измерение ПЭМИ АРМ на базе ПЭВМ