МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МУРМАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор ИМА

Баева Л. С.
Ф.И.О.

подпись

«23» января 2019 года

РАБОЧАЯ ПРОГРАММА

Дисциплина **Б1.Б.44 Основы защиты информационных систем**
код и наименование дисциплины

Направление подготовки/специальность 11.05.01 Радиоэлектронные системы и комплексы
код и наименование направления подготовки /специальности

Направленность/специализация специализация №2 "Радиоэлектронные системы передачи информации"
наименование направленности (профиля) /специализации образовательной программы

Квалификация выпускника специалист
указывается квалификация (степень) выпускника в соответствии с ФГОС ВО

Кафедра-разработчик Радиоэлектронных систем и транспортного радиооборудования
наименование кафедры-разработчика рабочей программы

Мурманск
2019

Лист согласования

1 Разработчик(и)

Ст. преподаватель	РЭСиТРО			Шульженко А.Е.
Часть 1 должность	кафедра		подпись	Ф.И.О.
Часть 2 должность	кафедра		подпись	Ф.И.О.
Часть 3 должность	кафедра		подпись	Ф.И.О.

2. Рассмотрена и одобрена на заседании кафедры-разработчика рабочей программы

Радиоэлектронных систем и транспортного радиооборудования 23.01.2019 г.
наименование кафедры дата

Протокол № 8 _____ Борисова Л.Ф.
подпись Ф.И.О. заведующего кафедры – разработчика

3*. Рабочая программа СОГЛАСОВАНА с выпускающей кафедрой по направлению подготовки /специальности.

Заведующий выпускающей кафедрой _____
наименование кафедры

_____ _____ _____
дата подпись Ф.И.О.

* *Если кафедра-разработчик является выпускающей, то пункт не заполняется.*

Лист изменений и дополнений, вносимых в РП*

к рабочей программе по дисциплине, входящей в состав ОПОП по направлению специальности 11.05.01Радиоэлектронные системы и комплексы, специализации №2 Радиоэлектронные системы передачи информации, 2017 года начала подготовки.

Таблица 1 Изменения и дополнения

№ п/п	Дополнение или изменение, вносимое в рабочую программу в части	Содержание дополнения или изменения	Основание для внесения дополнения или изменения	Дата внесения дополнения или изменения
1	Титульного листа			
2	Листа утверждений			
3	Структуры учебной дисциплины (модуля)			
4	Содержания учебной дисциплины (модуля)			
5	Методического обеспечения дисциплины (модуля)			
6	Структуры и содержания ФОС			
7	Рекомендуемой литературы			
8	Перечня интернет ресурсов (ЭБС)			
9	Перечня лицензионного программного обеспечения, профессиональных баз данных и информационных справочных систем			
10	Перечня МТО			

Дополнения и изменения внесены «____»_____ _____г

* *Изменения и дополнения в РП п. 1-8,10 таблицы 1 вносятся по необходимости; п. 9 требует ежегодного обновления. Листы изменений и дополнений включаются в структуру РП, их количество соответствует количеству вносимых изменений и дополнений*

Аннотация рабочей программы дисциплины

Коды циклов дисциплин, модулей, практик	Наименование циклов, разделов, дисциплин, модулей, практик	Краткое содержание (Цель, задачи, содержание разделов дисциплины, реализуемые компетенции, формы промежуточной аттестации)
1	2	3
Б1.Б.44	Основы защиты информационных систем	**Цель дисциплины**: Подготовить специалиста, владеющего основными положениями теории в соответствии с квалификационной характеристикой специалиста и учебным планом специальности 11.05.01 «Радиоэлектронные системы и комплексы». **Задачи дисциплины:** – изучить состав и содержание организационных и технических мер по обеспечению безопасности информации при ее обработке в информационных системах различного назначения – изучить правовые и организационные основы технической защиты информации – изучить методы и процедуры выявления угроз безопасности информации на объектах информатизации и оценки степени их опасности; – сформировать систему знаний практической отработкой способов и порядка проведения работ по ТЗИ; – изучить методы оценки состояния ТЗИ. – изучить нормативные правовые акты Российской Федерации в области защиты информации **В результате изучения дисциплины студент должен:** ***знать:*** - нормативные правовые акты Российской Федерации в области защиты информации, нормативные и методические документы в области технической защиты информации; – физические основы возникновения, классификацию и характеристики типовых каналов утечки информации и других угроз безопасности информации; – требования к средствам технической защиты информации, контроля технической защиты информации; – средства ТЗИ, возможности и порядок применения, перспективы развития; – виды юридической ответственности за нарушение законодательства Российской Федерации в области защиты информации. ***уметь:*** – различать между собой общедоступную информацию и информацию ограниченного доступа; – толковать и применять в профессиональной деятельности основные нормативно – правовые акты, регулирующие порядок работы с информацией, ограниченного доступа; – использовать полученные знания для защиты информации конфиденциального характера

		– определять возможные каналы утечки и другие угрозы безопасности информации; – определять требования к техническим, программным программно-техническим средствам, предназначенным для хранения, обработки и передачи информации ограниченного доступа; – применять действующую нормативную правовую и методическую базу в области ТЗИ; ***владеть:*** – навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; – криптографической терминологией; – навыками работы с нормативными правовыми актами; – методами формирования требований по защите информации; – методами технической защиты информации; **Содержание разделов дисциплины:** **Раздел 1.** Законодательная база технической защиты информации в РФ. **Раздел 2.** Основные виды угроз безопасности информации **Раздел 3.** Концепция построения систем защиты информации **Раздел 4.** Защиты автоматизированных система от несанкционированного доступа **Раздел 5.** Защита информации в электронных платежных системах **Раздел 6.** Основы криптографической защиты информации **Раздел 7.** Межсетевые экраны **Раздел 8.** Антивирусная защита информации **Реализуемые компетенции:** **ФГОС ВО** ОПК-1 **Формы отчетности:** Курс 3 – зачет, контрольная работа.

Пояснительная записка

1. Рабочая программа составлена на основе ФГОС ВО по направлению подготовки/ специальности 11.05.01 "Радиоэлектронные системы и комплексы»,
(код и наименование направления подготовки /специальности)

утвержденного №1031 от 11.08.2016 ,учебного плана
дата, номер приказа Минобрнауки РФ

в составе ОПОП по направлению подготовки/специальности 11.05.01 "Радиоэлектронные системы и комплексы», направленности специализации "Радиоэлектронные системы передачи информации" , 2017 года начала подготовки.

2. Цели и задачи учебной дисциплины (модуля)

Целью дисциплины (модуля) «Основы защиты информационных систем» является формирование компетенций в соответствии с квалификационной характеристикой специалиста и учебным планом для специальности 11.05.01 "Радиоэлектронные системы и комплексы"

Задачи:

– изучить состав и содержание организационных и технических мер по обеспечению безопасности информации при ее обработке в информационных системах различного назначения

– изучить правовые и организационные основы технической защиты информации

– изучить методы и процедуры выявления угроз безопасности информации на объектах информатизации и оценки степени их опасности;

– сформировать систему знаний практической отработкой способов и порядка проведения работ по ТЗИ;

– изучить методы оценки состояния ТЗИ.

– изучить нормативные правовые акты Российской Федерации в области защиты информации

3. Требования к уровню подготовки специалиста в рамках данной дисциплины

Процесс изучения дисциплины «Основы защиты информационных систем» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по направлению подготовки

Таблица 3.1 - Результаты обучения

№ п/п	Код и содержание компетенции	Степень реализации компетенции	Этапы формирования компетенции (Индикаторы сформированности компетенций)[†]
1.	ОПК – 1 Способен решать стандартные задачи профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий	Компетенция реализуется в части обеспечения информационной безопасности при работе в информационных системах	**Знать:** современные принципы поиска, хранения, обработки, анализа и представления в требуемом формате информации **Уметь:** решать задачи обработки данных с помощью современных средств автоматизации **Владеть:** навыками обеспечения информационной безопасности

[†] *Для ФГОС ВО 3*

4. Структура и содержание учебной дисциплины (модуля)

Таблица 4.1 - Распределение учебного времени дисциплины
Общая трудоемкость дисциплины составляет __2__ зачетных единиц, __72__ часов

Вид учебной нагрузки	Распределение трудоемкости дисциплины по формам обучения			
	Заочная			
	Семестр/курс			Всего часов
	3			
Лекции	4			4
Практические работы	4			4
Лабораторные работы				
Контактная работа для выполнения курсовой работы (проекта)	-			-
Самостоятельная работа	60			60
Выполнение курсовой работы (проекта)	-			
Подготовка к промежуточной аттестации	4			4
Всего часов по дисциплине	72			72

Формы промежуточной аттестации и текущего контроля

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

Таблица 4.2[*] - Содержание разделов дисциплины (модуля), виды работы

Содержание разделов (модулей), тем дисциплины	Количество часов, выделяемых на виды учебной подготовки по формам обучения			
	Заочная			
	Л	ЛР	ПР	СР
Раздел 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	-	-	-	7
Раздел 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	1	-	-	7
Раздел 3. **Концепция построения систем защиты информации**. Меры защиты компьютерных систем. Основные принципы построения систем защиты АС. Системно-концептуальный подход к защите информации. Принципы построения комплексной системы защиты информации.	-	2	-	8
Раздел 4. **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	1	-	-	8
Раздел 5. **Защита информации в электронных платежных системах.** Принцип функционирования электронной платежной системы. Платежные карты. Аутентификация магнитной и EMV-карты. Транзакции в платежных системах.	-	-	-	8
Раздел 6. **Основы криптографической защиты информации.** Криптосистемы: симметричные и ассиметричные. Требования к криптографическим системам. Криптоатаки. Базовые симметричные криптосистемы. Ассиметричные алгоритмы. Функции хэширования.	1	-	-	8

[*] *Разработчикам РП можно убирать столбцы с формами обучения, если данная форма не реализуется в МГТУ*

Раздел 7. Сетевая безопасность. Межсетевые экраны. Архитектура безопасности сети предприятия. Политика сетевой безопасности. Межсетевые экраны: виды и выполняемые задачи. Фильтрация трафика.	1	-	2	7
Раздел 8. Антивирусная защита информации. Фильтрация трафика. Вредоносные программы. Технологии обнаружения вирусов. Режимы работы антивирусов. Комплексная система антивирусной защиты	-	-	-	7
Итого:	4		4	60

Таблица 4.3 - Соответствие компетенций, формируемых при изучении дисциплины (модуля), и видов занятий с учетом форм текущего контроля

Перечень компетенций	Виды занятий								Формы контроля
	Л	ЛР	ПР	КР/ КП	р	к/р	э	СР	
ОПК-1	+	-	+	-	-	+	-	+	Тест, отчет по практической работе, конспект

Примечание: Л – лекции, ЛР – лабораторные работы, ПР – практические работы, КР/КП – курсовая работа (проект), р – реферат, к/р – контрольная работа, э - эссе, СР – самостоятельная работа

Таблица 4.4 - Перечень лабораторных работ

№ п\п	Наименование лабораторных работ	Количество часов		
		Очная	Очно-заочная	заочная
1	2	3	4	

Не предусмотрено учебным планом

Таблица 4.5 - Перечень практических работ

№ п\п	Темы лабораторных работ	Количество часов		
		Очная	Очно-заочная	Заочная
1	2	3	4	5
3	Настройка безопасности в операционной системе windows	4	-	-
6	Исследование межсетевого экрана ос Windows	2	-	-

Перечень примерных тем курсовой работы (проекта)

НЕ ПРЕДУСМОТРЕНО УЧЕБНЫМ ПЛАНОМ

---

6. Перечень учебно-методического обеспечения дисциплины (модуля)

1. Методические указания для практических работ по дисциплине «Основы защиты информационных систем» для специальности 11.05.01 «Радиоэлектронные системы и комплексы»
2. Методические указания для выполнения контрольной работы по дисциплине «Основы защиты информационных систем» для специальности 11.05.01 «Радиоэлектронные системы и комплексы»

---

7. Фонд оценочных средств (является компонентом ОП, разрабатывается в форме отдельного документа) и включает в себя:

Фонд оценочных средств является компонентом ОП, разрабатывается в форме отдельного документа и включает в себя критерии оценивания сформированности компетенций на различных этапах их формирования и процедуры оценивания.

8. Перечень основной и дополнительной учебной литературы

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»

9. Перечень ресурсов информационно - телекоммуникационной сети «Интернет»

1. Электронно-библиотечная система ЭБС - http://www.rucont.ru/
2. ЭБС издательства "ЛАНЬ" - http://e.lanbook.com
3. ЭБС BOOK.ru - http://book.ru/
4. ЭБС ibooks.ru - http://ibooks.ru/
5. ЭБС znanium.com издательства "ИНФРА-М" - http://www.znanium.com
6. ЭБС НИТУ "МИСиС" - http://lib.misis.ru/registr.html

10. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, реквизиты подтверждающего документа. (Пример)

1. MS Office 2007

11. Материально-техническое обеспечение дисциплины (модуля)

Таблица 11.1 - Материально-техническое обеспечение

№ п./п.	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	512 В Учебная аудитория для проведения занятий лекционного и семинарского типа, практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации	Мультимедийный проектор Epson – 1 шт. Переносной ноутбук Samsung – 1 шт. Посадочных мест – 20
2.	**213С** Специальное помещение для самостоятельной работы	Укомплектовано специализированной мебелью и техническими средствами обучения: – доска аудиторная – 1 шт. – персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета: Intel(R) Core(TM) 2 DUO CPU E7200 2,53 ГГц, 1 Гб ОЗУ – 2 шт.; Intel(R) Pentium(R) CPU G840 2,8 ГГц, 2 Гб ОЗУ – 3 шт.; Intel(R) Celeron(R) CPU 2,8 ГГц, 1 Гб ОЗУ – 1 шт.; Intel(R) Pentium(R) 4CPU 2,8 ГГц, 1,5 Гб ОЗУ – 1 шт.; Посадочных мест – 11 1. Операционная система Microsoft Windows XP Professional ver 2002 Service Pack 3, лицензия №44335756 от 29.07.2008 г. (договор №32/379 от 14.07.08 г.) 2. Офисный пакет Microsoft Office 2007 Russian Academic OPEN, лицензия № 45676388 от 08.07.2009 (договор 32/224 от 14.07.2009 г.) 3. Офисный пакет Microsoft Office 2010 Russian Academic OPEN, лицензия № 47233444 от 30.07.2010 (договор 32/285 от 27 июля 2010 г.) 4. Wolfram Mathematica Professional (Network Server, Network Increment) 8.x/9.x (сетевая версия), номер лицензии L3477-6735 от 20.11.2012 (договор 26/32/277 от 15 ноября 2012 г.) 5. MathWorks MATLAB 2009 /2010 (сетевая версия) License Number 619865 от 11.12.2009 (договор 32/356 от 10 декабря 2009 г.) 6. Microsoft Visual Studio 2010 Professional – участие в академической программе Microsoft Imagine Premium (700514554) (счет (договор-оферта)

		№Tr000159698 от 18.05.2017 г.)
3.	506 В «Компьютерный класс» Учебная аудитория для проведения занятий лекционного типа, практических и лабораторных занятий, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации.	506В: Количество столов - 8 Количество стульев - 16 Посадочных мест - 16 Доска аудиторная - 1 ПК для проведения виртуальных лабораторных и практических работ - 7 шт. Программное обеспечение: Операционная система Microsoft Windows XP Professional Service Pack 3 (подписка на образовательные лицензии, сетевые версии), участие в академической программе Microsoft Azure Dev Tools for Teaching (с февраля 2019 г., ранее Microsoft Imagine, ранее Microsoft DreamSpark, ранее Microsoft MSDN Academic Alliance). Подписки действительны по 10.12.2019 (счет-фактура №IM22116 от 12.11.2018, счет №9552401799 от 10.12.2018)

Таблица 12 - Технологическая карта дисциплины (промежуточная аттестация -зачет)

Дисциплина _Основы защиты информационных систем_____

№	Контрольные точки	Зачетное количество баллов		График прохождения (неделя сдачи)
		min	max	
	Текущий контроль			
1.	**Посещение лекций (2 лекций)**	20	30	15-ая неделя
	Нет посещений – 0 баллов, 1 лекция – 20 баллов, 2 лекции – 30 баллов			
2.	**Выполнение практических работ (2 раб.)**	20	30	По расписанию
	Выполнение одной п/р : 7,5 балла - отлично, 5 балла – хорошо. 4 балла – удовл.,(выполнение фиксируется преподавателем)			
3.	**Контрольная работа**	20	40	10,14-ая неделя
	Одна к/р – от 20 до 40 баллов. Отлично – 40 баллов, хорошо – 30 баллов, удовлетворительно – 20 баллов			
	ИТОГО за работу в семестре	**60**	**10**	15-ая неделя
	1. Если обучающийся набрал зачетное количество баллов согласно установленному диапазону по дисциплине с зачетом, то он считается аттестованным. **2. Если обучающийся набрал зачетное количество баллов согласно установленному диапазону по дисциплине с дифференцированным зачетом, то он считается аттестованным с оценкой согласно шкале баллов для определения итоговой оценки:** 91 - 100 баллов - оценка «5», 81-90 баллов - оценка «4», 60- 80 баллов - оценка «3». **Итоговая оценка** проставляется в экзаменационную ведомость и зачетку обучающегося			

Таблица 13 - Ведомость для фиксирования результатов текущего контроля (промежуточная аттестация –зачет)

(заполняется преподавателем в последний рабочий день месяца)

ФИО	Количество баллов			
	Посещение лекций	Выполнение практич. работ	Выполнение к/р	Итого