

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное
образовательное учреждение высшего образования

«Московский технический университет связи и информатики» (МТУСИ)
Волго-Вятский филиал

УТВЕРЖДЕНА
(с учетом изменений и дополнений)
на заседании кафедры
инфокоммуникационных
и профессиональных дисциплин
Протокол заседания № 1
от «30» августа 2021 г.

Рабочая программа дисциплины

«Основы информационной безопасности»

Направление подготовки

11.03.02 «Инфокоммуникационные технологии и системы связи»

Направленность (профиль) программы

«Инфокоммуникационные системы и сети»


Квалификация (степень) выпускника

Бакалавр


Форма обучения

Очная, Заочная

Москва 2020 г.

Заведующий кафедрой ИКиПД
 В.В. Мазниченко

Авторы:


Ст. преподаватель кафедры
ИКиПД, Сочнева Н.В.

Разработано на основе Федерального
государственного образовательного стандарта
высшего образования по направлению
подготовки

11.03.02

**Инфокоммуникационные технологии и
системы связи,**

утверждённого приказом Министерства
образования и науки РФ от 19 сентября 2017 г. №
930.

1. Цели освоения дисциплины

Целями освоения дисциплины являются развитие у обучающихся творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства. Развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления, привитие стремления к поиску оптимальных, простых и надежных решений. Расширение кругозора в области обеспечения информационной безопасности государства, методологии создания систем защиты информации.

Основными задачами дисциплины является изучение терминологического и понятийного аппарата теории информационной безопасности, основных методов защиты информации от базовых угроз, методов и средств ведения информационных войн. А также получение навыков оценки защищенности и обеспечения информационной безопасности.

В результате изучения настоящей дисциплины обучающиеся должны получить знания, имеющие не только самостоятельное значение, но и обеспечивающие базовую подготовку для усвоения ряда последующих дисциплин в области инфокоммуникационных технологий.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» включена в обязательную часть блока дисциплин учебного плана «Инфокоммуникационные системы и сети» (Б1.О.18). Дисциплина «Основы информационной безопасности» реализуется в соответствии с требованиями ФГОС, ОПОП ВО и Учебного плана по направлению подготовки *11.03.02 «Инфокоммуникационные технологии и системы связи», (направленность (профиль) программы Инфокоммуникационные системы и сети).*

Изучение дисциплины должно опираться на знания, умения и компетенции, полученные обучающимися при изучении следующих предшествующих дисциплин: «Вычислительная техника », «Информатика» и др. В свою очередь, данный курс, помимо самостоятельного значения, является предшествующей дисциплиной для курсов: «Основы криптографии»; «Инфокоммуникационные системы и сети ».

Рабочая программа дисциплины «Основы информационной безопасности» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа). Процесс изучения дисциплины реализуется при очной форме обучения в 4 семестре, при заочной форме обучения в 5 семестре. Промежуточная аттестация предусматривает зачет.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индекс индикатора достижения компетенции	Содержание индикатора достижения компетенции
	ОПК-2	Способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных	ОПК-2.1	Находит и критически анализирует информацию, необходимую для решения поставленной задачи
	ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.1	Знает основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и трактам телекоммуникационных систем
	ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.2	Знает принципы, основные алгоритмы и устройства цифровой обработки сигналов; принципы построения телекоммуникационных систем различных типов и способы распределения информации в сетях связи
	ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.3	Умеет решать задачи обработки данных с помощью средств вычислительной техники
	ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.5	Владеет методами и навыками обеспечения информационной безопасности

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ семестрам представлено в таблице 2.

Распределение трудоёмкости дисциплины по видам работ по семестрам ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2а

Вид учебной работы	Трудоёмкость			
	час.	В т.ч. по семестрам		Из них практическая подготовка
		4		
Общая трудоёмкость дисциплины по учебному плану	72	72		
1. Контактная работа:	30	30		
Аудиторная работа				
<i>лекции (Л)</i>	14	14		
<i>практические занятия (ПЗ)</i>	16	16		
<i>лабораторные работы (ЛР)</i>	-	-		
2. Общая самостоятельная работа и контроль	42	42		
<i>курсовая работа/проект (КР/КП) (подготовка)</i>	-	-		
<i>самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.) (СР), иная контактная работа (ИКР) и подготовка к зачету (при его наличии):</i>	33	33		
<i>Подготовка к зачету</i>	9	9		
Вид промежуточного контроля:	Зачет			

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2б

Вид учебной работы	Трудоёмкость			
	час.	В т.ч. по семестрам		Из них практическая подготовка
		5		
Общая трудоёмкость дисциплины по учебному плану	72	72		
1. Контактная работа:	6	6		
Аудиторная работа				
<i>лекции (Л)</i>	2	2		
<i>практические занятия (ПЗ)</i>	4	4		
<i>лабораторные работы (ЛР)</i>	-	-		
2. Общая самостоятельная работа и контроль	66	66		
<i>курсовая работа/проект (КР/КП) (подготовка)</i>	-	-		

Вид учебной работы	Трудоёмкость			
	час.	В т.ч. по семестрам		Из них практическая подготовка
		5		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.) (СР), иная контактная работа (ИКР) и подготовка к зачету (при его наличии):	57	57		
Подготовка к зачету	9	9		
Вид промежуточного контроля:	Зачет			

4.2 Содержание дисциплины

Тематический план учебной дисциплины ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3а

Наименование разделов дисциплины	Всего	Аудиторная работа			Внеаудиторная работа СР
		Л	ПЗ	ЛР	
Раздел 1 Основные термины и определения теории ИБ	18	4	6	-	8
Раздел 2 Основные методы защиты информации от базовых угроз	16	4	4	-	8
Раздел 3 Стандарты информационной безопасности	16	4	4	-	8
Раздел 4 Проблематика построения систем защиты информации	13	2	2	-	9
Всего за 4 семестр	63	14	16	-	33
<i>Зачет</i>	9	-	-	-	9
Итого по дисциплине	72	14	16	-	42

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3б

Наименование разделов дисциплины	Всего	Аудиторная работа			Внеаудиторная работа СР
		Л	ПЗ	ЛР	
Раздел 1 Основные термины и определения теории ИБ	16,5	0,5	1	-	15
Раздел 2 Основные методы защиты информации от базовых угроз	16,5	0,5	1	-	15
Раздел 3 Стандарты информационной безопасности	13,5	0,5	1	-	12
Раздел 4 Проблематика построения систем защиты информации	16,5	0,5	1	-	15
Всего за 4 семестр	63	2	4	-	57
<i>Зачет</i>	9	-	-	-	9
Итого по дисциплине	72	2	4	-	66

4.3 Лекции/лабораторные/практические/ занятия

Содержание лекций/лабораторного практикума/практических занятий ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 4а

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол-во Часов
1.	Раздел 1. Основные термины и определения теории ИБ			
	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Лекция № 1. Понятие национальной безопасности. Виды безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства. Базовые свойства информации как объекта защиты	ОПК-3.1	2
		Практическая работа № 1. Виды защищаемой информации. Носители информации	ОПК-2.1 ОПК-3.5	2
	Тема 2. Основные термины и определения теории ИБ	Лекция № 2. Угрозы, уязвимые элементы и риски информационной безопасности	ПК-3.2	2
		Практическая работа № 2. Связь и взаимное влияние базовых свойств информации как объекта защиты. Методы построения полного списка угроз.	ПК-2.1 ПК-3.3	2
		Практическая работа № 3. Модель нарушителя информационной безопасности. Информационные ресурсы информационной системы. Способы оценки рисков информационной безопасности.	ПК-2.1 ПК-3.3	2
2.	Раздел 2. Основные методы защиты информации от базовых угроз			
	Тема 3. Основные методы защиты информации от базовых угроз	Лекция № 3. Основные методы защиты от угроз нарушения конфиденциальности информации.	ПК-3.1	2
		Лекция № 4. Основные методы защиты от угроз нарушения целостности и доступности информации.	ПК-3.2	2
		Практическая работа № 4. Способы разграничения доступа к информации в информационной системе. Идентификация и аутентификация.	ПК-3.5 ПК-3.5	2
		Практическая работа № 5. Модели обеспечения целостности. Модель Кларка-Вилсона. Модель Биба. Методы обеспечения доступности информации: резервирование и дублирование в информационной системе.	ПК-2.1 ПК-3.5	2
3.	Раздел 3. Стандарты информационной безопасности			
	Тема 4. Стандарты информационной безопасности	Лекция № 5. Стандарты информационной безопасности. Роль стандартов. Основные оценочные стандарты.	ПК-3.1	2
		Лекция № 6. Стандарты информацион-	ПК-3.1	2

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол-во Часов
		ной безопасности. Основные управленческие стандарты (спецификации). Понятие об управлении информационной безопасностью		
		Практическая работа № 6. Оценочные стандарты 1-го поколения: Оранжевая книга, РД ФСТЭК. Оценочные стандарты. «Общие критерии». Основные подходы к оценке. Среда безопасности.	ПК-3.5 ПК-3.3	2
		Практическая работа № 7. Управленческие стандарты. Стандарты серии BS. Управление информационной безопасностью, управление рисками. Управленческие стандарты. Сетевая безопасность. Основные требования спецификации X.800.	ПК-3.5 ПК-3.3	2
4.	Раздел 4. Проблематика построения систем защиты информации			
	Тема Проблематика построения СЗИ	Лекция № 7. Функциональная модель системы защиты информации. Проблемы защиты информации в системах.	ПК-3.1	2
		Практическая работа № 8. Показатели уязвимости и защищенности в информационных системах. Компоненты функциональной модели системы защиты информации.	ПК-2.1 ПК-3.3	2

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 46

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол-во Часов
1.	Раздел 1. Основные термины и определения теории ИБ			
	Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Лекция № 1. Понятие национальной безопасности. Виды безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства. Базовые свойства информации как объекта защиты	ОПК-3.1	0,25
		Практическая работа № 1. Виды защищаемой информации. Носители информации	ОПК-2.1 ОПК-3.5	0,5
	Тема 2. Основные термины и определения теории ИБ	Лекция № 2. Угрозы, уязвимые элементы и риски информационной безопасности	ПК-3.2	0,25
		Практическая работа № 2. Связь и взаимное влияние базовых свойств информации как объекта защиты. Методы построения полного списка угроз.	ПК-2.1 ПК-3.3	0,25
		Практическая работа № 3. Модель нарушителя информационной безопасности. Информационные ресурсы информационной системы. Способы оцен-	ПК-2.1 ПК-3.3	0,25

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол-во Часов
		ки рисков информационной безопасности.		
2.	Раздел 2. Основные методы защиты информации от базовых угроз			
	Тема 3. Основные методы защиты информации от базовых угроз	Лекция № 3. Основные методы защиты от угроз нарушения конфиденциальности информации.	ПК-3.1	0,25
		Лекция № 4. Основные методы защиты от угроз нарушения целостности и доступности информации.	ПК-3.2	0,25
		Практическая работа № 4. Способы разграничения доступа к информации в информационной системе. Идентификация и аутентификация.	ПК-3.5 ПК-3.5	0,5
		Практическая работа № 5. Модели обеспечения целостности. Модель Кларка-Вилсона. Модель Биба. Методы обеспечения доступности информации: резервирование и дублирование в информационной системе.	ПК-2.1 ПК-3.5	0,5
3.	Раздел 3. Стандарты информационной безопасности			
	Тема 4. Стандарты информационной безопасности	Лекция № 5. Стандарты информационной безопасности. Роль стандартов. Основные оценочные стандарты.	ПК-3.1	0,25
		Лекция № 6. Стандарты информационной безопасности. Основные управленческие стандарты (спецификации). Понятие об управлении информационной безопасностью	ПК-3.1	0,25
		Практическая работа № 6. Оценочные стандарты 1-го поколения: Оранжевая книга, РД ФСТЭК. Оценочные стандарты. «Общие критерии». Основные подходы к оценке. Среда безопасности.	ПК-3.5 ПК-3.3	0,5
		Практическая работа № 7. Управленческие стандарты. Стандарты серии BS. Управление информационной безопасностью, управление рисками. Управленческие стандарты. Сетевая безопасность. Основные требования спецификации X.800.	ПК-3.5 ПК-3.3	0,5
4.	Раздел 4. Проблематика построения систем защиты информации			
	Тема Проблематика построения СЗИ	Лекция № 7. Функциональная модель системы защиты информации. Проблемы защиты информации в системах.	ПК-3.1	0,5
		Практическая работа № 8. Показатели уязвимости и защищенности в информационных системах. Компоненты функциональной модели системы защиты информации.	ПК-2.1 ПК-3.3	1

5. Учебно-методическое обеспечение самостоятельной работы обучающихся. Оценочные материалы для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Контрольные вопросы и задания

1. Сущность и понятие информационной безопасности. Характеристика ее составляющих.
2. Информационные ресурсы. Особенности информационных ресурсов.
3. Требования к информации как к объекту защиты.
4. Информационное общество. Определение и характеристика, проблемы ИБ в информационном обществе.
5. Понятие национальной безопасности. Место информационной безопасности в системе национальной безопасности.
6. Виды безопасности. Классификация видов безопасности.
7. Модель нарушителя информационной безопасности.
8. Компьютерные преступления.
9. Информационная война как комплексная угроза государству.
10. Содержание информационного противоборства на межгосударственном уровне
11. Информационное оружие, его классификация и возможности.
12. Угрозы в информационной безопасности . Классификация угроз.
13. Базовые угрозы информационной безопасности.
14. Уязвимости в информационной безопасности. Классификация уязвимостей
15. Носители информации. Классификация носителей информации.
16. Человек – как носитель защищаемой информации.
17. Угрозы нарушения конфиденциальности информации. Основные методы защиты от угроз нарушения конфиденциальности
18. Угрозы нарушения целостности информации. Основные методы защиты от угроз нарушения целостности информации
19. Угрозы нарушения доступности информации. Основные принципы построения систем защиты от угроз нарушения доступности.
20. Методы защиты внешнего периметра.
21. Классы межсетевых экранов. Особенности с точки зрения защиты от угроз конфиденциальности.
22. Алгоритм функционирования системы IDS
23. Модель контроля целостности информации Кларка-Вилсона.
24. Протоколирование и аудит. Роль в защите от угроз конфиденциальности.
25. Базовая схема идентификации и аутентификации.
26. Идентификация. Определение, виды идентификаторов.
27. Аутентификация. Определение, основные методы аутентификации.
28. Криптографические методы обеспечения целостности информации. Цифровая подпись.

29. RAID – массивы как средство защиты от угроз нарушения доступности и целостности.
30. Понятие о физической защите. Виды физической защиты информации.
31. Классификация защищаемой информации по характеру сохраняемой тайны.
32. Разграничение доступа. Основные методы разграничения доступа.
33. Стандарты информационной безопасности. Роль стандартов в обеспечении ИБ. Виды стандартов.
34. Оранжевая книга. Основные положения. Значение для развития информационной безопасности.
35. Общие критерии. Основные положения.
36. РД ФСТЭК. Основные положения и принципы защиты от НСД.
37. Методы оценки защищенности компьютерных систем от НСД (РД ФСТЭК).
38. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем (РД ФСТЭК).
39. Управленческие стандарты серии BS.
40. Особенности ИБ сетей. Основные положения спецификаций серии X.800.

5.2. Темы письменных контрольных работ

1. «Основные термины и определения теории информационной безопасности»
2. «Стандарты информационной безопасности»

5.3. Оценочные средства

Оценочные материалы (оценочные средства) для проведения текущего контроля и промежуточной аттестации по дисциплине «Основы информационной безопасности» прилагаются

5.4. Перечень видов оценочных средств

1. Вопросы к зачету
2. Тестовые контрольные работы по отдельным темам дисциплины.
3. Контрольные задания для текущего контроля успеваемости.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные. — СПб.: Санкт-Петербургский политехнический университет Петра Великого,

2014. — 322 с.— Режим доступа: <http://www.iprbookshop.ru/43960>. — ЭБС «IPRbooks», по паролю

2. Галатенко, В. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / В. А. Галатенко. — 3-е изд. — Электрон. текстовые данные — М.: Интернет-Университет Информационных Технологий (ИНТУ-ИТ), 2020. — 266 с. — 978-5-4497-0675-1. — Режим доступа: <http://www.iprbookshop.ru/97562>. — ЭБС «IPRbooks», по паролю

6.2 Дополнительная литература

1. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-методический комплекс/ Сычев Ю.Н.— Электрон. Текстовые данные. — М.: Евразийский открытый институт, 2012. — 342 с.— Режим доступа: <http://www.iprbookshop.ru/14642>. — ЭБС «IPRbooks», по паролю

2. Алексеев, А. П. Многоуровневая защита информации [Электронный ресурс] / А. П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 128 с. — 978-5-904029-72-2. — Режим доступа: <http://www.iprbookshop.ru/75387>. — ЭБС «IPRbooks», по паролю

6.3 Периодические издания

1. **Anti-Malware** | <https://www.anti-malware.ru/>
2. **Thratpost** <https://threatpos>

7. Перечень ресурсов информационно-телекоммуникационной сети

1. ЭБС издательства «Лань»: <http://www.e.lanbook.com/>
2. ЭБС IPRbooks: <http://iprbookshop.ru>
3. Научная электронная библиотека eLIBRARY.RU: <https://elibrary.ru/>
4. ЭБС POLPRED.COM: <https://polpred.com/>
5. Российская государственная библиотека (РГБ): <https://www.rsl.ru/>
6. Российская национальная библиотека (РНБ): <http://nlr.ru/>
7. Государственная публичная научно-техническая библиотека (ГПНТБ): <http://www.gpntb.ru/>
8. Президентская библиотека: <https://www.prlib.ru/>
9. Российский фонд фундаментальных исследований: <https://podpiska.rfbr.ru/>
10. Информационная система «Регламент»: <https://www.reglament.pro/>
11. Информационная система «Единое окно доступа к образовательным ресурсам»: <http://window.edu.ru/>
12. Росстандарт: <http://www.gost.ru/>
13. Сайт Европейской организации по стандартизации (ETSI): <http://www.etsi.org>
14. Сайт Международного союза электросвязи: <http://www.itu.int>

8. Перечень программного обеспечения и информационных справочных систем

1. ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
2. 7-Zip (свободно распространяемое ПО);
3. Mozilla Firefox (свободно распространяемое ПО);
4. Foxit Reader (свободно распространяемое ПО);
5. Yandex Browser (свободно распространяемое ПО);
6. VSCodium (свободно распространяемое ПО);
7. Pinta (свободно распространяемое ПО);
8. Adobe Reader (свободно распространяемое ПО);
9. LibreOffice (свободно распространяемое ПО).

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

1. Учебная аудитория для проведения лекционных занятий, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающими тематические иллюстрации, соответствующие рабочей программе дисциплины.

2. Учебная аудитория для проведения практических занятий, укомплектованная специализированными техническими средствами обучения и оснащенная:

Коммутатор Comrex SRX2224

Интерактивная доска Classic Solution

Дистрибутив ПО ViPNet Client

Дистрибутив СКЗИ "КриптоПро CSP" версии 4.0.

Дистрибутив ПО ViPNet Administrator

3. Учебная аудитория для проведения консультаций, текущего контроля и промежуточной аттестации, оснащенная компьютерной техникой.

4. Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду МТУСИ и в электронно-библиотечную систему МТУСИ.

10. Методические рекомендации студентам по освоению дисциплины

В процессе изучения дисциплины предусмотрены следующие формы контроля по овладению компетенциями: текущий, промежуточный контроль (зачет), контроль самостоятельной работы обучающихся.

Текущий контроль осуществляется в течение семестра в виде устного опроса обучающихся на практических занятиях, в виде письменных проверочных работ по текущему материалу, а так же в виде сетевого

тестирования в рамках контрольных точек, проводимых в соответствии с графиками учебного процесса. Устные ответы и письменные работы обучающихся оцениваются. Оценки доводятся до сведения обучающихся. Результаты тестирования суммируются с баллами, полученными по остальным формам контроля, и выставляются в электронные рейтинговые ведомости.

Промежуточный контроль осуществляется в форме зачета в конце семестра.

Контроль самостоятельной работы обучающихся осуществляется в течение всего семестра. Преподаватель самостоятельно определяет формы контроля самостоятельной работы обучающихся в зависимости от содержания разделов и тем, выносимых на самостоятельное изучение. Такими формами могут являться: тестирование, презентации. Результаты контроля самостоятельной работы обучающихся учитываются при осуществлении промежуточного контроля по дисциплине.

Самостоятельная работа является неотъемлемой частью обучения. На этот вид работы отводится до 50% от общего объема часов.

На самостоятельное изучение выносятся задания, направленные на:

- глубокую проработку теоретического материала;
- подготовку к сообщениям и докладам на практических занятиях;
- овладение и закрепление основной терминологии по направлению;
- работу со специальной литературой как способом приобщения к последним мировым научным достижениям в профессиональной сфере.

Самостоятельная работа может быть аудиторной (выполнение отдельных заданий на занятиях) и внеаудиторной.

Для выполнения самостоятельной работы используются:

1. Учебники и учебные пособия.
2. Мультимедийные средства: работа в сети Интернет (использование обучающих программ и учебных сайтов, электронных образовательных ресурсов).

Самостоятельная работа обучающихся по дисциплине включает:

- проработку лекционного материала, а также материала, изучаемого на практических занятиях;
- подготовку к зачету.

УТВЕРЖДАЮ

Зам. Директора ВВФ МТУСИ по УМО

С.А. Маринин

«__» _____ 2022 г.

Лист актуализации рабочей программы дисциплины
«Основы информационной безопасности»

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль): Инфокоммуникационные системы и сети

Форма обучения: Очная, заочная. Рабочая программа действует без изменений.

Разработчик (и): Сочнева Н.В.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИКиПД,
протокол № 7 от 28 августа 2022 года

И.о. заведующий кафедрой



Мазниченко В.В.