

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

**«Обеспечение доверия и безопасности  
в инфокоммуникационных сетях»**

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:



Доцент кафедры ИКиПД, к.ф.м.н.  
доцент Чернявский А.Д.

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**

*Целью* преподавания дисциплины «Обеспечение доверия и безопасности в инфокоммуникационных сетях» является изучение системы обеспечения информационной безопасности (ИБ) как неотъемлемой составной части инфокоммуникационных сетей (ИКС).

Задачи освоения дисциплины:

1. Знакомство с основами российского и зарубежного законодательства в области ИБ.
2. Изучение российских и международных стандартов в области ИБ ИКС.
3. Овладение основами методологии обеспечения ИБ ИКС.
4. Получение знаний по основным методам и протоколам обеспечения ИБ используемым в ИКС.

## **2. Место дисциплины в учебном процессе**

Дисциплина «Обеспечение доверия и безопасности в инфокоммуникационных сетях» включена в перечень дисциплин учебного плана формируемую участниками образовательных отношений (Б1.В.15). Дисциплина «Обеспечение доверия и безопасности в инфокоммуникационных сетях» 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).*

Для успешного усвоения данной дисциплины необходимо, чтобы обучающийся владел знаниями, умениями и компетенциями, сформированными в процессе изучения дисциплин: «Инфокоммуникационные технологии и программирование», «Общая теория связи».

Дисциплина «Обеспечение доверия и безопасности в инфокоммуникационных сетях» является предшествующей для изучения следующих дисциплин: «Проектирование инфокоммуникационных сетей», «Основы интернета вещей». Знания и умения обучающихся, сформированные в результате освоения этой дисциплины, используются обучающимися при разработке курсовых и выпускных квалификационных работ.

Рабочая программа дисциплины «Обеспечение доверия и безопасности в инфокоммуникационных сетях» 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 3 зачетные единицы (108 часов). Процесс изучения дисциплины реализуется при очной форме обучения в 5 семестре и в 6-м при заочной форме обучения. Промежуточная аттестация предусматривает экзамен в 5 и 6 семестре соответственно.

## Требования к результатам освоения учебной дисциплины

Таблица 1

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индекс индикатора достижения компетенции	Содержание индикатора достижения компетенции
1.	ПК-6	Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	ПК-6.1	Знает архитектуру, протоколы и общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
2.	ПК-6	Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	ПК-6.2	Знает основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств
3.	ПК-6	Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	ПК-6.3	Умеет применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
4	ПК-6	Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	ПК-6.4	Пользоваться нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных систем

5	ПК-6	Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	ПК-6.5	Владеет навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа
6	ПК-16	Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	ПК-16.1	Знает общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети. Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
7	ПК-16	Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	ПК-16.2	Умеет подключать и настраивать современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работать с контрольно-измерительными аппаратными и программными средствами
8	ПК-16	Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	ПК-16.3	Владеет навыками установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация
9	ПК-16	Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	ПК-16.4	Владеет навыками документирования настроек средств обеспечения безопасности удаленного доступа

#### 4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ 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 прак- тическая подготовка
		5		
<b>Общая трудоёмкость дисциплины по учебному плану</b>	<b>108</b>	<b>108</b>		
<b>1. Контактная работа:</b>	<b>54</b>	<b>54</b>		
лекции (Л)	22	22		
практические занятия (ПЗ)	20	20		15
лабораторные работы (ЛР)	12	12		12
<b>2. Общая самостоятельная работа и контроль</b>	<b>54</b>	<b>54</b>		
курсовая работа/проект (КР/КП) (подготовка)	-	-		
самостоятельное изучение разделов, самоподго- товка (проработка и повторение лекционного ма- териала и материала учебников и учебных пособий, подготовка к лабораторным и практическим заня- тиям, коллоквиумам и т.д.) (СР), иная контактная работа (ИКР) и подготовка к зачету (при его нали- чии):	18	18		
<b>Подготовка к экзамену и контактная работа в сессию (КРС)</b>	<b>36</b>	<b>36</b>		
Вид промежуточного контроля:	Экзамен			

#### ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2б

Вид учебной работы	Трудоёмкость			
	час.	В т.ч. по семестрам		Из них прак- тическая подготовка
		6		
<b>Общая трудоёмкость дисциплины по учебному плану</b>	<b>108</b>	<b>108</b>		
<b>1. Контактная работа:</b>	<b>12</b>	<b>12</b>		
лекции (Л)	4	4		
практические занятия (ПЗ)	4	4		3
лабораторные работы (ЛР)	4	4		4
<b>2. Общая самостоятельная работа и контроль</b>	<b>96</b>	<b>96</b>		
курсовая работа/проект (КР/КП) (подготовка)	-	-		
самостоятельное изучение разделов, самоподго- товка (проработка и повторение лекционного ма- териала и материала учебников и учебных пособий, подготовка к лабораторным и практическим заня- тиям, коллоквиумам и т.д.) (СР), иная контактная работа (ИКР) и подготовка к зачету (при его нали- чии):	60	60		

Вид учебной работы	Трудоёмкость		
	час.	В т.ч. по семестрам	
		6	Из них практическая подготовка
Подготовка к экзамену и контактная работа в сессию (КРС)	36	36	
Вид промежуточного контроля:	Экзамен		

## 4.2 Содержание дисциплины

### Тематический план учебной дисциплины ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3а

Наименование разделов и тем дисциплин	Всего	Аудиторная работа			Внеаудиторная работа СР
		Л	ПЗ	ЛР	
Раздел 1 Основные понятия информационной безопасности (ИБ).	22	8	6	4	4
Раздел 2 Нормативная правовая и нормативная техническая база в области информационной безопасности (ИБ) инфокоммуникаций (ИК).	16	6	6	-	4
Раздел 3 Организационные методы обеспечения ИБ ИК.	12	4	4	-	4
Раздел 4 Технологии обеспечения ИБ ИК	22	4	4	8	6
<b>Всего за 5 семестр</b>	<b>72</b>	<b>22</b>	<b>20</b>	<b>12</b>	<b>18</b>
Экзамен	36	-	-	-	36
<b>Итого по дисциплине</b>	<b>108</b>	<b>22</b>	<b>20</b>	<b>12</b>	<b>54</b>

### ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3б

Наименование разделов и тем дисциплин	Всего	Аудиторная работа			Внеаудиторная работа СР
		Л	ПЗ	ЛР	
Раздел 1 Основные понятия информационной безопасности (ИБ).	22	2	1	1	18
Раздел 2 Нормативная правовая и нормативная техническая база в области информационной безопасности (ИБ) инфокоммуникаций (ИК).	16	1	1	-	14
Раздел 3 Организационные методы обеспечения ИБ ИК.	12	0,5	1	-	10,5
Раздел 4 Технологии обеспечения ИБ ИК	22	0,5	1	3	17,5
<b>Всего за 6 семестр</b>	<b>72</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>60</b>
Экзамен	36	-	-	-	36
<b>Итого по дисциплине</b>	<b>108</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>96</b>

## 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.	<b>Раздел 1. Основные понятия информационной безопасности</b>			
	Тема 1. Основные понятия и определения ИБ и их взаимосвязь	Лекция №1 Основные понятия и определения ИБ и их взаимосвязь	ПК-6.1	2
		Практическое занятие № 1. Аппаратные, программные средства и человеческий фактор как источники уязвимостей	ПК-6.3	2
		Лекция № 2. Классификация и типовые модели угроз.	ПК-6.1	2
		Практическое занятие № 2. Классификация сетевых атак.	ПК-6.1	2
	Тема 2. Основные сервисы ИБ и отечественные аппаратно- программные платформы для их реализации	Лекция №3 Основные сервисы безопасности: контроль доступа; конфиденциальность; целостность; доступность; невозможность отказа от совершенных действий; аутентификация.	ПК-6.1	2
		Лекция №4 Отечественные аппаратно-программные платформы для обеспечения ИБ ИК.	ПК-16.1	2
		Практическое занятие № 3 Отечественная аппаратно-программная платформа Эльбрус и ОС Альт.	ПК-6.5	1
		Практическое занятие № 4. Интерфейс, основные команды и сетевые утилиты ОС Альт.	ПК-6.5	1
		Лабораторная работа № 1 Настройка сетевых интерфейсов ВК Эльбрус .	ПК-6.5	2
		Лабораторная работа № 2 Статическая маршрутизация в ОС Альт на ВК Эльбрус	ПК-6.5	2
2.	<b>Раздел 2. Нормативная правовая и нормативная техническая база в области ИБ ИК</b>			
	Тема 3. Нормативная правовая база ИБ ИК	Лекция №5 Анализ нормативной правовой базы в области ИБ ИК. Понятие ИБ ИК и ее обеспечение в российском законодательстве.	ПК-6.4	2
		Практическое занятие № 5. Основные нормативные правовые акты Российской Федерации в области ИБ ИК	ПК-6.4	2
	Тема 4. Нормативная техническая база ИБ ИК	Лекция №6 Анализ нормативной технической базы в области ИБ ИК.	ПК-6.4	2
		Практическое занятие № 6 Отечественные стандарты и рекомендации в области ИБ ИК	ПК-6.4	2
		Лекция №7 Деятельность международных организа-	ПК-6.4	2

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол- во часов
		ций в области стандартизации ИБ ИК		
		Практическое занятие № 7 Стандарты ISO/IEC. Рекомендации МСЭ-Т	ПК-6.4	2
3.	<b>Раздел 3. Организационные методы обеспечения ИБ ИК.</b>			
	Тема 5. Основные участники обеспечения ИБ ИК и их задачи	Лекция №8 Роль государственных органов в обеспечении ИБ ИК	ПК-6.4	2
		Практическое занятие № 8 Взаимодействие государства и бизнеса в области обеспечения ИБ ИК	ПК-6.4	2
	Тема 6. Организационные методы обеспечения ИБ ИК	Лекция №9 Политика безопасности как совокупность документированных решений направленных на обеспечение ИБ.	ПК-16.4	2
		Практическое занятие № 9 Уровни детализации политики безопасности. Программы реализации политики безопасности – цели, структура и связь с жизненным циклом системы.	ПК-16.4	2
4.	<b>Раздел 4. Технологии обеспечения ИБ ИК</b>			
	Тема 7. Криптографические методы обеспечения ИБ ИК	Лекция №10 Основные алгоритмы шифрования и их применение для обеспечения ИБ ИК	ПК-6.2	2
		Лабораторная работа №3 Передача нешифрованной и зашифрованной информации между компьютерами	ПК-6.5	2
	Тема 8. Методы обеспечения ИБ ИК при межсетевом взаимодействии.	Лекция №11 Межсетевое экранирование в Интернет	ПК-16.1	2
		Практическое занятие №10 Межсетевое экранирование на основе ОС Альт	ПК-16.2	4
		Лабораторная работа № 4 Межсетевой экран для рабочей станции.	ПК-16.3	2
		Лабораторная работа № 5 Межсетевой экран локальной сети.	ПК-16.3	2
		Лабораторная работа №6 Межсетевое экранирование и доступ из внешней сети по протоколу SSH.	ПК-16.4	2

### ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 4б

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол- во часов
1.	<b>Раздел 1. Основные понятия информационной безопасности</b>			
	Тема 1. Основные понятия и определения ИБ и их вза-	Лекция №1 Основные понятия и определения ИБ и их взаимосвязь	ПК-6.1	0,5

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол- во часов
	ИМОСВЯЗЬ	Практическое занятие № 1. Аппаратные, программные средства и человеческий фактор как источники уяз- вимостей	ПК-6.3	0,25
		Лекция № 2. Классификация и типовые модели угроз.	ПК-6.1	0,5
		Практическое занятие № 2. Классификация сетевых атак.	ПК-6.1	0,25
	Тема 2. Основные сервисы ИБ и отечественные аппаратно- про- граммные плат- формы для их реа- лизации	Лекция №3 Основные сервисы безопасности: кон- троль доступа; конфиденциальность; це- лостность; доступность; невозможность отказа от совершенных действий; аутен- тификация.	ПК-6.1	0,5
		Лекция №4 Отечественные аппаратно-программные платформы для обеспечения ИБ ИК.	ПК-16.1	0,5
		Практическое занятие № 3 Отечественная аппаратно-программная платформа Эльбрус и ОС Альт.	ПК-6.5	0,25
		Практическое занятие № 4. Интерфейс, основные команды и сетевые утилиты ОС Альт.	ПК-6.5	0,25
		Лабораторная работа № 1 Настройка сетевых интерфейсов ВК Эль- брус .	ПК-6.5	0,5
		Лабораторная работа № 2 Статическая маршрутизация в ОС Альт на ВК Эльбрус	ПК-6.5	0,5
	<b>2. Раздел 2. Нормативная правовая и нормативная техническая база в области ИБ ИК</b>			
	Тема 3. Норматив- ная правовая база ИБ ИК	Лекция №5 Анализ нормативной правовой базы в области ИБ ИК. Понятие ИБ ИК и ее обеспечение в российском законодатель- стве.	ПК-6.4	0,3
		Практическое занятие № 5. Основные нормативные правовые акты Российской федерации в области ИБ ИК	ПК-6.4	0,3
	Тема 4. Норматив- ная техническая база ИБ ИК	Лекция №6 Анализ нормативной технической базы в области ИБ ИК.	ПК-6.4	0,3
		Практическое занятие № 6 Отечественные стандарты и рекоменда- ции в области ИБ ИК	ПК-6.4	0,3
		Лекция №7 Деятельность международных организа- ций в области стандартизации ИБ ИК	ПК-6.4	0,4
		Практическое занятие № 7 Стандарты ISO/IEC. Рекомендации МСЭ- Т	ПК-6.4	0,4

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Кол-во часов
3.	<b>Раздел 3. Организационные методы обеспечения ИБ ИК.</b>			
	Тема 5. Основные участники обеспечения ИБ ИК и их задачи	Лекция №8 Роль государственных органов в обеспечении ИБ ИК	ПК-6.4	0,25
		Практическое занятие № 8 Взаимодействие государства и бизнеса в области обеспечения ИБ ИК	ПК-6.4	0,5
	Тема 6. Организационные методы обеспечения ИБ ИК	Лекция №9 Политика безопасности как совокупность документированных решений направленных на обеспечение ИБ.	ПК-16.4	0,25
		Практическое занятие № 9 Уровни детализации политики безопасности. Программы реализации политики безопасности – цели, структура и связь с жизненным циклом системы.	ПК-16.4	0,5
4.	<b>Раздел 4. Технологии обеспечения ИБ ИК</b>			
	Тема 7. Криптографические методы обеспечения ИБ ИК	Лекция №10 Основные алгоритмы шифрования и их применение для обеспечения ИБ ИК	ПК-6.2	0,25
		Лабораторная работа №3 Передача нешифрованной и зашифрованной информации между компьютерами	ПК-6.5	1
	Тема 8. Методы обеспечения ИБ ИК при межсетевом взаимодействии.	Лекция №11 Межсетевое экранирование в Интернет	ПК-16.1	0,25
		Практическое занятие №10 Межсетевое экранирование на основе ОС Альт	ПК-16.2	1
		Лабораторная работа № 4 Межсетевой экран для рабочей станции.	ПК-16.3	0,5
		Лабораторная работа № 5 Межсетевой экран локальной сети.	ПК-16.3	0,5
		Лабораторная работа №6 Межсетевое экранирование и доступ из внешней сети по протоколу SSH.	ПК-16.4	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 (для самостоятельного изучения)

1. Возможности, ограничения и взаимосвязь трех основных направлений обеспечения информационной безопасности (ИБ): нормативного правового регулирования, технического регулирования и образовательно-культурологической деятельности.

2. Основные положения Конституции Российской Федерации в сфере информационной безопасности.
3. Основные положения ФЗ «Об информации, информационных технологиях и о защите информации».
4. Основные положения ФЗ «О техническом регулировании» и нормативных правовых актов, обеспечивающих его выполнение, в части информационной безопасности.
5. Основные положения ФЗ «О государственной тайне».
6. Основные положения ФЗ «О персональных данных» и нормативных правовых актов, обеспечивающих его выполнение.
7. Основные положения ФЗ «Об оперативно-разыскной деятельности» и нормативные правовые акты, обеспечивающие его выполнение.
8. Основные положения ФЗ «Об электронной подписи».
9. Основные положения ФЗ «О связи» и нормативных правовых актов, обеспечивающих его выполнение, в части информационной безопасности.
10. Основные положения ФЗ «О лицензировании отдельных видов деятельности» и нормативных правовых актов, обеспечивающих его выполнение, в части информационной безопасности.
11. Основные положения ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
12. Ответственность за нарушение обязательных требований в сфере обеспечения информационной безопасности систем и сетей связи .
13. Основные направления совершенствования нормативной правовой базы в сфере обеспечения информационной безопасности систем и сетей связи
14. Основные задачи регуляторов в сфере обеспечения информационной безопасности систем и сетей связи.
15. Создание отечественных программных платформ на базе свободного программного обеспечения.
16. Профилактика правонарушений, совершаемых с использованием ИКТ.
17. Техническое регулирование обеспечения информационной безопасности систем и сетей связи.
18. Роль и место стандартизации информационной безопасности систем и сетей связи.
19. Стандартизация кибербезопасности.
20. Требования к базовому уровню информационной безопасности операторов связи.
21. Направления технической стандартизации информационной безопасности в МСЭ.
22. Требования к системе обнаружения потерь доходов операторов связи и потребителей.
23. Стандартизация управления идентификацией.
24. Стандартизация построения инфраструктуры открытых ключей.
25. Управление информационной безопасностью на предприятии.
26. Категории нарушителей информационной безопасности.
27. Категории атак и методов противодействия атакам.

28. Гуманитарные аспекты информационной безопасности.
29. Формирование информационной культуры, этика в сфере использования информационных технологий.

## **5.2. Темы письменных работ**

Темы рефератов для самостоятельной работы

1. Возможности, ограничения и взаимосвязь трех основных направлений обеспечения информационной безопасности (ИБ): нормативного правового регулирования, технического регулирования и образовательно-культурологической деятельности.
2. Основные положения Конституции Российской Федерации в сфере информационной безопасности.
3. Основные задачи регуляторов в сфере обеспечения информационной безопасности систем и сетей связи.
4. Основные направления законодательного регулирования ИБ в Российской Федерации.
5. Основные направления стандартизации ИБ в ИК17 МСЭ-Т. Отличия технического и правового регулирования ИБ.
6. Просветительские, культурологические и этические нормы ИБ.
7. Основные положения ФЗ "Об информации, информационных технологиях и о защите информации" в части ИБ.
8. Основные положения ФЗ «О персональных данных» в части ИБ.
9. Основные положения ФЗ "О связи" в части ИБ.
10. Основные положения ФЗ "Об электронной подписи" в части ИБ.
11. Основные положения европейской директивы о защите персональных данных.
12. Основные положения ФЗ «О государственной тайне» в части ИБ.
13. Основные положения ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
14. Структура МСЭ-Т, сфера деятельности, задачи, представительство.
15. Стандартизация кибербезопасности.
16. Стандартизация управления идентификацией.
17. Процессный подход к управлению в организации. Цикл Деминга.
18. Управление информационной безопасностью на предприятии. Стандарт ISO/IEC 27001:2013.
19. Основные задачи СОРМ. Нормативные документы, регламентирующие реализацию СОРМ.
20. Активный и пассивный методы реализации СОРМ. Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность.
21. Создание отечественных программных платформ на базе свободного программного обеспечения.
22. Профилактика правонарушений, совершаемых с использованием ИКТ.

23. Категории нарушителей информационной безопасности.
24. Категории атак и методов противодействия атакам.
25. «Информационный терроризм» и «информационная война».
26. Социально-психологические последствия внедрения и широкого распространения современных информационных технологий.

### **5.3. Оценочные средства**

Оценочные материалы (оценочные средства) для проведения текущего контроля и промежуточной аттестации по дисциплине «Обеспечения доверия и безопасности в инфокоммуникационных сетях» прилагаются.

### **5.4. Перечень видов оценочных средств**

1. Вопросы для экзамена
2. Темы рефератов и вопросы для практических занятий.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Основная литература**

1. Кремер А.С. Обеспечение доверия и безопасности при использовании ИКТ: Учебное пособие: учебно-методическое пособие/Кремер А.С., Мальянов С.А., Малюк А.А. [Электронный ресурс].-М.:ЭБС МТУСИ, 223 с. Режим доступа: [http://elib.mtuci.ru/catalogue/download.php?book\\_id=2387](http://elib.mtuci.ru/catalogue/download.php?book_id=2387)
2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: <http://www.iprbookshop.ru/52209> .— ЭБС «IPRbooks»

### **6.2 Дополнительная литература**

1. Лапони́на О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]/ Лапони́на О.Р.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 242 с.— Режим доступа: <http://www.iprbookshop.ru/52217> .— ЭБС «IPRbooks»
2. Основы технологии сети Интернет: учебно-методическое пособие/МТУСИ; Кремер А.С., Иванюк А.В., Севрук К.А.,-М.: ООО ФОП, 2019. – 200 с.
3. Основы технологии сети Интернет: лабораторный практикум/МТУСИ; Кремер А.С., Иванюк А.В., Севрук К.А.,-М.: ООО ФОП, 2019. – 376 с.

### **6.3 Периодические издания**

Профильные журналы: «Документальная электросвязь», «Электросвязь», «Т-Comm: Телекоммуникации и транспорт» и другие.

## **7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)**

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 и лабораторных занятий, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации 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 (экзамен), контроль самостоятельной работы обучающихся.

Текущий контроль осуществляется в течение семестра в виде устного опроса студентов 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 экзамена 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, рефераты, контрольные работы (для ЗФО) и т.д. 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:

- работу с операционной системой, с электронными образовательными ресурсами;
- овладение и закрепление основной терминологии по направлению;
- работу со специальной литературой как способом приобщения к последним мировым научным достижениям в профессиональной сфере;
- основные приемы составления аннотаций и написания рефератов.

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 обучающегося по дисциплине включает:

- Проработку лекционного материала, а также материала, изучаемого на практических занятиях;
- Написание реферата по теме ИБ ИК;
- Подготовку к экзамену;

Методические указания по практикуму имеются в библиотеке МТУСИ.

УТВЕРЖДАЮ

Зам. Директора ВВФ МТУСИ по УМО

С.А. Маринин

«\_\_» \_\_\_\_\_ 2022 г.

**Лист актуализации рабочей программы дисциплины**  
**«Обеспечение доверия и безопасности в инфокоммуникационных сетях»**

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): к.ф.-м.н. Чернявский А.Д.

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

И.о. заведующий кафедрой



Мазниченко В.В.