ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УВР
_____ А.Г. Жуковский
«28» 08 2019 г.

Основы организационно-правового обеспечения информационной безопасности сетей и систем Б1.В.10

рабочая программа дисциплины

Кафедра **Общенаучной подготовки**
Направление подготовки **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль **Защищенные системы и сети связи**
Формы обучения **очная, заочная**

Распределение часов дисциплины по семестрам (ОФ), курсам (ЗФ)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	2	72/5	2	72/3
Контактная работа, в том числе (по семестрам, курсам):		32/5		16/3
Лекции		12/5		8/3
Лабораторных работ				
Практических занятий				
Семинаров		20/2		8/3
Самостоятельная работа		40		56/3
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам, курсам		1/5		1/3
Число экзаменов с разбивкой по семестрам				

Программу составил:

Доцент кафедры Общенаучной подготовки, к.п.н., Жуковский Д.А.

Рецензент:
Заведующий кафедрой ИТСС к.т.н. доцент Юхнов В.И.

Рабочая программа дисциплины

«Основы организационно-правового обеспечения информационной безопасности сетей и систем»

Разработана в соответствии с ФГОС ВО:
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ
утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930

Составлена на основании учебного плана
направления 11.03.02 Инфокоммуникационные технологии и системы связи профиля «Защищенные системы и сети связи», одобренного Учёным советом СКФ МТУСИ, Протокол № 5 от 24.12.2018 г. № 1, и утвержденного директором СКФ МТУСИ 15.01.2019 г.

Рассмотрена и одобрена на заседании кафедры
«Общенаучной подготовки»

Протокол от «___» _____ 20__ г. № ____

Зав. кафедрой _____Конкин Б.Б.

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Общенаучной подготовки»

Протокол от _ ________ 20__ г. № _
Зав. кафедрой ______________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Общенаучной подготовки»

Протокол от _ ________ 20__ г. № _
Зав. кафедрой ______________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Общенаучной подготовки»

Протокол от _ ________ 20__ г. № _
Зав. кафедрой ______________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Общенаучной подготовки»

Протокол от _ ________ 20__ г. № _
Зав. кафедрой ______________________

1. Цели изучения дисциплины

Целью освоения дисциплины «Основы организационно-правового обеспечения информационной безопасности сетей и систем» является изучение организационно-правовых основ обеспечения информационной безопасности в современных телекоммуникационных системах, а также содействие формированию научного мировоззрения и развитию системного мышления.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***технологической деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм имеющихся ресурсов и ограничений
Знать:
Виды ресурсов и ограничений для решений профессиональных задач; Основные методы оценки разных способов решения задач; Действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
Уметь:
Проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; Анализировать альтернативные варианты для достижения намеченных результатов; Использовать нормативно-правовую документацию в сфере профессиональной деятельности
Владеть:
Методиками разработки цели и задач проекта; Методами оценки потребности в ресурсах, продолжительности и стоимости проекта; Навыками работы с нормативно-правовой документацией

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.В.03 Производственный менеджмент
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.04 Маркетинг в отрасли инфокоммуникаций

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 72 часа, 32 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 3 , Семестр 5					
Модуль 1. Правовое обеспечение информационной деятельности 36 (16+20) часов					
1.1	Информационные отношения, как объект правового регулирования. Законодательство РФ в области информационной безопасности. Структура информационной сферы и характеристика ее элементов. Виды информации. Конституционные гарантии прав на информацию и механизм их реализации. Понятие и структура информационной безопасности.	Лек.	4	УК-2	Л1.1 Л3.1 Л2.2
1.2	Правовой режим защиты государственной тайны. Правовое обеспечение защиты государственной тайны. Контроль и надзор за обеспечением защиты государственной тайны.	Лек	2	УК-2	Л1.1 Л2.1
1.3	Правовые режимы защиты информации конфиденциального характера. Правовая защита конфиденциальной информации. Нормативно-правовое регулирование профессиональной и служебной тайны. Организационные меры по охране конфиденциальности информации.	С.	4	УК-2	Л2.1 Л2.1
1.4	Законодательство РФ в области информационной безопасности. Технологические меры поддержания безопасности. Организация режима секретности. Допуск к государственной тайне. Защита компьютерной информации.	С.	4	УК-2	Л1.1 Л3.1
1.5	Правовые режимы защиты информации конфиденциального характера. Государственное регулирование деятельности в области защиты информации.	С.	2	УК-2	Л2.1 Л3.1
1.6	Законодательство РФ в области информационной безопасности. Изучение положений о государственном лицензировании деятельности в области защиты информации. Защита компьютерной информации. Технические каналы утечки компьютерной информации. Защита информации от утечки по техническим каналам.	СР	20	УК-2	Л1.1 Л2.1 Л2.2 Л3.1
Модуль 2. Организационное обеспечение информационной безопасности 36 (16+20) часов					
2.1	Понятие организационной защиты информации. Направления, принципы и условия организационной защиты информации. Подходы и требования к организации системы защиты информации. Методы, силы и средства, используемые для организации защиты информации.	Лек.	6	УК-2	Л1.1 Л3.1 Л2.2
2.2	Методы обеспечения физической безопасности. Средства и методы физической защиты объекта. Структура системы физической защиты.	С.	4	УК-2	Л2.1
2.3	Правовая охрана результатов интеллектуальной дея-	С.	4	УК-2	Л2.1

	тельности. Преступления в сфере компьютерной информации.				
2.4	Понятие организационной защиты информации. Методы обеспечения физической безопасности/ Изучение положения о сертификации средств вычислительной техники и связи. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.	С.	2	УК-2	Л1.1 Л3.1
2.7	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации. Система сертификации средств криптографической защиты информации. Преступления в сфере компьютерной информации. Классификация компьютерных преступлений. Криминалистические особенности расследования компьютерных преступлений. Международные стандарты и соглашения в области безопасности информационных технологий.	СР.	20	УК-2	Л1.1 Л2.1 Л3.1 Л3.2

4.2 Заочная форма обучения (всего 72 часа, 16 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 3					
Модуль 1. Правовое обеспечение информационной деятельности 36 (8+28) часов					
1.1	Информационные отношения, как объект правового регулирования. Законодательство РФ в области информационной безопасности. Структура информационной сферы и характеристика ее элементов. Виды информации. Конституционные гарантии прав на информацию и механизм их реализации. Понятие и структура информационной безопасности.	Лек.	2	УК-2	Л1.1 Л3.1 Л2.2
1.2	Правовой режим защиты государственной тайны. Правовое обеспечение защиты государственной тайны. Контроль и надзор за обеспечением защиты государственной тайны.	Лек	2	УК-2	Л1.1 Л2.1
1.3	Правовые режимы защиты информации конфиденциального характера. Правовая защита конфиденциальной информации. Нормативно-правовое регулирование профессиональной и служебной тайны. Организационные меры по охране конфиденциальности информации.	С.	2	УК-2	Л2.1 Л2.1
1.4	Законодательство РФ в области информационной безопасности. Технологические меры поддержания безопасности. Организация режима секретности. Допуск к государственной тайне. Защита компьютерной информации.	С.	2	УК-2	Л1.1 Л3.1
1.5	Правовые режимы защиты информации конфиденциального характера. Государственное регулирование деятельности в области защиты информации.	СР	4	УК-2	Л2.1 Л3.1

1.6	Законодательство РФ в области информационной безопасности. Изучение положений о государственном лицензировании деятельности в области защиты информации. Защита компьютерной информации. Технические каналы утечки компьютерной информации. Защита информации от утечки по техническим каналам.	СР	24	УК-2	Л1.1 Л2.1 Л2.2 Л3.1
Модуль 2. Организационное обеспечение информационной безопасности 36 (8+28) часов					
2.1	Понятие организационной защиты информации. Направления, принципы и условия организационной защиты информации. Подходы и требования к организации системы защиты информации. Методы, силы и средства, используемые для организации защиты информации.	Лек.	4	УК-2	Л1.1 Л3.1 Л2.2
2.2	Методы обеспечения физической безопасности. Средства и методы физической защиты объекта. Структура системы физической защиты.	С.	2	УК-2	Л2.1
2.3	Правовая охрана результатов интеллектуальной деятельности. Преступления в сфере компьютерной информации.	С.	2	УК-2	Л2.1
2.4	Понятие организационной защиты информации. Методы обеспечения физической безопасности/ Изучение положения о сертификации средств вычислительной техники и связи. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.	СР	4	УК-2	Л1.1 Л3.1
2.7	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации. Система сертификации средств криптографической защиты информации. Преступления в сфере компьютерной информации. Классификация компьютерных преступлений. Криминалистические особенности расследования компьютерных преступлений. Международные стандарты и соглашения в области безопасности информационных технологий.	СР.	24	УК-2	Л1.1 Л2.1 Л3.1 Л3.2

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 1.1	А.И. Овчинников, А.Ю. Мамычев, А.Г. Кравченко	Основы национальной безопасности: Учебное пособие	М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 235 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э1
Л 1.2	Е.К. Баранова, А. В. Бабаш	Информационная безопасность и защита информации: Учебное пособие.	М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э2
5.1.2. Дополнительная литература для самостоятельной работы обучающегося				
	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 2.1	Е.Б. Белов и др.	Основы информационной безопасности: Учебное пособие для вузов.	М.: Гор. линия-Телеком, 2011. - 558 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э3
Л 2.2	В.В. Золотарев, Е. А. Данилова.	Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : Учебное пособие.	Красноярск: Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э4
Л 2.3	Ю.И. Коваленко	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие.	М.: Гор. линия-Телеком, 2012. - 140 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э5
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающегося				
	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 3.1	Е.К.Баранова, А.В.Бабаш	Моделирование системы защиты информации: Практикум: Учебное пособие.	М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э6
Л 3.2	А.П. Курило, Н.Г. Милославская,	Вопросы управления информационной	М.:Гор. линия-Телеком, 2013. - 244 с. - Режим доступа:	Э7

	М.Ю. Сенаторов.	безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью.	http://znanium.com - ЭБС «Znanium.com»	
Л 3.3	М. Н. Жукова, В. Г. Жуков, В. В. Золотарев.	Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : Учебное пособие.	Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э8
Л 3.4	А.В. Васильков, И.А. Васильков.	Безопасность и управление доступом в информационных системах: Учебное пособие.	М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: http://znanium.com - ЭБС «Znanium.com»	Э9

5.2. Электронные образовательные ресурсы	
Э1	http://znanium.com/catalog.php?bookinfo=508513
Э2	http://znanium.com/catalog.php?bookinfo=495249
Э3	http://znanium.com/catalog.php?bookinfo=405159
Э4	http://znanium.com/catalog.php?bookinfo=463037
Э5	http://znanium.com/catalog.php?bookinfo=358911
Э6	http://znanium.com/bookread2.php?book=476047
5.3. Программное обеспечение	
П.1	MS Power Point
П.2	MS Word

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном.
6.2 МТО рубежных контролей, зачетов, экзаменов	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет.

7. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 3.

Таблица 3 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ и др.	Часов всего: 40	Неделя
Модуль 1		20	1-8
1	Законодательство РФ в области информационной безопасности.	4	1
2	Изучение положений о государственном лицензировании деятельности в области защиты информации.	4	2
3	Защита компьютерной информации.	2	3
4	Технические каналы утечки компьютерной информации	2	4
5	Защита информации от утечки по техническим каналам.	2	5
6	Государственное регулирование деятельности в области защиты информации.	2	6
7	Организация режима секретности.	2	7
8	Допуск к государственной тайне.	2	8
Модуль 2		20	10-17
1	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	4	10-11
2	Система сертификации средств криптографической защиты информации.	4	12-13
3	Классификация компьютерных преступлений.	2	14
4	Криминалистические особенности расследования компьютерных преступлений.	4	15
5	Международные стандарты и соглашения в области безопасности информационных технологий.	4	16
6	Преступления в сфере компьютерной информации.	2	17

Студенты заочной формы обучения могут осваивать вопросы для самостоятельного изучения, представленные в подразделе 4.2 в произвольной последовательности, в удобное для них время. Однако к началу сессии они должны ориентироваться в представленном материале.

Дополнения и изменения в Рабочей программе