МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по учебной работе
Д.Ш. Султанова
«07» июня 2021 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1060
Подписал Проректор по учебной работе Д.Ш. Султанова
Дата 07.06.2021

РАБОЧАЯ ПРОГРАММА
по дисциплине **«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Направление подготовки:	10.03.01 Информационная безопасность
Профиль:	Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная
Институт:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Факультет:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Кафедра-разработчик:	Казанский межвузовский инженерный центр "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет"
Курс; семестр	3; 6

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	18	0,5
Практическое занятие	18	0,5
Контроль самостоятельной работы	54	1,5
Самостоятельная работа	81	2,25
Форма аттестации: Курсовая работа (6 сем), Экзамен (6 сем)	27	0,75
Всего	216	6

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1427 от 17.11.2020) по направлению подготовки 10.03.01 Информационная безопасность для профиля «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент А.Ю. Сенцова

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании Казанского межвузовского инженерного центра "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет", протокол от 19.05.2021 г. № 6.

Директор ***Согласовано*** А.Ф. Махоткин

У Т В Е Р Ж Д Е Н О

Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» являются:
а) изучение основных нормативных правовых актов в области информационной безопасности и защиты информации;
б) изучение правовых основ организации защиты государственной тайны и конфиденциальной информации;
в) изучение правовых норм и стандартов по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
г) овладение навыками работы с нормативными правовыми актами.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части ООП и формирует у обучающихся по профилю «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:
1. Документоведение
2. Основы информационной безопасности
3. Правоведение

Дисциплина «Организационное и правовое обеспечение информационной безопасности» является предшествующей и необходима для успешного освоения последующих дисциплин:
1. Основы управления информационной безопасностью
2. Подготовка к процедуре защиты и защита выпускной квалификационной работы
3. Производственная практика (преддипломная практика)

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

ОПК-10.1. Знает современные принципы рационального выбора средств защиты в зависимости от вида объекта защиты, системный подход к выполнению и организации проектирования средств защиты, нормативные и распорядительные документы, регламентирующие деятельность по обеспечению защищенности объектов информатизации в условиях существовании угроз предприятия, подразделений, должностные инструкции

ОПК-10.2. Умеет применять стандарты по оценке защищенности автоматизированных систем при анализе и проектировании систем защиты информации в автоматизированныз системах, выполнять обследование объектов обеспечения защищенности информации в условиях существовании угроз, анализ предметной области в соответствии с поставленными задачами

ОПК-10.3. Владеет современными методами оценки и исследования информационной безопасности различных объектов

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ОПК-12.1. Знает общие подходы к анализу угроз информационной безопасности объектов

ОПК-12.2. Умеет использовать изученные методы для принятия экономических и технических решений, применять методы обеспечения безопасности информационных систем.

ОПК-12.3. Владеет современными методами обоснования и поддержания надёжности информационных систем

В результате освоения дисциплины обучающийся должен

Знать:

нормативные и распорядительные документы, регламентирующие деятельность по обеспечению защищенности объектов информатизации в условиях существовании угроз предприятия

подходы к анализу угроз информационной безопасности объектов

средства обеспечения защиты информации

Уметь:

применять стандарты по оценке защищенности автоматизированных систем при анализе и проектировании систем защиты информации в автоматизированныз системах

участвует в разработке и формировании исходных данных для проектирования средств и систем защиты информации, комплекса мер по обеспечению информационной безопасности,

управлении процессом их реализации

Владеть:

методами оценки и исследования информационной безопасности различных объектов

способностью проводить подготовку исходных данных для проектирования средств обеспечения защиты информации

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Правовое обеспечение информационной безопасности	6	10	9	10	26	29	Лабораторная работа
2.	Организационное обеспечение информационной безопасности	6	8	9	8	14	16	Лабораторная работа; Экзамен
3.	Курсовая работа	6				14	36	Курсовая работа
	Итого по семестру	**6**	**18**	**18**	**18**	**54**	**81**	**Курсовая работа, Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Правовое обеспечение информационной безопасности	2	Основы обеспечения информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
				ОПК-12.3
2.		2	Государственная система защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
3.		2	Защита персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
4.		2	Защита государственной и коммерческой тайны	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
5.		2	Электронная подпись. Защита прав и законных интересов субъектов информационной сферы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
6.	Организационное обеспечение информационной безопасности	2	Организационные основы защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
7.		2	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
8.		2	Организация допуска и доступа персонала к конфиденциальной информации.	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
9.		2	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Правовое обеспечение информационной безопасности	9	Информационная безопасность в системе национальной безопасности Российской Федерации. Национальные интересы в информационной сфере. Доктрина	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
			информационной безопасности	ОПК-12.3
2.	Организационное обеспечение информационной безопасности	9	Виды ответственности за нарушение законодательства в области защиты информации. УК и КАПП	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
	ВСЕГО	**18**		

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Правовое обеспечение информационной безопасности	4	Государственная система защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
2.		2	Защита персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
3.		2	Защита государственной и коммерческой тайны	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
4.		2	Электронная подпись. Защита прав и законных интересов субъектов информационной сферы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
5.	Организационное обеспечение информационной безопасности	4	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
6.		4	Организация допуска и доступа персонала к конфиденциальной информации.	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
	ВСЕГО	**18**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Основы обеспечения информационной безопасности. Государственная система защиты информации.	10	подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
2.	Защита персональных данных.Защита государственной и коммерческой тайны. Электронная подпись. Защита прав и законных интересов субъектов информационной сферы	19	подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
3.	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений. Организация допуска и доступа персонала к конфиденциальной информации.Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.	16	подготовка к лабораторной работе, подготовка к экзамену	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
4.	Курсовая работа	36	выполнение курсовой работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
	ВСЕГО	**81**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Основы обеспечения информационной безопасности. Государственная система защиты информации.	13	прием лабораторной работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
2.	Защита персональных данных.Защита государственной и коммерческой тайны. Электронная подпись. Защита прав и законных интересов субъектов информационной сферы	13	прием лабораторной работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
3.	Отнесение сведений к конфиденциальной информации. Засекречивание и рассекречивание сведений. Организация допуска и доступа персонала к конфиденциальной информации.Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.	14	прием лабораторной работы, прием экзамена	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
4.	Курсовая работа	14	проверка курсовой работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-12.1 ОПК-12.2 ОПК-12.3
	ВСЕГО	**54**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Организационное и правовое обеспечение информационной безопасности» используется рейтинговая система. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО КНИТУ.

Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Мин.баллов	Макс.баллов
6-й семестр			
Лабораторная работа	6	36	60
Экзамен	1	24	40
Итого		**60**	**100**
6-й семестр			
Курсовая работа	1	60	100
Итого		**60**	**100**

10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

11. Информационно-методическое обеспечение дисциплины

11.1. Основная литература

При изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
Е.К. Баранова, А.В. Бабаш, Информационная безопасность и защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР; Москва : ООО "Научно-издательский центр ИНФРА-М", 2016	http://znanium.com/go.php?id=495249 Режим доступа: по подписке КНИТУ
С.В. Озерский, Н.И. Улендеева, Информатика и информационные технологии в профессиональной деятельности. Часть 1. Информатика [Прочее] Учебное пособие: Самара : Самарский юридический институт ФСИН России, 2020	http://znanium.com/catalog/document?id=375195 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
А.В. Бабаш, П.Н. Башлы, Информационная безопасность и защита информации [Прочее] : Москва : Издательский Центр РИОР, 2013	http://znanium.com/go.php?id=405000 Режим доступа: по подписке КНИТУ
И.С. Клименко, Информационная безопасность и защита информации: модели и методы управления [Прочее] Монография: Москва : ООО "Научно-издательский центр ИНФРА-	http://new.znanium.com/go.php?id=1018665 Режим доступа: по подписке КНИТУ

М", 2020	

11.3. Электронные источники информации

При изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» предусмотрено использование электронных источников информации:
1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/
6. ЭБС IPR SMART: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

УНИЦ
Согласовано

11.4. Профессиональные базы данных и информационные справочные системы

Базы данных
Wiley Online Library: https://onlinelibrary.wiley.com/
Springer Nature: https://link.springer.com/
zbMath : https://zbmath.org/

Информационные справочные системы
Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru
Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

12. Материально-техническое обеспечение дисциплины

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое в учебном процессе при освоении дисциплины «Организационное и правовое обеспечение информационной безопасности»:

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard
Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

Офисные и деловые программы: 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях
Офисные и деловые программы: Константа: Управление процессами.

Дополнительное ПО доступное по бесплатной подписке от Microsoft

Офисные и деловые программы: Microsoft Office 365 Версия для студентов
Офисные и деловые программы: Microsoft Office 365 Версия для преподавателей
ПО для коллективной работы Microsoft Teams

Moodle 3.10

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
1. Ноутбук на базе процессора AMD Dual-Core E-350
2. Проектор мультимедийный EB-W10, экран для проектора.
3. Экран проекционный настенный.

Помещения для самостоятельной работы оснащены компьютерной техникой:
компьютер преподавателя
11 компьютеров студента тип AMD A4-6300
кондиционер SystemAir Sysplit Wall Smart
Проектор Acer H5360BD с доской интерактивной, экран
с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ..Допускается замена оборудования его виртуальными аналогами.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Организационное и правовое обеспечение информационной безопасности» составляет 9 ч.

В процессе освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» используются следующие образовательные технологии:
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция);