МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Нижегородский государственный технический университет
им. Р.Е. Алексеева» (НГТУ)

Институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
“__10_”_____06_____2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.2 Организационно-правовые основы информационной безопасности
(индекс и наименование дисциплины по учебному плану)
для подготовки магистров

Направление подготовки: 09.04.02 Информационные системы и технологии

Направленность: Безопасность информационных систем

Форма обучения: очная
Год начала подготовки 2021

Выпускающая кафедра ИСУ

Кафедра-разработчик ИСУ

Объем дисциплины 180 / 5
часов/з.е
Промежуточная аттестация экзамен

Разработчик: Карпычев В.Ю., д.т.н., профессор

Нижний Новгород

2021

Рецензент: _____ д.т.н., доцент Жевнерчук Д.В.

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом МИНОБРНАУКИ РОССИИ от 19 сентября 2017 года № 917 на основании учебного плана принятого УМС НГТУ

протокол от ___13.12.2020_ №___4__

Рабочая программа одобрена на заседании кафедры протокол от __09.06.2021_№ 10_____
Зав. кафедрой к.т.н, доцент, Тимофеева О.П. _____
(подпись)
Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от_____10.06.2021_____№____1

Рабочая программа зарегистрирована в УМУ регистрационный № 09.04.02 – б-10___
Начальник МО _____

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области обеспечения информационной безопасности организаций.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Организационно-правовые основы информационной безопасности» способствует подготовке студентов к решению следующих профессиональных задач:

1. Правовое обеспечение организационно-технических мероприятий в организациях.
2. Организация защиты информации на объектах защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Организационно-правовые основы информационной безопасности» Б1.В.ОД.2 включена в обязательный перечень дисциплин вариативной части (формируемой участниками образовательных отношений), определяющий направленность образовательной. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по данному направлению подготовки.

Дисциплина базируется на дисциплинах базовой части программы магистратуры по направлению «Информационные системы и технологии»: «Социальные и философские проблемы информационного общества».

Дисциплина «Организационно-правовые основы информационной безопасности» является основополагающей для изучения следующих дисциплин: «Управление информационной безопасностью», также практики: практика по получению профессиональных умений и опыта научно-исследовательской деятельности.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)[i]

Дисциплина «Организационно-правовые основы информационной безопасности» формирует компетенцию ПКС-2 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Дисциплинарная часть компетенции ПКС-2 «Способен проводить разработку и анализ объектов информационной безопасности»: способен обеспечивать разработку объектов информационной безопасности с точки зрения нормативно-правовых документов, действующих в области ИБ.

Таблица 3.1 - Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»			
	1	*2*	*3*	*4*
ПКС-2 Способен проводить разработку и анализ объектов информационной безопасности				
Математические основы криптологии				
Организационно-правовые основы информационной безопасности				
Интеллектуальные методы в информационной безопасности				
Компьютерная вирусология				
Моделирование систем информационной безопасности				
Технологии центров обработки данных				
Программирование на языках низкого уровня в задачах защиты информации				
Программно-аппаратная защита информации				
Управление информационной безопасностью				
Стеганографические методы защиты информации				
Алгоритмы цифровой обработки ЦСП в системах управления				
Ознакомительная				
Практика по получению профессиональных умений и опыта научно-исследовательской деятельности				
Научно-исследовательская работа				
Преддипломная				
Выполнение и защита ВКР				

Таблица 3.2 - Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной Аттестации**
ПКС-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-2.1. Разрабатывает объекты информационной безопасности	***Знать:*** основы правового регулирования отношений в области обеспечения информационной безопасности; организационные основы обеспечения информационной безопасности; ответственность за нарушения в сфере обеспечения информационной безопасности	***Уметь:*** разрабатывать организационно-нормативную документацию в области обеспечения информационной безопасности	***Владеть:*** основами организационно-правового обеспечения ИБ	Опрос на практических занятиях по тематике рефератов	Вопросы для устного собеседования – 40 вопросов

Освоение дисциплины причастно к ТФ С/03.7 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачи обеспечения информационной безопасности с точки зрения нормативных правовых актов в области защиты информации; принятия организационных мер по защите информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 5 зач. ед. 180 часов, распределение часов по видам работ семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		2 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**180**	**180**
1. Контактная работа:	**58**	**58**
1.1 Аудиторная работа, в том числе:	**51**	**51**
занятия лекционного типа (Л)	17	17
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)	34	34
лабораторные работы (ЛР)		
1.2 Внеаудиторная, в том числе	**7**	**7**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	5	5
контактная работа на промежуточном контроле (КРА)	2	2
2. Самостоятельная работа (СРС)	**86**	**86**
реферат/эссе (подготовка)	42	42
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа		
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	44	44
Подготовка к экзамену (контроль)	36	36

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.2 - Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов				
		Лекции (час)	Лабораторные работы	Практические занятия	КСР					
2 семестр										
Раздел 1. Введение										
ПКС-2 - ИПКС-2.1	**Тема 1.1** Система обеспечения ИБ	0,5		0,5		2	Подготовка к лекциям [1-6]			
	Тема 1.2 Правовые средства обеспечения ИБ	1		2		2	Подготовка к лекциям [1-6]			
	Тема 1.3 Организационные средства обеспечения ИБ	0,5		1,5		2	Подготовка к лекциям [1-6],			
	Тема практических занятий: «Основы организационно-правового обеспечения ЗИ»						Подготовка к практическим занятиям работе [1-6]	Мозговой штурм		
	Итого по 1 разделу	**2**		**4**	**0,5**	**6**				
Раздел 2. Правовые основы обеспечения информационной безопасности РФ										

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов				
		Лекции (час)	Лабораторные работы	Практические занятия	КСР					
ПКС-2 - ИПКС-2.1	**Тема 2.1** Конституция РФ, Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности», Доктрина информационной безопасности, ФЗ «Об информации, информационных технологиях и защите информации	2		4		4	Подготовка к лекциям [1-6], работа над рефератом			
	Тема 2.2 Уголовно-правовые и административно-правовые средства обеспечения ИБ	1		2		2	Подготовка к лекциям [1-6]			
	Тема 2.3 Виды тайн в отечественном законодательстве	1		2		2	Подготовка к лекциям [1-6], работа над рефератом			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов				
		Лекции (час)	Лабораторные работы	Практические занятия	КСР					
	Тема 2.4 Закон о персональных данных	0,5		1		2	Подготовка к лекциям [1-6], работа над рефератом			
	Тема 2.5 Ответственность за нарушение ИБ	0,5		1		2	Подготовка к лекциям [1-6], работа над рефератом			
	Тема практических занятий: Правовые основы обеспечения информационной безопасности							Мозговой штурм		
	Итого по 2 разделу	**5**		**10**	**1**	**12**				
Раздел 3. Стандарты в области обеспечения ИБ										
ПКС-2 - ИПКС-2.1	**Тема 3.1** Система стандартов по информационной безопасности (обзор)	3		6		8	Подготовка к лекциям [1-6], работа над рефератом			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов				
		Лекции (час)	Лабораторные работы	Практические занятия	КСР					
	Тема практических занятий: “ Стандарты в области обеспечения ИБ ”						Подготовка к практическим занятиям [1-6]	Мозговой штурм		
	Итого по 3 разделу	**3**		**6**	**0,5**	**8**				
Раздел 4. Нормативно-методические документы ФСТЭК РФ										
ПКС-2 - ИПКС-2.1	**Тема 4.1.** Документы ФСТЭК в области безопасности персональных данных	1		2		3	Подготовка к лекциям [1-6], работа над рефератом			
	Тема 4.2. Руководящие документы ФСТЭК в области ТЗИ	1		2		3	Подготовка к лекциям [1-6], работа над рефератом			
	Тема практических занятий: «Нормативно-методические документы						Подготовка к практическим занятиям [1-6]			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов				
		Лекции (час)	Лабораторные работы	Практические занятия	КСР					
	ФСТЭК РФ»									
	Итого по разделу	**2**		**4**	**1**	**6**				
Раздел 5. Локальные нормативные акты в области ИБ										
ПКС-2 - ИПКС-2.1	**Тема 5.1.** Нормативно-правовые документы	1		**2**		**3**	Подготовка к лекциям [1-6], работа над рефератом			
	Тема 5.2. Индивидуально-правовые документы	1		**2**		**2**	Подготовка к лекциям [6.1.1, 6.1.3], работа над рефератом			
	Тема практических занятий: Локальные нормативные акты в области ИБ						Подготовка к практическим занятиям [1-6]			
	Итого по разделу	2		**4**	**1**	**5**				
Раздел 6. Организационные основы ИБ										
	Тема 6.1. Структура обеспечения ИБ в РФ	0,5		1		2	Подготовка к лекциям [6.1.1, 6.1.3], работа над рефератом			
	Тема 6.2.	0,5		1		1	Подготовка к			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов				
		Лекции (час)	Лабораторные работы	Практические занятия	КСР					
	Структура системы ИБ в организации						лекциям [6.1.1, 6.1.3], работа над рефератом			
	Тема 6.3. Основные организационные мероприятия в области ИБ	1		2		2	Подготовка к лекциям [6.1.1, 6.1.3], работа над рефератом			
	Тема 6.4. Документальное обеспечения ИБ	1		2		2	Подготовка к лекциям [6.1.1, 6.1.3], работа над рефератом			
	Тема практических занятий: Организационные основы ИБ						Подготовка к практическим занятиям [1-6]			
	Итого по разделу	3		**6**	**1**	**7**				
	Подготовка к экзамену (контроль)				**2**	**36**				
	Итого за семестр	**17**	**34**		**7**	**86**				

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Таблица 5.1 - Паспорт оценочных средств (текущая аттестация)

Номер раздела	**Наименование раздела дисциплины**	**Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индиккаторы достижения компетенций**	**Лекционные занятия**		**Практические занятия**		**Самостоятельная работа**	
			Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств
2	Законодательные основы обеспечения информационной безопасности РФ	ПКС-2 – ИПКС-2.1	-	-	Собеседование	Вопросы темплана	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части
3	Стандарты в области обеспечения ИБ	ПКС-2 – ИПКС-2.1	-	-	Собеседование	Вопросы темплана	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части
4	Нормативно-методические документы ФСТЭК РФ	ПКС-2 – ИПКС-2.1	-	-	Собеседование	Вопросы темплана	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части
5	Локальные нормативные акты в области ИБ	ПКС-2 – ИПКС-2.1	-	-	Собеседование	Вопросы темплана	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части

Номер раздела	Наименование раздела дисциплины	Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индиккаторы достижения компетенций	Лекционные занятия		Практические занятия		Самостоятельная работа	
			Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств
6	Организационные основы ИБ	ПКС-2 – ИПКС-2.1	-	-	Собеседование	Вопросы темплана	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части

Таблица 5.2 - Паспорт оценочных средств (промежуточная аттестация)

Наименование дисциплины	Формируемые компетенции	**Знаниевая компонента**	
		Процедура оценивания	Наименование оценочных средств
«Организационно-правовые основы информационной безопасности»	ПКС-2	Устное собеседование по вопросам	Вопросы к экзамену

Таблица 5.3 - Оценочные средства дисциплины, для промежуточной аттестации

	Формируемые Компетенции	Оценочные материалы
1	ПКС-2	Вопросы к экзамену 1-41

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информатика и системы управления».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется **традиционная** система контроля и оценки успеваемости студентов.

При промежуточном контроле успеваемость студентов оценивается по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.4 – Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименовани индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка **«хорошо» /** «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка **«отлично» /** «зачтено» 90-100% от max рейтинговой оценки контроля
ПКС-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-2.1. Разрабатывает объекты информационной безопасности	Изложение учебного материала бессистемное, неполное, не освоены базовые понятия дисциплины. Не знает основы правового регулирования отношений в области обеспечения информационной безопасности; организационные основы обеспечения информационной безопасности; ответственность за нарушения в сфере обеспечения информационной безопасности	Фрагментарные, поверхностные знания базовых понятий. Имеет представление о разработке организационно-нормативной документации в области обеспечения информационной безопасности. Владеет некоторыми основами организационно-правового обеспечения ИБ	Знает базовые понятия дисциплины. Умеет разрабатывать организационно-нормативную документацию в области обеспечения информационной безопасности. Владеет основами организационно-правового обеспечения ИБ.	Имеет глубокие знания всего материала дисциплины. Владеет навыками организации защиты информации и правового обеспечения.

Таблица 5.5 - Критерии оценивания

Оценка	Критерии оценивания
Высокиий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

1. Гафарова, Е.А. Организационно-правовое обеспечение информационной безопасности : учеб. пособие / Е.А. Гафарова. Челябинск: «Библиотека А. Миллера», 2019. 153 с.
2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / Т.А. Полякова [и др.]. – М.: Юрайт, 2018. 325 с.
3. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учеб. пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н/ Прохожев. СПб.: Университет ИТМО, 2016. 168 с.
4. Трещев, И.А. Организационное и правовое обеспечение информационной безопасности: для студентов и специалистов / И.А.Трещев. Екатеринбург: Издательские решения, 2019. 760 с.
5. Организационное и правовое обеспечение информационной безопасности / под ред. М.П. Сычева. М.: МГТУ им. Н.Э. Баумана, 2018. 292 с.
6. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин. – СПб.: СПбНИУИТМО, 2014. – 173 с.
7. Карпычев В.Ю. Защита информации: организационно-правовые основы: учеб. пособие / В.Ю. Карпычев; Нижегород. гос. техн. ун-т. им. Р.Е. Алексеева. – Нижний Новгород, 2021. 119 с.

6.3 Перечень журналов по профилю дисциплины:

Журнал «Информационное право» (http://lawinfo.ru/catalog/contents/informacionnoe-pravo/1/)

6.4 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению практически работ по дисциплине

«Организационно-правовые основы информационной безопасности» в бумажном варианте находятся на кафедре «Информатика и системы управления», в библиотеке НГТУ им. Р.Е. Алексеева. Электронные варианты методических указаний по выполнению практических заданий отправляются на электронные адреса групп.

Карпычев В.Ю. Защита информации: организационно-правовые основы: учеб. пособие / В.Ю. Карпычев; Нижегород. гос. техн. ун-т. им. Р.Е. Алексеева. – Нижний Новгород, 2021. 119 с.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

7.1 Перечень информационных справочных систем

Таблица 7.1 - Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	Лань	https://e.lanbook.com/
2	Юрайт	https://biblio-online.ru/

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
-	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html)
	Linux (https://www.linux.com/)
	OpenOffice (FreeWare) https://www.openoffice.org/ru/
	JDK 8 и выше (https://adoptopenjdk.net/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4 – Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	**2**	**3**
1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts

2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
3	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/accenv/

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	версия для слабовидящих

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);
- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

Перечень материально-технического обеспечения, необходимого для реализации программы магистратуры и проведения практических работ для студентов очного, обучения, включает в себя компьютерные классы

1. Ауд. 4408 кафедры «Информатика и системы управления»

Компьютеры, оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов.

мультимедийный проектор BenQ PB6240,

ноутбук Lenovo V130-151KB,

стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView.

Пакеты ПО (лицензионное):

- Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021).

Пакеты ПО (распространяемое по свободной лицензии):

- Apache OpenOffice;
- Linux Ubuntu 20.04 (https://releases.ubuntu.com/20.04/)

– Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/community/)

Также, для самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	**6421** учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; г. Нижний Новгород, Казанское ш., 12	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе AMD Athlon 2.8 Ггц, 4 Гб ОЗУ, 250 ГБ HDD, монитор 19” – 1шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• Microsoft Windows7 (подписка DreamSpark Premium, договор №Tr113003 от 25.09.14) • Gimp 2.8 (свободное ПО, лицензия GNU GPLv3); • Microsoft Office Professional Plus 2007 (лицензия № 42470655); • Open Office 4.1.1 (свободное ПО, лицензия Apache License 2.0) • Adobe Acrobat Reader (FreeWare); • 7-zip для Windows (свободнораспространяемое ПО, лицензиея GNU LGPL); Dr.Web (Сертификат №EL69-RV63-YMBJ-N2G7 от 14.05.19).
	6543 компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 12)	• Проектор Accer – 1шт; • ПК на базе IntelCoreDuo 2.93 ГГц, 2 Гб ОЗУ, 320 Гб HDD, монитор Samsung 19` – 11 шт.. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14); • Microsoft Office (лицензия № 43178972); • Adobe Design Premium CS 5.5.5 (лицензия № 65112135); • Adobe Acrobat Reader (FreeWare); • 7-zip для Windows (свободнораспространяемое ПО, лицензиея GNU LGPL); • Dr.Web (Сертификат №EL69-RV63-YMBJ-N2G7 от 14.05.19) • КонсультантПлюс (ГПД № 0332100025418000079 от 21.12.2018); Gimp 2.8 (свободное ПО, лицензия GNU GPLv3)

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Организационно-правовые основы информационной безопасности», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, практических занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием подробно разбираются на практических занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется балльно-рейтинговая система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме экзамена с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с заданиями, вопросами, использует в ответе дополнительный материал. Все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты, проявляет самостоятельность при выполнении заданий.

Результат обучения считается сформированным на пороговом уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент последовательно, четко и логически излагает учебный материал; справляется с заданиями, вопросами, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже трех по оценочной системе, что соответствует допороговому уровню.

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6) . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 Методические указания по освоению дисциплины на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Приводятся конкретные методические указания для обучающихся по выполнению реферата или эссе, требования к их оформлению, порядок сдачи

Примерная тематика рефератов

1. Доктрина информационной безопасности. Закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ.
2. Уголовный кодекс Российской Федерации (обеспечение ИБ) в т.ч. ст. 183 УК РФ Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну; глава 28 УК РФ Компьютерные преступления;
3. Обеспечение ИБ в трудовом кодексе РФ. Обеспечение ИБ в Кодексе об административных правонарушениях РФ. Ответственность за нарушение информационной безопасности
4. Виды тайн: Законы «О государственной тайне» , «О коммерческой тайне», «О персональных данных»
5. Правовое регулирование технической защиты информации, в том числе Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам».
6. Правовое регулирование Лицензирования в области ИБ, в том числе "Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79" (утв. ФСТЭК России 24.07.2017).
7. Правовое регулирование аттестации объектов информатизации
8. Правовое регулирование сертификации средств защиты информации
9. **Критическая информационная инфраструктура**

9.1. Закон 187-ФЗ 2017 «О безопасности критической информационной инфраструктуры Российской Федерации».

9.2. Приказ **ФСТЭК** от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

9.3. Приказ ФСТЭК от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»,

9.4. Приказ от 21 декабря 2017 г. N 235 Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования,

10. Документы ФСТЭК по персональным данным

10.1. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

10.2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год

10.3. Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

10.4. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (2 человека)

11. Документы ФСТЭК по ГИС

11.1. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказ ФСТЭК России от 11.02.2013г. N 17 (Зарегистрировано в Минюсте России 31.05.2013г. N 28608);

11.2. Методический документ. Меры защиты информации в государственных информационных системах», Приказ ФСТЭК России от 11 февраля 2014г.

10.5 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.6 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1 Типовые контрольные задания или иные +материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

Для текущего контроля знаний студентов по дисциплине проводится **комплексная оценка знаний,** включающая

- выполнение и защита рефератов **для студентов всех форм обучения**

Перечень тем рефератов – 18 шт.

11.1.1.Типовые задания для практических работ

Типовые задания для практических работ приведены в учебно-методических пособиях по проведению практических занятий.

11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

11.2.1.Защита курсового проекта/ работы

Курсовая работа не предусмотрена учебным планом

11.2.2.Экзамен для студентов очной формы обучения в 2 семестре.

Типовые вопросы для промежуточной аттестации в форме экзамена для студентов всех форм обучения

1. Конституция Российской Федерации: аспекты обеспечения ИБ
2. Стратегия национальной безопасности РФ до 2020 г: аспекты обеспечения ИБ
3. Доктрина информационной безопасности
4. Уголовный кодекс Российской Федерации (за исключением главы 28 и ст. 183 УК РФ)
5. Статья 183 УК РФ Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
6. Компьютерные преступления (глава 28 УК РФ)
7. Виды тайн по гражданскому кодексу РФ.
8. Обеспечение ИБ в трудовом кодексе РФ.
9. Обеспечение ИБ в кодексе об административных правонарушениях РФ.
10. Законы о государственной тайне и о служебной тайне
11. Иные виды тайн (по федеральным законам).
12. Закон об информации, информационных технологиях и защите информации № 149-ФЗ
13. Ответственность за нарушение информационной безопасности
14. Система стандартов по информационной безопасности
15. Стандарты ГОСТ Р ИСО/МЭК 1333х-х-200х (4 стандарта). Информационная технология. Методы и средства обеспечения безопасности.
16. ГОСТ Р ИСО/МЭК 15408-х-2008 (3 стандарта). Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.17. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Прчактические правила управления информационной безопасностью.

17. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Прчактические правила управления информационной безопасностью.

18. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

19. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

20. Р 50.1.056 Техническая защита информации. Основные термины и определения.

21. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

22. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

23. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

24. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения.

25. ГОСТ Р 53113.х-200х. (2 стандарта)Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов.

26. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

27. Отраслевые стандарты информационной безопасности

28 Стандарты Банка России

29 Нормативные документы ФСТЭК России

30. "Концепция защиты СВТ и АС от НСД к информации";

31. "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации"

32. "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ"

33. "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"

34. "Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов"

35. РД 19.06 2002. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий

36. РД. 04.06.1999. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

37. РД. 25.07 1997 Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации

38. РД.30.03.1992. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации

39. РД.30.03.1992. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

40. РД.30.03.1992. Защита от несанкционированного доступа к информации. Термины и определения

41. РД.30.03.1992. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации

В полном объеме оценочные средства имеются на кафедре Информатика и системы управления». Оценочные средства могут быть получены по требованию.

УТВЕРЖДАЮ:

Директор института ИРИТ

_____
“____”_____2021 г.

Лист актуализации рабочей программы дисциплины
«Б1.В.ОД.2 Организационно-правовые основы информационной безопасности**»**
индекс по учебному плану, наименование

для подготовки бакалавров/ специалистов/ **магистров**
Направление: 09.04.02 Информационные системы и технологии
Направленность: Безопасность информационных систем
Форма обучения очная
Год начала подготовки: 2021

Курс 1
Семестр 2
В рабочую программу не вносятся изменения. Программа актуализирована для 2021 г. начала подготовки.

Разработчик (и): __Карпычев В.Ю. д.т.н., профессор_____
(ФИО, ученая степень, ученое звание)
«__»_____20__г.
Рабочая программа пересмотрена и одобрена на заседании кафедры ИСУ
_____ протокол № _____ от «__» _____20__ г.

Заведующий кафедрой _____

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИСУ _____ «__» _____ 20__ г.

Методический отдел УМУ:_____ «__» _____ 20__ г.
_____