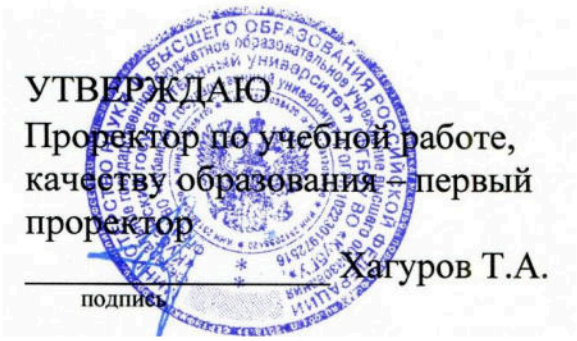
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий



УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись

«02» __июня__ 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.08 ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление
подготовки/специальность 10.04.01 Информационная безопасность_

Направленность (профиль) / специализация Информационная безопасность_
интеллектуальных автоматизированных систем_____

Форма обучения _____очная_____

Квалификация _____магистр_____

Краснодар
2026

Рабочая программа дисциплины «ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ » составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 «Информационная безопасность»

Программу составил(и):

О. Н. Лапина, доцент., кандид. физ.-мат. наук
И.О. Фамилия, должность, ученая степень, ученое звание

подпись

Рабочая программа дисциплины утверждена на заседании кафедры вычислительных технологий, протокол № 11 «14 » мая 2026 г.

И.о. заведующего кафедрой (разработчика) Приходько Т.А. ___
(фамилия, инициалы подпись

Рабочая программа обсуждена на заседании кафедры вычислительных технологий № 11 «14 » мая 2026 г.

И.о. заведующего кафедрой (выпускающей) Приходько Т.А.___
(фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета
компьютерных технологий и прикладной математики
протокол №3 от «15» мая 2026 г.
Председатель УМК факультета

Н. Ю. Добровольская

подпись

фамилия, инициалы

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Схаляхо Ч.А., доцент КВВУ им.С.М.Штеменко, к.ф.-м.н., доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель и задачи освоения дисциплины

Целью преподавания и изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» является формирование у обучающихся фундаментальных и прикладных знаний в области основ организации и правового обеспечения работ в области информационной безопасности, а также формирование практических умений, навыков и компетенций по применению организационных и правовых принципов и норм для защиты информации.

1.2 Задачи дисциплины

Задачами дисциплины являются:

- приобретение студентами знаний по организационному обеспечению защиты информации и формирование практических навыков работы в конкретных условиях, необходимых для комплексного обеспечения безопасности информации;
- обеспечение основ правовой подготовки специалистов в области защиты информации, развитие навыков работы с нормативно-правовыми документами, приобретение знаний и навыков, необходимых для комплексного обеспечения безопасности информации.

1.3 Место дисциплины (модуля) в образовательной программе

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части блока Б1 Дисциплины (модули).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Обеспечение безопасности компьютерных систем», «Теоретические основы информационной безопасности».

Знания, получаемые при изучении основ защиты информации, используются при изучении других дисциплин и работе над выпускной работой.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **профессиональных компетенций и соотнесенных с ними индикаторов достижения компетенций:** ОПК-2; ОПК-5.

Код и наименование индикатора*	**Результаты обучения по дисциплине** ***(знает, умеет, владеет (навыки и/или опыт деятельности))***
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	
ОПК-2.1. Знает методы концептуального проектирования технологий систем обеспечения информационной безопасности	Знает методы организации и правового обеспечения работ по защите информации

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-2.2. Умеет разрабатывать технический проект системы (подсистемы, либо компонента системы) обеспечения информационной безопасности	Умеет разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности предприятия
ОПК-2.3. Владеет навыками проектирования подсистемы обеспечения информационной безопасности	Владеет навыками проектирования подсистемы обеспечения защиты информационной безопасности .
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	
ОПК-5.1 Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает научно-методологические основы обеспечения работ по защите информации
ОПК-5.2 Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет разрабатывать системы типовых документов по защите информации.
ОПК-5.3 Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет навыками подготовки научно-технических отчетов, обзоров научных трудов, официальных документов в области защиты информации.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.
Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 5 зач. ед. (180 часа), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид учебной работы	Всего часов	Семестры (часы)	
		1	
Контактная работа в том числе:	**92,3**	**92,3**	
Аудиторные занятия (всего):	72	72	
В том числе:			
Занятия лекционного типа	36	36	
Занятия семинарского типа (семинары, практ. занятия)			
Лабораторные занятия	36	36	
Иная контактная работа	0,3	0,3	
Контроль самостоятельной работы (КСР)	20	20	
Промежуточная аттестация (ИКР)			
Самостоятельная работа, в том числе	**52**	**52**	
В том числе:			
Курсовая работа			
Проработка учебного (теоретического) материала	26	26	
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	26	26	
Реферат			

Подготовка к текущему контролю			
Контроль:	**экзамен**	**экзамен**	
Подготовка к экзамену	35,7	35,7	
Общая трудоёмкость	**180**	**180**	
в т.ч. контактная работа	**72,3**	**72,3**	

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины. Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	КСР	ЛР	СРС
1	2	3	4	5	6	7
1.	Информация как объект правового регулирования	6	2		2	2
2.	Угрозы информационной безопасности.	10	2	2	2	4
3.	Организация работ по защите информации	8	2	2	2	2
4.	Нормативно-правовая база обеспечения защиты информации в России	10	2	2	2	4
5.	Структура и функции органов защиты информации.	10	4		4	2
6.	Правовой режим защиты государственной тайны	10	2	2	2	4
7.	Правовые режимы защиты конфиденциальной информации	10	2	2	2	4
8.	Подбор персонала и организация допуска к информации ограниченного доступа	6	2		2	2
9.	Организация работы с персоналом, обладающим конфиденциальной информацией.	12	4	2	2	4
10.	Организация защиты информации при взаимодействии со сторонними организациями	6	2		2	2
11.	Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.	10	2	2	2	4
12	Правовая охрана результатов интеллектуальной деятельности	10	2	2	2	4

13	Правовая защита информации, составляющей персональные данные.	10	2	2	2	4
14.	Особенности правовой защиты сведений, составляющих различные виды тайн	8	2		2	4
15.	Правовое обеспечение безопасности информации в информационных системах.	18	4	2	6	6
	ИТОГО по разделам дисциплины	144	36	20	36	52
	Подготовка к экзамену	35,7				
	ИКР	0,3				
	КСР					
	Общая трудоёмкость по дисциплине	180				

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Информация как объект правового регулирования	Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Правовое определение понятия "информация". Документирование информации. Понятие информационных ресурсов. Виды информации по категориям доступа и распространения. Общедоступная информация. Информация ограниченного доступа. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ. Понятие и виды защищаемой информации по законодательству РФ. Цели защиты информации.	ЛР
2	Угрозы информационной безопасности.	Основные понятия. Классификация угроз. Источники и каналы утечки информации.	

3	Организация работ по защите информации	Перечень и общее содержание основных вопросов обеспечения работ по защите информации. Общая структура системы обеспечения защиты информации. Определение понятия «Комплексная система защиты информации» и элементы этой системы. Понятие "Организационная защита информации". Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией.	
4	Нормативно-правовая база обеспечения защиты информации в России	Конституционное законодательство о защите информации. Доктрина информационной безопасности Российской Федерации. Обзор законодательных актов общего характера, содержащих положения о защите информации. Специальное законодательство по защите информации. Особая роль законов «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О государственной тайне», "О персональных данных", "Об электронной подписи", "Об оперативно-розыскной деятельности", "О техническом регулировании», "О безопасности критической информационной инфраструктуры Российской Федерации". Законы субъектов РФ, регламентирующие вопросы защиты информации. Подзаконные правовые акты, регулирующие процессы защиты информации. Роль подзаконных нормативных документов ФСТЭК РФ и ФСБ РФ. Основные документы ФСТЭК России определяющие требования по защите информации. Нормативно-правовые акты, устанавливающие юридическую ответственность за правонарушения в сфере защиты информации.	
5	Структура и функции органов защиты информации.	Органы государственной власти, ответственные за защиту информации в стране. Нормативно-правовые акты, определяющие права и обязанности органов государственной власти, юридических и физических лиц по защите информации. Служба информационной безопасности предприятия. Состав, задачи, основные направления деятельности службы информационной безопасности предприятия. Основные направления деятельности по взаимодействию с правоохранительными органами и службами обеспечения информационной безопасности. Политика информационной безопасности предприятия.	

6	Правовой режим защиты государственной тайны	Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в РФ. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная)	
7	Правовые режимы защиты конфиденциальной информации	Понятие информации конфиденциального характера по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (дисциплинарная, гражданско-правовая, административная и уголовная).	
8	Подбор персонала и организация допуска к информации ограниченного доступа.	Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Порядок подбора персонала на должности, связанные с работой с конфиденциальной информацией. Особенности документирования трудовых отношений с персоналом, обладающим конфиденциальной информацией. Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.	
9	Организация работы с персоналом, обладающим конфиденциальной информацией.	Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Основные формы воздействия на персонал как методы мотивации: использование различных форм вознаграждения, управление карьерой, привлечение к участию в прибылях, воспитание фирменного патриотизма и др. Дисциплинарная ответственность. Организация контроля за соблюдением персоналом требований режима защиты информации. Основные меры по защите	

		информации при увольнении сотрудника. Понятие служебное расследование по фактам разглашения информации. Цели и задачи служебного расследования. Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.	
10	Организация защиты информации при взаимодействии со сторонними организациями	. Отражение вопросов защиты информации в гражданско-правовых договорах о взаимодействии. Организация защиты информации при подготовке материалов к открытому опубликованию. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Подготовка помещений для проведения конфиденциальных9 мероприятий, организация их аттестации. Организация защиты информации при приеме в организации посетителей и командированных лиц.	
11	Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.	Понятие лицензирования по российскому законодательству. В Закон "О лицензировании отдельных видов деятельности". Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие подтверждения соответствия по российскому законодательству, формы подтверждения. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.	
12	Правовая охрана результатов интеллектуальной деятельности	Понятие интеллектуальной собственности. Общие положения по регулированию отношений в области защиты интеллектуальной собственности. Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав. Особенности правовой защиты объектов патентного права. Защита авторских прав на программы для ЭВМ и базы данных. Правовая защита секретов производства (ноу-хау). Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право). Правовая охрана баз данных, топологий	

		интегральных микросхем и единых технологий. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав. Ответственность за правонарушения в сфере интеллектуальной собственности.	
13	Правовая защита информации, составляющей персональные данные.	Определение понятия «Персональные данные». Принципы и условия обработки персональных данных. Особенности обработки и защиты персональных данных в информационных системах. Ответственность за правонарушения.	
14	Особенности правовой защиты сведений, составляющих различные виды тайн	Личная и семейная тайна. Тайна голосования. Тайна исповеди. Тайна усыновления. Служебная тайна. Защита сведений, составляющих тайну следствия и судопроизводства. Налоговая тайна. Таможенная тайна. Защита профессиональной тайны. Журналистская тайна. Нотариальная тайна. Страховая тайна. Врачебная тайна. Тайна аудита. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Банковская тайна.	
15	Правовое обеспечение безопасности информации в информационных системах.	Доктрина информационной безопасности России об угрозах безопасности информационным системам. Особенности правовой защиты информационных и телекоммуникационных систем. Гражданско-правовые, уголовно-правовые и административно-правовые нормы защиты информации в информационных и телекоммуникационных системах.	

2.3.2 Занятия семинарского типа

Учебным планом не 5предусмотрены.

2.3.3 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ
1	1	*Характеристика правоотношений в сфере защиты информации.* Проработка нормативно-правовых актов: Указа Президента РФ от 6 марта 1997г. № 188, ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
2	2	*Угрозы информационной безопасности.* Проработка пройденного материала. Изучение документов ФСТЭК РФ: Приказ ФСТЭК России от 11 февраля 2013 г. N 17 База данных угроз (bdu.fstec.ru); Методический документ ФСТЭК РФ «Методика оценки угроз безопасности информации»
3	3	Проработка нормативно-правового акта: ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ,

4	4	*Проработка нормативно-правовых актов:* "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020), Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
5	5	*Структура и функции органов защиты информации.* Проработка нормативно-правовых актов: Указ Президента РФ от 20.01.1996 N 71 "Вопросы Межведомственной комиссии по защите государственной тайны", Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю", Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ
6	5	*Служба информационной безопасности предприятия.* Изучение документов: Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановление Правительства РФ от 15.07.2022 N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и11 типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)", "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности", "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования”.
7	6	*Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.* Изучение документов: Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ, Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности
8	7	*Правовые режимы защиты конфиденциальной информации.* Поиск и работа с нормативно-правовыми актами по тематике. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
9	8	*Подбор персонала и организация допуска к информации ограниченного доступа.* Изучение документов Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ.Проработка нормативно-правовых актов ГОСТ Р ИСО/МЭК 27002- 2012 "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил

		менеджмента информационной безопасности
10	9	*Текущая работа с персоналом, обладающим конфиденциальной информацией*. Проработка нормативно-правовых актов: Трудовой кодекс РФ, ГОСТ "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности" (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст)
11	10	*Организация защиты информации при взаимодействии со сторонними организациями.* Проработка нормативно-правовых актов: "ГОСТ Р ИСО/МЭК 27002- 2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности" (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст), Гражданский кодекс РФ; Приказ ФСТЭК России от 29 апреля 2021 г. N 77
12	11	Проработка нормативно-правовых актов: Закон "О лицензировании отдельных видов деятельности". Постановление Правительства Российской Федерации от 15 апреля 1995 г. N 333 Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79, О лицензировании деятельности по технической защите конфиденциальной информации. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ О техническом регулировании.
13	12	*Правовая защита информации, составляющей интеллектуальную собственность.* Проработка нормативно-правовых актов: Гражданский кодекс РФ, "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149- ФЗ, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
14	13	*Правовая защита информации, составляющей персональные данные.* Работа с нормативно-правовыми актами: Федеральный закон от 27 июля 2006 г. N 152-ФЗ, Приказ ФСТЭК России от 18 февраля 2013 г. N 21; Приказ ФСБ России от 10 июля 2014 года N 378
15	14	Особенности правовой защиты сведений, составляющих различные виды тайн. Поиск и работа с нормативно-правовыми актами по тематике.
16	15	*Правовое обеспечение безопасности информации в информационных системах*. Проработка нормативно-правовых актов: Доктрина информационной безопасности России, ГК РФ, УК РФ, КОАП РФ, Приказ ФСТЭК России от 11 февраля 2013 г. N 17, Приказ ФСТЭК России от 18 февраля 2013 г. N 21
17	15	Разработка проекта технического задания по созданию системы обеспечения информационной безопасности.
18	15	Защита проекта технического задания по созданию системы обеспечения информационной безопасности.

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.3.5 Самостоятельное изучение разделов дисциплины

Раздел 2. Обзор руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России). Аспекты защищённых ИС, фигурирующие в требованиях ФСТЭК.

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

– Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

– Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.

– Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

– Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:

– Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.

– Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

– Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

– Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

– Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

– Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.

– Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя:

– работа в малых группах (команде) - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности;

– проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

– анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

– развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	количество интерактивных часов
1	Л, ЛР	Практические занятия в режимах взаимодействия «преподаватель – студент» и «студент – студент»	10
Итого			10

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Методы поисковой оптимизации».

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств итоговой аттестации (экзамен в 6 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на экзамене (для выявления знания и понимания теоретического материала дисциплины).

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1.	Информация как объект правового регулирования	ОПК-2.	ЛР	Вопросы 1-8
2.	Угрозы информационной безопасности.	ОПК-2	ЛР	Вопросы 9-10
3.	Организация работ по защите информации	ОПК-2	ЛР	Вопрос 11-14

4.	Нормативно-правовая база обеспечения защиты информации в России	ОПК-5	ЛР	Вопросы 15-19
5.	Структура и функции органов защиты информации.	ОПК-2	ЛР	Вопросы 20-22
6.	Правовой режим защиты государственной тайны	ОПК-5	ЛР	Вопросы 23-26
7.	Правовые режимы защиты конфиденциальной информации	ОПК-5	ЛР	Вопросы 27-29
8.	Подбор персонала и организация допуска к информации ограниченного доступа.	ОПК-2	ЛР	Вопросы 30-33
9.	Организация работы с персоналом, обладающим конфиденциальной информацией.	ОПК-2	ЛР	Вопросы 34-37
10.	Организация защиты информации при взаимодействии со сторонними организациями	ОПК-2	ЛР	Вопросы 38-41
11.	Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.	ОПК-5	ЛР	Вопросы 42-46
12.	Правовая охрана результатов интеллектуальной деятельности	ОПК-5	ЛР	Вопросы 47-52
13.	Правовая защита информации, составляющей персональные данные.	ОПК-5	ЛР	Вопросы 53-54
14.	Особенности правовой защиты сведений, составляющих различные виды тайн	ОПК-5	ЛР	Вопросы 55-61
15.	Правовое обеспечение безопасности информации в информационных системах.	ОПК-2	ЛР	Вопросы 62-64

Показатели, критерии и шкала оценки сформированных компетенций

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **удовлетворительно /зачтено**)				
<u>на пороговом уровне</u>:				

1	ОПК-2.1. Знает методы концептуального проектирования технологий систем обеспечения информационной безопасности	Знает некоторые методы организации и правового обеспечения работ по защите информации	Опрос по теме лабораторных работ.	Вопросы 30-41, выносимые на экзамен
2	ОПК-2.2. Умеет разрабатывать технический проект системы (подсистемы, либо компонента системы) обеспечения информационной безопасности	Умеет разрабатывать типовой технический проект компонента системы обеспечения информационной безопасности предприятия	Опрос по теме лабораторных работ.	Вопросы 1-14,20-22 выносимые на экзамен
3	ОПК-2.3 Владеет навыками проектирования подсистемы обеспечения информационной безопасности	Владеет некоторыми навыками проектирования компонентов подсистемы обеспечения защиты информационной безопасности	Опрос по теме лабораторных работ.	Вопросы 62-64, выносимые на экзамен
4	ОПК-5.1 Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает методы анализа научно-методических материалов, официальных документов в области организации работ по защите информации	Опрос по теме лабораторных работ.	Вопросы 15-19, 23-29 выносимые на экзамен
5	ОПК-5.2 Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет разрабатывать типовые документы по защите информации.	Опрос по теме лабораторных работ.	Вопросы 42-61, выносимые на экзамен
6	ОПК-5.3 Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет базовыми навыками обзоров официальных документов в области защиты информации.	Опрос по теме лабораторных работ.	Вопросы 42-61, выносимые на экзамен
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **хорошо /зачтено**)				
<u>на базовом уровне:</u>				
7	ОПК-2.1. Знает методы концептуального проектирования технологий систем обеспечения информационной безопасности	Знает основные методы организации и правового обеспечения работ по защите информации	Опрос по теме лабораторных работ.	Вопросы 30-41, выносимые на экзамен

8	ОПК-2.2. Умеет разрабатывать технический проект системы (подсистемы, либо компонента системы) обеспечения информационной безопасности производства, для решения задач профессиональной деятельности	Умеет разрабатывать технический проект системы (либо подсистемы, либо компонента системы) обеспечения информационной безопасности предприятия	Опрос по теме лабораторных работ.	Вопросы 1-14,20-22 выносимые на экзамен
9	ОПК-2.3. Владеет навыками проектирования подсистемы обеспечения информационной безопасности	Владеет базовыми навыками проектирования подсистемы обеспечения защиты информационной безопасности	Опрос по теме лабораторных работ.	Вопросы 62-64, выносимые на экзамен
10	ОПК-5.1 Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает методы научного исследования научных трудов, официальных документов в области организации работ по защите информации	Опрос по теме лабораторных работ.	Вопросы 15-19, 23-29 выносимые на экзамен
11	ОПК-5.2 Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет разрабатывать системы типовых документов по защите информации.	Опрос по теме лабораторных работ.	Вопросы 42-61, выносимые на экзамен
12	ОПК-5.3 Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет навыками подготовки научно-технических отчетов, обзоров научных трудов, официальных документов в области защиты информации.	Опрос по теме лабораторных работ.	Вопросы 42-61, выносимые на экзамен
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **отлично /зачтено**)				
<u>на продвинутом уровне:</u>				
13	ОПК-2.1. Знает методы концептуального проектирования технологий систем обеспечения информационной безопасности	Знает методы организации и правового обеспечения работ по эффективной защите информации .	Опрос по теме лабораторных работ.	Вопросы 30-41, выносимые на экзамен
14	ОПК-2.2. Умеет разрабатывать технический проект системы (подсистемы,	Умеет разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения	Опрос по теме лабораторных работ.	Вопросы 1-14,20-22 выносимые на экзамен

	либо компонента системы) обеспечения информационной безопасности	комплексной информационной безопасности предприятия		
15	ОПК-2.3 Владеет навыками проектирования подсистемы обеспечения информационной безопасности	Владеет навыками проектирования подсистемы обеспечения комплексной защиты информации	Опрос по теме лабораторных работ.	Вопросы 62-64, выносимые на экзамен
16	ОПК-5.1 Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает научно-методологические основы обеспечения работ по защите информации	Опрос по теме лабораторных работ.	Вопросы 15-19, 23-29 выносимые на экзамен
17	ОПК-5.2 Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет разрабатывать системы типовых документов по комплексной защите информации.	Опрос по теме лабораторных работ.	Вопросы 42-61, выносимые на экзамен
18	ОПК-5.3 Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет навыками подготовки научно-технических отчетов, обзоров научных трудов, официальных документов, докладов, статей в области комплексной защиты информации.	Опрос по теме лабораторных работ.	Вопросы 42-61, выносимые на экзамен

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств для итоговой аттестации (экзамен в 7 семестре).

Оценка успеваемости осуществляется по результатам:
- выполнения лабораторных работ;
- ответа на экзамене.

Текущий контроль включает контрольную работу по итогам первой половины курса.

4.2.1 Перечень вопросов к экзамену

1. Понятие информационной системы, основные компоненты информационной системы.
2. Структура информационной сферы и характеристика ее элементов.
3. Информация как объект правоотношений. Правовое определение понятия "информация".
4. Документирование информации. Понятие информационных ресурсов. Виды информации по категориям доступа и распространения. Общедоступная информация. Информация ограниченного доступа.
5. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
6. Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности.

7. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
8. Понятие и виды защищаемой информации по законодательству РФ. Цели защиты информации.
9. Классификация угроз информационной безопасности.
10. Источники и каналы утечки информации.
11. Перечень и общее содержание основных вопросов обеспечения работ по защите информации.
12. Общая структура системы обеспечения защиты информации. Определение понятия «Комплексная система защиты информации» и элементы этой системы.
13. Понятие "Организационная защита информации". Сущность организационных методов защиты информации.
14. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией.
15. Конституционное законодательство о защите информации. Доктрина информационной безопасности Российской Федерации.
16. Обзор законодательных актов общего характера, содержащих положения о защите информации. Специальное законодательство по защите информации.
17. Законы субъектов РФ, регламентирующие вопросы защиты информации.
18. Подзаконные правовые акты, регулирующие процессы защиты информации. Роль подзаконных нормативных документов ФСТЭК РФ и ФСБ РФ. Основные документы ФСТЭК России определяющие требования по защите информации.
19. Нормативно-правовые акты, устанавливающие юридическую ответственность за правонарушения в сфере защиты информации.
20. Органы государственной власти, ответственные за защиту информации в стране. Нормативно-правовые акты, определяющие права и обязанности органов государственной власти, юридических и физических лиц по защите информации.
21. Служба информационной безопасности предприятия. Состав, задачи, основные направления деятельности службы информационной безопасности предприятия.
22. Основные направления деятельности по взаимодействию с правоохранительными органами и службами обеспечения информационной безопасности. Политика информационной безопасности предприятия.
23. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в РФ.
24. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
25. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны.
26. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).
27. Понятие информации конфиденциального характера по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.
28. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
29. Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (дисциплинарная, гражданско-правовая, административная и уголовная).
30. Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Порядок подбора персонала на должности, связанные с работой с конфиденциальной информацией.
31. Особенности документирования трудовых отношений с персоналом, обладающим

конфиденциальной информацией.

32. Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа.
33. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.
34. Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Основные формы воздействия на персонал как методы мотивации: использование различных форм вознаграждения, управление карьерой, привлечение к участию в прибылях, воспитание фирменного патриотизма и др. Дисциплинарная ответственность.
35. Организация контроля за соблюдением персоналом требований режима защиты информации. Основные меры по защите информации при увольнении сотрудника.
36. Понятие служебное расследование по фактам разглашения информации. Цели и задачи служебного расследования. Основания для проведения служебного расследования.
37. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.
38. Отражение вопросов защиты информации в гражданско-правовых договорах о взаимодействии.
39. Организация защиты информации при подготовке материалов к открытому опубликованию.
40. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Подготовка помещений для проведения конфиденциальных мероприятий, организация их аттестации.
41. Организация защиты информации при приеме в организации посетителей и командированных лиц.
42. Понятие лицензирования по российскому законодательству. Закон "О лицензировании отдельных видов деятельности". Виды деятельности, подлежащие лицензированию.
43. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации.
44. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности.
45. Понятие подтверждения соответствия по российскому законодательству, формы подтверждения.
46. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.
47. Понятие интеллектуальной собственности. Общие положения по регулированию отношений в области защиты интеллектуальной собственности.
48. Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав.
49. Особенности правовой защиты объектов патентного права. Защита авторских прав на программы для ЭВМ и базы данных.
50. Правовая защита секретов производства (ноу-хау). Объекты и субъекты авторского права. Авторские права (личные неимущественные права и исключительное право).
51. Правовая охрана баз данных, топологий интегральных микросхем и единых технологий. Защита интеллектуальных прав.
52. Юридическая ответственность за нарушение авторских прав. Ответственность за правонарушения в сфере интеллектуальной собственности.
53. Определение понятия «Персональные данные». Принципы и условия обработки персональных данных.
54. Особенности обработки и защиты персональных данных в информационных системах. Ответственность за правонарушения.
55. Личная и семейная тайна. Тайна голосования. Тайна исповеди. Тайна усыновления.
56. Служебная тайна. Защита сведений, составляющих тайну следствия и судопроизводства.

57. Налоговая тайна. Таможенная тайна. Защита профессиональной тайны.
58. Журналистская тайна. Нотариальная тайна.
59. Врачебная тайна. Тайна аудита.
60. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
61. Банковская тайна. Страховая тайна.
62. Доктрина информационной безопасности России об угрозах безопасности информационным системам.
63. Особенности правовой защиты информационных и телекоммуникационных систем.
64. Гражданско-правовые, уголовно-правовые и административно-правовые нормы защиты информации в информационных и телекоммуникационных системах.

Код контролируемой компетенции: ОПК-2; ОПК-5

4.2.2 Образцы билетов

Билет №1

1. Понятие информационной системы, основные компоненты информационной системы.
2. Понятие интеллектуальной собственности. Общие положения по регулированию отношений в области защиты интеллектуальной собственности.

Билет №2

1. Понятие и виды защищаемой информации по законодательству РФ. Цели защиты информации.
2. Особенности обработки и защиты персональных данных в информационных системах. Ответственность за правонарушения.

4.2.3 Критерии оценивания результатов обучения

Методические рекомендации, определяющие процедуры оценивания лабораторных работ.

Задание считается выполненным, если предоставлен исходный текст программы, который содержит не более 3 синтаксических ошибок, логика работы программы эффективна, программа работает на любых входных данных.

Методические рекомендации, определяющие процедуры оценивания на экзамене

Оценка «отлично»: точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «хорошо»: при ответе на один вопрос даны точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями; при ответе на второй вопрос имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или

неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «удовлетворительно»: при ответе на оба вопроса имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «неудовлетворительно»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

5. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ, ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Нормативные документы и ГОСТы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. № 237. 25.12.1993.
2. Гражданский кодекс Российской Федерации (Часть первая) от 30 ноября 1994 года N 51-ФЗ
3. Гражданский кодекс Российской Федерации (Часть вторая) от 26.01.1996 № 14- ФЗ // СЗ РФ. 1996. № 5. ст. 410.
4. Гражданский кодекс Российской Федерации часть 3 (ГК РФ ч.3) от 26 ноября 2001 года N 146-ФЗ
5. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) от 18.12.2006 № 230-ФЗ
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. ст. 2954.
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174- ФЗ // СЗ РФ. 2001. № 52 (ч. I).ст. 4921.
8. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Российская газета. № 256., 31.12.2001.
9. Гражданский кодекс Российской Федерации (Часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (1 ч.).ст. 5496.
10. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. стр. 8220-8235.
11. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ.1996. № 6. ст. 492.
12. Федеральный закон от 07.08.2001 № 119-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2001. № 33 (часть I).ст. 3422.
13. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной подписи» // СЗ РФ. 2002. № 2. ст. 127.
14. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ
15. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ
16. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. ст. 2895.
17. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.
18. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.
20. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3451.
21. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
22. Указ Президента РФ от 20.01.1996 N 71 "Вопросы Межведомственной комиссии по защите государственной тайны"

23. Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"
24. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
25. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40- ФЗ
26. Федеральный закон от 31.05.1996 N 61-ФЗ «Об обороне»
27. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера"
28. Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"
29. Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»
30. Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации»
31. Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации
32. Постановление Правительства РФ от 02.06.2008 N 418 "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации"
33. Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 03.02.2023) "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"
34. Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 10.07.2020) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"
35. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации"
36. Постановление Правительства РФ от 15.07.2022 N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)"
37. Приказ ФСБ РФ от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств"
38. Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

39. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

40. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

41. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

42. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

43. Приказ ФСТЭК России от 23 марта 2017 г. N 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. n 21, и в требования 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, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. n 31»

44. Приказ ФСТЭК России от 03.04.2018 N 55 (ред. от 19.09.2022) "Об утверждении Положения о системе сертификации средств защиты информации"

45. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

46. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

47. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности

48. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

49. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

5.2 Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583236 .
2. Организационное и правовое обеспечение информационной безопасности : учебник

для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372

3. *Суворова, Г. М.* Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588515

4. *Внуков, А. А.* Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584050

Дополнительная литература

1.. *Внуков, А. А.* Защита информации в банковских системах : учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2026. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584051

2. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/586060

5.3 Периодическая литература

1. Базы данных компании «Ист Вью» http://dlib.eastview.com
2. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

5.4 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронная библиотека Научной библиотеки КубГУ

http://megapro.kubsu.ru/MegaPro/Web

Электронный каталог
Поступления литературы в библиотеки филиалов
Поступления диссертаций и авторефератов
Статьи из периодики и научных сборников с 2016 г.
Статьи из периодики и научных сборников до 2016 г.
Газеты и журналы
Электронная библиотека трудов ученых КубГУ.

Электронно-библиотечные системы (ЭБС)

1. ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru/
2. ЭБС «Лань» https://e.lanbook.com
3. Образовательная платформа «Юрайт» https://urait.ru/
4. ЭБС «ZNANIUM» https://znanium.ru/
5. ЭБС «BOOK.ru» https://www.book.ru

Профессиональные базы данных российские

1. Национальная электронная библиотека https://rusneb.ru/
2. Базы данных компании «ИВИС» https://eivis.ru/
3. Научная электронная библиотека eLIBRARY.RU (НЭБ) http://www.elibrary.ru/
4. МИАН. Полнотекстовая коллекция математических журналов http://www.mathnet.ru
5. Журнал Квантовая электроника https://quantum-electron.lebedev.ru/arhiv/
6. Журнал Успехи физических наук https://ufn.ru/
7. Полнотекстовая коллекция журналов на платформе РЦНИ (Электронные версии научных журналов РАН) https://journals.rcsi.science/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная библиотечная система социо-гуманитарного знания «SOCHUM» https://sochum.ru/

Информационные справочные системы

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Профессиональные базы данных зарубежные

1. Журналы издательства Wiley https://onlinelibrary.wiley.com/
2. Полнотекстовая коллекция книг eBook Collections издательства SAGE Publications https://sk.sagepub.com/books/discipline
3. Полнотекстовая коллекция книг EBSCO eBook https://books.kubsu.ru/
4. Ресурсы Springer Nature https://link.springer.com/, https://www.nature.com/
5. Chemical Abstracts Service (CAS) SciFinder Discovery Platform https://scifinder-n.cas.org
6. Questel. База данных Orbit Premium edition https://www.orbit.com
7. Полнотекстовые коллекции книг издательства American Institute of Physics Publishing (AIPP Ebook) https://pubs.aip.org/books
8. Полнотекстовая архивная коллекция журналов издательства American Institute of Physics Publishing (AIPP Digital Archive) https://pubs.aip.org/
9. China National Knowledge Infrastructure. БД CNKI Academic Reference (AR) https://ar.oversea.cnki.net/

Базы данных открытого доступа

1. КиберЛенинка http://cyberleninka.ru/;
2. Американская патентная база данных https://www.uspto.gov/patents/search/patent-public-search
3. Лекториум ТВ - видеолекции ведущих лекторов России http://www.lektorium.tv/
4. Приоритетные научные направления РУДН. Специальные коллекции https://priority-lib.rudn.ru/

Базы данных КубГУ

1. Открытая среда модульного динамического обучения КубГУ https://openedu.kubsu.ru/
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://infoneeds.kubsu.ru/
3. Электронный архив документов КубГУ http://docspace.kubsu.ru/

6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для освоения учебного материала студенту необходимо ознакомиться со структурой курса и методикой овладения материалом. Весь курс построен от простого к сложному, и каждая его тема основана на материалах предыдущих тем. В этой связи студенту необходимо не терять логику курса и строго ей следовать. В лекционном материале даются, как правило, теоретические сведения, которые раскрываются на практических примерах. Для закрепления теоретических знаний студент получает индивидуальное задание к циклу лабораторных работ, который охватывает весь теоретический материал. Каждая лабораторная работы защищается по мере выполнения. Таким образом, выполняя весь цикл лабораторных работ, студент получает и осваивает знания в соответствии с компетенциями курса. По выступлениям на круглом столе с преподавателем согласовывается тема выступления и готовится само выступление. Во время текущей аттестации могут проводиться контрольные опросы по начитанному теоретическому и практическому материалу.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся-инвалидом или лицом с ограниченными возможностями здоровья.

7. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1 Перечень информационных технологий

– Проверка домашних заданий и консультирование посредством электронной почты.

– Использование электронных презентаций при проведении лекций и практических занятий.

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения

1. Visual Studio Code, версия 1.52+.
2. Visual Studio 19 и выше.
3. Программы для демонстрации и создания презентаций.

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
3.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
4.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Примечание: конкретизация аудиторий и их оснащение определяется ОПОП.