Министерство науки и высшего образования РФ

ФГБОУ ВО Уральский государственный лесотехнический университет

Социально-экономический институт

Кафедра экономики и экономической безопасности

Рабочая программа дисциплины

включая фонд оценочных средств и методические указания
для самостоятельной работы обучающихся

Б1.О.21 ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) – "Цифровая экономика"
Квалификация – бакалавр
Количество зачётных единиц (*часов*) – 3 (*108*)

г. Екатеринбург, 2025

Разработчик: доцент, к.п.н. И.В.Щепеткина

Рабочая программа утверждена на заседании кафедры экономики и экономической безопасности (протокол № 2 от «05» 02 2025 года)

Заведующий кафедрой С.И.Колесников

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией и социально-экономического института
(протокол № 2 от «06» марта 2025 года)

Председатель методической комиссии СЭИ А.В. Чевардин

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ Ю.А. Капустина

« 06 » марта 2025 г.

Оглавление

1. Общие положения

Дисциплина «Правовые основы защиты информации» относится к обязательной части блока Б1 учебного плана, входящего в состав образовательной программы высшего образования 09.03.03 Прикладная информатика (профиль – Цифровая экономика).

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Правовые основы защиты информации» являются:

- Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 08.08.2024) "Об образовании в Российской Федерации" (с изм. и доп., вступ. в силу с 01.09.2024).
- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный приказом Минобрнауки России от 06.04.2021 № 245.
- Учебные планы образовательной программы высшего образования направления 09.03.03 – Прикладная информатика (профиль – Цифровая экономика) подготовки бакалавров по очной, заочной, очно-заочной формам обучения, одобренные Ученым советом УГЛТУ (Протокол № 03 от 20.03.2025) и утвержденного ректором УГЛТУ (20.03.2025).
- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.03 «Прикладная информатика» (уровень высшего образования бакалавриат), утвержденный приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 922.
- Профессиональный стандарт 06.015 Профессиональный стандарт "Специалист по информационным системам", утвержденный приказом Министерства труда и социальной защиты Российской Федерации, утвержден приказом Министерства труда и социальной защиты Российской Федерации от 13.07.2023 № 586н

Обучение по образовательной программе 09.03.03 – Прикладная информатика (профиль – Цифровая экономика) осуществляется на русском языке.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемыми результатами обучения по дисциплине являются знания, умения, владения и/или опыт деятельности, характеризующие этапы/уровни формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы в целом.

Цель дисциплины – усвоение законодательно-правовых основ правового обеспечения информационной безопасности, принципов построения систем обеспечения информационной безопасности, анализа и оценки угроз информационной безопасности объектов, средств и методов физической защиты объектов, изучение лицензионной и сертификационной деятельности в области защиты информации

Задачи дисциплины:

– формирование теоретических знаний в области правовых и организационных основ защиты информации, средств и методов защиты информации, построения и организации функционирования систем защиты информации в компьютерных системах, методов несанкционированного доступа и взлома;

– изучение вопросов политики безопасности, стандартов безопасности России и развитых стран;

– изучение тенденций и перспектив развития средств защиты информации;

– выработка умения разрабатывать политику безопасности организации, организовать защиту рабочего места, локальной сети.

Процесс изучения дисциплины направлен на формирование следующих профессиональных компетенций:

– **УК-2 –** способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

– **ОПК-3 –** способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

– **ОПК-**4 - способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

В результате изучения дисциплины обучающийся должен:

знать:

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– нормативные документы в обеспечения защиты информации ограниченного доступа;

– принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;

– нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе.

уметь:

– осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей;

– применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

владеть

– навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки передачи информации;

– навыками соблюдения режима секретности;

– навыками противодействия утечке компьютерной информации;

– навыками использования электронной цифровой подписи;

– специальной терминологией, применяемой в процессе защиты информации;

– навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности.

3. Место дисциплины в структуре образовательной программы

Данная учебная дисциплина относится к обязательным дисциплинам, что означает формирование в процессе обучения у бакалавра основных профессиональных знаний и компетенций в рамках выбранного профиля.

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин ОПОП и написания выпускной квалификационной работы.

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

Обеспечивающие	Сопутствующие	Обеспечиваемые
Правоведение	Методы принятия решений Разработка программных приложений Управление проектами	Интеллектуальные информационные системы Информационная безопасность

Указанные связи дисциплины дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что обеспечивает требуемый теоретический уровень и практическую направленность в системе обучения и будущей деятельности выпускника.

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины

Вид учебной работы	Всего академических часов		
	Очная форма обучения	Заочная форма обучения	Очно-заочная форма обучения
Контактная работа с преподавателем*:	**46,25**	**12,25**	**32,25**
лекции (Л)	16	4	18
практические занятия (ПЗ)	30	8	14
лабораторные работы (ЛР)	-	-	-
иные виды контактной работы	0,25	0,25	0,25
Самостоятельная работа обучающихся:	**61,75**	**95,75**	**75,75**
изучение теоретического курса	30	72	52
подготовка к текущему контролю	20	20	20
Контрольная работа	-		
подготовка к промежуточной аттестации	**11,75**	**3,75**	**3,75**
Вид промежуточной аттестации:	**Зачет**	**Зачет**	**Зачет**
Общая трудоемкость, з.е./ часы	**3/108**	**3/108**	**3/108**

*Контактная работа обучающихся с преподавателем, в том числе с применением дистанционных образовательных технологий, включает занятия лекционного типа, и (или) занятия семинарского типа, лабораторные занятия, и (или) групповые консультации, и (или) индивидуальную работу обучающегося с преподавателем, а также аттестационные испытания промежуточной аттестации. Контактная работа может включать иные виды учебной деятельности, предусматривающие групповую и индивидуальную работу обучающихся с преподавателем. Часы контактной работы определяются Положением об организации и проведении контактной работы при реализации образовательных программ высшего образования, утвержденным Ученым советом УГЛТУ от 25 февраля 2020 года.

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов

5.1. Трудоемкость разделов дисциплины

очная форма обучения

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Основные понятия в области охраны и защиты информации	2	2		4	4
2	Регламентация деятельности по информационной безопасности РФ	2	6		8	6
3	Правовое регулирование вопросов в области государственной тайны	2	6		8	10
4	Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	4	6		10	10
5	Правовое регулирование вопросов в области конфиденциальной информации	4	6		10	10
6	Правовое обеспечение защиты информационных ресурсов	2	4		6	10
Итого по разделам:		**16**	**30**		**46**	**50**
Промежуточная аттестация		x	x	x	**0,25**	**11,75**
Всего		**108**				

Заочная форма обучения

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Основные понятия в области охраны и защиты информации	1	-		1	15
2	Регламентация деятельности по информационной безопасности РФ	1	2		3	16
3	Правовое регулирование вопросов в области государственной тайны	1	2		3	15
4	Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	-	-		-	15
5	Правовое регулирование вопросов в области	-	2		2	15

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
	конфиденциальной информации					
6	Правовое обеспечение защиты информационных ресурсов	1	2		3	16
Итого по разделам:		**4**	**8**		**12**	**92**
Промежуточная аттестация		x	x	x	**0,25**	**3,75**
Всего		**108**				

Очно-заочная форма обучения

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Основные понятия в области охраны и защиты информации	2	2		4	12
2	Регламентация деятельности по информационной безопасности РФ	2	2		4	12
3	Правовое регулирование вопросов в области государственной тайны	2	2		4	12
4	Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	4	2		6	12
5	Правовое регулирование вопросов в области конфиденциальной информации	4	2		6	12
6	Правовое обеспечение защиты информационных ресурсов	4	4		8	12
Итого по разделам:		**18**	**14**		**32**	**72**
Промежуточная аттестация		x	x	x	**0,25**	**3,75**
Всего		**108**				

5.2 Содержание занятий лекционного типа

Тема 1 Основные понятия в области охраны и защиты информации

Понятие системы права. Понятие и виды защищаемой информации по российскому законодательству. Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота. Четыре уровня правового обеспечения защиты информации. Характеристика уровней правового обеспечения защиты информации. Категории информации с ограниченным доступом.

Тема 2 Регламентация деятельности по информационной безопасности РФ

Органы законодательства, регламентирующие деятельность по информационной безопасности. Структура органов власти по защите информации в Российской Федерации. Совет Безопасности Российской Федерации. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ). Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ). Комитет по вопросам информационной безопасности. Анализ законодательства РФ в области информационной безопасности РФ. Конституционные основы правового обеспечения информационной безопасности РФ. Доктрина информационной безопасности РФ.

Тема 3 Правовое регулирование вопросов в области государственной тайны

Перечень сведений, отнесенных законодателем к категории: государственная тайна по сферам жизнедеятельности общества и государства. Правовой режим защиты государственной тайны. Степени секретности сведений и грифы секретности носителей этих сведений. Органы защиты государственной тайны. Три формы допуска к секретным сведениям. Организация допуска должностных лиц и граждан к государственной тайне. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Тема 4 Правовое регулирование вопросов в области остальных видов информации ограниченного доступа

Понятие коммерческой тайны. Правовой режим защиты коммерческой тайны. Требования для классификации сведений категории коммерческой тайны. Понятие банковской тайны. Объекты банковской тайны. Правовой режим защиты банковской тайны. Понятие профессиональной тайны. Требования для классификации сведений категории профессиональной тайны. Объекты профессиональной тайны.

Тема 5 Правовое регулирование вопросов в области конфиденциальной информации

Правовой режим защиты конфиденциальной информации. Понятие служебной тайны. Требования для классификации сведений категории служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне. Понятие персональных данных. Регуляторы в области защиты персональных данных. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Основные объекты интеллектуальной собственности. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области защиты интеллектуальной собственности в области конфиденциальной информации. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Тема 6 Правовое обеспечение защиты информационных ресурсов

Информационные ресурсы как объект защиты. Классификация информационных ресурсов. Государственные и негосударственные информационные ресурсы. Пользование информационными ресурсами. Системы защиты информационных ресурсов.

5.3 Темы и формы занятий семинарского типа

Учебным планом по дисциплине предусмотрены практические занятия.

№	Наименование раздела дисциплины (модуля)	Форма проведения занятия	Трудоемкость, час		
			Очная форма обучения	Заочная форма обучения	Очно-заочная форма обучения
1	Основные понятия в области охраны и защиты информации	Рассмотрение учебных ситуаций по теме, обсуждение проблемных ситуаций	2	-	2
2	Регламентация деятельности по информационной безопасности РФ	Рассмотрение учебных ситуаций по теме, работа в малых группах, обсуждение проблемных ситуаций	6	2	2
3	Правовое регулирование вопросов в области государственной тайны	Рассмотрение учебных ситуаций по теме, работа в малых группах, обсуждение проблемных ситуаций	6	2	2
4	Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	Рассмотрение учебных ситуаций по теме, обсуждение проблемных ситуаций, деловая игра	6	-	2
5	Правовое регулирование вопросов в области конфиденциальной информации	Рассмотрение учебных ситуаций по теме, работа в малых группах, обсуждение проблемных ситуаций, деловая игра	6	2	2
6	Правовое обеспечение защиты информационных ресурсов	Рассмотрение учебных ситуаций по теме, обсуждение проблемных ситуаций	4	2	4
Итого часов:			**30**	**8**	**14**

5.4 Детализация самостоятельной работы

№	Наименование раздела дисциплины (модуля)	Вид самостоятельной работы	Трудоемкость, час		
			Очная форма обучения	Заочная форма обучения	Очно-заочная форма обучения
1	Основные понятия в области охраны и защиты информации	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	4	15	12

№	Наименование раздела дисциплины (модуля)	Вид самостоятельной работы	Трудоемкость, час		
			Очная форма обучения	Заочная форма обучения	Очно-заочная форма обучения
2	Регламентация деятельности по информационной безопасности РФ	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	6	16	12
3	Правовое регулирование вопросов в области государственной тайны	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	10	15	12
4	Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	10	15	12
5	Правовое регулирование вопросов в области конфиденциальной информации	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	10	15	12
6	Правовое обеспечение защиты информационных ресурсов	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	10	16	12
9	Подготовка к промежуточной аттестации	Подготовка к текущему контролю (тесту, опросу), подготовка докладов и презентаций	**11,75**	**3,75**	**3,75**
Итого часов:			**61,75**	**96**	**75,75**

6. Перечень учебно-методического обеспечения по дисциплине
Основная и дополнительная литература

№	Автор, наименование	Год издания	Примечание
	Основная литература		
1	Прохорова, О.В. Информационная безопасность и защита информации / О.В. Прохорова. - 5-е изд., стер. - Санкт-Петербург: Лань, 2023. - 124 с. - ISBN 978-5-507-46010-6. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/293009 - Режим доступа: для авториз. пользователей.	2023	Полнотекстовый доступ при входе по логину и паролю*
	Дополнительная литература		
2	Леонтьев, А. С. Защита информации: учебное пособие / А. С. Леонтьев. - М.: РТУ МИРЭА, 2021. - 79 с. - Текст: электронный // Лань: электронно-библиотечная система. - URL:	2021	Полнотекстовый доступ при входе по логину и паролю*

№	Автор, наименование	Год издания	Примечание
	https://e.lanbook.com/book/182491 - Режим доступа: для авториз. пользователей.		
3	Груздева, Л. М. Защита информации: учебное пособие / Л. М. Груздева. - М.: РУТ (МИИТ), 2019. - 144 с. - ISBN 978-5-7876-0326-2. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/188703 — Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*
4	Информационное право: учебно-методическое пособие / составители О.А. Воробьёва, Ю.А. Полякова. - Тольятти: ТГУ, 2021. - 93 с. - ISBN 978-5-8259-1594-4. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/243215 - Режим доступа: для авториз. пользователей.	2021	Полнотекстовый доступ при входе по логину и паролю*
5	Леонтьев, А. Н. Информационное право: учебное пособие / А. Н. Леонтьев. - Волгоград: ВолгГТУ, 2019. - 76 с. - ISBN 978-5-9948-3293-6. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/157203 - Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*
6	Милкина, Е. В. Информационное право: учебно-методическое пособие / Е. В. Милкина. – М.: РТУ МИРЭА, 2019. - 99 с. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/171458 - Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*

*- прежде чем пройти по ссылке, необходимо войти в систему

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий.

Электронные библиотечные системы

– электронно-библиотечная система «Лань», коллекции издательства "Лань" Дог. №025/24/-ЕП-44-03 от 25.03.24; срок действия с 09.04.2024 до 9.04.2025; коллекции других издательств Дог. №024/24/-ЕП-44-03 от 25.03.24; срок действия с 09.04.2024 до 09.04.2025; коллекция "ФПУ. 10-11 кл. Изд-во "Просвещение" Дог. № 035/24-ЕП-44-03 от 29.05.2024; срок действия с 01.09.2024 до 01.09.2025; сетевая электронная библиотека Дог. №0136/20-223-06 от 24.03.20;

– электронно-библиотечная система «Университетская библиотека онлайн». Договор №038/24-ЕП-44-03 от 19.06.2024

- универсальная база данных East View (ООО «ИВИС»), Договор № 407-П/002/25-ЕП-44-0 от 13.01.25;

Срок действия договоров продлевается ежегодно.

Справочные и информационные системы

– справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/). Договор сопровождения экземпляров системы КонсультантПлюс №025/ЗК от 25.02.2025. Срок с 25.02.2025 г по 24.02.2026 г.;

– справочно-правовая система «Система ГАРАНТ». Свободный доступ (режим доступа:

http://www.garant.ru/company/about/press/news/1332787/);
– программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат. ВУЗ» (URL: https://www.antiplagiat.ru/). Договор №6414/0107/23-ЕП-223-03 от 27.02.2023 года.
– Информационная система 1С: ИТС (http://its.1c.ru/). Режим доступа: свободный
Срок действия договоров продлевается ежегодно.

Профессиональные базы данных

– Федеральная служба государственной статистики. Официальная статистика (http://www.gks.ru/). Режим доступа: свободный.
– Электронный фонд правовых и нормативно-технических документов // Акционерное общество «Информационная компания «Кодекс» (https://docs.cntd.ru/). Режим доступа: свободный.
– Экономический портал (https://institutiones.com/). Режим доступа: свободный.
– Информационная система РБК (https://ekb.rbc.ru/). Режим доступа: свободный.
– Официальный интернет-портал правовой информации (http://pravo.gov.ru/). Режим доступа: свободный
– База полнотекстовых и библиографических описаний книг и периодических изданий (http://www.ivis.ru/products/udbs.htm). Режим доступа: свободный
– ГлавбухСтуденты: Образование и карьера (http://student.1gl.ru/). Режим доступа: свободный.

Нормативно-правовые акты

1. Гражданский кодекс Российской Федерации от 30 ноября 1994 года N 51-ФЗ
2. Профессиональный стандарт 06.015 - " Специалист по информационным системам", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 17 сентября 2014 г. N 645н.
3. Конституция РФ Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ
5. Федеральный закон от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике»
6. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 года № 1-ФЗ
7. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»
8. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
10. Федеральный закон от 9 февраля 2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»
11. Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности»
12. Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации»
13. Указ Президента РФ от 10 января 2000 г. № 24 «О Концепции национальной безопасности Российской Федерации»
14. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
15. Указ Президента Российской Федерации от 1 ноября 2008 года № 1576 «О Совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации»
16. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»

17. Постановление Правительства Российской Федерации от 28 февраля 1996 г. № 226 «О государственном учете и регистрации баз и банков данных» (с изм. от 2 марта 2005 г.)

18. Постановление Правительства Российской Федерации от 22 октября 2007 г. № 689 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

19. Постановление Правительства РФ от 6 ноября 2007 года № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»

20. Постановление Правительства Российской Федерации от 25 декабря 2007 г. № 931 «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям»

21. Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 947 «Об утверждении Правил разработки, апробации, доработки и реализации типовых программно-технических решений в сфере региональной информатизации»

22. Постановление Правительства Российской Федерации от 17 марта 2008 г. № 179 «Об утверждении Положения о пользовании сайтами в сети Интернет, на которых осуществляется проведение открытых аукционов в электронной форме, и требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами, а также к системам, обеспечивающим проведение открытых аукционов в электронной форме»

23. Постановление Правительства Российской Федерации от 28 марта 2008 г. № 215 «О Правительственной комиссии по федеральной связи и информационным технологиям»

24. Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям

25. Постановление Правительства Российской Федерации от 15 июня 2009 г. № 478 «О единой системе информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет»

26. Постановление Правительства РФ от 10 сентября 2009 г. N 723 «О порядке ввода в эксплуатацию отдельных государственных информационных систем»

27. Распоряжение Правительства Российской Федерации от 6 мая 2008 г. № 632-р (Концепция Формирования в Российской Федерации электронного правительства до 2010 года)

28. Распоряжение Правительства Российской Федерации от 25 августа 2008 г. № 1243-р Перечень технологий, имеющих важное социально-экономическое значение или важное значение для обороны страны и безопасности государства (критические технологии)

29. Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 3

30. Приказ Министерства информационных технологий и связи РФ от 11 марта 2008 г. № 32

31. Письмо Высшего Арбитражного суда Российской Федерации от 12 июля 2007 г. № ВАС-С01/УИС-984

32. Письмо Министерства финансов Российской Федерации от 12 сентября 2007 года № 03-07-08/255

33. «О взимании НДС с работ по разработке компьютерных программ» Письмо Министерства финансов Российской Федерации от 29 декабря 2007 г. № 03-07-11/648

34. Письмо Министерства экономического развития и торговли Российской Федерации от 7 марта 2008 г. № 2857-АП/Д05

35. Письмо Департамента налоговой и таможенно-тарифной политики Министерства

финансов Российской Федерации от 7 июля 2009 г. № 03-07-14/63

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Формируемые компетенции	Вид и форма контроля
УК-2 – способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**Промежуточный контроль:** контрольные вопросы к зачету **Текущий контроль:** практические задания, задания в тестовой форме, подготовка презентаций и докладов
ОПК-3 – способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**Промежуточный контроль:** контрольные вопросы к зачету **Текущий контроль:** практические задания, задания в тестовой форме, подготовка презентаций и докладов
ОПК-4 - способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**Промежуточный контроль:** контрольные вопросы к зачету **Текущий контроль:** практические задания, задания в тестовой форме, подготовка презентаций и докладов

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии оценивания устного ответа на зачете (промежуточный контроль формирования компетенций УК-2; ОПК-3; ОПК-4)

Показатель: совокупность проявленных знаний, умений, навыков. *Критерии* оценивания:

– знание основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– знание правовых основ организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– знание нормативных документов в обеспечения защиты информации ограниченного доступа;

– знание принципов и методов организационной защиты информации, организационного обеспечения информационной безопасности в организации;

– знание нормативных методических документов, регламентирующих порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе.

– умение осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей;

– умение применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– умение контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– умение оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

– владение навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки передачи информации;

– владение навыками соблюдения режима секретности;

– владение навыками противодействия утечке компьютерной информации;

– владение навыками использования электронной цифровой подписи;

– владение специальной терминологией, применяемой в процессе защиты информации;

– владение навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности.

Устный ответ обучающегося оценивается по пятибалльной шкале.

Зачтено - дан полный, развернутый ответ на поставленные вопросы, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки, показана способность быстро реагировать на уточняющие вопросы.

на *высоком* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *высоком* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *высоком уровне* способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«4» (хорошо) - дан полный, развернутый ответ на поставленные вопросы, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью «наводящих» вопросов.

на *базовом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *базовом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *базовом* способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«3» (удовлетворительно) - дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

на *пороговом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *пороговом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *пороговом* способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«2» (неудовлетворительно) - обучающийся демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминологией, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии.

не способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

не способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3;

не способен способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

Критерии оценивания выполнения заданий в тестовой форме (текущий контроль формирования компетенций УК-2; ОПК-3; ОПК-4)

Показатель: количество правильных ответов. *Критерии* оценивания:

– знание основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– знание правовых основ организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– знание нормативных документов в обеспечения защиты информации ограниченного доступа;

– знание принципов и методов организационной защиты информации, организационного обеспечения информационной безопасности в организации;

– знание нормативных методических документов, регламентирующих порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе.

– умение осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей;

– умение применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– умение контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– умение оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

– владение навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки передачи информации;

– владение навыками соблюдения режима секретности;

– владение навыками противодействия утечке компьютерной информации;

– владение навыками использования электронной цифровой подписи;

– владение специальной терминологией, применяемой в процессе защиты информации;

– владение навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности.

По итогам выполнения тестовых заданий оценка производится по пятибальной шкале. При правильных ответах на:

86-100% заданий – оценка *«отлично»;*

71-85% заданий – оценка *«хорошо»;*

51-70% заданий – оценка *«удовлетворительно»;*

менее 51% - оценка *«неудовлетворительно».*

Критерии оценивания практических заданий (текущий контроль формирования компетенций УК-2; ОПК-3; ОПК-4):

Показатели: выполнение всех практических заданий; уровень ответа на контрольные вопросы при защите заданий. *Критерии* оценивания:

– знание основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– знание правовых основ организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– знание нормативных документов в обеспечения защиты информации ограниченного доступа;

– знание принципов и методов организационной защиты информации, организационного обеспечения информационной безопасности в организации;

– знание нормативных методических документов, регламентирующих порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе.

– умение осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей;

– умение применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– умение контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– умение оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

– владение навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки передачи информации;

– владение навыками соблюдения режима секретности;

– владение навыками противодействия утечке компьютерной информации;

– владение навыками использования электронной цифровой подписи;

– владение специальной терминологией, применяемой в процессе защиты информации;

– владение навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности.

«5» (отлично)*:* выполнены все задания без ошибок, обучающийся четко и без ошибок ответил на все контрольные вопросы при защите работы. Обучающийся демонстрирует системные теоретические знания; уверенно показывает умение правильно идентифицировать, оценивать, классифицировать и систематизировать положения науки управления персоналом.

на *высоком* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *высоком* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *высоком* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

***«4» (хорошо)**:* выполнены все практические задания, обучающийся ответил на все контрольные вопросы с отдельными замечаниями. Обучающийся демонстрирует прочные теоретические знания, умеет правильно идентифицировать, оценивать, классифицировать и систематизировать положения науки управления персоналом.

на *базовом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *базовом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3;

на *базовом* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

***«3» (удовлетворительно)**:* выполнены все практические задания с замечаниями, обучающийся ответил на все контрольные вопросы с замечаниями. Обучающийся проявляет слабые теоретические знания; демонстрирует слабо сформированные умения: правильно идентифицировать, оценивать, классифицировать и систематизировать положения науки управления персоналом.

на *пороговом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *пороговом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *пороговом* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

***«2» (неудовлетворительно)**:* обучающийся не выполнил или выполнил неправильно задания, ответил на контрольные вопросы с ошибками или не ответил на контрольные вопросы. Обучающийся имеет слабые, фрагментарные, разрозненные знания категорий и понятий дисциплины; не умеет правильно идентифицировать, оценивать, классифицировать и систематизировать положения науки управления персоналом.

не способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

не способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

не способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

Показатели и критерии оценивания участия в работе малой группы (текущий контроль, формирование компетенций УК-2; ОПК-3; ОПК-4):

Показатель: совокупность проявленных знаний, умений, навыков. *Критерии оценивания*:

– знание основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– знание правовых основ организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– знание нормативных документов в обеспечения защиты информации ограниченного доступа;

– знание принципов и методов организационной защиты информации, организационного обеспечения информационной безопасности в организации;

– знание нормативных методических документов, регламентирующих порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе.

– умение осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей;

– умение применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– умение контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– умение оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

– владение навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки передачи информации;

– владение навыками соблюдения режима секретности;

– владение навыками противодействия утечке компьютерной информации;

– владение навыками использования электронной цифровой подписи;

– владение специальной терминологией, применяемой в процессе защиты информации;

– владение навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности.

«5» (отлично) - обучающийся демонстрирует системные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, на высоком уровне раскрывает содержание категорий и понятий дисциплины по теме семинара, приводит примеры; уверенно владеет навыками самостоятельной работы с нормативными документами; владеет навыками профессионального общения в коллективе; демонстрирует свободное владение монологической речью и способность быстро реагировать на уточняющие вопросы. Обучающийся:

на *высоком* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *высоком* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *высоком* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«4» (хорошо) обучающийся демонстрирует прочные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, раскрывает содержание категорий и понятий дисциплины по теме семинара и дискуссии, приводит примеры; владеет навыками самостоятельной работы с нормативными документами; владеет навыками

профессионального общения в коллективе; демонстрирует свободное владение монологической речью, но при этом делает несущественные ошибки, которые быстро исправляет самостоятельно или при незначительной коррекции преподавателем. Обучающийся:

на *базовом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *базовом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *базовом* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«3» (удовлетворительно) - обучающийся демонстрирует слабые знания содержания категорий и понятий дисциплины по теме семинара и дискуссии, затрудняется формулировать аргументированные выводы, делать обобщения; испытывает затруднения в процессе самостоятельной работы с нормативными документами; проявляет недостаточно свободное владение навыками профессионального общения в коллективе; показывает недостаточно свободное владение монологической речью, терминологией, логичностью и последовательностью изложения, делает ошибки, которые может исправить только при коррекции преподавателем. Обучающийся:

на *пороговом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *пороговом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *пороговом* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«2» (неудовлетворительно) - обучающийся демонстрирует слабые, фрагментарные, разрозненные знания содержания категорий и понятий дисциплины по теме семинара и дискуссии; не владеет терминологией, не умеет делать аргументированные выводы и приводить примеры, не владеет навыками самостоятельной работы с нормативными документами; не владеет навыками профессионального общения в коллективе; демонстрирует слабое владение монологической речью, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается участвовать в дискуссии. Обучающийся:

не способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

не способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

не способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

Критерии оценивания презентаций и докладов (текущий контроль формирования компетенций УК-2; ОПК-3; ОПК-4):

Показатель: совокупность проявленных знаний, умений, навыков. *Критерии оценивания*:

– знание основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– знание правовых основ организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

– знание нормативных документов в обеспечения защиты информации ограниченного доступа;

– знание принципов и методов организационной защиты информации, организационного обеспечения информационной безопасности в организации;

– знание нормативных методических документов, регламентирующих порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе.

– умение осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей;

– умение применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– умение контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

– умение оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации.

– владение навыками применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки передачи информации;

– владение навыками соблюдения режима секретности;

– владение навыками противодействия утечке компьютерной информации;

– владение навыками использования электронной цифровой подписи;

– владение специальной терминологией, применяемой в процессе защиты информации;

– владение навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности.

«5» (отлично)*:* работа выполнена в соответствии с требованиями, выбранная тема раскрыта полностью, материал актуален и достаточен, обучающийся четко и без ошибок ответил на все контрольные вопросы.

на *высоком* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *высоком* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *высоком* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«4» (хорошо)*:* работа выполнена в соответствии с требованиями, выбранная тема раскрыта, материал актуален, обучающийся ответил на все контрольные вопросы с замечаниями.

на *базовом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *базовом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *базовом* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

***«3» (удовлетворительно)**:* работа выполнена в соответствии с требованиями, выбранная тема частично раскрыта, по актуальности доклада есть замечания, обучающийся ответил на все контрольные вопросы с замечаниями.

на *пороговом* уровне способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

на *пороговом* уровне способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

на *пороговом* уровне способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

«2» (неудовлетворительно): обучающийся не подготовил работу или подготовил работу, не отвечающую требованиям, ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы.

не способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

не способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

не способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4)

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Контрольные вопросы к зачету (промежуточный контроль)

1. Понятие системы права.
2 Понятие и виды защищаемой информации по российскому законодательству.
3 Информация как объект гражданских прав.
4 Виды информации, подлежащие защите в процессе обычного гражданского оборота.
5 Четыре уровня правового обеспечения защиты информации.
6 Характеристика уровней правового обеспечения защиты информации.
7 Категории информации с ограниченным доступом.
8 Органы законодательства, регламентирующие деятельность по информационной безопасности.
9 Структура органов власти по защите информации в Российской Федерации.
10 Совет Безопасности Российской Федерации.
11 Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ).
12 Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ).
13 Комитет по вопросам информационной безопасности.
14 Анализ законодательства РФ в области информационной безопасности РФ.
15 Конституционные основы правового обеспечения информационной безопасности РФ.

16 Доктрина информационной безопасности РФ.

17 Перечень сведений, отнесенных законодателем к категории: государственная тайна по сферам жизнедеятельности общества и государства.

18 Правовой режим защиты государственной тайны.

19 Степени секретности сведений и грифы секретности носителей этих сведений.

20 Органы защиты государственной тайны.

21 Три формы допуска к секретным сведениям.

22 Организация допуска должностных лиц и граждан к государственной тайне.

23 Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.

24 Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности.

27 Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны.

28 Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющим государственную тайну.

29 Понятие коммерческой тайны.

30 Правовой режим защиты коммерческой тайны.

31 Требования для классификации сведений категории коммерческой тайны.

32 Понятие банковской тайны.

33 Объекты банковской тайны.

34 Правовой режим защиты банковской тайны.

35 Понятие профессиональной тайны.

36 Требования для классификации сведений категории профессиональной тайны. Объекты профессиональной тайны.

37 Правовой режим защиты конфиденциальной информации.

38 Понятие служебной тайны. Требования для классификации сведений категории служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне.

39 Понятие персональных данных. Регуляторы в области защиты персональных данных.

40 Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

41 Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

42 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

43 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

44 Основные объекты интеллектуальной собственности.

45 Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности.

46 Уголовная ответственность за правонарушения в области защиты интеллектуальной собственности в области конфиденциальной информации. Уголовная ответственность за правонарушения в области конфиденциальной информации.

47 Информационные ресурсы как объект защиты.

48 Классификация информационных ресурсов.

49 Государственные и негосударственные информационные ресурсы.

50 Пользование информационными ресурсами.

51 Системы защиты информационных ресурсов.

Задания в тестовой форме (текущий контроль) (фрагмент)

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы

- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

29) К служебной тайне не относится …
- профессиональная тайна
- тайна деятельности соответствующего органа
(+) вред, причиненный здоровью работника в связи с производственной травмой

30) Вредоносные программы, выраженные в объективной форме и имеющие творческий характер, … охраноспособными.
(+) являются
- не являются

31) В правовой режим документированной информации входит …
- государственная тайна
- тайна частной жизни
- банковская тайна
(+) электронная цифровая подпись
- персональные данные

32) Исключите неправильный постулат:
- информация не связана с определенным конкретным носителем
- информация не существует без материального носителя
(+) содержание информации меняется одновременно со сменой материального носителя

33) К государственной тайне не относятся сведения, защищаемые государством …, распространение которых может нанести ущерб государству.
- в экономической области
- в контрразведывательной деятельности
- в оперативно-разыскной деятельности
(+) о частной жизни политических деятелей

34) Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений…
(+) которые составляют финансово-экономическую информацию и позволяют избежать
(+) неоправданных расходов
- безопасности пищевых продуктов
- о показателях производственного травматизма, профессиональной заболеваемости
- о системе оплаты и условиях труда

35) Ответственность за создание вредоносной программы наступает в…
- любом случае
(+) совокупности с ответственностью за ее использование
- случаях, установленных законодательством

36) Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных…
- осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник
- необходима в связи с осуществлением правосудия
- необходима в соответствии с оперативно-розыскной деятельностью
(+) необходима в связи с выездом за пределы Российской Федерации

37) Субъектами
- муниципальные образования
- Российская Федерация
- трудовой коллектив
(+) трансграничные информационно-телекоммуникационные сети

38) Признак, не относящийся к охраноспособной информации – это …:
- охране подлежит только документированная информация
- доступ к охраноспособной информации ограничен только законом
(+) доступ к охраноспособной информации ограничен владельцем информационных ресурсов
- защита охраноспособной информации устанавливается Законом

39) Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений…

- о размере и составе имущества некоммерческих организаций
- об оплате труда работников некоммерческих организаций
- об использовании безвозмездного труда граждан в деятельности некоммерческой организации

(+) об использовании новых технологий, позволяющих получить коммерческую выгоду

Практические задания (текущий контроль) (фрагмент)

Задание 1

Назовите юридические свойства информации. Проиллюстрируйте примерами такие из них, как: распространяемость (тиражируемость); экземплярность.

Задание 2

Дайте определение и выделите признаки документированной информации. В каких нормативных актах Российской Федерации дано понятие документированной информации?

Задание 3

Приведите примеры (не менее 10) информации, предоставление которой является обязанностью органов государственной власти. Ответ проиллюстрируйте ссылками на конкретные правовые нормы.

Задание 4

В информационном праве используется вся совокупность способов регулирующего воздействия на информационные правоотношения. Со ссылками на конкретные информационно-правовые нормы приведите примеры диспозитивного регулирования (свобода выбора, равенство сторон, децентрализация, координация) и императивного регулирования (централизация, строгая субординация).

Задание 5

Как соотносятся нормы конституционного и информационного права в информационной сфере?

Задание 6

Основываясь на нормах информационного права, смоделируйте информационные правоотношения: возникающие:

- по поводу доступа к информации;
- по поводу создания информации;
- по поводу обеспечения информационной безопасности;
- по поводу оказания информационных услуг.

Назовите все элементы структуры смоделированного информационно-правового отношения (субъектов, объект, содержание, юридический факт, способ правовой защиты).

Задание 7

Журналисты газеты «Звезда» решили посетить судебное заседание районного суда, по делу гражданина Порохова, обвиняемого в хищение предметов, имеющих особую историческую и художественную ценность. Судебный пристав-исполнитель ничем не мотивируя свои действия, не пустил журналистов в здание суда. *Какие принципы правового регулирования в сфере информации в данном случае были нарушены?*

Задание 8

Гражданин РФ Петров, поступая на муниципальную службу в администрацию муниципального образования, подготовил требуемые законом документы. Однако документы у него не приняли, указывая на их недостаточность. К собранным документам глава администрации потребовал приложить справки (информацию), из находящихся в муниципальном образовании психиатрической больницы, венерического диспансера, туберкулезного диспансера, а также потребовал предоставить аналогичные справки (информацию) на членов своей семьи.

Имеет ли право глава администрации муниципального образования требовать данного рода информацию? Какие принципы правового регулирования информационных правоотношений на ваш взгляд нарушены? Какая информация в соответствии с законом должна быть предоставлена гражданином при поступлении на: муниципальную службу, государственную гражданскую службу?

Задание 9

На основе действующего законодательства проведите соотношение между такими субъектами информационных отношений как «оператор информационной системы» и «обладатель информации». Может ли оператор информационной системы одновременно быть обладателем информации и наоборот? Заполните следующую таблицу.

	Права	***Обязанности***	***Ответственность***
Обладатель информации			
Оператор информационной системы			

Задание 10

Со ссылками на действующие нормативные акты заполните следующую таблицу.

Наименование органа государственного управления	***Полномочия в области обеспечения доступа к информации***		***Полномочия в области обеспечения охраны государственной тайны***	
	права	***обязанности***	***права***	***обязанности***

Задание 11

Какие полномочия в области обеспечения защиты государственной тайны, а также в области обеспечения режима конфиденциальной информации имеют органы законодательной и судебной власти? Свой ответ обоснуйте ссылками на нормы действующего законодательства.

Задание 12

Решением Городской Думы г. Пензы было установлено, что информация о деятельности муниципальных служащих данного муниципального образования имеет статус служеб-

ных сведений (служебной тайны) и является конфиденциальной информацией порядок доступа, к которой определяется непосредственно руководителями органов местного самоуправления, в которых осуществляют свою деятельность муниципальные служащие.

Оцените законность решения представительного органа местного самоуправления г. Пензы с точки зрения действующего законодательства. Какими полномочиями наделены органы местного самоуправления в области обеспечения режима конфиденциальной информации?

Задание 13

На примере свердловской области постройте систему органов государственной власти субъекта РФ имеющих полномочия в области обеспечения права граждан на доступ к информации. И укажите со ссылками на нормативно-правовые акты субъектов РФ данные полномочия.

Задание 14

Проанализировав Постановление Правительства РФ от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» разделите указанный в нем перечень информации на 4 однородных группы, самостоятельно определяя критерии деления.

Задание 15

Назовите признаки, присущие информации, находящейся в режиме тайны и раскройте их содержание.

Задание 16

Перечислите категории сведений, доступ к которым не подлежит какому-либо ограничению.

Задание 17

В каких случаях не требуется согласие субъекта персональных данных на их обработку.

Задание 18

Могут ли получить допуск к сведениям, составляющим государственную тайну несовершеннолетние? В каких случаях студенты высших и средних специальных учебных заведений могут быть допущены к сведениям, составляющим государственную тайну?

Задание 19

Могут ли быть допущены к сведениям, составляющим государственную тайну лица, имеющие двойное гражданство, лица без гражданства, иностранные граждане? *Свой ответ обоснуйте ссылками на нормы действующего законодательства.*

Задание 20

Руководитель фирмы «Градиент» составил для персонала фирмы инструкцию по работе с документами, составляющими коммерческую тайну.

Инструкция содержала следующие положения:

- работники фирмы должны были давать соответствующую подписку о неразглашении коммерческой тайны либо это обязательство должно было включаться в качестве отдельного пункта в трудовое соглашение того или иного сотрудника.
- если в сведения, составляющие коммерческую тайну, приходилось посвящать деловых партнеров или клиентов фирмы, то положения о неразглашении тайны обязательно должны были включаться в соответствующие договоры с участниками правоотношений.

- в целях предотвращения утечки коммерческой информации сотрудникам фирмы запрещалось передавать любую информацию правоохранительным органам; информацию мог передавать лишь руководитель фирмы.

- фото- и киносъемка служебных и иных помещений фирмы могут осуществляться только с письменного разрешения директора фирмы.

Дайте правовую оценку каждого положения этой инструкции с точки зрения норм информационного права.

Задание 21

На основании действующего законодательства выстройте систему федеральных органов исполнительной власти обладающих полномочиями в области обеспечения информационной безопасности личности, общества, государства.

Задание 22

Со ссылками на федеральное законодательство впишите в нижеприведенную таблицу по три примера полномочий указанных органов в области обеспечения информационной безопасности личности, общества, государства.

	Личность	***Общество***	***Государство***
Правительство РФ			
МИД РФ			
ФСБ РФ			
МВД РФ			
Минобороны РФ			

Задание 23

Двое бывших сотрудников компании «ПРЕМИУМ», воспользовавшись паролем администратора, удалили с сервера компании файлы, составлявшие крупный (на несколько миллионов долларов) проект иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери были незначительны.

Разберите приведенную ситуацию и определите:

- что является источником угрозы информационной безопасности;

- какой в данном случае вид угрозы информационной безопасности (например, внутренняя или внешняя);

- чьи интересы в информационной сфере в данной ситуации страдают?

Подлежат ли действия бывших сотрудников компании «ПРЕМИУМ» ответственности в соответствии с действующим законодательством Российской Федерации?

Задание 24

Определите значение лицензированию и сертификации в области обеспечения информационной безопасности.

Какие виды деятельности в Российской Федерации подлежат лицензированию в целях обеспечения информационной безопасности личности, общества, государства?
Сертификация каких товаров обязательна в Российской Федерации в целях обеспечения информационной безопасности личности, общества, государства?

Задание 25

В соответствии с Доктриной информационной безопасности Российской Федерации дайте характеристику методам обеспечения информационной безопасности в Российской Федерации.

Подготовка презентаций и докладов (текущий контроль)

Темы презентаций и докладов

1 Аттестация объектов информатизации по требованиям безопасности информации.

2 Понятие интеллектуальной собственности, ее виды и объекты образования (авторские и лицензионные договоры).

3 Основы авторского права. Основные положения патентного права.

4 Законодательство об интеллектуальной собственности.

5 Особенности правового регулирования общественных отношений при использовании современных технических средств обработки информации и при разработке шифрсредств.

6 Правовое регулирование использования электронной цифровой подписи и защиты информации в системах и средствах электронного документооборота.

7 Статус и организация деятельности удостоверяющих центров.

8 Правовое регулирование защиты информации в системах связи.

9 Использование персональных данных владельцев доменных имен сети Интернет и проблемы защиты конституционных прав граждан на неприкосновенность персональных данных.

10 Основные понятия и система сертификации продукции и услуг в сфере информационной безопасности.

11 Особенности сертификации средств защиты информации по требованиям безопасности.

12 Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации

13 Отрасли права, обеспечивающие законность в области защиты информации.

14 Конституция и Гражданский кодекс Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности.

15 Международное законодательство в области защиты информации.

16 Основные понятия, положения, организационная структура системы государственного лицензирования.

17 Аттестация объектов информатизации по требованиям безопасности информации.

18 Причины и условия, обусловливающие правонарушения в сфере информационной безопасности (защиты конфиденциальной информации, обеспечение режима секретности)

19 Характеристика личности правонарушителя в сфере информационной безопасности.

20 Понятие и виды юридической ответственности за нарушение правовых норм в области защиты информации.

21 Уголовная ответственность за нарушение правовых норм в сфере информационной безопасности.

22 Административная ответственность за нарушение правовых норм в сфере информационной безопасности.

23 Проведение административного расследования по фактам нарушения установленного порядка обеспечения информационной безопасности.

24 Особенности юридической ответственности за нарушение правовых норм информационной безопасности в области трудовых и гражданско-правовых отношений.

25 Меры предупреждение правонарушений

26 Актуальность проблемы правового регулирования в сфере информационной безопасности.

27 Факторы и проблемы правового регулирования в сфере информационной безопасности.

28 Состояние и закономерности практики правового регулирования информационной безопасности.

29 Направления развития теоретических аспектов законодательства в сфере информационной безопасности

30 Методология и организация исследований в области правового регулирования информационной безопасности.

31 Факторы и проблемы правового регулирования в сфере информационной безопасности.

32 Состояние и закономерности практики правового регулирования информационной безопасности.

33 Направления развития теоретических аспектов законодательства в сфере информационной безопасности.

34 Развитие информационного права как эффективного инструментария регулирования конституционных прав человека в информационной сфере.

.

7.4. Соответствие балльной шкалы оценок и уровней сформированных компетенций

Уровень сформированных компетенций	Оценка	Пояснения
Высокий	Зачтено	Теоретическое содержание дисциплины освоено полностью, все поставленные в ней цели и задачи достигнуты, все предусмотренные программой обучения учебные задания выполнены без замечаний. Компетенции сформированы. Обучающийся на *высоком* уровне способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

Уровень сформированных компетенций	Оценка	Пояснения
Базовый	Зачтено	Теоретическое содержание дисциплины освоено полностью, все поставленные в ней цели и задачи достигнуты, все предусмотренные программой обучения учебные задания выполнены с отдельными незначительными замечаниями. Компетенции сформированы. Обучающийся на *базовом* уровне способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью
Пороговый	Зачтено	Теоретическое содержание дисциплины освоено частично, предусмотренные программой обучения учебные задания выполнены с замечаниями. Компетенции сформированы. Обучающийся на *пороговом* уровне способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью
Низкий	Не зачтено	Теоретическое содержание дисциплины не освоено, компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий. Обучающийся *не способен*: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

8. Методические указания для обучающихся по освоению дисциплины

Вид учебных занятий	Организация деятельности обучающегося
Занятия лекционного типа	В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на выполнение самостоятельной работы. В ходе лекций обучающимся рекомендуется: - вести конспектирование учебного материала; - обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению; - задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. В рабочих конспектах желательно оставлять поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также пометки, подчеркивающие особую важность тех или иных теоретических положений. Для успешного овладения курсом необходимо посещать все лекции, так как тематический материал взаимосвязан между собой. В случаях пропуска занятия обучающемуся необходимо самостоятельно изучить материал и ответить на контрольные вопросы по пропущенной теме во время индивидуальных консультаций.
Занятия семинарского типа (лабораторные занятия)	Семинарские (лабораторные занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения лабораторных занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор кейсов по теме занятия; работа с правовыми информационно-справочными системами. В обязанности преподавателя входят: оказание методической помощи и консультирование обучающихся по соответствующим темам курса. Лабораторные занятия – это активная форма учебного процесса. При подготовке к занятиям обучающемуся необходимо изучить основную литературу, ознакомиться с дополнительной литературой, нормативными документами, учесть рекомендации преподавателя. Большая часть тем дисциплины предполагает выполнение заданий и анализ правовых ситуаций.
Самостоятельная работа (изучение теоретического курса, подготовка к лабораторным занятиям)	Самостоятельная работа – это процесс активного, целенаправленного приобретения обучающимися новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности. Самостоятельная работа, связанная с текущей проработкой курса, включает чтение и обобщение лекционного материала, а также учебной и научной литературы. Основная функция учебников – ориентировать обучающегося в системе знаний, умений и навыков, которые должны быть усвоены по данной дисциплине. После проработки теоретического материала по изучаемой теме обучающийся должен ответить на вопросы для самоконтроля. При подготовке к семинару целесообразно оформить тезисный конспект выступления, представляющий собой изложение в письменном

Вид учебных занятий	Организация деятельности обучающегося
	виде результатов теоретического анализа и практической работы обучающегося по заданной теме. Материал по теме дискуссии следует излагать, выделяя ключевые положения. При этом требуется приводить соответствующую аргументацию, увязывать предыдущий материал с последующим. Раскрывая тему, необходимо сравнивать, если возможно, различные точки зрения. Если по какому-либо теоретическому вопросу нет единства взглядов, то следует привести высказывания нескольких авторов, попытаться дать критическую оценку их позиций, а также аргументировано изложить собственное видение по данному вопросу. Подготовка к лабораторным занятиям предполагает изучение лекционного материала и литературных источников по заданной тематике. Закреплению умений и навыков, формированию профессиональных компетенций по дисциплине способствует выполнение домашних заданий по указанию преподавателя, а также практических заданий для самостоятельной работы, аналогичных предлагаемым на занятиях. Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит инструктаж по выполнению задания, который включает информирование о цели и содержании задания, сроках его выполнения, ориентировочном объеме работы, основных требованиях к результатам работы и критериях оценки, возможных типичных ошибках при выполнении. Инструктаж проводится за счет объема времени, отведенного на изучение дисциплины. Контроль результатов внеаудиторной самостоятельной работы обучающихся может проходить в письменной, устной или смешанной форме.
Подготовка к зачету	Подготовка к зачету предполагает: - изучение рекомендуемой литературы; - изучение и анализ нормативных документов; - изучение конспектов лекций; - участие в проводимых контрольных опросах; - тестирование по темам; - выполнение заданий; -выполнение заданий по анализу практических ситуаций. Зачет выставляется в соответствии с критериями, представленными в пункте 7.2.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Для успешного овладения дисциплиной используются следующие информационные технологии обучения:

• при проведении лекций используются презентации материала в программе Microsoft Office (PowerPoint), выход на профессиональные сайты, использование видеоматериалов различных интернет-ресурсов;

• практические занятия по дисциплине проводятся с использованием платформы MOODLE, справочной правовой системы «Консультант Плюс».

Для дистанционной поддержки дисциплины используется система управления образовательным контентом Moodle. Для работы в данной системе все обучающиеся на первом курсе получают индивидуальные логин и пароль для входа в систему, в которой размещаются: программа дисциплины, материалы для лекционных и иных видов занятий, задания, контрольные вопросы.

Для достижения цели задач дисциплины используются в основном традиционные информативно-развивающие технологии обучения с учетом различного сочетания пассивных форм (лекция, практическое занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно-иллюстративное изложение) и практических методов обучения (выполнение расчетных работ).

Университет обеспечен необходимым комплектом лицензионного программного обеспечения:

– операционная система Windows 7, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно;

- операционная система Astra Linux Special Edition. Договор №Pr000013979/0385/22-ЕП-223-06 от 01.07.2022. Срок: бессрочно;

– пакет прикладных программ Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно;

– пакет прикладных программ Р7-Офис.Профессиональный. Договор №Pr000013979/0385/22-ЕП-223-06 от 01.07.2022. Срок: бессрочно;

– антивирусная программа Kaspersky Endpoint Security для бизнеса - Расширенный Договор 0436/ЗК;

– операционная система Windows Server. Контракт на услуги по предоставлению лицензий на право использовать компьютерное обеспечение № 067/ЭА от 07.12.2020 года. Срок бессрочно;

– система видеоконференцсвязи Пруффми. Договор № 2576620-2 / 0120/24-ЕП-223-03 от 16 марта 2024 г.;

– система управления обучением LMS Moodle – программное обеспечение с открытым кодом, распространяется по лицензии GNU Public License (rus);

– браузер Yandex (https://yandex.ru/promo/browser/) – программное обеспечение распространяется по простой (неисключительной) лицензии; Яндекс 360 Тариф «Оптимальный для образования»

Цифровые инструменты и сервисы

Применение цифровых технологий в рамках преподавания дисциплины предоставляет расширенные возможности по организации учебных занятий в условиях цифровизации образования и позволяет сформировать у обучающихся навыки применения цифровых сервисов и инструментов в повседневной жизни и профессиональной деятельности,.

Для реализации этой цели в рамках изучения дисциплины могут применяться следующие цифровые инструменты и сервисы.

Инструменты для коммуникации

Сервис WEEEK (https://weeek.net/ru) – сервис для коммуникации, распространяется по лицензии trialware

Сферум (https://sferum.ru/?p=start) – мессенджер, распространяется по лицензии FreeWare

VK Мессенджер (https://vk.me/app?mt_click_id=mt-v7eix5-1660908314-1651141140) – мессенджер, распространяется по лицензии FreeWare

Инструменты для организации удаленной связи и видеоконференций

Pruffme – система для организации коллективной работы и онлайн-встреч, распространяется по проприетарной лицензии;

Mirapolis – система для организации коллективной работы и онлайн-встреч, распространяется по проприетарной лицензии;

Webinar (https://webinar.ru/) – платформа для вебинаров, обучения, распространяется по лицензии trialware;

Видеозвонки Mail.ru (https://calls.mail.ru/) – сервис для видеозвонков, распространяется по лицензии ShareWare

Яндекс.Телемост (https://telemost.yandex.ru/) – сервис для видеозвонков, распространяется по лицензии ShareWare

COMDI (https://www.comdi.com/) – сервис для онлайн-мероприятий, распространяется по лицензии trialware

Планирование времени и встреч

Яндекс.Календарь (https://calendar.yandex.ru/) – онлайн календарь-планер, распространяется по лицензии ShareWare

Shtab (https://shtab.app/) – планировщик задач, распространяется по лицензии FreeWare

Сервис WEEEK (https://weeek.net/ru), распространяется по лицензии trialware

Инструменты для управления удаленной работой, командой

Сервис WEEEK (https://weeek.net/ru) – сервис для управления командой, распространяется по лицензии trialware;

Pruffme – система для организации коллективной работы и онлайн-встреч, распространяется по проприетарной лицензии;

Mirapolis – система для организации коллективной работы и онлайн-встреч, распространяется по проприетарной лицензии;

VK WorkSpace (https://biz.mail.ru/) – платформа для совместной удаленной работы (почта, сервис для коммуникаций, хранилище), распространяется по лицензии trialware;

Сервис Padlet (https://ru.padlet.com/my/dashboard) – распространяется по лицензии trialware

Инструменты для обмена информацией (совместное использование файлов)

Яндекс.Документы (https://docs.yandex.ru/) – инструмент для создания и совместного использования документов, распространяется по лицензии trialware;

Yandex Forms (https://cloud.yandex.ru/services/forms) – бесплатный сервис для создания форм для опроса, регистрации и т.д., распространяется по лицензии trialware;

@Облако (https://cloud.mail.ru/) – сервис для создания, хранения и совместного использования файлов, распространяется по лицензии trialware;

Яндекс.Диск – сервис для хранения и совместного использования документов, распространяется по лицензии trialware

Конструкторы онлайн-курсов

CoreApp (https://coreapp.ai/) — это онлайн-платформа конструирования образовательных материалов и проверки знаний с обратной связью и электронным журналом, распространяется по академической лицензии

Eduardo (https://eduardo.studio/) – платформа для создания и запуска онлайн-курсов, распространяется по лицензии trialware;

iSpring (https://www.ispring.ru/) – платформа для онлайн-обучения, распространяется по лицензии trialware;

We.Study (https://webinar.ru/products/westudy/) – платформа для создания онлайн-курсов и организации обучения, распространяется по лицензии trialware;

УДОБА (https://udoba.org/) – конструктор и хостинг открытых образовательных ресурсов

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Реализация учебного процесса осуществляется в учебных аудиториях университета для Реализация учебного процесса осуществляется в специальных учебных аудиториях университета для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Все аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. При необходимости обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.

Самостоятельная работа обучающихся выполняется в специализированной аудитории, которая оборудована учебной мебелью, компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УГЛТУ.

Есть помещение для хранения и профилактического обслуживания учебного оборудования.

Оснащенность аудиторий и помещений

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Помещение для лекционных и практических занятий, групповых и индивидуальных консультаций, текущей и промежуточной аттестации.	Переносная мультимедийная установка (проектор, экран). Учебная мебель
Помещения для самостоятельной работы	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет.
Помещение для хранения и профилактического обслуживания учебного оборудования	Стеллажи. Раздаточный материал.