Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)
Факультет среднего профессионального образования –
Хабаровский техникум железнодорожного транспорта

УТВЕРЖДАЮ
И.о.декана ФСПО - ХТЖТ
_____Д.Н. Никитин
« 21 » мая 2021 г

РАБОЧАЯ ПРОГРАММА

дисциплины ***ОП.01 Основы информационной безопасности***

Для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Профиль:

Составитель(и): Преподаватель Касьяненко А.Ю.

Обсуждена на заседании ПЦК ***Информационная безопасность автоматизированных систем***

Протокол от « 20 » мая 2021 г. № 9

Методист _____Л.В. Петрова

г. Хабаровск
2021 г.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

в рабочую программу ОП.01 Основы информационной безопасности

наименование структурного элемента ОПОП

10.02.05 Обеспечение информационной безопасности автоматизированных систем

с указанием кода направления подготовки и профиля

На основании

решения заседания кафедры (ПЦК) **Информационная безопасность автоматизированных систем**

полное наименование кафедры (ПЦК)

"26 " мая 2022 г., протокол № 9

на 2022 / 2023 учебный год внесены изменения:

№ / наименование раздела	Новая редакция
	Изменений нет

Заведующий кафедрой (председатель ПЦК)

_____А.Ю. Касьяненко

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

в рабочую программу ОП.01 Основы информационной безопасности

наименование структурного элемента ОПОП

10.02.05 Обеспечение информационной безопасности автоматизированных систем

с указанием кода направления подготовки и профиля

На основании

решения заседания кафедры (ПЦК) **Информационная безопасность автоматизированных систем**

полное наименование кафедры (ПЦК)

"26 " мая 2023 г., протокол № 9

на 2023 / 2024 учебный год внесены изменения:

№ / наименование раздела	Новая редакция
	Изменений нет

Заведующий кафедрой (председатель ПЦК)

_____А.Ю. Касьяненко

Рабочая программа дисциплины ОП.01 Основы информационной безопасности

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 09.12.2016 г. № 1553

Квалификация **Техник по защите информации**

Форма обучения **Очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МДК, ПМ) В ЧАСАХ С УКАЗАНИЕМ ОБЯЗАТЕЛЬНОЙ И МАКСИМАЛЬНОЙ НАГРУЗКИ ОБУЧАЮЩИХСЯ

Общая трудоемкость **115 ЧАС**

Часов по учебному плану 115

Виды контроля в семестрах:

Другие формы промежуточной аттестации 1

Зачет (семестр) 2

Распределение часов дисциплины (МДК, ПМ) по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		**2 (1.2)**		Итого	
Недель	13(4)		19(4)			
Вид занятий	УП	РПД	УП	РПД	УП	РПД
Лекции, уроки	31	31	48	48	79	79
Практические занятия						
Лабораторные занятия	8	8	28	28	36	36
Семинарские занятия.						
Курсовая работа						
Промежуточная аттестация						
Индивидуальный проект						
Самостоятельная работа						
Консультации						
Итого	39	39	76	76	115	115

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МДК, ПМ)	
1.1	Основные понятия и задачи информационной безопасности. Обзор защищаемых объектов и систем. Основы защиты информации. Понятия государственной тайны и конфиденциальной информации. Угрозы безопасности защищаемой информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации. Методологические подходы к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации. Нормативно правовое регулирование защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Защита информации в автоматизированных (информационных) системах. Инженерная защита и техническая охрана объектов информатизации. Работа с кадрами и внутриобъектовый режим.

2. МЕСТО ДИСЦИПЛИНЫ (МДК, ПМ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	ОП.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Дисциплина изучается в 1,2 семестре 1 курса
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (МДК, ПМ) необходимо как предшествующее:**
2.2.1	МДК.02.01 Программные и программно-аппаратные средства защиты информации
2.2.2	МДК.02.02 Криптографические средства защиты информации
2.2.3	МДК.03.01 Техническая защита информации
2.2.4	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МДК, ПМ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОК 03: Планировать и реализовывать собственное профессиональное и личностное развитие
Знать: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития
ОК 06: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
Знать: сущность гражданско-патриотической позиции. Общечеловеческие ценности. Правила поведения в ходе выполнения профессиональной деятельности
Уметь: описывать значимость своей профессии. Презентовать структуру профессиональной деятельности по специальности
ОК 09: Использовать информационные технологии в профессиональной деятельности
Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
ОК 10: Пользоваться профессиональной документацией на государственном и иностранном языках
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
ОК 11: Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
Знать: методы планирования предпринимательской деятельности в профессиональной сфере.
Уметь: использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере.
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
Иметь практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

В результате освоения дисциплины (МДК, ПМ)обучающийся должен

3.1	**Знать:**
3.1.1	содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; сущность гражданско-патриотической позиции. Общечеловеческие ценности. Правила поведения в ходе выполнения профессиональной деятельности; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности; правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; методы планирования предпринимательской деятельности в профессиональной сфере; особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
3.2	**Уметь:**
3.2.1	определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития; описывать значимость своей профессии. Презентовать структуру профессиональной деятельности по специальности; **п**рименять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; использовать полученные знания и опыт в организации предпринимательской деятельности в профессиональной сфере; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
3.3	**Иметь практический опыт:**
3.3.1	решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МДК, ПМ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература		Примечание	
	Раздел 1. Лекционные занятия							
1.1	Основные понятия и задачи информационной безопасности.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.2	Основные понятия и задачи информационной безопасности.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.3	Основные понятия и задачи информационной безопасности.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.4	Основные понятия и задачи информационной безопасности.	1/1	1	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			

1.5	Обзор защищаемых объектов и систем	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.6	Обзор защищаемых объектов и систем	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.7	Обзор защищаемых объектов и систем	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.8	Обзор защищаемых объектов и систем	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.9	Основы защиты информации.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.10	Основы защиты информации.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.11	Основы защиты информации.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.12	Основы защиты информации.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.13	Понятие государственной тайны и конфиденциальной информации	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.14	Понятие государственной тайны и конфиденциальной информации	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.15	Понятие государственной тайны и конфиденциальной информации	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.16	Понятие государственной тайны и конфиденциальной информации	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.17	Угрозы безопасности защищаемой информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.18	Каналы и методы несанкцио-нированного доступа к информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.19	Уязвимости. Методы оценки уязвимости информации	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.20	Уязвимости. Методы оценки уязвимости информации	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			

1.21	Методологические подходы к защите информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.22	Методологические подходы к защите информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.23	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.24	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.25	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.26	Виды мер и основные принципы защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.27	Виды мер и основные принципы защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.28	Виды мер и основные принципы защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.29	Нормативно правовое регулирование защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.30	Нормативно правовое регулирование защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.31	Законодательные акты в области защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.32	Законодательные акты в области защиты информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.33	Российские и международные стандарты, определяющие требования к защите информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.34	Российские и международные стандарты, определяющие требования к защите информации.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.35	Защита информации в автоматизированных (информационных) системах.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			

1.36	Защита информации в автоматизированных (информационных) системах.	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.37	Инженерная защита и техническая охрана объектов информатизации	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.38	Инженерная защита и техническая охрана объектов информатизации	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.39	Работа с кадрами и внутриобъектовый режим	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
1.40	Работа с кадрами и внутриобъектовый режим	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
	Раздел 2. Лабораторные занятия							
2.1	Определение объектов защиты на типовом объекте информатизации.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.2	Определение объектов защиты на типовом объекте информатизации.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.3	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.4	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	1/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.5	Определение угроз объекта информатизации и их классификация	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.6	Определение угроз объекта информатизации и их классификация	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.7	Определение угроз объекта информатизации и их классификация	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.8	Определение угроз объекта информатизации и их классификация	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.9	Определение угроз объекта информатизации и их классификация	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			

2.10	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.11	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.12	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.13	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.14	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.15	Выбор мер защиты информации для автоматизированного рабочего места	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.16	Выбор мер защиты информации для автоматизированного рабочего места	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.17	Выбор мер защиты информации для автоматизированного рабочего места	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
2.18	Выбор мер защиты информации для автоматизированного рабочего места	2/1	2	ОК 03; ОК 06; ОК 09; ОК10; ОК 11; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
	Раздел 3. Контроль							
3.1	Другие формы промежуточной аттестации	1/1		ОК 03;ОК 06; ОК 09;ОК 10; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			
3.2	Зачет	2/1		ОК 03;ОК 06; ОК 09;ОК 10; ПК.2.4	Л1.1, Л1.2, Л2.1, Л3.1, Л3.2, Э1, Э2, Э3			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещен в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МДК, ПМ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Громов Ю.Ю.	Информационная безопасность и защита информации.	Старый Оскол: ТНТ, 2016
Л1.2	Прохорова О. В.	Информационная безопасность и защита информации.	Самара: Самарский государственный архитектурно-строительный университет, 2014

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Башлы П. Н., Баранова Е. К., Бабаш А. В.	Информационная безопасность	Москва: Евразийский открытый институт, 2011

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (МДК, ПМ)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Долгов В.А., Анисимов В.В.	Криптографические методы защиты информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008
Л3.2	Крат Ю.Г., Шрамкова И.Г.	Основы информационной безопасности: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (МДК, ПМ)

Э1	Научная электронная библиотека eLIBRARY.RU	Режим доступа: https://elibrary.ru/defaultx.asp?
Э2	Электронно-библиотечная система «Книгафонд	Режим доступа: http://knigafund.ru/
Э3	Электронный каталог НТБ	Режим доступа: http://catalog.lib.tpu.ru/ec/simple

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (МДК, ПМ), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

	- Win XP, 7
	- DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220
	- Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94
	- Права на ПО NetPolice School для Traffic Inspector Unlimited
	- Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special
	-Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)
	Windows 7 Pro, лиц. 60618367,
	Office Pro Plus 2007, лиц. 45525415 (ГК 111 от 22.04.2009).

6.3.2 Перечень информационных справочных систем

	Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
234	Учебная аудитория для проведения теоретических занятий (уроков), практических и лабораторных, групповых и индивидуальных занятий, консультаций, текущего контроля и промежуточной аттестации.	Рабочие места на базе вычислительной техники, подключенными к локальной вычислительной сети и сети «Интернет». - Win XP, 7 - DreamSpark Premium Electronic Software Delivery (3 years) Renewal 1203984220 - Kaspersky Endpoint Security 10 для Windows - 356¬160615-113525¬730¬94 - Права на ПО NetPolice School для Traffic Inspector Unlimited - Права на ПО Traffic Inspector Anti-Virus powered by Kaspersky Special -Traffic Inspector (Контракт 524 ДВГУПС от 15.07.2019)
303	Учебная аудитория для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория технических средств защиты информации Лаборатория "Системы передачи и защиты дискретной информации. ДВ сетевая академия CISCO".	Комплект учебной мебели. Технические средства обучения: ПК, блок питания - 48/80, Патп-панель, коммутатор cisco cafalyst 3560, коммутатор cisco cafalyst 35666, коммутатор cisco cafalyst 2960, маршрутизатор cisco 2800, маршрутизатор cisco 2801, коммутатор ZyxeL Ies-1000, межсетевой экран cisco, AKB. Windows 7 Pro, лиц. 60618367, Office Pro Plus 2007, лиц. 45525415 (ГК 111 от 22.04.2009).

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МДК, ПМ)

Лекционное занятие (урок)

Работа на лекции является очень важным видом деятельности обучающихся для изучения дисциплины, т.к. лектор дает нормативно-правовые акты, которые в современной России подвержены частому, а иногда кардинальному изменению, что обуславливает «быстрое устаревание» учебного материала, изложенного в основной и дополнительной учебной литературе. Лектор ориентирует обучающихся в действующем законодательстве Российской Федерации и соответственно в учебном материале. Краткие записи лекций (конспектирование) помогает усвоить материал. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями: «важно», «особо важно», «хорошо запомнить» и т.п. или подчеркивать красной ручкой. Целесообразно разработать собственную символику, сокращения слов, что позволит сконцентрировать внимание обучающихся на важных сведения. Работая над конспектом лекций, всегда следует использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор, в том числе нормативно-правовые акты соответствующей направленности. По результатам работы с конспектом лекции следует обозначить вопросы, термины, материал, который вызывают трудности, пометить и попытаться найти ответ в рекомендуемой литературе.

Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лабораторном занятии. Лекционный материал является базовым, с которого необходимо начать освоение соответствующего раздела или темы.

Лабораторные занятия

Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Ознакомление с темами и планами лабораторных занятий. Анализ основной нормативно-правовой и учебной литературы, после чего работа с рекомендованной дополнительной литературой.

Просмотр рекомендуемой литературы, работа с текстами нормативно- правовых актов. Решение задач выданных обучающемуся для решения самостоятельно. Устные ответы обучающихся по контрольным вопросам на лабораторных занятиях. Ответы должно быть компактным и вразумительным, без неоправданных отступлений и рассуждений. Обучающийся должен излагать (не читать) изученный материал свободно. В случае неточностей и (или) непонимания какого-либо вопроса пройденного материала.

Приложение 1

Оценочные материалы при формировании рабочей программы дисциплины ОП. 01 Основы информационной безопасности

1. Описание показателей, критериев и шкал оценивания компетенций.

1.1. Показатели и критерии оценивания компетенций ОК 03, ОК 06, ОК 09, ОК 10, ОК 11, ПК 2.4.

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения **не ниже порогового**

1.2. Шкалы оценивания компетенций ОК 03, ОК 06, ОК 09, ОК 10, ОК 11, ПК 2.4. при сдаче других форм промежуточной аттестации (устный опрос) и зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Устный опрос (зачет)
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно (Не зачтено)
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно (Зачтено)
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо (Зачтено)
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично (Зачтено)

1.3. Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительно (Не зачтено)	Удовлетворительно (Зачтено)	Хорошо (Зачтено)	Отлично (Зачтено)
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Иметь практический опыт	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Примерный перечень вопросов к другим формам промежуточной аттестации (устному опросу).

2.1 Примерный перечень вопросов к другим формам промежуточной аттестации (устному опросу).

Компетенция ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4.

1. Основные понятия и задачи информационной безопасности.
2. Обзор защищаемых объектов и систем.
3. Основы защиты информации.
4. Понятия государственной тайны и конфиденциальной информации.
5. Понятие национальной безопасности.

Компетенция ОК 03, ОК 06, ПК 2.4.

1. Определение информационной безопасности
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства
3. Место информационной безопасности в системе национальной безопасности
4. Интересы личности в информационной сфере
5. Интересы общества в информационной сфере
6. Интересы государства в информационной сфере
7. Виды угроз информационной безопасности
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Внешние источники угроз информационной безопасности

Компетенция ОК 09, ОК 10, ОК 11, ПК 2.4.

1. Внутренние источники угроз информационной безопасности государства
2. Информационное оружие, его классификация и возможности
3. Доктрина информационной войны
4. Методы и средства ведения информационной войны
5. Понятие информационного противоборства
6. Причины искажения информации

2.2 Примерный перечень вопросов к зачету.

Компетенция ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4.

1. Виды искажения информации
2. Каналы утечки
3. Естественные и искусственные каналы утечки информации
4. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.

Компетенция ОК 03, ОК 06, ПК 2.4.

1. Критерии и классы защищенности средств ВТ
2. Компьютерная система как объект информационной безопасности.
3. Информационные процессы как объект информационной безопасности
4. Влияние человеческого фактора на обеспечение информационной безопасности
5. Программно-аппаратные средства обеспечения информационной безопасности.

Компетенция ОК 09, ОК 10, ОК 11, ПК 2.4.

1. Классификация программно-аппаратных средств обеспечения информационной безопасности
2. Защита от несанкционированного доступа
3. Антивирусная защита
4. Межсетевые экраны
5. VPN-технологии
6. Криптографические методы защиты информации

3. Тестовые задания. Оценка по результатам тестирования

3.1. Примерные задания теста к другим формам промежуточной аттестации (устному опросу).

Компетенция ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4.

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

Компетенция ОК 03, ОК 06, ПК 2.4.

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

Компетенция ОК 09, ОК 10, ОК 11, ПК 2.4.

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

3.2. Примерные задания теста для зачета

Компетенция ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4.

1) Принципом политики информационной безопасности является принцип:

- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

2) 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

3) Принципом политики информационной безопасности является принцип:

- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

4) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

5) 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

6) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа

7) ЭЦП – это:

- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор

Компетенция ОК 03, ОК 06, ПК 2.4.

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

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

10) 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

11) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

12) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальность

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

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

Компетенция ОК 09, ОК 10, ОК 11, ПК 2.4.

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

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

17) 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

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

3.3. Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующих таблиц:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Не зачтено»	Низкий уровень
	74 – 61 баллов	«Зачтено»	Пороговый уровень
	84 – 75 баллов		Повышенный уровень
	100 – 85 баллов		Высокий уровень

4. Оценка ответа обучающегося на вопросы других форм промежуточной аттестации (устного опроса) и зачета.

4.1 Оценка ответа обучающегося на вопросы других форм промежуточной аттестации (устного опроса)

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.

4.2 Оценка ответа обучающегося на вопросы зачета.

Элементы оценивания	Содержание шкалы оценивания			
	«Не зачтено»	«Зачтено»		
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам	Значительные погрешности	Незначительные погрешности	Полное соответствие
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию	Незначительное несоответствие критерию	Соответствие критерию при ответе на все вопросы.

Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	1. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.