МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

24.12.2020 г.

протокол № 13

Зав. кафедрой Бахтеева Е.И.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

20 января 2021 г.

протокол № 6

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Правовые аспекты информационной безопасности
Направление подготовки	38.03.01 Экономика
Профиль	Экономическая безопасность и управление рисками
Форма обучения	очная
Год набора	2021

Разработана:
Доцент, к.э.н.
Матвеев Е.В.

Екатеринбург
2021 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.01 Экономика (приказ Минобрнауки России от 12.08.2020 г. № 954)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

является формирование у студентов целостного представления о процессах и основных тенденциях современного развития информационных технологий и правовых методов их защиты

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточный контроль	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Практические занятия, включая курсовое проектирование		
Семестр 7						
Зачет	216	56	28	28	160	6

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
организационно-управленческий	
ПК-5 Выработка способности осуществления профессиональной деятельности на основе развитого правосознания, правового мышления и правовой культуры	ИД-1.ПК-5 Знать: Основные теоретические аспекты противодействия коррупции
	ИД-2.ПК-5 Уметь: Четко разграничивать формы коррупционного поведения

ПК-5 Выработка способности осуществления профессиональной деятельности на основе развитого правосознания, правового мышления и правовой культуры	ИД-3.ПК-5 Иметь практический опыт: Противодействия коррупционному поведению на основе развитого правосознания, правового мышления и правовой культуры

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 7		16					
Тема 1.	Организационно-технические аспекты информационной безопасности	16	2		2	12	
Семестр 7		28					
Тема 2.	Правовые основы информационной безопасности	28	4		4	20	
Семестр 7		20					
Тема 3.	Теория организации доступа в информационных системах	20	4		4	12	
Семестр 7		28					
Тема 4.	Правовые основы защиты от вредоносных программ	28	4		4	20	
Семестр 7		28					
Тема 5.	Понятие и правовые аспекты сетевой безопасности	28	4		4	20	
Семестр 7		26					
Тема 6.	Национальные интересы и информационная безопасность: организационно-правовой аспект	26	4		2	20	
Семестр 7		24					
Тема 7.	Организационно-правовая основа системы обеспечения информационной безопасности	24	2		2	20	
Семестр 7		26					
Тема 8.	Организационно-правовой механизм предотвращения угроз информационной безопасности РФ	26	2		2	22	
Семестр 7		20					
Тема 9.	Юридическая ответственность за правонарушения в сфере компьютерной информации	20	2		4	14	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Темы 1-3	Контрольная работа (Приложение 4)	Содержатся вопросы и практические задания	Средство проверки умений применять полученные знания для решения задач определенного типа по теме (от 0 до 10 баллов)
Темы 4-6	Контрольная работа (Приложение 4)	Содержатся вопросы и практические задания	Средство проверки умений применять полученные знания для решения задач определенного типа по теме (от 0 до 10 баллов)
Темы 7-9	Контрольная работа (Приложение 4)	Содержатся вопросы и практически е задания	Средство проверки умений применять полученные знания для решения задач определенного типа по теме (от 0 до 10 баллов)
Промежуточный контроль (Приложение 5)			
7 семестр (За)	Билет для зачета (Приложение 5)	Билет включает в себя 1 теоретический вопрос и 1 практикоориентированное задание	Ответ правильный, всесторонне и глубоко освещает предложенный вопрос, устанавливает взаимосвязь теории с практикой, показывает умение студента работать с литературой, делать выводы (правильный и полный ответ) – 85 -100 баллов. Ответ отвечает основным

			предъявляемым требованиям; студент обстоятельно владеет материалом, однако не на все вопросы дает глубокие, исчерпывающие и аргументированные ответы (точный, но неполный ответ) – 70-84 баллов. Ответ неполно раскрывает поставленные вопросы. Студент владеет материалом, однако поверхностно отвечает на вопросы, допускает существенные недочеты (неточный и неполный ответ) – 50-69 баллов. Ответы на вопросы неправильны и не отличаются аргументированностью. Студент не показывает необходимых минимальных знаний по предмету, а также, если студент отказывается отвечать (неправильный ответ, отказ от ответа) – 0-49 баллов.

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущей и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущая аттестация. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Организационно-технические аспекты информационной безопасности

История и современные цели информационной безопасности. Три основных аспекта обеспечения информационной безопасности. История становления процесса защиты информации, его правовое регулирование. Организационно-правовые методы предупреждения угроз и предотвращения реализации угроз защиты информации.

Тема 2. Правовые основы информационной безопасности

Месторасположения источника и уровня воздействия на информацию. Обзор общей ситуации в области правовой защиты информации. Нормативные акты, регулирующие защиту государственной и коммерческой тайны. Средства технической, организационной и правовой защиты информации. Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.

Тема 3. Теория организации доступа в информационных системах

Организационно-правовая и общая классификация субъектов и объектов информационных систем. Задачи информационной безопасности в обеспечении ограниченных прав действий субъектов над объектами. Права доступа к информации; ограничение доступа и неограниченный доступ к получению информации. Нормативно-правовая база обеспечения информационной безопасности.Теория организации доступа в информационных системах: организационно-правовой аспект.

Тема 4. Правовые основы защиты от вредоносных программ

Вредоносные программы и их примеры. Цели использования вредоносных программ. Внедрение и управление кодом информационной систем. Классификация нарушений конфиденциальности, целостность или доступность информации. Классификация вредоносных программ. Цели и сущность троянские программы. Нормативно-правовая база обеспечения информационной безопасности.

Тема 5. Понятие и правовые аспекты сетевой безопасности

Классификация, цели и источники угроз информации, обрабатываемой в компьютерных сетях. Причины, вызывающие возможность реализации этих угроз на практике: организационно-правовой аспект. Нормативно-правовая база обеспечения информационной безопасности

Тема 6. Национальные интересы и информационная безопасность: организационно-правовой аспект

Национальные интересы и информационная безопасность РФ: организационно-правовой аспект Понятие правовой и общей защищенности национальных интересов в информационной сфере. Интересы общества, личности и государства в информационной сфере. Национальные интересы РФ в информационной сфере. Обеспечение соблюдения конституционных прав и свобод человека и гражданина в области получения информации и пользования ею. Защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных и телекоммуникационных систем; цели информационного воздействия. Нормативно-правовая база

Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности

Основные функции системы обеспечения информационной безопасности Российской Федерации. Функции системы обеспечения информационной безопасности Российской Федерации и их содержание. Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в сфере обеспечения информационной безопасности. Нормативная правовая база обеспечения информационной безопасности.

Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ

Понятие и виды угроз информационной безопасности РФ. Виды и сущность угроз информационной безопасности. Понятие и виды источников угроз информационной безопасности РФ. Виды и сущность источников угроз информационной безопасности. Нормативная правовая база обеспечения информационной безопасности.

Тема 9. Юридическая ответственность за правонарушения в сфере компьютерной информации

Ответственность за правонарушения в сфере компьютерной информации

Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.

7.2 Содержание практических занятий и лабораторных работ

Тема 1. Организационно-технические аспекты информационной безопасности Классификация угроз информационной безопасности. Правовые угрозы информационной безопасности. Информационные угрозы, их причины и виды.
Тема 2. Правовые основы информационной безопасности Нормативные акты, регулирующие защиту государственной и коммерческой тайны. Средства технической, организационной и правовой защиты информации. Нормативно-правовая база обеспечения информационной безопасности.
Тема 3. Теория организации доступа в информационных системах Задачи информационной безопасности в обеспечении ограниченных прав действий субъектов над объектами. Права доступа к информации; ограничение доступа и неограниченный доступ к получению информации.
Тема 4. Правовые основы защиты от вредоносных программ Задачи информационной безопасности в обеспечении ограниченных прав действий субъектов над объектами. Права доступа к информации; ограничение доступа и неограниченный доступ к получению информации.
Тема 5. Понятие и правовые аспекты сетевой безопасности Классификация, цели и источники угроз информации, обрабатываемой в компьютерных сетях. Причины, вызывающие возможность реализации этих угроз на практике: организационно-правовой аспект. Объекты информационной безопасности в учреждении, на предприятии. Система защиты информации.
Тема 6. Национальные интересы и информационная безопасность: организационно-правовой аспект Национальные интересы и информационная безопасность РФ: организационно-правовой аспект. Особенности современного информационного общества. Элементы информационной инфраструктуры. Понятие конфиденциальности, целостности и доступности информации.
Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности Общая характеристика и правовые методы обеспечения информационной безопасности РФ. Совокупность методов обеспечения интересов РФ в информационной сфере. Классификация методов обеспечения информационной безопасности. Характеристика организационно-технических и экономических методов обеспечения информационной безопасности РФ. Нормативно-правовая база обеспечения информационной безопасности.
Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ Понятие и виды угроз информационной безопасности РФ. Виды и сущность угроз информационной безопасности. Понятие и виды источников угроз информационной безопасности РФ. Виды и сущность источников угроз информационной безопасности.
Тема 9. Юридическая ответственность за правонарушения в сфере компьютерной информации Виды правонарушений в сфере компьютерной информации. Основания и виды ответственности за правонарушения в сфере компьютерной информации.

7.3. Содержание самостоятельной работы

Тема 1. Организационно-технические аспекты информационной безопасности Вопросы: 1. Классификация угроз информационной безопасности. 2. Правовые угрозы информационной безопасности. 3. Нормативно-правовая база обеспечения информационной безопасности.
Тема 2. Правовые основы информационной безопасности Вопросы: 1. Нормативные акты, регулирующие защиту государственной и коммерческой тайны. 2. Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности.

Тема 3. Теория организации доступа в информационных системах
Вопросы:
1. Права доступа к информации; ограничение доступа и неограниченный доступ к получению информации.
2. Задачи информационной безопасности в обеспечении ограниченных прав действий субъектов над объектами.

Тема 4. Правовые основы защиты от вредоносных программ
Вопросы:
1. Цели и сущность троянских программ.
2. Виды вредоносных программ.
3. Средства защиты от вредоносных программ.

Тема 5. Понятие и правовые аспекты сетевой безопасности
Вопросы:
1. Цели и сущность троянских программ.
2. Виды вредоносных программ.
3. Средства защиты от вредоносных программ.

Тема 6. Национальные интересы и информационная безопасность: организационно-правовой аспект
Вопросы:
1. Защита информационных ресурсов от несанкционированного доступа.
2. Обеспечение безопасности информационных и телекоммуникационных систем.

Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности
Вопросы:
1. Система обеспечения информационной безопасности Российской Федерации.
2. Компетенция федеральных органов государственной власти в сфере обеспечения информационной безопасности.
3. Компетенция органов государственной власти субъектов Российской Федерации в сфере обеспечения информационной безопасности.
4. Какие обеспечивающие подсистемы включает система защиты информации?
5. Что такое конфиденциальность, целостность и доступность информации?

Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ
Вопросы:
1. Методы обеспечения информационной безопасности.
2. Экономические методы обеспечения информационной безопасности в РФ
3. Организационно-технические методы обеспечения информационной безопасности.
4. Назовите информационные угрозы для государства.
5. Что угрожает личности (физическому лицу)?
6. Какие действия и события нарушают ИБ?
7. Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз ИБ?
8. Назовите основные компьютерные вирусы.
9. Назовите причины информационных угроз

Тема 9. Юридическая ответственность за правонарушения в сфере компьютерной информации
Вопросы:
1. Характеристика уголовных преступлений в сфере компьютерной информации.
2. Характеристика административных правонарушений в сфере компьютерной информации.
3. Гражданско-правовая ответственность за нарушение информационной безопасности.
4. Дисциплинарная ответственность в сфере компьютерной информации.
5. Какие вы знаете компьютерные преступления?

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Не предусмотрена учебным планом.

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Не предусмотрена учебным планом

7.6 Методические рекомендации по выполнению курсовой работы
Не предусмотрена учебным планом.

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

1. Русскевич Е. А. Уголовное право и "цифровая преступность": проблемы и решения. [Электронный ресурс]:монография. - Москва: ИНФРА-М, 2020. - 227 – Режим доступа: https://znanium.com/catalog/product/1061706

2. Овчинский В. С. Криминология цифрового мира. [Электронный ресурс]:учебник для магистратуры. - Москва: Норма: ИНФРА-М, 2020. - 352 – Режим доступа: https://znanium.com/catalog/product/1059377

3. Бачило И. Л. Информационное право. [Электронный ресурс]:Учебник для вузов. - Москва: Юрайт, 2020. - 419 – Режим доступа: https://urait.ru/bcode/449666

4. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 223 – Режим доступа: https://znanium.com/catalog/product/1189349

5. Ковалева Н. Н., Брянцев И. И., Брянцева О. В., Варламова Е. В., Ересько П. В., Жирнова Н. А., Изотова В. Ф., Ильгова Е. В., Сергеева Е. Ю., Солдаткина О. Л., Тугушева Ю. М., Холодная Е. В., Чайковский Д. С. Информационное право. [Электронный ресурс]:Учебник для вузов. - Москва: Юрайт, 2020. - 353 – Режим доступа: https://urait.ru/bcode/466887

6. Сычев Ю.Н. Защита информации и информационная безопасность. [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 201 – Режим доступа: https://znanium.com/catalog/product/1013711

Дополнительная литература:

1. Основы борьбы с киберпреступностью и кибертерроризмом. [Электронный ресурс]:хрестоматия. - Москва: Норма, 2017. - 528 – Режим доступа: https://znanium.com/catalog/product/771246

2. Гришина Н. В. Основы информационной безопасности предприятия. [Электронный ресурс]:учебное пособие для студентов вузов, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2019. - 216 – Режим доступа: https://znanium.com/catalog/product/1017663

3. Степанов О. А. Противодействие кибертерроризму в цифровую эпоху. [Электронный ресурс]:Монография. - Москва: Юрайт, 2020. - 103 – Режим доступа: https://urait.ru/bcode/448300

4. Архипов В. В. Интернет-право. [Электронный ресурс]:Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 249 – Режим доступа: https://urait.ru/bcode/450761

5. Рассолов И. М. Информационное право. [Электронный ресурс]:Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 347 – Режим доступа: https://urait.ru/bcode/449839

6. Правовые аспекты информационной безопасности. Учебное пособие. Ч. 1. [Электронный ресурс]:. - Екатеринбург: [Издательство УрГЭУ], 2015. - 98 – Режим доступа: http://lib.usue.ru/resource/limit/ump/15/p485369.pdf

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии 30.09.2023.

Astra Linux Common Edition. Договор № 1 от 13 июня 2018, акт от 17 декабря 2018. Срок действия лицензии - без ограничения срока.

Corel Painter 2017. Договор № 34-С 2017 от 27.03.2017, Акт № Tr007267 от 24.01.2020. Срок действия лицензии -бессрочное пользование.

CorelDRAW Graphics Suite X8. Договор № 34-С 2017 от 27.03.2017, Акт № Tr007267 от 24.01.2020. Срок действия лицензии -бессрочное пользование.

Corel PaintShop Pro X9. Договор № 34-С 2017 от 27.03.2017, Акт № Tr007267 от 24.01.2020. Срок действия лицензии -бессрочное пользование.

Конфигурация 1С:Зарплата и Управление Персоналом 8. Договор Б/Н от 02.06.2009 г., Лицензионное соглашение № 8971903, Акт № 62 от 15.07.2009 "1С:Зарплата и кадры бюджетного учреждения 8" (рег. номер 9648728).

Microsoft Dynamics CRM. Соглашение от 23.08.2016.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

ВККБ Бизнес-курс Максимум. Договор, Лицензия № БК-М1-КОЛ-1316. Срок действия лицензии - без ограничения срока.

Adobe Lightroom CC.Договор № 140/223-ПО/2020 от 19.10.2020. Срок действия лицензии 13.12.2021.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Консультант +. Договор № 163/223-У/2020 от 14.12.2020. Срок действия лицензии до 31.12.2021

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.