МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

16.11.2022 г.

протокол № 4

Зав. кафедрой Карпов А.Е.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

14 декабря 2022 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная безопасность телекоммуникационных систем
Направление подготовки	02.03.03 Математическое обеспечение и администрирование информационных систем
Профиль	Разработка и администрирование информационных систем
Форма обучения	очная
Год набора	2023

Разработана:
Профессор, д.т.н.
Часовских В.П.

Екатеринбург
2022 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 02.03.03 Математическое обеспечение и администрирование информационных систем (приказ Минобрнауки России от 23.08.2017 г. № 809)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

раскрытие сущности информационной безопасности и защиты информации, определение теоретических, методологических и организационных основ обеспечения безопасности информации, ознакомление с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации

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	Лабораторные		
Семестр 5						
Зачет	144	56	28	28	88	4
Семестр 6						
Экзамен, Курсовая работа	144	36	0	36	72	4
	288	92	28	64	160	8

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

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

Шифр и наименование компетенции	Индикаторы достижения компетенций

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	ИД-1.УК-8 Знать: основы безопасности жизнедеятельности, телефоны служб спасения.
	ИД-2.УК-8 Уметь: оказать первую помощь в чрезвычайных ситуациях, создавать безопасные условия реализации профессиональной деятельности.
	ИД-3.УК-8 Иметь практический опыт поддержания безопасных условий жизнедеятельности.

Шифр и наименование компетенции	Индикаторы достижения компетенций
производственно-технологический	
ПК-1 Оптимизация работы систем безопасности с целью уменьшения нагрузки на работу БД	ИД-1.ПК-1 Знать: характеристики различных систем обеспечения безопасности, влияющие на производительность БД; методы и средства обеспечения безопасности данных при работе с установленной БД.

ПК-1 Оптимизация работы систем безопасности с целью уменьшения нагрузки на работу БД	ИД-2.ПК-1 Уметь: оценивать степень нагрузки различных инструментов обеспечения безопасности на производительность БД; настраивать параметры инструментов системы безопасности в соответствии с установленными критериями.
	ИД-3.ПК-1 Иметь практический опыт: определения возможностей оптимизации работы систем безопасности с целью уменьшения нагрузки на работу БД; выбора наиболее эффективных путей снижения нагрузки при обеспечении заданного уровня безопасности данных на уровне БД.
ПК-2 Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным	ИД-1.ПК-2 Знать: программно-технические средства защиты данных от несанкционированного доступа, их возможности; способы и методы несанкционированного доступа к данным и механизмы противодействия попыткам несанкционированного доступа.
	ИД-2.ПК-2 Уметь: разворачивать и настраивать программно-аппаратные средства защиты данных; создавать и настраивать автоматизированные процедуры выявления попыток несанкционированного доступа к данным.
	ИД-3.ПК-2 Иметь практический опыт: анализа возможностей программирования процедур для выявления попыток несанкционированного доступа к данным; применения средств программирования для разработки автоматизированных процедур выявления попыток несанкционированного доступа к данным.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
организационно-управленческий	
ПК-7 Разработка политики информационной безопасности на уровне БД	ИД-1.ПК-7 Знать: угрозы безопасности БД и способы их предотвращения; инструменты обеспечения безопасности БД и их возможности
	ИД-2.ПК-7 Уметь: выявлять угрозы безопасности на уровне БД; разрабатывать мероприятия по обеспечению безопасности на уровне БД.
	ИД-3.ПК-7 Иметь практический опыт: анализа возможных угроз для безопасности данных; выбора основных средств поддержки информационной безопасности на уровне БД.

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов

	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		144					
Тема 1.	Основные понятия и анализ угроз информационной безопасности. Разработка политики информационной безопасности на уровне БД (УК-8, ПК-7)	12	2			10	
Тема 2.	Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным. (ПК-1, ПК-2)	22	2	10		10	
Тема 3.	Классическая криптография (ПК-1, ПК-2)	12	2			10	
Тема 4.	Симметричные алгоритмы шифрования (ПК-1, ПК-2)	20	2	8		10	
Тема 5.	Хэш-функции (ПК-1, ПК-2)	22	2	10		10	
Тема 6.	Электронно-цифровая подпись (ПК-1, ПК-2)	12	2			10	
Тема 7.	Асимметричные алгоритмы шифрования (ПК-1, ПК-2)	12	2			10	
Тема 8.	Стеганография и стеганоанализ (ПК-1, ПК-2)	12	2			10	
Тема 9.	Уязвимости программного обеспечения (ПК-1, ПК-2)	10	2			8	
Тема 10.	Компьютерные вирусы и методы их обнаружения (ПК-1, ПК-2)	2	2				
Тема 11.	Разделение прав в операционных системах (ПК-1, ПК-2)	2	2				
Тема 12.	Методы авторизации и аутентификации пользователей (ПК-1, ПК-2)	3	3				
Тема 13.	Безопасность сетей ЭВМ (ПК-1, ПК-2)	3	3				
Семестр 6		108					
Тема 14.	Ассиметричные алгоритмы шифрования (продолжение) (ПК-1, ПК-2)	10		10			
Тема 15.	Стеганография и стеганоанализ (продолжение) (ПК-1, ПК-2)	10		10			
Тема 16.	Уязвимости программного обеспечения (продолжение) (ПК-1, ПК-2)	8		8			
Тема 17.	Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-1, ПК-2)	26		8		18	
Тема 18.	Разделение прав в операционных системах (продолжение) (ПК-1, ПК-2)	18				18	
Тема 19.	Методы авторизации и аутентификации пользователей (продолжение) (ПК-1, ПК-2)	18				18	

Тема 20.	Безопасность сетей ЭВМ (продолжение) (ПК-1, ПК-2)	18				18	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1, тема 2, тема 3, тема 4, тема 5, тема 6	Тест №1 (Приложение 4)	Тест по вариантам из 66 вопросов	66 баллов: 1 балл за каждый вопрос
Тема 7, тема 8, тема 9, тема 10, тема 11, тема 12, тема 13	Тест №2 (Приложение 4)	Тест по вариантам из 54 вопросов	54 баллов: 1 балл за каждый вопрос
Тема 14, тема 15, тема 16, тема 17, тема 18, тема 19, тема 20	Тест №3 (Приложение 4)	Тест по вариантам из 60 вопросов	60 баллов: 1 балл за каждый вопрос
Промежуточный контроль (Приложение 5)			
5 семестр (За)	Зачетные билеты (Приложение 5)	15 билетов, состоящих из 1 теоретического и 1 практического задания	70 баллов: 20 + 50 соответственно
6 семестр (Эк)	Экзаменационные билеты (Приложение 5)	15 билетов, состоящих из 1 теоретического и 1 практического задания	70 баллов: 20 + 50 соответственно
6 семестр (КР)	Курсовая работа (Приложение 3, Приложение 7)	Перечень тем курсовых работ приведен в Приложении 3. Методические указания к выполнению курсовой работы приведены в Приложении 7	Максимальное количество баллов - 100

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 профессиональных задач
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. Основные понятия и анализ угроз информационной безопасности. Разработка политики информационной безопасности на уровне БД (УК-8, ПК-7) Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности и их классификация
Тема 2. Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным. (ПК-1, ПК-2) Основные понятия криптографической защиты информации. Модульная арифметика, сравнения и матрицы. Алгебраические структуры (группы, кольца, поля). Простые числа и уравнения сравнения
Тема 3. Классическая криптография (ПК-1, ПК-2) Симметричные шифры замены и перестановок. Шифры: афинный, Вижинера, Хилла. Криптоанализ классических шифров.
Тема 4. Симметричные алгоритмы шифрования (ПК-1, ПК-2) Алгоритмы DES, AES, ГОСТ 28147-89
Тема 5. Хэш-функции (ПК-1, ПК-2) Одностороння функция и одностороння функция с секретом. Хэш-функции, их свойства и применение. Обзор хэш-функций SHA, Whirpool
Тема 6. Электронно-цифровая подпись (ПК-1, ПК-2) Понятия об электронно-цифровой подписи (ЭЦП). Схема формирования ЭЦП.
Тема 7. Асимметричные алгоритмы шифрования (ПК-1, ПК-2) Алгоритмы RSA, системы шифрования на эллиптических кривых
Тема 8. Стеганография и стеганоанализ (ПК-1, ПК-2) Классическая и компьютерная стенография. Методы компьютерной стеганографии. Цифровые водяные знаки. Стеганоанализ. Методы стеганоанализа
Тема 9. Уязвимости программного обеспечения (ПК-1, ПК-2) Уязвимости переполнения буфера, переполнения целочисленных значений, форматирующей строки, возвращения управления в lips. Основы работы с отладчиком и дизассемблером.
Тема 10. Компьютерные вирусы и методы их обнаружения (ПК-1, ПК-2) Классификация вредоносного программного обеспечения. Способы обнаружения компьютерных вирусов. Антивирусы
Тема 11. Разделение прав в операционных системах (ПК-1, ПК-2) Принципы построения многопользовательской операционной системы. Принципы организации безопасности на уровне операционной системы
Тема 12. Методы авторизации и аутентификации пользователей (ПК-1, ПК-2) Методы авторизации и аутентификации пользователей. Фиксированные и одноразовые пароли.
Тема 13. Безопасность сетей ЭВМ (ПК-1, ПК-2) Безопасность на прикладном, на транспортном, на сетевом уровнях. Принципы построения виртуальных защищенных сетей. Принципы работы межсетевых экранов и систем обнаружения вторжений

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным. (ПК-1, ПК-2) Нахождение НОД. Нахождение модульных инверсий. Нахождение обратных матриц. Испытание простоты чисел
Тема 4. Симметричные алгоритмы шифрования (ПК-1, ПК-2) Знакомство с пакетом OpenSSL
Тема 5. Хэш-функции (ПК-1, ПК-2) Симметричное шифрование. Работа с пакетом OpenSSL
Тема 14. Ассиметричные алгоритмы шифрования (продолжение) (ПК-1, ПК-2) Ассиметричное шифрование. Работа с пакетом OpenSSL
Тема 15. Стеганография и стеганоанализ (продолжение) (ПК-1, ПК-2) Текстовая стеганография. Работа с пакетом OpenPuff
Тема 16. Уязвимости программного обеспечения (продолжение) (ПК-1, ПК-2) Исследование уязвимостей программного обеспечения. Работа с программой IDA Pro
Тема 17. Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-1, ПК-2) Исследование компьютерных вирусов в дизассемблере. Работа с программой IDA Pro

7.3. Содержание самостоятельной работы

Тема 1. Основные понятия и анализ угроз информационной безопасности. Разработка политики информационной безопасности на уровне БД (УК-8, ПК-7) Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности и их классификация
Тема 2. Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным. (ПК-1, ПК-2) Основные понятия криптографической защиты информации. Модульная арифметика, сравнения и матрицы. Алгебраические структуры (группы, кольца, поля). Простые числа и уравнения сравнения.
Тема 3. Классическая криптография (ПК-1, ПК-2) Симметричные шифры замены и перестановок. Шифры: афинный, Вижинера, Хилла. Криптоанализ классических шифров.
Тема 4. Симметричные алгоритмы шифрования (ПК-1, ПК-2) Алгоритмы DES, AES, ГОСТ 28147-89
Тема 5. Хэш-функции (ПК-1, ПК-2) Односторонняя функция и односторонняя функция с секретом. Хэш-функции, их свойства и применение. Обзор хэш-функций SHA, Whirpool

Тема 6. Электронно-цифровая подпись (ПК-1, ПК-2) Понятие об электронно-цифровая подпись (ЭЦП). Схема формирования ЭЦП.
Тема 7. Асимметричные алгоритмы шифрования (ПК-1, ПК-2) Алгоритм RSA, системы шифрования на эллиптических кривых
Тема 8. Стеганография и стеганоанализ (ПК-1, ПК-2) Классическая и компьютерная стеганография. Методы компьютерной стеганографии. Цифровые водяные знаки. Стеганоанализ. Методы стеганоанализа
Тема 9. Уязвимости программного обеспечения (ПК-1, ПК-2) Уязвимости переполнения буфера, переполнения целочисленных значений, форматирующей строки, возвращения управления в libc. Основы работы с отладчиком и дизассемблером
Тема 17. Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-1, ПК-2) Классификация вредоносного программного обеспечения. Способы обнаружения компьютерных вирусов. Антивирусы
Тема 18. Разделение прав в операционных системах (продолжение) (ПК-1, ПК-2) Принципы построения многопользовательской операционной системы. Принципы организации безопасности на уровне операционной системы
Тема 19. Методы авторизации и аутентификации пользователей (продолжение) (ПК-1, ПК-2) Методы авторизации и аутентификации пользователей. Фиксированные и одноразовые пароли
Тема 20. Безопасность сетей ЭВМ (продолжение) (ПК-1, ПК-2) Безопасность на прикладном, на транспортном, на сетевом уровнях. Принципы построения виртуальных защищенных сетей. Принципы работы межсетевых экранов и систем обнаружения вторжений

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
Приложение 3

7.4. Электронное портфолио обучающегося
Размещается курсовая работа

7.5. Методические рекомендации по выполнению контрольной работы
Материалы не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
Приложение 7

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. Крамаров С.О., Тищенко Е.Н. Криптографическая защита информации. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2018. - 324 с. – Режим доступа: https://znanium.com/catalog/product/901659

2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2019. - 592 с. – Режим доступа: https://znanium.com/catalog/product/996789

3. Крамаров С.О., Тищенко Е.Н. Криптографическая защита информации. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2019. - 324 с. – Режим доступа: https://znanium.com/catalog/product/1018903

4. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 118 с. – Режим доступа: https://znanium.com/catalog/product/1178153

5. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 223 с. – Режим доступа: https://znanium.com/catalog/product/1178148

6. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 с. – Режим доступа: https://znanium.com/catalog/product/1843022

7. Ищейнов В. Я., Мецатунян М. В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 256 с. – Режим доступа: https://znanium.com/catalog/product/1861659

8. Моргунов А.В. Информационная безопасность [Электронный ресурс]:Учебно-методическая литература. - Новосибирск: Новосибирский государственный технический университет (НГТУ), 2019. - 83 с. – Режим доступа: https://znanium.com/catalog/product/1866895

9. Гришина Н. В. Основы моделирования процессов и систем защиты информации [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 107 с. – Режим доступа: https://znanium.com/catalog/product/1891122

Дополнительная литература:

1. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2021. - 320 с. – Режим доступа: https://znanium.com/catalog/product/1232287

2. Баранова Е.К., Бабаш А.В., Ларин Д.А. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2022. - 236 с. – Режим доступа: https://znanium.com/catalog/product/1843171

3. Гришина Н. В. Основы управления информационной безопасностью [Электронный ресурс]:Учебно-методическая литература. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 99 с. – Режим доступа: https://znanium.com/catalog/product/1859951

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.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023.

Adobe Reader. Лицензия freeeware. Срок действия лицензии - без ограничения срока.

Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

hMailServer. Лицензия AGPL. Срок действия лицензии - без ограничения срока.

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

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

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.