МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

24.11.2022 г.

протокол № 4

Зав. кафедрой Бахтеева Е.И.

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	Организационное и правовое обеспечение информационной безопасности
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2023

Разработана:
Доцент, к.ю.н.
Богатова Е.В.

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 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Получение знаний, умений, навыков, необходимых для формирования компетенций, связанных со способностью осуществления администрирования подсистем защиты информации в операционных системах; программно-аппаратных средств защиты информации в компьютерных сетях; подготовки данных для проведения аналитических работ по исследованию больших данных

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 5						
Зачет	108	84	28	56	24	3

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
эксплуатационный	

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-1.ПК-1 Знать: Архитектура и принципы построения операционных систем Программные интерфейсы операционных систем Виды политик управления доступом и информационными потоками применительно к операционным системам Архитектура подсистем защиты информации в операционных системах Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы Состав типовых конфигураций программно-аппаратных средств защиты информации Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам Порядок реализации методов и средств антивирусной защиты в операционных системах Программно-аппаратные средства и методы защиты информации в операционных системах Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-1 Уметь: Формулировать политики безопасности операционных систем Настраивать политики безопасности операционных систем Оценивать угрозы безопасности информации операционных систем Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах Настраивать антивирусные средства защиты информации в операционных системах Устанавливать обновления программного обеспечения и средств антивирусной защиты Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-3.ПК-1 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации Конфигурирование программно-аппаратных средств защиты информации в операционных системах Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах Управление антивирусной защитой операционных систем в соответствии с действующими требованиями
ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-1.ПК-2 Знать: Принципы построения компьютерных сетей Стек сетевых протоколов операционных систем Стек протоколов сетевого оборудования Порядок реализации методов и средств межсетевого экранирования Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Виды политик управления доступом и информационными потоками в компьютерных сетях Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации Программно-аппаратные средства и методы защиты информации в компьютерных сетях Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации

ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-2.ПК-2 Уметь: Оценивать угрозы безопасности информации в компьютерных сетях Настраивать правила фильтрации пакетов в компьютерных сетях Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях
	ИД-3.ПК-2 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-1.ПК-3 Знать: Архитектура подсистем защиты информации в операционных системах Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их эксплуатации Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-3 Уметь: Анализировать угрозы безопасности информации программного обеспечения Формулировать правила безопасной эксплуатации программного обеспечения Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-3.ПК-3 Иметь практический опыт: Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнение работ по обнаружению вредоносного программного обеспечения Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулирование требований к встроенным средствам защиты информации программного обеспечения

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		108					
Тема 1.	Организационные и правовые аспекты информационной безопасности (ПК-1)	8	2		4	2	
Тема 2.	Правовые основы информационной безопасности (ПК-2)	10	2		6	2	
Тема 3.	Теория организации доступа в информационных системах: организационно-правовой аспект (ПК-3)	12	4		6	2	
Тема 4.	Правовые основы защиты от вредоносных программ (ПК-1)	12	4		6	2	
Тема 5.	Понятие и правовые аспекты сетевой безопасности (ПК-2)	16	4		8	4	
Тема 6.	Национальные интересы и информационная безопасность (ПК-1)	18	4		8	6	
Тема 7.	Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации (ПК-3)	14	4		8	2	
Тема 8.	Организационно-правовой механизм предотвращения угроз информационной безопасности (ПК-1)	10	2		6	2	
Тема 9.	Юридическая ответственность за правонарушения в сфере компьютерной информации (ПК-1)	8	2		4	2	

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)	Комплект контрольных практикоориентированных заданий и теоретические вопросы для изучения материала по темам	Средство проверки умений применять полученные знания для решения задач определенного типа по темам От 0 до 10 баллов
Темы 4-6	Контрольная работа (Приложение 4)	Комплект контрольных практикоориентированных заданий и теоретические вопросы для изучения материала по темам	Средство проверки умений применять полученные знания для решения задач определенного типа по темам От 0 до 10 баллов
Темы 7-9	Контрольная работа (Приложение 4)	Комплект контрольных практикоориентированных заданий и теоретические вопросы для изучения материала по темам	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу От 0 до 10 баллов
Темы 1-9	Тестовое задание (Приложение 4)	Тестовое задание по изучаемым темам	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу От 0 до 10 баллов
Промежуточный контроль (Приложение 5)			
5 семестр (За)	Билет к зачету (Приложение 5)	Билет включает в себя 2 теоретических вопроса 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 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. Организационные и правовые аспекты информационной безопасности (ПК-1)
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 (ПК-2)
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-правовой аспект (ПК-3)
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.

Тема 4. Правовые основы защиты от вредоносных программ (ПК-1)
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 (ПК-2)
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 (ПК-1)
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 обеспечения информационной безопасности.

Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации (ПК-3)
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 (ПК-1)
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 (ПК-1)
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. Организационные и правовые аспекты информационной безопасности (ПК-1)
Вопросы:
1.Классификация угроз информационной безопасности.
2. Правовые угрозы информационной безопасности.
3. Информационные угрозы, их причины и виды.

Тема 2. Правовые основы информационной безопасности (ПК-2)
Вопросы:
1. Нормативные акты, регулирующие защиту государственной и коммерческой тайны.
2. Средства технической, организационной и правовой защиты информации.
3. Нормативно-правовая база обеспечения информационной безопасности.

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

Тема 4. Правовые основы защиты от вредоносных программ (ПК-1)
Вопросы:
1. Классификация нарушений конфиденциальности, целостность или доступность информации.
2. Классификация вредоносных программ.
3. Цели и сущность троянские программы.
4. Нормативно-правовая база обеспечения информационной безопасности.

Тема 5. Понятие и правовые аспекты сетевой безопасности (ПК-2)
Вопросы:
1. Цели и источники угроз информации, обрабатываемой в компьютерных сетях.
2. Объекты информационной безопасности в учреждении, на предприятии.
3. Система защиты информации.

Тема 6. Национальные интересы и информационная безопасность (ПК-1)
Вопросы:
1. Элементы информационной инфраструктуры.
2. Понятие конфиденциальности, целостности и доступности информации.
3. Интересы общества, личности и государства в информационной сфере.

Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации (ПК-3)
Вопросы:
1. Правовые методы обеспечения информационной безопасности РФ.
2. Классификация методов обеспечения информационной безопасности.
3. Характеристика организационно-технических и экономических методов обеспечения информационной безопасности РФ.
4. Нормативно-правовая база обеспечения информационной безопасности.

Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности (ПК-1)
Вопросы:
1. Понятие и виды источников угроз информационной безопасности РФ.
2. Виды и сущность источников угроз информационной безопасности.

Тема 9. Юридическая ответственность за правонарушения в сфере компьютерной информации (ПК-1)
Вопросы:
1. Объективная сторона правонарушений в сфере компьютерной информации.
2. Основания и виды ответственности за правонарушения в сфере компьютерной информации.

7.3. Содержание самостоятельной работы

Тема 1. Организационные и правовые аспекты информационной безопасности (ПК-1)
Вопросы:
1.Классификация угроз информационной безопасности.
2. Правовые угрозы информационной безопасности.
3. Информационные угрозы, их причины и виды.

Тема 2. Правовые основы информационной безопасности (ПК-2)
Вопросы:
1. Нормативные акты, регулирующие защиту государственной и коммерческой тайны.
2. Средства технической, организационной и правовой защиты информации.
3. Нормативно-правовая база обеспечения информационной безопасности.

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

Тема 4. Правовые основы защиты от вредоносных программ (ПК-1)
Вопросы:
1. Классификация нарушений конфиденциальности, целостность или доступность информации.
2. Классификация вредоносных программ.
3. Цели и сущность троянские программы.
4. Нормативно-правовая база обеспечения информационной безопасности.

Тема 5. Понятие и правовые аспекты сетевой безопасности (ПК-2)
Вопросы:
1. Цели и источники угроз информации, обрабатываемой в компьютерных сетях.
2. Объекты информационной безопасности в учреждении, на предприятии.
3. Система защиты информации.

Тема 6. Национальные интересы и информационная безопасность (ПК-1)
Вопросы:
1. Элементы информационной инфраструктуры.
2. Понятие конфиденциальности, целостности и доступности информации.
3. Интересы общества, личности и государства в информационной сфере.

Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации (ПК-3)
Вопросы:
1. Правовые методы обеспечения информационной безопасности РФ.
2. Классификация методов обеспечения информационной безопасности.
3. Характеристика организационно-технических и экономических методов обеспечения информационной безопасности РФ.
4. Нормативно-правовая база обеспечения информационной безопасности.

Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности (ПК-1)
Вопросы:
1. Понятие и виды источников угроз информационной безопасности РФ.
2. Виды и сущность источников угроз информационной безопасности.

Тема 9. Юридическая ответственность за правонарушения в сфере компьютерной информации (ПК-1)
Вопросы:
1. Объективная сторона правонарушений в сфере компьютерной информации.
2. Основания и виды ответственности за правонарушения в сфере компьютерной информации.

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

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
Не предусмотрены

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. Партыка Т. Л., Попов И.И. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2021. - 432 с. – Режим доступа: https://znanium.com/catalog/product/1189328

2. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления [Электронный ресурс]:Монография. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 180 – Режим доступа: https://znanium.com/catalog/product/1137902

3. Козьминых С. И. Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики [Электронный ресурс]:Монография. - Москва: КноРус, 2021. - 281 с. – Режим доступа: https://book.ru/book/941548

Дополнительная литература:

1. Озерский С.В., Попов И.В., Рычаго М.Е., Улендеева Н.И. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Самара: Самарский юридический институт ФСИН России, 2019. - 84 с. – Режим доступа: https://znanium.com/catalog/product/1094244

2. Гришина Н. В. Информационная безопасность предприятия [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2019. - 239 – Режим доступа: https://znanium.com/catalog/product/1001363

3. Чернопятов А. М., под ред. Наука, образование и практика: профессионально-общественная аккредитация, тьюторство, информационные технологии, информационная безопасность [Электронный ресурс]:Монография. - Москва: Русайнс, 2020. - 159 с. – Режим доступа: https://book.ru/book/934840

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.

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

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.

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

Справочно-правовая система Консультант +. Срок действия лицензии до 31.12.2023

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.