

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Силин Яков Петрович
Должность: Ректор
Дата подписания: 20.09.2021 07:06:11
Уникальный программный ключ:
24f866be2aca16484036a8cbb3c509a9531e605f

Одобрена
на заседании кафедры

24.12.2020 г.
протокол № 13
Зав. кафедрой Бахтеева Е.И.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Уральский государственный экономический университет»

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	Организационное и правовое обеспечение информационной безопасности
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2021*
Разработана:	
Доцент, к.э.н.	
Матвеев Е.В.	

Екатеринбург
2021 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	3
3. ОБЪЕМ ДИСЦИПЛИНЫ	3
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП	3
5. ТЕМАТИЧЕСКИЙ ПЛАН	8
6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ	9
7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	12
8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	16
9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	16
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	17
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	19

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.
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					3.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	

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

<p>ПК-1 Администрирование подсистем защиты информации в операционных системах</p>	<p>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</p>
<p>ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях</p>	<p>ИД-1.ПК-2 Знать: Принципы построения компьютерных сетей Стек сетевых протоколов операционных систем Стек протоколов сетевого оборудования Порядок реализации методов и средств межсетевое 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 Организацонные меры по защите информации</p>

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

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

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		22					
Тема 1.	Организационно-технические аспекты информационной безопасности	22	6		10	6	
Семестр 5		18					
Тема 2.	Правовые основы информационной безопасности	18	4		10	4	
Семестр 5		6					
Тема 3.	Теория организации доступа в информационных системах: организационно-правовой аспект	6	2		2	2	
Семестр 5		20					
Тема 4.	Правовые основы защиты от вредоносных программ	20	6		10	4	
Семестр 5		12					
Тема 5.	Понятие и правовые аспекты сетевой безопасности	12	2		8	2	
Семестр 5		12					
Тема 6.	Национальные интересы и информационная безопасность: организационно-правовой аспект	12	2		8	2	
Семестр 5		6					
Тема 7.	Организационно-правовая основа системы обеспечения информационной безопасности	6	2		2	2	
Семестр 5		6					
Тема 8.	Организационно-правовой механизм предотвращения угроз информационной безопасности РФ	6	2		2	2	
Семестр 5		6					

Тема 9.	Юридическая ответственность за правонарушения в сфере компьютерной информации	6	2		4		
---------	---	---	---	--	---	--	--

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)	Содержит вопросы, практические задачи,	0-10 баллов
Темы 4-6	Контрольная работа (Приложение 4)	Содержит вопросы, практические задачи	0-10 баллов
Темы 7-9	Контрольная работа (Приложение 4)	Содержит вопросы, кейс-задания	0-10 баллов
Промежуточный контроль (Приложение 5)			
5 семестр (За)	Билеты для зачета	Билет включает в себя 2 теоретических вопроса и 1 практикоориентированное задание	<p>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.</p> <p>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.</p>

			<p>Ответ неполно раскрывает поставленные вопросы. Студент владеет материалом, однако поверхностно отвечает на вопросы, допускает существенные недочеты (неточный и неполный ответ) – 50-69 баллов.</p> <p>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.</p>
--	--	--	--

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 учебных 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

<p>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</p>
<p>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.</p>
<p>Тема 3. Теория организации доступа в информационных системах: организационно-правовой аспект 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</p>
<p>Тема 4. Правовые основы защиты от вредоносных программ Вредоносные программы и их примеры. Цели использования вредоносных программ. Внедрение и управление кодом информационных систем. Классификация нарушений конфиденциальности, целостность или доступность информации. Классификация вредоносных программ. Цели и сущность троянские программы. Нормативно-правовая база обеспечения информационной безопасности.</p>
<p>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</p>
<p>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</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>

7.2 Содержание практических занятий и лабораторных работ

<p>Тема 1. Организационно-технические аспекты информационной безопасности Классификация угроз информационной безопасности. Правовые угрозы информационной безопасности. Информационные угрозы, их причины и виды.</p>
<p>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.</p>
<p>Тема 3. Теория организации доступа в информационных системах: организационно-правовой аспект Задачи информационной безопасности в обеспечении ограниченных прав действий субъектов над объектами. Права доступа к информации; ограничение доступа и неограниченный доступ к</p>
<p>Тема 4. Правовые основы защиты от вредоносных программ Классификация нарушений конфиденциальности, целостность или доступность информации. Классификация вредоносных программ. Нормативно-правовая база обеспечения информационной безопасности.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>Вопросы:</p> <ol style="list-style-type: none"> 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. Содержание самостоятельной работы

<p>Тема 1. Организационно-технические аспекты информационной безопасности Вопросы:</p> <ol style="list-style-type: none"> 1. Классификация угроз информационной безопасности. 2. Правовые угрозы информационной безопасности. 3. Нормативно-правовая база обеспечения информационной безопасности.

<p>Тема 2. Правовые основы информационной безопасности</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 1. Нормативные акты, регулирующие защиту государственной и коммерческой тайны. 2. Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности.
<p>Тема 3. Теория организации доступа в информационных системах: организационно-правовой аспект</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 1. Права доступа к информации; ограничение доступа и неограниченный доступ к получению информации. 2. Задачи информационной безопасности в обеспечении ограниченных прав действий субъектов
<p>Тема 4. Правовые основы защиты от вредоносных программ</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 1. Цели и сущность троянских программ. 2. Виды вредоносных программ. 3. Средства защиты от вредоносных программ.
<p>Тема 5. Понятие и правовые аспекты сетевой безопасности</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 1. Понятие сетевой безопасности. 2. Источники угроз информации. 3. Организационно-правовые средства сетевой безопасности.
<p>Тема 6. Национальные интересы и информационная безопасность: организационно-правовой аспект</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 1. Защита информационных ресурсов от несанкционированного доступа. 2. Обеспечение безопасности информационных и телекоммуникационных систем.
<p>Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 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?
<p>Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ</p> <p>Вопросы:</p> <ol style="list-style-type: none"> 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

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

4. Корабельников С. М. Преступления в сфере информационной безопасности. [Электронный ресурс]: Учебное пособие для вузов. - Москва: Юрайт, 2020. - 110 – Режим доступа: <https://urait.ru/bcode/448295>

5. Архипов В. В. Интернет-право. [Электронный ресурс]: Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 249 – Режим доступа: <https://urait.ru/bcode/450761>
6. Полякова Т. А., Чубукова С. Г., Ниесов В. А. Организационное и правовое обеспечение информационной безопасности. [Электронный ресурс]: Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 325 – Режим доступа: <https://urait.ru/bcode/450371>
7. Федотов М. А., Антонова А. В., Будник Р. А., Войниканис Е. А., Околеснова О. А., Петрин И. В., Примакова А. В., Семенова Е. В., Тедеев А. А. Информационное право. [Электронный ресурс]: Учебник для вузов. - Москва: Юрайт, 2020. - 497 – Режим доступа: <https://urait.ru/bcode/451031>
8. Рассолов И. М. Информационное право. [Электронный ресурс]: Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 347 – Режим доступа: <https://urait.ru/bcode/449839>
9. Бачило И. Л. Информационное право. [Электронный ресурс]: Учебник для вузов. - Москва: Юрайт, 2020. - 419 – Режим доступа: <https://urait.ru/bcode/449666>
10. 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>
11. 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>
12. Полякова Т. А., Чубукова С. Г., Ниесов В. А. Организационное и правовое обеспечение информационной безопасности. [Электронный ресурс]: Учебник и практикум Для СПО. - Москва: Юрайт, 2020. - 325 – Режим доступа: <https://urait.ru/bcode/451933>

Дополнительная литература:

1. Куняев Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. [Электронный ресурс]: [монография]. - Москва: Логос, 2010. - 348 – Режим доступа: <https://znanium.com/catalog/product/469026>
2. Ефремов А. А. Защита государственного суверенитета РФ в информационном пространстве. [Электронный ресурс]: [монография]. - Москва: Норма, 2017. - 128 – Режим доступа: <https://znanium.com/catalog/product/929113>
3. 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>
4. Бачило И. Л. Информационное право.: учебник для магистров : учебник для студентов вузов, обучающихся по юридическим направлениям и специальностям. - Москва: Юрайт, 2015. - 564
5. Бирюков А. А. Информационная безопасность: защита и нападение.: производственно-практическое издание. - Москва: ДМК Пресс, 2017. - 433

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.

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.

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

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

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

GIMP. Лицензия GNU GENERAL PUBLIC LICENSE. Срок действия лицензии - без ограничения срока.

Inkscape. Лицензия GNU GENERAL PUBLIC LICENSE. Срок действия лицензии - без ограничения срока.

Autodesk 3D Studio MAX. Эл. лицензия для вуза. Срок действия лицензии - без ограничения срока.

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

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.

R Studio (среда для языка программирования R). Лицензия GNU Affero General Public License v3. Срок действия лицензии - без ограничения срока.

Язык программирования Python. Python Software Foundation License (PSFL). Срок действия лицензии - без ограничения срока.

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

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

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

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.