МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

26.12. 2019 г.

протокол № 4

Зав. кафедрой Гончаров Д.Ю.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

15 января 2020 г.

протокол № 5

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	2020

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

Екатеринбург
2020 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 по направлению подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (уровень бакалавриата) (приказ Минобрнауки России от
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 базовой 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	180	48	24	24	132	5

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

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

Общекультурные компетенции (ОК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	ИД-1.ОК-4 Знает необходимые для осуществления профессиональной деятельности правовые нормы, регулирующие экономические правоотношения. Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности с учетом полученных правовых знаний. Владеет навыками применения нормативно-правовой базы для решения экономических задач в области избранных видов профессиональной деятельности.

Общепрофессиональные компетенции (ОПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций

ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности	ИД-1.ОПК-5 Знает основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. Владеет навыками использования навыками использования нормативно-правовых актов в профессиональной деятельности.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
организационно-управленческая	
ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1.ПК-15 Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области. Уметь: пользоваться нормативными документами по защите информации; обеспечивать сохранность и неизменность обрабатываемой информации. Владеть навыками: защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
эксплуатационная	
ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ИД-1.ПК-5 Знать: организацию аттестации объектов по требованиям безопасности информации; способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов; виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия; инструментальные средства и системы программирования для решения профессиональных задач. Уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; проводить предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности; оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности. Владеть навыками: способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности

Шифр и наименование компетенции	Индикаторы достижения компетенций
профессионально-специализированная	
ПСК-1 способность решать задачи первичного финансового мониторинга в рамках функционирования служб внутреннего контроля субъектов финансового мониторинга	ИД-1.ПСК-1 Знать: сущность первичного финансового мониторинга; особенности функционирования служб внутреннего контроля; основные составляющие финансовой и налоговой отчетности; положения нормативно-правовых документов в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем. Уметь: анализировать финансовые операции (сделки) клиентов организации в деталях выявления их связи с ОД/ФТ, анализировать материалы финансовых расследований, схем отмывания преступных доходов в целях ПОД/ФТ; самостоятельно использовать теоретические знания методов первичного финансового мониторинга; применять на практике навыки по реализации системы внутреннего контроля и идентификации клиентов; выявлять операции, подлежащие обязательному контролю, а также операции, попадающие подкритерии и признаки необычных сделок. Владеть навыками: решения первичного финансового мониторинга; реализации политики финансового мониторинга в организациях, осуществляющих операции с денежными средствами или иным имуществом, системы внутреннего контроля в целях ПОД/ФТ; процедурами идентификации сомнительных сделок клиентов в процессе банковского обслуживания
ПСК-4 способность реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	ИД-1.ПСК-4 Знать: перечень и содержание мероприятий по защите информации в автоматизированных системах; особенности программно-аппаратных средств защиты информации; особенности защиты информации в автоматизированных системах финансовых и экономических структур; основные подходы к выбору мероприятий по защите информации в автоматизированных системах финансовых и экономических структур с помощью современных методов и средств Уметь: эффективно использовать современные программно-аппаратные средства защиты информации. обоснованно выбирать наиболее подходящие методы и средства защиты информации в автоматизированных системах финансовых и экономических структур; формулировать и реализовывать политику безопасности в системах финансовых и экономических структур. Владеть навыками: использования новых образцов программно-технических средств и информационных технологий, направленных на защиту информации в автоматизированных системах финансовых и экономических структур; методами и средствами выявления угроз безопасности автоматизированных систем; приемами и методами проведения мероприятий по защите информации в

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.	Организационные и правовые аспекты информационной безопасности	22	4		4	14	
Семестр 5		16					
Тема 2.	Правовые основы информационной безопасности	16	4		4	8	
Семестр 5		16					
Тема 3.	Теория организации доступа в информационных системах: организационно-правовой аспект	16	2		2	12	
Семестр 5		18					
Тема 4.	Правовые основы защиты от вредоносных программ	18	2		2	14	
Семестр 5		18					
Тема 5.	Понятие и правовые аспекты сетевой безопасности	18	2		2	14	
Семестр 5		18					
Тема 6.	Национальные интересы и информационная безопасность	18	2		2	14	
Семестр 5		4					
Тема 7.	Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации	4	2		2		
Семестр 5		18					
Тема 8.	Организационно-правовой механизм предотвращения угроз информационной безопасности	18	2		2	14	
Семестр 5		18					
Тема 9.	Организационно-правовые методы обеспечения информационной безопасности	18	2		2	14	
Семестр 5		32					
Тема 10.	Организационно-правовое обеспечение информационной безопасности	32	2		2	28	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Организационно-правовой механизм предотвращения угроз информационной безопасности РФ	Комплект заданий (Приложение 4)	Содержит вопросы, практические задачи, кейс-задания	Средство проверки умений применять полученные знания для решения задач определенного типа баллы

Организационно-правовое обеспечение информационной безопасности РФ в различных сферах общественной жизни	Комплект заданий (Приложение 4)	Содержит вопросы, практические задачи	Средство проверки умений применять полученные знания для решения задач определенного типа баллы
Правовые основы информационной безопасности	Комплект заданий (Приложение 4)	Содержит вопросы, практические задачи	Средство проверки умений применять полученные знания для решения задач определенного типа баллы
Промежуточный контроль (Приложение 5)			
5 семестр (За)	Зачет (Приложение 5)	Билет включает в себя 1 теоретический вопрос и 1 практикоориентированное задание	Ответ правильный, всесторонне и глубоко освещает предложенный вопрос, устанавливает взаимосвязь теории с практикой, показывает умение студента работать с литературой, делать выводы (правильный и полный ответ) – 85 -100 баллов. Ответ отвечает основным предъявляемым требованиям; студент обстоятельно владеет материалом, однако не на все вопросы дает глубокие, исчерпывающие и аргументированные ответы (точный, но неполный ответ) –

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

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

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

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

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

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

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

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

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

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

Средний уровень – 69% - 50% - удовлетворительно.

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

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Организационные и правовые аспекты информационной безопасности Тема 1. История и современные цели информационной безопасности. Три основных аспекта обеспечения информационной безопасности. Историю становления процесса защиты информации, его правовое регулирование. Организационно-правовые методы предупреждения угроз и предотвращения реализации угроз защиты информации. Классификация угроз информационной безопасности. Правовые угрозы информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 2. Правовые основы информационной безопасности Тема 2. Правовые основы информационной безопасности Месторасположения источника и уровня воздействия на информацию. Обзор общей ситуации в области правовой защиты информации. Нормативные акты, регулирующие защиту государственной и коммерческой тайны. Средства технической, организационной и правовой защиты информации. Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 3. Теория организации доступа в информационных системах: организационно-правовой аспект 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
Тема 4. Правовые основы защиты от вредоносных программ Тема 4. Правовые основы защиты от вредоносных программ Вредоносные программы и их примеры. Цели использования вредоносных программ. Внедрение и управление кодом информационной систем. Классификация нарушений конфиденциальности, целостность или доступность информации. Классификация вредоносных программ. Цели и сущность троянские программы. Нормативно-правовая база обеспечения информационной безопасности.
Тема 5. Понятие и правовые аспекты сетевой безопасности Тема 3. Понятие и правовые аспекты сетевой безопасности Классификация, цели и источники угроз информации, обрабатываемой в компьютерных сетях. Причины, вызывающие возможность реализации этих угроз на практике: организационно-правовой аспект. Нормативно-правовая база обеспечения информационной безопасности.
Тема 6. Национальные интересы и информационная безопасность 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 Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации 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. Нормативно-правовая база обеспечения информационной безопасности.

Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ. Понятие и виды угроз информационной безопасности РФ. Виды и сущность угроз информационной безопасности. Понятие и виды источников угроз информационной безопасности РФ. Виды и сущность источников угроз информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 9. Организационно-правовые методы обеспечения информационной безопасности Тема 9. Организационно-правовые методы обеспечения информационной безопасности РФ Общая характеристика и правовые методы обеспечения информационной безопасности РФ. Совокупность методов обеспечения интересов РФ в информационной сфере. Классификация методов обеспечения информационной безопасности. Характеристика организационно-технических и экономических методов обеспечения информационной безопасности РФ. Нормативно-правовая база обеспечения информационной безопасности.
Тема 10. Организационно-правовое обеспечение информационной безопасности Тема 10. Организационно-правовое обеспечение информационной безопасности РФ в различных сферах общественной жизни. Информационная безопасность Российской Федерации как составляющая часть национальной и государственной безопасности России. Организационно-правовые особенности обеспечения информационной безопасности РФ в экономической сфере. Меры по обеспечению информационной безопасности РФ в сфере экономики. Нормативно-правовая база обеспечения информационной безопасности.

7.2 Содержание практических занятий и лабораторных работ

Тема 1. Организационные и правовые аспекты информационной безопасности Тема 1. История и современные цели информационной безопасности. Три основных аспекта обеспечения информационной безопасности. Историю становления процесса защиты информации, его правовое регулирование. Организационно-правовые методы предупреждения угроз и предотвращения реализации угроз защиты информации. Классификация угроз информационной безопасности. Правовые угрозы информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 2. Правовые основы информационной безопасности Тема 2. Правовые основы информационной безопасности Месторасположения источника и уровня воздействия на информацию. Обзор общей ситуации в области правовой защиты информации. Нормативные акты, регулирующие защиту государственной и коммерческой тайны. Средства технической, организационной и правовой защиты информации. Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 3. Теория организации доступа в информационных системах: организационно-правовой аспект 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
Тема 4. Правовые основы защиты от вредоносных программ Тема 4. Правовые основы защиты от вредоносных программ Вредоносные программы и их примеры. Цели использования вредоносных программ. Внедрение и управление кодом информационной систем. Классификация нарушений конфиденциальности, целостность или доступность информации. Классификация вредоносных программ. Цели и сущность троянские программы. Нормативно-правовая база обеспечения информационной безопасности.

Тема 5. Понятие и правовые аспекты сетевой безопасности Тема 3. Понятие и правовые аспекты сетевой безопасности Классификация, цели и источники угроз информации, обрабатываемой в компьютерных сетях. Причины, вызывающие возможность реализации этих угроз на практике: организационно-правовой аспект. Нормативно-правовая база обеспечения информационной безопасности.
Тема 6. Национальные интересы и информационная безопасность 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 Тема 7. Организационно-правовая основа системы обеспечения информационной безопасности Российской Федерации 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. Нормативно-правовая база обеспечения информационной безопасности.
Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ. Понятие и виды угроз информационной безопасности РФ. Виды и сущность угроз информационной безопасности. Понятие и виды источников угроз информационной безопасности РФ. Виды и сущность источников угроз информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 9. Организационно-правовые методы обеспечения информационной безопасности Тема 9. Организационно-правовые методы обеспечения информационной безопасности РФ Общая характеристика и правовые методы обеспечения информационной безопасности РФ. Совокупность методов обеспечения интересов РФ в информационной сфере. Классификация методов обеспечения информационной безопасности. Характеристика организационно-технических и экономических методов обеспечения информационной безопасности РФ. Нормативно-правовая база обеспечения информационной безопасности.
Тема 10. Организационно-правовое обеспечение информационной безопасности Тема 10. Организационно-правовое обеспечение информационной безопасности РФ в различных сферах общественной жизни. Информационная безопасность Российской Федерации как составляющая часть национальной и государственной безопасности России. Организационно-правовые особенности обеспечения информационной безопасности РФ в экономической сфере. Меры по обеспечению информационной безопасности РФ в сфере экономики. Нормативно-правовая база обеспечения информационной безопасности.

7.3. Содержание самостоятельной работы

Тема 1. Организационные и правовые аспекты информационной безопасности Тема 1. История и современные цели информационной безопасности. Три основных аспекта обеспечения информационной безопасности. Историю становления процесса защиты информации, его правовое регулирование. Организационно-правовые методы предупреждения угроз и предотвращения реализации угроз защиты информации. Классификация угроз информационной безопасности. Правовые угрозы информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.

Тема 2. Правовые основы информационной безопасности Тема 2. Правовые основы информационной безопасности Месторасположения источника и уровня воздействия на информацию. Обзор общей ситуации в области правовой защиты информации. Нормативные акты, регулирующие защиту государственной и коммерческой тайны. Средства технической, организационной и правовой защиты информации. Уголовная, административная и гражданско-правовая ответственность за нарушения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 3. Теория организации доступа в информационных системах: организационно-правовой аспект 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
Тема 4. Правовые основы защиты от вредоносных программ Тема 4. Правовые основы защиты от вредоносных программ Вредоносные программы и их примеры. Цели использования вредоносных программ. Внедрение и управление кодом информационной систем. Классификация нарушений конфиденциальности, целостность или доступность информации. Классификация вредоносных программ. Цели и сущность троянские программы. Нормативно-правовая база обеспечения информационной безопасности.
Тема 5. Понятие и правовые аспекты сетевой безопасности Тема 3. Понятие и правовые аспекты сетевой безопасности Классификация, цели и источники угроз информации, обрабатываемой в компьютерных сетях. Причины, вызывающие возможность реализации этих угроз на практике: организационно-правовой аспект. Нормативно-правовая база обеспечения информационной безопасности.
Тема 6. Национальные интересы и информационная безопасность 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 8. Организационно-правовой механизм предотвращения угроз информационной безопасности Тема 8. Организационно-правовой механизм предотвращения угроз информационной безопасности РФ. Понятие и виды угроз информационной безопасности РФ. Виды и сущность угроз информационной безопасности. Понятие и виды источников угроз информационной безопасности РФ. Виды и сущность источников угроз информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности.
Тема 9. Организационно-правовые методы обеспечения информационной безопасности Тема 9. Организационно-правовые методы обеспечения информационной безопасности РФ Общая характеристика и правовые методы обеспечения информационной безопасности РФ. Совокупность методов обеспечения интересов РФ в информационной сфере. Классификация методов обеспечения информационной безопасности. Характеристика организационно-технических и экономических методов обеспечения информационной безопасности РФ. Нормативно-правовая база обеспечения информационной безопасности.

Тема 10. Организационно-правовое обеспечение информационной безопасности
Тема 10. Организационно-правовое обеспечение информационной безопасности РФ в различных сферах общественной жизни.
Информационная безопасность Российской Федерации как составляющая часть национальной и государственной безопасности России. Организационно-правовые особенности обеспечения информационной безопасности РФ в экономической сфере. Меры по обеспечению информационной безопасности РФ в сфере экономики. Нормативно-правовая база обеспечения информационной безопасности.

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. Баранова Е.К., Бабаш А.В.. Основы информационной безопасности:Учебник. - Москва: Издательский Центр РИОР, 2019. - 202 с.

1. Бабаш А. В., Баранова Е. К., Ларин Д. А.. Информационная безопасность. История специальных методов криптографической деятельности:учебное пособие. - Москва: РИОР: ИНФРА- М, 2019. - 236 с.

1. Глинская Е. В., Чичварин Н. В.. Информационная безопасность конструкций ЭВМ и систем:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 09.03.03 «Прикладная информатика» и 10.04.01 «Информационная безопасность» (квалификация (степень) «бакалавр»). - Москва: ИНФРА-М, 2016. - 118 с.

1. Баранова Е.К., Бабаш А.В.. Основы информационной безопасностиv922:. - Москва: Издательский Центр РИОР, 2019. - 202 с.

1. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А.. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:Учебник и практикум. - Москва: Издательство Юрайт, 2019. - 325 – Режим доступа: https://www.biblio-online.ru/bcode/432966

2. Партыка Т. Л., Попов И. И.. Информационная безопасность:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники. - Москва: Форум: ИНФРА-М, 2019. - 432 с.

3. Глинская Е.В., Чичварин Н.В.. Информационная безопасность конструкций ЭВМ и систем:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 09.03.03 "Прикладная информатика" и 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2019. - 118 с.

4. Баранова Е. К., Бабаш А. В.. Информационная безопасность и защита информации:учебное пособие для студентов, обучающихся по направлению "Прикладная информатика". - Москва: РИОР: ИНФРА-М, 2019. - 336 с.

5. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 09.00.00 «Информатика и вычислительная техника». - Москва: ФОРУМ: ИНФРА-М, 2019. - 416 с.

6. Нестеров С. А.. Информационная безопасность [Электронный ресурс]:Учебник и практикум. - Москва: Издательство Юрайт, 2019. - 321 – Режим доступа: https://www.biblio-online.ru/bcode/442312

7. Нестеров С. А.. Информационная безопасность [Электронный ресурс]:Учебник и практикум. - Москва: Издательство Юрайт, 2019. - 321 – Режим доступа: https://www.biblio-online.ru/bcode/434171

8. Казарин О. В., Шубинский И. Б.. Основы информационной безопасности: надежность и безопасность программного обеспечения [Электронный ресурс]:Учебное пособие. - Москва: Издательство Юрайт, 2019. - 342 – Режим доступа: https://www.biblio-online.ru/bcode/431080

9. Внуков А. А.. Основы информационной безопасности: защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательство Юрайт, 2019. - 240 – Режим доступа: https://www.biblio-online.ru/bcode/431332

Дополнительная литература:

1. Башлы П. Н., Бабаш А. В., Баранова Е. К.. Информационная безопасность и защита информации:учебник. - Москва: РИОР, 2013. - 222 с.

2. Гришина Н. В.. Информационная безопасность предприятия:учебное пособие для студентов вузов, обучающихся по направлению подготовки 090900.62 "Информационная безопасность". - Москва: ФОРУМ: ИНФРА-М, 2015. - 240 с.

3. Гришина Н. В.. Информационная безопасность предприятия:учебное пособие для студентов вузов, обучающихся по направлению подготовки 090900.62 "Информ. безопасность". - Москва: ФОРУМ: ИНФРА-М, 2016. - 240 с.

4. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 09.00.00 "Информатика и вычислительная техника". - Москва: ФОРУМ: ИНФРА-М, 2017. - 416 с.

5. Гришина Н. В.. Информационная безопасность предприятия:учебное пособие для студентов вузов, обучающихся по направлению подготовки 10.03.01 "Иинформационная безопасность" (квалификация (степень) «бакалавр»). - Москва: ФОРУМ: ИНФРА, 2017. - 239 с.

6. Партыка Т. Л., Попов И. И.. Информационная безопасность:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники. - Москва: ФОРУМ: ИНФРА-М, 2018. - 432 с.

7. Баранова Е.К., Бабаш А.В.. Информационная безопасность и защита информации:учебное пособие для студентов, обучающихся по направлению «Прикладная информатика". - Москва: РИОР: ИНФРА-М, 2018. - 336 с.

11. Глинская Е.В., Чичварин Н.В.. Информационная безопасность конструкций ЭВМ и систем:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 09.03.03 "Прикладная информатика" и 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2019. - 118 с.

12. Баранова Е. К., Бабаш А. В.. Информационная безопасность и защита информации:учебное пособие для студентов, обучающихся по направлению "Прикладная информатика". - Москва: РИОР: ИНФРА-М, 2019. - 336 с.

13. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 09.00.00 «Информатика и вычислительная техника». - Москва: ФОРУМ: ИНФРА-М, 2019. - 416 с.

15. Сычев Ю.Н.. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2019. - 223 с. – Режим доступа: https://new.znanium.com/catalog/product/979415

16. Баранова Е.К., Бабаш А.В.. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2019. - 236 с. – Режим доступа: https://new.znanium.com/catalog/product/987215

17. Баранова Е.К., Бабаш А.В.. Основы информационной безопасности [Электронный ресурс]:Учебник. - Москва: Издательский Центр РИОР, 2019. - 202 с. – Режим доступа: https://new.znanium.com/catalog/product/1014830

18. Баранова Е.К., Бабаш А.В.. Основы информационной безопасности [Электронный ресурс]:Учебник. - Москва: Издательский Центр РИО, 2019. - 202 с. – Режим доступа: http://znanium.com/go.php?id=1014830znanium.com

19. Гришина Н. В.. Основы информационной безопасности предприятия [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2019. - 216 с. – Режим доступа: https://new.znanium.com/catalog/product/1017663

20. Глинская Е. В., Чичварин Н. В.. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 09.03.03 «Прикладная информатика» и 10.04.01 «Информационная безопасность» (квалификация (степень) «бакалавр»). - Москва: ИНФРА-М, 2016. - 118 с. – Режим доступа: http://znanium.com/go.php?id=507334

21. Баранова Е.К., Бабаш А.В.. Основы информационной безопасности [Электронный ресурс]:Учебник. - Москва: Издательский Центр РИО, 2019. - 202 с. – Режим доступа: http://znanium.com/go.php?id=1014830znanium.com

22. Глинская Е.В., Чичварин Н.В.. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 09.03.03 "Прикладная информатика" и 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2019. - 118 с. – Режим доступа: http://znanium.com/go.php?id=991792

23. Баранова Е. К., Бабаш А. В.. Информационная безопасность и защита информации [Электронный ресурс]:учебное пособие для студентов, обучающихся по направлению "Прикладная информатика". - Москва: РИОР: ИНФРА-М, 2019. - 336 с. – Режим доступа: http://znanium.com/go.php?id=1009606

24. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 09.00.00 «Информатика и вычислительная техника». - Москва: ФОРУМ: ИНФРА-М, 2019. - 416 с. – Режим доступа: http://znanium.com/go.php?id=1009605

25. Баранова Е.К., Бабаш А.В.. Основы информационной безопасности [Электронный ресурс]:учебник. - Москва: РИОР: ИНФРА-М, 2019. - 202 с. – Режим доступа: http://znanium.com/go.php?id=1014830znanium.com

26. Сычев Ю. Н.. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]:учебное пособия для студентов вузов, обучающихся по укрупненной группе специальностей и направлений 10.03.00 «Информационная безопасность». - Москва: ИНФРА-М, 2019. - 223 с. – Режим доступа: http://znanium.com/go.php?id=979415znanium.com

27. Чусавитина Г. Н., Курзаева Л.В.. Подготовка будущих учителей к обеспечению информационной безопасности [Электронный ресурс]:Монография. - Москва: Издательство "Флинта", 2019. - 188 с. – Режим доступа: https://new.znanium.com/catalog/product/1065529

28. Чусавитина Г. Н., Давлеткиреева Л.З.. Информационная безопасность и вопросы профилактики кибер-экстремизма среди молодежи [Электронный ресурс]:Сборник научных трудов. - Москва: Издательство "Флинта", 2019. - 161 с. – Режим доступа: https://new.znanium.com/catalog/product/1065527

29. Брюхомицкий Ю.А.. Искусственные иммунные системы в информационной безопасности [Электронный ресурс]:ВО - Специалитет. - Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2019. - 147 с. – Режим доступа: https://new.znanium.com/catalog/product/1088177

30. Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А., Полякова Т. А., Стрельцов А. А.. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник и практикум для бакалавриата и магистратуры. - Москва: Юрайт, 2019. - 325 с. – Режим доступа: https://www.biblio-online.ru/bcode/432966

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

Перечень лицензионное программное обеспечение:

Microsoft Windows 10 .Акт предоставления прав № Tr060590 от 19.09.2017. Срок действия лицензии 30.09.2020.

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

Microsoft Office 2016. Акт предоставления прав № Tr060590 от 19.09.2017. Срок действия лицензии 30.09.2020.

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

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

Corel Painter 2017. Акт предоставления прав № Tr025968 от 26.04.2017, Лицензия № 175844. Срок действия лицензии 27.02.2022.

Corel PaintShop Pro X9. Акт предоставления прав № Tr025968 от 26.04.2017, Лицензия № 175844. Срок действия лицензии 27.02.2022.

Adobe Acrobat DC Pro. Договор № 180-С-2019 от 17.12.2019. Срок действия лицензии 13.12.2020.

Adobe Lightroom CC. Договор № 180-С-2019 от 17.12.2019. Срок действия лицензии 13.12.2020.

Adobe After Effects CC. Договор № 180-С-2019 от 17.12.2019. Срок действия лицензии 13.12.2020.

Adobe InCopy CC. Договор № 180-С-2019 от 17.12.2019. Срок действия лицензии

Adobe Illustrator CC. Договор № 180-С-2019 от 17.12.2019. Срок действия лицензии 13.12.2020.

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

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

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

Graphisoft ArchiCad. Эл. лицензия для вуза. Срок действия лицензии 11.08.2019.

Конфигурация 1С: Бухгалтерия государственного учреждения. 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).

Конфигурация 1С: Зарплата и кадры бюджетного учреждения. 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).

Embarcadero RAD Studio. Эл. лицензия, Информационное письмо. Срок действия лицензии 05.05.2020.

ГИС MapInfo Professional. Лицензионный договор № 79/2016-У от 7 сентября 2016, Акт № 215 от 22 сентября 2016.

Maple 11. Договор № 67Т от 04.07.2007 г..

Crystal Reports XI Professional. Договор № 67Т от 04.07.2007 г..

IBM SPSS Statistics Base Edition Edition Campus Value Unit Term License Subscription and Support 12 Month. Договор №33-ПО.2019 от 26.03.2019 г., Акт №Sk000236 от 02.04.2019. Срок действия 02.04.2020.

Microsoft Dynamics CRM. Соглашение от 23.08.2016.

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

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без органичения 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 № 194-У-2019 от 09.01.2020. Срок действия лицензии до 31.12.2020

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.