МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

02.12.2025 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная безопасность
Специальность	38.05.01 Экономическая безопасность
Специализация	Экономическая безопасность
Форма обучения	очная
Год набора	2026

Разработана:
Ассистент
Голубин А.В.

Профессор, д.э.н.
Назаров Д.М.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

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

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - специалитет по специальности 38.05.01 Экономическая безопасность (приказ Минобрнауки России от 14.04.2021 г. № 293)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование у студентов теоретических и практических знаний в области информационной безопасности, принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 6						
Зачет с оценкой	144	64	32	32	53	4

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

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

Шифр и наименование компетенции	Индикаторы достижения компетенций
информационно-аналитический	

ПК-1 Раскрытие информации о рисках организации, в т.ч. кредитной организации, в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или принимаемыми стратегическими решениями	ИД-1.ПК-1 Знать: Законодательство Российской Федерации по виду деятельности организации и требования (рекомендации) области управления рисками; Международные и российские стандарты по риск-менеджменту и риск -ориентированному управлению организацией; Перечень заинтересованных сторон; Организацию внешней и внутренней отчетности организации, бизнес-подразделений; Состав, форму и порядок формирования отчетности с учетом рисков; Подходы к коммуникации и доведению информации до исполнительных органов и совета директоров; Нормы профессиональной этики; Иностранный язык в объеме, необходимом для выполнения трудовой функции; Защиту персональных данных; Основы работы в операционных системах; Принципы соблюдения информационной безопасности, сохранения конфиденциальности данных.
	ИД-2.ПК-1 Уметь: Определять заинтересованные стороны в реализации риск-ориентированного управления в организации на уровне акционеров, совета директоров, партнеров, руководства организации; Организовывать работы по раскрытию информации о рисках в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или с принима-емыми стратегическими решениями; Выстраивать коммуникации с заинтересованными сторонами; Создавать и воспроизводить видеоролики, презентации, слайд-шоу, медиафайлы и итоговую продукцию из исходных аудиокомпонентов, визуальных и мультимедийных компонентов; Применять подходы безопасной работы в информационно-телекоммуникационной сети "Ин-тернет" (защита персональных данных, антивирусная защита, информационная гигиена); Управлять размещением цифровой информации, в том числе в дисковых хранилищах локаль-ной и глобальной компьютерной сети; Формировать медиатеки для структурированного хранения и каталогизации цифровой ин-формации.
	ИД-3.ПК-1 Иметь практический опыт: Определения заинтересованных сторон на уровне акционеров, совета директоров, партнеров, руководства организации для раскрытия информации о рисках; Организации работы по раскрытию информации о рисках в отчетах для внешних сторон, свя-занных с требованиями регуляторов и достижением стратегических целей или с принимае-мыми стратегическими решениями; Создания каналов коммуникации для передачи и эскалации информации в области управле-ния рисками с акционерами, советом директоров, партнерами, руководством организации.

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов

	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 6		117					
Тема 1.	Информационная безопасность: законодательные и нормативно-правовые основы. Виды информационных ресурсов по категориям доступа (ПК-1)	7	3			4	
Тема 2.	Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации (ПК-1)	12	3		6	3	
Тема 3.	Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации (ПК-1)	6	3			3	
Тема 4.	Защита информации от утечки по техническим каналам (ПК-1)	6	3			3	
Тема 5.	Защита информации в компьютерных системах (ПК-1)	42	8		14	20	
Тема 6.	Криптографические методы защиты (ПК-1)	30	4		6	20	
Тема 7.	Вопросы управления ИБ (ПК-1)	14	8		6		

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1. Информационная безопасность: законодательные и нормативно-правовые основы. Виды информационных ресурсов по категориям доступа	Контрольная работа №1 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

Тема 2. Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации	Тест (Приложение 4)	10 вопросов. Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Оценивается знание изученного материала. <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации	Контрольная работа №2 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации. <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 4. Защита информации от утечки по техническим каналам	Контрольная работа №3 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации. <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

Тема 5. Защите информации в компьютерных системах	Контрольная работа №4 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации. <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 6. Криптографические методы защиты	Контрольная работа №5 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации. <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Промежуточная аттестация (Приложение 5)			
6 семестр (ЗаО)	Билет к зачету с оценкой	в билете 2 теоретических вопроса и 1 практический	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации. <30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

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

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

Текущий контроль. 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. Информационная безопасность: законодательные и нормативно-правовые основы. Виды информационных ресурсов по категориям доступа (ПК-1)
Введение: предмет, содержание и задачи дисциплины, ее место среди других дисциплин учебного плана, формы отчетности, основная и дополнительная литература.
Место информационной безопасности в общей системе безопасности государства. Концепция информационной безопасности. Структура и основные положения нормативных правовых актов в области информационной безопасности. Государственные стандарты, используемые в области информационной безопасности.

Тема 2. Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации (ПК-1)
Понятие государственной системы защиты информации. Принципы функционирования государственной системы защиты информации. Правовые основы деятельности государственной системы защиты информации. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Цели и задачи государственной системы защиты информации. Организационная и функциональная структура государственной системы защиты информации. Стандартизация в области обеспечения информационной безопасности. Пользование стандартами информационной безопасности.
Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима. Регламентация доступа персонала к информационным и вычислительным ресурсам. Организация работы с конфиденциальными документами. Требования и рекомендации по защите конфиденциальной информации. Учет, хранение, использование и уничтожение документов (носителей) с конфиденциальной информацией. Организация контроля за соблюдением исполнителями должностных инструкций. Правовое регулирование в сфере информационных отношений. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности. Пользование стандартами информационной безопасности. Международные и отечественные нормативные и руководящие документы, связанные с информационной безопасностью. Руководящие документы Гостехкомиссии РФ.

Тема 3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации (ПК-1)
Система лицензирования на право проведения работ и оказания услуг в области защиты информации с ограниченным доступом. Нормативные документы, определяющие порядок лицензирования в области защиты конфиденциальной информации. Условия лицензирования деятельности по защите конфиденциальной информации. Общие принципы лицензирования в области защиты конфиденциальной информации. Лицензионные требования для получения лицензии на деятельность в области технической защиты конфиденциальной информации. Перечень документов, представляемых для получения лицензий в области защиты конфиденциальной информации. Система сертификации средств защиты информации. Структура средств защиты информации, подлежащих сертификации. Аттестация объектов информатизации на соответствие требованиям безопасности информации. Объекты, подлежащие аттестации. Перечень основных нормативных документов, определяющих порядок и объём аттестационных испытаний объектов информатизации. Общие требования по аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации. Порядок проведения аттестации объектов информатизации.

Тема 4. Защита информации от утечки по техническим каналам (ПК-1)
Общая характеристика и классификация технических каналов утечки информации (ТКУИ). Элементарная модель канала утечки информации. Основные и вспомогательные технические средства и системы. Контролируемая зона. Основные виды ТКУИ. Технические каналы утечки информации обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ): электромагнитные; электрические; параметрические. Технические каналы утечки акустической (речевой) информации: воздушные; вибрационные; акустоэлектрические; параметрические; оптико-электронный (лазерный). Технические каналы перехвата информации при ее передаче по каналам связи. Технические каналы утечки видовой информации.
Инженерно-технические средства и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект. Основные виды технических каналов и источников утечки информации. Противодействие наблюдению в оптическом диапазоне. Защита от прослушивания акустических сигналов. Средства борьбы с закладными подслушивающими устройствами. Защита речевой информации, передаваемой по каналам связи. Пассивные и активные методы защиты информации от утечки в результате электромагнитных излучений и наводок.
Комплексное обеспечение защиты информации от утечки по техническим каналам. Методика принятия решения на защиту от утечки информации в организации. Возможные виды квалификации злоумышленников. Оценка возможностей вероятных злоумышленников. Оценка своей организации как возможного источника информации для злоумышленников. Порядок организации защиты информации на этапе определения задач защиты. Порядок выбора целесообразных мер и средств защиты. Критерии оценки уровня защиты. Организационные способы защиты.

Тема 5. Защита информации в компьютерных системах (ПК-1)
Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Угрозы безопасности в компьютерных системах. Классификация способов несанкционированного доступа к информации в компьютерных системах. Модель поведения потенциального нарушителя. Алгоритм подготовки и реализации атаки нарушителем. Атака на политику безопасности. Атака на сменные элементы системы безопасности. Атака на протоколы информационного взаимодействия. Анализ способов нарушений информационной безопасности.
Противодействие несанкционированного доступа к информации в компьютерных системах. Требования к системе защиты информации. Принципы и правила организации защиты информации от несанкционированного доступа к информации в компьютерных системах. Этапы развития систем информационной безопасности. Средства защита информации в компьютерных системах. Система защиты информации на базе программно-аппаратного комплекса. Подсистемы защиты информации. Состав типового комплекса защиты от несанкционированного доступа к информации. Механизмы работы комплекса защиты от несанкционированного доступа к информации.
Многоуровневая модель защиты объектов информатизации. Способы защиты информации от утечки за счет ПЭМИН. Активные устройства защиты от утечки по каналам ПЭМИН.
Международные стандарты информационного обмена. Аппаратно-технические средства для организации технической защиты в сфере международного информационного обмена. Технологии защиты информации. Аппаратные межсетевые экраны. Рекомендации Microsoft по безопасному подключению почтового сервера к интернет. Безопасность браузеров. Схема подключения брандмауэров или файлволлов или межсетевого экрана. Брандмауэр Agnitum Outpost Firewall Pro. Защита локальный вычислительных сетей брандмауэром с одним сетевым интерфейсом. Средства защиты информации eToken, Symantec Antivirus for Ms Exchange, Symantec Antivirus client. Электронная цифровая подпись, порядок функционирования. Гипотетическая (гетерогенная) вычислительная сеть. Комплексный план технической защиты информации. Алгоритм создания системы информационной безопасности. Совершенствование организационных мероприятий, меры противодействия взлому защиты. Логическая архитектура информационно-вычислительного комплекса.
Защита информации в компьютерных системах от случайных угроз. Создание и управление учетными записями пользователей. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. Аудит ресурсов и событий системы защиты. Настройка системных параметров безопасности. Настройка параметров безопасности подключения к Интернет. Повышение безопасности информации встроенными средствами. Шифрования операционной системы. Архивация и восстановление данных.
Понятия о видах вирусов. Классификация вирусов: по среде обитания; по способу заражения; по степени опасности деструктированных воздействий; по алгоритму функционирования. Механизм работы вирусов. Способы внедрения потенциально опасных программ. Методы обнаружения вирусов: сканирование; обнаружение изменений; эвристический анализ; использование резидентных сторожей; вакцинирование программ; аппаратно-программная защита. Антивирусные программы: Norton AntiVirus; McAfee; Dr. Web; Kaspersky Anti-Virus; Антивирус Касперского OEM. Профилактика заражения вирусами компьютерных систем. Сущность комплексного подхода к безопасности информации в компьютерных системах.

Тема 6. Криптографические методы защиты (ПК-1)
Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования. Ключи и алгоритмы шифрования. Методы шифрования с симметричным ключом. Методы замены (подстановки) и перестановки. Гаммирование. Шифрование, использующее генераторы (датчики) псевдослучайных последовательностей. Системы блочного шифрования на основе отечественного ГОСТа и стандарта DES (США). Системы несимметричного шифрования: с открытым ключом для шифрования и закрытым - для дешифрования. Односторонние функции. Криптографическая система RSA. Электронная цифровая подпись на основе криптографического преобразования. Особенности стандартизации и сертификации криптографических средств.

Тема 7. Вопросы управления ИБ (ПК-1) Вопросы управления ИБ

7.2 Содержание практических занятий и лабораторных работ

Тема 5. Защита информации в компьютерных системах (ПК-1) Противодействие несанкционированного доступа к информации в компьютерных системах. Требования к системе защиты информации. Принципы и правила организации защиты информации от несанкционированного доступа к информации в компьютерных системах. Этапы развития систем информационной безопасности. Средства защита информации в компьютерных системах. Система защиты информации на базе программно-аппаратного комплекса. Подсистемы защиты информации. Состав типового комплекса защиты от несанкционированного доступа к информации. Механизмы работы комплекса защиты от несанкционированного доступа к информации.
Тема 6. Криптографические методы защиты (ПК-1) Проверка криптостойкости шифров
Тема 7. Вопросы управления ИБ (ПК-1) Изучение современных подходов к обеспечению безопасности коммерческой информации.

7.3. Содержание самостоятельной работы

Тема 2. Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации (ПК-1) Тест
Тема 3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации (ПК-1) Тест
Тема 4. Защита информации от утечки по техническим каналам (ПК-1) Тест
Тема 5. Защита информации в компьютерных системах (ПК-1) контрольные работы
Тема 6. Криптографические методы защиты (ПК-1) Контрольная работа

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 предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
Материалы 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:

2. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2025. - 355 – Режим доступа: https://znanium.com/catalog/product/2173934

3. Фомичёв В. М., Мельников Д. А. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 209 – Режим доступа: https://urait.ru/bcode/560804

4. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 349 – Режим доступа: https://urait.ru/bcode/561077

5. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 357 – Режим доступа: https://urait.ru/bcode/560516

6. Внуков А. А. Защита информации [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 161 – Режим доступа: https://urait.ru/bcode/561313

7. Гришина Н. В. Основы информационной безопасности предприятия [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2025. - 216 – Режим доступа: https://znanium.com/catalog/product/2206781

8. Овчинский В.С. Криминология цифрового мира [Электронный ресурс]:Учебник. - Москва: ООО "Юридическое издательство Норма", 2026. - 352 – Режим доступа: https://znanium.com/catalog/product/2232927

Дополнительная литература:

2. Сотов А. И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации:монография. - Москва: РУСАЙНС, 2024. - 126, [1]

3. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024. - 357 – Режим доступа: https://urait.ru/bcode/555950

4. Райтман М. Информационная безопасность для пользователя. Правила самозащиты в Интернете:производственно-практическое издание. - Санкт-Петербург: БХВ-Петербург, 2023. - 400

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 -Без ограничения срока.

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

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

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. 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 № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

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.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену

К зачету с оценкой

1. Понятие информационных угроз.
2. Информационные войны.
3. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ.
4. Виды противников. Хакеры.
5. Компьютерные вирусы. История. Определение по УК РФ.
6. Виды, принципы действия вирусов, демаскирующие признаки.
7. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
8. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор.
9. Угрозы компьютерной информации, реализуемые на аппаратном уровне.
10. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей.
11. Правовое урегулирование защиты информации.
12. Роль, задачи и обязанности администратора безопасности КС.
13. Защита данных криптографическими методами. Методы шифрования.
14. Защита данных криптографическими методами. Алгоритмы шифрования.
15. Требования к шифрам. Сравнение DES и ГОСТ 28147-89
16. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.
17. Политика безопасности и ее составляющие.
18. Модели защиты информации в КС.
19. Технологии защиты и разграничения доступа.
20. Стандарты ИБ.

Приложение 2
к рабочей программе

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

ПК-1 Раскрытие информации о рисках организации, в т.ч. кредитной организации, в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или принимаемыми стратегическими решениями

Знать: законодательство Российской Федерации по виду деятельности организации и требования (рекомендации) области управления рисками; международные и российские стандарты по риск-менеджменту и риск-ориентированному управлению организацией; перечень заинтересованных сторон; организацию внешней и внутренней отчетности организации, бизнес-подразделений; состав, форму и порядок формирования отчетности с учетом рисков; подходы к коммуникации и доведению информации до исполнительных органов и совета директоров; нормы профессиональной этики; иностранный язык в объеме, необходимом для выполнения трудовой функции; защиту персональных данных; основы работы в операционных системах; принципы соблюдения информационной безопасности, сохранения конфиденциальности данных.

Уметь: определять заинтересованные стороны в реализации риск-ориентированного управления в организации на уровне акционеров, совета директоров, партнеров, руководства организации; организовывать работы по раскрытию информации о рисках в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или с принима-емыми стратегическими решениями; выстраивать коммуникации с заинтересованными сторонами; создавать и воспроизводить видеоролики, презентации, слайд-шоу, медиафайлы и итоговую продукцию из исходных аудиокомпонентов, визуальных и мультимедийных компонентов; применять подходы безопасной работы в информационно-телекоммуникационной сети "Ин-тернет" (защита персональных данных, антивирусная защита, информационная гигиена); управлять размещением цифровой информации, в том числе в дисковых хранилищах локаль-ной и глобальной компьютерной сети; формировать медиатеки для структурированного хранения и каталогизации цифровой ин-формации.

Иметь практический опыт: определения заинтересованных сторон на уровне акционеров, совета директоров, партнеров, руководства организации для раскрытия информации о рисках; организации работы по раскрытию информации о рисках в отчетах для внешних сторон, свя-занных с требованиями регуляторов и достижением стратегических целей или с принимае-мыми стратегическими решениями; создания

каналов коммуникации для передачи и эскалации информации в области управле-ния рисками с акционерами, советом директоров, партнерами, руководством организации.

Задания закрытого типа

1. Какой тип кибератаки использует социальную инженерию, для того, чтобы обмануть людей? (**ПК-1**)

a) DDoS

b) Фишинг

c) SQL-инъекция

d) Кросс-сайтовый скриптинг

2. Какое программное обеспечение используется для обнаружения и устранения вредоносных программ? (**ПК-1**)

a) Фаервол

b) Антивирус

c) Интранет

d) VPN

3. Какой нормативный акт определяет общие принципы организации информационной безопасности в организациях и органах государственной власти Российской Федерации? (**ПК-1**)

a) Федеральный закон "Об информации, информационных технологиях и о защите информации"

b) Федеральный закон "Об информационной безопасности"

c) Постановление Правительства Российской Федерации "Об утверждении правил защиты конфиденциальной информации"

d) Приказ Министерства связи и массовых коммуникаций Российской Федерации "Об утверждении требований к защите персональных данных"

4. Какой документ определяет требования к методам и средствам защиты информации от несанкционированного доступа, утечки и искажения? (**ПК-1**)

a) ГОСТ Р ИСО/МЭК 27001-2013 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

b) ГОСТ Р 52854-2007 "Защита информации. Термины и определения"

c) Руководство по защите информации в государственных органах Российской Федерации

d) Методические рекомендации по организации системы защиты информации в банковской сфере

5. Какой документ содержит требования к организации процесса управления информационной безопасностью и управлению рисками? (**ПК-1**)

a) ГОСТ Р 52854-2007 "Защита информации. Термины и определения"

b) Постановление Правительства Российской Федерации "Об утверждении правил защиты конфиденциальной информации"

c) Руководство по защите информации в государственных органах Российской Федерации

d) Методические рекомендации по организации системы защиты информации в банковской сфере

6. Какой документ содержит перечень мер по защите информации на предприятии? (**ПК-1**)

a) Федеральный закон "Об информации, информационных технологиях и о защите информации"

b) Приказ Министерства связи и массовых коммуникаций Российской Федерации "Об утверждении требований к защите персональных данных"

c) Руководство по защите информации в государственных органах Российской Федерации

d) Методические рекомендации по защите информации на предприятии

7. Какой документ содержит требования к защите персональных данных в информационных системах? (**ПК-1**)

a) Федеральный закон "Об информации, информационных технологиях и о защите информации"

b) Постановление Правительства Российской Федерации "Об утверждении правил защиты конфиденциальной информации"

c) Приказ Министерства связи и массовых коммуникаций Российской Федерации "Об утверждении требований к защите персональных данных"

d) Руководство по защите информации в государственных органах Российской Федерации

8. Какой тип шифрования является наиболее безопасным? (**ПК-1**)

a) DES

b) AES

c) RC4

d) MD5

9. Какой тип угрозы безопасности данных может привести к потере данных, если вы не сделаете резервную копию? (**ПК-1**)

a) Хакерские атаки

b) Вирусы

c) Кража личной информации

d) Ошибка пользователя

10. Что означает термин "социальная инженерия"? (**ПК-1**)

a) Атака на базу данных

b) Хакерский взлом

c) Использование обмана для получения доступа к системе

d) Использование программного обеспечения для взлома паролей

11. Какой тип кибератаки пытается перегрузить веб-сервер, отправляя большое количество запросов? (**ПК-1**)

a) Фишинг

b) DDoS

c) Кросс-сайтовый скриптинг

d) SQL-инъекция

12. Какое программное обеспечение защищает компьютеры от вредоносных программ? (**ПК-1**)

a) Антивирус

b) Фаервол

c) VPN

d) Интранет

13. Что такое пароль? (**ПК-1**)

a) Символьная строка, используемая для доступа к устройству или приложению

b) Метка, которая идентифицирует устройство в сети

c) Физическое устройство, которое используется для хранения данных

d) Название компании, которая разработала операционную систему

14. Что такое антивирусное программное обеспечение? (**ПК-1**)

a) Программа, которая защищает компьютер от вирусов

b) Программа, которая создает вирусы

c) Программа, которая удаляет важные файлы с компьютера

d) Программа, которая ускоряет работу компьютера

15. Что такое фишинг? (**ПК-1**)

a) Мошенничество, направленное на получение личной информации пользователя

b) Программа, которая защищает компьютер от вирусов

c) Метод атаки на сеть, использующий множество компьютеров

d) Название определенного типа вируса

Что такое шифрование? (**ПК-1**)

a) Процесс преобразования понятного текста в зашифрованный текст

b) Процесс преобразования зашифрованного текста в понятный текст

c) Метод атаки на сеть, использующий множество компьютеров

d) Название определенного типа вируса

16. Что означает термин "фишинг" в контексте информационной безопасности? (**ПК-1**)

a) Кража паролей и логинов с уязвимых сайтов

b) Отправка ложных сообщений с целью обмана пользователей

c) Незаконный доступ к защищенным данным

d) Использование вредоносного ПО для получения доступа к системе

Задания открытого типа

1. Что такое пароль? Приведите пример типов паролей. (**ПК-1**)

2. Какие существуют методы аутентификации пользователей? Приведите пример одного из методов. (**ПК-1**)

3. Какие существуют типы атак на веб-приложения? Приведите пример одного из типов атак. (**ПК-1**)

4. Что такое фишинг? Приведите пример разновидностей фишинга. (**ПК-1**)

5. Что такое DoS-атака? Приведите пример методов проведения DoS-атак. (**ПК-1**)

6. Что такое многофакторная аутентификация? Приведите пример методов реализации многофакторной аутентификации. (**ПК-1**)

7. Какие существуют типы вредоносного ПО? Приведите пример каждого типа вредоносного ПО. (**ПК-1**)

8. Что такое антивирус? Приведите пример популярных антивирусов. (**ПК-1**)

9. Что такое хакер? Приведите пример разновидностей хакеров. (**ПК-1**)

10. Что такое спам? Приведите пример типов спама. (**ПК-1**)

11. Что такое социальная инженерия? Приведите пример методов социальной инженерии. (**ПК-1**)

12. Что такое VPN? Приведите пример популярных VPN-сервисов. (**ПК-1**)

13. Что такое анализ угроз и как он используется для определения уровня риска в информационной безопасности? Приведите пример инструментов для проведения анализа угроз. (**ПК-1**)

14. Какие документы регламентируют требования к хранению и обработке персональных данных в Российской Федерации? Приведите пример требований, установленных данными документами. (**ПК-1**)

16. Какие нормативные акты регулируют порядок работы с государственной тайной в Российской Федерации? Приведите пример одного из них. (**ПК-1**)

17. Какой документ определяет общие требования к организации системы управления информационной безопасностью в организациях и органах государственной власти Российской Федерации? Приведите пример одного из требований. (**ПК-1**)

18. Какие методические документы используются для определения угроз информационной безопасности? Приведите пример одного из них. (**ПК-1**)

19. Какие методические документы используются для определения угроз информационной безопасности? Приведите пример одного из них. (**ПК-1**)

20. Какие требования установлены для защиты информации в области электронной торговли? Приведите пример одного из таких требований. (**ПК-1**)

21. Что такое социальная инженерия? Приведите пример методов социальной инженерии. (**ПК-1**)

22. Что такое шифрование данных? Приведите пример алгоритмов шифрования. (**ПК-1**)

23. Что такое VPN? Приведите пример популярных VPN-сервисов. (**ПК-1**)

24. Что такое межсетевой экран? Приведите примеры использования межсетевых экранов. (**ПК-1**)

25. Каковы основные принципы криптографии и как они используются для обеспечения информационной безопасности? Приведите пример алгоритмов криптографии. (**ПК-1**)

26. Что такое ботнеты и как они используются для проведения кибератак? Приведите пример ботнетов. (**ПК-1**)

27. Какие существуют методы защиты от SQL-инъекций? Приведите пример инструментов для защиты от SQL-инъекций. (**ПК-1**)

28. Что такое безопасность веб-сервисов и как она обеспечивается? Приведите пример уязвимостей веб-сервисов и методов их защиты. (**ПК-1**)

29. Как работает система защиты информации на уровне операционной системы? Приведите пример операционных систем и методов защиты информации на уровне ОС. (**ПК-1**)

30. Что такое защита от DDoS-атак и как она реализуется? Приведите пример инструментов и технологий для защиты от DDoS-атак. (**ПК-1**)

31. Какие существуют методы защиты от фишинга и социальной инженерии? Приведите пример инструментов и технологий для защиты от фишинга и социальной инженерии. (**ПК-1**)

32. Как работает система управления доступом и как она обеспечивает безопасность в информационных системах? Приведите пример инструментов для управления доступом и методов их применения. (**ПК-1**)