Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный университет им. А.Н. Косыгина
(Технологии. Дизайн. Искусство)»

Институт филиал РГУ им. А. Н. Косыгина в г. Твери
Кафедра гуманитарных наук и дизайна

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность информационных систем

Уровень образования	бакалавриат
Направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные технологии в дизайне
Срок освоения образовательной программы	4 года 6 месяцев
Форма(-ы) обучения	Очно-заочная

Рабочая программа учебной дисциплины «Безопасность информационных систем» основной профессиональной образовательной программы высшего образования, рассмотрена и одобрена на заседании кафедры, протокол № 9 от 24.05.2024 г.

Разработчик(и) рабочей программы учебной дисциплины:

1. Доцент _____ Д.А.Цуркан

Заведующий кафедрой Доктор филологических наук, доцент _____ О.В.Новоселова

1. ОБЩИЕ СВЕДЕНИЯ

Учебная дисциплина «Безопасность информационных систем» изучается в восьмом семестре.
Курсовая работа – не предусмотрена

1.1. Форма промежуточной аттестации:

экзамен

1.2. Место учебной дисциплины в структуре ОПОП

Учебная дисциплина Безопасность информационных систем относится к обязательной части.
Основой для освоения дисциплины являются результаты обучения по предшествующим дисциплинам и практикам:

- Проектирование информационных систем в дизайне;
- Технология программирования в дизайне.

Результаты обучения по учебной дисциплине, используются при изучении следующих дисциплин и прохождения практик:

- Производственная практика. Эксплуатационная.

Результаты освоения учебной дисциплины в дальнейшем будут использованы при прохождении учебной/производственной практики и (или) выполнении выпускной квалификационной работы.

2. ЦЕЛИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Целями изучения дисциплины Безопасность информационных систем являются:

- формирование у обучающихся системных теоретических знаний и практических навыков в области защиты информации, обеспечения конфиденциальности, целостности и доступности информационных ресурсов.
- овладение современными методами и средствами обеспечения информационной безопасности, включая администрирование аппаратно-программных комплексов защиты информации
- развитие способностей к анализу угроз информационной безопасности, оценке рисков и выбору адекватных мер защиты для различных классов информационных систем
- освоение принципов работы с нормативно-технической документацией в области информационной безопасности и применения требований регуляторов на практике
- формирование умений организации работ по обеспечению безопасности информационных ресурсов на всех этапах их жизненного цикла
- подготовка к профессиональной деятельности в условиях постоянно развивающихся киберугроз и технологий защиты информации, способности к разработке и реализации эффективных систем безопасности
- формирование у обучающихся компетенции(-й), установленной(-ых) образовательной программой в соответствии с ФГОС ВО по данной дисциплине.

Результатом обучения по дисциплине является овладение обучающимися знаниями, умениями, навыками и опытом деятельности, характеризующими процесс формирования компетенции(й) и обеспечивающими достижение планируемых результатов освоения учебной дисциплины.

2.1. Формируемые компетенции, индикаторы достижения компетенций, соотнесённые с планируемыми результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ПК-5 Способен организовать работы по обеспечению безопасности информационных ресурсов	ИД-ПК-5.1 Знание нормативно-технической документацией в области безопасности информационных ресурсов	**Знать:** основные нормативно-правовые акты РФ в области информационной безопасности; требования отраслевых стандартов и руководящих документов (РД ФСТЭК, ФСБ); международные стандарты информационной безопасности (серия ISO 27000). **Уметь:** анализировать нормативные требования применительно к конкретной информационной системе; разрабатывать организационно-распорядительные документы (положения, инструкции) по обеспечению безопасности информационных ресурсов. **Владеть:** навыками работы с системами правовой информации для поиска актуальных нормативных документов; методикой применения нормативных требований на различных этапах жизненного цикла информационной системы.
	ИД-ПК-5.2 Администрирование и эксплуатация аппаратно-программных средств защиты информации информационных ресурсов	**Знать:** архитектуру и принципы работы современных аппаратно-программных средств защиты информации. **Уметь:** выполнять установку, настройку и обновление программных средств защиты информации; администрировать системы защиты в соответствии с политикой безопасности организации; анализировать журналы событий и реагировать на инциденты безопасности. **Владеть:** практическими навыками настройки межсетевых экранов и систем обнаружения вторжений; методами эксплуатации комплексов криптографической защиты информации; технологиями резервного копирования и восстановления данных после сбоев и инцидентов.
	ИД-ПК-5.3 Анализ методов реализации информационной безопасности для защиты Web-ресурсов и мультимедийных приложений	

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоёмкость учебной дисциплины по учебному плану составляет:

по очно-заочной форме обучения –	6	**з.е.**	192	**час.**

3.1. Структура учебной дисциплины для обучающихся по видам занятий (очная форма обучения)

Структура и объем дисциплины									
Объем дисциплины по семестрам	форма промежуточной аттестации	всего, час	Контактная аудиторная работа, час				Самостоятельная работа обучающегося, час		
			лекции, час	практические занятия, час	лабораторные занятия, час	практическая подготовка, час	курсовая работа/ курсовой проект	самостоятельная работа обучающегося, час	промежуточная аттестация, час
8 семестр	экзамен	192	28	28	28			76	32
Всего:		192	28	28	28			76	32

3.2. Структура учебной дисциплины для обучающихся по разделам и темам дисциплины: (очная форма обучения)

Планируемые (контролируемые) результаты освоения: код(ы) формируемой(ых) компетенции(й) и индикаторов достижения компетенций	Наименование разделов, тем; форма(ы) промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	Лабораторные работы/ индивидуальные занятия час	Практическая подготовка, час		
	Восьмой семестр						
ИД-ПК-5.1 ИД-ПК-5.2	**Раздел I. Основы информационной безопасности и криптографической защиты**					30	
	Тема 1.1 Введение в информационную безопасность	4					Формы текущего контроля по разделу I: отчет с результатами выполненных экспериментально-практических заданий
	Тема 1.2 Киберугрозы современности: аналитика атак	4					
	Тема 1.3 Криптографические методы защиты информации	4					
	Тема 1.4 Управление ключами и электронная подпись	4					
	Лабораторная работа № 1.1 Исследование кибератак в дизайн-индустрии			4			
	Лабораторная работа № 1.2 Разработка моделей угроз и оценка рисков информационной безопасности			4			
	Лабораторная работа № 1.3 Применение криптографических алгоритмов для защиты данных			4			
	Лабораторная работа № 1.4 Реализация системы управления ключами шифрования			4			
ИД-ПК-5.1 ИД-ПК-5.2	**Раздел II. Технические средства и организационные мероприятия защиты информации**					10	Формы текущего контроля по разделу II: - отчет с результатами выполненных экспериментально-практических заданий
	Тема 2.1 Аппаратно-программные средства защиты информации	4					
	Тема 2.2 Защита от вредоносного программного обеспечения	4					
	Тема 2.3 Безопасность сетевых технологий и коммуникаций	4					
	Тема 2.4 Аудит и мониторинг информационной безопасности	6					
	Лабораторная работа № 2.1 Настройка и администрирование межсетевых экранов			4			
	Лабораторная работа № 2.2 Анализ и нейтрализация			4			

Планируемые (контролируемые) результаты освоения: код(ы) формируемой(ых) компетенции(й) и индикаторов достижения компетенций	Наименование разделов, тем; форма(ы) промежуточной аттестации	Виды учебной работы				Самостоятельная работа, час	Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости; формы промежуточного контроля успеваемости
		Контактная работа					
		Лекции, час	Практические занятия, час	Лабораторные работы/ индивидуальные	Практическая подготовка, час		
	вредоносного программного обеспечения						
	Лабораторная работа № 2.3 Защита беспроводных сетей и настройка VPN			4			
	Лабораторная работа № 2.4 Проведение аудита защищенности информационной системы			6			
	Экзамен						Устный опрос
	ИТОГО за весь период	**34**		**34**		**40**	

3.3. Краткое содержание учебной дисциплины

№ пп	Наименование раздела и темы дисциплины	Содержание раздела (темы)
Раздел I	**Основы информационной безопасности и криптографической защиты**	
Тема 1.1	Введение в информационную безопасность	Основные понятия и определения информационной безопасности. Концепция CIA (Confidentiality, Integrity, Availability). Классификация угроз информационной безопасности. Законодательная база РФ в области ИБ (ФЗ-152, ФЗ-187). Роль и место информационной безопасности в современном digital-пространстве.
Тема 1.2	Киберугрозы современности: аналитика атак	Анализ современных векторов кибератак: фишинг, целевые атаки (APT), ransomware. Тактики, техники и процедуры (TTP) современных киберпреступников. Кейсы реальных инцидентов информационной безопасности. Методы социальной инженерии и защиты от них.
Тема 1.3	Криптографические методы защиты информации	Основные понятия криптографии: шифрование, дешифрование, криптостойкость. Симметричные криптосистемы (AES, DES) и асимметричные криптосистемы (RSA, Эль-Гамаль). Хэш-функции и их применение (MD5, SHA-256). Криптографические протоколы и стандарты.
Тема 1.4	Управление ключами и электронная подпись	Жизненный цикл криптографических ключей. Методы генерации, хранения и распределения ключей. Электронная подпись: принципы работы, виды и области применения. Инфраструктура открытых ключей (PKI). Юридическая сила электронной подписи.
Раздел II	**Технические средства и организационные мероприятия защиты информации**	
Тема 2.1	Аппаратно-программные средства защиты информации	Классификация средств защиты информации. Межсетевые экраны (firewall), системы обнаружения и предотвращения вторжений (IDS/IPS). Системы контроля доступа и аутентификации. Аппаратные модули безопасности (HSM). Защищенные операционные системы.
Тема 2.2	Защита от вредоносного программного обеспечения	Классификация вредоносного ПО: вирусы, черви, трояны, шпионское ПО. Методы обнаружения и нейтрализации угроз. Антивирусные решения и системы песочницы (sandboxing). Поведенческий анализ и эвристические методы обнаружения.
Тема 2.3	Безопасность сетевых технологий и коммуникаций	Принципы безопасной сетевой архитектуры. Защита беспроводных сетей (WPA2, WPA3). Технологии VPN и их криптографические основы. Безопасность протоколов передачи данных (TLS/SSL). Сегментация сетей как метод защиты.
Тема 2.4	Аудит и мониторинг информационной безопасности	Методы и средства мониторинга информационной безопасности. Системы SIEM (Security Information and Event Management). Процедуры аудита безопасности. Реагирование на инциденты информационной безопасности. Метрики и показатели эффективности системы защиты.

3.4. Организация самостоятельной работы обучающихся

Самостоятельная работа студента – обязательная часть образовательного процесса, направленная на развитие готовности к профессиональному и личностному самообразованию, на проектирование дальнейшего образовательного маршрута и профессиональной карьеры.

Самостоятельная работа обучающихся по дисциплине организована как совокупность аудиторных и внеаудиторных занятий и работ, обеспечивающих успешное освоение дисциплины.

Аудиторная самостоятельная работа обучающихся по дисциплине выполняется на учебных занятиях под руководством преподавателя и по его заданию. Аудиторная самостоятельная работа обучающихся входит в общий объем времени, отведенного учебным планом на аудиторную работу, и регламентируется расписанием учебных занятий.

Внеаудиторная самостоятельная работа обучающихся – планируемая учебная, научно-исследовательская, практическая работа обучающихся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия, расписанием учебных занятий не регламентируется.

Внеаудиторная самостоятельная работа обучающихся включает в себя:

- подготовку к лекциям, практическим занятиям, зачету;
- изучение учебных пособий;
- изучение разделов/тем, не выносимых на лекции и практические занятия самостоятельно;
- написание тематических докладов и эссе на проблемные темы;
- проведение исследовательских работ;
- изучение теоретического и практического материала по рекомендованным источникам;
- подготовка к контрольной работе;
- выполнение индивидуальных заданий.

Самостоятельная работа обучающихся с участием преподавателя в форме иной контактной работы предусматривает групповую и (или) индивидуальную работу с обучающимися и включает в себя:

- проведение индивидуальных и групповых консультаций по отдельным темам/разделам дисциплины;
- проведение консультаций перед зачетом;
- консультации по организации самостоятельного изучения отдельных разделов/тем, базовых понятий учебных дисциплин профильного/родственного бакалавриата, которые формировали ОПК и ПК, в целях обеспечения преемственности образования.

Перечень разделов/тем/, полностью или частично отнесенных на самостоятельное изучение с последующим контролем:

№ пп	Наименование раздела /темы дисциплины, выносимые на самостоятельное изучение	Задания для самостоятельной работы	Виды и формы контрольных мероприятий (учитываются при проведении текущего контроля)	Трудоемкость, час
Раздел I	**Основы информационной безопасности и криптографической защиты**			
Тема 1.1	Введение в информационную безопасность	1. Подготовить аналитический обзор изменений в ФЗ-152 "О персональных данных" за последние 3 года. 2. Составить глоссарий из 20 основных терминов по информационной безопасности с расшифровкой и примерами.	Презентация	**10**

Тема 1.2	Киберугрозы современности: аналитика атак	Подготовить обзор методов социальной инженерии и способов защиты от них.	Презентация	**10**
Раздел II	**Технические средства и организационные мероприятия защиты информации**			
Тема 2.4	Аудит и мониторинг информационной безопасности	1. Разработать программу аудита информационной безопасности для малого предприятия. 2. Подготовить шаблон отчета о проведении аудита ИБ. 3. Разработать метрики для мониторинга эффективности системы защиты информации.	Отчет	**20**

3.5. Применение электронного обучения, дистанционных образовательных технологий

При реализации программы учебной дисциплины электронное обучение и дистанционные образовательные технологии не применяются.

4. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, КРИТЕРИИ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ, СИСТЕМА И ШКАЛА ОЦЕНИВАНИЯ

4.1. Соотнесение планируемых результатов обучения с уровнями сформированности компетенции(й).

Уровни сформированности компетенции(-й)	**Итоговое количество баллов в 100-балльной системе по результатам текущей и промежуточной аттестации**	**Оценка в пятибалльной системе по результатам текущей и промежуточной аттестации**	**Показатели уровня сформированности**
			общепрофессиональной(-ых) компетенций
			ИД-ПК-5.1 ИД-ПК-5.2
высокий	85 – 100	отлично/ зачтено (отлично)/ зачтено	Демонстрирует системное понимание и творческое применение: • Свободно анализирует и применяет нормативно-техническую документацию для разработки организационно-распорядительных документов по безопасности • Критически оценивает и выбирает оптимальные аппаратно-программные средства защиты, разрабатывает рекомендации по их совершенствованию • Способен проектировать комплексные системы защиты информации и организовывать работы по их внедрению • Глубоко анализирует угрозы безопасности и разрабатывает эффективные меры противодействия
повышенный	65 – 84	хорошо/ зачтено (хорошо)/ зачтено	Демонстрирует уверенное применение знаний: • Уверенно работает с нормативно-технической документацией, применяет требования на практике • Эффективно администрирует аппаратно-программные средства защиты, настраивает и обслуживает их • Может анализировать риски информационной безопасности и выбирать адекватные меры защиты • Способен выявлять и устранять типовые уязвимости в системах защиты
базовый	41 – 64	удовлетворительно/ зачтено (удовлетворительно)/ зачтено	Демонстрирует минимально необходимый уровень: • Знает основные нормативные документы и может их применять под руководством • Выполняет базовые операции по администрированию средств защиты по инструкции • Распознает основные угрозы информационной безопасности, но испытывает трудности в выборе мер защиты • Может выполнять стандартные процедуры обеспечения безопасности информации
низкий	0 – 40	неудовлетворительно/ не зачтено	Не демонстрирует минимально необходимый уровень

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ, ВКЛЮЧАЯ САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

При проведении контроля самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации по учебной дисциплине «Безопасность информационных систем» проверяется уровень сформированности у обучающихся компетенций и запланированных результатов обучения по дисциплине, указанных в разделе 2 настоящей программы.

5.1. Формы текущего контроля успеваемости, примеры типовых заданий:

№ пп	Формы текущего контроля	Примеры типовых заданий
1	Презентация	Темы для презентаций: «Исследование кибератак в дизайн-индустрии» (на выбор)
2	Презентация	Темы для презентаций: 1. Фишинговые атаки: эволюция методов и современные способы защиты пользователей и организаций» Описать механизмы современных фишинговых кампаний, предложить рекомендации по повышению осведомленности сотрудников и внедрению технических мер защиты. 2.«Атаки с использованием социальной инженерии: психологический аспект и стратегии предотвращения угроз» Проанализировать влияние психологии поведения человека на уязвимости системы безопасности, описать меры превентивной подготовки персонала и организации процессов контроля рисков. 3.«Современные криптографические угрозы и защита инфраструктуры цифровых подписей» Изучить потенциальные риски для алгоритмов шифрования, используемые хакерами в условиях современной цифровой среды, представить сценарии усиления защиты PKI-инфраструктуры. 4.«Анализ и профилактика инсайдерских угроз в корпоративной среде» Исследовать наиболее распространённые виды внутренних кибератак, обсудить инструменты мониторинга и раннего выявления аномалий среди привилегированных пользователей. 5.«Использование машинного обучения для обнаружения сетевых вторжений и мошенничества» Оценить эффективность внедрения ML-технологий в системах анализа безопасности, выявить ограничения и перспективы развития решений на основе AI. 6.«DDoS-атаки нового поколения: техника защиты высоконагруженных ресурсов и облачных сервисов» Обсудить самые эффективные техники защиты распределённых вычислительных платформ и веб-сервисов от DDoS-атак с привлечением облачной инфраструктуры. 7.«Опасности атак класса Zero Day и методики реагирования на подобные инциденты»

№ пп	Формы текущего контроля	Примеры типовых заданий
		Раскрыть суть проблемы нулевого дня, рассмотреть опыт крупных компаний по управлению рисками и выработке рекомендаций по экстренному восстановлению после взлома. 8.«Применение концепции DevSecOps для интеграции безопасности в жизненный цикл разработки ПО» Объяснить преимущества интеграции подходов CI/CD и SecDevOps, продемонстрировать пути встраивания процедур оценки риска и автоматизированного тестирования безопасности на всех этапах процесса разработки программного продукта.
3	Отчет	Отчет по проведению аудита безопасности выбранного объекта. Структура и содержание отчета • Титульный лист. • Введение и цели аудита. Целями могут быть: выявление уязвимых мест в действующей системе охраны, оценка возможного ущерба, разработка рекомендаций по предотвращению угроз и т.д. • Описание объекта. • Методология и объем проверки. Перечень использованных методов (опросы, осмотр, анализ документации, тестирование систем) и границ аудита (проверялись ли все подразделения или выборочно). • Оценка системы защиты. Описание состояния и работоспособности всех проверенных систем • Выявленные риски и уязвимости. • Рекомендации по устранению недостатков: для каждого выявленного риска должны быть предложены конкретные, реалистичные и измеримые меры по его устранению с приоритетами выполнения (краткосрочные/долгосрочные).

5.2. Критерии, шкалы оценивания текущего контроля успеваемости:

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
	Содержание презентации соответствует заявленной тематике. Студент полностью		5

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
Презентация	и самостоятельно логично излагает материал, владеет специальной терминологией, демонстрирует общую эрудицию в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на ресурсы Интернета, соотносит теорию с практическими задачами. Развернуто отвечает на дополнительные вопросы.		
	Содержание презентации соответствует заявленной тематике. Студент логично излагает материал, владеет специальной терминологией, демонстрирует базовые знания в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на ресурсы Интернета. На дополнительные вопросы дает обоснованные ответы.		4
	Содержание презентации соответствует заявленной тематике не в полном объеме. Студент излагает материал в опоре на помощь преподавателя, демонстрирует отдельные знания в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на ресурсы Интернета. На вопросы отвечает фрагментарно.		3
	Не предоставил доклад		2
Презентация	Содержание презентации соответствует заявленной тематике. Студент полностью и самостоятельно логично излагает материал, владеет специальной терминологией, демонстрирует общую эрудицию в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на ресурсы Интернета, соотносит теорию с практическими задачами. Развернуто отвечает на дополнительные вопросы.		5
	Содержание презентации соответствует заявленной тематике. Студент логично излагает материал, владеет специальной терминологией, демонстрирует базовые знания в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на ресурсы Интернета. На дополнительные вопросы дает обоснованные ответы.		4
	Содержание презентации соответствует заявленной тематике не в полном объеме. Студент излагает материал в опоре на помощь преподавателя, демонстрирует		3

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
	отдельные знания в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на ресурсы Интернета. На вопросы отвечает фрагментарно.		
	Не предоставил доклад		2
Отчет	Отчет демонстрирует глубокое понимание методологии аудита. Все разделы полностью завершены, включая детальный анализ угроз и уязвимостей. Рекомендации носят практический характер, с четкими сроками реализации и оценкой эффективности. Документ соответствует профессиональным стандартам оформления.		5
	Отчет содержит все обязательные разделы, но анализ некоторых аспектов может быть недостаточно глубоким. Выводы в основном обоснованы, но могут отсутствовать некоторые доказательства. Рекомендации реализуемы, но требуют уточнения по срокам и ресурсам.		4
	Отчет содержит существенные пробелы в анализе. Методология аудита применена частично. Выводы носят поверхностный характер, рекомендации недостаточно конкретны. Структура документа требует существенного улучшения.		3
	Не предоставил отчет		2

5.3. Промежуточная аттестация:

Форма промежуточной аттестации	Типовые контрольные задания и иные материалы для проведения промежуточной аттестации:
Экзамен	Список вопросов: 1. Что составляет основу концепции информационной безопасности "CIA"? 2. Назовите основные виды угроз конфиденциальности информации. 3. Какие российские законы составляют основу правового регулирования в области информационной безопасности? 4. В чем заключается принципиальное различие между симметричным и асимметричным шифрованием? 5. Какую функцию в защите данных выполняют хэш-суммы?

	6. Что представляет собой инфраструктура открытых ключей (PKI)? 7. Каковы основные этапы процесса управления рисками информационной безопасности? 8. Назовите основные классы вредоносного программного обеспечения. 9. Как работает и для чего предназначен межсетевой экран (firewall)? 10. В чем разница между системами обнаружения (IDS) и предотвращения (IPS) вторжений? 11. Какие основные угрозы безопасности характерны для беспроводных сетей Wi-Fi? 12. Какой принцип является фундаментальным для модели безопасности Zero Trust? 13. Что такое фишинг и каковы его основные признаки? 14. Каковы цели и задачи проведения аудита информационной безопасности? 15. Что такое инцидент информационной безопасности и каковы этапы работы с ним? 16. Для чего используются системы мониторинга и управления событиями информационной безопасности (SIEM)? 17. Что подразумевается под социальной инженерией в контексте информационной безопасности? 18. Какие организационные меры защиты информации вы знаете? 19. Как технология VPN обеспечивает безопасность передаваемых данных? 20. В чем заключаются основные этические принципы работы специалиста по информационной безопасности?

5.4. Критерии, шкалы оценивания промежуточной аттестации учебной дисциплины:

Форма промежуточной аттестации	**Критерии оценивания**	**Шкалы оценивания**		
Наименование оценочного средства		**100-балльная система**	**Пятибалльная система**	
Экзамен	Обучающийся знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины.		Зачтено	41%-100%
	Обучающийся не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине.		не зачтено	40% и менее 40%

5.5. Система оценивания результатов текущего контроля и промежуточной аттестации.

Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.

Форма контроля	100-балльная система	Пятибалльная система
Текущий контроль:		
- презентация	0 - 20 баллов	2 – 5
- презентация	0 - 20 баллов	2 – 5
- отчет	0 - 30 баллов	2 – 5
Промежуточная аттестация зачет	0 - 30 баллов	зачтено не зачтено
Итого за семестр зачёт	0 - 100 баллов	

Полученный совокупный результат конвертируется в пятибалльную систему оценок в соответствии с таблицей:

100-балльная система	пятибалльная система	
	зачет с оценкой/экзамен	зачет
85 – 100 баллов	отлично зачтено (отлично)	зачтено
65 – 84 баллов	хорошо зачтено (хорошо)	
41 – 64 баллов	удовлетворительно зачтено (удовлетворительно)	
0 – 40 баллов	неудовлетворительно	не зачтено

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Реализация программы предусматривает использование в процессе обучения следующих образовательных технологий:

- проблемная лекция;
- групповых дискуссий;
- анализ ситуаций и имитационных моделей;
- поиск и обработка информации с использованием сети Интернет;
- применение электронного обучения;
- использование на лекционных занятиях видеоматериалов и наглядных пособий.

7. ПРАКТИЧЕСКАЯ ПОДГОТОВКА

Практическая подготовка в рамках учебной дисциплины реализуется при проведении практических занятий, связанных с будущей профессиональной деятельностью.

Проводятся отдельные занятия лекционного типа, которые предусматривают передачу учебной информации обучающимся, которая необходима для последующего выполнения практической работы.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуального обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения, проведение дополнительных индивидуальных консультаций по изучаемым теоретическим вопросам и практическим занятиям, оказание помощи при подготовке к промежуточной аттестации.

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения.

Учебные и контрольно-измерительные материалы представляются в формах, доступных для изучения студентами с особыми образовательными потребностями с учетом нозологических групп инвалидов:

Для подготовки к ответу на практическом занятии, студентам с ограниченными возможностями здоровья среднее время увеличивается по сравнению со средним временем подготовки обычного студента.

Для студентов с инвалидностью или с ограниченными возможностями здоровья форма проведения текущей и промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Промежуточная аттестация по дисциплине может проводиться в несколько этапов в форме рубежного контроля по завершению изучения отдельных тем дисциплины. При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся создаются, при необходимости, фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины при обучении с использованием традиционных технологий обучения.

Наименование учебных аудиторий, лабораторий, мастерских, библиотек, спортзалов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.	**Оснащенность учебных аудиторий, лабораторий, мастерских, библиотек, спортивных залов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.**
аудитории для проведения занятий лекционного типа	комплект учебной мебели, технические средства обучения, служащие для представления учебной информации большой аудитории: ~ ноутбук; ~ проектор.
аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	комплект учебной мебели, технические средства обучения, служащие для представления учебной информации большой аудитории:

Наименование учебных аудиторий, лабораторий, мастерских, библиотек, спортзалов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.	Оснащенность учебных аудиторий, лабораторий, мастерских, библиотек, спортивных залов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.
	~ ноутбук, ~ проектор
аудитории для проведения занятий по практической подготовке, групповых и индивидуальных консультаций	комплект учебной мебели, технические средства обучения, служащие для представления учебной информации большой аудитории: ~ 5 персональных компьютеров, ~ принтеры.
Помещения для самостоятельной работы обучающихся	**Оснащенность помещений для самостоятельной работы обучающихся**
читальный зал библиотеки:	~ компьютерная техника; подключение к сети «Интернет»

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

№ п/п	Автор(ы)	Наименование издания	Вид издания (учебник, УП, МП и др.)	Издательство	Год издания	Адрес сайта ЭБС или электронного ресурса	Количество экземпляров в библиотеке Университета
10.1 Основная литература, в том числе электронные издания							
1	Бондаренко И. С.	Информационная безопасность	Учебник	Издательство "МИСИС"	2023	https://e.lanbook.com/book/360344	-
2	Ерохин В. В., Погонышева Д. А., Степченко И. Г.	Безопасность информационных систем	Учебное пособие	Издательство "ФЛИНТА"	2022	https://e.lanbook.com/book/232457	-
3	Нефедов В. С.	Безопасность прикладных информационных технологий и систем	Учебное пособие	МИРЭА - Российский технологический университет	2025	https://e.lanbook.com/book/504831	-
10.2 Дополнительная литература, в том числе электронные издания							
1	Баланов А. Н.	Комплексная информационная безопасность	Учебное пособие	Издательство "Лань"	2025	https://e.lanbook.com/book/460715	-
2	Давидюк Н. В., Космачева И. М.	Мониторинг безопасности информационных систем	Учебное пособие	ИЦ Интермедия	2020	https://e.lanbook.com/book/161352	-
10.3 Методические материалы (указания, рекомендации по освоению дисциплины авторов РГУ им. А. Н. Косыгина)							
-	-	-	-	-	-	-	-

11. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

11.1. Ресурсы электронной библиотеки, информационно-справочные системы и профессиональные базы данных:

№ пп	Электронные учебные издания, электронные образовательные ресурсы
1.	ЭБС «Лань» http://www.e.lanbook.com/
2.	«Znanium.com» научно-издательского центра «Инфра-М» http://znanium.com/
3.	Электронные издания «РГУ им. А.Н. Косыгина» на платформе ЭБС «Znanium.com» http://znanium.com/

11.2. Перечень программного обеспечения

№п/п	Программное обеспечение	Реквизиты подтверждающего документа/ Свободно распространяемое
1.	Windows 10 Pro, MS Office 2019	контракт № 18-ЭА-44-19 от 20.05.2019

ЛИСТ УЧЕТА ОБНОВЛЕНИЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

В рабочую программу учебной дисциплины внесены изменения/обновления и утверждены на заседании кафедры:

№ пп	год обновления РПД	характер изменений/обновлений с указанием раздела	номер протокола и дата заседания кафедры