

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Белгородский Валерий Савельевич
Должность: Ректор
Дата подписания: 18.06.2025 14:47:56
Уникальный программный ключ:
8df276ee93e17c18e7bee9e7cad2d0ed9ab82473

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	Институт экономики и менеджмента
Кафедра	Информационных технологий

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Уровень образования	бакалавриат
Направление подготовки	09.03.02 Информационные системы и технологии
Профиль)/Специализация	Информационные технологии и искусственный интеллект в бизнесе
Срок освоения образовательной программы по очной форме обучения	4 года
Форма обучения	очная

Рабочая программа учебной дисциплины «Информационная безопасность» основной профессиональной образовательной программы высшего образования, рассмотрена и одобрена на заседании кафедры, протокол №9 от 15.04.2025 г.

Разработчик рабочей программы «Информационная безопасность»

1	Доцент	А.Р. Муртазина
2	Преподаватель	А.В. Щербак

Заведующий кафедрой: канд. техн. наук, доц. И.Б. Разин

1. ОБЩИЕ СВЕДЕНИЯ

Учебная дисциплина «Информационная безопасность» изучается в четвертом семестре.
Курсовая работа– не предусмотрена

Форма промежуточной аттестации: зачет.

1.1. Место учебной дисциплины в структуре ОПОП

Учебная дисциплина «Информационная безопасность» относится к обязательной части.

Основой для освоения дисциплины являются результаты обучения по предшествующим дисциплинам:

- Дифференциальное и интегральное исчисления
- Программирование
- Дискретная математика и программирование

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

2. ЦЕЛИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Целями изучения дисциплины «Информационная безопасность» являются:

- изучение общих инструментов соблюдения требований по информационной безопасности;
- изучение возможных угроз безопасности информации, обрабатываемой в информационных системах;
- формирование умения обеспечить защиту информации и объектов информатизации;
- изучение основных направлений, методов и средств обеспечения безопасности информации в информационных системах;
- освоение методов ориентирования и взаимодействия с ресурсами информационной среды, осуществления выбора различных моделей использования информационных и коммуникационных технологий в профессиональной деятельности;
- изучение методов поиска, анализа и обработки информации;
- формирование навыков оформления документов на основе библиографической культуры с использованием информационно-коммуникационных технологий, с учетом соблюдения авторского права;
- формирование у обучающихся компетенций, установленных образовательной программой в соответствии с ФГОС ВО по данной дисциплине.

Результатом обучения по учебной дисциплине является овладение обучающимися знаниями, умениями, навыками и опытом деятельности, характеризующими процесс формирования компетенций 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
	ИД-ОПК-3.1	

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Подготовка документов на основе библиографической культуры с использованием информационно-коммуникационных технологий	– Анализирует и систематизирует отечественную и зарубежную научно-техническую информацию. – Описывает базовые понятия и определения, используемые в сфере информационной безопасности. – Перечисляет основные угрозы безопасности информации, а также методы и средства противодействия этим угрозам – Показывает способности в понимании и практическом использовании инструментов для защиты информации – Описывает современное состояние уровня и направлений развития технических и программных средств универсального и специального назначения. – Владеет основными методами, способами и средствами получения, хранения, переработки, передачи и защиты информации. – Обрабатывает результаты информационно-библиографического поиска
	ИД-ПК-3.2 Подготовка аналитических обзоров для решения стандартных задач профессиональной деятельности с учетом соблюдения авторского права	
	ИД-ПК-3.3 Соблюдение требований по информационной безопасности	

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ/МОДУЛЯ

Общая трудоёмкость учебной дисциплины по учебному плану составляет:

Очная форма обучения	4	з.е.	128	час.
----------------------	---	------	-----	------

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

Структура и объем дисциплины				
Объем дисциплины по семестрам	фо	рм	а	пр
	во	го,	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,	промежуточная аттестация, час
4 семестр	Зачет	96	16	18	30			32	
Всего:	Зачет	96	16	18	30			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		
	Четвертый семестр						
		16	18	30		32	
ОПК-3 ИД-ОПК-3.1 ИД-ОПК-3.2 ИД-ОПК-3.3	Раздел 1. Общие вопросы информационной безопасности и защиты информации						Формы текущего контроля по разделам: 1. Контроль посещаемости 2. Письменный отчет с результатами выполненных заданий лабораторной работы 3. Реферат 4. Информационное сообщение в форме презентации 5. Участие (достижения) в профессиональных конкурсах. 5. Научная и/или практическая работа.
	Тема 1.1 Основы безопасности	2					
	Лабораторная работа 1.1 Восстановление данных.			5			
	Практическое занятие 1.1 Основы безопасности		2				
	Тема 1.2 Защита информации	2					
	Практическое занятие 1.2 Защита информации		2				
	Тема 1.3 Шифры замены	2					
	Лабораторная работа 1.2 Шифр Цезаря			5			
	Практическое занятие 1.3 Шифры замены		3				
	Тема 1.4 Шифры перестановки	2					
	Практическое занятие 1.4 Шифры перестановки		2				
	Тема 1.5 Шифры гаммирования	2					
	Лабораторная работа 1.3 Генерация простых чисел			5			
	Практическое занятие 1.5.Шифры гаммирования		3				
Реферат «Защита информации»					20		
ОПК-3 ИД-ОПК-3.1 ИД-ОПК-3.2 ИД-ОПК-3.3	Раздел 2. Алгоритмы шифрования						
	Тема 2.1 Симметричные криптосистемы.	2					
	Практическое занятие 2.1 Симметричные криптосистемы.		2				
	Тема 2.2 Асимметричные криптосистемы	2					
	Практическое занятие 2.2 Асимметричные криптосистемы		2				

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		
	Тема 2.3 Электронные подписи	2					
	Практическое занятие 2.3 Электронные подписи		2				
	Лабораторная работа 2.1 Алгоритмы шифрования DES			5			
	Лабораторная работа 2.2 Алгоритм Эль Гамала			5			
	Лабораторная работа 2.3 Алгоритм на основе задачи об укладке рюкзака			5			
	Информационное сообщение «Алгоритмы шифрования»					10	
Все индикаторы всех компетенций	Электронные подписи					2	Зачет в устной форме.
	ИТОГО	16	18	30		32	

3.3. Краткое содержание учебной дисциплины

№ пп	Наименование раздела и темы дисциплины	Содержание раздела (темы)
Раздел 1	Общие вопросы информационной безопасности и защиты информации	
Тема 1.1	Основы безопасности	Информационная безопасность. Основные понятия. Значение безопасности в ИТ. Виды защищаемой информации. Основные угрозы безопасности. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Будущее безопасности ИТ. Роль искусственного интеллекта в обеспечении безопасности
Практическое занятие 1.1	Основы безопасности	Модели информационной безопасности. Методы обеспечения безопасности. Стандарты безопасности.
Тема 1.2	Защита информации	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Основные угрозы для информации: Физические, технические и кибернетические угрозы. Стандарты информационной безопасности: ISO/IEC, PCI DSS, FISMA и другие Технологии защиты информации. Методы предотвращения утечек информации. Правовые аспекты защиты информации
Практическое занятие 1.2	Защита информации	Описание и примеры использования основных инструментов. Сканеры безопасности. Анализаторы уязвимостей. Тестеры на проникновение. Системы обнаружения и предотвращения вторжений (IDS/IPS). Средства анализа сетевого трафика. Инструменты управления инцидентами. Средства мониторинга и аудита. Критерии выбора и оценка эффективности прикладных инструментов.
Тема 1.3	Шифры замены	Определение шифра замены. История развития шифров замены. Основы теории криптографии. Классификация шифров замены. Моноалфавитные шифры замены. Метод Цезаря. Метод Вижинера. Полиалфавитные шифры замены. Безопасность и уязвимости шифров замены. Стойкость шифров замены к криптоанализу.
Практическое занятие 1.3	Шифры замены	Процесс шифрования и дешифрования с использованием шифра замены. Практическое использование шифров замены.
Тема 1.4	Шифры перестановки	История развития шифров перестановки Классификация шифров перестановки. Простые перестановки. Простая перестановка с фиксированным периодом. Простая перестановка со случайным периодом. Сложные перестановки. Устойчивость и уязвимость шифров перестановки Шифры перестановки с фиксированным периодом. Табличные шифры перестановки Перестановка по усложнённым маршрутам.

Практическое занятие 1.4	Шифры перестановки	Основы работы с шифрами перестановки. Процессы шифрования и расшифрования с использованием шифров перестановки. Практическое использование шифров перестановки
Тема 1.5	Шифры гаммирования	Определение шифра гаммирования. Математические основы асимметричной криптографии. Малая теорема Ферма. Китайская теорема об остатках. Проверка чисел на простоту Криптосистема Эль-Гамала
Практическое занятие 1.5	Шифры гаммирования	Работа шифра гаммирования. Виды шифров гаммирования. Примеры использования. Сравнение с другими методами
Раздел 2.	Алгоритмы шифрования	
Тема 2.1	Симметричные криптосистемы.	Симметричные и ассиметричные системы шифрования. Шифрование и расшифрование данных Ключи шифрования и алгоритм работы. Стойкость к криптоанализу. Основные алгоритмы симметричного шифрования: блочное шифрование, поточное шифрование, хеширование
Практическое занятие 2.1	Симметричные криптосистемы.	Принципы работы симметричных криптосистем. DES и его модификации. AES. RC4. MD5 (Message-Digest Algorithm 5). SHA (Secure Hash Algorithm).
Тема 2.2	Асимметричные криптосистемы	Определение асимметричной криптосистемы. Использование асимметричных криптосистем в современной криптографии. Предпосылки создания асимметричных криптосистем. Открытый и закрытый ключи. Стойкость к криптоанализу и атаки на асимметричные системы. Алгоритмы асимметричного шифрования. Применение асимметричных криптосистем. Защита информации в Интернете. Безопасность и стандартизация в области криптографии
Практическое занятие 2.2	Асимметричные криптосистемы	Принципы работы асимметричных криптосистем. Алгоритм цифровой подписи DSA. Алгоритм шифрования RSA. Процессы шифрования и дешифровки. Сравнение с симметричными криптосистемами.
Тема 2.3	Электронные подписи	Цифровые подписи (Электронные подписи). Виды электронных подписей. Создание и проверка электронной подписи. Цифровые подписи и сертификаты. Системы блокчейн и криптовалюты. Стандарты и регуляция в области электронных подписей. Развитие технологий. Риски и угрозы.
Практическое занятие 2.3	Электронные подписи	Принцип работы электронной подписи. Использование электронных подписей в разных сферах.

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 и лабораторным занятиям, зачету;
- изучение учебных пособий;
- изучение теоретического и практического материала по рекомендованным источникам;
- подготовка информационного сообщения в форме презентации;
- подготовка к выполнению лабораторных работ и отчетов по ним;
- написание тематического реферата на проблемную тему;
- подготовка к промежуточной аттестации в течение семестра.

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 экзаменом, перед зачетом по необходимости;
- 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/модуля, выносимые на самостоятельное изучение	Задания для самостоятельной работы	Виды и формы контрольных мероприятий (учитываются при проведении текущего контроля)	Трудоемкость, час
1	Раздел 1. Общие вопросы информационной безопасности и защиты информации	Подготовить реферат по теме «Защита информации»	реферат	20
2	Раздел 2. Алгоритмы шифрования	Подготовить информационное сообщение в форме презентации по теме «Алгоритмы шифрования»	Информационное сообщение	10

3.5. Применение электронного обучения, дистанционных образовательных технологий

При реализации программы учебной дисциплины возможно применение электронного обучения и дистанционных образовательных технологий.

Реализация программы учебной дисциплины с применением электронного обучения и дистанционных образовательных технологий регламентируется действующими локальными актами университета.

Применяются следующий вариант реализации программы с использованием ЭО и ДОТ

В электронную образовательную среду, по необходимости, могут быть перенесены отдельные виды учебной деятельности:

использование ЭО и ДОТ	использование ЭО и ДОТ	объем, час	включение в учебный процесс
смешанное обучение	Лекции	16	в соответствии с расписанием учебных занятий
	Практические	18	
	Лабораторные занятия	30	

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

4.1. Соотнесение планируемых результатов обучения с уровнями сформированности компетенций.

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) компетенции(-й)
			ОПК-3 ИД-ОПК-3.1 ИД-ОПК-3.2 ИД-ОПК-3.3
высокий	85 – 100	отлично/ зачтено (отлично)/ зачтено	Обучающийся: – исчерпывающе и логически стройно излагает учебный материал, умеет связывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения; – демонстрирует высокий уровень анализа предметной области и составления литературного обзора; – свободно ориентируется в учебной и профессиональной литературе; – даёт развёрнутые, исчерпывающие, профессионально грамотные ответы на вопросы, в том числе, дополнительные.
повышенный	65 – 84	хорошо/ зачтено (хорошо)/ зачтено	Обучающийся: – достаточно подробно, грамотно и по существу излагает изученный материал, приводит и раскрывает в тезисной форме основные понятия; – допускает единичные негрубые ошибки; – достаточно хорошо ориентируется в учебной и профессиональной литературе; – ответ отражает знание теоретического и практического материала, не допуская существенных неточностей.

базовый	41 – 64	удовлетворительно/ зачтено (удовлетворительно)/ зачтено	Обучающийся: – демонстрирует теоретические знания основного учебного материала дисциплины в объёме, необходимом для дальнейшего освоения ОПОП; – демонстрирует фрагментарные знания основной учебной литературы по дисциплине; – ответ отражает знания на базовом уровне теоретического и практического материала в объёме, необходимом для дальнейшей учёбы и предстоящей работы по профилю обучения.
низкий	0 – 40	неудовлетворительно/ не зачтено	Обучающийся: – демонстрирует фрагментарные знания теоретического и практического материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации; – испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами; – выполняет задания только по образцу и под руководством преподавателя; – ответ отражает отсутствие знаний на базовом уровне теоретического и практического материала в объёме, необходимом для дальнейшей учёбы.

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 «Информационная безопасность» 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	Формируемая компетенция
1	Лабораторная работа 1.1 Восстановление данных.	Часть 1. Провести анализ инструментов для программного восстановления данных, составить сравнительную таблицу (функциональные возможности, ОС, лицензия, файловая система, типы восстановления). Изучить программы для гарантированного уничтожения данных с электронных носителей, составить	ОПК-3 ИД-ОПК-3.1 ИД-ОПК-3.2

№ пп	Формы текущего контроля	Примеры типовых заданий	Формируемая компетенция
		сравнительную таблицу (функциональные возможности, ОС, лицензия, файловая система, методы удаления, возможность восстановления). Часть 2. С выбранными программами в части 1 провести эксперименты для разных типов файлов: текст, звук, графика, электронная таблица. Оценить полученные результаты, построить графики. Сделать выводы.	ИД-ОПК-3.3
2	Лабораторная работа 1.2 Шифр Цезаря	Реализовать алгоритм шифрования «Ключ Цезаря». Приложение должно быть с графическим интерфейсом для шифрования/дешифрования для многострочных сообщений, записанных кириллицей. Символы, которые не входят в алфавит, следует игнорировать. На форму вести таблицу символов. Выполнить обработку исключительных ситуаций.	
3	Лабораторная работа 1.3 Генерация простых чисел	Часть 1. Реализовать приложение с графическим интерфейсом, позволяющее выполнять следующие действия. 1. Генерировать псевдослучайную последовательность с помощью алгоритма одного из алгоритмов в таблице (см. ниже): а) все входные параметры генератора должны задаваться из файла или вводиться в приложении; б) сгенерированная последовательность, состоящая из 0 и 1, должна сохраняться в файл. 2. Проверять полученную псевдослучайную последовательность на равномерность и случайность с помощью трёх рассмотренных тестов: 1) результат проверки каждого теста должен отображаться в приложении; 2) все вычисляемые промежуточные значения (все шаги алгоритма теста) могут отображаться в приложении или сохраняться в файл. Возможные алгоритмы: 1) Алгоритм FIPS–186. 2) Алгоритм ANSI X9.17. 3) Алгоритм BBS. 4) Алгоритм RSA. 5) Алгоритм Yarrow–160 Часть 2. С помощью реализованного приложения выполнить следующие задания.	

№ пп	Формы текущего контроля	Примеры типовых заданий	Формируемая компетенция
		1. Протестировать правильность работы разработанного приложения. 2. Сгенерировать последовательность из не менее 10 000 бит и исследовать её на равномерность и случайность. 3. Сделать вывод о случайности сгенерированной последовательности и о возможности её использования в качестве криптографически безопасной псевдослучайной последовательности.	
4	Реферат информации» «Защита	Темы рефераты по теме «Защита информации» 1. Методы борьбы с фишинговыми атаками. 2. Законодательство о персональных данных. 3. Защита авторских прав. 4. Назначение, функции и типы систем видеозащиты. 5. Как подписывать с помощью ЭЦП электронные документы различных форматов.	
5	Лабораторная работа 2.1 Алгоритмы шифрования DES	1. Разработать приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться готовыми библиотеками либо программными кодами, реализующими некоторые блочные алгоритмы. Приложение должно реализовывать следующие операции: • разделение входного потока данных на блоки требуемой длины с необходимым дополнением последнего блока; • выполнение требуемых преобразований ключевой информации; • выполнение операций зашифрования/расшифрования; • оценка скорости выполнения операций зашифрования/расшифрования; • пошаговый анализ лавинного эффекта с подсчетом количества изменяющихся символов по отношению к исходному слову. 2. Проанализировать влияние слабых ключей и полуслабых ключей на конечный результат зашифрования и на лавинный эффект. 3. Оценить степень сжатия (используя любой доступный архиватор) открытого текста и соответствующего зашифрованного текста. Дать пояснения к полученному результату.	

№ пп	Формы текущего контроля	Примеры типовых заданий	Формируемая компетенция
6	Лабораторная работа 2.2 Алгоритм Эль Гамала	4. Результаты оформить в виде отчета по установленным правилам. 1. С помощью простого консольного приложения составить табличную или графическую форму зависимости времени вычисления параметра u, функционально заданного выражением вида: $u \equiv y = a^x \bmod n,$ от параметров: a (десятичные числа от 5 до 35; можно взять 1 или 2 числа), x (числа, желательно простые, из диапазона от 103 до 10100; для примера взять 5–10 чисел, равномерно распределенных в указанном диапазоне), n (для примера взять числа, в двоичном виде состоящие из 1024 и 2048 битов). 2. Разработать приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами. В основе вычислений – кодировочные таблицы ASCII. Приложение должно реализовывать следующие операции: • зашифрование и расшифрование текстовых документов на основе алгоритмов RSA и Эль-Гамала; • определение времени выполнения операций. Результаты оформить в виде отчета по установленным правилам.	
7	Лабораторная работа 2.3 Алгоритм на основе задачи об укладке рюкзака	Разработать приложение для формирования рюкзачного вектора. При этом можно воспользоваться доступными библиотеками либо программными кодами. В основе вычислений – кодировочные таблицы ASCII. Приложение должно реализовывать следующие операции: • генерация сверхвозрастающей последовательности (закрытого ключа); старший член последовательности – 100-битное число; в простейшем случае принимается $z = 8$ (для кодировки ASCII); • вычисление нормальной последовательности (открытого ключа); • зашифрование сообщения, состоящего из кириллицы; • расшифрование сообщения; • оценка времени выполнения операций зашифрования и расшифрования.	

№ пп	Формы текущего контроля	Примеры типовых заданий	Формируемая компетенция
		Проанализировать время выполнения операций зашифрования/расшифрования при увеличении числа членов ключевой последовательности; при использовании разных таблиц кодировки. Результаты оформить в виде отчета по установленным правилам.	
8	Информационное сообщение «Алгоритмы шифрования»	Подготовить информационное сообщение в форме презентации на тему «Алгоритмы шифрования». 1. Критерии оценки безопасности компьютерных систем 2. Основные принципы формирования пользовательских паролей. 3. Сравнительная характеристика симметричных и асимметричных алгоритмов 4. Классификация угроз информационной безопасности.	
9	Участие (достижения) в профессиональных конкурсах	Участие или призовое место в соревновании с официальным участием РГУ им. А.Н. Косыгина	
10	Научная и/или практическая работа	Участие в научной конференции или ином научном мероприятии в качестве представителя РГУ им. А.Н. Косыгина	

5.2. Критерии, шкалы оценивания текущего контроля успеваемости:

Наименование оценочного средства (контрольно-оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
Письменный отчет с результатами выполненных заданий лабораторной работы	Работа выполнена полностью. Нет ошибок в логических рассуждениях и в реализации задания в виде файла. Возможно наличие одной неточности или описки, не являющиеся следствием незнания или непонимания учебного материала и не влияющей на функциональные качества программы. Обучающийся показал полный объем знаний, умений в освоении, пройденных тем и применение их на практике. Работа зачтена.	4,25-5	5

Наименование оценочного средства (контрольно- оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
	Работа выполнена полностью, но выбран неэффективный алгоритм или метод реализации, обоснований шагов решения недостаточно. Допущена одна ошибка или два-три недочета, которые незначительно влияют на качество представленной работы. Работа зачтена.	3,25-4,25	4
	Допущены более одной ошибки или более двух-трех недочетов, которые оказывают значительное влияние на представляемый файл или компьютерную программу, ухудшают их информативность и функциональные возможности. Работа зачтена.	2,05-3,25	3
	Работа выполнена не полностью. Допущены грубые ошибки. Файлы не содержат необходимой информации, компьютерная программа выдаёт неправильные результаты при вычислении тестовых примеров. Работа не зачтена.	0-2	2
Информационное сообщение в форме презентации и доклад	Обучающийся, в процессе доклада по Презентации, продемонстрировал глубокие знания поставленной в ней проблемы, раскрыл ее сущность, слайды были выстроены логически последовательно, содержательно, приведенные иллюстрационные материалы поддерживали текстовый контент, была оформлена с учетом четких композиционных и цветовых решений. При изложении материала студент продемонстрировал грамотное владение терминологией, ответы на все вопросы были четкими, правильными, лаконичными и конкретными.	4,25-5	5
	Обучающийся, в процессе доклада по Презентации, продемонстрировал знания поставленной в ней проблемы, слайды были выстроены логически последовательно, но не в полной мере отражали содержание заголовков, приведенные иллюстрационные материалы не во всех случаях поддерживали текстовый контент, презентация не имела ярко выраженной идентификации с точки зрения единства оформления. При изложении материала студент не всегда корректно употреблял терминологию, отвечая на все вопросы, студент не всегда четко формулировал свою мысль.	3,25-4,25	4
	Обучающийся слабо ориентировался в материале, в рассуждениях не демонстрировал логику ответа, плохо владел профессиональной терминологией, не раскрывал суть проблем. Презентация была оформлена небрежно, иллюстрации не отражали текстовый контент слайдов.	2,05-3,25	3
	Обучающийся не выполнил задания	0-2	2

Наименование оценочного средства (контрольно- оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
Реферат	– работа выполнена самостоятельно, носит творческий характер, возможно содержание элементов научной новизны; – собран, обобщен и проанализирован достаточный объем литературных источников; – при написании и работы продемонстрированы: высокий уровень сформированности универсальных, общепрофессиональных и профессиональных компетенций, теоретические знания и наличие практических навыков; – работа правильно оформлена и своевременно представлена на кафедру, полностью соответствует требованиям, предъявляемым к содержанию и оформлению рефератов; - на защите освещены все вопросы исследования, ответы на вопросы профессиональные, грамотные, исчерпывающие, результаты исследования подкреплены статистическими критериями.	12,75-15	5
	– тема работы раскрыта, однако выводы и рекомендации не всегда оригинальны и / или не имеют практической значимости, есть неточности при освещении отдельных вопросов темы; – собран, обобщен и проанализирован необходимый объем профессиональной литературы, но не по всем аспектам исследуемой темы сделаны выводы и обоснованы практические рекомендации; – при написании и защите работы продемонстрирован: средний уровень сформированности универсальных, общепрофессиональных и профессиональных компетенций, наличие теоретических знаний и достаточных практических навыков; – работа своевременно представлена на кафедру, есть отдельные недостатки в ее оформлении; - в процессе защиты работы были даны неполные ответы на вопросы.	9,75-12,75	4
	– тема работы раскрыта частично, но в основном правильно, допущено поверхностное изложение отдельных вопросов темы;	6,15-9,75	3

Наименование оценочного средства (контрольно- оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
	– в работе недостаточно полно была использована профессиональная литература, выводы и практические рекомендации не отражали в достаточной степени содержание работы; – при написании и защите работы продемонстрирован удовлетворительный уровень сформированности универсальных, общепрофессиональных и профессиональных компетенций, поверхностный уровень теоретических знаний и практических навыков; – работа своевременно представлена на кафедру, однако не в полном объеме по содержанию и / или оформлению соответствует предъявляемым требованиям; в процессе защиты недостаточно полно изложены основные положения работы, ответы на вопросы даны неполные.		
	– содержание работы не раскрывает тему, вопросы изложены бессистемно и поверхностно, нет анализа практического материала, основные положения и рекомендации не имеют обоснования; – работа не оригинальна, основана на компиляции публикаций по теме; – при написании и защите работы продемонстрирован неудовлетворительный уровень сформированности универсальных, общепрофессиональных и профессиональных компетенций; – работа несвоевременно представлена на кафедру, не в полном объеме по содержанию и оформлению соответствует предъявляемым требованиям; на защите показаны поверхностные знания по исследуемой теме, отсутствие представлений об актуальных проблемах по теме работы, даны неверные ответы на вопросы.	0-6,15	2
Участие (достижение) в профессиональных конкурсах	– Обучающийся предоставил Приказ или Распоряжение об участии в мероприятии на внешней площадке, а также наградной документ (диплом 1, 2 или 3 место)	4,25-5	5
	– Обучающийся предоставил Приказ или Распоряжение об участии в мероприятии на площадке университета, а также наградной документ (диплом 1, 2 или 3 место)	3,25-4,25	4

Наименование оценочного средства (контрольно- оценочного мероприятия)	Критерии оценивания	Шкалы оценивания	
		100-балльная система	Пятибалльная система
	– Обучающийся предоставил Приказ или Распоряжение об участии в мероприятии на внешней площадке, а также документ, подтверждающий участие		
	– Обучающийся предоставил Приказ или Распоряжение об участии в мероприятии на площадке университета, а также документ, подтверждающий участие	2,05-3,25	3
	– Обучающийся не предоставил комплект документов, подтверждающих участие	0	2
Прохождение обучения по программам ДПО	– Обучающийся предоставил документ государственного образца о прохождении курсов дополнительного образования на внешних площадках	4,25-5	5
	– Обучающийся предоставил документ государственного образца о прохождении курсов дополнительного образования на площадке университета	3,25-4,25	4
	– Обучающийся предоставил сертификат о прохождении курсов дополнительного образования	2,05-3,25	3
	– Обучающийся не предоставил комплект документов, подтверждающих обучение	0	2

5.3. Промежуточная аттестация:

Форма промежуточной аттестации	Типовые контрольные задания и иные материалы для проведения промежуточной аттестации:	
Зачет: в устной форме по вопросам	Перечень вопросов: 1. Понятие информационной безопасности. Основные составляющие информационной безопасности. 2. Важность и сложность проблемы информационной безопасности 3. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность. 4. Понятие сервиса информационной безопасности. Идентификация и аутентификация.	ОПК-3 ИД-ОПК-3.1 ИД-ОПК-3.2 ИД-ОПК-3.3

5.4. Критерии, шкалы оценивания промежуточной аттестации учебной дисциплины:

Форма промежуточной аттестации	Критерии оценивания	Шкалы оценивания	
Наименование оценочного средства		100-балльная система	Пятибалльная система
Зачет по вопросам	Обучающийся: – демонстрирует знания, отличающиеся глубиной и содержательностью, даёт полный исчерпывающий ответ, как на основные вопросы, так и на дополнительные; – логично и доказательно раскрывает проблему, предложенную в вопросе; – свободно выполняет практические задания повышенной сложности, предусмотренные программой, демонстрирует системную работу с основной и дополнительной литературой.	25,5-30	5

Форма промежуточной аттестации	Критерии оценивания	Шкалы оценивания	
Наименование оценочного средства		100-балльная система	Пятибалльная система
	Ответ не содержит фактических ошибок и характеризуется глубиной, полнотой, уверенностью суждений, иллюстрируется примерами, в том числе из собственной практики.		
	Обучающийся: – показывает достаточное знание учебного материала, но допускает несущественные фактические ошибки, которые способен исправить самостоятельно, благодаря наводящему вопросу; – недостаточно раскрыта проблема по вопросу; – недостаточно логично построено изложение вопроса; – успешно выполняет предусмотренные в программе практические задания средней сложности, активно работает с основной литературой, – демонстрирует, в целом, системный подход к решению практических задач, к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. В ответе раскрыто, в основном, содержание вопроса, имеются неточности при ответе на дополнительные вопросы.	19,5-25,5	4
	Обучающийся: – показывает знания фрагментарного характера, которые отличаются поверхностностью и малой содержательностью, допускает фактические грубые ошибки; – не может обосновать закономерности и принципы, объяснить факты, нарушена логика изложения, отсутствует осмысленность представляемого материала, представления о межпредметных связях слабые; – справляется с выполнением практических заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой, допускает погрешности и ошибки при теоретических ответах и в ходе практической работы.	12,3-19,5	3

Форма промежуточной аттестации	Критерии оценивания	Шкалы оценивания	
Наименование оценочного средства		100-балльная система	Пятибалльная система
	Содержание вопроса раскрыто слабо, имеются неточности при ответе на основные и дополнительные вопросы, ответ носит репродуктивный характер. Неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.		
	Обучающийся, обнаруживает существенные пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой практических заданий. На большую часть дополнительных вопросов затрудняется дать ответ или не даёт верных ответов.	0-12,3	2

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:		
- Выполнение лабораторной работы	0-40	2 – 5
- Презентация	0-5	2 – 5
- Реферат	0-15	2 – 5
- участие (достижения) в профессиональных конкурсах	0-5	2 – 5
- научная и/или практическая работа	0-5	2 – 5
Промежуточная аттестация (зачет)	0-30	отлично хорошо
Итого за семестр зачет	0-100	удовлетворительно неудовлетворительно

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;
- проектная деятельность;
- проведение интерактивных лекций;
- поиск и обработка информации с использованием сети Интернет;
- дистанционные образовательные технологии;
- использование на лекционных занятиях видеоматериалов и наглядных пособий

7. ПРАКТИЧЕСКАЯ ПОДГОТОВКА

Практическая подготовка в рамках учебной дисциплины не реализуется.

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

Характеристика материально-технического обеспечения дисциплины соответствует требованиям ФГОС ВО.

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.
119071, г. Москва, Малый Калужский переулок, дом 1, строение 3	
аудитории для проведения занятий лекционного типа	комплект учебной мебели, технические средства обучения, служащие для представления учебной информации большой аудитории: – ноутбук; – проектор,

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.
	– экран
аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, по практической подготовке, групповых и индивидуальных консультаций	комплект учебной мебели, технические средства обучения, служащие для представления учебной информации большой аудитории: – ноутбук; – проектор, – экран
Помещения для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся
читальный зал библиотеки	– компьютерная техника; подключение к сети «Интернет»

Материально-техническое обеспечение учебной дисциплины при обучении с использованием электронного обучения и дистанционных образовательных технологий.

Необходимое оборудование	Параметры	Технические требования
Персональный компьютер/ноутбук/планшет, камера, микрофон, динамики, доступ в сеть Интернет	Веб-браузер	Версия программного обеспечения не ниже: Chrome 72, Opera 59, Firefox 66, Edge 79, Яндекс. Браузер 19.3
	Операционная система	Версия программного обеспечения не ниже: Windows 7, macOS 10.12 «Sierra», Linux
	Веб-камера	640x480, 15 кадров/с
	Микрофон	любой
	Динамики (колонки или наушники)	любые
	Сеть (интернет)	Постоянная скорость не менее 192 кБит/с

Технологическое обеспечение реализации программы осуществляется с использованием элементов электронной информационно-образовательной среды университета.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ/УЧЕБНОГО МОДУЛЯ

№ п/п	Автор(ы)	Наименование издания	Вид издания (учебник, УП, МП и др.)	Издательство	Год издания	Адрес сайта ЭБС или электронного ресурса (заполняется для изданий в электронном виде)	Количество экземпляров в библиотеке Университета
10.1 Основная литература, в том числе электронные издания							
1.	С. А. Нестеров	Основы информационной безопасности	учебник	Санкт-Петербург : Лань	2024	https://e.lanbook.com/book/370967	
2.	А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин.	Защита информации	учебное пособие	Москва : РИОР : ИНФРА-М	2023	https://znanium.com/catalog/product/1912992	
3.	О. В. Прохорова.	Информационная безопасность и защита информации	учебник для вузов	СПб: Лань	2023	https://e.lanbook.com/book/293009	
4.	С. М. Рацеев	Математические методы защиты информации	учебное пособие для вузов	СПб: Лань	2023	https://e.lanbook.com/book/326153	
5.	М. В. Тумбинская, М. В. Петровский	Комплексное обеспечение информационной безопасности на предприятии	учебник	Санкт-Петербург : Лань	2022	https://e.lanbook.com/book/207095	
10.2 Дополнительная литература, в том числе электронные издания							
1.	Ю. М. Краковский	Методы защиты информации пользователей.	учебное пособие для вузов	СПб: Лань	2021	https://e.lanbook.com/book/156401	
2.	Н.З. Емельянова, Т.Л. Партыка, И.И. Попов.	Защита информации в персональном компьютере	учебное пособие	Москва : РИОР : ИНФРА-М	2021	https://znanium.com/catalog/product/1189325	

3.	С.О. Крамаров, О.Ю. Митясова, С.В. Соколов	Криптографическая защита информации	учебное пособие	Москва : РИОР : ИНФРА-М	2023	https://znanium.com/catalog/product/1899016	
4.	Ю.Н. Сычев.	Защита информации и информационная безопасность	учебное пособие	Москва : РИОР : ИНФРА-М	2023	https://znanium.com/catalog/product/1912987	

10.3 Методические материалы (указания, рекомендации по освоению дисциплины (модуля) 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/
4.	ЭБС «ИВИС» http://dlib.eastview.com/
Профессиональные базы данных, информационные справочные системы	
1.	Scopus https://www.scopus.com (международная универсальная реферативная база данных, индексирующая более 21 тыс. наименований научно-технических, гуманитарных и медицинских журналов, материалов конференций примерно 5000 международных издательств);
2.	Scopus http://www.Scopus.com/
3.	Научная электронная библиотека eLIBRARY.RU https://elibrary.ru (крупнейший российский информационный портал в области науки, технологии, медицины и образования);

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
2.	Adobe Reader	свободно распространяемое
3.	Google Chrome	свободно распространяемое
4.	Spyder-Anaconda. Среда разработки на Python.	Свободно распространяемое
5.	Visual Studio Code	Свободно распространяемое

**ЛИСТ УЧЕТА ОБНОВЛЕНИЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ
ДИСЦИПЛИНЫ/МОДУЛЯ**

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

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