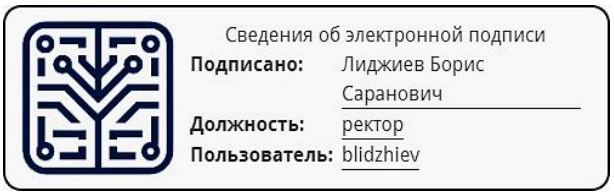
Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.



«04» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.02.02 СОВРЕМЕННАЯ КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ

Для направления подготовки:
09.03.01 Информатика и вычислительная техника
(уровень бакалавриата)

Типы задач профессиональной деятельности:
производственно-технологический

Направленность (профиль):
Информационные системы

Форма обучения:
очная, очно-заочная, заочная

г. Элиста, 2024

Разработчик: Горяев Владимир Михайлович, кандидат педагогических наук, заведующий кафедрой Математики и информационных технологий Автономной некоммерческой организации высшего образования «Информационно-технологический университет».

Рабочая программа разработана в соответствии с требованиями ФГОС ВО 09.03.01 Информатика и вычислительная техника (уровень бакалавриата), утв. Приказом Министерства образования и науки РФ № 929 от 19.09.2017 г.

СОГЛАСОВАНО:
Заведующий кафедрой
Математики и информационных технологий
АНО ВО ИТУ
канд. пед. наук Горяев В.М.

Протокол заседания кафедры № 01 от «04» июня 2024 г.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель освоения дисциплины: сформировать знания, умения и компетенции в области современной криптографии и стеганографии.

Задачи:

• раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии;

• ознакомить с основными видами шифров;

• ознакомить с современными стандартами криптографической защиты;

• дать представление об атаках на криптографические системы;

• раскрыть основные направления современной криптографии и стеганографии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Место дисциплины в учебном плане:

Блок: Блок 1. Дисциплины (модули).

Часть: формируемая участниками образовательных отношений, элективные дисциплины.

Осваивается (семестр):

очная форма обучения – 6

очно-заочная форма обучения – 7

заочная форма обучения - 7

3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-2 - способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

ПК-2 - способен разрабатывать компоненты программных комплексов и баз данных в соответствии с требованиями технического задания, используя современные инструментальные средства и технологии программирования, оформлять программную и пользовательскую документацию в соответствии с принятыми стандартами.

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2.** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов

ПК-2 Способен разрабатывать компоненты программных комплексов и баз данных в соответствии с требованиями технического задания, используя современные инструментальные средства и технологии программирования, оформлять программную и пользовательскую документацию в соответствии с принятыми стандартами	**ПК-2.1.** Выбирает современные инструментальные средства и технологии программирования для решения задач в профессиональной деятельности, оформляет программную и пользовательскую документацию в соответствии с принятыми стандартами	**Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных **Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами **Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Современная криптография и стеганография» для студентов всех форм обучения, реализуемых в АНО ВО ИТУ по направлению подготовки 09.03.01 Информатика и вычислительная техника составляет: 3 з.е. / 108 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)		
	Очная	Очно-заочная	Заочная
Аудиторные занятия	54	32	12
в том числе:			
Лекции	18	10	4
Практические занятия	18	10	4
Лабораторные работы	18	12	4
Самостоятельная работа	54	76	92
в том числе:			
часы на выполнение КР / КП	-	-	-
Промежуточная аттестация:			
Вид	Зачет – 6 сем.	Зачет – 7 сем.	Зачет – 7 сем.
Трудоемкость (час.)	-	-	4
Общая трудоемкость з.е. / час.	**3 з.е. / 108 час.**		

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№	Наименование темы дисциплины	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
Очная форма обучения					
1	Симметричные и асимметричные криптосистемы	4	4	4	13
2	Электронные цифровые подписи. Управление	4	4	4	13

№	Наименование темы дисциплины	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
	криптографическими ключами				
3	Стеганографические системы	5	5	5	14
4	Современные направления в криптографии и криптоанализе	5	5	5	14
	Итого (часов)	18	18	18	54
	Форма контроля:	**Зачет**			**-**
Очно-заочная форма обучения					
1	Симметричные и асимметричные криптосистемы	2	2	3	19
2	Электронные цифровые подписи. Управление криптографическими ключами	2	2	3	19
3	Стеганографические системы	3	3	3	19
4	Современные направления в криптографии и криптоанализе	3	3	3	19
	Итого (часов)	10	10	12	76
	Форма контроля:	**Зачет**			**-**
Заочная форма обучения					
1	Симметричные и асимметричные криптосистемы	1	1	1	23
2	Электронные цифровые подписи. Управление криптографическими ключами	1	1	1	23
3	Стеганографические системы	1	1	1	23
4	Современные направления в криптографии и криптоанализе	1	1	1	23
	Итого (часов)	4	4	4	92
	Форма контроля:	**Зачет**			**4**
	Всего по дисциплине:	**3 з.е. / 108 час.**			

СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

Тема 1. Симметричные и асимметричные криптосистемы

Основные классы симметричных криптосистем. Общие сведения о блочных шифрах. Генерирование блочных шифров. Алгоритмы блочного шифрования. Алгоритм DES и его модификации. Стандарт AES. Алгоритм Rijndael. Алгоритм RC6. Российский стандарт шифрования ГОСТ 28147–89. Алгоритмы SAFER, SAFER. Режимы применения блочных шифров. Потоковые шифры. Общие сведения о потоковых шифрах. Самосинхронизирующиеся шифры. Синхронные шифры. Примеры потоковых шифров.

Асимметричные системы шифрования. Криптосистема Эль-Гамаля. Криптосистема, основанная на проблеме Диффи-Хеллмана. Криптосистема Ривеста-Шамира-Адлемана. Криптосистемы Меркля-Хеллмана и Хора-Ривеста. Криптосистемы, основанные на эллиптических кривых.

Тема 2. Электронные цифровые подписи. Управление криптографическими ключами

Алгоритмы электронной цифровой подписи. Цифровые подписи, основанные на асимметричных криптосистемах. Стандарт цифровой подписи DSS. Стандарт цифровой подписи ГОСТ Р 34.10–94. Стандарт цифровой подписи ГОСТ Р 34.10–2001. Цифровые подписи, основанные на симметричных криптосистемах. Функции хэширования. Функция хэширования SHA. Функции хэширования SHA-256, SHA-512 и SHA-384. Функция хэширования ГОСТ Р 34.11–94. Функция хэширования MD5.

Система управления ключами. Управление ключами, основанное на системах с открытым ключом. Протокол обмена секретным ключом. Использование сертификатов. Протоколы аутентификации. Анонимное распределение ключей.

Тема 3. Стеганографические системы

Скрытие данных в неподвижных изображениях. Человеческое зрение и алгоритмы сжатия изображений. Скрытие данных в пространственной области. Скрытие данных в области преобразования.

Обзор стегоалгоритмов встраивания информации в изображения. Аддитивные алгоритмы. Стеганографические методы на основе квантования. Стегоалгоритмы, использующие фрактальное преобразование.

Скрытие данных в аудиосигналах. Скрытие данных в видеопоследовательностях. Современные стеганографические продукты.

Тема 4. Современные направления в криптографии и криптоанализе

Криптография в беспроводных сетях. Цифровая сотовая связь. Система безопасности GSM. Алгоритмы A3, A5, A8. Методы криптоанализа шифра A5. Безопасность телефонных переговоров. Беспроводные сети Wi-Fi. Методы шифрования WEP и WPA. Программные продукты, использующие шифрование.

Криптография в «Интернете вещей». Квантовая криптография и квантовые вычисления. Криптография и технология блокчейн. Криптографическая защита биометрических данных. Другие актуальные и перспективные направления криптографии.

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

Курсовая работа не предусмотрена

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

9.1. Рекомендуемая литература:

- Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2016. — 256 с. — ISBN 5-98003-002-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/90248.html
- Шелухин, О. И. Основы стеганографии. Часть 1. Скрытие данных в аудио- и текстовых файлах : учебное пособие / О. И. Шелухин, Бен Т. Б. К. Режеб. — Москва : Московский технический университет связи и информатики, 2015. — 129 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/61517.html
- Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102017.html

- Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — Москва : СОЛОН-Пресс, 2018. — 262 с. — ISBN 978-5-91359-173-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/90375.html
- Теоретико-числовые методы в криптографии : учебное пособие / составители Ф. Б. Тебуева, В. О. Антонов. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 107 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/75601.html
- Хасанов, Р. И. Основы стеганографии : учебное пособие / Р. И. Хасанов. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016. — 102 с. — ISBN 978-5-7410-1555-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/78809.html

9.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.

АНО ВО ИТУ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства.

Программное обеспечение, необходимое для осуществления образовательного процесса по дисциплине:

Лицензионное программное обеспечение (в том числе, отечественного производства):

Операционная система Windows Professional 10;

ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц;

Цифровой образовательный сервис «Личная студия обучающегося» (отечественное ПО);

Цифровой образовательный сервис «Личный кабинет преподавателя» (отечественное ПО);

Платформа проведения вебинаров (отечественное ПО);

Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО).

Информационная технология. Программа управления образовательным процессом.

Свободно распространяемое программное обеспечение (в том числе отечественного производства):

Мой Офис Веб-редакторы https://edit.myoffice.ru (отечественное ПО);

ПО OpenOffice.Org Calc - http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html;

ПО OpenOffice.Org.Base http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html;

ПО OpenOffice.org.Impress

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.Org Writer

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО Open Office.org Draw

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами.

9.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://window.edu.ru/ - единое окно доступа к образовательным ресурсам
2. http://www.iprbookshop.ru - Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний
3. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
4. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
5. https://www.garant.ru/ - справочная правовая система Гарант
6. https://gufo.me/ - справочная база энциклопедий и словарей
7. https://slovaronline.com - справочная база, полная поисковая система по всем доступным словарям, энциклопедиям и переводчикам в режиме Онлай
8. Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» https://reestr.digital.gov.ru/
9. Общество с ограниченной ответственностью «Интерактивные обучающие технологии» https://htmlacademy.ru/tutorial/php/mysql
10. Web-технологии https://htmlweb.ru/php/mysql.php

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для осуществления образовательного процесса по дисциплине представляют собой аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

Список аудиторий:

1. Лекционная аудитория, аудитория для групповых и индивидуальных консультаций.

2. Аудитория для проведения практических и семинарских занятий, текущего контроля и промежуточной аттестации.

3. Аудитория для самостоятельной работы обучающихся.

4. Многофункциональная аудитория для лиц с ограниченными возможностями здоровья, актовый зал, электронная библиотека.

5. Аудитория информационных технологий.

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины проводится в форме лекций, практических и/или лабораторных занятий, организации самостоятельной работы студентов, консультаций. Главное назначение лекции - обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у студентов ориентиры для самостоятельной работы над учебной дисциплиной.

Основной целью практических и/или лабораторных занятий является обсуждение наиболее сложных теоретических вопросов, их методологическая и методическая проработка, выполнение практических заданий.

Самостоятельная работа с учебной, учебно-методической и научной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с информационными базами, электронными образовательными ресурсами в электронной информационно-образовательной среде организации и сети Интернет.

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление и расширение теоретических знаний с целью их применения на уровне межпредметных связей;
- систематизация и закрепление полученных теоретических знаний и практических навыков;
- формирование умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;
- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;
- развитие научно-исследовательских навыков;
- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа является неотъемлемой частью образовательного процесса.

Самостоятельная работа предполагает инициативу самого обучающегося в процессе сбора и усвоения информации, приобретения новых знаний, умений и навыков и ответственность его за планирование, реализацию и оценку результатов учебной деятельности. Процесс освоения знаниями при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа по подготовке письменных работ должна:

- быть выполнена индивидуально (или являться частью коллективной работы);
- представлять собой законченную разработку (этап разработки), в которой анализируются актуальные проблемы по определенной теме и ее отдельных аспектов;
- отражать необходимую и достаточную компетентность автора;
- иметь учебную, научную и/или практическую направленность;
- быть оформлена структурно и логически последовательно;
- содержать краткие и четкие формулировки, убедительную аргументацию, доказательность и обоснованность выводов;
- соответствовать этическим нормам (правила цитирования и парафраз; ссылки на использованные библиографические источники; исключение плагиата, дублирования собственного текста и использования чужих работ).

Особенности организации образовательного процесса для обучающихся с ограниченными возможностями здоровья

Обучающиеся с ограниченными возможностями здоровья имеют свои специфические особенности восприятия и переработки учебного материала. Подбор и разработка учебных материалов должны производиться с учетом того, чтобы

предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально.

Выбор средств и методов обучения осуществляется самим преподавателям. При этом в образовательном процессе рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений обучающихся с ограниченными возможностями здоровья с научно-педагогическими работниками и другими обучающимися, создания комфортного психологического климата при освоении учебного материала.

Лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь; лица с ограниченными возможностями здоровья по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для лиц с ОВЗ в одной аудитории совместно с обучающимися, не имеющими ОВЗ, если это не создает трудностей для лиц с ОВЗ и иных обучающихся при прохождении аттестации;
- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся с ОВЗ необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);
- пользование необходимыми обучающимся с ОВЗ техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся с ОВЗ в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося с ОВЗ продолжительность сдачи экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении аттестации:

а) для лиц с нарушением зрения:

- задания и иные материалы для сдачи экзамена оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением, либо зачитываются ассистентом;
- письменные задания выполняются обучающимися с использованием клавиатуры с азбукой Брайля, либо надиктовываются ассистенту;

б) для лиц с нарушением слуха:

- с использованием информационной системы "Исток";
- аттестационные процедуры проводятся в электронной или письменной форме по выбору обучающихся.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

Приложение 1

Автономная некоммерческая организация высшего образования
«Информационно-технологический университет»
(АНО ВО ИТУ)

Фонд оценочных средств

Текущего контроля и промежуточной аттестации
по дисциплине (модулю)

Б1.В.ДЭ.02.02 СОВРЕМЕННАЯ КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ

Для направления подготовки:
09.03.01 Информатика и вычислительная техника
(уровень бакалавриата)

Типы задач профессиональной деятельности:
производственно-технологический

Направленность (профиль):
Информационные системы

Форма обучения:
очная, очно-заочная, заочная

г. Элиста, 2024

Результаты обучения по дисциплине

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**УК-2.2.** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов
ПК-2 Способен разрабатывать компоненты программных комплексов и баз данных в соответствии с требованиями технического задания, используя современные инструментальные средства и технологии программирования, оформлять программную и пользовательскую документацию в соответствии с принятыми стандартами	**ПК-2.1.** Выбирает современные инструментальные средства и технологии программирования для решения задач в профессиональной деятельности, оформляет программную и пользовательскую документацию в соответствии с принятыми стандартами	**Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных **Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами **Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации

Показатели оценивания результатов обучения

Шкала оценивания			
Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
УК-2.2. Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения			
Не знает: методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Не умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Не владеет:** способами решения конкретных задач в профессиональной	**Поверхностно знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **В целом умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но испытывает затруднения **В целом владеет:**	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения, но допускает несущественные ошибки **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но иногда	**Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной

деятельности, исходя из действующих норм, имеющихся ресурсов	способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но испытывает сильные затруднения	допускает небольшие ошибки **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но иногда допускает ошибки	деятельности, исходя из действующих норм, имеющихся ресурсов
ПК-2.1. Выбирает современные инструментальные средства и технологии программирования для решения задач в профессиональной деятельности, оформляет программную и пользовательскую документацию в соответствии с принятыми стандартами			
Не знает: основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных **Не умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами **Не владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации	**Поверхностно знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных **В целом умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами, но испытывает затруднения **В целом владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации, но испытывает сильные затруднения	**Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных, но допускает несущественные ошибки **Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами, но иногда допускает небольшие ошибки **Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации, но иногда допускает ошибки	**Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных **Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами **Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации

Оценочные средства

Задания для текущего контроля

Темы устного доклада
Раздел 1

1. Принципы криптографической защиты информации.
2. Шифр DES. Его «сильные» и «слабые» стороны.
3. Обзор развития способов проектирования блочных шифров.
4. Криптосистема RSA. Практическое использование.
5. Криптоанализ шифров перестановки.
6. Криптоанализ шифров замены.
7. Блочные шифры и их ключевая система.
8. Сеть Файстеля.
9. Дифференциальный криптоанализ.
10. Криптосистема Эль-Гамаля.
11. Криптосистема Гольдвассер-Микали.
12. Криптосистема Блюма-Гольдвассер.
13. Криптосистема Меркла-Хэллмана.
14. Протоколы типа «запрос-ответ» с использованием симметричных алгоритмов.
15. Жизненный цикл ключей.
16. Сопоставление блочных и поточных шифров.
17. Комбинированные криптосистемы.
18. Шифрование методом гаммирования.
19. Шифры сложной замены.
20. Американский стандарт AES.

Раздел 2

1. Хэш-функции. Тенденции в способах построения.
2. Криптографические хэш-функции и требования к ним.
3. Криптосистема Диффи-Хэллмана.
4. Понятие электронной цифровой подписи и требования к ней.
5. Подпись RSA, Эль-Гамаля.
6. Подпись Фиата-Шамира.
7. Подпись Онга-Шнорра-Шамира.
8. Неотрицаемая подпись Шаума-ван-Антверпена.
9. Стандарты цифровой подписи.
10. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
11. Шифр Эль-Гамаля на эллиптической кривой.
12. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.
13. Односторонняя передача ключей с использованием симметричного шифрования и хэширования.
14. Базовый протокол Kerberos.
15. Одношаговый протокол передачи ключа с использованием асимметричного шифрования.
16. Одноразовые пароли на основе однонаправленной функции.
17. Односторонняя и взаимная идентификация с использованием цифровой подписи и временных меток.
18. Протокол распределения ключей Otway-Rees.
19. Протокол формирования общего ключа для конференцсвязи.

20. Функции центра нотаризации.

Раздел 3

1. Свойства зрения, которые нужно учитывать при построении стегоалгоритмов.
2. Принципы сжатия изображений.
3. Скрытие данных в пространственной области.
4. Краткое описание стандарта MPEG и возможности внедрения данных.
5. Критерии секретности стегосистем.
6. Основные методы построения стегосистем.
7. Основы стегоанализа.
8. Схема внедрения данных в изображение.
9. Пропускная способность стегоканала.
10. Виды квантования, их различия.
11. Скрытие данных в аудиосигналах.
12. Методы маскирования цифровых водяных знаков.
13. Скрытие данных в видеопоследовательностях.
14. Статистики JPEG-файлов, используемые при стегоанализе.
15. Объективные метрики для оценки качества видеокодеков.
16. Методика исследования статистических критериев оценки искажений файлов-контейнеров.
17. Основные области применения цифровых водяных знаков.
18. Математическая модель стегосистемы.
19. Стеганографические протоколы.
20. Атаки на стегосистемы и противодействия им.

Раздел 4

1. Юридические вопросы криптографической деятельности.
2. Криптография в программных продуктах: PGP, Skype и др.
3. Криптографические протоколы.
4. Проблемы передачи информации и их комплексное решение.
5. Протоколы PPTP и MPPE.
6. Протоколы IPSec, AH, ESP, ISAKMP, Oakley.
7. Стек протоколов SSL/TLS.
8. Протоколы типа «запрос-ответ» с использованием симметричных алгоритмов.
9. Описание функций сервера имен абонентов и сертификационного центра.
10. Особенности электронных платежных систем.
11. Шифрование в сетевых протоколах.
12. Цифровые сертификаты. Получение и регистрация сертификата.
13. Проблема аутентификации данных.
14. Квантовая криптография и квантовые вычисления.
15. Криптография в «Интернете вещей».
16. Криптография в «Интернете вещей».
17. Криптографическая защита биометрических данных.
18. Методы шифрования WEP и WPA.
19. Программные продукты, использующие шифрование.
20. Криптография в беспроводных сетях.

Оценка доклада производится по шкале «зачтено» / «не зачтено».

Пример теста:

1.Обеспечивает скрытность информации в информационных массивах	
a)	стеганография
b)	криптоанализ
c)	криптография
d)	криптология

2. Способы защиты информации:	
a)	стеганография
b)	физическая защита материального носителя информации от противника
c)	криптография
d)	форматирование

3. Основные цели криптографии:	
a)	обеспечение конфиденциальности данных
b)	обеспечение целостности данных
c)	обеспечение аутентификации
d)	обеспечение идентификации

4. Верны ли утверждения: A) Способ защиты информации – наиболее надежный и распространенный в наши дни – криптографический. B) Шифр – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты. Подберите правильный ответ	
a)	A - да, B - нет
b)	A - нет, B - да
c)	A - нет, B - нет
d)	A - да, B - да

5. Верны ли утверждения: A) Симметричная криптография является одним из ключевых компонентов технологии блокчейн. B) Роторные машины сделали возможными сложные методы шифрования, но именно изобретение компьютера подняло криптографию на совершенно новый уровень. Подберите правильный ответ	
a)	A - да, B - нет
b)	A - да, B - да
c)	A - нет, B - нет
d)	A - нет, B - да

6. Укажите соответствие между базовым классом симметричных криптосистем и его описанием:	
a) Подстановки	1) вид преобразований, заключающийся в замене символов исходного текста на другие по более или менее сложному правилу
b) Перестановки	2) вид преобразований, заключающийся в перестановке местами символов исходного текста по некоторому правилу
c) Гаммирование	3) вид преобразований, при котором его символы складываются (по модулю, равному размеру алфавита) с символами псевдослучайной последовательности, вырабатываемой по некоторому правилу

7. Объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей -	
a)	стеганография

b)	криптоанализ
c)	криптография
d)	криптология

8. В асимметричных системах шифрования	
a)	открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
b)	для зашифрования и расшифрования используется один ключ
c)	секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
d)	секретный и открытый ключи доступны всем желающим

9. Верны ли утверждения: А) Способ защиты информации – наиболее надежный и распространенный в наши дни – криптографический. В) Шифр – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты. Подберите правильный ответ	
a)	А - да, В - нет
b)	А - нет, В - да
c)	А - нет, В - нет
d)	А - да, В - да

10. Верны ли утверждения: А) Симметричная криптография является одним из ключевых компонентов технологии блокчейн. В) Роторные машины сделали возможными сложные методы шифрования, но именно изобретение компьютера подняло криптографию на совершенно новый уровень. Подберите правильный ответ	
a)	А - да, В - нет
b)	А - да, В - да
c)	А - нет, В - нет
d)	А - нет, В - да

11.Укажите соответствие между базовым классом симметричных криптосистем и его описанием:	
a) Подстановки	a) вид преобразований, заключающийся в замене символов исходного текста на другие по более или менее сложному правилу
b) Перестановки	b) вид преобразований, заключающийся в перестановке местами символов исходного текста по некоторому правилу
c) Гаммирование	c) вид преобразований, при котором его символы складываются (по модулю, равному размеру алфавита) с символами псевдослучайной последовательности, вырабатываемой по некоторому правилу

12.Верны ли утверждения: А) Асимметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации – ключа, одинакового для отправителя и получателя сообщения. В) Симметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, и, возможно, открытый ключ, но неизвестен закрытый ключ, известный только получателю. Подберите правильный ответ	
a)	А - да, В - нет
b)	А - да, В - да
c)	А - нет, В - нет
d)	А - нет, В - да

13. Если открытый текст представляется в виде бинарной последовательности, то гаммирование осуществляется по модулю	
a)	2

b)	8
c)	10
d)	16

14. открытый текст представляется в виде последовательности байтов, то гаммирование осуществляется по модулю	
a)	2
b)	10
c)	256
d)	16

15. К _____ методам подстановки относятся пропорциональные или монофонические шифры, в которых уравнивается частота появления зашифрованных знаков для защиты от раскрытия с помощью частотного анализа	
a)	многоалфавитным
b)	одноалфавитным
c)	цифровым
d)	знаковым

16. Если открытый текст - последовательность цифр, то гаммирование осуществляется по модулю	
a)	2
b)	10
c)	256
d)	16

17. Поставьте в соответствие типу гаммирования условие представления открытого текста:	
a) По модулю 2	1) если открытый текст представляется в виде бинарной последовательности
b) По модулю 10	2) если открытый текст представляется в виде последовательности цифр
c) По модулю 256	3) если открытый текст представляется в виде последовательности байтов

18. Верны ли утверждения: A) Маршрутные перестановки основаны на некоторой геометрической фигуре. B) Криптография – наука о защите информации от прочтения ее посторонними. Подберите правильный ответ	
a)	A - да, B - нет
b)	A - да, B - да
c)	A - нет, B - нет
d)	A - нет, B - да

19.Выберите название таблицы (кодировки, набора), в которой некоторым распространённым печатным и непечатным символам сопоставлены числовые коды.	
a)	ASCII
b)	RGB
c)	WEB
d)	CMYK

20. К восьмибитным кодировкам относятся:	
a)	ASCII
b)	KOI8
c)	UTF8
d)	Windows-1251

21.К основным аппаратным средствам защиты информации относятся:	
a)	устройства для ввода идентифицирующей пользователя информации (магнитных и

	пластиковых карт, отпечатков пальцев и т.п.)
b)	устройства для шифрования информации
c)	устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы)
d)	программы шифрования информации

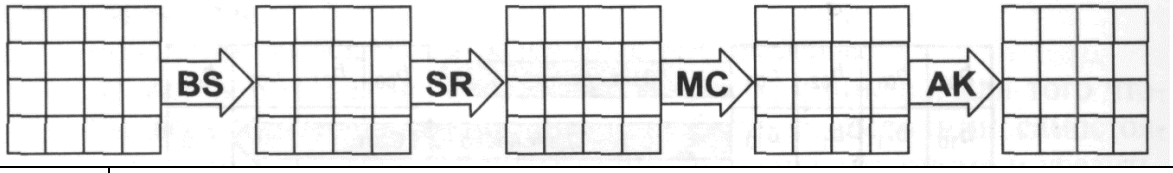
22.К основным программным средствам защиты информации относятся:	
a)	программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т.п.) от несанкционированного изменения, использования и копирования
b)	устройства для шифрования информации
c)	устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы)
d)	программы шифрования информации

23. К вспомогательным программным средствам защиты информации относятся:	
a)	программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т.п.)
b)	программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий
c)	устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы)
d)	программы шифрования информации

24.Верны ли утверждения? A) Во всех распространенных операционных системах имеются встроенные средства шифрования файлов. B) Символьное кодирование — способ кодирования информации, которая кодируется с помощью чисел. Подберите правильный ответ.	
a)	A - да, B - нет
b)	A - да, B - да
c)	A - нет, B - нет
d)	A - нет, B - да

25.Укажите соответствие между способами кодирования и их определениями:	
a) Числовое	1) кодирование, при котором информация кодируется с помощью чисел
b) Символьное	2) кодирование, при котором информация кодируется с помощью символов того же алфавита, что и исходящий текст
c) Графическое	3) кодирование, при котором информация кодируется с помощью рисунков или значков

26.Программно-аппаратная реализация криптографических систем и средств в мировой практике основывается на криптографических стандартах:	
a)	DES
b)	ГОСТ 28147 — 89
c)	AES
d)	RC4

27.Выберите, что представлено на рисунке	
	
a)	обобщенная схема шифрования в алгоритме DES

b)	раунд алгоритма AES
c)	схема алгоритма ГОСТ 28147-89
d)	выработка гаммы шифра в режиме гаммирования

28.Функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом, -	
a)	хеш-функция
b)	функция Фибоначчи
c)	производная
d)	функция Виженера

29.На рисунке изображена:

a)	хеш-функция
b)	схема проверки электронной подписи
c)	схема формирования электронной цифровой подписи
d)	функция Виженера

30._____ — это двоичное сжатое представление тела основного документа, формируемое хэшированием	
a)	Хэш-значение
b)	RSA
c)	Аутентификация
d)	Функция Виженера

31.К алгоритмам цифровой подписи относятся:	
a)	RSA
b)	EGSA
c)	DSA
d)	MSA

32.Законодательством РФ прописаны следующие виды электронной цифровой подписи:	
a)	простая или ПЭП
b)	неквалифицированная или НЭП
c)	квалифицированная или КЭП
	двойная зашифрованная или ДЗЭП

33.Верны ли утверждения:

A) Усиленная электронная квалифицированная подпись является наиболее защищенным вариантов ЭП. B) Хэширование служит и для обнаружения изменений в теле документа, т.е. используется для образования криптографической контрольной суммы. Подберите правильный ответ	
a)	A - да, B - нет
b)	A - да, B - да
c)	A - нет, B - нет
d)	A - нет, B - да

34.Односторонняя аутентификация позволяет:	
a)	подтвердить подлинность только одной стороны информационного обмена
b)	обнаружить нарушение целостности передаваемой информации
c)	обнаружить проведение атаки типа «повтор передачи»
d)	гарантировать, что передаваемыми аутентификационными данными может воспользоваться только проверяющая сторона
e)	получить дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с тем партнером, которому были предназначены аутентификационные данные

35. Электронная цифровая подпись содержит следующую информацию:	
a)	дату подписи
b)	срок окончания действия ключа данной подписи
c)	информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы)
d)	идентификатор подписавшего (имя открытого ключа)
e)	собственно цифровую подпись
f)	QR-код

36. Выберите алгоритмы хэширования:	
a)	ГОСТ Р34.11–94.
b)	MD (Message Digest)
c)	SHA-1 (Secure Hash Algoritm)
d)	RC4 (от англ. Rivest cipher 4 или Ron’s code)

37. Электронная цифровая подпись обладает следующими основными достоинствами рукописной подписи:	
a)	удостоверяет, что подписанный текст исходит от лица, поставившего подпись
b)	не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом
c)	гарантирует целостность подписанного текста
d)	гарантирует репликацию подписанного текста

38.Функция хэширования должна обладать следующими свойствами:	
a)	хэш-функция может быть применена к аргументу любого размера
b)	выходное значение хэш-функции имеет фиксированный размер
c)	хэш-функцию h(x) достаточно просто вычислить для любого x
d)	хэш-функция должна быть многонаправленной

Оценка формируется следующим образом:

- оценка «отлично» - 85-100% правильных ответов;
- оценка «хорошо» - 70-84% правильных ответов;
- оценка «удовлетворительно» - 40-69% правильных ответов;
- оценка «неудовлетворительно» - менее 39% правильных ответов.

Промежуточная аттестация

Примерные вопросы к зачету:

1. Алгоритмы симметричного шифрования
2. Криптосистемы с открытым ключом, однонаправленные функции
3. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
4. Прямая и арбитражная ЭП
5. Электронная подпись
6. Однонаправленные хэш-функции.
7. Алгоритм шифрования RSA
8. Схема распределения ключей Диффи-Хеллмана на основе эллиптических кривых.
9. Алгоритм шифрования DES, тройной DES
10. Алгоритм электронной подписи на основе эллиптических кривых ECDSA
11. Алгоритм шифрования Эль-Гамаля
12. Криптография с использованием эллиптических кривых
13. Алгоритм шифрования Blowfish
14. Квантовая криптография
15. Алгоритм хеширования MD5
16. Сеть Фейстеля
17. Система распределения ключей Диффи-Хеллмана
18. Нелинейные регистры сдвига с обратной связью
19. Гаммирование, линейный регистр сдвига с обратной связью
20. Программные датчики ПСП чисел
21. Предметная область стеганографии. Классификация стеосистем
22. Алгоритмы создания цифровых водяных знаков
23. Алгоритмы стеганографического скрытия информации в пространственном представлении контейнеров-изображений
24. Алгоритмы стеганографического скрытия информации в частотном представлении контейнеров-изображений
25. Алгоритмы стегоанализа

Критерии оценки при проведении промежуточной аттестации

Оценивание знаний обучающихся осуществляется по 4-балльной шкале при проведении экзаменов и зачетов с оценкой (оценки «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно») или 2-балльной шкале при проведении зачета («зачтено», «не зачтено»).

При прохождении обучающимися промежуточной аттестации оцениваются:

1. Полнота, четкость и структурированность ответов на вопросы, аргументированность выводов.

2. Качество выполнения практических заданий (при их наличии): умение перевести теоретические знания в практическую плоскость; использование правильных форматов и методологий при выполнении задания; соответствие результатов задания поставленным требованиям.

3. Комплексность ответа: насколько полно и всесторонне обучающийся раскрыл тему вопроса и обратился ко всем ее аспектам.

Критерии оценивания

4-балльная шкала и 2-балльная шкалы	**Критерии**
«Отлично» или «зачтено»	1. Полные и качественные ответы на вопросы, охватывающие все необходимые аспекты темы. Обучающийся обосновывает свои выводы с использованием соответствующих фактов, данных или источников, демонстрируя глубокую аргументацию. 2. Обучающийся успешно переносит свои теоретические знания в практическую реализацию. Выполненные задания соответствуют высокому уровню качества, включая использование правильных форматов, методологий и инструментов. 3. Обучающийся анализирует и оценивает различные аспекты темы, демонстрируя способность к критическому мышлению и самостоятельному исследованию.
«Хорошо» или «зачтено»	1. Обучающийся предоставляет достаточно полные ответы на вопросы с учетом основных аспектов темы. Ответы обучающегося имеют ясную структуру и последовательность, делая их понятными и логически связанными. 2. Обучающийся способен применить теоретические знания в практических заданиях. Выполнение задания в целом соответствует требованиям, хотя могут быть некоторые недочеты или неточные выводы по полученным результатам. 3. Обучающийся представляет хорошее понимание темы вопроса, охватывая основные аспекты и направления ее изучения. Ответы обучающегося содержат достаточно информации, но могут быть некоторые пропуски или недостаточно глубокие суждения.
«Удовлетворительно» или «зачтено»	1. Ответы на вопросы неполные, не охватывают всех аспектов темы и не всегда структурированы или логически связаны. Обучающийся предоставляет верные выводы, но они недостаточно аргументированы или основаны на поверхностном понимании предмета вопроса. 2. Обучающийся способен перенести теоретические знания в практические задания, но недостаточно уверен в верности примененных методов и точности в их выполнении. Выполненное задание может содержать некоторые ошибки, недочеты или расхождения. 3. Обучающийся охватывает большинство основных аспектов темы вопроса, но демонстрирует неполное или поверхностное их понимание, дает недостаточно развернутые объяснения.
«Неудовлетворительно» или «не зачтено»	1. Обучающийся отвечает на вопросы неполно, не раскрывая основных аспектов темы. Ответы обучающегося не структурированы, не связаны с заданным вопросом, отсутствует их логическая обоснованность. Выводы, предоставляемые обучающимся, представляют собой простые утверждения без анализа или четкой аргументации. 2. Обучающийся не умеет переносить теоретические знания в практический контекст и не способен применять их для выполнения задания. Выполненное задание содержит много ошибок, а его результаты не соответствуют поставленным требованиям и (или) неправильно интерпретируются.

	3. Обучающийся ограничивается поверхностным рассмотрением темы и не показывает понимания ее существенных аспектов. Ответ обучающегося частичный или незавершенный, не включает анализ рассматриваемого вопроса, пропущены важные детали или связи.

ФОС для проведения промежуточной аттестации одобрен на заседании кафедры (Протокол заседания кафедры № 01 от «04» июня 2024 г.).