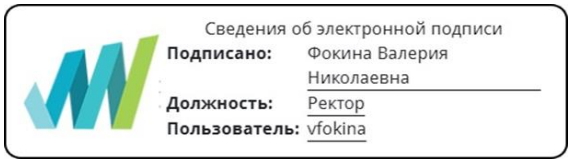
Автономная некоммерческая организация высшего образования
«ОТКРЫТЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА»

УТВЕРЖДАЮ:

Ректор АНО ВО ОУЭП, Фокина В.Н.



«19» апреля 2023 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

Разработчик: канд. тех. наук, Колесников С.М.
Протокол заседания кафедры «Информатики»
№ 27-03 от 27.03.2023 г.

Москва – 2023

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 «Открытый университет экономики, управления и права» 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 по компетенциям, представлено на сайте в разделе «оценочные материалы».

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.

Программное обеспечение АНО ВО ОУЭП, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных технологиях:

- тренинговые и тестирующие программы;
- интеллектуальные роботизированные системы оценки качества выполнения работ.

Информационные и роботизированные системы, программные комплексы, программное обеспечение для доступа к компьютерным обучающим, тренинговым и тестирующим программам:

- ПК «КОП»;
- ИР «Каскад».

Программное обеспечение, необходимое для реализации дисциплины:

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

Операционная система Windows Professional 10

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

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

Платформа проведения вебинаров (отечественное ПО)

Информационная технология. Онлайн тестирование цифровой платформы Ровеб (отечественное ПО)

Электронный информационный ресурс. Экспертный интеллектуальный информационный робот Аттестация асессоров (отечественное ПО)

Информационная технология. Аттестационный интеллектуальный информационный робот контроля оригинальности и профессионализма «ИИР КОП» (отечественное ПО)

Электронный информационный ресурс «Личная студия обучающегося» (отечественное ПО)

Свободно распространяемое программное обеспечение:

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. https://gufo.me/ - справочная база энциклопедий и словарей Gufo.me
2. https://slovaronline.com - поисковая система по всем доступным словарям и энциклопедиям
3. Реестр профессиональных стандартов https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/
4. Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» https://reestr.digital.gov.ru/
5. Общество с ограниченной ответственностью «Интерактивные обучающие технологии» https://htmlacademy.ru/tutorial/php/mysql
6. Web-технологии https://htmlweb.ru/php/mysql.php
7. Научная электронная библиотека. http://elibrary.ru
8. Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний http://www.iprbookshop.ru
9. Справочно-правовая система «Гарант»;
10. Справочно-правовая система «Консультант Плюс»

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине представлено в приложении - «Сведения о материально-техническом обеспечении программы высшего образования – программы бакалавриата направления подготовки 09.03.01 Информатика и вычислительная техника

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Продуктивность усвоения учебного материала во многом определяется интенсивностью и качеством самостоятельной работы студента. Самостоятельная работа предполагает формирование культуры умственного труда, самостоятельности и инициативы в поиске и приобретении знаний; закрепление знаний и навыков, полученных на всех видах учебных занятий; подготовку к предстоящим занятиям, экзаменам; выполнение контрольных работ.

Самостоятельный труд развивает такие качества, как организованность, дисциплинированность, волю, упорство в достижении поставленной цели, вырабатывает умение анализировать факты и явления, учит самостоятельному мышлению, что приводит к развитию и созданию собственного мнения, своих взглядов. Умение работать

самостоятельно необходимо не только для успешного усвоения содержания учебной программы, но и для дальнейшей творческой деятельности.

Основу самостоятельной работы студента составляет работа с учебной и научной литературой. Из опыта работы с книгой (текстом) следует определенная последовательность действий, которой целесообразно придерживаться. Сначала прочитать весь текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом (не запоминать, а понять общий смысл прочитанного). Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом.

Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать.

Результаты конспектирования могут быть представлены в различных формах:

- **План** – это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект.
- **Конспект** – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов.
- **План-конспект** – это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.
- **Текстуальный конспект** – это воспроизведение наиболее важных положений и фактов источника.
- **Свободный конспект** – это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.
- **Тематический конспект** – составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

В процессе изучения материала источника, составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым, удобным для работы.

Подготовка к практическому занятию включает 2 этапа:

Первый этап – организационный;

Второй этап - закрепление и углубление теоретических знаний.

На первом этапе студент планирует свою самостоятельную работу, которая включает:

- уяснение задания на самостоятельную работу;
- подбор рекомендованной литературы;
- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В

процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.

Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам.

В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь.

При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

Методические рекомендации для обучающихся с ОВЗ и инвалидов по освоению дисциплины

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья имеют возможность изучать дисциплину по индивидуальному плану, согласованному с преподавателем и администрацией АНО ВО ОУЭП.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения.

При освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья по индивидуальному плану предполагаются: изучение дисциплины с использованием информационных средств; индивидуальные консультации с преподавателем (разъяснение учебного материала и углубленное изучение материала), индивидуальная самостоятельная работа.

В процессе обучения студентам из числа инвалидов и лиц с ограниченными возможностями здоровья информация предоставляется в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа (с возможностью увеличения шрифта).

В случае необходимости информация может быть представлена в форме аудиофайла.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Индивидуальные консультации с преподавателем проводятся по отдельному расписанию, утвержденному заведующим кафедрой (в соответствии с индивидуальным графиком занятий обучающегося).

Индивидуальная самостоятельная работа обучающихся проводится в соответствии с рабочей программой дисциплины и индивидуальным графиком занятий.

Текущий контроль по дисциплине осуществляется в соответствии с фондом оценочных средств, в формах адаптированных к ограничениям здоровья и восприятия информации обучающихся

Приложение 1

Автономная некоммерческая организация высшего образования
«ОТКРЫТЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА»

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

Москва – 2023

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 деятельности, исходя из действующих норм, имеющихся ресурсов	**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:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но испытывает сильные затруднения	**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 допускает небольшие ошибки **Владеет:** способами решения конкретных задач в	**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

		профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но иногда допускает ошибки	
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

Разъясните основные понятия:

№	Понятие	Определение
1.	Стеганографические методы	Стеганографические методы позволяют скрывать секретные сообщения путем их встраивания в послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

2.	Криптография	Взаимно-однозначное математическое преобразование, зависящее от ключа (секретного параметра преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок зашифрованной информации, также представленной в цифровой кодировке.
3.	Шифрование	Процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц.
4.	Расшифрование	Процесс преобразования шифротекста в открытый текст.
5.	Симметричная криптосистема	Криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи.
6.	Асимметричная криптосистема	Асимметричная криптосистема использует пару ключей, один из которых является открытым, а другой – закрытым, известным только его владельцу.
7.	Криптоанализ	Наука о методах вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным.
8.	Криптоаналитическая атака	Попытка проведения криптоанализа шифра.
9.	Взломом шифра	Взломом, или вскрытием шифра является успешная криптоаналитическая атака, в результате которой противнику становится известным содержание зашифрованного сообщения.
10.	Стойкость шифра	Стойкость шифра – это его способность противостоять криптоаналитическим атакам.

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что представляет собой стеганографическая система?	Стеганографическая система или стегосистема – это совокупность методов и средств, которые используются для формирования скрытого канала передачи информации. Она содержит контейнер и сообщение. Контейнер – любая открытая информация, предназначенная для сокрытия тайных сообщений.

		Сообщение – конфиденциальная информация любого типа (например, текст, изображение, аудиоданные), подлежащая скрытию.
2.	Какие существуют методы компьютерной стеганографии?	Методы компьютерной стеганографии основаны на использовании специальных свойств компьютерных форматов, к которым относятся: – использование специальных свойств полей форматов текстовых файлов, не отображаемых на экране; – скрытие в неиспользуемых местах носителей информации секретной информации; – использование зарезервированных для расширения полей форматов данных или нечитаемых данных для устройств, которым предназначен носитель информации.
3.	Что такое криптоанализ?	Наука о методах вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным.
4.	В каких случаях целесообразно использовать криптографическую защиту?	Криптография применяется: – при защите конфиденциальности информации, передаваемой по открытым каналам связи; – аутентификации (подтверждении подлинности) передаваемой
		информации; – защите конфиденциальной информации при ее хранении на открытых носителях; – обеспечении целостности информации при ее передаче по открытым каналам связи или хранении на открытых носителях; – обеспечении неоспоримости, передаваемой по сети информации; – защите программного обеспечения и других информационных ресурсов от несанкционированного использования и копирования.

5.	Что представляет собой шифрование способом перестановки?	При использовании способа перестановки символы открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом. При расшифровании применяется обратная перестановка.
6.	В чем состоит основное достоинство многоалфавитной подстановки?	Главное достоинство многоалфавитной подстановки состоит в том, что в шифротексте маскируется частота появления различных символов открытого текста, поэтому криптоаналитик не может при вскрытии шифра использовать частотный словарь букв естественного языка.
7.	Что представляет собой побайтное шифрование?	Побайтное шифрование является разновидностью шифрования с применением многоалфавитной подстановки, при котором каждый следующий байт открытого текста складывается с предыдущим байтом, а нулевой байт открытого текста — с последним байтом.
8.	Что представляет собой шифрование способом гаммирования?	При гаммировании шифротекст получается путем наложения на открытый текст гаммы шифра с помощью какой-либо обратимой операции (например, поразрядного сложения по модулю 2).
9.	Что такое электронная цифровая подпись?	Электронная цифровая подпись – это относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже — отдельно) с подписываемым с ее помощью документом. Механизм ЭЦП состоит из двух
		процедур: получение (простановка) подписи с помощью секретного ключа автора документа и проверка ЭЦП при помощи открытого ключа автора документа.

Тестовые задания:

1	Электронные и электронно-механические устройства, включаемые в состав технических средств компьютерной системы и выполняющие некоторые функции обеспечения информационной безопасности, называются: a) аппаратными средствами защиты информации; b) антивирусной программой; **c) криптографической системой защиты информации;** d) электронным сторожем.
2	Криптосистема, в которой при шифровании и расшифровании используются разные ключи, называется a) двухфазной системой; b) ключевой системой; c) симметричной криптосистемой; **d) асимметричной криптосистемой.**
3	Процесс преобразования шифротекста в открытый текст, называется: a) шифрованием; b) открытием кода; **c) расшифрованием;** d) преобразованием кода.
4	Криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи, называется: **a) симметричной криптосистемой;** b) продольной криптосистемой; c) простой ключевой системой;
	d) однородной кодовой системой.

5	Процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц: a) криптографированием; b) дешифрованием; c) **шифрованием;** d) ниделированием.
6	Однозначное распознавание уникального имени субъекта компьютерной системы, называется: a) рекриацией; **b) идентификацией;** c) паспортеризацей.
7	Порция секретной информации (секретный ключ), необходимая для встраивания и извлечения сообщения из контейнера. **Стеганографический ключ**
8	Канал передачи заполненных стегоконтейнеров. Стеганографический канал образует скрытый канал передачи сообщений, когда неочевиден сам факт передачи секретной информации. **Стеганографический канал**
9	Атрибут электронного документа, который позволяет установить авторство и неизменность после подписания, называется: a) *астрибутивом;* **b) *электронной подписью;*** c) *провайзером.*
10	Действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости, называется: a) спинанием;

	b) инкременцией системы; **c) атакой на компьютерную систему.**

Ключ к тестовым заданиям

1	**2**	**3**	**4**	**5**
c	d	c	a	c
6	**7**	**8**	**9**	**10**
b	Стеганографический ключ	Стеганографический канал	b	c

Критерии оценки при проведении промежуточной аттестации

Оценивание знаний студентов 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 студентами 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 студент 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. Студент обосновывает свои выводы с использованием соответствующих фактов, данных или источников, демонстрируя глубокую аргументацию. 2. Студент успешно переносит свои теоретические знания в практическую реализацию. Выполненные задания соответствуют высокому уровню качества, включая использование правильных форматов, методологий и инструментов. 3. Студент анализирует и оценивает различные аспекты темы, демонстрируя способность к критическому мышлению и самостоятельному исследованию.
«Хорошо» или «зачтено»	1. Студент предоставляет достаточно полные ответы на вопросы с учетом основных аспектов темы. Ответы студента имеют ясную структуру и последовательность, делая их понятными и логически связанными. 2. Студент 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. Студент представляет хорошее понимание темы вопроса, охватывая основные аспекты и направления ее изучения. Ответы студента 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. Студент предоставляет верные выводы, но они недостаточно аргументированы или основаны на поверхностном понимании предмета вопроса. 2. Студент 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. Студент охватывает большинство основных аспектов темы вопроса, но демонстрирует неполное или поверхностное их понимание, дает недостаточно развернутые объяснения.
«Неудовлетворительно» или «не зачтено»	1. Студент отвечает на вопросы неполно, не раскрывая основных аспектов темы. Ответы студента не структурированы, не связаны с заданным вопросом, отсутствует их логическая обоснованность. Выводы, предоставляемые студентом, представляют собой простые утверждения без анализа или четкой аргументации. 2. Студент 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. Студент ограничивается поверхностным рассмотрением темы и не показывает понимания ее существенных аспектов. Ответ студента частичный или незавершенный, не включает анализ рассматриваемого вопроса, пропущены важные детали или связи.

№ п/п	Наименование формы проведения текущего контроля успеваемости и промежуточной аттестации	Описание показателей оценочного материала	Представление оценочного материала в фонде	Критерии и описание шкал оценивания *(шкалы: 0 – 100%, четырехбалльная, тахометрическая)*
1	*Тест-тренинг*	Вид тренингового учебного занятия, задачей которого является закрепление учебного материала, а также проверка знаний обучающегося как по дисциплине в целом, так и по отдельным темам (разделам) дисциплины	Система стандартизированных заданий (тестов)	- от 0 до 69,9 % выполненных заданий – не зачтено; - 70 до 100 % выполненных заданий – зачтено.
2	*Тест*	2-я часть зачета: выполнение электронного тестирования (аттестационное испытание промежуточной аттестации с использованием информационных тестовых систем)	Система стандартизированных заданий (тестов)	*Описание шкалы оценивания электронного тестирования:* – от 0 до 49,9 % выполненных заданий – неудовлетворительно; – от 50 до 69,9% – удовлетворительно; – от 70 до 89,9% – хорошо; – от 90 до 100% – отлично