Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО ОУЭП)

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

Б1.В.ДЭ.05.02 Современная криптография и стеганография

Образовательная программа направления подготовки
09.03.01 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»,
направленность (профиль): «Информатика и вычислительная техника»
Квалификация: бакалавр

Рассмотрено к утверждению на заседании кафедры
информатики
(протокол № 14-01 от 14.01.2022г.)

Разработчик:
Чернышенко С.В., д.б.н.; д.ф.-м. н., проф.

Москва 2022

1. Цели и задачи дисциплины

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

Задачи дисциплины:

• 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 ОП

Блок 1 «Дисциплины (модули)», часть, формируемая участниками образовательных отношений, элективные дисциплины.

3. Планируемые результаты обучения по дисциплине

В результате изучения дисциплины обучающийся должен освоить:

Обобщенную трудовую функцию (ОТФ):

Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

С24/6 Развертывание ИС у заказчика

Трудовые действия:

Настройка ИС для оптимального решения задач заказчика

профессиональную компетенцию:

ПК-6. Способен находить оптимальные решения при проектировании и разработке информационных систем, обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности..

Результаты освоения дисциплины, установленные индикаторы достижения компетенций

Наименование компетенции	**Индикаторы достижения компетенции**	**Показатели (планируемые) результаты обучения**
ПК-6. Способен находить оптимальные решения при проектировании и разработке информационных систем, обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности.	ПК-6.1. Знает: предметную область автоматизации, инструменты и методы оценки качества и эффективности информационной системы, инструменты и методы оптимизации информационных систем, современные инструменты и методы управления организацией, в том числе методы планирования деятельности, распределения поручений, контроля исполнения, принятия решений	**Знать:** ● способы разграничения доступа и средства их реализации
	ПК-6.2. Умеет: находить оптимальные решения при проектировании и разработке информационных систем, обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	**Уметь:** ● проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности
	ПК-6.3. Владеет: методами оптимизации информационных систем, методами принятия решений, методиками проведения экспериментов по проверке корректности и эффективности проектных решений	**Владеть:** ● методами аудита безопасности информационных систем

Знания, умения и навыки, приобретаемые обучающимися в результате изучения дисциплины «Современная криптография и стеганография», являются необходимыми для последующего поэтапного формирования компетенций и изучения дисциплин.

4. Объем дисциплины и виды учебной работы

Учебным планом предусматриваются следующие виды работы по дисциплине:

№ п/п	Виды учебных занятий	Всего часов по формам обучения, ак. ч			
		Очная		Заочная	
		всего	в том числе	всего	в том числе
1	**Контактная работа (объем работы обучающихся во взаимодействии с преподавателем) (всего)**	**54,2**		**8,2**	
	В том числе в форме практической подготовки		**2**		***2***
1.1	занятия лекционного типа (лекции)	12		2	
1.2	занятия семинарского типа (практические)*, в том числе:	40		4	
1.2.1	семинар-дискуссия, практические занятия		0 40		0 4
	в форме практической подготовки		2		*2*
1.2.2	занятия семинарского типа: лабораторные работы (лабораторные практикумы)				
1.2.3	курсовое проектирование (выполнение курсовой работы)				
1.3	контроль промежуточной аттестации и оценивание ее результатов, в том числе:	2,2		2,2	
1.3.1	консультация групповая по подготовке к промежуточной аттестации		2		2
1.3.2	прохождение промежуточной аттестации		0,2		0,2
2	**Самостоятельная работа (всего)**	**74**		**129**	
2.1	работа в электронной информационно-образовательной среде с образовательными ресурсами учебной библиотеки, компьютерными средствами обучения для подготовки к текущей и промежуточной аттестации, к курсовому проектированию (выполнению курсовых работ)	74		129	
2.2	самостоятельная работа при подготовке к промежуточной аттестации	**15,8**		**6,8**	
3	**Общая трудоемкость дисциплины**	**4 з.е. / 144 час.**			
	Форма промежуточной аттестации	экзамен			

*
_____
Семинар – семинар-дискуссия
ГТ - практическое занятие - глоссарный тренинг
ТТ - практическое занятие - тест-тренинг
ПЗТ - практическое занятие - позетовое тестирование
ЛС - практическое занятие - логическая схема
УД - семинар-обсуждение устного доклада
РФ – семинар-обсуждение реферата
Асессмент реферата - семинар-асессмент реферата
ВБ - вебинар
УЭ - семинар-обсуждение устного эссе
АЛТ - практическое занятие - алгоритмический тренинг

5. Содержание дисциплины

5.1. Содержание разделов и тем

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
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.
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.
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.
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.

6. Методические указания по освоению дисциплины

6.1 Учебно-методическое обеспечение дисциплины

Методические указания для преподавателя

Изучение дисциплины проводится в форме лекций, практических 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 курсом.

Основной целью практических занятий является обсуждение наиболее сложных теоретических вопросов курса, их методологическая и методическая проработка. Они проводятся в форме опроса, диспута, тестирования, обсуждения докладов и пр.

Самостоятельная работа с научной и учебной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с информационными базами, образовательным ресурсов электронной информационно-образовательной среды и сети Интернет.

Оценочные материалы по компетенциям представлены на сайте в разделе «оценочные материалы».

6.2 Методические материалы обучающимся по дисциплине, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические материалы доступны на сайте «Личная студия» в разделе «Методические указания и пособия».

1. Методические указания «Введение в технологию обучения».
2. Методические указания по проведению учебного занятия «Вебинар».
3. Методические указания по проведению занятия «Семинар-обсуждение устного эссе», «Семинар-обсуждение устного доклада».
4. Методические указания по проведению занятия «Семинар – семинар-асессмент реферата».
5. Методические указания по проведению занятия «Семинар – обсуждение реферата».
6. Методические указания по проведению учебного занятия с компьютерным средством обучения «Практическое занятие - тест-тренинг».
7. Методические указания по проведению учебного занятия с компьютерным средством обучения «Практическое занятие - глоссарный тренинг».
8. Методические указания по проведению занятия «Практическое занятие - позетовое тестирование».
9. Положение о реализации электронного обучения, дистанционных образовательных технологий.
10. Методические указания по проведению занятия «Практическое занятие - алгоритмический тренинг».

Указанные методические материалы для обучающихся доступны в Личной студии обучающегося, в разделе ресурсы

6.3 Особенности реализации дисциплины в отношении лиц из числа инвалидов и лиц с ограниченными возможностями здоровья

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала.

Подбор и разработка учебных материалов должны производится с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

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 с другими студентами, создании комфортного психологического климата в студенческой группе.

Разработка учебных материалов и организация учебного процесса проводится с учетом следующих нормативных документов и локальных актов образовательной организации:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53 (ч. 1). Ст. 7598;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации» // СЗ РФ. 1995. № 48. Ст. 4563;
- Федерального закона от 03.05.2012 № 46-ФЗ «О ратификации Конвенции о правах инвалидов» // СЗ РФ. 2012. № 19. Ст. 2280;
- Приказа Минобрнауки России от 09.11.2015 № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2016. № 4;
- Приказ Министерства науки и высшего образования РФ от 06 апреля 2021 г. N 245 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры";
- Методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн;

- Положения об организации и осуществлении образовательной деятельности по реализации образовательных программ высшего образования с применением электронного обучения, дистанционных образовательных технологий (локальный нормативный акт утв. приказом АНО ВО ОУЭП от 20.01.2021 № 10;

- Положения об обучении инвалидов и лиц с ограниченными возможностями здоровья (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);

- Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5).

- Порядка разработки оценочных материалов и формирования фонда оценочных материалов для проведения промежуточной и итоговой (государственной итоговой) аттестации и критерии оценивания при текущем контроле успеваемости (локальный нормативный акт утв. приказом АНО ВО ОУЭП от 20.01.2021 № 10);

- Положения об экзаменационной комиссии (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5).

- Правил подачи и рассмотрения апелляций по результатам вступительных испытаний (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);

- Положения о разработке и реализации адаптированных учебных программ АНО ВО ОУЭП (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Студенческим советом протокол от 20.01.2021 № 13 и Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);

- Положения об организации обучения обучающихся по индивидуальному учебному плану (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);

- Положения об оказании платных образовательных услуг для лиц с ограниченными возможностями (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5).

В соответствии с нормативными документами инвалиды и лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь; инвалиды и 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 инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;

- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);

- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом 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 слепых:

- задания и иные материалы для сдачи экзамена оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

- письменные задания выполняются обучающимися с использованием клавиатуры с азбукой Брайля, либо надиктовываются ассистенту;

б) для слабовидящих:

- задания и иные материалы для сдачи экзамена оформляются увеличенным шрифтом и\или использованием специализированным программным обеспечением Jaws;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- имеется в наличии информационная система "Исток" для коллективного использования слабослышащими;

- по их желанию испытания проводятся в электронной или письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата:

- тестовые и тренинговые задания по текущей и промежуточной аттестации выполняются обучающимися на компьютере через сайт «Личная студия" с использованием электронного обучения и дистанционных технологий;

- в процессе обучения студентам предоставляется возможность использования электронных образовательных ресурсов, разработанных в Университете, а так же разработана доступная электронная информационно-образовательная среда;

- по их желанию испытания проводятся в устной форме.

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).

6.4 Методические рекомендации по самостоятельной работе студентов

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 знаний при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа должна:

- быть выполнена индивидуально (или являться частью коллективной работы). В случае, когда СР подготовлена в порядке выполнения группового задания, в работе делается соответствующая оговорка;

- 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 в логической последовательности: титульный лист, оглавление, основная часть, заключение, выводы, список литературы, приложения,

- 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).

6.4.1 Формы самостоятельной работы обучающихся по разделам дисциплины

Раздел 1

Темы устного доклада

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

Темы устного доклада

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

Темы устного доклада

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
Темы устного доклада

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.

7. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине

Фонд оценочных средств по дисциплине для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложение 1 к настоящей рабочей программе дисциплины.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Рекомендуемая литература

Основная литература

1. 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 c. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102017.html

2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — Москва : СОЛОН-Пресс, 2018. — 262 c. — ISBN 978-5-91359-173-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/90375.html

3. Теоретико-числовые методы в криптографии : учебное пособие / составители Ф. Б. Тебуева, В. О. Антонов. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 107 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/75601.html

4. Хасанов, Р. И. Основы стеганографии : учебное пособие / Р. И. Хасанов. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016. — 102 c. — ISBN 978-5-7410-1555-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/78809.html

Дополнительная литература

1. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2016. — 256 c. — ISBN 5-98003-002-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/90248.html

2. 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 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/61517.html

8.2. 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. https://uisrussia.msu.ru/ - база данных и аналитических публикаций университетской информационной системы Россия
3. http://www.iprbookshop.ru - Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний
4. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
5. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
6. https://www.garant.ru/ - справочная правовая система Гарант
7. https://gufo.me/ - справочная база энциклопедий и словарей
8. https://slovaronline.com - справочная база, полная поисковая система по всем доступным словарям, энциклопедиям и переводчикам в режиме Онлайн
9. Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» https://reestr.digital.gov.ru/
10. https://basegroup.ru/community/camp - Кампус BaseGroup Labs площадка для обмена аналитиками опытом: вопросы и ответы, статьи, книги, база знаний, блоги, презентации, выступления. Описание методик, алгоритмов, практических кейсов и проектного опыта в области программных продуктов.
11. https://www.sciencedirect.com/browse/journals-and-books?contentType=JL&subject=computer-science – коллекция журналов в открытом доступе по информатике
12. https://basegroup.ru/community/camp - кампус BaseGroup Labs - площадка для обмена аналитиками опытом: вопросы и ответы, статьи, книги, база знаний, блоги, презентации, выступления (описание методик, алгоритмов, практических кейсов и проектного опыта в области программных продуктов)
13. http://expert.ru/dossier/story/tehnologii/ - статьи журнала «Эксперт» в области информационных технологий
14. http://www.emanual.ru/ - сайт, посвящённый всем значимым событиям в IT-индустрии: новейшие разработки, уникальные методы и горячие новости

9. Материально-техническое обеспечение дисциплины

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине представлено в приложении 8 «Сведения о материально-техническом обеспечении программы высшего образования – программы бакалавриата направления подготовки 09.03.01 «Информатика и вычислительная техника».

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая программное обеспечение, в том числе отечественного производства

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 (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

Приложение 1

Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО ОУЭП)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Текущего контроля и промежуточной аттестации
по дисциплине

Б1.В.ДЭ.05.02 Современная криптография и стеганография

Образовательная программа направления подготовки
09.03.01 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»,
направленность (профиль): «Информатика и вычислительная техника»
Квалификация: бакалавр

Москва 2022

7.1. Оценочные средства

Назовите основные понятия:

№	Определение	Ответ
1.	Данные методы позволяют скрывать секретные сообщения путем их встраивания в послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.	Стеганографические методы
2.	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.	Криптография
3.	Процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц.	Шифрование
4.	Процесс преобразования шифротекста в открытый текст.	Расшифрование
5.	Криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи.	Симметричная криптосистема
6.	Данный вид криптосистем использует пару ключей, один из которых является открытым, а другой – закрытым, известным только его владельцу.	Асимметричная криптосистема
7.	Наука о методах вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным.	Криптоанализ
8.	Попытка проведения криптоанализа шифра.	Криптоаналитическая атака
9.	Успешная криптоаналитическая атака, в результате которой противнику становится известным содержание зашифрованного сообщения.	Взломом шифра
10.	Способность шифра противостоять криптоаналитическим атакам.	Стойкость шифра

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Как называется совокупность методов и средств, которые используются для формирования скрытого канала передачи информации?	Стеганографическая система
2.	Как называется любая открытая информация, предназначенная для сокрытия тайных сообщений?	Контейнер
3.	Что представляет собой конфиденциальная информация любого типа (например, текст, изображение, аудиоданные), подлежащая скрытию?	Сообщение
4.	Как называется техника сокрытия или скрытой передачи информации внутри других незаметных цифровых объектов, таких как изображения, звуковые файлы, видео или текстовые документы?	Метод компьютерной стеганографии
5.	Как называется наука о методах вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным?	Криптоанализ
6.	Что представляет собой процесс применения криптографических методов и алгоритмов для обеспечения конфиденциальности, целостности и аутентификации данных и коммуникаций, использующий различные математические и алгоритмические техники для шифрования информации таким образом, чтобы только авторизованные пользователи могли получить доступ к расшифрованной информации?	Криптографическая защита
7.	При использовании какого способа символы открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом?	Шифрование способом перестановки
8.	Как называется разновидность шифрования с применением многоалфавитной подстановки, при котором каждый следующий байт открытого текста складывается с предыдущим байтом, а нулевой байт открытого текста — с последним байтом?	Побайтное шифрование
9.	При каком виде шифрования шифротекст получается путем наложения на открытый текст гаммы шифра с помощью какой-либо обратимой операции?	Шифрование способом гаммирования
10.	Что представляет собой относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже — отдельно) с подписываемым с ее помощью документом?	Электронная цифровая подпись

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	Стеганографический	b	c

	ключ	канал		

7.2. Система оценивания результатов текущего контроля успеваемости и промежуточной аттестации, а также критерии выставления оценок, описание шкал оценивания

Критерии и описание шкал оценивания приведены в Порядке разработки оценочных материалов и формирования фонда оценочных материалов для проведения промежуточной и итоговой (государственной итоговой) аттестации и критерии оценивания при текущем контроле успеваемости (локальный нормативный акт утв. приказом АНО ВО ОУЭП 20.01.2021 № 10)

№ 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	- от 0 до 69,9 % выполненных заданий – не зачтено; - 70 до 100 % выполненных заданий – зачтено.
2	*Экзамен*	1-я часть экзамена: выполнение обучающимися практико-ориентированных заданий (аттестационное испытание промежуточной аттестации, проводимое устно с использованием телекоммуникационных технологий)	Практико-ориентированные задания	*Критерии оценивания преподавателем практико-ориентированной части экзамена:* – соответствие содержания ответа заданию, полнота раскрытия темы/задания (оценка соответствия содержания ответа теме/заданию); – умение проводить аналитический анализ прочитанной учебной и научной литературы, сопоставлять теорию и практику; – логичность, последовательность изложения ответа; – наличие собственного отношения обучающегося к теме/заданию; – аргументированность, доказательность излагаемого материала. *Описание шкалы оценивания практико-ориентированной части экзамена* Оценка «*отлично*» выставляется за ответ, в котором содержание соответствует теме или заданию, обучающийся глубоко и прочно усвоил учебный материал, последовательно,

				четко и логически стройно излагает его, демонстрирует собственные суждения и размышления на заданную тему, делает соответствующие выводы; умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, приводит материалы различных научных источников, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения задания, показывает должный уровень сформированности компетенций. Оценка «*хорошо*» выставляется обучающемуся, если ответ соответствует и раскрывает тему или задание, показывает знание учебного материала, грамотно и по существу излагает его, не допуская существенных неточностей при выполнении задания, правильно применяет теоретические положения при выполнения задания, владеет необходимыми навыками и приемами его выполнения, однако испытывает небольшие затруднения при формулировке собственного мнения, показывает должный уровень сформированности компетенций. Оценка «*удовлетворительно*» выставляется обучающемуся, если ответ в полной мере раскрывает тему/задание, обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении учебного материала по заданию, его собственные суждения и размышления на заданную тему носят поверхностный характер. Оценка *«неудовлетворительно*» выставляется обучающемуся, если не раскрыта тема, содержание ответа не соответствует теме, обучающийся не обладает знаниями по значительной части учебного материала и не

				может грамотно изложить ответ на поставленное задание, не высказывает своего мнения по теме, допускает существенные ошибки, ответ выстроен непоследовательно, неаргументированно. Итоговая оценка за экзамен выставляется преподавателем в совокупности на основе оценивания результатов электронного тестирования обучающихся и выполнения ими практико-ориентированной части экзамена
		2-я часть экзамена: выполнение электронного тестирования (аттестационное испытание промежуточной аттестации с использованием информационных тестовых систем)	Система стандартизирован-ных 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