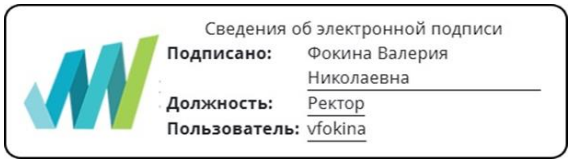
Автономная некоммерческая организация высшего образования
«ОТКРЫТЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА»

УТВЕРЖДАЮ:

Ректор АНО ВО ОУЭП, Фокина В.Н.



«19» апреля 2023 г.

Б1.О.04 МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.15 ЗАЩИТА ИНФОРМАЦИИ

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: формирование у обучающихся теоретических знаний и практических навыков применения методов и средств защиты информации в профессиональной деятельности.

Задачи:

– формирование системы знаний в сфере источников угроз безопасности информации в компьютерной системе;

– формирование системы знаний в сфере юридических основ правового обеспечения безопасности компьютерных систем;

– формирование системы знаний о технических и программных средствах обеспечения безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Место дисциплины в учебном плане:

Блок: Блок 1. Дисциплины (модули).

Часть: Обязательная часть.

Модуль: модуль общепрофессиональной подготовки.

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.

ОПК-3 - способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

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

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.2**. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает:** методологию проведения научно-исследовательской работы **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеет:** навыками самостоятельного проведения научно-исследовательской работы

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Защита информации» 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: 4 з.е. / 144 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)		
	Очная	Очно-заочная	Заочная
Аудиторные занятия	54	30	12
в том числе:			
Лекции	18	10	4
Практические занятия	36	20	8
Лабораторные работы	-	-	-
Самостоятельная работа	54	78	123
в том числе:			
часы на выполнение КР / КП	-	-	-
Промежуточная аттестация:			
Вид	Экзамен – 6 сем.	Экзамен – 7 сем.	Экзамен – 7 сем.
Трудоемкость (час.)	36	36	9
Общая трудоемкость з.е. / час.	**4 з.е. / 144 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	Введение в информационную безопасность	3	7		10
2	Организационно-правовое обеспечение защиты информации	3	7		11

№	Наименование темы дисциплины	Лекции	Практические занятия	Лабораторные работы	Самост. работа *(в т.ч. КР / КП)*
3	Методы и средства технической защиты информации	3	7		11
4	Программно-технические средства защиты информации	4	7		11
5	Криптографические средства защиты информации	4	8		11
	Итого (часов)	18	36		54
	Форма контроля:	**Экзамен**			**36**
Очно-заочная форма обучения					
1	Введение в информационную безопасность	2	4		15
2	Организационно-правовое обеспечение защиты информации	2	4		15
3	Методы и средства технической защиты информации	2	4		16
4	Программно-технические средства защиты информации	2	4		16
5	Криптографические средства защиты информации	2	4		16
	Итого (часов)	10	20		78
	Форма контроля:	**Экзамен**			**36**
Заочная форма обучения					
1	Введение в информационную безопасность	0,5	1		24
2	Организационно-правовое обеспечение защиты информации	0,5	1		24
3	Методы и средства технической защиты информации	1	2		25
4	Программно-технические средства защиты информации	1	2		25
5	Криптографические средства защиты информации	1	2		25
	Итого (часов)	4	8		123
	Форма контроля:	**Экзамен**			**9**
	Всего по дисциплине:	**4 з.е. / 144 час.**			

СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

Тема 1. Введение в информационную безопасность

Особенности обеспечения информационной безопасности Российской Федерации (роль и место информационной безопасности в общей системе национальной безопасности РФ. Основные цель и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ. Внешние и внутренние источники угроз информационной безопасности в РФ).

Информация как объект защиты (определение, виды и источники информации, подлежащей защите. Информация как объект права собственности. Виды защищаемой информации. Угрозы и возможные каналы утечки конфиденциальной информации. Обзор способов реализации угроз информации. Анализ моделей нарушителя. Категории потенциальных нарушителей).

Анализ существующих подходов к обеспечению безопасности информации (особенности современных информационных систем, существенные с точки зрения безопасности. Законодательный, административный и процедурный уровни информационной безопасности. Основные понятия политики безопасности. Структура политики безопасности организации. Программно-технический уровень информационной безопасности. Сервисы безопасности. Место сервисов безопасности в архитектуре информационных систем)

Тема 2. Организационно-правовое обеспечение защиты информации

Международные и отечественные стандарты в сфере защиты информации (роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернет. Отечественные стандарты безопасности информационных технологий).

Сертификация и аттестация в области защиты информации (назначение и общая характеристика. Проведение сертификационных испытаний. Аттестация объектов информатизации. Сертификация на региональном и международном уровнях).

Организационные меры по защите информации (концепция безопасности предприятия и ее содержание. Политика информационной безопасности предприятия. Назначение, содержание и структура политики безопасности. Служба безопасности предприятия).

Основы правового обеспечения защиты информации (международный опыт правового обеспечения информационной безопасности. Государственная система правового обеспечения информационной безопасности. Содержание основных законов РФ в области информационной безопасности. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации)

Тема 3. Методы и средства технической защиты информации

Виды и методы технической защиты информации (пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры).

Технические каналы утечки информации (общая характеристика технических каналов утечки информации и их классификация. Каналы утечки речевой информации. Технические средства и методы получения информации по этим каналам. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок. Технические средства и методы получения информации с использованием этих каналов).

Методы и средства защиты информации от утечки по техническим каналам (основные методы, используемые при создании систем защиты информации. Заземление технических средств передачи информации. Использование сетевых фильтров. Экранирование помещений. Методы защиты от утечек по акустическим каналам. Защита средств связи и телекоммуникаций)

Тема 4. Программно-технические средства защиты информации

Защита информации от несанкционированного доступа (идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Идентификация и аутентификация субъектов “пользователь” и “процесс” при запросах на доступ к компьютерным ресурсам. Использование простого и динамически изменяющегося паролей. Биометрическая идентификация. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Разграничение доступа. Защита программных средств от несанкционированного копирования и модификации).

Защита от компьютерных вирусов (основные виды вирусов и схемы их функционирования. Основные каналы распространения вирусов и других вредоносных программ. Обнаружение вирусов и меры по защите и профилактике. Антивирусные программы и комплексы).

Технологии межсетевых экранов (функции межсетевых экранов. Фильтрация трафика. Выполнение функций посредничества. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе

межсетевых экранов. Схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Обзор современных межсетевых экранов)

Тема 5. Криптографические средства защиты информации

Принципы криптографической защиты информации (основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированные криптосистемы шифрования. Электронная цифровая подпись и функция хэширования. Правовые аспекты применения электронной цифровой подписи).

Криптографические алгоритмы. Средства криптографиической защиты информации (классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Алгоритм шифрования RSA. Алгоритм Диффи-Хеллмана. Алгоритмы цифровой подписи. Средства криптографической защиты информации. Правовые основы разработки и использования средств криптографической защиты информации).

Компьютерная стеганография (принципы компьютерной стеганографии. Секретные средства связи и передачи информации. Методики стеганографии. Стегосистема. Контейнер. Стегоключ)

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:

- Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html
- Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 c. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/74381.html
- Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных : учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 c. — ISBN 978-5-9227-0783-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/80747.html
- Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс] : учебное пособие / С.Н. Никифоров. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 80 c. — 978-5-9227-0762-6. — Режим доступа: http://www.iprbookshop.ru/74382

- Алексеев А.П. Многоуровневая защита информации [Электронный ресурс] / А.П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 128 c. — 978-5-904029-72-2. — Режим доступа: http://www.iprbookshop.ru/75387
- Корнеева Е.В. Программно-технические средства защиты информации. [Электронный ресурс]: рабочий учебник / Корнеева Е.В. - 2022. - http://libary.roweb.online
- Корнеева Е.В., Белянина Н.В. Криптографические средства защиты информации. [Электронный ресурс]: рабочий учебник / Корнеева Е.В., Белянина Н.В. - 2022. - http://libary.roweb.online

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. https://www.kaspersky.ru/ - сайт компании Лаборатория Касперского
7. http://security.mosmetod.ru/ - Сайт «Безопасный интернет»
8. https://ligainternet.ru/ - Лига безопасного Интернета.
9. Web-технологии https://htmlweb.ru/php/mysql.php
10. Научная электронная библиотека. http://elibrary.ru
11. Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний http://www.iprbookshop.ru
12. Справочно-правовая система «Гарант»;
13. 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.О.04.15 ЗАЩИТА ИНФОРМАЦИИ

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
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.2**. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает:** методологию проведения научно-исследовательской работы **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеет:** навыками самостоятельного проведения научно-исследовательской работы

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,	**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	**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

	исходя из действующих норм, имеющихся ресурсов, но испытывает сильные затруднения	**Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но иногда допускает ошибки	
ОПК-3.2. Самостоятельно проводит научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
Не знает: методологию проведения научно-исследовательской работы **Не умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Не владеет:** навыками самостоятельного проведения научно-исследовательской работы	**Поверхностно знает:** методологию проведения научно-исследовательской работы **В целом умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, но испытывает затруднения **В целом владеет:** навыками самостоятельного проведения научно-исследовательской работы, но испытывает сильные затруднения	**Знает:** методологию проведения научно-исследовательской работы, но допускает несущественные ошибки **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ошибки **Владеет:** навыками самостоятельного проведения научно-исследовательской работы, но иногда допускает ошибки	**Знает:** методологию проведения научно-исследовательской работы **Умеет:** самостоятельно проводить научно-исследовательскую работу с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **Владеет:** навыками самостоятельного проведения научно-исследовательской работы

Оценочные средства

Разъясните основные понятия:

№	Понятие	Определение
1.	Методы и средства защиты информации	Методы и средства защиты информации – это организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и
		эксплуатации компьютерной системы для обеспечения защиты информации.
2.	Политика безопасности	Политика безопасности — это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.
3.	Угроза безопасности информации	Угроза безопасности информации в компьютерной системе – это событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.
4.	Утечка	Утечка – это неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.
5.	Уязвимость информации	Уязвимость информации – это возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
6.	Целостность информации	Целостность информации – неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

7.	Собственник информационных ресурсов, систем и технологий	Собственник информационных ресурсов, систем и технологий – это субъект с полномочиями владения, пользования и распоряжения указанными объектами.
8.	Разглашение	Разглашение – это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).
9.	Непреднамеренное воздействие	Непреднамеренное воздействие на защищаемую информацию - воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).
10.	Конфиденциальность информации	Конфиденциальность информации – это известность ее содержания только имеющим соответствующие полномочия субъектам.

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что такое умышленная угроза информационной безопасности?	К умышленным угрозам относятся: − несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС); − несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

2.	Что относится к непреднамеренным угрозам компьютерных систем?	К непреднамеренным угрозам относятся: − ошибки в проектировании КС; − ошибки в разработке программных средств КС; − случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения; − ошибки пользователей КС; − воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной
		совместимости) и др.
3.	Какие существуют непосредственные каналы утечки информации?	Непосредственными каналами утечки информации являются: − хищение носителей информации; − сбор производственных отходов с информацией (бумажных и магнитных носителей); − копирование носителей информации; − намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей КС; − маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т. п.); − обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.
4.	Какие существуют косвенные каналы утечки информации?	Косвенными каналами утечки называют каналы, не связанные с физическим доступом к элементам КС: − использование подслушивающих (радио закладных) устройств; − дистанционное видеонаблюдение; − перехват побочных электромагнитных излучений и наводок (ПЭМИН).

5.	Что включают в себя организационные методы защиты информации?	Методы и средства организационной защиты информации включают в себя: − ограничение физического доступа к объектам КС и реализация режимных мер; − ограничение возможности перехвата ПЭМИН (перехват побочных электромагнитных излучений и наводок); − разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при
		ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок); − резервное копирование наиболее важных с точки зрения утраты массивов документов; − профилактику заражения компьютерными вирусами.

6.	Какие существуют уровни правового обеспечения информационной безопасности?	Можно выделить четыре уровня правового обеспечения информационной безопасности. Первый уровень образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России. Второй уровень составляют подзаконные акты, к которым относятся указы Президента РФ и постановления Правительства РФ, а также письма Высшего Арбитражного Суда РФ и постановления пленумов Верховного Суда РФ. Третий уровень составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами. Четвертый уровень образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.
7.	Какая информация является конфиденциальной?	В соответствии с российским законодательством к конфиденциальной относится следующая информация: − служебная тайна (врачебная, адвокатская, тайна суда и следствия и т.п.); − коммерческая тайна; − персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).
8.	Что является опосредованной угрозой безопасности информации в КС?	Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.

9.	Что представляет собой системно-концептуальный подход решении задачи защиты информации в КС?	При решении задачи защиты информации в КС необходимо применять так называемый системно-концептуальный подход. В соответствии с ним решение задачи должно подразумевать: − системность целевую, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества; − системность пространственную, предполагающую взаимосвязанность защиты информации во всех элементах КС; − системность временную, предполагающую непрерывность защиты информации; − . системность организационную, предполагающую единство организации всех работ по защите информации в КС и управления ими.
10.	Какие существуют методы и средства защиты информации?	Существующие методы и средства защиты информации можно подразделить на четыре основные группы: − методы и средства организационно-правовой защиты информации; − методы и средства инженерно-технической защиты информации; − криптографические методы и средства защиты информации; − программно-аппаратные методы и средства защиты информации.

Тестовые задания:

1	Упорядоченная совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы, называется:

	a) информационной системой; b) политикой безопасности; c) информационной технологией; d) информационным процессором.
2	Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется **Защитой информации**
3	Получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней, называется **Несанкционированным доступом**
4	Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа, называется: a) защитой информации; **b) политикой безопасности;** c) стратегией защиты информации; d) правилами поведения.
5	Информация, содержание которой может быть понятно любому субъекту, называется: a) сказкой; b) инструкцией хакера; c) криптосистемой; **d) открытым текстом.**

6	Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати): a) компьютерным шпионажем; **b) разглашением;**
	c) вредительством; d) предательством.
7	Субъект с полномочиями владения информационными ресурсами, их пользования и распоряжения, называется a) сетевым администратором; **b) собственником информационных ресурсов;** c) программистом; d) пользователем.
8	Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками: a) расползанием информации; b) информационным предательством; c) вредительством; **d) утечкой.**
9	Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации, называется**:** a) устареванием политики безопасности; b) сбоем системы защиты информации; **c) уязвимостью информации;** d) обходом защиты информации.

10	Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий, называется: **a) непреднамеренным воздействием;** b) самоатакой; c) глюком.

Ключ к тестовым заданиям

1	**2**	**3**	**4**	**5**
a	зашитой информации;	несанкционированным доступом;	b	d
6	**7**	**8**	**9**	**10**
b	b	d	c	a

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 экзамена: 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