Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.ДЭ.07.02
Работа с конфиденциальной информацией
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 64
самостоятельная работа 43,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Контактная работа на аттестации	0,2	0,2	0,2	0,2
В том числе в форме практ.подготовки	8	8	8	8
Итого ауд.	64	64	64	64
Контактная работа	64,2	64,2	64,2	64,2
Сам. работа	43,8	43,8	43,8	43,8
Итого	108	108	108	108

Программу составил(и):
к.т.н., доцент, Капустин С.А.

Рецензент(ы):
д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Работа с конфиденциальной информацией

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	приобретение студентами знаний по работе с
1.2	конфиденциальной информацией в организациях и предприятиях различных
1.3	направлений деятельности и различных форм собственности и формирование
1.4	практических навыков работы в реальных конкретных условиях.

Задачи: научить студентов в конкретных условиях анализировать наиболее значимые аспекты безопасности создания, формирования, жизненного цикла и документопотоков конфиденциальной информации;
 изучение основных методов организационной защиты конфиденциальных документов;
 научить студентов осуществлять правильный выбор организационных форм защиты конфиденциальной информации в зависимости от ее вида, ценности, объема, и способа представления, а также в зависимости от стоимости используемых технических средств, удобства их использования и надежности функционирования;
 изучение основных нормативно-правовых актов, регламентирующих защиту и обработку конфиденциальных документов.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДЭ.07
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы информационной безопасности
2.1.2	Экономика защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика: Преддипломная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах	
ПК-9.1: Формулирование правил работы персонала со средствами защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний правил работы персонала со средствами защиты информации
Уровень 2	Уровень знаний правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, без ошибок
ПК-9.2: Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему	
Уметь	
Уровень 1	Продемонстрированы основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты

	информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки сопоставлять результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1					
1.1	Организационные и правовые основы обеспечения безопасности конфиденциальной информации /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.2	Организационные и правовые основы обеспечения безопасности конфиденциальной информации /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.3	Организационные и правовые основы обеспечения безопасности конфиденциальной информации /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.4	Организационные источники и каналы утечки информации /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.5	Организационные источники и каналы утечки информации /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.6	Организационные источники и каналы утечки информации /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.7	Технические и программные средства защиты информации /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.8	Технические и программные средства защиты информации /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.9	Технические и программные средства защиты информации /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.10	Коммерческая тайна и порядок её определения /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.11	Коммерческая тайна и порядок её определения /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.12	Коммерческая тайна и порядок её определения /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.13	Организация работ с информацией, составляющей коммерческую тайну /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.14	Организация работ с информацией, составляющей коммерческую тайну /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.15	Организация работ с информацией, составляющей коммерческую тайну /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

1.16	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.17	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.18	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.19	Организация деятельности службы безопасности объекта /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.20	Организация деятельности службы безопасности объекта /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.21	Организация деятельности службы безопасности объекта /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.22	Организация внутриобъектового режима /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.23	Организация внутриобъектового режима /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.24	Организация внутриобъектового режима /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.25	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.26	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.27	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

1.28	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.29	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.30	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.31	Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.32	Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.33	Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.34	Охрана объектов /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.35	Охрана объектов /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.36	Охрана объектов /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.37	Организация защиты информации при подготовке и проведению совещаний и переговоров /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.38	Организация защиты информации при подготовке и проведению совещаний и переговоров /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.39	Организация защиты информации при подготовке и проведению совещаний и переговоров /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

1.40	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.41	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	1
1.42	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.43	Подготовка лиц, ответственных за обеспечение безопасности информации /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.44	Подготовка лиц, ответственных за обеспечение безопасности информации /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.45	Подготовка лиц, ответственных за обеспечение безопасности информации /Ср/	6	2,7	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.46	Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией /Лек/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.47	Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией /Пр/	6	2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
1.48	Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией /Ср/	6	3,3	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
	Раздел 2. Промежуточная аттестация					
2.1	Зачет /КА/	6	0,2	ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Организационные методы обеспечения безопасности конфиденциальной информации.
2. Требования к построению систем безопасности предприятия и учреждения.

3. Правовые основы организационного обеспечения безопасности конфиденциальной информации.
4. Характеристика защитных действий от утечки информации.
5. Способы пресечения разглашения защищаемой информации.
6. Противодействие несанкционированному доступу к конфиденциальной информации.
7. Технические средства защиты конфиденциальной информации.
8. Программные средства защиты конфиденциальной информации.
9. Организация работ с информацией, составляющей коммерческую тайну.
10. Порядок допуска к работам с информацией, составляющей коммерческую тайну.
11. Порядок подбора персонала на должности, связанные с работой с информацией ограниченного доступа.
12. Порядок заключения контрактов и соглашений о неразглашении конфиденциальной информации.
13. Задачи службы безопасности организации.
14. Организационная структура и функции службы безопасности.
15. Структурные подразделения службы безопасности.
16. Основные задачи организации внутриобъектового режима.
17. Организация охраны объектов на территории предприятия.
18. Организация инженерно-технической безопасности предприятия.
19. Организация безопасности функционирования информационных систем.
20. Назначение и основные задачи контрольно-пропускного пункта объекта.
21. Защита периметра территории зданий и открытых площадок с помощью технических средств охраны.
22. Защита помещений объекта с помощью технических средств охраны.
23. Системы контроля и управления доступом к конфиденциальной информации.
24. Системы охранного телевидения и оповещения.
25. Организация приема посетителей в организации. Классификация посетителей.
26. Угрозы информационной безопасности, исходящие от посетителей.
27. Правила при приеме руководителем фирмы (предприятия) и руководящим составом различных категорий посетителей.
28. Работа с иностранными представителями.
29. Назначение и порядок проведения проверки наличия документов, дел и носителей конфиденциальной информации.
30. Организация служебного расследования по фактам разглашения сотрудниками конфиденциальной информации.
31. Организация охраны объектов.
32. Организация пропускного режима.
33. Основные факторы, приводящие к разглашению конфиденциальной информации на совещании и переговорах.
34. Этапы проведения конфиденциальных совещаний и переговоров.
35. Документы, составляемые при подготовке конфиденциального совещания и порядок подготовки и проведения конфиденциального совещания.
36. Основные обязанности сотрудников службы безопасности при подготовке и проведении совещаний и переговоров.
37. Порядок доступа участников на конфиденциальные совещания.
38. Организация защиты информации при осуществлении научнопублицистической деятельности.
39. Организации защиты конфиденциальной информации при рекламной деятельности.
40. Понятие информационно-аналитической работы.
41. Основные задачи и функции информационно-аналитического подразделения службы безопасности.
42. Аналитическая работа с источниками угрозы конфиденциальной информации.
43. Выбор и подготовка персонала к работе, связанной с секретами фирмы.
44. Обучение персонала правилам защиты конфиденциальной информации.
45. Организационные мероприятия по работе с персоналом,

получившим доступ к конфиденциальной информации.
46. Анализ нарушений режима конфиденциальности информации.
47. Меры предупреждения обстоятельств организационноуправленческого, воспитательного и правового характера.
48. Изучение личности нарушителя режима конфиденциальности

5.2. Темы письменных работ

1. Понятие, проблемы и структура экономической безопасность предпринимательской деятельности (на примере фирм различных типов).
2. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3. Информационная безопасность, история формирования.
4. Концепция информационной безопасности.
5. Основы экономической безопасности предпринимательской деятельности.
6. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
7. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
8. Информационная безопасность (по материалам зарубежных источников и литературы).
9. Правовые основы защиты конфиденциальной информации.
10. Экономические основы защиты конфиденциальной информации.
11. Организационные основы защиты конфиденциальной информации.
12. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.
13. Построение и функционирование защищенного документооборота.
14. Анализ инструкции по обработке и хранению конфиденциальных документов.
15. Направления и методы защиты документов на бумажных носителях.
16. Направления и методы защиты машиночитаемых документов.
17. Направления и методы защиты электронных документов.
18. Архивное хранение конфиденциальных документов.
19. Направления и методы защиты аудио и визуальных документов.
20. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
21. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
22. Соотношение источников, каналов распространения и каналов утечки информации.
23. Анализ опыта защиты информации в зарубежных странах.
24. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
25. Основы технологии обработки и хранения конфиденциальных документов.
26. Назначение, виды, структура и технология функционирования системы защиты информации.
27. Направления экономического анализа системы защиты информации.
28. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
29. Направления и методы защиты профессиональной тайны.
30. Направления и методы защиты служебной тайны.
31. Направления и методы защиты персональных данных о гражданах.
32. Методы защиты личной и семейной тайны.
33. Защита секретов в дореволюционной России.
34. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.
35. Порядок подбора персонала для работы с конфиденциальной информацией.
36. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.
37. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

38. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.
39. Классификация посетителей фирмы, характеристика каждой группы.
40. Защита информации в рекламной и выставочной деятельности.
41. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
42. Направления защиты компьютеров и локальных сетей от несанкционированного доступа к информации.
43. Составление библиографии по проблемам экономической безопасности, защиты предпринимательской тайны и конфиденциальной информации (российская и зарубежная литература).
44. Процессуальные проблемы защиты информации в зарубежных странах.
45. Анализ существующих схем доступа персонала в помещения фирмы.
46. Аналитический обзор опыта зарубежных стран в регламентации управления персоналом, обладающим конфиденциальной информацией.
47. Аналитический обзор российского и зарубежного исторического опыта в предотвращении утраты ценной информации по вине сотрудников.
48. Анализ существующих правил поведения персонала и охраны фирмы в экстремальных ситуациях различного типа.
49. Проблемы управления персоналом и защиты информации в предпринимательской деятельности (теоретический очерк).
50. Психологические и профессиональные особенности личности человека, владеющего тайной, мотивации мышления и поведения.
51. Цели, задачи, стадии и методы работы с персоналом, обладающим конфиденциальной информацией.
52. Технологическая схема приема (перевода) сотрудников на работу, связанную с владением конфиденциальной информацией.
53. Классификация персонала фирмы и окружающих фирму людей по степени их осведомленности в тайнах фирмы, анализ каждой классификационной группы.
54. Классификация экстремальных ситуаций, угрожающих персоналу фирмы в рабочее и нерабочее время, анализ выделенных классификационных групп и методов локализации опасности.
55. Порядок и методика проведения служебного расследования по фактам нарушения правил защиты секретов фирмы.
56. Факторы, предпосылки и условия применения различных форм морального и материального стимулирования ответственного отношения сотрудников к обеспечению информационной безопасности фирмы.
57. Место и роль психологического климата в коллективе при проведении воспитательной работы в коллективе фирмы.
58. Классификация противоправных действий персонала фирмы с конфиденциальной информацией.
59. Принципы построения, организация и совершенствование пропускного режима на фирме, методика идентификации различных категорий сотрудников и посетителей.
60. Анализ функциональной и информационной взаимосвязи службы безопасности и службы персонала фирмы.

5.3. Фонд оценочных средств

Должна ли предусматривать разрешительная система доступ к конфиденциальной информации должностных лиц из внешних организаций, выполняющих совместную работу с организацией где введен режим конфиденциальности?
Выберите один из 3 вариантов ответа:
1) нет, не должна
2) да, должна
3) зависит от индивидуального решения руководителя, даже если это ставит под угрозу срыва выполнение совместных работ

Имеют ли право на доступ к различным видам конфиденциальной информации сотрудники уполномоченных органов государственной власти (налоговая служба, служба судебных приставов, органы МВД и др.)?
Выберите один из 3 вариантов ответа:
1) нет, не имеют
2) имеют, в пределах своей компетенции

3) имеют, в пределах своей компетенции, при этом обязаны обеспечить защиту полученной информации от разглашения и неправомерного использования

Укажите правильный порядок введения в действие Регламента доступа к конфиденциальной информации
Укажите порядок следования всех 6 вариантов ответа:
1) Подпись (заверение) Регламента всеми членами экспертной комиссии
2) Назначение приказом директора должностных лиц в составе Экспертной комиссии по защите конфиденциальной информации.
3) Визирование Регламента всеми лицами, имеющими право давать разрешение на доступ к КИ
4) Разработка Регламента
5) Введение в действие Регламента приказом руководителя организации
6) Ознакомление с Регламентом всех сотрудников, работающих с КИ

Кто входит в круг лиц, имеющих право давать разрешение на допуск и доступ к конфиденциальной информации? Ответов несколько.
Выберите несколько из 5 вариантов ответа:
1) Руководитель организации
2) Любой сотрудник, имеющий доступ к КИ
3) Руководитель структурного подразделения всем сотрудникам
4) Руководитель структурного подразделения в пределах своей компетенции
5) Заместитель руководителя в пределах своей сферы деятельности

В каком виде выдается разрешение на работу с конфиденциальными документами?
Выберите один из 3 вариантов ответа:
1) в устной форме
2) в виде письма по почте
3) в виде резолюции

В случае организации системы доступа к КИ с сотрудниками из других организаций какие документы будут с ними подписаны?
Выберите один из 4 вариантов ответа:
1) договор и обязательство о неразглашении
2) только договор
3) только обязательство
4) все зависит от пожеланий руководителя организации

Кто такой контрагент в рамках реализации работ с КИ со сторонней организацией?
Выберите один из 3 вариантов ответа:
1) это постороннее для организации лицо
2) это адресат
3) это сторона гражданско-правового договора

Обязан ли контрагент сообщить обладателю конфиденциальной информации о допущенном им же (контрагентом) факте разглашения КИ?
Выберите один из 2 вариантов ответа:
1) да
2) нет

Кому сотрудник сообщит о попытке посторонних лиц получить от него КИ и кому сотрудник в случае увольнения сдаст все носители КИ?
Выберите один из 4 вариантов ответа:
1) сотруднику службы конфиденциального делопроизводства и руководителю организации
2) никому ничего не должен сообщать и передавать
3) руководителю организации и сотруднику службы конфиденциального делопроизводства
4) в вариантах не перечислено этих лиц

Что относится к специальным (особым) категориям персональных данных?

Выберите один из 3 вариантов ответа:
1) состояние здоровья, политические взгляды, национальность
2) фамилия, имя, отчество
3) биометрические данные
Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Что не относится к общедоступной информации?
Информация о состоянии окружающей среды
Информация из библиотек, музеев и архивов
Информация о полномочиях органов власти
Информация о дислокации режимных объектов

Какие сведения могут относиться к государственной тайне?
Сведения в области контрразведки
Сведения в области внешней политики и экономики
Сведения в области охраны здоровья нации
Только первый и второй пункты

Какой профессиональной тайны не существует?
Тайны работника социальной службы
Тайны почтовых отправлений
Тайны работника промышленных объектов
Нотариальной тайны

В каком случае журналисты могут использовать информацию о частной жизни людей?
При наличии государственных, общественных и иных публичных интересов
В случаях, когда информация о частной жизни человека ранее стала общедоступной
Если информация о частной жизни раскрыта самим гражданином или по его воле
Во всех трех случаях

В каких случаях для использования персональных данных надо получить обязательное согласие человека?
Если осуществляется использование общедоступных персональных данных
Если публикуются данные из деклараций чиновников
Если персональные данные журналисту передал работодатель субъекта персональных данных
Если персональные данные публикуются ради общественного интереса

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=364911
Л1.3	Емельянова Н.З., Партыка Т. Л., Попов И.И.	Защита информации в персональном компьютере: Учебное пособие	Москва: Издательство "ФОРУМ", 2021, URL: https://znanium.com/catalog/document?id=365335

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2017, URL: https://book.ru/book/922538
Л2.2	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2018, URL: https://book.ru/book/931784

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Интернет университет информационных технологий ИНТУИТ . - Режим доступа: https://www.intuit.ru/studies/courses
Э2	Федеральный центр информационно-образовательных ресурсов . - Режим доступа: http://fcior.edu.ru/
Э3	Естественно-научный образовательный портал. - Режим доступа: http://www.en.edu.ru/
Э4	Единое окно доступа к образовательным ресурсам Единое окно доступа к образовательным ресурсам . - Режим доступа: http://window.edu.ru
Э5	Электронная библиотечная система Znanium. - Режим доступа: http://new.znanium.com/
Э6	Электронная библиотечная система Ibooks . - Режим доступа: http://www.ibooks.ru
Э7	Электронные ресурсы Академии ИМСИТ . - Режим доступа: http://eios.imsit.ru/
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	
6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Кодекс – Профессиональные справочные системы https://kodeks.ru
6.3.2.2	Консультант Плюс http://www.consultant.ru

7. МТО (оборудование и технические средства обучения)			
Ауд	Наименование	ПО	Оснащение
125	Лаборатория электронного документооборота	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL Archimate SMath Studio Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		gvSIG Desktop Python	
114	Кабинет защищенного документооборота	Яндекс Браузер LibreOffice Inkscape Visual Studio Code Blender Gimp Adobe Reader DC MAC OS Big Sure УМКК «Информационные технологии»	Стол - 21 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., ноутбук – 1шт., персональный компьютер - 20 шт., многофункциональное устройство – 1 шт., принтер цветной – 1шт., интерактивная панель EliteBoard LR-75UT40i7 - 1 шт., соответствующее программное обеспечение, обучающие стенды и материалы
235	Аудитория (защищаемое помещение) для проведения учебных занятий, с информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Стол – 8 шт., стул - 20 шт., рабочее место преподавателя – 1 шт., мультимедийный проектор (переносной) – 1 шт., переносной ноутбук – 1 шт., технические средства защиты
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Работа с конфиденциальной информацией». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).

Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.

Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.

Методические указания и материалы по видам учебных занятий по дисциплине:

Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Работа с конфиденциальной информацией».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями