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.О.30

Организационное и правовое обеспечение информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра педагогики и межкультурных коммуникаций**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 48
самостоятельная работа 23,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
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.	48	48	48	48
Контактная работа	48,2	48,2	48,2	48,2
Сам. работа	23,8	23,8	23,8	23,8
Итого	72	72	72	72

Программу составил(и):

к.п.н, доцент, Прилепский В.В.

Рецензент(ы):

к.псих.н., зав. каф. психологии личности и общей психологии ФГБОУ ВО "Кубанский государственный университет" , Лупенко Н.Н.;директор МАОУ СОШ№ 107, г. Краснодар , Чирухина Н.Н.

Рабочая программа дисциплины

Организационное и правовое обеспечение информационной безопасности

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 педагогики и межкультурных коммуникаций

Протокол от 30.10.2023 г. № 3

Зав. кафедрой Прилепский Вадим Владимирович

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	Сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;
1.2	Разработка нормативной и правовой документации по вопросам обеспечения информационной безопасности.
Задачи: 1. Изучить понятийный аппарат, основные понятия и категории информационного права и информационного законодательства РФ. 2. Изучить общетеоретические основы правового регулирования в сфере обеспечения национальной безопасности в информационной сфере. 3. Изучить правовой режим секретной и конфиденциальной информации, организацию защиты информации ограниченного доступа при размещении ее в информационной системе. 4. Сформировать у студентов способности самостоятельно работать с различными источниками правовой информации, государственными информационными ресурсами и системами. 5. Выработать навыки правильного толкования и применения норм информационного законодательства РФ. 6. Сформировать общекультурные, общепрофессиональные и профессиональные компетенции, необходимые для решения профессиональных задач в соответствии с видами профессиональной деятельности.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы национальной безопасности
2.1.2	Экономика
2.1.3	Право
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информационных процессов в компьютерных системах
2.2.2	Основы управления информационной безопасностью

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	
УК-10.1: Анализирует гуманитарные и правовые последствия экстремизма, терроризма и коррупционной деятельности, в том числе собственных действий или бездействий	
Знать	
Уровень 1	Минимальный необходимый уровень знаний анализа гуманитарных и правовых последствий экстремизма, терроризма и коррупционной деятельности, в том числе собственных действий или бездействий
Уровень 2	Уровень знаний правовых последствий экстремизма, терроризма и коррупционной деятельности, в том числе собственных действий или бездействий в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний правовых последствий экстремизма, терроризма и коррупционной деятельности, в том числе собственных действий или бездействий в объёме, соответствующем программе подготовки, без ошибок
УК-10.2: Выбирает правомерные формы взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях	
Уметь	
Уровень 1	Продемонстрированы основные умения выбирать правомерные формы взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения выбирать правомерные формы взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения выбирать правомерные формы взаимодействия с гражданами, структурами гражданского общества и органами государственной власти в типовых ситуациях, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	
ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний особенностей разработки проектов локальных правовых актов,

	инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации
Уровень 2	Уровень знаний особенностей разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний особенностей разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации в объёме, соответствующем программе подготовки, без ошибок
ОПК-5.2: Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	
Уметь	
Уровень 1	Продемонстрированы основные умения формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования основных требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования основных требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования основных требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации без ошибок и недочётов

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	
ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний моделей угроз и модели нарушителя объекта информатизации
Уровень 2	Уровень знаний моделей угроз и модели нарушителя объекта информатизации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний моделей угроз и модели нарушителя объекта информатизации в объёме, соответствующем программе подготовки, без ошибок
ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа	
Уметь	
Уровень 1	Продемонстрированы основные умения определения политики контроля доступа работников к информации ограниченного доступа, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определения политики контроля доступа работников к информации ограниченного доступа, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения определения политики контроля доступа работников к информации ограниченного доступа, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования требований, предъявляемых к физической защите

	объекта и пропускному режиму в организации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования требований, предъявляемых к физической защите объекта и пропускному режиму в организации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования требований, предъявляемых к физической защите объекта и пропускному режиму в организации без ошибок и недочётов
ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	
Владеть	
Уровень 1	Имеется минимальный набор навыков разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации без ошибок и недочётов

ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	
ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем	
Уметь	
Уровень 1	Продемонстрированы основные умения определения подлежащих защите информационных ресурсов автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определения подлежащих защите информационных ресурсов автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения определения подлежащих защите информационных ресурсов автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	
Уметь	
Уровень 1	Продемонстрированы основные умения составления комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения составления комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные составления комплексов правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации	
Уметь	
Уровень 1	Имеется минимальный набор навыков организации работы персонала автоматизированной системы с учетом требований по защите информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки организации работы персонала автоматизированной системы с учетом требований по защите информации с некоторыми недочётами
Уровень 3	Продемонстрированы базовые навыки Организует работу персонала автоматизированной системы с учетом требований по защите информации без ошибок и недочётов
ОПК-4.1.4: Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	
Владеть	
Уровень 1	Имеется минимальный набор навыков подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации с некоторыми недочётами
Уровень 3	Продемонстрированы базовые навыки подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее

	эксплуатации с некоторыми недочётами

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. Основы законодательства РФ по обеспечению национальной и информационной безопасности					
1.1	Основы защиты конституционного строя. Силы и средства обеспечения национальной безопасности /Лек/	5	4	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Информационная безопасность в системе национальной безопасности Российской Федерации. Национальные интересы в информационной сфере. Доктрина информационной безопасности /Пр/	5	8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	2
1.3	Информационные отношения как объект правового регулирования. Источники угроз информационной безопасности РФ. Понятие информационной войны /Ср/	5	4,8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 2. Раздел 2. Правовое обеспечение информационной безопасности.					

2.1	Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера.Правовая охрана результатов интеллектуальной деятельности. /Лек/	5	4	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.2	Преступления в сфере компьютерной информации. Правовые режимы защиты информации ведущих мировых держав /Ср/	5	5,4	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.3	Виды ответственности за нарушение законодательства в области защиты информации. УК и КАПП. /Пр/	5	8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	2
	Раздел 3. Раздел 3. Организационные методы защиты информации					
3.1	Понятие организационной защиты информации. Допуск к государственной тайне /Лек/	5	4	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

3.2	Методы обеспечения физической безопасности. Технологические меры поддержания безопасности /Пр/	5	8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	2
3.3	Организация режима секретности /Ср/	5	6,8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 4. Раздел 4. Лицензирование и сертификация в области защиты информации					
4.1	Понятие лицензирования и сертификации по российскому законодательству. Виды деятельности, подлежащие лицензированию. /Лек/	5	4	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.2	Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации /Пр/	5	8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	2

4.3	Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением условий ведения лицензионной деятельности. Организация сертификационной деятельности в области защиты информации /Ср/	5	6,8	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 5. Промежуточная аттестация					
5.1	Зачет /КА/	5	0,2	УК-10.1 УК-10.2 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-8.1 ОПК-8.2 ОПК-8.3 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Понятие, предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
2. Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.
3. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.
4. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.
5. Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.
6. Особенности правовой защиты сведений, составляющих государственную тайну.
7. Основные объекты института коммерческой тайны.
8. Субъекты информационных правоотношений, возникающих по поводу коммерческой тайны.
9. Правовой режим коммерческой тайны.
10. Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.
11. Институты профессиональных тайн и их значение для обеспечения защиты прав и свобод человека и гражданина, коммерческих интересов организаций и учреждений.
12. Основные категории сведений, защищаемых в режиме профессиональной тайны.
13. Система правового регулирования отдельных институтов профессиональных тайн.
14. Понятие и характеристика правонарушений в информационной сфере.
15. Криминалистическая характеристика преступлений в сфере компьютерной информации.
16. Ответственность за правонарушения в сфере компьютерной информации.

5.2. Темы письменных работ

1. Электронная цифровая подпись. Защита прав и законных интересов субъектов информационной сферы. Законодательство об электронной цифровой подписи. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Институты сертификата ключа электронной цифровой подписи и владельца сертификата. Институт удостоверяющих центров.

2. Организационные структуры обеспечения информационной безопасности.
Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. Административный уровень обеспечения информационной безопасности. Корпоративная нормативная база по защите информации.

3. Организация и проведение лицензирования, сертификации и аттестации.

Порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с использованием сведений, составляющих государственную тайну и иной конфиденциальной информации, созданием средств защиты информации, осуществлением мероприятий и (или) оказанием услуг по защите информации.

4. Организация и проведение лицензирования, сертификации и аттестации.

Организация и проведение специальных экспертиз предприятий (организаций). Порядок рассмотрения заявлений о выдаче лицензии. Основания для выдачи (отказе в выдаче), приостановлении действия или аннулировании лицензии.

5. Организация защиты информации на предприятии.

Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение и изменение грифа секретности документам и изделиям. Основания и порядок рассекречивания сведений (документов, изделий).

6. Организация защиты информации на предприятии.

Введение и снятие ограничения доступа к иной конфиденциальной информации. Перечни сведений, отнесенных к конфиденциальным. Полномочия по отнесению сведений к конфиденциальным и снятию грифа ограничения доступа.

7. Организация защиты информации на предприятии.

Особенности доступа различных категорий персонала и командированных лиц. Обязанности лиц, допущенных к защищаемым сведениям.

8. Организация защиты информации на предприятии.

Организация охраны объектов информатизации и персонала. Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, прочие материальные и финансовые ценности. Виды и способы охраны. Понятие о рубежах охраны. Факторы выбора приемов и средств охраны.

9. Организация защиты информации на предприятии.

Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Понятие пропуска. Порядок оформления и выдачи пропусков. Бюро пропусков и контрольно-пропускные пункты, их оборудование и организация работы. Порядок прохода и проезда на территорию объекта. Порядок вывоза (выноса), ввоза (вывоза) материальных ценностей и документации.

10. Организация защиты информации на предприятии.

Понятие внутри объектового режима. Общие требования внутри объектового режима. Организационные требования к помещениям, в которых расположены защищаемые источники информации. Порядок доступа персонала в охраняемые помещения. Создание отдельных (выделенных) производственных зон (зон доступа) с самостоятельными системами организации и контроля доступа.

11. Организация защиты информации на предприятии.

Общие требования к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам. Обязанности лиц, участвующих в переговорах и ответственных за их проведение.
Требования к помещениям, в которых проводятся совещания и переговоры. Подготовка программы проведения совещаний. Составление списков участников; порядок прохода приглашенных; документирование хода совещаний и их результатов; ведение записей; особенности использования технических средств документирования.

12. Организация защиты информации на предприятии.

Порядок реализации режимных мер в ходе подготовки и проведения совещаний и переговоров. Определение состава информации, используемой в ходе совещаний и переговоров. Документирование хода совещания (переговоров) и их результатов.

13. Организация защиты информации на предприятии.

Требования режима защиты информации при приеме посетителей. Порядок доступа посетителей к конфиденциальной информации. Порядок пребывания посетителей на объекте. Организация контроля исполнения режимных требований в период пребывания посетителей. Особенности защитных мероприятий, осуществляемых при приеме различных категорий посетителей.

14. Организация защиты информации на предприятии.

Основания для приема на объекте иностранных граждан. Требования к программе приема иностранных граждан. Основные положения плана мероприятий по обеспечению режима конфиденциальности в период пребывания иностранных граждан на объекте. Требования к помещениям, в которых проводится прием представителей другой страны.

15. Организация защиты информации на предприятии.

Порядок ознакомления иностранных граждан со сведениями, составляющими конфиденциальную информацию. Особенности документирования в процессе переговоров. Порядок пересылки (передачи) документации этим лицам. Обязанности лиц, участвующих в работе с посетителями, в том числе с иностранными гражданами. Порядок отчетности о результатах работы.

16. Организация защиты информации на предприятии.
Понятия «издательская, рекламная и выставочная деятельность», виды, формы, особенности.
Основные методы защиты информации в процессе этих видов деятельности и оценка эффективности защитных мероприятий.
Особенности издательской деятельности. Общие требования режима защиты информации при опубликовании материалов в общедоступных изданиях (СМИ).

17. Организация защиты информации на предприятии.
Порядок создания и функционирования Экспертных комиссий, процедуры представления и рассмотрения материалов, предназначенных для открытого опубликования. Основания к принятию решений по результатам рассмотрения и оценки материалов. Документирование процессов рассмотрения материалов и принятия решений.

18. Организация защиты информации на предприятии.
Разработка и проведение мероприятий по обеспечению режима конфиденциальности изделий (продукции). Организация учета. Основные требования при хранении, получении, транспортировке и уничтожении изделий. Документирование хода и результатов уничтожения изделий.

19. Организация защиты информации на предприятии.
Понятие «внутреннее (служебное) расследование» по фактам нарушения режима конфиденциальности. Основания, цели и задачи внутреннего (служебного) расследования. Процедура внутреннего (служебного) расследования.

20. Организация защиты информации на предприятии.
Права и обязанности членов комиссии по проведению внутреннего (служебного) расследования. Документирование хода и результатов внутреннего (служебного) расследования. Взаимодействие с правоохранительными и судебными органами.

5.3. Фонд оценочных средств

1. Какие преступления относятся к преступлениям в сфере компьютерной информации?

а) создание вредоносных компьютерных программ;

б) распространение порнографических материалов с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

в) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

г) все ответы правильные.

2. Родовым объектом преступлений в сфере компьютерной информации являются:

а) экономическая безопасность;

б) отношения в сфере охраны авторского права;

в) информационная безопасность;

г) общественная безопасность и общественный порядок.

3. Субъектом преступлений в сфере компьютерной информации является:

а) юридическое или физическое лицо, не имеющие разрешения для работы с информацией определенной категории;

б) физическое, вменяемое лицо, достигшее 18-летнего возраста;

в) физическое, вменяемое лицо, достигшее 16-летнего возраста;

г) физическое лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

4. К компьютерной информации относятся:

а) собственно информационные ресурсы (базы данных, текстовые, графические файлы и т.д.), представленные в форме электрических сигналов;

б) программы, обеспечивающие функционирование компьютера или информационно-телекоммуникационных сетей, хранение, обработку и передачу данных;

в) информация на машинном носителе, в компьютере или информационно-телекоммуникационных сетях;

г) все ответы правильные.

5. Преступление, предусмотренное ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» считается оконченным:

а) с момента совершения неправомерного доступа к охраняемой законом компьютерной информации;

б) только в случае уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) только при наступлении тяжких последствий в случае уничтожения, блокирования, модификации либо копирования компьютерной информации;

г) все ответы правильные.

6. В ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» не предусмотрена уголовная ответственность за:

а) внесение изменений в существующие программы;

б) распространение машинных носителей с вредоносными программами;

в) несанкционированное копирование охраняемой законом компьютерной информации;

г) нет правильного ответа.

7. Преступление, предусмотренное ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», считается оконченным:

а) только при наступлении тяжких последствий;

б) только в случае несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) с момента использования или распространения вредоносной программы;

г) с момента создания, использования или распространения вредоносной программы.

8. Субъектом преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», является:

а) физическое, вменяемое лицо, достигшее 16-летнего возраста;

б) физическое, вменяемое лицо, достигшее 18-летнего возраста;

в) лицо, имеющее право на доступ к компьютеру или информационно-телекоммуникационным сетям;

г) лицо, не имеющее права на доступ к компьютеру или информационно-телекоммуникационным сетям.

9. В числе квалифицирующих признаков в ст. 273 УК РФ предусмотрено совершение данного преступления:

а) с целью скрыть другое преступление или облегчить его совершение;

б) из корыстной заинтересованности;

в) из хулиганских побуждений;

г) по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы.

10. Преступление, предусмотренное ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», считается оконченным:

а) с момента нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

б) с момента уничтожения, блокирования, модификации либо копирования компьютерной информации;

в) если это деяние причинило крупный ущерб;

г) только при наступлении тяжких последствий.

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). 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	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2023, URL: https://znanium.com/catalog/document?id=418929
Л1.2	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2023, URL: https://znanium.com/catalog/document?id=416550
Л1.3	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2023, URL: https://znanium.com/catalog/document?id=420080

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Партыка Т. Л., Попов И.И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2020, URL: https://znanium.com/catalog/document?id=353520
Л2.2	Партыка Т. Л., Попов И.И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2021, URL: https://znanium.com/catalog/document?id=364624

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	Электронная библиотечная система BOOK.ru . - Режим доступа: http://www.book.ru
Э8	Электронные ресурсы Академии ИМСИТ. - Режим доступа: http://eios.imsit.ru/
Э9	Web-ресурс «Официальный сайт Академии ИМСИТ . - Режим доступа: http://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
123	Кабинет информационной безопасности	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 Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	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
4	Кабинет правовых дисциплин	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Стол - 14 шт., стул - 29 шт., рабочее место преподавателя – 1 шт., доска учебная – 1 шт., персональный компьютер – 1 шт., многофункциональное устройство– 1 шт., мультимедийный проектор– 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение, учебно-наглядные методические пособия
114а	Лаборатория программно-аппаратных средств защиты информации	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	Стол - 20 шт., стул - 22 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., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт.,

		Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
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 «Организационное и правовое обеспечение информационной безопасности». 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 «Организационное и правовое обеспечение информационной безопасности».
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