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.08

Введение в направление подготовки и планирование профессиональной карьеры

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 48
самостоятельная работа 59,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 1

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		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
Итого ауд.	48	48	48	48
Контактная работа	48,2	48,2	48,2	48,2
Сам. работа	59,8	59,8	59,8	59,8
Итого	108	108	108	108

Программу составил(и):
к.э.н., доцент, Исикова Н.П.

Рецензент(ы):
д.т.н., профессор кафедры информационных систем и программирования КубГТУ, Видовский Л.А.

Рабочая программа дисциплины
Введение в направление подготовки и планирование профессиональной карьеры

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	Формирование у студентов базовых знаний о принципах развития
1.2	современных средств вычислительной техники, интеллектуальных систем,
1.3	основных методах проектирования интеллектуальных систем и основ нормативных
1.4	документов и стандартов в области проектирования.
Задачи: – освоение теоретических основ организации современной вычислительной техники; – изучение современных проблем развития средств вычислительной техники и способов их преодоления; - получение опыта участия в проектных работах в области создания информационных и интеллектуальных систем; – изучение правил составления технической документации.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Гуманитарные аспекты информационной безопасности
2.2.2	Основы национальной безопасности
2.2.3	Организационное и правовое обеспечение информационной безопасности

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
УК-6: Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	
УК-6.1: Использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей	
Знать	
Уровень 1	Минимальный необходимый уровень знаний использования инструментов и методов управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей
Уровень 2	Уровень знаний использования инструментов и методов управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний использования инструментов и методов управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей в объёме, соответствующем программе подготовки, без ошибок
УК-6.2: Определяет задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения	
Уметь	
Уровень 1	Продемонстрированы основные умения определять задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определять задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все определять задачи саморазвития и профессионального роста, распределяет их на долго-, средне- и краткосрочные с обоснованием актуальности и определением необходимых ресурсов для их выполнения, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
УК-6.3: Использует основные возможности и инструменты непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы развития деятельности и требований рынка труда	
Владеть	
Уровень 1	Имеется минимальный набор навыков использования основных возможностей и инструментов непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы развития деятельности и требований рынка труда с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки использования основных возможностей и инструментов непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом

	личностных возможностей, временной перспективы развития деятельности и требований рынка труда с некоторыми недочётами
Уровень 3	Продемонстрированы навыки использования основных возможностей и инструментов непрерывного образования (образования в течение всей жизни) для реализации собственных потребностей с учетом личностных возможностей, временной перспективы развития деятельности и требований рынка труда без ошибок и недочётов

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 анализа гуманитарных и 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 анализа гуманитарных и 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 ситуация, 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 ситуация, 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 ситуация, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

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	Краткий исторический экскурс в развитие средств информационной безопасности /Лек/	1	4	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.2	Краткий исторический экскурс в развитие средств информационной безопасности /Ср/	1	12	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.3	Краткий исторический экскурс в развитие средств информационной безопасности /Пр/	1	8	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.4	Основные направления развития информационной безопасности /Лек/	1	4	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.5	Основные направления развития информационной безопасности /Ср/	1	23,8	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.6	Основные направления развития информационной безопасности /Пр/	1	8	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	

1.7	Основные препятствия на пути развития информационной безопасности /Лек/	1	4	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.8	Основные препятствия на пути развития информационной безопасности /Ср/	1	12	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.9	Основные препятствия на пути развития информационной безопасности /Пр/	1	8	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.10	Перспективы эволюционного развития средств информационной безопасности /Лек/	1	4	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.11	Перспективы эволюционного развития средств информационной безопасности /Ср/	1	12	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
1.12	Перспективы эволюционного развития средств информационной безопасности /Пр/	1	8	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	
	Раздел 2. Промежуточная аттестация					
2.1	Зачет /КА/	1	0,2	УК-6.1 УК-6.2 УК-6.3 УК-10.1 УК-10.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в программе « цифровая экономика».
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.
29. Организационное обеспечение ИБ.
30. Организация конфиденциального делопроизводства.
31. Организационно-экономическое обеспечение ИБ.
32. Инженерно-техническое обеспечение компьютерной безопасности.

33. Организационно-правовой статус службы безопасности.
34. Защита информации в Интернете.
35. Электронная почта и ее защита.
36. Защита от компьютерных вирусов.
37. «Больные» мобильники и их «лечение».
38. Популярные антивирусные программы и их классификация.
39. Этапы и освоение защиты информации экономических объектов.
40. Криптографические методы защиты информации.
41. Оценка эффективности инвестиций в информационную безопасность.
42. Российские компании в сфере ИБ.
43. Фирмы, оценивающие работу персонала в компании.
44. Менеджмент и аудит ИБ на уровне предприятия.
45. Аудит ИБ автоматизированных банковских систем.
46. Аудит ИБ электронной коммерции.
47. Информационная безопасность предпринимательской деятельности.

5.2. Темы письменных работ

1.Методы борьбы с фишинговыми атаками.

2.Законодательство о персональных данных.

3.Защита авторских прав.

4.Назначение, функции и типы систем видеозащиты.

5.Как подписывать с помощью ЭЦП электронные документы различных форматов.

6.Обзор угроз и технологий защиты Wi-Fi-сетей.

7.Проблемы внедрения дискового шифрования.

8.Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

9.Особенности процессов аутентификации в корпоративной среде.

10.Квантовая криптография.

11.Утечки информации: как избежать. Безопасность смартфонов.

12.Безопасность применения пластиковых карт - законодательство и практика.

13.Защита CD- и DVD-дисков от копирования.

14.Современные угрозы и защита электронной почты.

15.Программные средства анализа локальных сетей на предмет уязвимостей.

16.Безопасность применения платежных систем - законодательство и практика.

17.Аудит программного кода по требованиям безопасности.

18.Антишпионское ПО (antispyware).

19.Обеспечение безопасности Web-сервисов.

20.Защита от внутренних угроз.

21.Технологии RFID.

22.Уничтожение информации на магнитных носителях.

23.Ботнеты - плацдарм современных кибератак.

24.Цифровые водяные знаки в изображениях.

25.Электронный документооборот. Модели нарушителя.

26.Идентификация по голосу. Скрытые возможности.

27.Безопасность океанских портов.

28.Безопасность связи.

29.Безопасность розничной торговли.

30.Банковская безопасность.

31.Информатизация управления транспортной безопасностью.

32.Биопаспорт.

33.Обзор современных платформ архивации данных.

34.Что такое консалтинг в области ИБ.

35.Бухгалтерская отчетность как источник рассекречивания информации.

36.Управление рисками: обзор употребительных подходов.

37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38.Распределенные атаки на распределенные системы.

39.Оценка безопасности автоматизированных систем.

40.Windows и Linux: что безопаснее?

41.Функциональная безопасность программных средств.

42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43.Информационная безопасность: экономические аспекты.

5.3. Фонд оценочных средств

1) К правовым методам, обеспечивающим информационную
безопасность, относятся:
Разработка аппаратных средств обеспечения правовых данных
Разработка и установка во всех компьютерных правовых сетях журналов
учета действий
Разработка и конкретизация правовых нормативных актов обеспечения
безопасности
2) Основными источниками угроз информационной безопасности
являются все указанное в списке:
Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение
регламента работы
3) Виды информационной безопасности:
Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение,
предупреждение:
несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
Компьютерный сбой
Логические закладки («мины»)
Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
Электронно-цифровой преобразователь
Электронно-цифровая подпись
Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
Покупка нелицензионного ПО
Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных
20) Наиболее распространены средства воздействия на сеть офиса:
Слабый трафик, информационный обман, вирусы в интернет
Вирусы в сети, логические мины (закладки), информационный перехват
Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация,

характеризуемая:
Потерей данных в системе
Изменением формы информации
Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
Целостность
Доступность
Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
Вероятное событие
Детерминированное (всегда определенное) событие
Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
Регламентированной
Правовой
Защищаемой
25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
Программные, технические, организационные, технологические
Серверные, клиентские, спутниковые, наземные
Личные, корпоративные, социальные, национальные
26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
Владелец сети
Администратор сети
Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций

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	Москва: Форум, 2021, URL: https://ibooks.ru/reading.php?short=1&productid=361273
Л1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2019, URL: https://book.ru/book/932909
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	Самойлов В.Д.	Информационная безопасность в системе высшего образования России (компетентностный подход в подготовке специалистов). Монография: Монография	Москва: Русайнс, 2018, URL: https://book.ru/book/930048

	Авторы, составители	Заглавие	Издательство, год
Л2.2	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2022, URL: https://book.ru/book/944143

6.2. Электронные учебные издания и электронные образовательные ресурсы	
Э1	Интернет университет информационных технологий. - Режим доступа: https://www.intuit.ru/studies/courses%20
Э2	Естественно-научный образовательный портал. - Режим доступа: http://www.en.edu.ru/
Э3	Электронная библиотечная система Znanium. - Режим доступа: http://znanium.com/%20
Э4	Электронная библиотечная система Ibooks. - Режим доступа: http://www.ibooks.ru/
Э5	Электронная библиотечная система BOOK.ru. - Режим доступа: http://rpd.eios.imsit.ru:8080/RPD/Index/1636711/%20http://www.book.ru
Э6	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	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	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	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

		Python	
121	Компьютерный класс	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 ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack 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
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 «Введение в направление подготовки и планирование профессиональной карьеры». 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

Самостоятельная работа студентов в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических и интерактивных занятиях, а также для индивидуального изучения дисциплины «Введение в направление подготовки и планирование профессиональной карьеры» в соответствии с программой и рекомендованной литературой.
Самостоятельная работа выполняется в виде подготовки домашнего задания или сообщения по отдельным вопросам, написание и защита научно-исследовательского проекта.
Контроль качества выполнения самостоятельной (домашней) работы может осуществляться с помощью устного опроса на лекциях или практических занятиях, обсуждения подготовленных научно-исследовательских проектов, проведения тестирования.
Устные формы контроля помогут оценить владение студентами жанрами научной речи (дискуссия, диспут, сообщение, доклад и др.), в которых раскрывается умение студентов передать нужную информацию, грамотно использовать языковые средства, а также ораторские приемы для контакта с аудиторией.
Письменные работы позволяют оценить владение источниками, научным стилем изложения, для которого характерны: логичность, точность терминологии, обобщенность и отвлеченность, насыщенность фактической информацией.