Министерство культуры Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
**«КРАСНОДАРСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ»**
Факультет гуманитарного образования
Кафедра информационно-библиотечной деятельности и документоведения

УТВЕРЖДАЮ
Зав. кафедрой ИБДиД
_____ А.В.Штратникова
«20» шкуна 2023 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

## Б1.О.30 Информационная безопасность и защита информации

Направление подготовки – 51.03.06 Библиотечно-информационная деятельность

Профиль подготовки - «Технология автоматизированных библиотечно-информационных систем»

Квалификация (степень) выпускника – бакалавр

Форма обучения – очная, заочная

Краснодар
2023

Рабочая программа предназначена для преподавания дисциплины «Информационная безопасность и защита информации» базовой части студентам очной и заочной формы обучения в качестве дисциплины по выбору по направлению подготовки 51.03.06 Библиотечно-информационная деятельность в 3-4 семестрах.

Рабочая программа учебной дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки 51.03.06 Библиотечно-информационная деятельность, утвержденному приказом Министерства образования и науки Российской Федерации от 06 декабря 2017 года № 1182 и основной профессиональной образовательной программой.

**Рецензенты:**
Заслуженный работник культуры РФ, Директор Централизованной библиотечной системы г. Краснодара — Е.А. Мирошниченко

Доктор педагогических наук, доцент, профессор кафедры социально-культурной деятельности ФГБОУ ВО «Краснодарский государственный институт культуры» — Д.А. Горбачева

**Составитель:**
Багдасарян Р.Х., к.т.н., доцент

Рабочая программа учебной дисциплины рассмотрена и утверждена на заседании кафедры ИБДиД «20» марта 2023 г. протокол № 11.

Рабочая программа учебной дисциплины Б1.О.30 «Информационная безопасность и защита информации» одобрена и рекомендована к использованию в учебном процессе Учебно-методическим советом ФГБОУ ВО «КГИК» «30» марта 2023 г. протокол № 8.

## Содержание

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цели** освоения дисциплины (модуля)

- освоение методики и технологий защиты информации и информационной безопасности;

**Задачи:**

- изучить виды доступа к информации
- рассмотреть способы защиты информации
- выяснить методы шифрования и дешифрования информации

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к элективным дисциплинам части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)».

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С УСТАНОВЛЕННЫМИ В ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ.

В результате освоения дисциплины обучающиеся должны демонстрировать следующие результаты.

| Наименование компетенций | Индикаторы сформированности компетенций | | |
|---|---|---|---|
| | знать | уметь | владеть |
| Готовность к инновационно-проектной деятельности в библиотечно-информационной сфере, внедрению цифровых технологий в организацию и использование электронных информационных систем (ПК-4) | Классификацию, технологии создания различных видов электронных информационных ресурсов | Проводить сравнительный анализ электронных информационных ресурсов; выявлять целевые группы пользователей электронных информационных ресурсов и их информационные потребности; принимать решения по выбору обеспечивающих средств создания и модернизации различны видов | Общей и специальными технологиями создания электронных информационных ресурсов |

| | | | |
|---|---|---|---|
| | | электронных информационных ресурсов | |

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 4.1. Структура дисциплины

### Очная форма обучения

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

| № | Раздел дисциплины | Семестр | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)* |
|---|---|---|---|---|---|---|---|
| | | | Л | ПЗ | ИЗ | СР | |
| 1 | Раздел I. Концептуальные основы информационной безопасности и защиты информации | 3 | 12 | 16 | | 10 | |
| 2 | Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации | 3 | 12 | 16 | | 10 | |
| 3 | Раздел III. Организация и документационное обеспечение защиты информации | 4 | 12 | 16 | | 10 | |
| 4 | Раздел 4. Правовое обеспечение защиты информации | 4 | 12 | 16 | | 11 | |
| | итого | | 48 | 64 | | 41 | 27 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | 180 |

## 4.2. Тематический план освоения дисциплины по видам учебной деятельности и виды самостоятельной (внеаудиторной) работы

| Наименование разделов и тем | Содержание учебного материала (темы, перечень раскрываемых вопросов): лекции, практические занятия (семинары), индивидуальные занятия, самостоятельная работа обучающихся, курсовая работа | Объем часов / з.е. | Формируемые компетенции (по теме) |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| **3-4 семестр** | | | |
| **Раздел I. Концептуальные основы информационной безопасности и защиты информации** | | | |
| **Тема 1.1.** Правовое регулирование информационной безопасности и защиты информации | Лекции:<br>Понятия правового регулирования и информационных документов. Федеральный закон "об информации, информатизации и защите информации", законы РФ "о безопасности", "о средствах массовой информации", "о правовой охране программ для ЭВМ и баз данных" и др. Гражданский и уголовный кодексы РФ об ответственности за противоправные действия информационного характера. Указы президента России и постановления информационной безопасности.<br>Государственная система защиты информации. Деятельность федеральных органов государственной власти (федеральной службы безопасности, федерального агентства правительственной связи и информации при президенте РФ государственной технической комиссии при президенте РФ) в сфере информационной безопасности. Система нормативных подзаконных актов по защите информации. | *4* | ПК-4 |
| | Практические занятия (семинары):<br>Компьютерные преступления: классификация, особенности, характерные черты, мотивы, основные виды, способы обнаружения. | *6* | |
| | | | |
| | Самостоятельная работа<br>Реферат по теме: Лицензирование деятельности и сертификация продуктов и услуг в области защиты информации. | *6* | |

| | | | |
|---|---|---|---|
| | Аттестация объектов информатики. | | |
| **Тема 1.2.** Угрозы информационной безопасности и противодействие угрозам | Лекции:<br>Понятие угрозы информационной безопасности. Источники угроз, классификация угроз по цели реализации, способу и объекту воздействия.<br>Угрозы информационной безопасности России: виды, внешние и внутренние источники. Угрозы конституционным правам и свободам граждан; угрозы духовной жизни общества; угрозы информационной инфраструктуре и ресурсам.<br>Дестабилизирующие факторы: типы, источники, классификация.<br>Органы добывания информации и основные сферы их интересов. Техническая и агентурная разработка. Легальные и нелегальные способы добывания информации. Условия и методы несанкционированного доступа к добываемой информации. Основные способы дистанционного добывания информации: наблюдение, подслушивание, перехват. Общие принципы добывания и защиты информации.<br>Инженерная защита и техническая охрана объектов. Информационное и энергетическое скрытие. Дезинформирование, маскировка, ослабление сигнала, зашумление.<br>Понятие абсолютной системы защиты. | *4* | ПК-4 |
| | Практические занятия (семинары)<br>Обсуждение тем: Специфические принципы защиты информации. Многозональность и многорубежность защитных мероприятий. Классификация методов защиты информации. | *6* | |
| | | | |
| | Самостоятельная работа<br>Разработать схему устранения информационных угроз | *6* | |
| **Тема 1.3.** Каналы утечки информации | Лекции:<br>Понятие утечки информации, канала утечки технического канала утечки. Особенности утечки информации по сравнению с утечкой материальных объектов.<br>Структура канала передачи информации. Отличия канала утечки от функционального канала; понятие опасного сигнала. Виды источников сигнала, | *4* | ПК-4 |

| | | | |
|---|---|---|---|
| | функции передатчика и приемника сигнала, параметры среды распространения.<br>Классификация кадров утечки по физической природе носителя, информативности, структуре, времени появления и действия. Основные показатели, характеризующие каналы утечки.<br>Сравнительная характеристика каналов утечки. Комплексное использование каналов утечки.<br>Оптический канал утечки информации. Особенности и структура оптического канала утечки. Среда распространения, основные виды приемников сигнала. Сравнительная характеристика фотографических, телевизионных изображений в ИК-диапазоне. Противодействие наблюдению в оптическом диапазоне. Способы маскировки и энергетического скрытия объекта защиты.<br>Акустический канал утечки информации. Структура, источники сигналов, среда распространения акустического канала утечки. Характеристики акустических волн как носителей информации, условия их затухания и поглощения. Составные акусто-радиоэлектронный и акусто-оптический каналы, их структура.<br>Способы и средства подслушивания. Классификация закладных устройств.<br>Противодействие подслушиванию. Информационное скрытие: техническое закрытие и шифрование телефонных переговоров, сравнительная характеристика маскираторов, скремблеров и вокодеров. Энергетическое скрытие: звукоизоляция, поглощение акустической волны, акустическое и вибрационное зашумление. Предотвращение несанкционированной записи речевой информации на магнитофон.<br>Обнаружение закладных устройств, определение их принадлежности и подавление. Демаскирующие признаки микрофонных, некамуфлированных и камуфлированных радиозакладок. Основные виды контроля отсутствия закладных устройств. Сущность, порядок | | |

| | | | |
|---|---|---|---|
| | осуществления и оборудование для оперативного визуального осмотра. Особенности и сроки проведения профилактического периодического контроля. Проверка помещения после капитального ремонта. Распознавание предметов с подозрением на наличие в них закладок, проверка представительских подарков. Выбор рационального состава средств для контроля помещений.<br>Радиоэлектронный канал утечки информации. Особенности, структура, среда распространения радиоэлектронного канала утечки, основные виды радиоэлектронных каналов. Виды носителей информации и их классификация. Помехи и их классификация по источникам возникновения. Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование источников поля. | | |
| | <u>Практические занятия (семинары)</u><br>Семинар:<br>- Материально-вещественный канал утечки информации.<br>- Источники и носители информации.<br>-Структура канала.<br>- Способы предотвращения утечки информации.<br>- Защита информации в отходах деятельности организации.<br>- Защита демаскирующих веществ. | *6* | |
| | | | |
| | <u>Самостоятельная работа</u><br>Презентация на темы: Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование источников поля. | *6* | |
| **Тема 1.4.** Криптографическая защита информации | <u>Лекции:</u><br>Понятия категории, криптографии, криптоанализа. Главные задачи криптографии и ее отличия от кодирования и стеганографии (тайнописи). Виды криптографических атак.<br>Обобщенная схема криптографической системы и основные варианты ее реализации. Симметричная и ассиметричная криптосистемы. Понятия | *8* | ПК-4 |

| | | | |
|---|---|---|---|
| | криптографической защиты, криптографического преобразования, шифра, ключа, имитовставки. Основные характеристики шифров, требования к шифрам, их основные виды.<br>Принципы рассеивания и перемещения как основа современных симметричных криптосистем. Составные шифры, перестановки и подстановки. Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики.<br>Критерии отнесения средств защиты информации к криптографическим. Сравнительная характеристика аппаратных и программных криптографических средств. Функции криптосредств, критически важные для поддержания надежности систем защиты информации. Критерии оценки и выбора криптосредств.<br>Основные режимы шифрования. Архивное шифрование, шифрование при работе в криптографической сети, обработка файлов в интерактивном и пакетном режимах, "прозрачный" режим шифрования.<br>Система ключевой информации. Понятия узла замены, главного, условленного, файлового ключей, ключа пользователя, пароля. Имитовставка: назначение, вычисление и проверка. Проблемы, возникающие при использовании ключей, и пути их решения.<br>Работа в криптографической сети при возможности связи каждого узла сети с любым другим. Понятия сетевой таблицы, ключа сетевой таблицы, сетевого ключа, сетевого набора, ключа сетевого набора. Обмен ключевой информацией между администратором и узлами сети.<br>Организация криптографической сети по схеме "звезда". Действия администратора сети и оператора узла при обмене ключевой информацией.<br>Сравнительный анализ двух схем построения криптографической сети. Общие рекомендации по работе с ключевой информацией. | | |
| | <u>Практические занятия (семинары)</u><br>Семинар:<br>- Принципы рассеивания и перемещения как основа современных симметричных | *6* | |

| | | | |
|---|---|---|---|
| | криптосистем.<br>- Составные шифры, перестановки и подстановки. | | |
| | | | |
| | Самостоятельная работа<br>Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики. | *4* | |
| **Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации** | | | |
| **Тема 2.1.**<br>Защита информации от компьютерных вирусов и других программ с потенциально опасными последствиями | Лекции:<br>Понятие программы с потенциально опасными последствиями, основные функции и виды этих программ.<br>Понятие компьютерного вируса, основные свойства вирусов. Классификация вирусов по среде обитания, алгоритму действия, деструктивным возможностям. Файловые, заголовочные, сетевые, макровирусы. Резидентные вирусы; вирусы, использующие «стелс»-алгоритмы и другие нестандартные приемы. Источники вирусов, основные правила защиты. Антивирусные программы, их типы, сравнительный анализ возможностей, методика использования. | *4* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар:<br>- Программные закладки, их классификация по месту внедрения и применения, основные функции.<br>- Организационно-технические меры защиты от вирусов и закладок. | *8* | |
| | | | |
| | Самостоятельная работа<br>Тест по теме | *6* | |
| **Тема 2.2.**<br>Защита информации в компьютерных сетях | Лекции:<br>Возможности, предоставляемые злоумышленнику общедоступными сетями, и недостатки основных сервисов Интернет с точки зрения информационной безопасности. Межсетевые экраны. Основные требования, предъявляемые к межсетевым экранам, их функции, компоненты межсетевых экранов и их разновидности. Фильтрующие маршрутизаторы, шлюзы сетевого и прикладного уровней. Криптографические маршрутизаторы. Организационные меры обеспечения сетевой информационной безопасности. | *4* | ПК-4 |
| | Практические занятия (семинары) | *8* | |

| | | | |
|---|---|---|---|
| | Работа с криптографическими маршрутизаторами. | | |
| | | | |
| | Самостоятельная работа<br>Реферат по теме | *6* | |
| **Раздел III. Организация и документационное обеспечение защиты информации** | | | |
| **Тема: 3.1.**<br>Документация по защите информации | Лекции:<br>Основные виды документов по защите информации: федеральные законы, локальные нормативные акты | *6* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№1<br>Правовые аспекты создания и распространения информации.<br>1.Информация как объект правового регулирования.<br>2.Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др. | *4* | |
| | | | |
| | Самостоятельная работа<br>Реферат по теме | *4* | |
| **Тема: 3.2.**<br>Система защиты информации | Лекции:<br>Основные способы построения системы защиты информации | *6* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№2.<br>Информационные ресурсы: классификация и характеристика их информационных свойств.<br>1.Основы правового режима информационных ресурсов.<br>Информационные ресурсы как элемент состава имущества и объект права собственности.<br>2. Государственные информационные ресурсы. Пользование информационными ресурсами.<br>3. Информационные ресурсы в условиях рыночных отношений. | *4* | |
| | | | |
| | Самостоятельная работа<br>«Стратегия развития информационного общества в Российской Федерации» | *3* | |
| **Раздел IV. Правовое обеспечение защиты информации** | | | |
| **Тема: 4.1.**<br>Основные правовые | Лекции:<br>Основные правовые документы, касающиеся защиты информации | *6* | ПК-4 |

| | | | |
|---|---|---|---|
| документы защиты информации | Практические занятия (семинары)<br>Семинар№3, №4<br>Защита информации и прав субъектов в области информационных процессов и информатизации<br>1. Защита информации и ее цели.<br>2. Характеристика основных методов и средств защиты информации.<br>3. Права и обязанности субъектов в области защиты информации.<br>4. Защита прав субъектов в сфере информационных процессов и информатизации.<br>5. Защита прав на доступ к информации. | *4* | |
| | | | |
| | Самостоятельная работа<br>Закон «О персональных данных» | | |
| Тема:<br>4.2. Управление процессом защиты информации | Лекции:<br>Основные процессы управления защитой информации | *6* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№5,6<br>Интеллектуальная собственность, как объект правовой охраны.<br>1.Понятие интеллектуальной собственности и система ее правовой охраны.<br>2.Основные институты права интеллектуальной собственности.<br>3.Система Российского законодательства об интеллектуальной собственности.<br>4.История развития Российского законодательства об охране интеллектуальной собственности. | *4* | |
| | | | |
| | Самостоятельная работа<br>Итоговый тест по дисциплине | | |
| Примерная тематика курсовой работы *(если предусмотрено)* | | | |
| Самостоятельная работа обучающихся над курсовой работой *(если предусмотрено)* | | | |
| **Вид итогового контроля** (зачет, экзамен, дифференцированный зачет) | | *Зачет, экзамен (27)* | |
| **ВСЕГО:** | | *180* | |

**Заочная форма обучения**

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

| № п/п | Раздел | Семестр | Виды учебной работы, включая самостоятельную работу студентов | Формы текущего контроля успеваемости *(по неделям* |
|---|---|---|---|---|

| | дисциплины | | и трудоемкость (в часах) | | | | *семестра)* Форма промежуточной аттестации *(по семестрам)* |
|---|---|---|---|---|---|---|---|
| | | | Л | ПЗ | ИЗ | СР | |
| 1 | Раздел I. Концептуальные основы информационной безопасности и защиты информации | 3 | 2 | 2 | | 40 | |
| 2 | Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации | 3 | 4 | 4 | | 40 | Зачет |
| 3 | Раздел III. Организация и документационное обеспечение защиты информации | 4 | 2 | 2 | | 40 | |
| 4 | Раздел 4. Правовое обеспечение защиты информации | 4 | 4 | 4 | | 16 | Экзамен |
| | итого | | 12 | 12 | | 136 | 20 |

**Тематический план освоения дисциплины по видам учебной деятельности и виды самостоятельной (внеаудиторной) работы**

| **Наименование разделов и тем** | **Содержание учебного материала (темы, перечень раскрываемых вопросов): лекции, практические занятия (семинары), индивидуальные занятия, самостоятельная работа обучающихся, курсовая работа** | **Объем часов / з.е.** | **Формируемые компетенции (по теме)** |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| **3-4 семестр** | | | |
| **Раздел I. Концептуальные основы информационной безопасности и защиты информации** | | | |

| | | | |
|---|---|---|---|
| **Тема 1.1.** Правовое регулирование информационной безопасности и защиты информации | Лекции:<br>Понятия правового регулирования и информационных документов.<br>Государственная система защиты информации. Деятельность федеральных органов государственной власти в сфере информационной безопасности. Система нормативных подзаконных актов по защите информации. | *1* | ПК-4 |
| | Практические занятия (семинары):<br>Компьютерные преступления: классификация, особенности, характерные черты, мотивы, основные виды, способы обнаружения. | *1* | |
| | | | |
| | Самостоятельная работа<br>Реферат по теме: Лицензирование деятельности и сертификация продуктов и услуг в области защиты информации. Аттестация объектов информатики. | *20* | |
| **Тема 1.2.** Угрозы информационной безопасности и противодействие угрозам | Лекции:<br>Понятие угрозы информационной безопасности. Источники угроз, классификация угроз по цели реализации, способу и объекту воздействия.<br>Угрозы информационной безопасности России: виды, внешние и внутренние источники. Угрозы конституционным правам и свободам граждан; угрозы духовной жизни общества; угрозы информационной инфраструктуре и ресурсам | *1* | ПК-4 |
| | Практические занятия (семинары)<br>Обсуждение тем: Специфические принципы защиты информации. Многозональность и многорубежность защитных мероприятий. Классификация методов защиты информации. | *1* | |
| | | | |
| | Самостоятельная работа<br>Разработать схему устранения информационных угроз | *20* | |
| **Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации** | | | |
| **Тема 2.1.** Защита информации от компьютерных вирусов и других программ | Лекции:<br>Понятие программы с потенциально опасными последствиями, основные функции и виды этих программ. | *1* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар: | *1* | |

| | | | |
|---|---|---|---|
| с потенциально опасными последствиями | - Программные закладки, их классификация по месту внедрения и применения, основные функции.<br>- Организационно-технические меры защиты от вирусов и закладок. | | |
| | | | |
| | Самостоятельная работа<br>Тест по теме | *20* | |
| **Тема 2.2.** Защита информации в компьютерных сетях | Лекции:<br>Возможности, предоставляемые злоумышленнику общедоступными сетями, и недостатки основных сервисов Интернет с точки зрения информационной безопасности. | *2* | ПК-4 |
| | Практические занятия (семинары)<br>Работа с криптографическими маршрутизаторами. | *2* | |
| | | | |
| | Самостоятельная работа<br>Реферат по теме | *20* | |
| **Раздел III. Организация и документационное обеспечение защиты информации** | | | |
| **Тема: 3.1.** Документация по защите информации | Лекции:<br>Основные виды документов по защите информации: федеральные законы, локальные нормативные акты | *1* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№1<br>Правовые аспекты создания и распространения информации.<br>1.Информация как объект правового регулирования.<br>2.Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др. | *1* | |
| | | | |
| | Самостоятельная работа<br>Реферат по теме | *20* | |
| **Тема: 3.2.** Система защиты информации | Лекции:<br>Основные способы построения системы защиты информации | *2* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№2.<br>Информационные ресурсы: классификация и характеристика их информационных свойств.<br>1.Основы правового режима информационных ресурсов.<br>Информационные ресурсы как элемент | *2* | |

| | | | |
|---|---|---|---|
| | состава имущества и объект права собственности.<br>2. Государственные информационные ресурсы. Пользование информационными ресурсами.<br>3. Информационные ресурсы в условиях рыночных отношений. | | |
| | | | |
| | Самостоятельная работа<br>«Стратегия развития информационного общества в Российской Федерации» | *10* | |
| **Раздел IV. Правовое обеспечение защиты информации** | | | |
| **Тема: 4.1.**<br>Основные правовые документы защиты информации | Лекции:<br>Основные правовые документы, касающиеся защиты информации | *2* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№3, №4<br>Защита информации и прав субъектов в области информационных процессов и информатизации<br>1. Защита информации и ее цели.<br>2. Характеристика основных методов и средств защиты информации.<br>3. Права и обязанности субъектов в области защиты информации.<br>4. Защита прав субъектов в сфере информационных процессов и информатизации.<br>5. Защита прав на доступ к информации. | *2* | |
| | | | |
| | Самостоятельная работа<br>Закон «О персональных данных» | *10* | |
| Тема:<br>4.2. Управление процессом защиты информации | Лекции:<br>Основные процессы управления защитой информации | *2* | ПК-4 |
| | Практические занятия (семинары)<br>Семинар№5,6<br>Интеллектуальная собственность, как объект правовой охраны.<br>1.Понятие интеллектуальной собственности и система ее правовой охраны.<br>2.Основные институты права интеллектуальной собственности.<br>3.Система Российского законодательства об интеллектуальной собственности.<br>4.История развития Российского законодательства об охране интеллектуальной собственности. | *2* | |
| | | | |
| | Самостоятельная работа<br>Итоговый тест по дисциплине | *16* | |

| | | |
|---|---|---|
| Примерная тематика курсовой работы *(если предусмотрено)* | | |
| Самостоятельная работа обучающихся над курсовой работой *(если предусмотрено)* | | |
| **Вид итогового контроля** (зачет, экзамен, дифференцированный зачет) | *Зачет, экзамен (20)* | |
| **ВСЕГО:** | *180* | |

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

| Номер п/п | Наименование раздела | Используемые образовательные технологии |
|---|---|---|
| 1 | 2 | 5 |
| 1 | **Раздел 1 Концептуальные основы информационной безопасности и защиты информации** | Индивидуальная работа студента с лекциями и учебной литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). Дискуссия: «Что такое защита информации и для чего ее необходимо изучать?». |
| 2 | **Раздел 2 Защита информации от несанкционированного доступа и разграничение доступа к информации** | Индивидуальная работа студента с первоисточниками и литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). Тестирование студентов по разделу дисциплины |
| 3 | **Раздел 3 Организация и документационное обеспечение защиты информации** | Индивидуальная работа студента с первоисточниками и литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). |
| 4 | **Раздел 4 Правовое обеспечение защиты информации** | Индивидуальная работа студента с первоисточниками и литературой. Традиционная технология (слайд-презентация, демонстрация фрагментов документальных фильмов). Тестирование студентов по разделу дисциплины Дискуссия: «Основные виды документов по защите информации». |

# 6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## 6.1. Контроль освоения дисциплины

Контроль освоения дисциплины производится в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации студентов ФГБОУ ВО «Краснодарский государственный институт культуры». Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля.

*Текущий контроль* успеваемости студентов по дисциплине производится в следующих формах:

- *устный опрос*
- *письменные индивидуальные задания*

*Рубежный контроль* предусматривает оценку знаний, умений и навыков студентов по пройденному материалу по данной дисциплине на основе текущих оценок, полученных ими на занятиях за все виды работ. В ходе рубежного контроля используются следующие методы оценки знаний:

*устные ответы,*
*письменные работы,*
*практические и лабораторные работы,*
*оценка выполнения самостоятельной работы студентов:*
*рефективнаяработа,*

*Промежуточный контроль* по результатам семестра по дисциплине проходит в форме экзамена.

## 6.2. Оценочные средства

### 6.2.1. Примеры тестовых заданий (ситуаций)

### Вопросы для контроля знаний студентов (тесты)

Тестовые задания:

1. Под вычислительными сетями (ВС) подразумевается:
   A. Множество связанных ЭВМ
   B. Передача многоадресных сообщений
   C. Концентрация больших объемов данных
   D. Абонентская система

ANSWER: A

2. Прообразом вычислительных систем (ВС) являлись:

A. Коммуникационные подсети

B. Базы данных
C. Системы телеобработки данных (СТД)
D. Первые локальные подсети
ANSWER: C

3. В каких годах XX века появились первые микроЭВМ:
A. В 60х
B. В 70х
C. В 80х
D. В 90х
ANSWER: C

4. На чем построены сети с селекцией информации
A. Моноканал
B. Мэйнфрейм
C. Клиентский модуль
D. Серверный модуль
ANSWER: A

5.Маршрутизация информации это:
A. Процесс передачи данных в базовых сетях
B. Процесс определения маршрута следования данных в сетях связи
C. Процесс планирования маршрута передачи данных в кластерных подсистемах
D. Сокращение объема информации при передаче
ANSWER: B

6. HTTP это:
A. Протокол передачи файлов
B. Протокол удаленного доступа
C. Протокол почтового соединения
D. Протокол передачи гипертекста
ANSWER: D

7. FTP это:
A. Протокол передачи гипертекста
B. Протокол удаленного доступа
C. Протокол передачи файлов
D. Протокол почтового соединения
ANSWER: B

8. Конечным устройством компьютерной телекоммуникационной сети является:
A. Сетевая карта ПК
B. LAN выход
C. Сетевой маршрутизатор
D. Модем

ANSWER: A

9. Основное требование к системам связи:
   A. Возможность использования нераспространенных протоколов
   B. Отсутствие факта прерывания связи
   C. Отсутствие ошибочных пакетов данных
   D. Завершение соединения при ухудшении сигнала
   ANSWER: B

10. Под телекоммуникационной системой понимается:
   A. Аналогово-цифровой преобразователь сигналов
   B. Комплекс аппаратно-программного обеспечения
   C. Адаптер приёма сигналов
   D. Комплекс сетевых преобразователей
   ANSWER: B

11. Среднее расстояние между ретрансляторами телекоммуникационных систем:
   A. 10-40км
   B. 40-80км
   C. 80-120км
   D. 120-160км
   ANSWER: B

12. Основной недостаток системы телеобработки данных
   A. Большой размер оборудования
   B. Потеря качества сигнала
   C. Ненадежность телекоммуникационного оборудования
   D. невысокое быстродействие
   ANSWER: D

13. Что обеспечивает система сотовой связи:
   A. Неограниченный рост качества передачи
   B. Передачу речи и других видов информации
   C. Локальное управление сетями
   D. Передачу данных свыше 5 гб/сек
   ANSWER: B

14. Какой вид телевизионного вещания экономически выгоден для небольших территорий:
   A. Аналоговое
   B. Кабельное
   C. Спутниковое
   D. Цифровое
   ANSWER: C

15. Что обозначают понятием DataTerminalEquipment (DTE).

A. Оборудование оконечного устройства сети
B. Оборудование ввода данных
C. Программное обеспечение
D. Базы данных
ANSWER: A

16. Трансивер – это
A. Оптоволоконный кабель
B. Сетевой приемопередатчик
C. Шина данных
D. Модуль памяти
ANSWER: B

17. Какие линии цифровой связи поддерживают самую высококачественную связь:
A. Медные
B. Спутниковые
C. Оптоволоконные
D. Мобильные
ANSWER: C

18. Терминал абонента это:
A. Учетная запись
B. Персональная ЭВМ
C. Сетевое облако
D. Личный кабинет
ANSWER: B

19. Какую форму в ЭВМ имеет информация:
A. Дискретная двоичная
B. Дискретная четверичная
C. 32бит
D. 64бит
ANSWER: A

20. Важнейшая характеристика модема:
A. Стоимость
B. Скорость
C. Размер
D. Архитектура
ANSWER: B

21. Организация программного обеспечения, принятая в современных сетях, носит название:
A. Технология «клиент-терминал»
B. Технология «спутник-ЭВМ»
C. Технология «сквозного шифрования»

D. Технология «клиент – сервер»
ANSWER: D

22. Программы «клиент» и «сервер» используют:
A. Двоичное шифрование
B. Кластерные подсети
C. Общие протоколы
D. Маршрутную идентификацию
ANSWER: C

23. Какому этапу развития информационных технологий характерна механизация:
A. Начало XIX века
B. Конец XIX века
C. Начало XX века
D. Середина XX века
ANSWER: B

24. Каким годам характерно начало «компьютерной» технологии:
A. 60-е
B. 70-е
C. 80-е
D. 90-е
ANSWER: C

25. Стимул использования it:
A. Конкуренция
B. Дешевизна
C. Доступность
D. Узкая направленность
ANSWER: A

26. С чем связан отрицательный эффект ведения бизнеса компании под определенную it-систему:
A. С необходимостью сокращений
B. С необходимостью ведения нормативной документации
C. С необходимостью приватизации бизнеса
D. С необходимостью перестройки всего бизнеса
ANSWER: D

27. Создание it-системы:
A. Легкий во внедрении процесс
B. Дорогой и слишком медленный процесс
C. Доступный по цене всем компаниям процесс
D. Не требующий никаких изменений процесс

ANSWER: B

28.Разработка и внедрение it-системы для определенной компании в среднем занимает около:

A. Двух лет
B. Десяти лет
C. Трех месяцев
D. Семи дней

ANSWER: A

29. Высвобожденные за счет аутсорсинга it-ресурсы направляются на решение задач поддержки:

A. Службы безопасности
B. Сектора технического сопровождения
C. Основного бизнеса
D. Службы мониторинга

ANSWER: C

30. Организационные задачи по управлению взаимоотношениями с клиентами решают такие it-системы как:

A. KDL-системы
B. CRM-системы
C. ESK-системы
D. WAP2-системы

ANSWER: B

## Разбалловка

| № Задания | Количество баллов за проявленный ответ |
|---|---|
| 1 | 4 |
| 2 | 4 |
| 3 | 4 |
| 4 | 4 |
| 5 | 4 |
| 6 | 4 |
| 7 | 4 |
| 8 | 4 |
| 9 | 4 |
| 10 | 4 |
| 11 | 4 |
| 12 | 4 |
| 13 | 4 |
| 14 | 4 |
| 15 | 4 |
| 16 | 4 |
| 17 | 4 |

| | |
|---|---|
| 18 | 4 |
| 19 | 4 |
| 20 | 4 |
| 21 | 2 |
| 22 | 2 |
| 23 | 2 |
| 24 | 2 |
| 25 | 2 |
| 26 | 2 |
| 27 | 2 |
| 28 | 2 |
| 29 | 2 |
| 30 | 2 |

Контролируемые компетенции ПК-4

Критерии оценки:

- «отлично» выставляется обучающемуся, если набрано 97-100 баллов

- «хорошо» выставляется обучающемуся, если набрано 92-96 баллов

- «удовлетворительно» выставляется обучающемуся, если набрано 84-91 баллов

Если набрано 83 тестовых баллов и менее, то тест не сдан.

1. Цель защиты информации:
а) предотвращение утечки, хищения, утраты, искажения, подделки информации;
б) предотвращения угроз безопасности личности, общества, государства;
в) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
г) защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
д) сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
е) защита прав и свобод в условиях новой политической системы;
ж) предотвращение создания новых технологий в сфере защиты информации.
2.В отношении чего устанавливается режим защиты информации:
а) в отношении сведений, отнесенных к государственной тайне;
б) в отношении библиографических сведений;
в) в отношении конфиденциальной документационной информации;
г) в отношении информации по безопасности жизнедеятельности;
д) в отношении персональных данных федеральным законом.

3.Объекты авторского права:

а) литературные произведения;

б) музыкальные произведения с текстом и без него;

в) произведения архитектуры, градостроительства и садово-паркового искусства;

г) информационные ресурсы;

д) государственные символы и знаки;

е) произведения народного творчества.

4.В каком документе закреплен правовой статус информации:

а) закон РФ «О библиотечном деле»;

б) закон РФ «Об авторском праве»;

г) закон РФ «Об информации, информатизации и защите информации».

5.Срок действия авторского права:

а) в течение всей жизни автора и 25 лет после его жизни;

б) в течение всей жизни автора и 50 лет после его жизни;

в) в течение всей жизни автора и 100 лет после его жизни.

6.Субьекты смежных прав:

а) исполнители;

б) авторы;

в) производители фонограмм;

г) организации эфирного или кабельного вещания.

7. Объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ):

а) информационная система;

б) база данных;

в) информационные ресурсы.

8. Факсимильное воспроизведение в любых размерах и форме одного или более экземпляров оригиналов или копий письменных и других графических произведений путем фотокопирования или с помощью других технических средств, иных, чем издания:

а) репродуцирование;

б) тиражирование;

в) дублирование.

9. Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах):

а) информационные процессы;

б) информационные процессы;

в) информация.

10. Показывать, исполнять, передавать в эфир или совершать иное действие (за исключением распространения экземпляров произведения или фонограммы), посредством которого произведения, фонограммы, исполнения, постановки, передачи организации эфирного или кабельного вещания

становится доступным для слухового и (или) зрительного восприятия, независимо от их фактического восприятия публикой:

а) публичный показ;

б) сообщать;

в) сообщения для всеобщего сведения.

11.Когда был опубликован и начал действовать закон РФ «Об информации, информатизации и защите информации»?

а)1989г.

б)1997г.

в)1993г.

г)1995г.

Определите понятие:

12. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления:

а) документ;

б) информация;

в) информационные ресурсы.

13. Любая исключительно звуковая запись исполнений или иных звуков:

а) запись;

б) произведения;

в) фонограмма.

14. Выпуск в обращение экземпляров произведения, произведение фонограммы в количестве, достаточном для удовлетворения разумных потребностей публики исходя из характера произведения, фонограммы:

а) воспроизведение произведения;

б) опубликование;

в) обнародования произведения.

15. Организационно-упорядоченная совокупность документов (массив документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы:

а) информатизация;

б) информационная система;

в) база данных.

16. Субъект в полном объеме реализующей полномочия владения, пользования, распоряжения указанными объектами:

а) собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения;

б) владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения;

в) пользователь информацией.

17. Демонстрация оригинала или экземпляра произведения непосредственно или на экране с помощью пленки, диапозитива, телевизионного кадра или иных технических средств, а также демонстрация

отдельных кадров аудиовизуального произведения без соблюдения их последовательности:

а) передача в эфир;

б) показ произведения;

в) репродуцирование.

18. Физическое или юридическое лицо, взявшее на себя инициативу и ответственность за изготовление такого произведения; при отсутствии доказательств иного изготовителя аудиовизуального произведения признается физическое или юридическое лицо, имя или наименование которого обозначено на этом произведении обычным путем:

а) изготовитель фонограммы;

б) изготовитель аудиовизуального произведения;

в) изготовитель декоративно – прикладного искусства.

19. Зафиксированная на материальном носителе информация с реквизитами, позволяющая ее идентифицировать:

а) информация;

б) документ;

в) база данных.

20. Представление произведений, фонограмм, исполнений, постановок посредством игры, декламация, пение, танца в живом исполнении или с помощью технических средств; показ кадров аудиовизуального произведения

в их последовательности (с сопровождением или без сопровождения звуком):

а) передача в эфир;

б) исполнение;

в) публичный показ.

21. Осуществленное с согласия автора действие, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, передачи в эфир или иным способом:

а) показ произведения;

б) обнародования произведения;

в) исполнение.

22. Субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом:

а) владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения;

б) собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения;

в) автор.

23. Копия произведения, изготовленная в любой материальной форме:

а) экземпляр произведения;

б) экземпляр фонограммы.

### 6.2.2. Контрольные вопросы для проведения текущего контроля

1.Информация как объект правового регулирования.

2.Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др.

3.Основы правового режима информационных ресурсов. Информационные ресурсы как элемент состава имущества и объект права собственности.

4.Государственные информационные ресурсы. Пользование информационными ресурсами.

5.Информационные ресурсы в условиях рыночных отношений.

6. Защита информации и ее цели.

7. Характеристика основных методов и средств защиты информации.

8. Права и обязанности субъектов в области защиты информации.

9. Защита прав субъектов в сфере информационных процессов и информатизации.

10. Защита прав на доступ к информации.

11.Понятие интеллектуальной собственности и система ее правовой охраны.

12.Основные институты права интеллектуальной собственности.

13.Система Российского законодательства об интеллектуальной собственности.

14.История развития Российского законодательства об охране интеллектуальной собственности.

15. Объекты авторского права.

16. Субъекты авторского права.

17. Права авторов произведений науки, литературы и искусства.

18. Авторский договор.

19. Защита авторских прав.

### 6.2.3. Тематика эссе, рефератов, презентаций

1. Теоретические основы защиты информации
2. Информационные ресурсы как объект права
3. Защита информации в автоматизированных системах обработки данных
4. Конфиденциальное делопроизводство
5. Деятельность национальных институтов Российской Федерации в области информационной безопасности
6. Информационная безопасность человека и общества
7. Концептуальная модель информационной безопасности
8. Основные функции системы обеспечения информационной безопасности Российской Федерации и элементы ее организационной основы
9. Общие методы обеспечения информационной безопасности Российской Федерации

10. Источники угроз информационной безопасности Российской Федерации
11. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни
12. Методология обеспечения информационной безопасности деятельности общества
13. Эволюция подходов к обеспечению информационной безопасности
14. Области и объекты по обеспечению ИБ и защите информационной деятельности
15. Объекты защиты информационной деятельности и обеспечения ИБ
16. Стратегии обеспечения ИБ фирм
17. Организационно-правовое обеспечение ИБ
18. Отечественные и международные нормативно-правовые акты обеспечение ИБ
19. Аудит информационной безопасности
20. Организационно-технические аспекты защиты информации

### 6.2.4. Вопросы к зачету по дисциплине

1. Информация как объект правового регулирования.
2. Законы Российской Федерации «Об информации, информатизации и защите информации», «О библиотечном деле», «Об авторском праве и смежных правах» и др.
3. Основы правового режима информационных ресурсов.
4. Информационные ресурсы как элемент состава имущества и объект права собственности.
5. Государственные информационные ресурсы. Пользование информационными ресурсами.
6. Информационные ресурсы в условиях рыночных отношений.
7. Защита информации и ее цели.
8. Характеристика основных методов и средств защиты информации.
9. Права и обязанности субъектов в области защиты информации.
10. Защита прав субъектов в сфере информационных процессов и информатизации.
11. Защита прав на доступ к информации.
12. Понятие интеллектуальной собственности и система ее правовой охраны.
13. Основные институты права интеллектуальной собственности.
14. Система Российского законодательства об интеллектуальной собственности.

15. История развития Российского законодательства об охране интеллектуальной собственности.
16. Объекты авторского права.
17. Субъекты авторского права.
18. Права авторов произведений науки, литературы и искусства.
19. Авторский договор.
20. Защита авторских прав.

**6.2.5. Вопросы к экзамену по дисциплине**

1. Доступ к информации (несанкционированный доступ).
2. Персональные данные – определение.
3. Понятие информация, ее ценность для владельца.
4. Политика безопасности - определение.
5. Конфиденциальная информация, государственная и коммерческая тайна.
6. Каналы утечки информации.
7. Три степени секретности информации.
8. Государственная тайна.
9. Три категории ценности коммерческой информации.
10. Защита информации от компьютерных вирусов.
11. Товарная ценность информации, пути ее получения.
12. Коммерческая тайна.
13. Основные методы определения объема информации.
14. Конфиденциальная информация.
15. Основные виды угроз ИБ РФ.
16. Правовые аспекты создания информации.
17. Четыре основных принципа обеспечения ИБ РФ.
18. Защита информации в компьютерных сетях.
19. Основные направления международного сотрудничества Российской Федерации в области ИБ.
20. Внутренние источники угроз ИБ РФ.
21. Правовые аспекты распространения информации.
22. Интеллектуальная собственность – объект правовой охраны.
23. Авторское право.
24. Основные функции системы обеспечения ИБ РФ.
25. Источники права на доступ к информации.
26. Технология защиты документной информации.
27. Комплексное обеспечение ИБ РФ.
28. Аудит информационной безопасности.
29. Информационные ресурсы как объект права.
30. Конфиденциальное делопроизводство.

31. Особенности обеспечения информационной безопасности РФ в различных сферах общественной жизни.
32. Специфические принципы защиты информации в компьютерных сетях.

### 6.2.6. Примерная тематика курсовых работ

Не предусмотрено

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 7.1. Основная литература


1. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974.
2. Рацеев, С. М. Математические методы защиты информации и их основы. Сборник задач / С. М. Рацеев. — Санкт-Петербург : Лань, 2023. — 140 с. — ISBN 978-5-507-45197-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292913.
3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009.
4. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с. — ISBN 978-5-8114-9563-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/200483.


### 7.2. Дополнительная литература


1. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206285
2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В.

Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744
3. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279
4. Петренко, В. И. Защита персональных данных в информационных системах. Практикум / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-507-45301-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/264242

### 7.3. Периодические издания

1. Информационная безопасность
2. Киберугрозы и безопасность

### 7.4. Интернет-ресурсы

http://otherreferats.allbest.ru/marketing/00068136_0.html учебники http://mirknig.com/ - теоретические и практические пособия

### 7.5. Методические указания и материалы по видам занятий

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 разделен на логически завершенные части темы, после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Форма текущего контроля знаний – работа студента на практическом занятии. Форма промежуточных аттестаций – письменная (домашняя) работа. Итоговая форма контроля знаний по дисциплине – контрольная работа с задачами по всему материалу курса.

**Рекомендации по организации самостоятельной работы студентов**

В учебном процессе выделяют два вида самостоятельной работы:

- аудиторная;
- внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Видами заданий для внеаудиторной самостоятельной работы являются:

-для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и Интернета и др.

- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста, повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей, составление плана, составление таблиц для систематизации учебною материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др), подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.

-для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, опытно экспериментальная работа, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Виды внеаудиторной СРС: подготовка и написание рефератов, эссе, создание презентаций и других письменных работ на заданные темы, выполнение домашних заданий разнообразного характера. Это - решение задач; перевод и пересказ текстов; подбор и изучение литературных источников; разработка и составление различных схем; выполнение графических работ; проведение расчетов и др.; выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы. Индивидуальное задание может получать как каждый студент,

так и часть студентов группы; подготовка к участию в научно-теоретических конференциях, смотрах, олимпиадах и др.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий, семинаров, выполнении лабораторного практикума и во время чтения лекций.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;
- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических и лабораторных занятиях;
- промежуточный контроль по окончании изучения раздела или модуля курса;
- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;
- итоговый контроль по дисциплине в виде зачета или экзамена;
- контроль остаточных знаний и умений спустя определенное время после завершения изучения дисциплины.

**Методические указания по выполнению рефератов и эссе**

Реферативная работа выполняется студентом самостоятельно под руководством преподавателя.

В реферате необходимо:

1)сформулировать актуальность и место решаемой задачи информационного обеспечения в предметной области;

2)проанализировать литературу и информацию, полученную с помощью глобальных систем в данной области или в смежных системных областях,

3)определить и конкретно описать выбранные бакалавром объемы, методы и средства решаемой задачи, проиллюстрировать данными и формами выходных документов, используемых при реализации поставленной задачи информационного обеспечения на модельном примере (но на реальной вычислительной технике, работающей в составе профессионально-ориентированной информационной системы);

4)проанализировать предлагаемые пути и способы.

К оформлению реферативной работы предъявляются следующие требования

1)Четкость и логическая последовательность изложения материала;

2)Убедительность аргументации;

3)Краткость и точность формулировок, исключающих возможностей неоднозначного толкования;

4)Конкретность изложения результатов работы;

5)Доказательность выводов и обоснованность рекомендаций.

Текст реферата печатается через 1,5 интервала на одной стороне стандартного листа бумаги формата А-4. Страницы работы должны иметь поля: левое - 30 мм, правое – 1,5 мм, нижнее -20 мм, верхнее - 20 мм.

Порядковый номер печатается в середине нижнего поля страницы. Первой страницей считается титульный лист, но на нем цифра "1" не ставится, на следующей странице проставляется цифра "2".

На титульном листе должны быть следующие сведения: фамилия и инициалы студента-бакалавра; тема реферативной работы; фамилия, инициалы, ученая степень и должность преподавателя.

*Семинар-исследование*. Во вступительном слове преподаватель закладывает общую ориентировочную основу исследовательской деятельности обучаемых на семинаре, совместно с ними определяет основные проблемы семинара, пути и методику их раскрытия и исследования. Основой организации проблемно-поискового семинара выступает метод постановки системы поисково-познавательных, исследовательского характера задач и упражнений, решение которых в ходе дискуссии раскрывает слушателям методику конкретного исследования, где каждая задача требует от обучаемого освоения в содержательном контексте строго определенных элементов исследовательской культуры. В зависимости от характера изучаемой темы, вынесенной на семинар, уровня подготовки группы выбираются задачи соответствующего уровня и последовательность их постановки: теоретико-аналитические, логико-методологические, контрольно-практические, прикладные. Отправной точкой постановки системы поисково-познавательных задач на семинаре, вовлечения слушателей в дискуссию-исследование, ее конкретизацию выступает доклад. В ходе доклада не только раскрывается проблема основные ее теоретические положения, но и ставятся перед аудиторией ряд конкретных задач творческого характера, создаются тем самым предпосылки для развертывания дискуссии вокруг практических аспектов проблемы. Для этого в основу доклада должны быть положены результаты исследований докладчика, что создает предпосылки для вывода семинарского занятия на исследовательский уровень, уровень решения практических задач. *Исследовательский подход* на семинаре предполагает использование познавательных задач в комплексе со всем набором познавательных средств, прежде всего, эмпирическими данными различной степени общности, схемами, вопросами, упражнениями и т.д. С их помощью слушателям представляется проблемное поле для коллективного решения общей задачи через ее составляющие.

*Семинар-взаимообучение*. Студенты готовятся по 4-6 вопросам семинарского занятия. Но каждый из них особенно тщательно изучает один из вопросов. К примеру, если их 12 человек, то можно распределить по 2 человека на один вопрос. На занятии обучаемые рассаживаются за столами попарно, в соответствии с изученными вопросами. По знаку преподавателя обучаемые в указанное время должны пересказать друг другу содержание, обсудить спорные моменты, прийти к общему мнению. Затем один из рядов смещается на одно место. 1-й обучаемый объясняет 4-му содержание первого вопроса, уточненное и расширенное в беседе со 2-м обучаемым. 4-й объясняет 1-му содержание 2-го вопроса и т.д. За полный круг все слушатели могут обменяться мнениями по всем вопросам. Преподаватель дает короткие

консультации тем, кто обращается к нему. Достоинство этого приема – в повышении вербальной активности обучаемых и в неоднократном обсуждении одной и той же проблемы. Это способствует углублению знаний, их закреплению и выяснению новых аспектов, а также выработке единого подхода. В заключительной части на общее обсуждение могут быть вынесены спорные вопросы. Окончательное заключение дает преподаватель. Данный метод требует четкой организации занятия.

**Методические указания для подготовки к семинарским занятиям**

Семинарские занятия проводятся в форме дискуссии, на которых проходит обсуждение конкретных экономических ситуаций. Обсуждения направлены на освоение научных основ, эффективных методов и приемов решения конкретных практических задач, на развитие способностей к творческому использованию получаемых знаний и навыков.

Основная цель проведения семинара заключается в закреплении знаний полученных в ходе прослушивания лекционного материала.

Семинар проводится в форме устного опроса студентов по вопросам семинарских занятий, а также в виде решения практических задач или моделирования практической ситуации.

В ходе подготовки к семинару студенту следует просмотреть материалы лекции, а затем начать изучение учебной литературы. Следует знать, что освещение того или иного вопроса в литературе часто является личным мнением автора, построенного на анализе различных источников, поэтому следует не ограничиваться одним учебником или монографией, а рассмотреть как можно больше материала по интересуемой теме.

Обязательным условием подготовки к семинару является изучение нормативной базы. Для этого следует обратится к любой правовой системе сети Интернет. В данном вопросе не следует полагаться на книги, так как законодательство претерпевает постоянные изменения и в учебниках и учебных пособиях могут находится устаревшие данные.

В ходе самостоятельной работы студенту для необходимы отслеживать научные статьи в специализированных изданиях, а также изучать статистические материалы, соответствующей каждой теме.

Студенту рекомендуется следующая схема подготовки к семинарскому занятию:

1. Проработать конспект лекций;
2. Прочитать основную и дополнительную литературу, рекомендованную по изучаемому разделу;
3. Ответить на вопросы плана семинарского занятия;
4. Выполнить домашнее задание;
5. Проработать тестовые задания и задачи;
6. При затруднениях сформулировать вопросы к преподавателю.

При подготовке к семинарским занятиям следует руководствоваться указаниями и рекомендациями преподавателя, использовать основную литературу из представленного им списка. Для наиболее глубокого

освоения дисциплины рекомендуется изучать литературу, обозначенную как «дополнительная» в представленном списке.

При подготовке доклада на семинарское занятие желательно заранее обсудить с преподавателем перечень используемой литературы, за день до семинарского занятия предупредить о необходимых для предоставления материала технических средствах, напечатанный текст доклада предоставить преподавателю.

**Содержание и методика выполнения практических и семинарских работ:**

- работа выполняется на ПЭВМ со стандартным программным обеспечением: Windows/Linux, а также с использованием специальных программ.

### 7.6. Программное обеспечение

Преподавание дисциплин обеспечивается следующими программными продуктами: операционные системы – Windows\Linux; пакет прикладных программ электронного офиса; справочно-правовые системы Консультант +, Гарант, МАРК-SQL, ИРБИС.

## 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Здания и сооружения института соответствуют противопожарным правилам и нормам.

Материально-техническая база КГИК обеспечивает проведение всех видов учебной, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Оборудованы учебные аудитории для проведения занятий лекционного и семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, в том числе служащими для представления учебной информации большой аудитории (на 180 и 450 мест).

Для проведения занятий лекционного типа имеется демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации к рабочим учебным программам дисциплин (модулей).

Функционирует лаборатория информационных технологий в социокультурной сфере.

Выделены помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с подключением к сети "Интернет" и электронной информационно-образовательной среде института.

**Дополнения и изменения**

**к рабочей программе учебной дисциплины (модуля)**

**_____**

на 20__-20__ уч. год

В рабочую программу учебной дисциплины вносятся следующие изменения:

- _____;
- _____;
- _____.
- _____;
- _____;
- _____.

Дополнения и изменения к рабочей программе рассмотрены и рекомендованы на заседании кафедры _____
_____
(наименование)
Протокол №____ от «___» _____ 20___г.

Исполнитель(и):
_____/_____/_____/_____
(должность) (подпись) (Ф.И.О.) (дата)
_____/_____/_____/_____
(должность) (подпись) (Ф.И.О.) (дата)

Заведующий кафедрой
_____/_____/_____/_____
(наименование кафедры) (подпись) (Ф.И.О.) (дата)