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 информационно-библиотечной деятельности и документоведения
_____О.М. Уржумова
«20» мая 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.02.01 Информационная безопасность и защита информации

Направление подготовки 51.03.06 «Библиотечно-информационная деятельность»
Профиль подготовки «Информационные и документные ресурсы в цифровой среде»
Квалификация (степень) выпускника – бакалавр
Форма обучения – очная, заочная
Год начала подготовки – 2026

Краснодар
2026

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:

Директор МУК «Централизованная библиотечная система» г. Краснодара — Н.Г. Гребещенко

Кандидат культурологии, заведующий кафедрой социально-культурной деятельности ФГБОУ ВО «Краснодарский государственный институт культуры» — Л.Н. Кондратьева

Составитель:

Багдасарян Р.Х., к.т.н., доцент

Рабочая программа учебной дисциплины «Информационная безопасность и защита информации» рассмотрена и утверждена на заседании кафедры ИБДиД от «20» мая 2026 г. протокол № 11.

Рабочая программа учебной дисциплины «Информационная безопасность и защита информации» Учебно-методическим советом ФГБОУ ВО «КГИК» «29» мая 2026 г. протокол № 10.

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-проектно деятельности в библиотечно-информационной сфере, внедрению цифровых техноло организацию и использование электр информационных систем (ПК-4)	основные методы защиты нормативн о-правовые основы обеспечения информацио нной безопасности	работать с основными методами защиты информации в библиотеке организовыва безопасную информационну	методами защиты в библиотеке

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Структура дисциплины

Очная форма обучения

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 часов).

№	Раздел	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в	Формы текущего контроля успеваемости *(по неделям семестра)* Форма

	дисциплины		часах)				промежуточной аттестации *(по семестрам)*
			Л	ПЗ	ИЗ	СР	
1	Раздел I. Концептуальные основы информационной безопасности и защиты информации	4	8	8		9	
2	Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации	4	8	8		9	
3	Раздел III. Организация и документационное обеспечение защиты информации	4	8	8		9	
4	Раздел 4. Правовое обеспечение защиты информации	4	8	8		8	
	итого		32	32			экзамен
							108

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.**	**Форми-руемые компе-тенции (по теме)**
1	**2**	**3**	**4**
Раздел I. Концептуальные основы информационной безопасности и защиты информации			
Тема 1.1. Введение в информационную безопасность и защиты информации	Лекции: Понятия правового регулирования и информационных документов. Понятия информационной безопасности, защиты информации, конфиденциальности, целостности, доступности.	*2*	ПК-4

	Угрозы информационной безопасности: классификация и примеры. Актуальные тенденции в области информационной безопасности		
	<u>Практические занятия (семинары):</u> Анализ угроз информационной безопасности в библиотечно-информационной сфере.	*2*	
	<u>Самостоятельная работа</u> Реферат по теме: Лицензирование деятельности и сертификация продуктов и услуг в области защиты информации. Аттестация объектов информатики.	*2*	
Тема 1.2. Угрозы информационной безопасности и противодействие угрозам	<u>Лекции:</u> Понятие угрозы информационной безопасности. Источники угроз, классификация угроз по цели реализации, способу и объекту воздействия. Угрозы информационной безопасности России. Дестабилизирующие факторы: типы, источники, классификация. Органы добывания информации и основные сферы их интересов. Техническая и агентурная разработка. Легальные и нелегальные способы добывания информации. Инженерная защита и техническая охрана объектов. .	*2*	ПК-4
	<u>Практические занятия (семинары)</u> Оценка рисков информационной безопасности. Практическое применение методов оценки рисков для библиотечных информационных ресурсов. Разработка матрицы рисков. Определение приоритетов в управлении рискам	*2*	
	<u>Самостоятельная работа</u> Разработать схему устранения информационных угроз	*2*	
Тема 1.3. Каналы утечки информации	<u>Лекции:</u> Понятие утечки информации, канала утечки технического канала утечки. Особенности утечки информации по сравнению с утечкой материальных объектов. Структура канала передачи	*2*	ПК-4

	информации. Отличия канала утечки от функционального канала; понятие опасного сигнала. Виды источников сигнала, функции передатчика и приемника сигнала, параметры среды распространения. Классификация кадров утечки по физической природе носителя, информативности, структуре, времени появления и действия. Сравнительная характеристика каналов утечки. Комплексное использование каналов утечки. Оптический канал утечки информации. Особенности и структура оптического канала утечки. Среда распространения, основные виды приемников сигнала. Способы маскировки и энергетического скрытия объекта защиты. Акустический канал утечки информации. Структура, источники сигналов, среда распространения акустического канала утечки. Характеристики акустических волн как носителей информации, условия их затухания и поглощения. Способы и средства подслушивания. Классификация закладных устройств. 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. Обнаружение закладных устройств, определение их принадлежности и подавление. Демаскирующие признаки микрофонных, некамуфлированных и камуфлированных радиозакладок. Основные виды контроля отсутствия закладных устройств. Радиоэлектронный канал утечки информации. Особенности, структура, среда распространения радиоэлектронного канала утечки, основные виды радиоэлектронных каналов.. Виды искусственных помех по эффекту воздействия, соотношению спектра помех и полезных сигналов, времени изучения. Перехват сигналов. Способы подавления опасных сигналов. Экранирование		

	источников поля.		
	Практические занятия (семинары) Семинар: - Материально-вещественный канал утечки информации. - Источники и носители информации. -Структура канала. - Способы предотвращения утечки информации. - Защита информации в отходах деятельности организации. - Защита демаскирующих веществ.	*2*	
	Самостоятельная работа 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.	*2*	
Тема 1.4. Криптографическая защита информации	Лекции: Понятия категории, криптографии, криптоанализа. Главные задачи криптографии и ее отличия от кодирования и стеганографии (тайнописи). Виды криптографических атак. Обобщенная схема криптографической системы и основные варианты ее реализации. Симметричная и ассиметричная криптосистемы. Понятия криптографической защиты, криптографического преобразования, шифра, ключа, имитовставки. Принципы рассеивания и перемещения как основа современных симметричных криптосистем. Составные шифры, перестановки и подстановки. Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики. 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. Основные режимы шифрования. Архивное шифрование, шифрование при работе в криптографической сети,	*2*	ПК-4

	обработка файлов в интерактивном и пакетном режимах, "прозрачный" режим шифрования. 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. Работа в криптографической сети при возможности связи каждого узла сети с любым другим. Организация криптографической сети по схеме "звезда". Действия администратора сети и оператора узла при обмене ключевой информацией. Сравнительный анализ двух схем построения криптографической сети. Общие рекомендации по работе с ключевой информацией.		
	Практические занятия (семинары) Семинар: - Принципы рассеивания и перемещения как основа современных симметричных криптосистем. - Составные шифры, перестановки и подстановки.	*2*	
	Самостоятельная работа Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики.	*3*	
Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации			
Тема 2.1. Защита информации от компьютерных вирусов и других программ с потенциально опасными последствиями	Лекции: Понятие программы с потенциально опасными последствиями, основные функции и виды этих программ. Понятие компьютерного вируса, основные свойства вирусов. Классификация вирусов по среде обитания, алгоритму действия, деструктивным возможностям. Двухфакторная аутентификация. Биометрическая аутентификация. Модели авторизации и управления доступом.	*4*	ПК-4
	Практические занятия (семинары) Семинар: - Программные закладки, их классификация по месту внедрения и применения, основные функции.	*4*	

	- Организационно-технические меры защиты от вирусов и закладок.		
	Самостоятельная работа Тест по теме	*4*	
Тема 2.2. Защита информации в компьютерных сетях	Лекции: 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) Аудит систем доступа к информации. Рекомендации по совершенствованию системы разграничения доступа	*4*	
	Самостоятельная работа Реферат по теме	*5*	
Раздел III. Организация и документационное обеспечение защиты информации			
Тема: 3.1. Организационные меры защиты информации	Лекции: Основные виды документов по защите информации: федеральные законы, локальные нормативные акты. Регламентирование процессов обработки информации. Физическая безопасность информационных систем.	*4*	ПК-4
	Практические занятия (семинары) Семинар№1 Правовые аспекты создания и распространения информации. 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.	*4*	
	Самостоятельная работа Реферат по теме	*4*	

Тема: 3.2. Система защиты информации	Лекции: Основные способы построения системы защиты информации Порядок резервного копирования и восстановления данных. Разработка планов действий в случае инцидентов информационной безопасности	*4*	ПК-4
	Практические занятия (семинары) Семинар№2. Информационные ресурсы: классификация и характеристика их информационных свойств. 1. Разработка инструкций по безопасной работе с информационными системами для сотрудников библиотеки. 2. Государственные информационные ресурсы. Пользование информационными ресурсами. 3. Разработка плана восстановления данных после сбоев и аварий..	*4*	
	Самостоятельная работа «Стратегия развития информационного общества в Российской Федерации»	*5*	
Раздел IV. Правовое обеспечение защиты информации			
Тема: 4.1. Основные правовые документы защиты информации	Лекции: Основные правовые документы, касающиеся защиты информации Конституционные принципы защиты информации. Федеральный закон "Об информации, информационных технологиях и о защите информации" (ФЗ-152) Законодательство о персональных данных (ФЗ-152, приказы Роскомнадзора).	*4*	ПК-4
	Практические занятия (семинары) Семинар№3, №4 Защита информации и прав субъектов в области информационных процессов и информатизации 1. Защита информации и ее цели. 2. Характеристика основных методов и средств защиты информации. 3. Права и обязанности субъектов в области защиты информации. 4. Разработка договора о конфиденциальности информации.	*4*	
	Самостоятельная работа Закон «О персональных данных»	*4*	
Тема: 4.2. Управление	Лекции: Основные процессы управления защитой	*4*	ПК-4

процессом защиты информации	информации		
	Практические занятия (семинары) Семинар№5,6 Интеллектуальная собственность, как объект правовой охраны. 1.Понятие интеллектуальной собственности и система ее правовой охраны. 2.Основные институты права интеллектуальной собственности. 3.Система Российского законодательства об интеллектуальной собственности. 4.История развития Российского законодательства об охране интеллектуальной собственности.	*4*	
	Самостоятельная работа Итоговый тест по дисциплине	*4*	
Примерная тематика курсовой работы *(если предусмотрено)*			
Самостоятельная работа обучающихся над курсовой работой *(если предусмотрено)*			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)		*экзамен*	
ВСЕГО:		*108*	

Заочная форма обучения

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 часов).

№ п/п	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	4	1	2		21	
2	Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации	4	1	2		21	

3	Раздел III. Организация и документационное обеспечение защиты информации	4	2	1		21	
4	Раздел 4. Правовое обеспечение защиты информации	4	2	1		21	Экзамен
			6	6		84	
	итого					108	

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

Заочная форма обучения

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.**	**Форми-руемые компе-тенции (по теме)**
1	**2**	**3**	**4**
Раздел I. Концептуальные основы информационной безопасности и защиты информации			
Тема 1.1. Введение в информационную безопасность и защиты информации	Лекции: Понятия правового регулирования и информационных документов. Понятия информационной безопасности, защиты информации, конфиденциальности, целостности, доступности. Угрозы информационной безопасности: классификация и примеры. Актуальные тенденции в области информационной безопасности	*0,25*	ПК-4
	Практические занятия (семинары): Анализ угроз информационной безопасности в библиотечно-информационной сфере.	*0,5*	
	Самостоятельная работа Реферат по теме: Лицензирование деятельности и сертификация продуктов и услуг в области защиты информации. Аттестация объектов информатики.	*5*	
Тема 1.2. Угрозы информационной безопасности и противодействие	Лекции: Понятие угрозы информационной безопасности. Источники угроз, классификация угроз по цели реализации, способу и объекту воздействия.	*0,25*	ПК-4

угрозам	Угрозы информационной безопасности России. Дестабилизирующие факторы: типы, источники, классификация. Органы добывания информации и основные сферы их интересов. Техническая и агентурная разработка. Легальные и нелегальные способы добывания информации. Инженерная защита и техническая охрана объектов. .		
	<u>Практические занятия (семинары)</u> Оценка рисков информационной безопасности. Практическое применение методов оценки рисков для библиотечных информационных ресурсов. Разработка матрицы рисков. Определение приоритетов в управлении рискам	*0,5*	
	<u>Самостоятельная работа</u> Разработать схему устранения информационных угроз	*5*	
Тема 1.3. Каналы утечки информации	<u>Лекции:</u> Понятие утечки информации, канала утечки технического канала утечки. Особенности утечки информации по сравнению с утечкой материальных объектов. Структура канала передачи информации. Отличия канала утечки от функционального канала; понятие опасного сигнала. Виды источников сигнала, функции передатчика и приемника сигнала, параметры среды распространения. Классификация кадров утечки по физической природе носителя, информативности, структуре, времени появления и действия. Сравнительная характеристика каналов утечки. Комплексное использование каналов утечки. Оптический канал утечки информации. Особенности и структура оптического канала утечки. Среда распространения, основные виды приемников сигнала. Способы маскировки и энергетического скрытия объекта защиты. Акустический канал утечки информации. Структура, источники	*0,25*	ПК-4

	сигналов, среда распространения акустического канала утечки. Характеристики акустических волн как носителей информации, условия их затухания и поглощения. Способы и средства подслушивания. Классификация закладных устройств. 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. Обнаружение закладных устройств, определение их принадлежности и подавление. Демаскирующие признаки микрофонных, некамуфлированных и камуфлированных радиозакладок. Основные виды контроля отсутствия закладных устройств. Радиоэлектронный канал утечки информации. Особенности, структура, среда распространения радиоэлектронного канала утечки, основные виды радиоэлектронных каналов.. 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> Семинар: - Материально-вещественный канал утечки информации. - Источники и носители информации. -Структура канала. - Способы предотвращения утечки информации. - Защита информации в отходах деятельности организации. - Защита демаскирующих веществ.	*0,5*	
	<u>Самостоятельная работа</u> 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	Лекции: Понятия категории, криптографии, криптоанализа. Главные задачи криптографии и ее отличия от кодирования и стеганографии (тайнописи). Виды криптографических атак. Обобщенная схема криптографической системы и основные варианты ее реализации. Симметричная и ассиметричная криптосистемы. Принципы рассеивания и перемещения как основа современных симметричных криптосистем. Критерии отнесения средств защиты информации к криптографическим. Сравнительная характеристика аппаратных и программных криптографических средств. Основные режимы шифрования. Архивное шифрование, шифрование при работе в криптографической сети, обработка файлов в интерактивном и пакетном режимах, "прозрачный" режим шифрования. Система ключевой информации. Понятия узла замены, главного, условленного, файлового ключей, ключа пользователя, пароля. Работа в криптографической сети при возможности связи каждого узла сети с любым другим. Организация криптографической сети по схеме "звезда". Действия администратора сети и оператора узла при обмене ключевой информацией. Сравнительный анализ двух схем построения криптографической сети. Общие рекомендации по работе с ключевой информацией.	*0,25*	ПК-4
	Практические занятия (семинары) Семинар: - Принципы рассеивания и перемещения как основа современных симметричных криптосистем. - Составные шифры, перестановки и подстановки.	*0,5*	
	Самостоятельная работа Отечественный алгоритм шифрования ГОСТ 28147-89 и его основные характеристики.	*5*	
Раздел II. Защита информации от несанкционированного доступа и разграничение доступа к информации			

Тема 2.1. Защита информации от компьютерных вирусов и других программ с потенциально опасными последствиями	Лекции: Понятие программы с потенциально опасными последствиями, основные функции и виды этих программ. Понятие компьютерного вируса, основные свойства вирусов. Классификация вирусов по среде обитания, алгоритму действия, деструктивным возможностям. Двухфакторная аутентификация. Биометрическая аутентификация. Модели авторизации и управления доступом.	*0,5*	ПК-4
	Практические занятия (семинары) Семинар: - Программные закладки, их классификация по месту внедрения и применения, основные функции. - Организационно-технические меры защиты от вирусов и закладок.	*1*	
	Самостоятельная работа Тест по теме	*10*	
Тема 2.2. Защита информации в компьютерных сетях	Лекции: 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.	*0,5*	ПК-4
	Практические занятия (семинары) Аудит систем доступа к информации. Рекомендации по совершенствованию системы разграничения доступа	*1*	
	Самостоятельная работа Реферат по теме	*11*	
Раздел III. Организация и документационное обеспечение защиты информации			
Тема: 3.1. Организационные меры защиты информации	Лекции: Основные виды документов по защите информации: федеральные законы, локальные нормативные акты. Регламентирование процессов обработки	*1*	ПК-4

	информации. Физическая безопасность информационных систем.		
	Практические занятия (семинары) Семинар№1 Правовые аспекты создания и распространения информации. 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.	*0,5*	
	Самостоятельная работа Реферат по теме	*11*	
Тема: 3.2. Система защиты информации	Лекции: Основные способы построения системы защиты информации Порядок резервного копирования и восстановления данных. Разработка планов действий в случае инцидентов информационной безопасности	*1*	ПК-4
	Практические занятия (семинары) Семинар№2. Информационные ресурсы: классификация и характеристика их информационных свойств. 1. Разработка инструкций по безопасной работе с информационными системами для сотрудников библиотеки. 2. Государственные информационные ресурсы. Пользование информационными ресурсами. 3. Разработка плана восстановления данных после сбоев и аварий..	*0,5*	
	Самостоятельная работа «Стратегия развития информационного общества в Российской Федерации»	*10*	
Раздел IV. Правовое обеспечение защиты информации			
Тема: 4.1. Основные правовые документы защиты информации	Лекции: Основные правовые документы, касающиеся защиты информации Конституционные принципы защиты информации. Федеральный закон "Об информации, информационных технологиях и о защите информации" (ФЗ-152) Законодательство о персональных данных (ФЗ-152, приказы Роскомнадзора).	*1*	ПК-4
	Практические занятия (семинары)	*0,5*	

	Семинар№3, №4 Защита информации и прав субъектов в области информационных процессов и информатизации 1. Защита информации и ее цели. 2. Характеристика основных методов и средств защиты информации. 3. Права и обязанности субъектов в области защиты информации. 4. Разработка договора о конфиденциальности информации.		
	Самостоятельная работа Закон «О персональных данных»	*8*	
Тема: **4.2**. Управление процессом защиты информации	Лекции: Основные процессы управления защитой информации	*1*	ПК-4
	Практические занятия (семинары) Семинар№5,6 Интеллектуальная собственность, как объект правовой охраны. 1.Понятие интеллектуальной собственности и система ее правовой охраны. 2.Основные институты права интеллектуальной собственности. 3.Система Российского законодательства об интеллектуальной собственности. 4.История развития Российского законодательства об охране интеллектуальной собственности.	*0,5*	
	Самостоятельная работа Итоговый тест по дисциплине	*13*	
Примерная тематика курсовой работы *(если предусмотрено)*			
Самостоятельная работа обучающихся над курсовой работой *(если предусмотрено)*			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)		*экзамен*	
ВСЕГО:		*108*	

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. Фонд оценочных средств

6.2.1. Примеры тестовых заданий (ситуаций)
Вопросы для контроля знаний студентов (тесты)

Тестовые задания:

1. Что является основным объектом защиты информации?
   a) Аппаратное обеспечение
   b) Программное обеспечение
   c) Сама информация
   d) Сетевое оборудование
   Ответ: c
2. Какое понятие охватывает меры, направленные на предотвращение разглашения информации?
   a) Целостность
   b) Доступность
   c) Конфиденциальность
   d) Аутентичность
   Ответ: c
3. Что такое угроза информационной безопасности?
   a) Слабое место в системе защиты
   b) Потенциальная возможность нанесения ущерба
   c) Процесс предотвращения несанкционированных действий
   d) Меры по восстановлению системы после атаки
   Ответ: b
4. Какая модель информационной безопасности предполагает разделение доступа на уровни "достоверности" и "чувствительности"?
   a) Модель Мак-Дональда
   b) Модель Белла-ЛаПадулы
   c) Модель Грэма-Деннинга
   d) Модель Брюса Снайдера
   Ответ: b
5. Какова формула для расчета риска?
   a) Risk=Impact×VulnerabilityRisk = Impact \times VulnerabilityRisk=Impact×Vulnerability
   b) Risk=Probability+ImpactRisk = Probability + ImpactRisk=Probability+Impact
   c) Risk=Probability×ImpactRisk = Probability \times ImpactRisk=Probability×Impact
   d) Risk=Vulnerability/ImpactRisk = Vulnerability / ImpactRisk=Vulnerability/Impact
   Ответ: c
6. Какой федеральный закон в РФ регулирует вопросы защиты информации?
   a) ФЗ-98
   b) ФЗ-152
   c) ФЗ-126
   d) ФЗ-230
   Ответ: b

7. Что такое персональные данные?
   a) Информация, не относящаяся к конкретному лицу.
   b) Информация, относящаяся к идентифицированному или идентифицируемому физическому лицу.
   c) Информация, доступная всем.
   d) Информация о финансовом состоянии компании.
   Ответ: b
8. Что такое аутентификация?
   a) Процесс предоставления прав доступа к информации
   b) Процесс сверки учетных данных пользователя
   c) Процесс шифрования данных
   d) Процесс резервного копирования данных
   Ответ: b
9. Какой метод аутентификации использует комбинацию логина, пароля и одноразового кода?
   a) Однофакторная аутентификация
   b) Двухфакторная аутентификация
   c) Биометрическая аутентификация
   d) Парольная аутентификация
   Ответ: b
10. Что такое межсетевой экран (firewall)?
    a) Программа для антивирусной защиты
    b) Устройство для защиты сети от несанкционированного доступа
    c) Программа для шифрования данных
    d) Программа для резервного копирования данных
    Ответ: b
11. В чем основная функция системы обнаружения вторжений (IDS)?
    a) Блокировка подозрительной активности
    b) Обнаружение и оповещение о подозрительной активности
    c) Шифрование данных
    d) Резервное копирование данных
    Ответ: b
12. Что такое симметричное шифрование?
    a) Использование разных ключей для шифрования и расшифрования
    b) Использование одного и того же ключа для шифрования и расшифрования
    c) Шифрование данных без использования ключей
    d) Шифрование только текстовой информации
    Ответ: b
13. Какой принцип подразумевает предоставление пользователю только тех прав доступа, которые необходимы для выполнения его обязанностей?
    a) Принцип необходимости знания
    b) Принцип минимальных привилегий
    c) Принцип конфиденциальности
    d) Принцип целостности
    Ответ: b
14. Что такое ACL (список контроля доступа)?
    a) Список доступных программного обеспечения.
    b) Список пользователей и их прав доступа к ресурсам.
    c) Список резервных копий данных.
    d) Список возможных угроз безопасности.
    Ответ: b
15. Что такое политика информационной безопасности?

a) Набор технических средств защиты информации
b) Документ, определяющий цели, принципы и методы защиты информации
c) Список пользователей с правами доступа
d) Набор инструкций по использованию программного обеспечения
Ответ: b

16. Какие организационные меры НЕ относятся к защите информации?
a) Обучение персонала
b) Физическая охрана
c) Установка антивируса
d) Разработка регламентов
Ответ: c

17. Какой тип резервного копирования создает полную копию данных каждый раз?
a) Инкрементное
b) Дифференциальное
c) Полное
d) Частичное
Ответ: c

18. Что такое план восстановления данных после сбоев?
a) Документ, определяющий процедуры резервного копирования.
b) Документ, описывающий шаги по восстановлению работоспособности системы после инцидента.
c) Документ, содержащий список программного обеспечения.
d) Документ, определяющий политику информационной безопасности.
Ответ: b

19. С какой целью необходимо проводить обучение персонала по вопросам информационной безопасности?
a) Для демонстрации преимуществ используемых технологий.
b) Для повышения осведомленности о рисках и методах защиты информации.
c) Для выполнения требований законодательства.
d) Для повышения производительности труда.
Ответ: b

20. Что регулируется Федеральным законом "О персональных данных"?
a) Защиту авторских прав
b) Обработку и защиту персональных данных
c) Защиту коммерческой тайны
d) Защиту объектов интеллектуальной собственности
Ответ: b

21. Какая статья УК РФ предусматривает ответственность за неправомерный доступ к информации?
a) 270
b) 272
c) 273
d) 282
Ответ: b

22. Что такое коммерческая тайна?
a) Публично доступная информация.
b) Информация, составляющая конкурентное преимущество и защищенная законом.
c) Информация, не имеющая ценности.
d) Любая информация, известная сотрудникам компании.
Ответ: b

23. Какая ответственность может наступить за нарушение правил защиты персональных данных?

a) Только уголовная
b) Только административная
c) Гражданско-правовая, административная и уголовная
d) Только дисциплинарная
Ответ: c

24. Что такое социальная инженерия?
a) Метод шифрования данных.
b) Метод использования человеческих факторов для получения доступа к информации.
c) Метод защиты от вредоносных программ.
d) Метод резервного копирования данных.
Ответ: b

25. Что является примером фишинга?
a) Отправка спама.
b) Создание поддельного веб-сайта для кражи учетных данных.
c) Взлом пароля.
d) Заражение компьютера вирусом.
Ответ: b

26. Что такое вредоносное программное обеспечение (malware)?
a) Программа для оптимизации работы компьютера.
b) Программа, предназначенная для нанесения вреда компьютерным системам.
c) Программа для резервного копирования данных.
d) Программа для создания резервных копий данных.
Ответ: b

27. Какова функция антивирусного программного обеспечения?
a) Шифрование данных
b) Обнаружение и удаление вредоносного программного обеспечения
c) Резервное копирование данных
d) Ускорение работы компьютера
Ответ: b

28. Что такое VPN?
a) Виртуальная память
b) Виртуальная частная сеть, обеспечивающая безопасное соединение через общедоступную сеть
c) Видеокарта
d) Вирусная программа
Ответ: b

29. О чем следует помнить при создании пароля?
a) Использовать легко запоминающиеся слова.
b) Использовать только цифры.
c) Использовать комбинацию прописных и строчных букв, цифр и символов.
d) Использовать только прописные буквы.
Ответ: c

30. Что такое DDoS-атака?
a) Атака на пароль пользователя.
b) Атака, направленная на перегрузку сервера запросами с целью вывода его из строя.
c) Атака, направленная на кражу личных данных.
d) Атака, направленная на распространение вирусов.
Ответ: b

31. Зачем нужно обновлять программное обеспечение?
a) Только для добавления новых функций.
b) Только для исправления ошибок.

c) Для исправления уязвимостей и повышения безопасности системы.
d) Обновление не требуется.
Ответ: c

32. Какое отношение имеет понятие "цифровая подпись" к информационной безопасности?
a) Она не имеет отношения к информационной безопасности.
b) Она используется для шифрования данных.
c) Она позволяет удостовериться в подлинности и целостности электронного документа.
d) Она используется для создания резервных копий данных.
Ответ: c

33. Что такое "нулевой день" (zero-day) уязвимость?
a) Уязвимость, которая известна производителю программного обеспечения.
b) Уязвимость, которая еще не известна производителю программного обеспечения. c) Уязвимость, которая легко устраняется.
d) Уязвимость, которая не представляет опасности.
Ответ: b

34. Что такое SIEM-система?
a) Система для управления базами данных.
b) Система сбора и анализа информации о безопасности для выявления инцидентов. c) Система для резервного копирования данных.
d) Система удаленного администрирования.
Ответ: b

35. Какие данные необходимо шифровать в первую очередь?
a) Текстовые документы.
b) Конфиденциальные данные, например, персональные данные и финансовую информацию.
c) Изображения. d) Музыкальные файлы. **Ответ: b**

36. Что такое "умный дом" с точки зрения информационной безопасности?
a) Совершенно безопасная и защищенная система.
b) Система, требующая особого внимания к вопросам безопасности из-за множества подключенных устройств.
c) Система, не требующая никакой защиты.
d) Система, полностью управляемая искусственным интеллектом.
Ответ: b

37. Что такое "радужные таблицы"?
a) Таблицы с расписанием работы сотрудников.
b) Предварительно вычисленные таблицы, используемые для взлома паролей.
c) Таблицы для управления базами данных.
d) Таблицы для резервного копирования данных
. **Ответ: b**

38. Каковы основные цели резервного копирования?
a) Увеличение скорости работы компьютера.
b) Защита от потери данных в случае сбоев, аварий или атак.
c) Автоматическое обновление программного обеспечения.
d) Оптимизация использования дискового пространства.
Ответ: b

39. Что такое инцидент информационной безопасности?
a) Плановое обслуживание системы.
b) Любое нарушение правил информационной безопасности или угроза безопасности.
c) Установка нового программного обеспечения.
d) Замена аппаратного обеспечения.

Ответ: b

40. Что такое "временная метка" в контексте информационной безопасности?
    a) Время, когда был создан аккаунт пользователя.
    b) Время, когда произошло событие, например, вход в систему или изменение файла.
    c) Время, когда была установлена операционная система.
    d) Время, когда был создан резервный экземпляр данных.
    Ответ: b
41. Какие меры следует предпринять при обнаружении вируса на компьютере?
    a) Продолжать работу, как обычно.
    b) Запустить антивирусную программу и удалить вирус.
    c) Переустановить операционную систему.
    d) Выключить компьютер и оставить его выключенным.
    Ответ: b
42. Что такое брандмауэр на уровне приложений (WAF)?
    a) Межсетевой экран, работающий на уровне сети.
    b) Межсетевой экран, защищающий веб-приложения от атак.
    c) Антивирусная программа.
    d) Система обнаружения вторжений.
    Ответ: b
43. Что такое endpoint security?
    a) Защита только серверов.
    b) Защита всех конечных устройств, таких как компьютеры, ноутбуки и мобильные устройства.
    c) Защита только сетевого оборудования.
    d) Защита только веб-сайтов.
    Ответ: b
44. Какие факторы следует учитывать при выборе антивирусного программного обеспечения?
    a) Только цену.
    b) Эффективность обнаружения вирусов, производительность и наличие дополнительных функций.
    c) Только наличие красивого интерфейса.
    d) Только количество лицензий.
    Ответ: b
45. Что такое GDPR (General Data Protection Regulation)?
    a) Закон США о защите информации.
    b) Закон Европейского Союза о защите персональных данных.
    c) Стандарт ISO для обеспечения информационной безопасности.
    d) Рекомендации по созданию паролей.
    Ответ: b

Разбалловка

№ Задания	Количество баллов за проявленный ответ	№ Задания	Количество баллов за проявленный ответ
1	1	23	2
2	1	24	2
3	1	25	2
4	1	26	2
5	1	27	2

6	1	28	2
7	1	29	2
8	1	30	2
9	1	31	2
10	1	32	2
11	1	33	2
12	1	34	2
13	1	35	2
14	1	36	2
15	1	37	2
16	1	38	2
17	1	39	2
18	1	40	2
19	1	41	2
20	1	42	2
21	2	43	2
22	2	44	2
		45	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 70 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.Субъекты 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. Предметная область и ее роль в проектировании информационных систем.

10. Основные отличия предметно-ориентированных и предметно-независимых информационных систем.

11. Жизненный цикл разработки предметно-ориентированных информационных систем.

12. Компоненты архитектуры предметно-ориентированной информационной системы.

13. Методологии разработки предметно-ориентированных информационных систем: обзор и сравнение.

14. Автоматизированные библиотечные системы (АБС) как примеры ПОИС: функциональные возможности и перспективы развития.

15. Системы управления электронными ресурсами (ERM): особенности предметной области и ключевые функции.

16. Системы управления цифровыми библиотеками (DSpace, Greenstone): архитектура и принципы работы.

17. Применение онтологий для организации и представления знаний в библиотечных информационных системах.

18. Системы анализа и визуализации данных для библиотек: ключевые возможности и примеры использования.

19. Реляционные базы данных и их применение в библиотечных информационных системах (СУБД: MySQL, PostgreSQL).

20. NoSQL базы данных и их потенциал для хранения и обработки больших объемов библиотечных данных.

21. Использование метаданных в предметно-ориентированных информационных системах для библиотек: стандарты и форматы (MARC, Dublin Core, MODS).

22. Разработка пользовательских интерфейсов для предметно-ориентированных информационных систем библиотек: принципы usability и accessibility.

23. API и интеграция предметно-ориентированных библиотечных систем с другими информационными ресурсами.

24. Искусственный интеллект и машинное обучение в библиотечных информационных системах: применение для каталогизации, поиска и рекомендаций.

25. Семантический веб и его возможности для обогащения библиотечных данных и улучшения поиска.

26. Облачные технологии в библиотечной сфере: преимущества и риски применения предметно-ориентированных информационных систем в облаке.

27. Блокчейн-технологии для защиты авторских прав и управления интеллектуальной собственностью в библиотечных системах.

28. Разработка мобильных приложений для доступа к библиотечным ресурсам как примеры предметно-ориентированных информационных систем.

29. Анализ функциональности и архитектуры автоматизированной библиотечной системы ИРБИС64.
30. Обзор систем управления электронными ресурсами (ERM): Ex Libris Primo, ProQuest Rialto.
31. Сравнение систем управления цифровыми библиотеками: DSpace, Greenstone, Fedora.
32. Анализ возможностей системы Koha для автоматизации библиотечных процессов.
33. Обзор потенциала системы Folio как современной открытой платформы для библиотек.
34. Проблема интеграции различных библиотечных информационных систем.
35. Проблема обеспечения интероперабельности библиотечных данных.
36. Проблема сохранения цифрового наследия и долгосрочного доступа к электронным ресурсам.
37. Проблема обеспечения безопасности библиотечных информационных систем от киберугроз.
38. Перспективы развития предметно-ориентированных информационных систем для библиотек в условиях цифровой трансформации.

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. Что такое предметно-ориентированная информационная система (ПОИС)? Чем она отличается от предметно-независимой?

13. Какова роль предметной области в проектировании и разработке ПОИС?
14. Опишите основные этапы жизненного цикла разработки ПОИС.
15. Какие основные компоненты включает в себя архитектура ПОИС?
16. Перечислите известные методологии разработки ПОИС. В чем их отличия?
17. Что такое онтология и как она может быть использована в ПОИС?
18. В чем заключаются принципы модульности и масштабируемости при проектировании ПОИС?
19. Какие типы информационных систем используются в библиотечной деятельности?
20. Каковы основные функциональные возможности Автоматизированных библиотечных систем (АБС)?
21. Чем отличаются системы управления электронными ресурсами (ERM) от АБС? Какие задачи они решают?
22. Какие системы управления цифровыми библиотеками вы знаете? Опишите их ключевые особенности.
23. Какова роль метаданных в библиотечных ПОИС? Какие стандарты метаданных используются наиболее часто?
24. Какие задачи в библиотечной деятельности могут быть решены с помощью систем анализа и визуализации данных?
25. Какие преимущества предоставляет использование API для интеграции библиотечных систем?
26. Опишите принципы работы реляционных баз данных. Как они применяются в библиотечных системах?
27. В чем преимущества и недостатки использования NoSQL баз данных для библиотечных систем? В каких случаях целесообразно их применение?
28. Какие существуют типы API? Для чего они нужны в контексте ПОИС?
29. Расскажите о принципах проектирования удобных (usable) и доступных (accessible) пользовательских интерфейсов для библиотечных систем.
30. Что такое облачные технологии? Какие преимущества и риски связаны с их использованием в библиотеках?
31. Какие методы шифрования данных используются для обеспечения безопасности информации в библиотечных системах?
32. Как искусственный интеллект и машинное обучение могут быть использованы в библиотечных информационных системах? Приведите примеры.
33. Что такое Семантический веб? Как он может расширить возможности поиска и доступа к информации в библиотеках?
34. Какие преимущества и риски связаны с использованием блокчейн-технологий в библиотечной сфере?

35. Каковы перспективы развития мобильных приложений для доступа к библиотечным ресурсам?

36. Какие основные проблемы существуют при интеграции различных библиотечных информационных систем?

37. Что такое интероперабельность данных? Почему она важна для библиотечных систем?

38. Какие меры необходимо предпринимать для обеспечения безопасности библиотечных информационных систем от киберугроз?

39. Каковы основные тенденции развития библиотечных информационных систем в условиях цифровой трансформации?

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.
5. Искусственный интеллект, аналитика и новые технологии : перевод с английского. – Москва : Альпина Паблишер, 2022. – 200 с. : ил. – (HarvardBusinessReview: 10 лучших статей). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=707465 (дата обращения: 14.02.2024). – Текст : электронный.
6. Косаренко, Николай Николаевич. Искусственный интеллект: теория, философия, история, право : монография / Н. Н. Косаренко ; Рос. эконом. ун-т им. Г. В. Плеханова. – Москва : Русайнс, 2022. – 313, [1] с. – ISBN 978-5-466-02029-8. – Текст (визуальный) : непосредственный.
7. Куприянов, Дмитрий Васильевич. Информационное и технологическое обеспечение профессиональной деятельности : учебник и практикум для вузов : для студентов, обучающихся по естественнонаучным

направлениям / Д. В. Куприянов. – Москва : Юрайт, 2021. – 254, [1] с. : ил. – (Высшее образование). – Текст (визуальный) : непосредственный.

8. Меркулова, Альмира Шевкетовна. Автоматизированные библиотечно-информационные системы : учебное пособие для студентов вузов, обучающихся по гуманитарным направлениям / А. Ш. Меркулова. – 2-е изд. – Москва : Юрайт ; Кемерово : КемГИК, 2023. – 129 с. : табл., рис. – (Высшее образование). – Текст (визуальный) : непосредственный.

9. Ниматулаев, Магомедхан Магомедович. Информационные технологии в профессиональной деятельности : учебник для студентов вузов / М. М. Ниматулаев. – Москва : ИНФРА-М, 2023. – 248, [1] с. : рис., табл. – (Высшее образование - специалитет). – Текст (визуальный) : непосредственный.

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

5. Оганисян, Элеонора Жоровна. Сборник контрольно-оценочных заданий по дисциплине "Введение в информационные технологии" для текущего контроля знаний студентов-бакалавров : [учебно-методическое пособие] / Э. Ж. Оганисян ; М-во культуры Рос. Федерации, Краснод. гос. ин-т культуры, Информ.-библ. фак., Каф. библ.-библиогр. деятельности и информ. технологий. – Краснодар : КГИК, 2022. – 90 с. : ил. – Текст (визуальный) : непосредственный.

6. Рахматуллаев, Марат Алимович. Проектирование информационно-библиотечных систем : учебник / М. А. Рахматуллаев. – Москва : ИНФРА-М,

2023. – 286 с. : табл. – (Высшее образование). – Текст (визуальный) : непосредственный.

7. Сбитнева, Галина Ивановна. Отраслевые информационные ресурсы : практикум / Г. И. Сбитнева. – 2-е изд. – Москва : Юрайт, 2022. – 154 с. – (Высшее образование). – Текст (визуальный) : непосредственный.

8. Соколов, Аркадий Васильевич. Науки об информации для библиотекарей : монография / А. В. Соколов. – Москва : Юрайт, 2021. – 189, [1] с. – (Актуальные монографии). – Текст (визуальный) : непосредственный.

9. Станкевич, Лев Александрович. Интеллектуальные системы и технологии : учебник и практикум для студентов вузов, обучающихся по инженерно-техническим направлениям / Л. А. Станкевич. – Москва : Юрайт, 2021. – 394, [2] с. – (Высшее образование). – Текст (визуальный) : непосредственный.

10. Удаленные образовательные ресурсы и их роль в профессиональной подготовке специалистов сферы культуры и искусства : коллективная монография / Н. Б. Зиновьева, А. С. Матвеева, А. В. Мельникова, Е. В. Рюмшина ; М-во культуры Рос. Федерации, Краснод. гос. ин-т культуры, Инф.-библ. фак., Каф. документоведения и проект. деятельности ; под общ. ред. Н. Б. Зиновьевой. – Краснодар : КГИК, 2021. – 170 с. : ил., табл. – Текст (визуальный) : непосредственный.

11.

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
https://culture.gov.ru Министерство культуры РФ
http://www.library.ru Информационно-справочный портал Library.ru
http://www.bibliograf.ru Электронный журнал «Библиотечное дело»
http://www.gpntb.ru Государственная публичная научно-техническая библиотека России
http://www.rsl.ru Сайт РГБ
https://www.prlib.ru Президентская библиотека
https://nlr.ru Российская национальная библиотека
https://rusneb.ru Национальная электронная библиотека

http://www.rba.ru/activities/conference/conf-2024/index Всероссийский библиотечный конгресс
http://old.libsmr.ru/lib2/upload/museum/Обновление_ЭКНД/Стратегия_развития_библиотечного_дела_до_2030.pdf
http://government.ru/docs/50395/ Стратегическое направление в области цифровой трансформации отрасли культуры Российской Федерации до 2030 года
https://bibliovaravva.ru ГБУК КК «Краснодарская краевая юношеская библиотека имени И.Ф. Вараввы»
https://pushkin.kubannet.ru/#gsc.tab=0 ГБУК КК «Краснодарская краевая универсальная научная библиотека им. А.С. Пушкина»
https://skbr21.ru/# сводный каталог библиотек России
https://kgik1966.ru Сайт КГИК
http://193.106.214.30/MarcWeb2/Default.asp Электронный каталог библиотеки КГИК
https://biblioclub.ru/index.php?page=ko Электронно-библиотечная система «Университетская библиотека онлайн»
http://нэб.рф Национальная электронная библиотека (НЭБ) (доступ в рамках читального зала библиотеки КГИК).
https://eivis.ru/ Электронная подписка на периодические издания ИВИС**.**
https://rd.springer.com/ Платформа Springer Link
https://www.nature.com/ Платформа Nature

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

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.

Заведующий кафедрой

_____/_____/_____/_____

(наименование кафедры) (подпись) (Ф.И.О.) (дата)