МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ХАБАРОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ»
(ХГИК)
Кафедра библиотечно-информационной деятельности,
документоведения и архивоведения

УТВЕРЖДАЮ
Проректор по учебной, научной
и международной деятельности

_____Е.В. Савелова

«24» мая 2022 г.

ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Уровень бакалавриата
(2022 год набора, заочная форма обучения)

направление подготовки
51.03.06 Библиотечно-информационная деятельность

профиль подготовки
«Менеджмент библиотечно-информационной деятельности»

Хабаровск
2022

Составитель:

Киселев Валерий Иванович, доцент кафедры библиотечно-информационной деятельности, документоведения и архивоведения.

Рабочая программа дисциплины «Информационная безопасность и защита информации» рассмотрена и одобрена на заседании кафедры библиотечно-информационной деятельности, документоведения и архивоведения «18» мая 2022 г., протокол № 9.

СОДЕРЖАНИЕ

1. Общие сведения о дисциплине……	4
1.1. Наименование дисциплины……..……..	4
1.2. Место дисциплины в структуре образовательной программы..	4
1.3. Цель освоения дисциплины……..……	4
1.4. Планируемые результаты обучения по дисциплине……..	5
2. Объём и содержание дисциплины…..…….	7
2.1. Объём дисциплины…….....	7
2.2. Тематический план……..……	8
2.3. Краткое содержание разделов и тем.……	9
3. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине……...	11
3.1. Планы семинарских занятий..……	11
3.2. Темы докладов и рефератов по дисциплине..……..	13
3.3. Вопросы для самоконтроля по разделам дисциплины.……...	13
4. Методические указания по освоению дисциплины……..….	14
5. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине…….	16
5.1. Перечень компетенций и этапы их формирования.…….	16
5.2. Показатели и критерии оценивания компетенций……..…….	17
5.3. Материалы для оценки и контроля результатов обучения…….	18
5.4. Методические материалы по оцениванию результатов обучения	19
6. Ресурсное обеспечение…….	25
6.1. Основная и дополнительная учебная литература……	25
6.2. Ресурсы информационно-телекоммуникационной сети Интернет	27
6.3. Информационные технологии, программное обеспечение, информационные справочные системы……..	28
6.4. Материально-техническая база…….	29
7. Воспитательная работа	29
7. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья	29

1. ОБЩИЕ СВЕДЕНИЯ О ДИСЦИПЛИНЕ

1.1. Наименование дисциплины

Рабочая программа дисциплины «Защита информации и информационная безопасность» предназначена для специалистов, обучающихся по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность», профиль подготовки «Менеджмент библиотечно-информационной деятельности», квалификации (степени) «бакалавр», в том числе для инклюзивного образования инвалидов и лиц с ограниченными возможностями здоровья. Программа разработана в соответствии с федеральным государственным образовательным стандартом высшего образования, утв. приказом Министерства образования и науки РФ от 06.12.2017 г. № 1182.

1.2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации и информационная безопасность» является дисциплиной части учебного плана, формируемой участниками образовательных отношений (Б1.В.03).

Особенность изучаемой дисциплины состоит в органической связи и взаимодействии со знаниями и умениями, полученными студентами в рамках следующих дисциплин ООП: «Информационные технологии в профессиональной деятельности», «Информационные технологии в управлении делопроизводством учреждений культуры».

Освоение данной дисциплины необходимо для последующего изучения таких дисциплин как «Информационно-коммуникационные технологии в библиотечном деле», «Менеджмент библиотечно-информационной деятельности».

1.3. Цель освоения дисциплины

Цель дисциплины «Защита информации и информационная безопасность», как одной из специальных дисциплин, заключается в формировании специалиста-профессионала в области создания, внедрения, анализа и сопровождения современных информационных систем, сетей и коммуникаций, уверенно ориентирующегося в вопросах защиты информации.

Задачами дисциплины являются:

- овладение понятийным аппаратом, описывающим различные аспекты сферы информационной безопасности, усвоение основных характери-

стик возможных угроз информации, методов и средств защиты информации от этих угроз,

– освоение практических методов защиты информации на основе типовых программных средств, приобретение навыков безопасной работы в среде локальных и глобальных вычислительных сетей.

– В результате изучения курса «Защита информации и информационная безопасность» студенты должны овладеть знаниями, умениями и навыками по способам защиты информации и информационной безопасности, принципам обеспечения условий безопасности и жизнедеятельности при разработке и эксплуатации информационных систем.

1.4. Планируемые результаты обучения по дисциплине

Код	Формулировка компетенции	Индикаторы достижения компетенции	Планируемые результаты практической деятельности, обеспечивающие формирование компетенций
УК-2	Способность определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	**УК-2.1. Знать:** - основы теории и состав профессиональных задач в будущей профессиональной деятельности; - нормативную базу и правовые нормы, регулирующие библиотечно-информационную деятельность; - знать состав имеющихся ресурсов и ограничения в их использовании; - источники профессиональной информации, средства и методы её получения.	**УК-2.1. Знать:** студент знает эффективные приемы: - постановки задач и выбора оптимальных способов их решения; - поиска и применения необходимой правовой и профессиональной информации.
		УК-2.2. Уметь: - формулировать цели и определять круг задач, решение которых необходимо для достижения этой цели; - выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; - использовать современные информационно-коммуникационные технологии для поиска и получения необходимой информации.	**УК-2.2. Уметь:** студент умеет: - формулировать цели и определять круг задач, решение которых необходимо для достижения этой цели; - выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; - использовать современные информационно-коммуникационные технологии для поиска и получения необходимой информации.
		УК-2.3. Владеть: - методами выбора опти-	**УК-2.3. Владеть:** студент уверенно владеет навыками:

		мальных способов решения задач; - методами поиска необходимой информации с использованием современных информационно-коммуникационных технологий.	- выбора оптимальных способов решения задач; - поиска необходимой информации с использованием современных информационно-коммуникаци-онных технологий.
УК-8	Способность создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций.	**УК-8.1. Знать:** - основные требования для поддержания безопасных условий жизнедеятельности; - требования правил техники безопасности; - основные способы оказания первой помощи в чрезвычайных ситуациях.	**УК-8.1. Знать:** студент знает эффективные приемы: - поддержания безопасных условий жизнедеятельности; - выполнения правил техники безопасности; - оказания первой помощи в чрезвычайных ситуациях.
		УК-8.2. Уметь: - организовывать и контролировать безопасные условия жизнедеятельности на рабочем месте; - оказывать первую помощь в чрезвычайных ситуациях.	**УК-8.2. Уметь:** студент умеет: - организовывать и контролировать безопасные условия жизнедеятельности на рабочем месте; - оказывать первую помощь в чрезвычайных ситуациях
		УК-8.3. Владеть: - основными методами организации и контроля безопасных условий жизнедеятельности; - правилами и приёмами оказания первой медицинской (и иной) помощи при чрезвычайных ситуациях.	**УК-8.3. Владеть:** студент уверенно владеет навыками: - организации и контроля безопасных условий жизнедеятельности; - оказания первой медицинской (и иной) помощи при чрезвычайных ситуациях.
ПК-8	Способность формировать и поддерживать рациональную систему документационного обеспечения	**ПК-8.1. Знать:** - основные нормативные документы, регулирующие систему документационного обеспечения; - приёмы и методы организации документооборота и делопроизводства.	**ПК-8.1. Знать:** студент знае эффективные приемы: - приёмы и методы организации документооборота и делопроизводства; - основные нормативные документы, регулирующие систему документационного обеспечения.
		ПК-8.2. Уметь: - выполнять правила организации документооборота; - организовывать делопроизводство в своей организации.	**ПК-8.2. Уметь:** студент умеет: - выполнять правила организации документооборота; - организовывать делопроизводство в своей организации.
		ПК-8.3. Владеть: - основными приёмами и методами организации документооборота и делопроиз-	**ПК-8.3. Владеть:** студент уверенно владеет навыками: - организации документооборота и делопроизводства.

		водства.	

2. ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины (заочная форма обучения)

Вид учебной работы	ОФО		ЗФО	
	Всего часов	Семестры	Всего часов	Курс
Аудиторные занятия (всего)			**22**	2
В том числе:				
- лекции (ЛЗ)			8	2
- семинары (СЗ)			4	2
- практические (ПЗ)			8	2
- мелкогрупповые (МГЗ)				
- индивидуальные (ИЗ)				
- групповое консультирование (Г)			2	2
- индивидуальное консультирование (И)				
Самостоятельная работа студента (всего)			**86**	2
СРС			82	
КОНТРОЛЬ			4	
В том числе:				
Подготовка курсовой работы				
Текущий контроль			4	
Промежуточный контроль				
Общая трудоемкость: (всего зач. ед./кол-во часов по ФГОС)			**3/108**	2
Вид промежуточной аттестации (зачет, экзамен)	семестры:		курс:	
зачет			2	
экзамен				

2.2. Тематический план

Тематический план (заочная форма обучения)

№ п/п	Наименование разделов и тем (формируемые компетенции)	Кол-во часов									
		Всего часов по ФГОС	Контактная работа					Самостоятельная работа студентов			
			Всего ауд. часов	ЛЗ	СЗ	ПЗ	Консультации	Всего часов СРС	СРС	контроль СРС	
										текущий	промежуточный
Раздел 1. Информационная безопасность человека и общества											
1.1	Информационные ресурсы. Информационная безопасность человека и общества (УК-8, ПК-8)	**9**	**1**	**1**				**8**	**8**		
1.2	Угрозы информационной безопасности (УК-8, ПК-8)	**11**	**3**	**1**	**1**	**1**		**8**	**8**		
Итого по разделу		**20**	**4**	**2**	**1**	**1**		**16**	**16**		
Раздел 2. Средства и методы защиты информации											
2.1	Основные направления обеспечения информационной безопасности (УК-2, УК-8, ПК-8)	**11**	**1**	**1**				**10**	**10**		
2.2	Правовая защита информации (УК-2, УК-8, ПК-8)	**10**	**2**	**1**		**1**		**8**	**8**		
2.3	Организационная защита информации (УК-2, ПК-8)	**9**	**1**			**1**		**8**	**8**		
2.4	Инженерно-техническая защита информации (УК-2, УК-8, ПК-8)	**10**	**2**		**1**	**1**		**8**	**8**		
Итого по разделу		**40**	**6**	**2**	**1**	**3**		**34**	**34**		
Раздел 3. Информационная безопасность в компьютерных системах											
3.1	Программные методы защиты информации (УК-2, ПК-8)	**13**	**3**	**1**	**1**	**1**		**10**	**10**		

3.2	Проблемы безопасности информации в компьютерных сетях и Интернет (УК-2, ПК-8)	**12**	**2**	**1**		**1**		**10**	**10**		
Итого по разделу		**25**	**5**	**2**	**1**	**2**		**20**	**20**		
Раздел 4. Криптография как метод защиты информации											
4.1	Основы криптографии (УК-2, ПК-8)	**9**	**3**	**1**	**1**	**1**		**6**	**6**		
4.2	Основные криптографические методы. Анализ криптографических систем (УК-2, ПК-8)	**10**	**4**	**1**		**1**	**2**	**6**	**6**		
Итого по разделу		**19**	**7**	**2**	**1**	**2**	**2**	**12**	**12**		
Подготовка к зачёту		**4**									**4**
Всего часов:		**108**	**24**	**8**	**4**	**8**	**2**	**84**	**82**		**4**

2.3. Краткое содержание разделов и тем

Раздел 1. Информационная безопасность человека и общества

Тема 1.1. Информационные ресурсы. Информационная безопасность человека и общества

Основные характеристики информационных ресурсов (государственных и негосударственных) в условиях информационного общества.

Определение цели и задачи защиты данных. Модель информационной безопасности (основные положения). Права и обязанности собственника, владельца и потребителя в области защиты информации.

Тема 1.2. Угрозы информационной безопасности

Определение угрозы. Классификации угроз информационной безопасности. Объекты защиты. Охраняемые сведения и демаскирующие признаки. Программы – шпионы. Троянские программы. Клавиатурные шпионы. Парольная защита ОС.

Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД.

Раздел 2. Средства и методы защиты информации

Тема 2.1. Основные направления обеспечения информационной безопасности.

Общие характеристики методов и средств защиты информации.

Основные направления обеспечения информационной безопасности.

Способы защиты информации. Основные положения. Характеристика защитных действий.

Тема 2.2. Правовая защита информации

Определение права. Международное и внутригосударственное право

Структура законодательства РФ. Государственная политика обеспечения информационной безопасности.

Тема 2.3. Организационная защита информации

Основные организационные мероприятия.

Организация защиты ПК и информационных систем. Применение средств защиты ПК и информационных систем. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу. Системы контроля доступа.

Тема 2.4. Инженерно- техническая защита информации

Основная классификация инженерно-технических средств защиты.

Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа. Запирающие устройства.

Аппаратные средства защиты. Средства обнаружения. Средства поиска и детальных измерений. Средства активного и пассивного противодействия. Аппаратные средства защиты ПК и информационных сетей.

Технические каналы утечки информации. Причины образования технических каналов утечки информации. Утечки информации по акустическим каналам. Утечка информации в волоконно-оптических линиях связи.

Раздел 3. Информационная безопасность в компьютерных сетях

Тема 3.1. Программные методы защиты информации

Программные средства защиты. Основные группы. Защита информации от НСД. Защита от копирования. Защита от разрушения.

Тема 3.2. Проблемы безопасности информации в компьютерных сетях и Интернет

Источники угроз в компьютерных сетях. НСД к сетям и сетевым ресурсам. Раскрытие и модификация данных и программ. Раскрытие, модификация и подмена трафика. Разработка и распространение компьютерных вирусов. Классификация антивирусных программ.

Раздел 4. Криптография как метод защиты информации

Тема 4.1. Основы криптографии

Криптографические методы защиты. Основные понятия криптографии и криптоанализа. Классификация криптографических методов.

Тема 4.2. Основные криптографические методы. Анализ криптографических систем.

Основные одноключевые криптографические методы. Блочные шрифты. Шифры сложной и простой перестановки. Шифры замены. Одноалфавитные шифры. Многоалфавитные шифры

Алгоритм шифрования DES. Алгоритм шифрования FEAL.

Шифры поточного шифрования: синхронные поточные шифры. Самосинхронизирующие поточные шифры. Комбинированные шифры.

Криптографические системы с открытым ключом. Ассиметрические криптографические методы. Принципы построения ассиметричных криптографических систем. Протоколы подтверждения подлинности информации. Протоколы распределения ключей. Основы анализа криптостойкости. Надежность криптографических систем.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

3.1. Планы практических и семинарских занятий

Семинарское занятие 1 (2 часа)

по теме: «Угрозы информационной безопасности. Инженерно-техническая защита информации».

Вопросы:

- определение и классификация угроз информационной безопасности;
- действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД;
- понятие инженерно-технических средств защиты и их классификация;
- физические средства защиты;
- аппаратные средства защиты;
- технические каналы утечки информации.

Семинарское занятие 2 (2 часа)

по теме: «Программные методы защиты информации. Основы криптографии».

Вопросы:

- программные средства защиты информации;
- защита информации от несанкционированного доступа, копирования, искажения и разрушения.
- криптографические методы защиты;
- основные понятия криптографии;
- классификация криптографических методов.

Практическое занятие 1 (2 часа)

по теме: «Угрозы информационной безопасности. Правовая защита информации».

Цель занятия – ознакомиться с основными угрозами информационной безопасности, изучить методы правовой защиты информации.

Задание:

Ознакомиться со следующими вопросами (и кратко законспектировать) –

- характеристики основных угроз информационной безопасности;
- способы реализации угроз информационной безопасности;
- основные правовые акты в сфере защиты информации;
- федеральный закон «Об информации, информационных технологиях и защите информации».

Практическое занятие 2 (2 часа)

по теме: «Организационная защита информации. Инженерно-техническая защита информации».

Цель занятия – изучить основные организационные и инженерно-технические методы защиты информации.

Задание:

Ознакомиться со следующими вопросами (и кратко законспектировать) –

- основные организационные мероприятия по защите информации;
- организация защиты ПК и информационных систем;
- назначение и задачи служб безопасности;
- классификация инженерно-технических средств защиты;
- физические и аппаратные средства защиты;
- технические каналы утечки информации.

Практическое занятие 3 (2 часа)

по теме: «Программные методы защиты информации. Проблемы безопасности информации в компьютерных сетях и Интернет».

Задание:

Ознакомиться со следующими вопросами (и кратко законспектировать) –

- характеристика программных методов защиты информации;
- пароли и их использование;
- мониторинг и аудит;
- особенности защиты информации в компьютерных сетях;
- технические средства защиты информации в компьютерных системах;
- программные средства защиты информации в компьютерных системах.

Практическое занятие 4 (2 часа)

по теме: «Основы криптографии. Основные криптографические методы. Анализ криптографических систем».

Цель занятия – ознакомление с основными понятиями криптографии.

Задание:

Ознакомиться со следующими вопросами (и кратко законспектировать) –

- криптографические методы защиты;
- основные понятия криптографии и криптоанализа;
- классификация криптографических методов;
- основные одноключевые криптографические методы;
- криптографические системы с открытым ключом.

3.2. Темы докладов и рефератов по дисциплине

Учебным планом для данной дисциплины доклады и рефераты не предусмотрены.

3.3. Вопросы для самоконтроля по разделам дисциплины

Вопросы к Разделу 1

1. Определение цели и задачи защиты данных. Модель информационной безопасности (основные положения). (УК-8, ПК- 8)
2. Права и обязанности собственника, владельца и потребителя в области защиты информации. (УК-8, ПК-8)
3. Основные характеристики информационных ресурсов (государственных и негосударственных) в условиях информационного общества. (УК-8, ПК-8)
4. Определение угрозы информационной безопасности. (УК-8, ПК-8)
5. Классификации угроз информационной безопасности. (УК-8, ПК-8)
6. Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД (несанкционированный доступ). (УК-8, ,ПК-8)

Вопросы к Разделу 2

1. Основные направления обеспечения информационной безопасности.
2. Законодательство РФ о защите информации. (УК-2, УК-8, ПК-8)
3. Основные организационные мероприятия информационной безопасности. (УК-2, УК-8, ПК-8)
4. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу. (УК-2, УК-8, ПК-8)
5. Способы защиты информации. Основные положения. (УК-2, УК-8, ПК-8)
6. Организация защиты ПК и информационных систем. (УК-2, УК-8, ПК-8)
7. Применение средств защиты ПК и информационных систем. (УК-2, УК-8, ПК-8)
8. Основная классификация инженерно-технических средств защиты. (УК-2, УК-8, ПК-8)
9. Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа. (УК-2, УК-8,,ПК-8)
10. Аппаратные средства защиты. Средства обнаружения, поиска и детальных измерений. (УК-2, УК-8, ПК-8)
11. Аппаратные средства защиты. Средства активного и пассивного противодействия. (УК-2, УК-8, ПК-8)

12. Аппаратные средства защиты ПК и информационных сетей. (УК-2, УК-8, ПК-8)

Вопросы к Разделу 3

1. Программные средства защиты. Основные группы. (УК-2, УК-8, ПК-8)
2. Программные средства защиты. Защита информации от НСД. (УК-2, УК-8, ПК-8)
3. Программные средства защиты. Защита от разрушения. Вирусы и антивирусные программы. (УК-2, УК-8, ПК-8)
4. Программные средства защиты. Архивирование информации. (УК-2, УК-8, ПК-8)
5. Защита информации в Интернете. (УК-2, УК-8, ПК-8)

Вопросы к Разделу 4

1. Криптографические методы защиты. (УК-2, УК-8, ПК-8)
2. Основные понятия криптографии и криптоанализа. (УК-2, УК-8, ПК-8)
3. Шифрование сообщений различными методами. (УК-2, УК-8, ПК-8)
4. Криптографическая система с открытым ключом. (УК-2, УК-8, ПК-8)

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для подготовки и успешного проведения практических занятий необходимо усвоить лекционный материал по теме, используя конспекты лекции. Настоятельно рекомендуется использовать рекомендуемую литературу и внимательно изучить соответствующие разделы учебников по теме.

Кроме этого необходимо, присутствуя на практических занятиях, проявлять активность и, самостоятельно или задавая вопросы преподавателю, выполнять практические работы, а не только фиксировать их в конспекте.

Усвоение материала дисциплины на лекциях, семинарах, практических занятиях и в результате самостоятельной подготовки и изучения отдельных вопросов дисциплины, позволят подойти к промежуточной аттестации подготовленным. Знания, накапливаемые постепенно и в различных ракурсах, с использованием противоположных мнений и взглядов на ту или иную проблему являются глубокими и качественными, и позволяют формировать соответствующие профессиональные компетенции как итог образовательного процесса.

Для систематизации знаний по дисциплине первоначальное внимание следует обратить на рабочую программу курса, которая включает в себя основные проблемы дисциплины (тематику занятий), в рамках которых и формируются вопросы для контроля и аттестации. Поэтому студент, заранее ознакомившись с программой курса, может лучше сориентироваться в последовательности освоения курса с позиций организации самостоятельной работы.

При организации процесса освоения дисциплины следует учитывать:

1. Планирование времени, отведенного на освоение дисциплины.

При планировании времени на освоение дисциплины следует руководствоваться: структурой дисциплины, в которой указаны количество академических часов в разрезе каждой темы, вида занятий (лекционное, практическое, семинарское) и часы на самостоятельную работу; формой текущего контроля успеваемости (тесты, выполнение индивидуальных и практических занятий и др.); формой промежуточной аттестации (экзамен).

2. Последовательность действий при освоении дисциплины.

Изучение каждой темы дисциплины целесообразно начинать со знакомства с содержанием дисциплины в разрезе тем; затем следует этап подбора источников из числа рекомендуемых и подобранных самостоятельно (научные статьи; информация с официальных сайтов государственных органов, органов местного самоуправления и др.). Изучение источниковой базы может сопровождаться конспектированием. Целесообразно вести перечень проблемных вопросов как по существу темы, обусловленных пробелами в научном и правовом поле и проблемами практического характера, так и в случае затруднений с уяснением смысла изложенного в источниках материала (указанные вопросы могут быть разрешены самостоятельно, во время сессионных занятий или на консультации с преподавателем).

Подготовка студентов к семинарским занятиям по данной дисциплине заключается в самостоятельной работе с источниками, представленными в списках основной и дополнительной литературы. Семинарские занятия проводятся в формах предусмотренных учебно-тематическим планом. На семинаре делаются доклады по темам занятий в виде выступлений, студент должен проявлять максимальную активность.

Для подготовки к практическим занятиям рекомендуется подробно изучить конспект лекций и материалы семинарских занятий, предшествующих практическому занятию. Также рекомендуется ознакомиться с технологией проведения практических занятий, которая включает следующие этапы: объяснение задания и навыков (компетенций), которые закрепляются в ходе его выполнения; знакомство с конкретными источниками информации для выполнения задания; обсуждение и уточнение вопросов в ходе анализа источников информации; совместный просмотр первичных результатов, оценка их соответствия по формальным и содержательным требованиям.

3. Использование учебно-методических материалов и работу с литературой.

Следует применять следующую последовательность источников для изучения тем дисциплины: нормативные правовые акты по дисциплине; комментарии к законодательным актам; научную и учебную литературу, а также другие источники.

4. Подготовку к текущему контролю успеваемости.

Основной задачей текущего контроля успеваемости обучающихся является повышение качества знаний, приобретение и развитие ими навыков самостоятельной работы. Текущий контроль знаний обучающихся по дисциплине может иметь следующие виды: устный опрос на лекциях, практических занятиях; проверка выполнения письменных самостоятельных работ и домашних за-

даний; тестирование.

Для эффективной подготовки к текущему контролю по дисциплине необходимо использовать рекомендованную основную и дополнительную литературу, конспекты лекций, разработки студентов, выполненные в результате подготовки и выполнения семинарских и практических занятий.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

5.1. Перечень компетенций и этапы их формирования

Согласно ФГОС ВО по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность» в рамках изучения дисциплины «Защита информации и информационная безопасность» у обучающихся должны быть сформированы следующие компетенции:

Код	Формулировка компетенции
УК	**Универсальные компетенции**
УК-2	Способность определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
УК-8	Способность создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций.
ПК	**Профессиональные компетенции**
ПК-8	Способность формировать и поддерживать рациональную систему документационного обеспечения

Этапы формирования компетенций:

Начальный – на этом этапе формируются знаниевые и инструментальные основы компетенции, осваиваются основные категории, формируются базовые умения. Студент воспроизводит термины, факты, методы, понятия, принципы и правила; решает учебные задачи по образцу. На начальном этапе студент знакомится с общими основами информационной безопасности, изучает угрозы информационной безопасности и знакомится с основными методами борьбы с этими угрозами. Если студент отвечает этим требования можно говорить об освоении им базового уровня компетенции.

Основной – знания, умения, навыки, обеспечивающие формирование компетенции, значительно возрастают, но еще не достигают итоговых значений. На этом этапе студент осваивает аналитические действия с предметными знаниями по конкретной дисциплине, способен самостоятельно решать учебные задачи, внося коррективы в алгоритм действий, осуществляя саморегуляцию в ходе работы, переносить знания и умения на новые условия. На основном этапе студент знакомится с организационно-правовыми основами деятель-

ности служб и органов информационной безопасности, изучает общие возможности технических и программных средств защиты информации, знакомится с элементами криптографии. Успешное прохождение этого этапа позволяет достичь среднего уровня сформированности компетенции;

Завершающий – на этом этапе студент достигает итоговых показателей по заявленной компетенции, то есть осваивает весь необходимый объем знаний, овладевает всеми умениями и навыками в сфере заявленной компетенции. Он способен использовать эти знания, умения, навыки при решении задач повышенной сложности и в нестандартных условиях. На завершающем этапе студент осваивает способы защиты информации и обеспечения информационной безопасности в своей профессиональной сфере и готов к их реальному применению. По результатам этого этапа студент демонстрирует итоговый уровень сформированности компетенции.

5.2. Показатели и критерии оценивания компетенций и шкала оценивания

Для оценивания результатов обучения в виде знаний используются следующие процедуры и технологии: тестирование; индивидуальное собеседование, письменные ответы на вопросы (в виде *текущего контроля*).

Промежуточный контроль реализуется в ходе сдачи обучающимися очной и заочной формы обучения зачёта. При сдаче зачёта студент отвечает на теоретический вопрос из билета и проходит тестирование по конкретным понятиям и ситуациям. В случае неудовлетворительной оценки студент имеет право пересдать зачёт в установленном порядке.

Критерии оценивания ответов	Оценка
Правильные и полные ответы на вопросы билета и дополнительные вопросы с чётким последовательным изложением материала и (при необходимости) с приведением примеров, иллюстрирующих теоретические положения. Правильное выполнение практического задания.	зачтено
Некоторые неточности при правильном (в целом) изложении материала, неполнота ответа. Незначительные ошибки при выполнении практического задания.	зачтено
Неточности при изложении материала, неполнота ответа и его логическая непоследовательность (фрагментарность). Существенные ошибки при выполнении практического задания (при общем правильном направлении его решения).	зачтено

Отсутствие знаний в области теории и практики, несвязное, нелогичное и существенно неполное изложение материала. Достаточно частые нарушения учебного процесса, значительные пропуски занятий, невыполнение текущих заданий.	не зачтено

5.3. Материалы для оценки и контроля результатов обучения

Форма проведения промежуточного контроля включает теоретическую и практическую (исполнительскую форму) части. В теоретической части студент отвечает на вопросы билета, а в практической проходит тест.

Теоретическая часть. Перечень вопросов к зачёту

Вопросы	**Формируемые компетенции**
Теоретические вопросы	
1. Определение цели и задачи защиты данных. Модель информационной безопасности (основные положения)	УК-2, УК-8, ПК-8
2. Права и обязанности собственника, владельца и потребителя в области защиты информации	УК-2, УК-8, ПК-8
3. Основные характеристики информационных ресурсов (государственных и негосударственных) в условиях информационного общества	УК-2, УК-8, ПК-8
4. Определение угрозы информационной безопасности	УК-2, УК-8, ПК-8
5. Классификации угроз информационной безопасности	УК-2, УК-8, ПК-8
6.Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД (несанкционированный доступ)	УК-2, УК-8, ПК-8
7. Основные направления обеспечения информационной безопасности	УК-2, УК-8, ПК-8
8. Законодательство РФ о защите информации	УК-2, УК-8, ПК-8
9. Основные организационные мероприятия информационной безопасности	УК-2, УК-8, ПК-8
10. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу	УК-2, УК-8, ПК-8
11. Способы защиты информации. Основные положения	УК-2, УК-8, ПК-8
12. Организация защиты ПК и информационных систем	УК-2, УК-8, ПК-8
13. Применение средств защиты ПК и информационных си-	УК-2, УК-8,

стем	ПК-8
14. Основная классификация инженерно-технических средств защиты	УК-2, УК-8, ПК-8
15. Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа	УК-2, УК-8, ПК-8
16. Аппаратные средства защиты. Средства обнаружения, поиска и детальных измерений	УК-2, УК-8, ПК-8
17. Аппаратные средства защиты. Средства активного и пассивного противодействия	УК-2, УК-8, ПК-8
18. Аппаратные средства защиты ПК и информационных сетей	УК-2, УК-8, ПК-8
19. Программные средства защиты. Основные группы.	УК-2, УК-8, ПК-8
20. Программные средства защиты. Защита информации от НСД.	УК-2, УК-8, ПК-8
21. Программные средства защиты. Защита от разрушения. Вирусы и антивирусные программы.	УК-2, УК-8, ПК-8
22. Программные средства защиты. Архивирование информации.	УК-2, УК-8, ПК-8
23. Защита информации в Интернете.	УК-2, УК-8, ПК-8
24. Криптографические методы защиты. Криптографическая система с открытым ключом	УК-2, УК-8, ПК-8
25. Основные понятия криптографии и криптоанализа.	УК-2, УК-8, ПК-8
26. Шифрование сообщений различными методами.	УК-2, УК-8, ПК-8

Практическая часть

Прохождение теста по основам защиты информации.

5.4.Методические материалы по оцениванию результатов обучения

Как уже было отмечено в пункте 5.2., для положительной сдачи зачёта студенту необходимо сдать теоретическую и практическую части, при этом:

- теоретическая часть сдаётся в форме ответа на вопрос из билета;
- практическая часть состоит в прохождении теста по конкретным понятиям и ситуациям.

На подготовку ответа отводится 30-45 минут. Оценка знаний производится по шкале «зачтено»-«не зачтено».

Ниже приводится вариант тестовых заданий для сдачи зачёта.

Тест для итогового контроля знаний (зачёт)

По дисциплине “Защита информации и информационная безопасность”
25 вопросов на 45 минут, вариант правильного ответа только один
(тест считается пройденным успешно, если получены правильные ответы более чем на 50% заданий теста)

Задание № 1
Что такое конфиденциальность информации?
- свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации;
- свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);
- свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора;
- свойство информации, заключающееся в ее шифровании.

Задание № 2
Что не относится к угрозам информационной безопасности?
- событие, действие, процесс или явления, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию;
- классификация информации по видам;
- стихийные бедствия (наводнения, ураган, землетрясение, пожар);
- сбои и отказы оборудования (технических средств) автоматизированных систем;
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников.

Задание № 3
Что относится к правовым мерам защиты информации?
- законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения;
- действия правоохранительных органов для защиты информационных ресурсов;
- организационно-административные меры для защиты информационных ресурсов;
- действия администраторов сети для защиты информационных ресурсов.

Задание № 4
Что такое государственная тайна?
- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ;

- сведения о состоянии окружающей среды;
- все сведения, которые хранятся в государственных базах данных;
- сведения о состоянии здоровья президента РФ.

Задание № 5
Что такое коммерческая тайна?
- информация, имеющая действительную или потенциальную коммерческую ценность в силу её неизвестности третьим лицам;
- информация, содержащая в учредительных документах;
- информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов.

Задание № 7
Что не входит в задачи службы безопасности организации?
- выявление лиц, проявляющих интерес к коммерческой тайне предприятия;
- разработка системы защиты секретных документов;
- определение уязвимых участков на предприятии, аварии или сбои в работе которых могут нанести урон работе предприятия;
- планирование, обоснование и организация мероприятий по защите информации;
- определение сведений, составляющих коммерческую тайну;
- арест нарушителей информационной безопасности.

Задание № 8
Что такое несанкционированный доступ (НСД)?
- доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;
- создание резервных копий в организации;
- правила и положения, выработанные в организации для обхода парольной защиты;
- удаление не нужной информации.

Задание № 9
Что такое идентификация?
- процесс распознавания элемента системы, обычно с помощью заранее определённого идентификатора или другой уникальной информации;
- указание на правильность выполненных операций по защите информации;
- определение файлов, которые изменены в информационной системе несанкционированно;
- выполнение процедуры засекречивания файлов;
- процесс периодического копирования информации.

Задание № 10

Что такое аутентификация?
- проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы;
- нахождение файлов, которые изменены в информационной системе несанкционированно;
- проверка количества переданной и принятой информации;
- определение файлов, из которых удалена служебная информация.

Задание № 11
Что такое асимметричный метод шифрования?
- метод защиты информации, где для шифрования и дешифрования информации используются различные ключи;
- метод защиты информации, где для шифрования и дешифрования информации используются больше трех ключей;
- метод защиты информации, где шифрование и дешифрование информации осуществляют без ключа.

Задание № 12
Что такое электронная цифровая подпись?
- реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный с использованием закрытого ключа и позволяющий идентифицировать владельца подписи, а также установить отсутствие искажения информации в документе;
- набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями;
- индивидуальный код, известный ограниченному кругу пользователей и зашифрованный симметричным ключом.

Задание № 13
Выберите правильные варианты ответов.
Какие из перечисленных программно-технических мероприятий не относятся к обеспечивающим безопасное использование информационных систем:
- аутентификация пользователя и установление его идентичности;
- управление доступом к базам данных;
- задействование законодательных и административных ресурсов;
- протоколирование и аудит.

Задание № 14
Выберите правильные варианты ответа.
Виды информации, которые не требуют защиты:
- государственная тайна;
- врачебная тайна;
- коммерческая тайна;
- информация о погоде.

Задание № 15
Вставьте пропущенное понятие.
В криптографических механизмах защиты используется секретный____.
- ключ;
- носитель;
- агент.

Задание № 16
Приведен перечень мероприятий:
1. Защита от несанкционированного доступа;
2. Защита файлов на магнитных дисках от изменения или уничтожения, обеспечение возможности по восстановлению уничтоженных файлов;
3. Архивирование файлов;
4. Шифрование данных.
Этот комплекс мероприятий соответствует следующему методу защиты информации:
- программному;
- техническому;
- организационному;
- законодательному;
- аппаратному.

Задание № 17
Какое из направлений защиты информации не относится к программным средствам?
- экранирование компьютерной техники;
- архивирование файлов;
- шифрование файлов.

Задание № 18
Какой из способов задания паролей является наиболее надежным?
- произвольная комбинация цифр и букв в нижнем и верхнем регистре;
- дата рождения пользователя;
- имя одного из членов семьи пользователя;
- название любимой книги (фильма, музыкального исполнителя);
- нецензурное выражение.

Задание № 19
Каким из способов защиты можно установить факт и виновного
в несанкционированном доступе к конфиденциальной информации?
- регистрация доступа к устройствам и данным;
- запись в специальном журнале, ответственного за безопасность системы;
- контроль ответственным за безопасность работы каждого пользователя системы;

- опрос всех пользователей, подозреваемых в содеянном.

Задание № 20
Для какого из способов защиты целесообразно применять программы-архиваторы файлов?
- резервного копирования файлов на съемные носители;
- санкционирования доступа к устройствам и данным;
- шифрование конфиденциальной информации.

Задание № 21
Процесс преобразования открытых данных в закрытые для защиты от несанкционированного использования (чтения, распространения) называется:
- шифрование;
- дешифрование;
- регистрация;
- аутентификация;
- секьюритизация.

Задание № 22
"Специально написанная, обычно небольшая по размерам программа, которая размножается путем записи своих копий в другие программы и в системные области дисков, производящая нежелательные действия". Это определение:
- компьютерного вируса;
- компьютерного драйвера;
- компьютерной оболочки;
- компьютерного змея.

Задание № 23
Вирусы, которые остаются в оперативной памяти компьютера после выполнения своих действий по заражению и размножению, называются:
- резидентными;
- адекватными;
- агентурными;
- ждущими;
- спящими.

Задание № 24
К умышленным нарушениям безопасности информации относятся:
- несанкционированное копирование данных;
- неверное исполнение программ, связанное с воздействием внешней среды;
- нарушение правил эксплуатации оборудования;
- несчастные случаи, стихийные бедствия.

Задание № 25
Программы криптографии предназначены для:

- шифрования информации;
- управления доступом к информационным массивам;
-обеспечения логического управления доступом в информационную систему;
-обеспечения подотчетностей пользователя и администрации;
-обнаружения попыток нарушения информационной безопасности.

6. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

6.1. Основная и дополнительная учебная литература

Основная литература

1.Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. –

URL: http://biblioclub.ru/index.php?page=book&id=93356

2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. –

URL: http://biblioclub.ru/index.php?page=book&id=276557

3. Киселёв В.И. Информационная безопасность и защита информации: Учебное пособие. –Хабаровск: ХГИК, 2018. – 122 с.

Дополнительная литература

1. Антивирусная защита компьютерных систем / Национальный Открытый Университет "ИНТУИТ". - М.: Интернет-Университет Информационных Технологий, 2007. - 282 с.: ил.; То же [Электронный ресурс]. –
URL: http://biblioclub.ru/index.php?page=book&id=233568
2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895
3. Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с.: ил.; То же [Электронный ресурс]. –
URL:http://biblioclub.ru/index.php?page=book&id=429032
4. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара: Самарский государственный архитек-

турно-строительный университет, 2014. - 113 с. : Библиогр. в кн. - ISBN 978-5-9585-0603-3; То же [Электронный ресурс]. –
URL: http://biblioclub.ru/index.php?page=book&id=438331

Электронные образовательные ресурсы

1. Анализ состояния защиты данных в информационных системах: учебно-методическое пособие / сост. В.В. Денисов. - Новосибирск : НГТУ, 2012. - 52 с. : ил., табл., схем. - ISBN 978-5-7782-1969-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228844
2. Антивирусная защита компьютерных систем / Национальный Открытый Университет "ИНТУИТ". - М.: Интернет-Университет Информационных Технологий, 2007. - 282 с.: ил.; То же [Электронный ресурс]. –
URL: http://biblioclub.ru/index.php?page=book&id=233568
3. Гуляев, В.П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплекс / В.П. Гуляев; Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. - Екатеринбург: Издательство Уральского университета, 2014. - 163 с. : ил., схем. - Библиогр. в кн. - ISBN 978-5-7996-1120-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=275706
4. Долозов, Н.Л. Программные средства защиты информации: конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск: НГТУ, 2015. - 63 с.: схем., ил. - Библиогр. в кн. - ISBN 978-5-7782-2753-8; То же [Электронный ресурс]. –
URL: http://biblioclub.ru/index.php?page=book&id=438307
5. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895
6. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. –
URL: http://biblioclub.ru/index.php?page=book&id=276557
7. Кияев, В. Безопасность информационных систем: курс / В. Кияев, О. Граничин. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с.: ил.; То же [Электронный ресурс]. –
URL:http://biblioclub.ru/index.php?page=book&id=429032
8. Михайлов, А.В. Компьютерные вирусы и борьба с ними: учебное пособие / А.В. Михайлов. - М.: Диалог-МИФИ, 2010. - 104 с.: ил. - ISBN 978-5-86404-236-6; То же [Электронный ресурс]. –
URL:http://biblioclub.ru/index.php?page=book&id=136089
9. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова; Министерство образования и науки РФ, Федераль-

ное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3; То же [Электронный ресурс]. –
URL: http://biblioclub.ru/index.php?page=book&id=438331
10. Ханипова, Л.Ю. Информационная безопасность и защита информации: учебное пособие / Л.Ю. Ханипова, Г.Р. Кутлова; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Башкирский государственный педагогический университет им. М. Акмуллы», Министерство образования и науки РФ. - Уфа: БГПУ, 2010. - 112 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-87978-681-1; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=438523

6.2. Ресурсы информационно-телекоммуникационной сети «Интернет»

В соответствии с лицензионными нормативами обеспечения библиотечно-информационными ресурсами библиотека организует индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет, к учебным материалам Электронно-библиотечных систем (ЭБС):

1. ЭБС «Университетская библиотека онлайн». Издательство: ООО «НексМедиа». Принадлежность сторонняя. www.biblioclub.ru. Количество ключей (пользователей): 100% on-line. Характеристики библиотечного фонда, доступ к которому предоставляется договором: доступ к базовой части ЭБС.

2. БД Электронная Система «Культура». База Данных Электронная Система «Культура». Принадлежность сторонняя. http://www.e-mcfr.ru.

3. Web ИРБИС Хабаровский государственный институт искусств и культуры (электронный каталог). Международная ассоциация пользователей и разработчиков электронных библиотек и новых информационных технологий (ассоциация ЭБНИТ). Принадлежность сторонняя. http://irbis.hgiik.ru.

4. eLIBRARY.ru – Научная электронная библиотека. ООО Научная электронная библиотека. Принадлежность сторонняя. http://elibrary.ru/ Лицензионное соглашение № 13863 от 03.10.2013 г. – бессрочно.

5. Электронно-библиотечная система ФГБОУ ВО «ХГИК». ФГБОУ ВО «ХГИК». Принадлежность собственная. Локальный доступ. http://carta.hgiik.ru. Приказ по Институту № 213-об от 07.10.2013 г.

6. Единое окно доступа к образовательным ресурсам. Электронная библиотека. ФГАУ ГНИИ ИТТ «Информика», Министерство образования и науки РФ. Принадлежность сторонняя. Свободный доступ. http://window.edu.ru

7. Единая коллекция Цифровых Образовательных Ресурсов. ФГАУ ГНИИ ИТТ «Информика». Принадлежность сторонняя. Свободный доступ.
http://school-collection.edu.ru

8. Федеральный центр информационно-образовательных ресурсов. Федеральный центр информационно- образовательных ресурсов, ФГАУ ГНИИ ИТТ «Информика». Принадлежность сторонняя. Свободный доступ.
http://fcior.edu.ru

Для подготовки курсовых, выпускных и научных работ обучающиеся могут использовать полнотекстовую базу данных Web of Science. Режим доступа: электронный, из внутренней сети института. Официальный
сайт: webofknowledge.com

6.3. Информационные технологии, программное обеспечение, информационные справочные системы

Программно-информационное обеспечение учебного процесса соответствует требованиям федерального государственного образовательного стандарта.

Для проведения занятий лекционного типа, занятий семинарского типа, занятий практического типа, групповых консультаций, текущего контроля и промежуточной аттестации используется следующее программное обеспечение:

– лицензионное проприетарное программное обеспечение:

1. Microsoft Windows
2. Microsoft Office (в состав пакета входят: Word, Excel, PowerPoint, FrontPage, Access)
3. Adobe Creative Suite 6 Master Collection (в состав пакета входят: Photoshop CS6 Extended, Illustrator CS6, InDesign CS6, Acrobat X Pro, Dreamweaver CS6, Flash Professional CS6, Flash Builder 4.6 Premium Edition, Dreamweaver CS6, Fireworks CS6, Adobe Premiere Pro CS6, After Effects CS6, Adobe Audition CS6, SpeedGrade CS6, Prelude CS6, Encore CS6, Bridge CS6, Media Encoder CS6);

– свободно распространяемое программное обеспечение:

1. набор офисных программ Libre Office
2. аудиопроигрыватель AIMP
3. видеопроигрыватель Windows Media Classic
4. интернет-браузер Chrome.

Для самостоятельной подготовки студентов к занятиям по дисциплине требуется обращение к программному обеспечению Microsoft Windows, Microsoft Office, в том числе для подготовки мультимедийных презентаций по темам семинаров в программе PowerPoint. Для создания конечных не редактируемых версий документа рекомендуется использовать Acrobat X Pro, входящий в состав пакета Adobe Creative Suite 6 Master Collection.

При изучении дисциплины обучающиеся имеют возможность использования информационно-справочных систем «Культура» и «Гарант», Всероссий-

скую отраслевую справочную систему «Информио», реферативных и библиометрических баз данных рецензируемой литературы Web of Science и Scopus, в соответствии с заключенными договорами.

На всех компьютерах в институте установлено лицензионное антивирусное программное обеспечение Kaspesky Endpoint Security. Необходимым условием информационной безопасности института является обязательная проверка на наличие вирусов внешних носителей перед их использованием с помощью Kaspesky Endpoint Security.

Перечисленное программное обеспечение обновляется по мере выхода новых версий программ в рамках соответствующих лицензий и соглашений.

6.4. Материально-техническая база

Материально-техническое обеспечение реализуемой дисциплины соответствует требованиям федерального государственного образовательного стандарта.

Для проведения занятий лекционного типа, занятий семинарского типа, занятий практического типа, групповых консультаций, текущего контроля и промежуточной аттестации в учебном процессе активно используются следующие специальные помещения:

- аудитория 309 с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду вуза.

Для самостоятельной работы студентов предназначены:

- ауд. 209 (читальный зал), оборудованный персональными компьютерами, обеспечивающими доступ к электронной информационно-образовательной среде организации, к сети «Интернет», к электронным библиотечным системам;

При необходимости в учебном процессе используются комплекты переносных демонстрационных комплексов (ноутбук, проектор, экран).

Все компьютеры Института объединены в локальную сеть, с каждого из них возможен выход в глобальную сеть Интернет. Институт использует выделенный канал со скоростью 10 Мб/с. Для студентов имеется возможность выхода в сеть Интернет с мобильных устройств посредством сети WiFi, которая установлена в читальном зале Института.

Проведение лекций по данной дисциплине может сопровождаться слайд-презентациями.

7. ВОСПИТАТЕЛЬНАЯ РАБОТА

Воспитание обучающихся при освоении ими основных профессиональных образовательных программ (далее – ОПОП) осуществляется на основе рабочей программы воспитания и календарного плана воспитательной работы, включаемых в ОПОП.

Цель воспитательной работы – создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

Задачи воспитательной работы: развитие мировоззрения и актуализация системы базовых ценностей личности, приобщение к общечеловеческим нормам морали, национальным устоям и академическим традициям; воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности; воспитание положительного отношения к труду, формирование культуры и этики профессионального общения; формирование личностных качеств, необходимых для эффективной профессиональной деятельности; воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде; повышение уровня культуры безопасного поведения.

Особенности и традиции Института обусловливают следующие основные направления воспитательной работы: патриотическое, гражданское, духовно-нравственное, культурно-творческое, научно-образовательное, профессионально-трудовое, волонтерское (добровольческое), экологическое, физическое. Виды деятельности обучающихся в воспитательной системе образовательной организации: проектная деятельность (как коллективное творческое дело), волонтерская деятельность, учебно-исследовательская и научно-исследовательская деятельность, досуговая, творческая и социально-культурная деятельность и др.

Воспитательный потенциал учебно-исследовательской и научно-исследовательской деятельности реализуется в процессе развития исследовательской компетентности обучающихся на протяжении всего срока их обучения в Институте. Результаты студенческой научно-исследовательской деятельности проходят апробацию в рамках научных и научно-практических конференций различного уровня, в т.ч. конференций, организованных Институтом.

Социально-культурная и творческая деятельность обучающихся реализуется при организации и проведении значимых событий и мероприятий гражданско-патриотической, научно-исследовательской, социокультурной и физкультурно-спортивной направленности. Виды творческой деятельности обучающихся в Институте: музыкальное творчество, хореографическое творчество, театральное творчество, научное творчество, медиапроекты и др.

Волонтерская деятельность обучающихся – широкий круг направлений созидательной деятельности, включающий различные формы гражданского участия. По инициативе обучающихся и при их активном участии в Институте осуществляет свою деятельность добровольческий отряд «Мы».

Реализацию Рабочей программы воспитания помогает обеспечивать взаимодействие с различными социальными институтами, субъектами воспитания. Особое значение для воспитательного процесса имеет организация практической деятельности обучающихся с целью развития профессиональных компетенций в условиях Института и профильных учреждений и организаций.

8. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В процессе изучения дисциплины и осуществления процедур текущего контроля успеваемости и промежуточной аттестации инвалидов и лиц с ограниченными возможностями здоровья применяются адаптированные формы обучения с учетом индивидуальных психофизиологических особенностей.

Обучение лиц с ограниченными возможностями и инвалидов организуется как совместно с другими обучающимися на лекционных и практических занятиях, так и по индивидуальному учебному плану. Во время приемной кампании, а также во время сдачи различных форм промежуточной и государственной итоговой аттестации в Институте созданы необходимые условия для оказания технической помощи инвалидам и лицам с ограниченными возможностями здоровья (при необходимости может быть допущено присутствие в аудитории ассистентов, сопровождающих лиц, собаки-поводыря и т.п.).

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья, при необходимости, могут быть обеспечены электронными и печатными образовательными ресурсами с учетом их индивидуальных потребностей. Для реализации доступной среды при необходимости в учебном процессе могут быть задействованы документ-камера для увеличения текстовых фрагментов и изображений (для лиц с нарушениями зрения) и переносная индукционная система для слабослышащих «Исток» А2 со встроенным плеером – звуковым информатором.

ЭБС «Университетская библиотека онлайн» предоставляет обучающимся с ОВЗ (по зрению) ряд возможностей для обеспечения эффективности процесса обучения. При чтении масштаб страницы сайта можно увеличить с помощью специального значка на главной странице. Можно использовать полноэкранный режим отображения книги или включить озвучивание непосредственно с сайта при помощи программ экранного доступа (например, Jaws , «Balabolka»). Скачиваемые фрагменты в формате pdf, имеющие высокое качество, могут использоваться тифлопрограммами для голосового озвучивания текстов, могут быть загружены в тифлоплееры, а также скопированы на любое устройство для комфортного чтения.

Сервис ЭБС «Цитатник» помогает пользователю извлечь цитату и автоматически формирует корректную библиографическую ссылку, что особенно актуально для лиц с ограниченными возможностями и облегчает процесс написания курсовой или выпускной квалификационной работы.

Для подготовки к занятиям обучающиеся с ОВЗ (по зрению) могут использовать мобильное приложение ЭБС «Лань», предназначенное для озвучивания текста книги. Режим доступа: электронный, приложение скачивается обучающимся самостоятельно с сайта e.lanbook.ru, необходимое условие: быть зарегистрированным в ЭБС «Лань». Используется свободно распространяемая программа экранного доступа Nvda.

Подробнее об организации доступной среды см. соответствующий раздел основной профессиональной образовательной программы.