Министерство культуры Российской Федерации
ФГБОУ ВО «Кемеровский государственный институт культуры»
Факультет информационных, библиотечных и музейных технологий
Кафедра цифровых технологий и ресурсов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Рабочая программа дисциплины

Направление подготовки

42.04.05 Медиакоммуникации

Профиль подготовки

«Медиаменеджмент»

Квалификация (степень) выпускника:
Магистр

Форма обучения:
заочная

Кемерово

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки 42.04.05 Медиакоммуникации, профилю подготовки «Медиаменеджмент», квалификация (степень) выпускника – магистр.

Утверждена на заседании кафедры цифровых технологий и ресурсов. Рекомендована к размещению на сайте Кемеровского государственного института культуры «Электронная информационно-образовательная среда КемГИК» по web-адресу http://edu2020.kemguki.ru (31.08.2022 г., протокол № 1).

Переутверждена на заседании кафедры цифровых технологий и ресурсов. Рекомендована к размещению на сайте Кемеровского государственного института культуры «Электронная информационно-образовательная среда КемГИК» по web-адресу http://edu2020.kemguki.ru (23.05.2023 г., протокол № 10).

Мишова, В.В. Информационная безопасность и защита информации: рабочая программа дисциплины по направлению подготовки 42.04.05 Медиакоммуникации, профилю подготовки «Медиаменеджмент», квалификация (степень) выпускника «магистр» / В.В. Мишова. – Кемерово: Кемеров. гос. институт культуры, 2022. – 20 с. – Текст : непосредственный.

Автор:
канд. пед. наук, доцент
Мишова В.В.

1. Цели освоения дисциплины (модуля)

формирование знаний в области информационной безопасности и практических умений, направленных на организацию обеспечения защиты информации.

2. Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Информационная безопасность и защита информации» входит в базовую часть блока дисциплин образовательной программы по направлению подготовки 42.04.05 Медиакоммуникации, квалификация (степень) «магистр». Дисциплина изучается в 1 семестре обучения на очнойи на заочной формах обучения. Для освоения дисциплины «Информационная безопасность и защита информации» необходимы знания, умения и компетенции, сформированные в результате изучения студентами программ бакавриата. Компетенции, сформированные при освоении дисциплины «Информационная безопасность и защита информации», также необходимы при прохождении производственной практики в процессе обучения.

3. Планируемые результаты обучения по дисциплине (модулю)

Изучение дисциплины направлено на формирование следующих компетенций (УК, ОПК, ПК) и индикаторов их достижения.

Код и наименование компетенции	**Индикаторы достижения компетенций**		
	знать	**уметь**	**владеть**
ПК-3. Способен организовать работу и руководить предприятием (подразделением), осуществляющим медиакоммуникационную деятельность	• компоненты концептуальной модели информационной безопасности; • классификацию и характеристику угроз информационной безопасности; • классификацию преступлений в сфере информационной безопасности; • нормативно-правовые документы в области защиты информации; • требования к комплексной системе защиты информации.	• выявлять угрозы информационной безопасности; • применять на практике нормативно-правовые документы в области защиты информации; • обосновывать и осуществлять выбор средств защиты информации.	• терминологией в сфере информационной безопасности; • способами предотвращения случайных и предумышленных угроз информационной безопасности.

4. Объем, структура и содержание дисциплины (модуля)

4.1 Объем дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 академических часа.

Для студентов очной формы обучения предусмотрено 48 часов контактной (аудиторной) работы с обучающимися (22 часов лекций, 22 часов практических занятий), 64 часа самостоятельной работы. 14 час (30 %) аудиторной работы проводится в интерактивных формах.

Для студентов заочной формы обучения предусмотрено 10 часов контактной (аудиторной) работы с обучающимися (4 часа лекций, 4 часов практических занятий) и 100 часов самостоятельной работы. 2 часа (30 %) аудиторной работы проводится в интерактивных формах.

Практическая подготовка при реализации учебной дисциплины организуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка включает в себя отдельные занятия лекционного типа, которые предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанной с будущей профессиональной деятельностью.

4.2. Структура дисциплины (модуля)

Очная форма обучения

№/№	Наименование модулей (разделов) и тем	Семестр	Виды учебной работы, и трудоемкость (в часах)				
			Всего	Лекции	Лаб. занятия	В т.ч. ауд. занятия в интерактивной форме*	СРО
Раздел 1. Концептуальные положения защиты информации в информационных системах							
1.1	Информационная безопасность: определение понятия, состав, назначение	4	16	4/2*	4	2* Лекция-дискуссия	8
1.2	Информационная система как объект защиты	4	12	2	2		8
1.3	Угрозы информационной безопасности в информационных системах	4	16	4/2*	4	2* Лекция-дискуссия	8
Раздел 2. Направления защиты информации в документационном обеспечении управления и архивном деле							
2.1	Правовое обеспечение информационной безопасности	4	16	4	4*	6* Реализация проекта	10
2.2	Организационное обеспечение информационной безопасности	4	14	2	2		10
2.3	Программно-техническое обеспечение информационной безопасности	4	14	4	4/2*	2* Реализация проекта	10

2.4	Комплексная система защиты информации	4	18	4	4/4*	4* Защита проекта	10
	Всего часов в интерактивной форме:					16*(30,5%)	
	Итого:		**108**	**24**	**24**	-	**64**

Заочная форма обучения

№/ №	**Наименование модулей (разделов) и тем**	**Семестр**	**Виды учебной работы, и трудоемкость (в часах)**				
			Всего	**Лекции**	**Лаб. занятия**	**В т.ч. ауд. занятия в интерактивной форме***	**СРО**
Раздел 1. Концептуальные положения защиты информации в информационных системах							
1.1	Информационная безопасность: определение понятия, состав, назначение	4	13	1*	-	1* Лекция-дискуссия	12
1.2	Информационная система как объект защиты	4	12	-			12
1.3	Угрозы информационной безопасности в информационных системах	4	13	1	-		12
Раздел 2. Направления защиты информации в документационном обеспечении управления и архивном деле							
2.1	Правовое обеспечение информационной безопасности	4	17	1			16
2.2	Организационное обеспечение информационной безопасности	4	16	-	-		16
2.3	Программно-техническое обеспечение информационной безопасности	4	18	-	2/1*		16
2.4	Комплексная система защиты информации	4	18	-	2/2*	3* Защита проекта	16
	Всего часов в интерактивной форме:					4*(33%)	
	Итого:		**108**	**4**	**4**	-	**100**

4.3 Содержание дисциплины (модуля)

№ п/п	Содержание дисциплины (Разделы. Темы)	Результаты обучения	Виды оценочных средств; формы текущего контроля, промежуточной аттестации
Раздел 1. Концептуальные положения защиты информации в информационных системах			
1.1	***Тема 1.1 Информационная безопасность: определение понятия, состав, назначение*** Понятие определения «информационная безопасность». Исторические аспекты возникновения и развития информационной безопасности. Концептуальная модель информационной безопасности. Основные составляющие информационной безопасности: доступность, целостность, конфиденциальность.	***Формируемые компетенции:*** • Способен организовать работу и руководить предприятием (подразделением), осуществляющим медиакоммуникационную деятельность (ПК-3). В результате изучения темы студент должен: ***знать:*** • компоненты концептуальной модели информационной безопасности; • классификацию и характеристику угроз информационной безопасности; • классификацию преступлений в сфере информационной безопасности; • нормативно-правовые документы в области защиты информации; • требования к комплексной системе защиты информации. ***уметь:*** • выявлять угрозы информационной безопасности; • применять на практике нормативно-правовые документы в области защиты информации; • обосновывать и осуществлять выбор средств защиты информации. ***владеть:*** • терминологией в сфере информационной безопасности; • способами предотвращения случайных и предумышленных угроз информационной безопасности.	Отчет о выполнении лабораторной работы
1.2	***Тема 1.2 Информационная система как объект защиты*** Определение и состав информационной системы, принципы ее функционирования. Оценка качества информационной системы. Проблемы защиты информационных систем. Факторы, обусловливающие необходимость защиты информационных ресурсов информационных систем. Характеристики информационных систем, влияющие на безопасность информации.		Отчет о выполнении лабораторной работы
1.3	***Тема 1.3 Угрозы информационной безопасности в информационных системах*** Классификация и характеристика угроз		Отчет о выполнении лабораторной работы

	информационной безопасности. Классификация и характеристика источников угроз информационной безопасности. Предпосылки появления угроз. Цели угроз информационной безопасности. Классификация преступлений в сфере информационной безопасности.		
Раздел 2. Направления защиты информации в документационном обеспечении управления и архивном деле			
2.1	***Тема 2.1 Правовое обеспечение информационной безопасности*** Основные положения государственной политики обеспечения информационной безопасности РФ. Государственные органы РФ, контролирующие деятельность в области защиты информации. Российское законодательство в области защиты информации. Особенности правового обеспечения информационной безопасности в документационном обеспечении управления и архивном деле.	***Формируемые компетенции:*** • Способен организовать работу и руководить предприятием (подразделением), осуществляющим медиакоммуникационную деятельность (ПК-3). В результате изучения темы студент должен: ***знать:*** • компоненты концептуальной модели информационной безопасности; • классификацию и характеристику угроз информационной безопасности; • классификацию преступлений в сфере информационной безопасности; • нормативно-правовые документы в области защиты информации; • требования к комплексной системе защиты информации. ***уметь:*** • выявлять угрозы информационной безопасности; • применять на практике нормативно-правовые документы в области защиты информации; • обосновывать и осуществлять выбор средств защиты информации. ***владеть:*** • терминологией в сфере информационной безопасности;	Отчет о выполнении лабораторной работы
2.2	***Тема 2.2 Организационное обеспечение информационной безопасности*** Состав политики и программы безопасности организации. Процедурные меры безопасности: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушение режима безопасности,		Отчет о выполнении лабораторной работы

	планирование восстановительных работ. Особенности организационного обеспечения информационной безопасности в документационном обеспечении управления и архивном деле.	• способами предотвращения случайных и предумышленных угроз информационной безопасности.	
2.3	***Тема 2.3 Программно-техническое обеспечение информационной безопасности*** Классификация средств программно-технической защиты информации. Назначение и характеристика средств защиты информации. Характеристика программно-технических методов, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. Средства криптографической защиты информации. Цифровая подпись.		Отчет о выполнении лабораторной работы, тестовый контроль
2.4	***Тема 2.4 Комплексная система защиты информации*** Требования к комплексной системе защиты информации. Принципы создания комплексной системы защиты информации. Этапы построения комплексной системы защиты информации. Эффективность защиты информации.		Защита проекта

5. Образовательные и информационно-коммуникационные технологии

5.1 Образовательные технологии

В ходе обучения используются традиционные образовательные технологии, включающие аудиторные занятия в форме лекций и лабораторных работ, а также развивающие проблемно-поисковые технологии: проблемное изложение лекционного материала; проблемно-исследовательские задания; дискуссии; проектные формы.

Освоение учебного материала сопровождается интерактивными формами обучения. При организации лекционных занятий используется форма лекции-дискуссии.

На лабораторных занятиях предполагается использование интерактивной формы – защита проектов.

Доля аудиторных занятий, проводимых в интерактивных формах обучения, составляет 30 % на очной форме обучения и 30% на заочной форме обучения, что соответствует требованиям ФГОС ВО по направлению подготовки 42.04.05 Медиакоммуникации.

В целях самоконтроля знаний студентов используются технологии проверки уровня овладения учебным материалом с использованием контрольных вопросов и тестовых заданий по разделам дисциплины.

Для диагностики компетенций применяются следующие формы контроля: устный опрос, защита отчетов о выполнении лабораторных работ, тестирование, защита учебного исследовательского проекта (на очной и заочной формах обучения), экзамен.

5.2 Информационно-коммуникационные технологии

При организации учебного процесса широко используется сочетание образовательных и информационно-коммуникационных технологий: практикуются мультимедийные лекционные занятия, информационно-коммуникационные технологии сопровождают проведение лабораторных работ, организацию самостоятельной работы студентов.

На сайте «Электронная образовательная среда КемГИК» (https://edu.kemgik.ru/course/view.php?id=4964) размещены теоретические, практические, справочные, методические, контрольно-измерительные электронные ресурсы по дисциплине.

Активизацию самостоятельной работы студентов и контроль результатов и сроков освоения разделов и тем дисциплины обеспечивает использование таких интерактивных элементов «Электронной образовательной среды КемГИК», как «Задание» и «Тест». Интерактивный элемент «Тест» включает различные типы вопросов и используется как одно из основных средств объективной оценки знаний студента в ходе самоконтроля, текущего и промежуточного контроля знаний по дисциплине.

Интерактивный элемент «Задание» позволяет преподавателю поддерживать обратную связь со студентом посредством проверки задания (отчетов о выполнении лабораторных работ, учебных исследовательских проектов) в виде рецензии или комментариев, а также обеспечить индивидуальный подход к обучающимся с учетом их психофизиологических особенностей. Интерактивные элементы с возможностью обратной связи имеют особое значение для заочной формы обучения, поскольку позволяют не только контролировать выполнение студентом заданий (контрольных работ), но и мотивировать его самоподготовку в межсессионный период.

Использование интерактивных элементов «Задание» и «Тест» также обеспечивает фиксацию хода образовательного процесса, результатов текущей и промежуточной успеваемости обучающихся по дисциплине.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

6.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Материалы для организации самостоятельной работы обучающихся по дисциплине «Информационная безопасность и защита информации» размещены в «Электронной образовательной среде» https://edu.kemgik.ru/course/view.php?id=4964) и включают:

Организационные ресурсы

- Тематический план дисциплины для студентов очной формы обучения
- Тематический план дисциплины для студентов заочной формы обучения

Учебно-практические ресурсы

- Описания лабораторных работ

Учебно-методические ресурсы

- Методические указания по выполнению учебных исследовательского проекта
- Методические указания по выполнению контрольной работы

Учебно-библиографические ресурсы

- Список рекомендуемой литературы

Фонд оценочных средств

- Контрольные вопросы по разделам дисциплины
- Вопросы к экзамену

6.2. Тематика проектного обучения

1. Разработать модель информационной безопасности областной архива.
2. Разработать модель информационной безопасности организации с электронным документооборотом.
3. Разработать модель информационной безопасности городского архива.
4. Разработать модель информационной безопасности администрации поселка N.

6.3. Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся (СРО) является обязательным видом учебной работы по дисциплине, выполняется в соответствии с выданным преподавателем заданием и в установленные сроки.

Видами СРО по дисциплине являются: самостоятельное изучение теоретического материала, подготовка к тестированию, выполнение учебного исследовательского проекта, подготовка к экзамену.

Методические указания по выполнению отдельных видов СРО, а также требования к оформлению и представлению результатов размещены в соответствующих модулях электронного учебно-методического комплекса дисциплины «Информационная безопасность и защита информации», размещенного в «Электронной образовательной среде» (https://edu.kemgik.ru/course/view.php?id=4964)

Содержание самостоятельной работы обучающихся

Темы для самостоятельной работы обучающихся	**Количество часов**		**Виды зданий и содержание самостоятельной работы**
	Для очной формы обучения	**Для заочной формы обучения**	
Раздел 1. Информационная безопасность: общая характеристика			
Информационная безопасность: определение понятия, состав, назначение		8	Самостоятельное изучение теоретического материала
Информационная система как объект защиты		8	Самостоятельное изучение теоретического материала
Угрозы информационной безопасности в информационных системах		6	Самостоятельное изучение теоретического материала
Раздел 2. Направления защиты информации в документационном обеспечении управления и архивном деле			

Правовое обеспечение информационной безопасности	4	10	Самостоятельное изучение теоретического материала
Организационное обеспечение информационной безопасности	4	4	Самостоятельное изучение теоретического материала
Программно-техническое обеспечение информационной безопасности	4	10	Самостоятельное изучение теоретического материала; подготовка к подготовка к тестированию
Комплексная система защиты информации	6	14	Самостоятельное изучение теоретического материала; выполнение учебного исследовательского проекта
	16	60	Подготовка к экзамену
	экзамен - 36		

6. 4. Методические указания для обучающихся по освоению дисциплины

Освоение учебной дисциплины «Информационная безопасность и защита информации» предполагает, как изучение теоретического материала в ходе лекций и самостоятельной работы обучающихся, так и выполнение лабораторных работ и учебных исследовательских проектов.

В структуре дисциплины выделяется два взаимосвязанных раздела. В первом разделе рассматривается понятийный аппарат информационной безопасности, даны основные составляющие информационной безопасности. Характеризуются угрозы информационной безопасности и их источники, а также приводится классификация преступлений в данной сфере деятельности.

Второй раздел посвящен вопросам обеспечения информационной безопасности в документационном обеспечении управления и архивном деле. Рассмотрены такие виды обеспечения информационной безопасности как правовое, организационное и программно-техническое. При его изучении у студентов формируется представление о защите информации как комплексном мероприятии, что повышает их компетентность в решении будущих задач профессиональной деятельности на основе информационной культуры.

Целью выполнения лабораторных работ является формирование умений и владений, связанных с обеспечением информационной безопасностью и защитой информации информационных ресурсов. Практические работы выполняются на персональных компьютерах в лаборатории факультета информационных, библиотечных и музейных технологий. Для выполнения лабораторных работ используются интернет-ресурсы, а также фонд организационно-правовых и нормативных документов.

Описания лабораторных работ размещены в «Электронной образовательной среде КемГИК» (https://edu.kemgik.ru/course/view.php?id= 4964). Описание практической работы включает цель, задачи, обеспечивающие средства работы, требования к отчету, технологию выполнения работы, контрольные вопросы и список рекомендуемой литературы. Формой отчета являются файлы с результатами выполнения заданий, предусмотренных практическими работами и оформленных в соответствии с заданными в описании конкретной практической работы требованиями. После выполнения каждой практической работы студенты самостоятельно размещают файлы в папку «Отчеты о выполнении лабораторных работ». Результаты выполнения каждой практической работы оцениваются преподавателем в баллах.

Самостоятельная работа студента в ориентирована на изучение литературы, анализ электронных информационных ресурсов и выполнение учебных исследовательских проектов.

Приступая к самостоятельному изучению учебной дисциплины «Информационная безопасность и защита информации», необходимо после ознакомления с ее структурой и содержанием обратиться к методическим указаниям по работе с литературой, которые представлены в составе электронного учебно-методического комплекса по дисциплине, размещенного в «Электронной образовательной среде КемГИК». Методические указания ориентированы на работу с документами, входящими в список как основной, так и дополнительной литературы.

Целью выполнения учебных исследовательских проектов по дисциплине «Информационная безопасность и защита информации» является освоение технологий создания модели информационной безопасности в документационном обеспечении управления и архивном деле с учетом нормативно-правовых документов, специфики пользователей и задач организации. Проекты выполняются в рамках контрольных работ студентами очной и заочной форм обучения в межсессионный период и размещается в папке «Контрольная работа» (по соответствующим разделам) в «Электронной образовательной среде КемГИК» (http://edu.kemguki.ru/course/view.php?id=4964). Подготовленный проект подлежит публичной защите, время которой назначается для студентов очной формы – перед экзаменационной сессией, для студентов заочной формы – в период сессии. Публичная защита проекта позволяет выявить достоинства и недостатки проектов. Представление и защита проекта является обязательным условием допуска студента к экзамену.

С целью обеспечения самоконтроля знаний по дисциплине для обучающегося предлагаются контрольные вопросы по разделам дисциплины.

Для обеспечения текущего контроля знаний по каждому разделу предусмотрено тестирование, которое осуществляется на платформе «Электронной образовательной среды КемГИК». Преподавателем устанавливается время прохождения каждого теста (после изучения конкретного раздела дисциплины).

7. Фонд оценочных средств

7.1 Оценочные средства для текущего контроля успеваемости

Текущий контроль успеваемости осуществляется в форме оценки результатов выполнения каждого практического задания, выполнения самостоятельной работы обучающихся, предусмотренных учебной программой курса.

7.1.1 Критерии оценки лабораторных работ

В ходе освоения учебной дисциплины предусмотрено 12 лабораторных работ (32 часа). Описания лабораторных работ представлены в электронном учебно-методическом комплексе дисциплины, размещенном на сайте «Электронная образовательная среда КемГИК»).

Критерии оценивания:

- выполнены все задания в практической работе, студент обнаруживает полное понимание материала, соблюдает требования к представлению результатов выполнения заданий практической работы - ***5 баллов***;
- выполнены все задания в практической работе, студент соблюдает требования к представлению результатов выполнения заданий практической работы, однако допускает единичные ошибки, неточности - ***4 балла***;
- выполнена большая часть заданий в практической работе, студент знает и понимает основные положения данной темы, но допускает единичные ошибки; студент в целом соблюдает требования к представлению результатов выполнения заданий практической работы, но допускает единичные неточности- ***3 балла***;
- выполнено меньше половины заданий практической работы, некоторые задания выполнены не в полном объеме или допущены единичные ошибки, неточности, студент нарушает некоторые требования к представлению результатов выполнения заданий практической работы - ***2 балла***;

- выполнено меньше половины заданий практической работы, задания выполнены не в полном объеме или допущены ошибки, неточности, студент нарушает требования к представлению результатов выполнения заданий практической работы- ***1 балл***;
- практическая работа не выполнена - ***0 баллов***.

7.1.2 Критерии оценки проекта и его защиты

Тема проекта выбирается из списка, рекомендованного преподавателем; также возможен вариант самостоятельного выбора студентом темы, при условии обязательного согласования с преподавателем.

Защита проекта – публичное выступление, представляющее собой развернутое изложение исследованной проблемы. Продолжительность выступления – до 10 мин.

Выполняемые студентами проекты оцениваются по каждому из представленных критериев:

Тема проекта выбирается из списка, рекомендованного преподавателем; также возможен вариант самостоятельного выбора студентом темы, при условии обязательного согласования с преподавателем.

Выполняемые студентами проекты оцениваются по каждому из представленных критериев:

Наименование критерия	Максимальное количество баллов
Критерии оценки проекта	
Соответствие содержания проекта заданной теме	2
Обоснованность результатов представленной работы	2
Грамотное использование цветового и шрифтового оформления	2
Качество представления графического материала, звуковой и видеоинформации	2
Гармоничность сочетания различных форм представления информации	2
Четкость и логичность выводов	2
Качество оформления отчета о выполненном проекте и презентации (отсутствие орфографических и синтаксических ошибок)	2
Критерии оценки выступлений	
Грамотность и логичность изложения материала	2
Глубина владения материалом	2
Аргументированность ответов на вопросы	2
	20

Каждый из критериев оценивается от 0 до 2 баллов, 1 – критерий выполнен частично, 2 – критерий выполнен в полном объеме. Таким образом, максимальное количество баллов за выполнение и защиту проекта составляет 20 баллов.

7.2. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.2.1 Вопросы к экзамену

1. Информационная безопасность: понятие, назначение
2. Состав концептуальной модели информационной безопасности
3. Доступность, целостность и конфиденциальность информации
4. Проблемы защиты информационных систем
5. Характеристики информационных систем, влияющие на безопасность информации
6. Классификация и характеристика угроз информационной безопасности

7. Причины и источники случайных воздействий на информационные системы
8. Причины и источники преднамеренных воздействий на информационные системы
9. Классификация преступлений в сфере информационной безопасности
10. Основные положения государственной политики обеспечения информационной безопасности РФ
11. Государственная тайна: понятие, средства защиты государственной тайны
12. Конфиденциальная информация: понятие, средства защиты конфиденциальной информации
13. Персональные данные: понятие, средства защиты персональных данных
14. Цели, задачи, содержание административного уровня обеспечения информационной безопасности.
15. Цели, задачи, содержание процедурного уровня обеспечения информационной безопасности.
16. Политика безопасности: определение, направления разработки
17. Классификация средств технической защиты информации.
18. Классификация средств программной защиты информации.
19. Компьютерные вирусы: классификация, деструктивные возможности
20. Виды антивирусных программ. Факторы, определяющие качество антивирусных программ
21. Правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
22. Идентификация и аутентификация пользователей

7.2.3 Методика и критерии оценки результатов обучения по дисциплине

Критерии оценивания

Общие правила оценки успеваемости студента в течение семестра

Виды работ	*Количество баллов*
Выполнение и защита лабораторных работ	Максимум 5 × 12= 60 баллов
Выполнение и защита проекта	Максимум – 20 баллов
Тестирование	Максимум 20 балла
Итого за семестр:	Максимум – 100 баллов

Знания, умения и навыки обучающихся при промежуточной аттестации **в форме экзамена** определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Положительная оценка выставляется, если обучающийся достиг **уровней формирования компетенций: продвинутый, повышенный, пороговый.**

Шкала перевода баллов в оценки при промежуточной аттестации в форме экзамена

Уровень формирования компетенции	**Оценка**	**Минимальное количество баллов**	**Максимальное количество баллов**
Продвинутый	Отлично	90	100
Повышенный	Хорошо	75	89
Пороговый	Удовлетворительно	60	74
Нулевой	Неудовлетворительно	0	59

«Отлично» **выставляется, если обучающийся достиг продвинутого уровня формирования компетенций;** обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок. Оценка «отлично» выставляется без собеседования, если ***этом выполняются следующие критерии:***

- ***количество баллов за выполнение всех*** лабораторных работ составляет ***не менее 54;***
- количество баллов за тест составляет не менее 18
- количество баллов за проект составляет не менее 18.

«Хорошо» **выставляется, если обучающийся достиг повышенного уровня формирования компетенций;** обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий. ***Оценка «хорошо» выставляется студенту в ходе собеседования при выполнении следующих критериев:***

- обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий;
- количество баллов за выполнение всех лабораторных работ составляет не менее 44;
- количество баллов за проект составляет не менее 16;
- количество баллов за тест составляет не менее 15.

«Удовлетворительно» **выставляется, если обучающийся достиг порогового уровня формирования компетенций;** обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий. ***Оценка «удовлетворительно» выставляется студенту в ходе собеседования при выполнении следующих критериев:***

- обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий;
- количество баллов за выполнение всех лабораторных работ составляет не менее 34;
- количество баллов за проект составляет не менее 14;
- количество баллов за тест составляет не менее 12.

«Неудовлетворительно» **соответствует нулевому уровню формирования компетенций;** обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи. ***Оценка «*неудовлетворительно*» выставляется студенту в ходе собеседования при выполнении следующих критериев:***

– обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи;

- количество баллов за проект составляет менее 14;
- количество баллов за выполнение лабораторных работ составляет менее 34;
- количество баллов за тест составляет менее 12.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1.Основная литература

Учебные издания

1. Исаев, Г.Н. Проектирование информационных систем: учеб. пособие / Г. Н. Исаев. – Москва: Изд-во «Омега-Л», 2013. – 424 с. – Текст: непосредственный.
2. Шишов, О. В. Современные технологии и технические средства информатизации:

учебник / О. В. Шишов. - Москва: ИНФРА-М, 2017. - 462 с. – Текст: непосредственный.

Нормативные документы

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Москва: Стандартинформ, 2008. – 8 с. – Текст: непосредственный.
4. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Москва: Стандартинформ, 2009. – 20 с. – Текст: непосредственный.
5. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Москва: Стандартинформ, 2008. – 20 с. – Текст: непосредственный.
6. Об утверждении «Доктрины информационной безопасности Российской Федерации»: указ Президента РФ от 05.12.2016 N 646 // Консультатнт Плюс: справочная правовая система. – Загл. с экрана. – URL: http://www.consultant.ru/document/ cons_doc_LAW_208191. – Текст: электронный.
7. Российская Федерация. Законы. О государственной тайне: федер. закон : [утв. 21.07.1993 г. N 5485-1 (ред. от 26.07.2017)] // Консультант Плюс: справочная правовая система. – Загл. с экрана. – URL: http://www.consultant.ru/document/cons_doc_LAW_2481/ – Текст: электронный.
8. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: федер. закон : [утв. 27.07.2006 г. N 149-ФЗ] // Консультант Плюс: справочная правовая система. – Загл. с экрана. – URL: http://www.consultant.ru/document/ cons_doc_LAW_61798. – Текст: электронный.
9. Российская Федерация. Законы. О персональных данных: федер. закон : [утв. 27.07.2006 N 152-ФЗ] // Консультант Плюс: справочная правовая система. – Загл. с экрана. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801. – Текст: электронный.

8.2. Дополнительная литература

1. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. – Москва-Берлин : Директ-Медиа, 2015. - 105 с. // Университетская библиотека online: электрон. библ. система. – Загл. с экрана. – URL: http://biblioclub.kemguki.ru/index.php?page=book&id=362895 – Текст: электронный.
2. Колкова, Н.И. Технологии создания электронных информационных ресурсов: учеб. пособие/ Н.И. Колкова, И.Л. Скипор. – Москва: Литера, 2013.– 360 с. – Текст: непосредственный.
3. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С.А. Нестеров. - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с. // Университетская библиотека online: электрон. библ. система. – Загл. с экрана. – URL: http://biblioclub.kemguki.ru/index.php?page=book&id=363040 – Текст: электронный.

8.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

- Правовой портал в сфере культуры: информационно-справочная база нормативных документов по культуре/ Министерство культуры Российской Федерации. – URL: http://pravo.roskultura.ru. – Текст: электронный.
- Лига безопасного интернета. – URL: http://www.ligainternet.ru/.. – Текст: электронный.
- Федеральное агентство по техническому регулированию и метрологии (Росстандарт). – URL: http://www.gost.ru. – Текст: электронный.
- Сервер отраслевой статистики Минкультуры России: официальный сайт/ Федеральное государственное бюджетное учреждение «Главный информационно-

вычислительный центр Министерства культуры Российской Федерации» (ГИВЦ Минкультуры России). – URL: http://mkstat.ru. – Текст: электронный.

- Консультант Плюс: справочная правовая система. - URL: http://www.consultant.ru.– Текст: электронный.

8.4. Программное обеспечение и информационные справочные системы

Для реализации образовательного процесса необходимо следующее программное обеспечение:

- операционная система Windows;
- любой интернет-браузер (Google Chrome, Internet Explorer, Opera, Mozilla Firefox, др.);
- программа виртуализации для операционных сред Oracle VM VirtualBox;
- справочные правовые системы.

8.5. Материально-техническое обеспечение дисциплины

Наличие учебной лаборатории, оснащенной проекционной и компьютерной техникой, интегрированной в Интернет.

9. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья применяется индивидуальный подход к освоению дисциплины, индивидуальные задания с учетом особенностей их психофизического развития и состояния здоровья.

При составлении индивидуального графика обучения предусмотрены различные варианты проведения занятий: в образовательной организации (в академической группе и индивидуально), на дому с использованием дистанционных образовательных технологий.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся создаются фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. С учетом индивидуальных психофизиологических особенностей обучающихся устанавливаются следующие адаптированные формы проведения текущего контроля успеваемости и промежуточной аттестации: для лиц с нарушением зрения задания предлагаются с укрупненным шрифтом, для лиц с нарушением слуха – оценочные средства предоставляются в письменной форме с возможностью замены устного ответа на письменный, для лиц с нарушением опорно-двигательного аппарата двигательные формы оценочных средств заменяются на письменные/устные с исключением двигательной активности. При необходимости студенту-инвалиду предоставляется дополнительное время для выполнения задания. При выполнении заданий для всех групп лиц с ограниченными возможностями здоровья допускается присутствие индивидуального помощника-сопровождающего для оказания технической помощи в оформлении результатов проверки сформированности компетенций. Форма проведения текущей и промежуточной аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Подбор и разработка учебных материалов осуществляется с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально. Обучающиеся инвалиды и лица с ограниченными возможностями здоровья обеспечены учебно-методическими ресурсами в формах, адаптированных к ограничениям их

здоровья. Учебно-методические ресурсы по дисциплине «Методы анализа предметных областей» размещены на сайте «Электронная образовательная среда КемГИК» (https://edu.kemgik.ru/course/view.php?id= 4964), которая имеет версию для слабовидящих.

10. Перечень ключевых слов

Авторизация
Анализ риска
Атака
Аудит информационной безопасности
Аутентификация
Доступность информации
Защита информации
Злоумышленник
Идентификация
Информационная безопасность
Источник угрозы
Компьютерное преступление
Концепция информационной безопасности
Конфиденциальность информации
Криптографическая защита информации
Модель угроз информационной безопасности
Мониторинг информационной безопасности
Нарушитель информационной безопасности
Несанкционированный доступ
Объект защиты информации
Организационное обеспечение защиты информации
Показатель эффективности защиты информации
Политика информационной безопасности
Правовое обеспечение защиты информации
Программное средство защиты информации
Программно-техническое средство защиты информации
Программно-техническое обеспечение защиты информации
Разграничение доступа
Техническое средство защиты информации
Угроза информационной безопасности
Уровень безопасности
Уязвимость
Физическая защита информации
Физическое средство защиты информации
Целостность информации
Цель защиты информации
Эффективность защиты информации

Содержание рабочей программы дисциплины (модуля)