

МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
Кемеровский государственный институт культуры
Факультет информационных, библиотечных и музейных технологий
Кафедра цифровых технологий и ресурсов

Рабочая программа дисциплины

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА
ИНФОРМАЦИИ**

Направление подготовки:

42.03.05 «Медиакоммуникации»

Профиль подготовки:

«Медиакоммуникации в коммерческой и социальной сферах»

Квалификация (степень) выпускника:

Бакалавр

Форма обучения:

Очная, заочная

Кемерово

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки 42.03.05 «Медиакоммуникации», профиль подготовки «Медиакоммуникации в коммерческой и социальной сферах», квалификация (степень) выпускника «бакалавр».

Утверждена на заседании кафедры цифровых технологий и ресурсов и рекомендована к размещению на сайте Кемеровского государственного института культуры «Электронная образовательная среда КемГИК» по web-адресу <http://edu2020.kemgiki.ru/> 23.05.2022 г., протокол № 10.

Переутверждена на заседании кафедры цифровых технологий и ресурсов и рекомендована к размещению на сайте Кемеровского государственного института культуры «Электронная образовательная среда КемГИК» по web-адресу <https://edu2020.kemgik.ru/> 23.05.2023 г., протокол № 10.

Переутверждена на заседании кафедры цифровых технологий и ресурсов и рекомендована к размещению на сайте Кемеровского государственного института культуры «Электронная образовательная среда КемГИК» по web-адресу <https://edu2020.kemgik.ru/> 23.05.2024 г., протокол № 11.

Мишова В. В. Информационная безопасность и защита информации: рабочая программа дисциплины для обучающихся по направлению подготовки 42.03.05 «Медиакоммуникации», профилю подготовки «Медиакоммуникации в коммерческой и социальной сферах», квалификация (степень) выпускника «бакалавр» / В.В. Мишова. – Кемерово: Кемеров. гос. ин-т культуры, 2022. – 15 с. – Текст: непосредственный.

1. Цели освоения дисциплины

формирование компетенций выпускника в области обеспечения информационной безопасности и защиты информации в профессиональной деятельности.

2. Место дисциплины в структуре, соответствующей ОПОП бакалавриата

Дисциплина «Информационная безопасность и защита информации» входит в состав дисциплин по выбору вариативной части блока дисциплин образовательной программы по направлению подготовки 42.03.05 «Медиакоммуникации», профиля «Медиакоммуникации в коммерческой и социальной сферах», квалификация (степень) «бакалавр». Дисциплина изучается в 6 семестре на очной форме обучения и в 5 и 6 семестрах на заочной форме обучения. Для освоения дисциплины «Информационная безопасность и защита информации» необходимы знания, умения и компетенции, сформированные в результате изучения студентами такой дисциплины профессиональной подготовки, как «Информационные технологии». Компетенции, сформированные при освоении дисциплины «Информационная безопасность и защита информации», также необходимы при прохождении учебной и производственных практик в процессе обучения.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Изучение дисциплины направлено на формирование следующей компетенции и индикаторов их достижения:

Код и наименование компетенции	Индикаторы достижения компетенций		
	знать	уметь	владеть
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	<ul style="list-style-type: none">• компоненты концептуальной модели информационной безопасности• задачи и функции защиты электронных информационных ресурсов• характеристики информационных систем, влияющие на безопасность информации классификацию и характеристику угроз информационной безопасности.• классификацию преступлений в сфере информационной безопасности• нормативно-правовые документы в	<ul style="list-style-type: none">• выявлять угрозы информационной безопасности• применять на практике нормативно-правовые документы в области защиты информации• принимать решения в организации информационной безопасности• обосновывать и осуществлять выбор средств защиты информации использовать современные методы и средства в комплексной системе защиты информации выполнять оценку эффективности	<ul style="list-style-type: none">• терминологией в сфере информационной безопасности• способами предотвращения случайных и преднамеренных угроз информационной безопасности• готовность к разработке политики информационной безопасности• навыками работы с программно-техническими средствами обеспечения информационной безопасности• способностью формулировать требования к системе защиты информации

	области защиты информации состав организационных документов обеспечения информационной безопасности • классификацию средств программно-технической защиты информации требования к комплексной системе защиты информации этапы построения системы защиты информации	защиты информации	
--	---	-------------------	--

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника

Профессиональные стандарты	Обобщенные трудовые функции	Трудовые функции
06.009 Профессиональный стандарт «Специалист по продвижению и распространению продукции средств массовой информации»	Управление информационными ресурсами	Управление информацией из различных источников
06.009 Профессиональный стандарт «Специалист по продвижению и распространению продукции средств массовой информации»	Техническая обработка и размещение информационных ресурсов на сайте	Размещение информации на сайте Ведение информационных баз данных

4. Объем, структура и содержание дисциплины

4.1 Объем дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 академических часа.

Для студентов очной формы обучения предусмотрено 46 часов контактной (аудиторной) работы с обучающимися (16 часов лекций, 30 часов практических занятий) и 26 часов самостоятельной работы. 9 часов (30 %) контактной работы проводится в интерактивных формах.

Для студентов заочной формы обучения предусмотрено 14 часов контактной (аудиторной) работы с обучающимися (6 часа лекций, 8 часов практических занятий) и 58 часов самостоятельной работы. 2,5 часа (31%) контактной 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.

Промежуточная аттестация – зачет.

4.2. Структура дисциплины

4.2.1 Структура дисциплины очной формы обучения

№/ №	Разделы/темы дисциплины	Семестр	Виды учебной работы, и трудоемкость (в часах)			
			Лекции	Практ. занятия	Интеракт. формы обучения	СРО
Раздел 1. Информационная безопасность: общая характеристика						
1.1	Информационная безопасность: определение понятия, состав, назначение	6	2*	4	2* Лекция- дискуссия	2
1.2	Информационная система как объект защиты	6	2	4		2
1.3	Угрозы информационной безопасности в информационных системах	6	4/2*	4	2* Лекция- дискуссия	4
Раздел 2. Обеспечение информационной безопасности организации						
2.1	Правовое обеспечение информационной безопасности организации	6	2	6		4
2.2	Организационное обеспечение информационной безопасности организации	6	2	4		4
2.3	Программно- техническое обеспечение информационной безопасности организации	6	2	4/2*	4* Защита проекта	6
2.4	Комплексная система защиты информации в организации	6	2	4/2*		6
	Всего часов в интерактивной форме:				9*(30%)	
	Итого:		16	30	-	26

4.2.2 Структура дисциплины очной формы обучения

№/№	Разделы/темы дисциплины	Семестр	Виды учебной работы, и трудоемкость (в часах)			
			Лекции	Практ. занятия	Интеракт. формы обучения	СРО
Раздел 1. Информационная безопасность: общая характеристика						
1.1	Информационная безопасность: определение понятия, состав, назначение	5	2	-		34
1.2	Информационная система как объект защиты	6	1	2		4
1.3	Угрозы информационной безопасности в информационных системах	6	2	-		4
Раздел 2. Обеспечение информационной безопасности организации						
2.1	Правовое обеспечение информационной безопасности организации	6	2	2		4
2.2	Организационное обеспечение информационной безопасности организации	6	1	-		4
2.3	Программно-техническое обеспечение информационной безопасности организации	6		2/0,5*		4
2.4	Комплексная система защиты информации в организации	6		2/2*	2,5* Защита проекта	4
	Всего часов в интерактивной форме:				2,5*(31%)	
	Итого:		6	8	-	58

4.3 Содержание дисциплины

№ п/п	Содержание дисциплины (Разделы. Темы)	Результаты обучения	Виды оценочных средств; формы текущего контроля, промежуточной аттестации
Раздел 1. Информационная безопасность: общая характеристика			
1.1	Тема 1.1 Информационная безопасность: определение понятия, состав, назначение	Формируемые компетенции: УК-2. В результате изучения темы студент должен:	Отчет о выполнении практической работы

	<p>Понятие определения «информационная безопасность». Исторические аспекты возникновения и развития информационной безопасности.</p> <p>Концептуальная модель информационной безопасности. Основные составляющие информационной безопасности: доступность, целостность, конфиденциальность.</p>	<p>знать:</p> <ul style="list-style-type: none"> компоненты концептуальной модели информационной безопасности <p>владеть:</p> <ul style="list-style-type: none"> терминологией в сфере информационной безопасности. 	
1.2	<p>Тема 1.2 Информационная система как объект защиты</p> <p>Определение и состав информационной системы, принципы ее функционирования. Оценка качества информационной системы. Проблемы защиты информационных систем. Факторы, обуславливающие необходимость защиты информационных ресурсов информационных систем. Характеристики информационных систем, влияющие на безопасность информации.</p>	<p>Формируемые компетенции: УК-2.</p> <p>В результате изучения темы студент должен:</p> <p>знать:</p> <ul style="list-style-type: none"> задачи и функции защиты электронных информационных ресурсов; характеристики информационных систем, влияющие на безопасность информации; <p>владеть:</p> <ul style="list-style-type: none"> терминологией в сфере информационной безопасности. 	Отчет о выполнении практической работы
1.3	<p>Тема 1.3 Угрозы информационной безопасности в информационных системах</p> <p>Классификация и характеристика угроз информационной безопасности.</p> <p>Классификация и характеристика источников угроз информационной безопасности. Предпосылки появления угроз. Цели угроз информационной безопасности.</p> <p>Классификация преступлений в сфере информационной безопасности.</p>	<p>Формируемые компетенции: УК-2.</p> <p>В результате изучения темы студент должен:</p> <p>знать:</p> <ul style="list-style-type: none"> классификацию и характеристику угроз информационной безопасности; классификацию преступлений в сфере информационной безопасности; <p>уметь:</p> <ul style="list-style-type: none"> выявлять угрозы информационной безопасности; <p>владеть:</p> <ul style="list-style-type: none"> способами предотвращения случайных и 	Отчет о выполнении практической работы

		предумышленных угроз информационной безопасности; • терминологией в сфере информационной безопасности.	
Раздел 2. Обеспечение информационной безопасности организации			
2.1	Тема 2.1 Правовое обеспечение информационной безопасности организации 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 организации.	Формируемые компетенции: УК-2. В результате изучения темы студент должен: знать: • нормативно-правовые документы в области защиты информации; уметь: • применять на практике нормативно-правовые документы в области защиты информации; владеть: • терминологией в сфере информационной безопасности.	Отчет о выполнении практической работы
2.2	Тема 2.2 Организационное обеспечение информационной безопасности организации Состав политики и программы безопасности организации. Процедурные меры безопасности: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушение режима безопасности, планирование восстановительных работ. Особенности организационного обеспечения информационной безопасности в организации.	Формируемые компетенции: УК-2. В результате изучения темы студент должен: знать: • состав организационных документов обеспечения информационной безопасности; уметь: • принимать решения в организации информационной безопасности; владеть: • готовность к разработке политики информационной безопасности.	Отчет о выполнении практической работы
2.3	Тема 2.3 Программно-техническое обеспечение	Формируемые компетенции: УК-2.	Отчет о выполнении

	<p>информационной безопасности организации</p> <p>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.</p>	<p>В результате изучения темы студент должен:</p> <p>знать:</p> <ul style="list-style-type: none"> • классификацию средств программно-технической защиты информации; <p>уметь:</p> <ul style="list-style-type: none"> • обосновывать и осуществлять выбор средств защиты информации; <p>владеть:</p> <ul style="list-style-type: none"> • навыками работы программно-техническими обеспечения информационной безопасности, используемых в организации. 	<p>практической работы, тестовый контроль</p>
2.4	<p>Тема 2.4 Комплексная система защиты информации в организации</p> <p>Требования к комплексной системе защиты информации. Принципы создания комплексной системы защиты информации. Этапы построения комплексной системы защиты информации. Эффективность защиты информации.</p>	<p>Формируемые компетенции:</p> <p>УК-2.</p> <p>В результате изучения темы студент должен:</p> <p>знать:</p> <ul style="list-style-type: none"> • требования к комплексной системе защиты информации в организации; <p>уметь:</p> <ul style="list-style-type: none"> • использовать современные методы и средства в комплексной системе защиты информации; <p>владеть:</p> <ul style="list-style-type: none"> • способностью формулировать требования к системе защиты информации. 	<p>Защита проекта</p>

5. Образовательные и информационно-коммуникационные технологии

5.1 Образовательные технологии

В ходе обучения используются традиционные образовательные технологии, включающие аудиторные занятия в форме лекций и практических 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 практических занятиях предполагается использование интерактивной формы – защита проектов.

Доля аудиторных занятий, проводимых в интерактивных формах обучения, составляет 30% на очной форме обучения и 30,5% на заочной форме обучения, что соответствует требованиям ФГОС ВО по направлению подготовки 42.03.05 «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 практических работ, тестирование, защита учебного исследовательского проекта (на очной и заочной формах обучения), зачет.

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 практических работ, организацию самостоятельной работы студентов.

На сайте «Электронная образовательная среда КемГИК» (<https://edu2020.kemgik.ru/course/view.php?id=5294>) 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 практических 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://edu2020.kemgik.ru/course/view.php?id=5294>) и включают:

Организационные ресурсы

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

Учебно-практические ресурсы

- Описания практических работ

Учебно-методические ресурсы

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

Учебно-наглядные ресурсы

- Электронные презентации

Учебно-библиографические ресурсы

- Список рекомендуемой литературы

Фонд оценочных средств

- Контрольные вопросы по разделам дисциплины
- Вопросы к зачету

6.2. Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа является основой вузовского образования. Она формирует готовность к самообразованию, закладывает основы непрерывного образования и повышения квалификации, способствует формированию креативной, творческой личности будущего специалиста. Самостоятельная работа по дисциплине призвана обеспечить прочное и глубокое освоение курса, формированию и развитию языковых навыков медиасреды. Используются 2 вида самостоятельной работы студентов под контролем преподавателя: самостоятельная работа на лекциях и в процессе проведения практических занятий и самостоятельная работа вне учебных занятий (в том числе выполнение индивидуальных домашних заданий). Обучающиеся выполняют самостоятельную работу разных уровней: от репродуктивного, реконструктивного до творческого.

Самостоятельная работа по дисциплине связана с осуществлением таких целей, как:

- формирование способностей трансформировать, осуществлять перенос исторических знаний и применять их при анализе современных проблем;
- формирование и развитие умений самостоятельно работать с учебной литературой (овладение приемами схематизации и свертывания информации, заполнение таблиц, составление кластеров и т.д.), с профессиональными Интернет-ресурсами;
- развитие познавательных способностей обучающихся, их преобразующей деятельности;
- овладение профессиональной терминологией;
- освоение оценивающей деятельности (развитие способностей к самостоятельному анализу, объяснению и оцениванию исторических фактов и явлений и т.д.);
- формирование умений публичного выступления, участия в дискуссии и диспуте.

Под руководством преподавателя осуществляется подготовка к интерактивным формам учебных занятий (участие в ситуативных и деловых играх), подготовка к тестированию, экзамену, выполнение творческих исследовательских заданий.

6.3. Организация самостоятельной работы

Самостоятельная работа является обязательным видом учебной работы по дисциплине, выполняется в соответствии с выданным преподавателем заданием и в отведенные сроки.

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	2	34	Самостоятельное изучение теоретического материала
Информационная система как объект защиты	2	4	Самостоятельное изучение теоретического материала

Угрозы информационной безопасности в информационных системах	4	4	Самостоятельное изучение теоретического материала
Раздел 2. Обеспечение информационной безопасности организации			
Правовое обеспечение информационной безопасности организации	4	4	Самостоятельное изучение теоретического материала
Организационное обеспечение информационной безопасности организации	4	4	Самостоятельное изучение теоретического материала
Программно-техническое обеспечение информационной безопасности организации	6	4	Самостоятельное изучение теоретического материала; подготовка к подготовке к тестированию
Комплексная система защиты информации в организации	6	4	Самостоятельное изучение теоретического материала; выполнение учебного исследовательского проекта
	26	58	Подготовка к зачету

7. Фонд оценочных средств

Включает оценочные средства для текущего контроля успеваемости и для промежуточной аттестации по итогам освоения дисциплины. Структура и содержание фонда оценочных средств представлены в электронной образовательной среде (<https://edu2020.kemgik.ru/course/view.php?id=5294>).

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

Учебные издания

1. Информационное право : учебник для вузов с приложением информационно-правового словаря / под редакцией М. А. Федотова. - Москва : Юрайт, 2023. - 868 с. - Текст : непосредственный.
2. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. - . Москва : Юрайт, 2023. - 415 с. - Текст : непосредственный.

Нормативные документы

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Москва: Стандартинформ, 2008. – 20 с. – Текст: непосредственный.
4. Об утверждении «Доктрины информационной безопасности Российской Федерации»: указ Президента РФ от 05.12.2016 N 646 // КонсультантПлюс: справочная правовая система. – Загл. с экрана. – URL: http://www.consultant.ru/document/cons_doc_LAW_208191. – Текст: электронный.
5. Российская Федерация. Законы. О государственной тайне: федер. закон : [утв. 21.07.1993 г. N 5485-1 (ред. от 26.07.2017)] // КонсультантПлюс: справочная правовая система. – Загл. с экрана. – URL: http://www.consultant.ru/document/cons_doc_LAW_2481/ – Текст: электронный.

6. 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.
7. 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. библиотечная система. – Загл. с экрана. – URL: <http://biblioclub.kemguki.ru/index.php?page=book&id=362895> – Текст: электронный.
2. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С.А. Нестеров. – Санкт-Петербург: Издательство Политехнического университета, 2014. – 322 с. // Университетская библиотека online: электрон. библиотечная система. – Загл. с экрана. – URL: <http://biblioclub.kemguki.ru/index.php?page=book&id=363040> – Текст: электронный.
3. Шишов, О. В. Современные технологии и технические средства информатизации: учебник / О. В. Шишов. – Москва: ИНФРА-М, 2017. – 462 с. – Текст: непосредственный.

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.
- Российская библиотечная ассоциация (РБА): официальный сайт. – URL: <http://www.rba.ru>. – Текст: электронный.
- Информационно-справочный портал «Library.ru»/ Российская государственная библиотека для молодежи. – URL: <http://www.library.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

Вуз располагает необходимыми техническими средствами и программным обеспечением для проведения лекционных и практических занятий, текущего тестового контроля и промежуточной аттестации, для самостоятельной работы обучающихся.

Программное обеспечение

• лицензионное программное обеспечение:

- операционная система – MS Windows (10, 8,7, XP)
- офисный пакет – Microsoft Office (MS Word, MS Excel, MS Power Point, MS Access)
- антивирус - Kaspersky Endpoint Security для Windows

- графические редакторы - Adobe CS6 Master Collection, CorelDRAW Graphics Suite X6
- **свободно распространяемое программное обеспечение:**
- офисный пакет – LibreOffice;
- графические редакторы – 3DS Max Autodesk (для образовательных учреждений).
- **базы данных, информационно-справочные и поисковые системы:**
- Консультант Плюс.

9. Материально-техническое обеспечение дисциплины

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

10. 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 размещены на сайте «Электронная образовательная среда КемГИК» (<https://edu.kemgik.ru/course/view.php?id=5294>), которая имеет версию для слабовидящих.

11. 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

1. Цели освоения дисциплины	2
2. Место дисциплины в структуре, соответствующей ОПОП бакалавриата.....	2
3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.....	2
4. Объем, структура и содержание дисциплины	3
4.1 Объем дисциплины.....	3
4.2. Структура дисциплины	4
4.2.1 Структура дисциплины очной формы обучения	4
4.2.2 Структура дисциплины очной формы обучения	5
4.3 Содержание дисциплины	5
5. Образовательные и информационно-коммуникационные технологии	8
5.1 Образовательные технологии.....	8
5.2 Информационно-коммуникационные технологии.....	9
6. Учебно-методическое обеспечение самостоятельной работы обучающихся	9
6.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся.....	9
6.2. Методические указания для обучающихся по организации самостоятельной работы.....	10
6.3. Организация самостоятельной работы.....	10
7. Фонд оценочных средств	11
8. Учебно-методическое и информационное обеспечение дисциплины	11
8.1. Основная литература.....	11
8.2. Дополнительная литература	12
8.3. Ресурсы информационно-телекоммуникационной сети «Интернет»	12
8.4. Программное обеспечение и информационные справочные системы.....	12
9. Материально-техническое обеспечение дисциплины	13
10. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.	13
11. Перечень ключевых слов	13