Министерство культуры Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КРАСНОДАРСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ»
Факультет гуманитарного образования
Кафедра истории, культурологии и музееведения

УТВЕРЖДАЮ
зав. кафедрой
истории, культурологии и музееведения
_____ А.В. Кудинова
Пр. № 20, 09 июня 2025 г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.05 Информационная безопасность в музеях

Направление подготовки – **51.03.04 Музеология и охрана объектов культурного и природного наследия**

Профиль подготовки – Цифровые технологии в музейной индустрии

Квалификация выпускника – академический бакалавр

Форма обучения – **очная, заочная**

Краснодар
2025

Рабочая программа предназначена для преподавания дисциплины обязательной части Блока 1, формируемая участниками образовательных отношений обучающихся по очной и заочной форме обучения по направлению подготовки 51.03.04 Музеология и охрана объектов культурного и природного наследия, профиль - Цифровые технологии в музейной индустрии.

Рабочая программа учебной дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки51.03.04 Музеология и охрана объектов культурного и природного наследия, утвержденному приказом Министерства образования и науки Российской Федерации от 6 декабря 2017 г. N 1180 "Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 51.03.04 Музеология и охрана объектов культурного и природного наследия" (с изменениями и дополнениями). Редакция с изменениями от 26.11.2020 и 8.02.2021 г. и основной образовательной программой.

Рецензенты:

Кандидат культурологии, доцент,
старший научный сотрудник научно-
методического отдела ГБУК КК
«Краснодарский государственный
историко-археологический музей-
заповедник им. Е.Д. Фелицына» А.Г. Ерёменко

Доцент, кандидат исторических наук,
доцент кафедры истории, культурологии
и музееведения КГИК Н.Е. Берлизов

Составитель: Р.С. Лаво, доктор философских наук, профессор, профессор кафедры кафедры истории, культурологии и музееведения КГИК.

Рабочая программа учебной дисциплины рассмотрена и утверждена на заседании кафедры истории, культурологии и музееведения «09» июня 2025 г., протокол № 20.

Рабочая программа учебной дисциплины одобрена и рекомендована к использованию в учебном процессе Учебно-методическим советом ФГБОУ ВО «КГИК» «25» июня 2025 г., протокол № 11.

Содержание

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность в музеях» изучение системы информационной безопасности в практике музейной деятельности. Получение студентами знаний по основным направлениям информационной безопасности в музеях и приобретения навыков прикладного использования системы информационной безопасности в современном музее.

Задачи: системно рассмотреть проблемы обеспечения информационной безопасности в современных музеях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность музеях» относится к дисциплинам части Блока 1, формируемой участниками образовательных отношений. Ее изучение базируется на знаниях, полученных обучающимися в ходе освоения дисциплин: «Психология» и «Введение в информационные технологии».

Программа адаптирована для инвалидов и лиц с ограниченными возможностями здоровья.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки:

общепрофессиональной компетенции (ОПК):

Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-2)

В результате освоения дисциплины обучающиеся должны:

Знать:

- понятийный аппарат технологий информационной безопасности, используемых в музеях;
- знать принципы организации системы информационной безопасности в музеях,

Уметь:

- ориентироваться в требованиях государственных и ведомственных стандартов по информационной безопасности в профессиональной деятельности;
- применять в профессиональной деятельности программные средства, обеспечивающие информационную безопасность в профессиональной деятельности.

Владеть:

- знаниями и программным обеспечением по информационной безопасности в профессиональной деятельности;
- основами знаний по управлению и контролю информационной безопасности в профессиональной деятельности;

Приобрести опыт деятельности в сфере организации и использования средств и программного обеспечения информационной безопасности в профессиональной деятельности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 ч.).

По очной форме обучения

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	К	СР	
1.		2	1-18	32	32	27	53	1-18 недели опрос; задания для практического выполнения; дискуссии
				32	32	27	53	144 /4
	Вид итогового контроля							*зачет*

4.1.2 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 ч.).

По заочной форме обучения

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	К	СР	

1.		2	1-18	6	6	12	120	1-18 недели опрос; задания для практического выполнения; дискуссии
				6	6	12	120	144 /4
	Вид итогового контроля							*зачет*

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

По очной форме обучения

Наименование разделов и тем	**Содержание учебного материала (темы, перечень раскрываемых вопросов): лекции, практические занятия (семинары), индивидуальные занятия, самостоятельная работа обучающихся, курсовая работа**	**Объем часов**	**Формируемые компетен-ции (по теме)**
1	**2**	**3**	**4**
2 семестр			
Раздел 1. Общие вопросы информационный безопасности			
Тема 1.1. Международные стандарты информационного обмена.	Лекции: Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная	4/ 0,11	ПК-3
	Практические занятия (семинары): Вопросы: 1.Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. 2.Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. 3.Защита информации, тайна, средства защиты информации. 4.Международные стандарты информационного	4/0,11	

	обмена. 5.Показатели информации: важность, полнота, адекватность, релевантность, толерантность. 6.Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная		
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	6/0,16	
Тема 1.2. Угрозы информационной безопасности. Понятие угрозы. Понятие о видах вирусов.	Лекции: Основные понятия. Механизмы безопасности. Классы безопасности. Основные определения и критерии классификации угроз. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	4/0,11	ПК-3
	Практические занятия (семинары): Вопросы: 1.Основные понятия. 2.Механизмы безопасности. Классы безопасности. 3.Основные определения и критерии классификации угроз. 4. Понятие нарушителя информационной безопасности. 5. Хакеры. Виды хакеров. Примеры хакерских атак. 6. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	4/0,11	
	Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы Изучение Интернет-ресурсов Подготовка к семинарскому занятию	6/0,16	
Тема 1.3. Информационная безопасность в условиях функционирования в России глобальных сетей	Лекции:Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура	4/ 0,11	ПК-3

	государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.		
	Практические занятия (семинары): Вопросы: 1.Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. 2.Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 3.Доктрина информационной безопасности Российской Федерации. 4.Структура государственной системы информационной безопасности. 5.Структура законодательной базы по вопросам информационной безопасности. 6. 6.Лицензирование и сертификация в области защиты информации. 7.Место информационной безопасности экономических систем в национальной безопасности страны.	4/ 0,11	
	Самостоятельная работа: Изучение лекционного материала Изучение информации основной и дополнительной литературы Изучение Интернет-ресурсов Подготовка к семинарскому занятию	6/0,16	
Раздел 2. Защита информации			
Тема 1.4. Теория и модели информационной безопасности.	Лекции: Основные положения теории информационной безопасности. Анализ различных моделей безопасности для учреждений социально-культурной сферы. Модели безопасности для музеев различных типов. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности	4/ 0,11	ПК-3
	Практические занятия (семинары): Вопросы: Основные положения теории информационной безопасности. Анализ различных моделей безопасности для учреждений социально-культурной сферы. Модели безопасности для музеев различных типов. Модели безопасности для домашней информационной системы.	4/ 0,11	

	Применение методов информационной безопасности		
	Самостоятельная работа: Изучение лекционного материала Изучение информации основной и дополнительной литературы Изучение Интернет-ресурсов Подготовка к семинарскому занятию	6/0,16	
Тема 1.5. Основные технологии построения защищенных систем.	Лекции: Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.	4/ 0,11	ПК-3
	Практические занятия (семинары): Вопросы: 1. Основные технологии построения защищенных систем. 2. Физические устройства. Их виды и использование. 3. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. 4. Правовые особенности использования средств информационной защиты. 5. Использование защищенных компьютерных систем. 6. Аппаратные и программные средства для защиты компьютерных систем от несанкционированных действий. 7. 2. Средства операционной системы. Средства резервирования данных. Проверка 8. целостности. Способы и средства восстановления работоспособности.	4/0,11	
	Самостоятельная работа: Изучение лекционного материала Изучение информации основной и дополнительной литературы Изучение информации Интернет-ресурсов Подготовка к семинарским и практическим занятиям	6/016	
Тема 1.6. Конфиденциальность информации	Лекции:Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.Элементы	4/0,11	ПК-3

	процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.		
	Практические занятия (семинары): Вопросы: 1. Целостность, доступность и конфиденциальность информации. 2. Классификация информации по видам тайны и степеням конфиденциальности. 3. Понятия государственной тайны и конфиденциальной информации. 4. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. 5. Элементы процесса менеджмента информационной безопасности. 6. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности в музее.	4/ 0,11	
	Самостоятельная работа: Изучение информации в основной и дополнительной литературе Изучение Интернет-ресурсов Изучение программного обеспечения Подготовка к практическим занятиям	6/0,16	
Тема 1.7 Алгоритмы безопасности в компьютерных сетях	Лекции:Межсетевые экраны. Проектирование межсетевых экранов. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы. Риски информационной безопасности для музеев. Мониторинг рисков.	4/0,11	ПК-3
	Практические занятия (семинары): Вопросы: 1.Межсетевые экраны. 2. Проектирование межсетевых экранов. 3. Снифферы. 4.Эксплоиты. 5. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». 6. Протоколирование. Сетевые защищенные протоколы. 7. Риски информационной безопасности для музеев. Мониторинг рисков.	4/0,11	
	Самостоятельная работа: Изучение информации в основной и	3/0,08	

	дополнительной литературе Изучение Интернет-ресурсов Изучение программного обеспечения Подготовка к практическим занятиям		
Тема 1.8. Нормативно правовое регулирование защиты информации	Лекции:Организационная структура системы защиты информации.Законодательные акты в области защиты информации.Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.	4/0,11	ПК-3
	Практические занятия (семинары): Вопросы: 1.Организационная структура системы защиты информации. 2.Законодательные акты в области защиты информации. 3.Российские и международные стандарты, определяющие требования к защите информации. 4.Система сертификации РФ в области защиты информации. 5. Основные правила и документы системы сертификации РФ в области защиты информации.	4/0,11	
	Самостоятельная работа: Изучение информации в основной и дополнительной литературе Изучение Интернет-ресурсов Изучение программного обеспечения Подготовка к практическим занятиям	2/ 0,05	
	Итого	144/4	
	Форма итоговой аттестации	*Экзамен*	

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

По заочной форме обучения

Наименование разделов и тем	**Содержание учебного материала (темы, перечень раскрываемых вопросов): лекции, практические занятия (семинары), индивидуальные занятия, самостоятельная работа обучающихся, курсовая работа**	**Объем часов / з.е.**	**Формируемые компетен-ции (по теме)**

1	2	3	4
2 семестр			
Раздел 1. Общие вопросы информационный безопасности			
Тема 1.1. Международные стандарты информационного обмена.	Лекции: Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная	-	ПК-3
	Практические занятия (семинары): Вопросы: 1.Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. 2.Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. 3.Защита информации, тайна, средства защиты информации. 4.Международные стандарты информационного обмена. 5.Показатели информации: важность, полнота, адекватность, релевантность, толерантность. 6.Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная	-	
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Тема 1.2. Угрозы информационной безопасности. Понятие угрозы. Понятие о видах вирусов.	Лекции: Основные понятия. Механизмы безопасности. Классы безопасности. Основные определения и критерии классификации угроз. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	2	ПК-3

	Практические занятия (семинары): Вопросы: 1.Основные понятия. 2.Механизмы безопасности. Классы безопасности. 3.Основные определения и критерии классификации угроз. 4. Понятие нарушителя информационной безопасности. 5. Хакеры. Виды хакеров. Примеры хакерских атак. 6. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	-	
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Тема 1.3. Информационная безопасность в условиях функционирования в России глобальных сетей	Лекции:Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.	-	ПК-3
	Практические занятия (семинары): Вопросы: 1.Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. 2.Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 3.Доктрина информационной безопасности Российской Федерации. 4.Структура государственной системы информационной безопасности. 5.Структура законодательной базы по вопросам информационной безопасности. 6. 6.Лицензирование и сертификация в области	2	

	защиты информации. 7.Место информационной безопасности экономических систем в национальной безопасности страны.		
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Раздел 2. Защита информации			
Тема 1.4. Теория и модели информационной безопасности.	Лекции: Основные положения теории информационной безопасности. Анализ различных моделей безопасности для учреждений социально-культурной сферы. Модели безопасности для музеев различных типов. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности	2	ПК-3
	Практические занятия (семинары): Вопросы: Основные положения теории информационной безопасности. Анализ различных моделей безопасности для учреждений социально-культурной сферы. Модели безопасности для музеев различных типов. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности	-	
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Тема 1.5. Основные технологии построения защищенных систем.	Лекции: Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.	-	ПК-3
	Практические занятия (семинары): Вопросы: 9. Основные технологии построения защищенных систем. 10. Физические устройства. Их виды и использование.	2	

	11. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. 12. Правовые особенности использования средств информационной защиты. 13. Использование защищенных компьютерных систем. 14. Аппаратные и программные средства для защиты компьютерных систем от несанкционированных действий. 15. 2. Средства операционной системы. Средства резервирования данных. Проверка 16. целостности. Способы и средства восстановления работоспособности.		
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Тема 1.6. Конфиденциальность информации	Лекции:Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	2	ПК-3
	Практические занятия (семинары): Вопросы: 7. Целостность, доступность и конфиденциальность информации. 8. Классификация информации по видам тайны и степеням конфиденциальности. 9. Понятия государственной тайны и конфиденциальной информации. 10. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. 11. Элементы процесса менеджмента информационной безопасности. 12. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики	-	

	безопасности в музее.		
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Тема 1.7 Алгоритмы безопасности в компьютерных сетях	Лекции:Межсетевые экраны. Проектирование межсетевых экранов. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы. Риски информационной безопасности для музеев. Мониторинг рисков.	-	ПК-3
	Практические занятия (семинары): Вопросы: 1.Межсетевые экраны. 2. Проектирование межсетевых экранов. 3. Снифферы. 4.Эксплоиты. 5. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». 6. Протоколирование. Сетевые защищенные протоколы. 7. Риски информационной безопасности для музеев. Мониторинг рисков.	2	
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
Тема 1.8. Нормативно правовое регулирование защиты информации	Лекции:Организационная структура системы защиты информации.Законодательные акты в области защиты информации.Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты	-	ПК-3

	информации.		
	Практические занятия (семинары): Вопросы: 1.Организационная структура системы защиты информации. 2.Законодательные акты в области защиты информации. 3.Российские и международные стандарты, определяющие требования к защите информации. 4.Система сертификации РФ в области защиты информации. 5. Основные правила и документы системы сертификации РФ в области защиты информации.	-	
	Консультации Самостоятельная работа: Изучение лекционного материала Изучение основной и дополнительной литературы. Изучение Интернет-ресурсов	1,5 15	
	Итого	144	
	Форма итоговой аттестации	*Экзамен*	

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения дисциплины используются следующие образовательные технологии:

Лекционные занятия: проблемные и интерактивные лекции.

Практические занятия: тренинги, операционные игры, логико-методологическое проектирование.

Самостоятельная работа: обязательная самостоятельная работа студента по заданию преподавателя, выполняемая во внеаудиторное время, индивидуальная самостоятельная работа студента под руководством преподавателя;

Занятия лекционного типа на очном отделении составляют 36 часов, что равняется 33% аудиторных занятий.

Объем учебных занятий, проводимых в интерактивных формах, составляет 36 часов, что равняется 50% аудиторных занятий.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6.1. Контроль освоения дисциплины

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

Текущий контроль успеваемости студентов по дисциплине производится в следующих формах:

- устный опрос
- письменные задания (рефераты);

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

- устные ответы,
- письменные работы,
- практические работы,
- оценка выполнения самостоятельной работы студентов:
- работа с первоисточниками,
- реферативная.

Промежуточный контроль по результатам семестров по дисциплине проходит в форме зачёта и экзамена.

6.2. Оценочные средства

6.2.1. Примерные тестовые задания (ситуации) – не предусмотрены

6.2.2. Вопросы для проведения текущего контроля

1.Угрозы информационной безопасности музею и средства борьбы с ними
2 Современные средства защиты информации
3 Современные системы компьютерной безопасности
4 Современные средства противодействия угрозам информационной безопасности
5 Классификация хакерских атак
6 Классификация средств антивирусной защиты
7 Правовые основы защиты информации
8 Технические аспекты обеспечения защиты информации. Современное состояние
9 Атаки на систему безопасности и современные методы защиты
10 Современные пути решения проблемы информационной безопасности РФ

6.2.3.Тематика эссе, рефератов, презентаций

6.2.4 Вопросы к зачету по дисциплине - зачет по дисциплине учебным планом не предусмотрен.

6.2.5. Вопросы к экзамену по дисциплине

1. Информационная безопасность: понятие и функции
2. Система информационной безопасности в музейной деятельности.
3. Национальные интересы РФ в сфере информационной безопасности.
4. Общие принципы обеспечения защиты информации в музейной сфере.
5. Виды угроз информационной безопасности в музее.
6. Источники наиболее распространенных угроз информационной безопасности в музейной сфере.
7. Виды сетевых атак.
8. Сниффинг и методы борьбы с ним.
9. Противодействие кибер-атакам на уровне приложений.
10. Проблемы обеспечения безопасности локальных сетей.
11. Распределенное хранение файлов.
12. Состав требований по обеспечению комплексной системы информационной безопасности
13. Уровни информационной защиты и их основные составляющие.
14. Принципы защиты информации от несанкционированного доступа.
15. Достоинства и недостатки программно-аппаратных средств защиты информации?
16. Виды механизмов защиты, которые могут быть реализованы для обеспечения идентификации и аутентификации пользователей
17. Задачи выполняемые подсистемой управления доступом.
18. Виды механизмов защиты, которые могут быть реализованы для обеспечения конфиденциальности данных и сообщений.
19. Задачи контроля участников взаимодействия.
20. Информационно-опасные сигналы и их основные параметры
21. Виды вирусных программ.
22. Атака в отказе в обслуживании.
23. Паразитические вирусы.
24. Способы распространения вирусов.
25. Методы обнаружения вирусов.
26. Модели многоуровневой защиты.
27. Задачи, которые решает система компьютерной безопасности.
28. Методы защиты информации в локальной сети музея.
29. Какой порядок организации системы видеонаблюдения?
30. Планирование защиты информационных систем.
31. Последовательность этапов работы по обеспечению информационной безопасности музея.
32. Характеритсика мобильные программы.
33. Характеристка метода «песочниц».
34. Политикой информационной безопасности.

35. Политика информационной безопасности РФ?
36. Нормативные документы РФ, определяющие концепцию защиты информации.

6.2.6. Примерная тематика курсовых работ

Курсовые работы учебным планом не предусмотрены

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

7.1. Основная литература

1. Васильева П.О. Музей в цифровую эпоху^ Перезагрузка / П. Васильева С. Феоктисова А. Михайлова, Д. Качуровская. - Москва: Издательские решения, 2018.-190 с. // URL: https://docs.yandex.ru/docs/view?tm=1687869479&tld=r&lang=ru&name=ПЕРЕЗАГРУЗКА_2018.pdf&text=Васильева%20П.О.%20Музей%20в%20цифровую%20эпоху.%20Перезагрузка.%20%20М.%3А%20hsemedia%2С%202019/ - Текст: электронный.
2. Информационная культура музеолога: учебник для студентов направления подготовки «Музеология и охрана объектов культурного и природного наследия»; квалификация (степень): бакалавр. - Кемерово: Кемеровский государственный институт культуры (КемГИК), 2022. - 227 стр.Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=701064 (дата обращения: 25.06.2023). – ISBN 978-5-8154-0650-6. – Текст: электронный.
3. Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дан : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 – ISBN 978-5-238-02857-6. – Текст: электронный.
4. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва; Берлин: Директ-Медиа, 2020. - 270 с. - URL: https://fileskachat.com/view/98421_33aec897f6da058d3549d2d809114079.html /
5. Трайнев, В. А. Системный подход к обеспечению информационной безопасности предприятия (фирмы) / В. А. Трайнев; Международная академия наук информации, информационных процессов и технологий (МАН ИПТ). – 5-е изд. – Москва: Дашков и К°, 2022. – 332 с.: схем., ил., табл. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=698555.– ISBN 978-5-394-05035-0. – Текст : электронный.

7.2. Дополнительная.

1.Зенков, А. В. Информационная безопасность и защита информации : учебное

пособие для вузов / А. В. Зенков. - 2-е изд., перераб. и доп. - Москва: Издательство Юрайт, 2023. - 107 с. - ISBN 978-5-534-16388-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 /

2.Информационное и технологическое обеспечение профессиональной деятельности : учебник и практикум для вузов : для студентов, обучающихся по естественнонаучным направлениям / Д. В. Куприянов. - Москва: Юрайт, 2021. - 254, [1] с.: ил. - ISBN 978-5-534-02523-1 : 720.01. - Текст (визуальный) : непосредственный.

3. Нестеров С. А. Основы информационной безопасности: Учебное пособие. - 3 е изд., стер. - СПб.: Издательство «Лань», 2017. - 324 с. - ISBN 978-5-8114-2290-6 // URL:https://www.kolledge39.ru/files/ uchebniki/10.02.05/ ОП.01%20 Основы_информационной_безопасности.pdf/

4. Щетинская, Н.Б. Развитие коммуникативной компетенции студентов с ограниченными возможностями здоровья: Методические рекомендации для студентов. – Краснодар: КГИК, 2016. – 28 с.

7.3. Периодические издания

1. Мир музея
2. Мир экскурсий
3. Музей
4. Музеум
5. Экспомир

7.4. Интернет-ресурсы

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности: URL: http://cyberrus.com/

2.Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ: URL: http://bit.mephi.ru/

3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): URL:www.fstec.ru

4. Информационно-справочная система по документам в области технической защиты информации: URL: www.fstec.ru

5. Образовательные порталы по различным направлениям образования и тематике: URL: http://depobr.gov35.ru/

6. Справочно-правовая система «Консультант Плюс»: URL: www.consultant.ru

7. Справочно-правовая система «Гарант»: URL: www.garant.ru

8. Федеральный портал «Российское образование: URL: www.edu.ru

9.Федеральный правовой портал «Юридическая Россия»: URL http://www.law.edu.ru/

10. Российский биометрический портал: URL: www.biometrics.ru

11. Федеральный портал «Информационно- коммуникационные технологии в

образовании»: URL: htpp//: www.ict.edu.ru
12. Сайт Научной электронной библиотеки: URL: www.elibrary.ru
13. Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: URL: http://window.edu.ru/
14. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс]. - Режим доступа:URL: http://www.vlibrary.ru/
15. Комплексное решение информационной безопасности для музеев [Электронный ресурс]. – Режим доступа: URL: https://dokumen.tips/software/-58ecca9b1a28ab02208b46ad.html?page=1/

7.5. Методические указания и материалы по видам занятий

Методические рекомендации по организации самостоятельной работы студентов

В учебном процессе выделяютдва вида самостоятельной работы:

- аудиторная;
- внеаудиторная.

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

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

Видами заданий для внеаудиторной самостоятельной работы являются:

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

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

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

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

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

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

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

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

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

Методические указания к выполнению реферативной работы

Реферат - краткое письменное изложение материала по определенной теме, выполняется с целью привития студентам навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу.

Реферат - это самостоятельная учебно-исследовательская работа учащегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер.

Этапы работы над рефератом

1.Формулирование темы. Тема должна быть не только актуальной по своему значению, но оригинальной, интересной по содержанию.

Тема реферата выбирается по желанию студента из списка, предлагаемого преподавателем. Выбранная тема согласовывается с преподавателем. После выбора темы требуется подобрать, изучить необходимую для ее разработки информацию. Тема может быть сформулирована студентом самостоятельно.

2.Подбор и изучение основных источников по теме (как правило, не менее 8-10).

3.Составление библиографии.

4.Обработка и систематизация информации.

5.Разработка плана реферата.

6.Написание реферата.

7.Публичное выступление с результатами исследования.

На семинарском занятии, заседании предметного кружка, студенческой научно-практической конференции.)

Содержание работы должно отражать знание современного состояния проблемы, обоснование выбранной темы, использование известных результатов и фактов, полноту цитируемой литературы, ссылки на работы ученых, занимающихся данной проблемой; актуальность поставленной проблемы; материал, подтверждающий научное, либо практическое значение в настоящее время.

План реферата должен включать в себя: введение, основной текст и заключение.

Во введении аргументируется актуальность выбранной темы, указываются цели и задачи исследования. В нем же можно отразить методику исследования и структуру работы.

Основная часть работы предполагает освещение материала в соответствии с планом. Основной текст желательно разбивать на главы и параграфы.

В заключении излагаются основные выводы и рекомендации по теме исследования.

Критерии оценки реферата:

- знание и понимание проблемы;

- умение систематизировать и анализировать материал, четко и обоснованно формулировать выводы;

- «трудозатратность» (объем изученной литературы, добросовестное отношение к анализу проблемы);

- самостоятельность, способность к определению собственной позиции по проблеме и к практической адаптации материала, недопустимость прямого плагиата;

- выполнение необходимых формальностей (точность в цитировании и указании источника текстового фрагмента, аккуратность оформления).

Рекомендации к подготовке мультимедиа-презентаций и докладов

1. Доклад - это сообщение по заданной теме, с целью внести знания из дополнительной литературы, систематизировать материл, проиллюстрировать примерами, развивать навыки самостоятельной работы с научной литературой, познавательный интерес к научному познанию.

2. Тема доклада должна быть согласована с преподавателем и соответствовать теме занятия.

3. Материалы при его подготовке должны соответствовать научно-методическим требованиям ВУЗа и быть указаны в докладе.

4. Необходимо соблюдать регламент, оговоренный при получении задания.

5. Иллюстрации должны быть достаточными, но не чрезмерными.

6. Работа студента над докладом-презентацией включает отработку навыков ораторства и умения организовать и проводить обсуждение.

7. Студент в ходе работы по презентации доклада отрабатывает умение ориентироваться в материале и отвечать на дополнительные вопросы слушателей.

8. Студент в ходе работы по презентации доклада отрабатывает умение самостоятельно обобщить материал и сделать выводы в заключении.

9. Студент обязан подготовить и выступить с докладом в строго отведенное время преподавателем и в установленный срок.

Докладчики и содокладчики - основные действующие лица. Они во многом определяют содержание, стиль, активность данного занятия. В докладе необходимо: сообщать новую информацию, использовать технические средства, знать и хорошо ориентироваться в теме всей презентации (семинара), уметь дискутировать и быстро отвечать на вопросы, четко выполнять установленный регламент, иметь представление о композиционной структуре доклада.

Выступление состоит из трех частей: вступление, основная часть и заключение. Вступление помогает обеспечить успех выступления по любой тематике. Вступление должно содержать: название презентации (доклада), сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов, акцентирование оригинальности подхода

Основная часть,в которой выступающий должен глубоко раскрыть суть затронутой темы, обычно строится по принципу отчета. Задача основной части - представить достаточно данных для того, чтобы слушатели и заинтересовались темой и захотели ознакомиться с материалами. При этом логическая структура теоретического блока не должны даваться без наглядных пособий, аудиовизуальных и визуальных материалов.

Заключение- это ясное четкое обобщение и краткие выводы.

Методические указания для подготовки к семинарским занятиям

Семинарские занятия проводятся в форме дискуссии, на которых проходит обсуждение конкретных экономических ситуаций. Обсуждения направлены на освоение научных основ, эффективных методов и приемов решения конкретных

практических задач, на развитие способностей к творческому использованию получаемых знаний и навыков.

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

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

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

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

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

Студенту рекомендуется следующая схема подготовки к семинарскому занятию:

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

При подготовке к семинарским занятиям следует руководствоваться указаниями и рекомендациями преподавателя, использовать основную литературу из представленного им списка. Для наиболее глубокого освоения дисциплины рекомендуется изучать литературу, обозначенную как «дополнительная» в представленном списке.

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

Методические указания к анализу кейсов – практических ситуаций

Кейс(в переводе с англ. - случай) представляет собой проблемную ситуацию, предлагаемую студентам в качестве задачи для анализа и поиска решения.

Обычно кейс содержит схематическое словесное описание ситуации, статистические данные, а также мнения и суждения о ситуациях, которые трудно предсказать или измерить. Кейс, охватывает такие виды речевой деятельности как чтение, говорение и письмо.

Кейсы наглядно демонстрируют, как на практике применяется теоретический материал. Данный материал необходим для обсуждения предлагаемых тем, направленных на развитие навыков общения и повышения профессиональной компетенции.

Зачастую в кейсах нет ясного решения проблемы и достаточного количества информации.

Типы кейсов:

- *Структурированный (highlystructured) кейс,* в котором дается минимальное количество дополнительной информации.
- *Маленькие наброски (shortvignettes)* содержащие, как правило, 1-10 страниц текста.
- *Большие неструктурированные кейсы (longunstructuredcases)* объемом до 50 страниц.

Способы организации разбора кейса:

- ведет преподаватель;
- ведет студент;
- группы студентов представляют свои варианты решения;
- письменная домашняя работа.

Для успешного анализа кейсов следует придерживаться ряда принципов: используйте знания, полученные в процессе лекционного курса, внимательно читайте кейс для ознакомления с имеющейся информацией, не торопитесь с выводами, не смешивайте предположения с фактами.

Анализ кейса должен осуществляться в определенной последовательности:

1. Выделение проблемы.
2. Поиск фактов по данной проблеме.
3. Рассмотрение альтернативных решений.
4. Выбор обоснованного решения.

При проведении письменного анализа кейса помните, что основное требование, предъявляемое к нему, – краткость.

7.6 Программное обеспечение

Преподавание дисциплин обеспечивается следующими программными продуктами: операционные системы – AstraLinux; пакет прикладных программ Р7-Офис.

7.7 Условия реализации программы для обучающихся инвалидов и лиц с ограниченными возможностями здоровья

Специфика получаемой направленности (профиля) образовательной программы предполагает возможность обучения следующих категорий инвалидов и лиц с ограниченными возможностями здоровья:

- с ограничением двигательных функций;
- с нарушениями слуха.
- с нарушениями зрения

Организация образовательного процесса обеспечивает возможность беспрепятственного доступа обучающихся с ограниченными возможностями здоровья и (или) инвалидов в учебные аудитории и другие помещения, для этого имеются пандусы,поручни, лифты и расширенные дверные проемы.

В учебных аудиториях и лабораториях имеется возможность оборудовать места для студентов-инвалидов с различными видами нарушения здоровья, в том числе опорно-двигательного аппарата и слуха. Освещенность учебных мест устанавливается в соответствии с положениями СНиП 23-05-95 «Естественное и искусственное освещения». Все предметы, необходимые для учебного процесса, располагаются в зоне максимальной досягаемости вытянутых рук.

Помещения предусматривают учебные места для лиц с ограниченными возможностями здоровья и инвалидов, имеющих сердечно-сосудистые заболевания, они оборудованы солнцезащитными устройствами (жалюзи), в них имеется система климат-контроля.

По необходимости для инвалидов и лиц с ограниченными возможностями здоровья разрабатываются индивидуальные учебные планы и индивидуальные графики, обучающиеся обеспечиваются печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Преподавание дисциплины в вузе обеспечено наличием аудиторий (в том числе оборудованных проекционной техникой) для всех видов занятий.

Действуют компьютерные классы с лицензионным программным обеспечением. Имеются рабочие места с выходом в Интернет для самостоятельной работы.

Все компьютерные классы подключены к локальной сети вуза и имеют выход в интернет, в наличии стационарное мультимедийное оборудование (проектор+ экран) в аудиториях 276,282,116,239, возможно проведение занятий на базе музея вуза (тачпанель, экран, проектор).

Обучающиеся пользуются

- вузовской библиотекой с электронным читальным залом;
- учебниками и учебными пособиями;

- аудио и видео материалами.

Все помещения соответствуют требованиям санитарного и противопожарного надзора.

Приложение

Дополнения и изменения
к рабочей программе учебной дисциплины (модуля)
_____
на 20__-20__ уч. год

В рабочую программу учебной дисциплины вносятся следующие изменения:

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

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

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

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