

**Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
Московский государственный институт культуры**

**УТВЕРЖДЕНО:  
Председатель УМС  
Библиотечно-  
информационного  
Факультета  
Мазурицкий А.М.**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (модулю)**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

<b>Направление подготовки:</b>	46.03.02. Документоведение и архивоведение
<b>Профиль подготовки:</b>	Электронный архив
<b>Квалификация (степень) выпускника:</b>	Бакалавр
<b>Форма обучения</b>	<i>очная</i>

**1. Перечень компетенций, формируемых в процессе освоения дисциплины**

## Контролируемые компетенции

Таблица 1

№	Код (шифр) компетенции	Наименование (содержание) компетенции
1.	УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
2.	ПК-4	Готовность к формированию электронного архива

## 2. Планируемые результаты обучения (знает, умеет, владеет (имеет навык)) по дисциплине

Таблица 2

Коды компетенции	результаты освоения ОПОП Содержание компетенций	Индикатор достижения компетенции	Перечень планируемых результатов обучения по учебной дисциплине
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Понимает цели и задачи безопасности жизнедеятельности, основные понятия, классификацию опасных и вредных факторов среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности	Знать: основные понятия, классификацию опасных и вредных факторов среды обитания человека
			Уметь: применять правовые и организационные основы безопасности жизнедеятельности в профессиональной и повседневной деятельности
			Владеть: навыками обеспечения экологической безопасности
ПК-4	Готовность формированию электронного архива	ПК- 4.2. Осуществляет информационно-технологические процессы создания и эксплуатации электронного архива	Знать: нормативные правовые акты Российской Федерации в области информационных технологий и защиты информации, цифровой трансформации основы теории баз данных, основные национальные и международные форматы хранения, передачи и оперирования архивными документами подходы к проектированию систем хранения электронных документов

			технологический процесс ввода и обработки данных в системе электронного архива
			Уметь: осуществлять операции ввода и поиска в базах данных разрабатывать техническое задание по проектированию систем хранения электронных документов для организаций различных типов применять технологические регламенты в системе электронного архива
			Владеть: навыками работы с базами данных приемами изложения задач ДОУ и архивного дела для разработчиков систем архивного хранения электронных документов навыками ввода и обработки данных в системе электронного архива

### 3. Описание средств, показателей, критериев и шкал оценивания компетенций на различных этапах формирования компетенции

Таблица 3

№	Индикатор достижения компетенции	Раздел дисциплины (тема)	Средство оценивания	Показатели оценивания	Критерии оценивания Шкалы оценивания
УК-8					
1.	З-1. виды информационных технологий, применяемых в ДОУ; области создания алгоритмов решения конкретных прикладных задач. Программы информационной безопасности	Раздел 1 Раздел 2 Раздел 3	Семинар Устный опрос Доклад Реферат	Выступление с докладом Анализ выступлений Ответы на вопросы Выступление с сообщением и презентацией Защита Реферата	Количество, Корректность
2.	У-1. дать оценку выбранным информационным технологиям, оценить их плюсы и минусы; применять на практике полученные знания в области компьютерных технологий. навыками использования программных продуктов в ДОУ;	Раздел 1 Раздел 2 Раздел 3	Семинар Устный опрос Доклад Реферат	Выступление с докладом Анализ выступлений Ответы на вопросы Выступление с сообщением и презентацией Защита Реферата	Полнота Прочность Системность
3.	В-1. навыками применения программ информационной безопасности способностью решать конкретные прикладные задачи с использованием ИТ.	Раздел 1 Раздел 2 Раздел 3	Семинар Устный опрос Доклад Реферат	Выступление с докладом Анализ выступлений Ответы на вопросы Выступление с сообщением и презентацией Защита Реферата	Обоснование актуальности темы, правильность выделения цели и задач; Соответствие содержания теме; Глубина проработки материала;
			зачёт	Ответы на вопросы	Полнота Прочность Системность
ПК-4					

№	Индикатор достижения компетенции	Раздел дисциплины (тема)	Средство оценивания	Показатели оценивания	Критерии оценивания Шкалы оценивания
4.	З-1. нормативно-правовую и методическую базу, регламентирующую процессы информационной безопасности и защиты информации	Раздел 1 Раздел 2 Раздел 3	Семинар Устный опрос Доклад Реферат	Выступление с докладом Анализ выступлений Ответы на вопросы Выступление с сообщением и презентацией Защита Реферата	Количество, Корректность
5.	У-1. определять задачи профессиональной деятельности на основе информационной и библиографической культуры	Раздел 1 Раздел 2 Раздел 3	Семинар Устный опрос Доклад Реферат	Выступление с докладом Анализ выступлений Ответы на вопросы Выступление с сообщением и презентацией Защита Реферата	Полнота Прочность Системность
6.	В-1. навыками применения информационно-коммуникационных технологий в области безопасности и защиты информации	Раздел 1 Раздел 2 Раздел 3	Семинар Устный опрос Доклад Реферат	Выступление с докладом Анализ выступлений Ответы на вопросы Выступление с сообщением и презентацией Защита Реферата	Обоснование актуальности темы, правильность выделения цели и задач; Соответствие содержания теме; Глубина проработки материала;
			Зачёт	Ответы на вопросы	Полнота Прочность Системность

## **4.Оценочные средства**

### **4.1Текущая аттестация**

*Задания для устного опроса, докладов и тестирования*

#### **Раздел 1. Борьба с угрозами несанкционированного доступа к информации**

1. Классификация способов несанкционированного доступа.
2. Функции межсетевого экранирования.
3. Основные функции системы защиты программы от копирования.
4. Методы противодействия отладчикам.
5. Классификация вредоносных закладок.
6. Методы и средства защиты от вредоносных закладок.
7. Основные средства защиты информации ПК.
8. Идентификация и аутентификация.
9. Организация контроля целостности.
- 10.Классификация атак.
- 11.Методы атак.
- 12.Этапы реализации атак
- 13.Модели атак.
- 14.Результаты атак.

*Примерные темы докладов*

#### **Раздел 2. Борьба с вирусным заражением информации.**

1. Статистический анализ и экспертные системы.
2. Признаки атак.
3. Категории атакующих.
4. Метод «рукопожатие».
5. Определение компьютерного вируса.
6. Классификация вирусов.
7. Особенности алгоритма вируса.
8. Способы заражения программ.
9. Способы создания парольной комбинации.
10. Требования к паролю.
11. Служба Microsoft dot Net Passport (определение, характеристика).
12. Вредоносное ПО.
13. Функции вредоносного ПО.
14. Инструментарий хакера.
15. Программы-шпионы: пути попадания на ПК.
16. Алгоритм работы клавиатурных шпионов.
17. Цели шпионского ПО.

18. Виды антивирусных программ.
19. Классификация способов защиты информации.
20. Структура системы защиты информации.
21. Цель разработки критериев безопасности.
22. Общая структура требований «Оранжевой книги».

### *Примерные темы рефератов*

## **Раздел 3. Организационно-правовое обеспечение информационной безопасности**

1. Основные направления информационной безопасности.
2. Угрозы информационной безопасности.
3. Основные компоненты критериев безопасности ITESC.
4. Инструментарий информационной безопасности.
5. Направление проведения инвентаризации.
6. Средствам защиты информации.
7. Уровни защиты информации.
8. Информационная война.
9. Информационное оружие.
10. Межсетевые экраны – брандмауэры.
11. Модель распределенной атаки.
12. Программные закладки.
13. История вирусологии.
14. Программа – полифаг «Aidstest»
15. Сравнение программ-сканеров и программ-детекторов
16. Государственная информационная политика
17. Авторское право

## **4.2. Промежуточная аттестация**

### *Типовые вопросы к зачёту*

1. Принципы обеспечения информационной безопасности.
2. Основные задачи в сфере обеспечения инфор безопасности.
3. Основные направления информационной безопасности.
4. Угрозы информационной безопасности.
5. Основные компоненты критериев безопасности ITESC.
6. Инструментарий информационной безопасности.
7. Направление проведения инвентаризации.
8. Средствам защиты информации.
9. Уровни защиты информации.
10. Классификация способов несанкционированного доступа.
11. Функции межсетевого экранирования.
12. Основные функции системы защиты программы от копирования.

13. Методы противодействия отладчикам.
14. Классификация вредоносных закладок.
15. Методы и средства защиты от вредоносных закладок.
16. Основные средства защиты информации ПК.
17. Идентификация и аутентификация.
18. Организация контроля целостности.
19. Классификация атак.
20. Методы атак.
21. Этапы реализации атак
22. Модели атак.
23. Результаты атак.
24. Статистический анализ и экспертные системы.
25. Признаки атак.
26. Категории атакующих.
27. Метод «рукопожатие».
28. Определение компьютерного вируса.
29. Классификация вирусов.
30. Особенности алгоритма вируса.
31. Способы заражения программ.
32. Способы создания парольной комбинации.
33. Требования к паролю.
34. Служба Microsoft dot Net Passport (определение, характеристика).
35. Вредоносное ПО.
36. Функции вредоносного ПО.
37. Инструментарий хакера.
38. Программы-шпионы: пути попадания на ПК.
39. Алгоритм работы клавиатурных шпионов.
40. Цели шпионского ПО.
41. Виды антивирусных программ.
42. Классификация способов защиты информации.
43. Структура системы защиты информации.
44. Цель разработки критериев безопасности.
45. Общая структура требований «Оранжевой книги».
46. Классы критериев безопасности компьютерных систем «Оранжевой книги».
47. Функции критериев Европейских критериев безопасности информационных технологий.
48. Федеральные критерии безопасности информационных технологий.
49. Общие требования к системе защиты информации.
50. Требования к техническому обеспечению.
51. Требования к документированию.
52. Требования по применению способов, методов и средств защиты.
53. Характеристические особенности компьютерных преступлений.
54. Предупреждение компьютерных преступлений.



«отлично»	обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция автора, сформулированы выводы, тема раскрыта полностью, даны правильные ответы на дополнительные вопросы;
«хорошо»	имеют место отдельные недочёты в раскрытии темы. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; на дополнительные вопросы даны неполные ответы;
«удовлетворительно»	имеются существенные отступления от требований к докладу сообщения. Тема освещена лишь частично; допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы. В конце доклада отсутствует вывод.
«неудовлетворительно»	выставляется студенту, если тема не раскрыта.

Разработано в соответствии с требованиями ФГОС ВО по направлению 46.03.02 Документоведение и архивоведение»

Разработчик: доцент, кандидат технических наук Адамьянц Армен Ованесович