Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 42.03.01 Реклама и связи с общественностью

Наименование образовательной программы: Реклама и связи с общественностью в цифровой среде

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Защита данных и методы хранения информации в цифровой рекламе и связей с общественностью

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Матвеев М.В. Идентификатор: R6a1bc0e9-MatveevMV-ce509dc6	М.В. Матвеев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Кахальников М.В. Идентификатор: R7ecedcd1-KakhalnikovMV-51d2b6	М.В. Кахальников
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Курилов С.Н. Идентификатор: R2f2f52fe-KurilovSN-7d2d7cde	С.Н. Курилов

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. пк-1 Способен разрабатывать и выбирать оптимальную PR-стратегию и организовывать комплексные мероприятия в рамках ее реализации

ИД-2 Демонстрирует способности выбирать оптимальную PR-стратегию

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. КМ 2 (Индивидуальный проект)
2. КМ 3 (Индивидуальный проект)
3. КМ 4 (Домашнее задание)

Форма реализации: Письменная работа

1. КМ 1 (Контрольная работа)

БРС дисциплины

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 КМ 1 (Контрольная работа)
КМ-2 КМ 2 (Индивидуальный проект)
КМ-3 КМ 3 (Индивидуальный проект)
КМ-4 КМ 4 (Домашнее задание)

Вид промежуточной аттестации – Зачет с оценкой.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
Комплексный подход к обеспечению информационной безопасности в цифровой рекламе					
Комплексный подход к обеспечению информационной безопасности в цифровой рекламе и связей с общественностью		+			
Защита от несанкционированного доступа к информации в цифровой рекламе					
Защита от несанкционированного доступа к информации в цифровой рекламе и связей с общественностью			+		

Криптографические методы и средства защиты информации в цифровой рекламе				
Криптографические методы и средства защиты информации в цифровой рекламе и связей с общественностью			+	
Защита от вредоносных программ и несанкционированного копирования информационных ресурсов в цифровой рекламе				
Защита от вредоносных программ и несанкционированного копирования информационных ресурсов в цифровой рекламе и связей с общественностью				+
Вес КМ:	25	25	25	25

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
пк-1	ИД-2$_{пк-1}$ Демонстрирует способности выбирать оптимальную PR-стратегию	Знать: Общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения Методы разграничения полномочий пользователей и модели управления доступом к объектам компьютерных систем и сетей Уметь: Использовать методы и средства криптографической защиты информации Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации	КМ-1 КМ 1 (Контрольная работа) КМ-2 КМ 2 (Индивидуальный проект) КМ-3 КМ 3 (Индивидуальный проект) КМ-4 КМ 4 (Домашнее задание)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. КМ 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Выполнение письменной работы.

Краткое содержание задания:

1. 1. Разработка программы разграничения полномочий пользователей на основе паролей .
2. 2. Изучение и освоение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: Методы разграничения полномочий пользователей и модели управления доступом к объектам компьютерных систем и сетей	1.В чем основной недостаток дискреционного управления доступом к объектам компьютерных систем? 2.Что такое авторизация субъектов компьютерной системы? 3.Что означает термин "роль" в ролевом разграничении доступа?

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Лабораторная работа 1 выполнена в точном соответствии с заданием, лабораторная работа 2 выполнена полностью

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Лабораторная работа 1 выполнена в основном в соответствии с заданием, лабораторная работа 2 выполнена полностью

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Лабораторная работа 1 выполнена в основном в соответствии с заданием

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Не выполнена ни одна из лабораторных работ 1-2

КМ-2. КМ 2

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Индивидуальный проект
Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Выполнение письменной работы.

Краткое содержание задания:

1. 1. Изучение и освоение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.
2. 2. Разработка и программная реализация алгоритмов симметричной криптографии и криптографического хеширования.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: Общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения	1.В чем разница между шифрованием и криптографическим хешированием? 2.На каких способах шифрования основаны симметричные криптосистемы? 3.Что такое многофакторная аутентификация в компьютерных системах?

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 90% контрольных вопросов при защите лабораторной работы 2, лабораторная работа 3 выполнена в точном соответствии с заданием

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 70% контрольных вопросов при защите лабораторной работы 2, лабораторная работа 3 выполнена в основном в соответствии с заданием

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 50% контрольных вопросов при защите лабораторной работы 2 или лабораторная работа 3 выполнена в основном в соответствии с заданием

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Правильные ответы даны менее чем 50% контрольных вопросов при защите лабораторной работы 2, лабораторная работа 3 не выполнена

КМ-3. КМ 3

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Индивидуальный проект
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Выполнение письменной работы.

Краткое содержание задания:

1. 1. Использование криптографических средств операционных систем в прикладных программах.
2. 2. Изучение и освоение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации	1.Как обеспечить возможность восстановления зашифрованных файлов при использовании шифрующей файловой системы? 2.Как создать самоподписанный сертификат открытого ключа? 3.Как добавить электронную подпись к макросу в документе офисного приложения?

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Лабораторная работа 4 выполнена в точном соответствии с заданием, лабораторная работа 5 выполнена полностью

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Лабораторная работа 4 выполнена в основном в соответствии с заданием, лабораторная работа 5 выполнена полностью

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Лабораторная работа 4 выполнена в основном в соответствии с заданием

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Не выполнена ни одна из лабораторных работ 4-5

КМ-4. КМ 4

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Домашнее задание
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Выполнение письменной работы.

Краткое содержание задания:

1. 1. Изучение и освоение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ.
2. 2. Разработка средств защиты программного обеспечения от несанкционированного использования и копирования.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: Использовать методы и средства криптографической защиты информации	1.Как просмотреть свойства сертификата открытого ключа, используемого при получении электронной подписи под документом офисного приложения? 2.Как выбрать объекты сканирования при использовании антивирусного программного обеспечения? 3.Какие средства языка и системы программирования используются при сборе сведений, собираемых при установке программы, защищенной от несанкционированного копирования? 4.Как реализовать в программе дополнительные действия, необходимые для установки и запуска приложений, защищенных от несанкционированного копирования?

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 90% контрольных вопросов при защите лабораторной работы 5, лабораторная работа 6 выполнена в точном соответствии с заданием

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 70% контрольных вопросов при защите лабораторной работы 5, лабораторная работа 6 выполнена в основном в соответствии с заданием

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 50% контрольных вопросов при защите лабораторной работы 5 или лабораторная работа 6 выполнена в основном в соответствии с заданием

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Правильные ответы даны менее чем 50% контрольных вопросов при защите лабораторной работы 6, лабораторная работа 3 не выполнена

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

1. Проблема защиты информации и подходы к ее решению.
1. 2. Протокол Диффи-Хеллмана.
2. 3. Зашифровать перестановкой P=*безопасность данных* на ключе K=*ФамилияИО* (фамилия и инициалы студента, без пробелов).

Процедура проведения

1. При подготовке студенты письменно отвечают на вопросы экзаменационного билета.
2. Студенты устно отвечают на вопросы экзаменационного билета и дополнительные вопросы преподавателя.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-2$_{ПК-1}$ Демонстрирует способности выбирать оптимальную PR-стратегию

Вопросы, задания

1.Основные понятия защиты информации
2.Зашифровать и расшифровать M=3 по алгоритму RSA (выбор ключей начать с p=3, q=11)
3.Методы обнаружения и удаления вредоносных программ
4.Компьютерная стеганография и ее применение
5.Принципы построения и свойства асимметричных криптосистем
6.Применение и обзор современных симметричных криптосистем
7.Аудит событий безопасности в ОС Windows и Unix
8.Дискреционное, мандатное и ролевое разграничение доступа к объектам
9.Протокол Kerberos
10.Способы аутентификации пользователей
11.Способы нарушения защищенности информации и защиты от него в компьютерных системах
12.Зашифровать P=*безопасность данных* многоалфавитной подстановкой на ключе K=*d,d,m,m* (день и месяц рождения студента, 4 цифры, первую цифру 0, если она есть в дате, заменить на 8, вторую цифру 0 – на 9)

Материалы для проверки остаточных знаний

1.В чем заключается проверка электронной подписи?
Ответы:
В сличении ее с эталонной В сличении ее с закрытым ключом автора документа В проверке совпадения расшифрованной на открытом ключе автора подписи и хеш-значения документа В проверке совпадения расшифрованной на закрытом ключе автора подписи и хеш-значения документа В проверке хеш-кода документа
Верный ответ: В проверке совпадения расшифрованной на открытом ключе автора подписи и хеш-значения документа
2.Что такое удостоверяющий центр?

Ответы:

Орган, создающий секретные ключи пользователей Орган, осуществляющий резервное копирование криптографических ключей Орган, занимающийся проверкой электронной подписи под документами Орган, выдающий сертификаты открытых ключей пользователей

Верный ответ: Орган, выдающий сертификаты открытых ключей пользователей

3.Какая из криптосистем не относится к асимметричным?

Ответы:

RSA AES ElGamal Эллиптических кривых

Верный ответ: AES

4.Чему равно -7 {mod 5}?

Ответы:

7 -2 3 5

Верный ответ: 3

5.Какое требование не применяется при построении идеального шифра (по К.Шеннону)?

Ответы:

Длина ключа >= длины открытого текста Ключ выбирается совершенно случайно В ключе равномерно распределены нулевые и единичные биты Ключ не используется дважды

Верный ответ: В ключе равномерно распределены нулевые и единичные биты

6.В чем основной недостаток дискреционного управления доступом к объектам?

Ответы:

Снижение производительности системы Невозможность аудита попыток доступа Возможность утечки конфиденциальной информации при выполнении санкционированных действий Сложность администрирования

Верный ответ: Возможность утечки конфиденциальной информации при выполнении санкционированных действий

7.Что является основным критерием при выборе элемента аппаратного обеспечения для аутентификации пользователей?

Ответы:

Стоимость изготовления Сложность копирования Скорость считывания ключевой информации Объем памяти и наличие микропроцессора

Верный ответ: Сложность копирования

8.Какие методы и средства защиты информации являются обязательными в любой системе защиты?

Ответы:

Криптографические Программно-аппаратные Инженерно-технические Организационные

Верный ответ: Организационные

9.Что означает термин "аутентификация"?

Ответы:

Проверка регистрации в базе данных Подтверждение подлинности Ограничение прав Учет и регистрация событий

Верный ответ: Подтверждение подлинности

10.В чем разница между криптографией и стеганографией?

Ответы:

Это тождественные понятия Целью криптографии является скрытие конфиденциальной информации и самого ее наличия, а целью стеганографии - только скрытие информации Целью криптографии является скрытие содержания конфиденциальной информации, а целью стеганографии - скрытие факта ее наличия

Верный ответ: Целью криптографии является скрытие содержания конфиденциальной информации, а целью стеганографии - скрытие факта ее наличия

11.Какие виды антивирусных программ принципиально могут обнаруживать только уже известные вредоносные программы?

Ответы:

Эвристические анализаторы Инспекторы (ревизоры) Сканеры Мониторы (сторожа) Вакцины

Верный ответ: Сканеры

II. Описание шкалы оценивания

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Точные и в основном полные ответы на вопросы экзаменационного билета и дополнительные вопросы

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Точные и в основном полные ответы на вопросы экзаменационного билета и большинство дополнительных вопросов

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Точные и в основном полные ответы на большинство вопросов экзаменационного билета и дополнительных вопросов

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Неточные ответы или отсутствие ответа на большинство вопросов экзаменационного билета и дополнительных вопросов

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.