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

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Теоретические основы защиты информации от несанкционированного доступа

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Капгер И.В. Идентификатор: R5d33df1e-KapgerIV-059b09ee	И.В. Капгер

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

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. РПК-1 Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ) организации на основе современных положений СМИБ

ИД-2 Проводит анализ безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС» (Контрольная работа)
2. Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных систем» (Контрольная работа)
3. Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации» (Тестирование)
4. Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС» (Тестирование)

БРС дисциплины

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС» (Контрольная работа)

КМ-2 Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации» (Тестирование)

КМ-3 Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных систем» (Контрольная работа)

КМ-4 Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС» (Тестирование)

Вид промежуточной аттестации – Зачет.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15

Угрозы и способы несанкционированного доступа к информации				
Понятие, угрозы, способы и причины несанкционированного доступа к информации	+	+		+
Политики безопасности для компьютерных систем и способы их реализации				
Определение и содержание политики безопасности для компьютерных систем				+
Системы аутентификации пользователей компьютерных систем и методы их построения				
Элементы, проблемы создания и использования систем аутентификации			+	
Вес КМ:	20	20	20	40

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
РПК-1	ИД-2$_{РПК-1}$ Проводит анализ безопасности компьютерных систем	Знать: состав и методы оценки качества систем аутентификации пользователей компьютерных систем и сетей методы оценки стоимости и уязвимости информации в компьютерных системах и сетях угрозы и способы несанкционированного доступа к информации в компьютерных системах и сетях и методы защиты от него Уметь: использовать методы построения формальных моделей подсистем защиты информации автоматизированных систем обосновывать выбор	КМ-1 Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС» (Контрольная работа) КМ-2 Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации» (Тестирование) КМ-3 Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных систем» (Контрольная работа) КМ-4 Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС» (Тестирование)

		системы аутентификации пользователей компьютерных систем и сетей	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Письменное контрольное задание.

Краткое содержание задания:

Изучить Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.» Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

1. Определить, чем класс защищенности 1Г отличается от класса защищенности 1Д
2. Определить класс защищенности для следующей информационной системы «АС – автономная автоматизированная система на базе ноутбука, не имеющая подключений к локальной вычислительной сети (ЛВС) и к сетям общего информационного пользования, в том числе общей информационной сети «Интернет». АС используется для работы одного пользователя с конфиденциальной информацией и обслуживается назначенным системным администратором»

№ п/п	Наименование составной части ОТСС	Модель, Заводской номер
1	Ноутбук	Asus F3S, 7AN0AS234921

1. Составить проект акта классификации по предоставленному образцу
2. Разработать проект приказа о порядке доступа в информационную систему.
3. Произвести настойки средства защиты информации «Secret Net Studio» в соответствии с классом защищенности

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: состав и методы оценки качества систем аутентификации пользователей компьютерных систем и сетей	1.**Что понимается под системой биометрической аутентификации?**

Описание шкалы оценивания:

Оценка: «зачтено»
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: «не зачтено»
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-2. Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Письменный опрос с вариантами ответов.

Краткое содержание задания:
Ответить на 20 вопросов по теме “Политики безопасности для компьютерных систем и теоретические основы их реализации”

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы и способы несанкционированного доступа к информации в компьютерных системах и сетях и методы защиты от него	1.**Что не относится к процессам защиты?**

Описание шкалы оценивания:

Оценка: «зачтено»
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: «не зачтено»
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-3. Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных систем»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Письменное контрольное задание.

Краткое содержание задания:
1. Исследуйте учебную аудиторию, определите актуальные каналы утечки информации, при условии, что в аудитории будет обсуждаться конфиденциальная информация.
2. Изменятся ли каналы утечки информации, если в аудитории конфиденциальная информация будет обрабатываться на компьютерной техники.
3. Определите организационные меры защиты информации для рассматриваемого помещения.
4. Определите технические меры защиты, если помещение будет использоваться для переговоров или для размещения компьютерной техники.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: обосновывать выбор системы аутентификации пользователей компьютерных	1.**Что является основной функцией идентификации и аутентификации?**

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
систем и сетей	

Описание шкалы оценивания:

Оценка: «зачтено»
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: «не зачтено»
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-4. Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 40
Процедура проведения контрольного мероприятия: Письменный опрос с вариантами ответов.

Краткое содержание задания:
Ответить на 20 вопросов по теме «Элементы и шаблоны построения систем аутентификации пользователей АС».

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: методы оценки стоимости и уязвимости информации в компьютерных системах и сетях	1.**Что не относится к оценке уровня влияния информационных систем?**
Уметь: использовать методы построения формальных моделей подсистем защиты информации автоматизированных систем	1.**Что такое базовый секрет?**

Описание шкалы оценивания:

Оценка: «зачтено»
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: «не зачтено»
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Зачет

Процедура проведения

Зачет проводится в устной форме по билетам согласно программе зачета

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

1. Компетенция/Индикатор: ИД-2$_{РПК-1}$ Проводит анализ безопасности компьютерных систем

Вопросы, задания

1.1.Перечислите специальные каналы утечки информации
2.2. Перечислите способы нарушения защиты информации
3.3. Какие особенности у одноразовых паролей
4.4. Чем отличается симметрическая криптография от ассиметричной
5.5. Какие бывают способы аутентификации
6.6. Какие основные функции идентификации и аутентификации
7.7. Что такое межсетевые экраны
8.8. Какие недостатки у DLP систем
9.9. Какие преимущества DLP систем
10.10. Какие системы являются защищенные
11.11. Что нельзя отнести к особенностям проходных шифраторов

Материалы для проверки остаточных знаний

1.**1.Что не относится к процессам защиты?**

Ответы:

а. Отказ
б. Атака
в. Защита
г. Утрата

Верный ответ: г

2.**2. Какой способ аутентификации пользователя является наиболее безопасным?**

Ответы:

а. С помощью логина
б. С помощью пароля
в. С помощью логина и пароля

Верный ответ: в

3.3. Что такое **DLP система**

Верный ответ: Специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

II. Описание шкалы оценивания

Оценка: «зачтено»

Описание характеристики выполнения знания: Работа выполнена верно или с несущественными недостатками

Оценка: «не зачтено»
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу