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
Методы и средства контроля эффективности 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: Компьютерное задание

1. Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД (Тестирование)
2. Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования (Тестирование)
3. Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux (Тестирование)
4. Тест №2 «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД (Тестирование)

БРС дисциплины

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Критерии безопасности компьютерных систем США и Европы					
Классификация методов и механизмов обеспечения компьютерной безопасности		+	+		
Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)		+	+		
Модели и механизмы информационной безопасности					
Модели и теоремы безопасности на основе дискреционной политики				+	+

Модели и теоремы безопасности на основе мандатной политики			+	+
Модели безопасности на основе ролевой политики			+	+
Понятие и разновидности скрытых каналов утечки информации в компьютерных системах			+	+
Модели и механизмы обеспечения целостности данных в компьютерных системах			+	+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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: этапы и технологию проектирования и создания безопасных информационных систем инструментальные программные и аппа-ратные средства анализа защищенности информационных систем и сетей современные технологии построения безопасных информационных систем современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах Уметь: использовать современные программные средства защиты информации разрабатывать структуру	Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux (Тестирование) Тест №2 «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД (Тестирование) Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД (Тестирование) Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования (Тестирование)

		защищенной информационной системы использовать современные аппаратные средства анализа защиты информационных процессов в компьютерных системах работать с основными программными и аппаратными средствами анализа защиты информационных систем	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тестирование по теме: «Общие сведения в предметной области дисциплины».

Краткое содержание задания:
Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

Контрольные вопросы/задания:

Знать: современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах	1.Если информационная система, гарантирует доступ к информации только тем лицам, которые на это имеют право, то она обеспечивает… - управление доступом + конфиденциальность - аутентичность - целостность - доступность 2.Организация надежной и эффективной системы резервного копирования организуется для… - защита от сбоев в электропитании - защита от сбоев серверов, рабочих станций и локальных компьютеров + защита от сбоев устройств для хранения информации - защита от утечек информации электромагнитных излучений. 3.Какая из перечисленных атак на поток информации является пассивной: + перехват. - имитация. - модификация. - фальсификация. - прерывание.
Уметь: использовать современные аппаратные средства анализа защиты информационных процессов в компьютерных системах	1.Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем - защита от сбоев в электропитании + защита от сбоев серверов, рабочих станций и локальных компьютеров - защита от сбоев устройств для хранения информации - защита от утечек информации электромагнитных

	излучений 2.Экранирование, фильтрация, заземление, электромагнитное зашумление используются для… - защита от сбоев в электропитании - защита от сбоев серверов, рабочих станций и локальных компьютеров - защита от сбоев устройств для хранения информации + защита от утечек информации электромагнитных излучений 3.Технические каналы утечки информации делятся на… + Все перечисленное - Акустические и виброакустические - Электрические - Оптические

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Тест №2 «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тестирование по теме: «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)»

Краткое содержание задания:
Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

Контрольные вопросы/задания:

Знать: этапы и технологию проектирования и создания	1.Какой уровень возможности нарушителя определяется возможностью управления

безопасных информационных систем	функционированием АС, путем воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования? - 2 +3 - 4 - 6. 2.Каковы основные характеристики технических средств защиты от НСД? 1 - степень полноты и качество охвата ПРД реализованной СРД; 2 - состав и качество обеспечивающих средств для СРД; 3 - гарантии правильности функционирования СРД и обеспечивающих ее средств; 4 - эффективность работы средств для СРД; 5 - стоимость технических средств защиты; 6 – все перечисленные; 7 – 1-3 3.Что включает в себя документация для оценки защищенности АС и СВТ от НСД? 1 – Политика безопасности; 2 - Руководство пользователя по использованию защитных механизмов; 3 - Руководство по управлению средствами защиты. 4 - Проектная документация; 5 - Описание процедур тестирования и их результатов; 6 – 2 - 5; 4 – 1 – 5.
Уметь: разрабатывать структуру защищенной информационной системы	1.К основным способам НСД относятся: 1 - непосредственное обращение к объектам доступа; 2 - создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты; 3 - модификация средств защиты, позволяющая осуществить НСД; 4 - внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД. 5 – 3, 4 + все перечисленные. 2.Что включает в себя документация для оценки защищенности АС и СВТ от НСД? 1 – Политика безопасности; 2 - Руководство пользователя по использованию защитных механизмов; 3 - Руководство по управлению средствами защиты. 4 - Проектная документация; 5 - Описание процедур тестирования и их результатов;

	6 – 2 - 5; 4 – 1 – 5.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тестирование по теме: «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)»

Краткое содержание задания:
Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

Контрольные вопросы/задания:

Знать: современные технологии построения безопасных информационных систем	1.Что является необходимыми исходными данными для проведения классификации конкретной АС? 1 - перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности; 2 - перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий; 3. матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС; 4 - режим обработки данных в АС; 5 – СЗИ, реализованные в АС; 6 – все перечисленные; 7 - 1-4. 2.Сколько классов защищенности АС от НСД устанавливается? 1 - 5;

	2 - 6; 3 - 7; 4 - 9. 3.Сколько классов защищенности АС от НСД установлено для группы многопользовательских АС, в которых одновременно хранится информация различных уровней конфиденциальности? 1 - 5; 2 - 6; 3 - 7; 4 - 9.
Уметь: использовать современные программные средства защиты информации	1.Какие относятся к числу определяющих признаков, по которым производится груп- пировка АС в различные классы: 1 - наличие в АС информации различного уровня конфиденциальности; 2 - уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации; 3 - режим обработки данных в АС; 4 – наличие в АС СЗИ; 5 – все перечисленные 6 - 1-3.
Уметь: работать с основными программными и аппаратными средствами анализа защиты информационных систем	1.Сколько классов защищенности АС от НСД установлено для группы многопользовательских АС, в которых одновременно хранится информация различных уровней конфиденциальности? 1 - 5; 2 - 6; 3 - 7; 4 - 9.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тестирование по теме: «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)»

Краткое содержание задания:
Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

Контрольные вопросы/задания:

Знать: инструментальные программные и аппа-ратные средства анализа защищенности информационных систем и сетей	1.Какая группа каждого класса защищенности СВТ от НСД характеризуется мандатной защитой? 1 – 2,3,4; 2 – 2,4,5; 3 – 3,4,5; 4 – 1,2,3 2.Что не входит в конструкторскую (проектную) документацию по защите СВТ от НСД? 1 – описание принципов работы СВТ;; 2 – общая схема КЗС; 3 – описание алгоритм криптографической защиты; 4 – описание интерфейсов КЗС; 5 – описание механизмов идентификации и аутентификации. 3.Сколько показателей защищенности от НСД оцениваются для СВТ 5 класса? 1 - 5; 2 - 7; 3 - 9; 4 - 11
Уметь: использовать современные программные средства защиты информации	1.Сколько классов защищенности СВТ от НСД устанавливается? 1 - 5; 2 - 6; 3 - 7; 4 - 9
Уметь: работать с основными программными и аппаратными средствами анализа защиты информационных систем	1.Для какого класса СВТ реализуются дискреционные ПРД? 1 - 5; 2 - 6; 3 - 7; 4 - 9 2.Сколько показателей защищенности от НСД оцениваются для СВТ 6 класса? 1 - 5; 2 - 6; 3 - 7;

	4 - 9

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3 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.Классификация методов и механизмов обеспечения компьютерной безопасности
2.Понятие угроз безопасности, основы их классификации
3.Понятие политики безопасности в компьютерных системах и ее формализованное выражение в моделях безопасности
4.Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)
5.Европейские критерии безопасности информационных технологий
6.Федеральные критерии безопасности информационных технологий Национального института стандартов и технологий и Агентства национальной безопасности США
7.Модели и теоремы безопасности на основе дискреционной политики (пятимерное пространство Хартсона)
8.Модели и теоремы безопасности на основе дискреционной политики (модель на основе матрицы доступа)
9.Модели исследования распространения прав доступа в системах с дискреционной политикой (модель Харисона-Руззо-Ульмана)
10.Модели исследования распространения прав доступа в системах с дискреционной политикой (модель типизованной матрицы доступа)
11.Модели исследования распространения прав доступа в системах с дискреционной политикой (модель TAKE-GRANT)
12.Модели исследования распространения прав доступа в системах с дискреционной политикой (расширенная модель TAKE-GRANT)
13.Недостатки моделей дискреционного доступа
14.Сценарий атаки "троянскими программами"
15.Модели и теоремы безопасности на основе мандатной политики (модель Белла-ЛаПадулы)
16.Модели и теоремы безопасности на основе мандатной политики (модель МакЛина)
17.Модели и теоремы безопасности на основе мандатной политики (модель Low-WaterMark)
18.Модели и теоремы безопасности на основе мандатной политики (модель Белла-ЛаПадулы)
19.Модели и теоремы безопасности на основе мандатной политики (модель МакЛина)
20.Модели и теоремы безопасности на основе мандатной политики (модель Low-WaterMark)
21.Модели безопасности на основе ролевой политики и технологии рабочих групп пользователей

22.Понятие и разновидности скрытых каналов утечки информации в компьютерных системах
23.Теоретико-вероятностные основы выявления и нейтрализации утечки информации (автоматная модель Гогена-Мессигера)
24.Модели и механизмы обеспечения целостности данных в компьютерных системах (дискреционная модель Кларка-Вильсона)
25.Модели и механизмы обеспечения целостности данных в компьютерных системах (мандатная модель Кена Биба)
26.Модели и механизмы обеспечения целостности данных в компьютерных системах (технологии и протоколы выполнения транзакций в клиент-серверных системах)

Материалы для проверки остаточных знаний

1.Какие функции выполняет элемент аппаратной защиты, предполагающий использование источников бесперебойного питания (UPS)?

Ответы:

а. защита от сбоев в электропитании
б. защита от сбоев серверов, рабочих станций и локальных компьютеров
в. защита от сбоев устройств для хранения информации
г. защита от утечек информации электромагнитных излучений.

Верный ответ: а

2.Какой уровень возможности нарушителя определяется возможностью управления функционированием АС, путем воздействия на базовое программное обеспечение системы
и на состав и конфигурацию ее оборудования?

Ответы:

а. 2
б. 3
в. 4
г. 6

Верный ответ: б

3.Какой технический канал утечки основан на распространении звуковых колебаний в любом звукопроводящем материале или среде?

Ответы:

а. Акустические и виброакустические
б. Электрические
в. Оптические
г. Радиоканалы

Верный ответ: а

4.По сведениям Media и Pricewaterhouse Coopers, 60% всех инцидентов IT-безопасности совершается за счет…

Ответы:

а. Хакерские атаки
б. Различные незаконные проникновения
в. Инсайдеры

Верный ответ: в

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

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