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
Защищенные информационные системы

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. ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

ИД-1 Самостоятельно осваивает и адаптирует к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Защита практического задания №1 «Межсетевые экраны» (Отчет)
2. Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет)
3. Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)
4. Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)

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
Модели и критерии оценки защищенных информационных систем					
Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС.			+		+
Программно-аппаратные средства защищенных информационных систем					
Классификация программно-аппаратных средств защиты ИС.		+	+	+	+
Инфраструктура открытых ключей в защищенных информационных системах					
Принципы аутентификации на основе модели «рукопожатия»		+		+	+
	Вес КМ:	20	25	20	35

$Общая часть/Для промежуточной аттестации$

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
ОПК-1	ИД-1$_{ОПК-1}$ Самостоятельно осваивает и адаптирует к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты	Знать: каналы распространения вредоносных программ, способы предупреждения заражения вредоносными программами и методы их обнаружения формальные модели, лежащие в основе защищенных информационных систем угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети Уметь: выбирать методы защиты информации при ее передаче по открытым компьютерным сетям проводить анализ информационных систем с точки зрения обеспечения	Защита практического задания №1 «Межсетевые экраны» (Отчет) Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет) Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет) Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)

		их защищенности использовать формальные модели построения защищенных информационных систем применять методы и программно-аппаратные средства защиты информационных систем	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Защита практического задания №1 «Межсетевые экраны»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выполнение практического задания

Краткое содержание задания:
Задание провести анализ технических возможностей применения межсетевых экранов. Необходимо выбрать ресурс для исследования. Номер межсетевого экрана соответствует порядковому номеру студента в списке группы. Студент под номером 5 выбирает 1 вариант; 6 – 2 и т.д.

Контрольные вопросы/задания:

Уметь: применять методы и программно-аппаратные средства защиты информационных систем	1.Перечислите классификационные признаки межсетевых экранов

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. Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Выполнение практического задания

Краткое содержание задания:

Задание провести анализ технических возможностей примения сканеров уязвимостей. Необходимо выбрать ресурс для исследования. Номер сканера безопасности соответствует порядковому номеру студента в списке группы. Студент под номером 5 выбирает 1 вариант; 6 – 2 и т.д.:

1.	Internet Scanner 7.0	Internet Security Systems	http://www.iss.net
2.	LanGuard 3.2	GFI	http://www.gfi.com
3.	Nessus 2.0.6	Renaud Deraison	http://www.nessus.org
4.	Retina 4.9.97	eEye Digital Security	http://www.eeye.com
5.	XSpider 7.0	Positive Technologies	http://www.ptsecurity.ru

Контрольные вопросы/задания:

Знать: угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети	1.Какие существуют оценки уровня влияния информационных систем?
Знать: формальные модели, лежащие в основе защищенных информационных систем	1.Что такое информационные системы?

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. Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выполнение практического задания

Краткое содержание задания:
Подготовить ответы на вопросы

Контрольные вопросы/задания:

Уметь: выбирать методы защиты информации при ее передаче по	1.Принцип работы этого метода заключается в обнаружении несоответствия между текущим

открытым компьютерным сетям	режимом функционирования КС и моделью штатного режима работы, заложенной в параметрах метода. О каком методе обнаружения атак идет речь?
Уметь: использовать формальные модели построения защищенных информационных систем	1.Преимуществом метода данного типа является возможность обнаружения новых атак без необходимости постоянного изменения параметров функционирования модуля. О каком методе идет речь?

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. Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 35
Процедура проведения контрольного мероприятия: Выполнение практического задания

Краткое содержание задания:
Подготовить ответы на вопросы

Контрольные вопросы/задания:

Знать: каналы распространения вредоносных программ, способы предупреждения заражения вредоносными программами и методы их обнаружения	1.Как называются СОА обнаруживающие атаки, направленные на всю сеть или сегмент?
Уметь: проводить анализ информационных систем с точки зрения обеспечения их защищенности	1.Для чего предназначен межсетевой экран?

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: Экзамен

Пример билета

НИУ «МЭИ»	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина: *Защищенные информационные системы*	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* *Протокол заседания кафедры №3* *«16» декабря 2021г.*
1. Характеристика мероприятий защищенности информационных систем. 2. Характеристика ключевых возможностей систем межсетевого экранирования по обеспечению безопасности информации в информационной системея стандартам 3. Практически сформировать параметры собственной политики безопасности защищенной информационной системы		

Процедура проведения

Экзамен проводится в устной форме по билетам согласно программе экзамена.

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

1. Компетенция/Индикатор: ИД-1$_{ОПК-1}$ Самостоятельно осваивает и адаптирует к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты

Вопросы, задания

1.Что сопровождает процесс внедрения систем контроля защищенности?
2.Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС.
3.Методология анализа защищенности ИС.
4.Надежность механизмов защиты ИС.
5.Основные угрозы информационной безопасности при подключении ИС к сети Интернет.
6.Программно-аппаратные средства защищенных информационных систем. Классификация программно-аппаратных средств защиты ИС.
7.Принцип работы и классификация межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сеансового и прикладного уровня. Настройка и использование межсетевых экранов.
8.Сканеры уязвимостей информационных систем. Системы обнаружения атак. Системы контроля содержимого.
9.Системы защиты от утечек данных (DLP-системы).
10.Вредоносные программы, их признаки и классификация.
11.Каналы распространения и предупреждение заражения вредоносными программами.
12.Методы обнаружения и удаления вредоносных программ.
13.Инфраструктура открытых ключей в защищенных информационных системах.
14.Принципы аутентификации на основе модели «рукопожатия».

15.Построение системы аутентификации на основе аппаратных и программных генераторов одноразовых паролей. Использование непрямой аутентификации.
16. Архитектура PKI. Отзыв сертификатов, его причины и стратегии.
17.Списки отозванных сертификатов, их структура и виды.
18.Распространение сертификатов и списков отозванных сертификатов.
19.Управление жизненным циклом сертификатов.
20.Способы хранения личных (закрытых) ключей.

Материалы для проверки остаточных знаний

1.**Что понимается под показателем защищенности информационной системы?**

Ответы:

а. Мера доверия, которая может быть оказана средствам защиты
б. Мера доверия, которая может быть оказана программно-аппаратной составляющей
в. Мера доверия, которая может быть оказана средствам антивирусной защиты
г. Мера доверия, которая может быть оказана методам управления терминалами

Верный ответ: б. Мера доверия, которая может быть оказана программно-аппаратной составляющей

2.**Что такое информационная система?**

Верный ответ: Информационная система (ИС) — система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

3.**Что такое угроза информационной безопасности?**

Верный ответ: Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

4.**Что является основной функцией идентификации и аутентификации?**

Ответы:

а. Идентификация и аутентификация локальных пользователей
б. Идентификация и аутентификация удаленных пользователей
в. Идентификация и аутентификация удаленных процессов
г. Идентификация и аутентификация локальных процессов

Верный ответ: а. Идентификация и аутентификация локальных пользователей

5.**Что такое IP-пакет?**

Верный ответ: IP-пакет — форматированный блок информации, передаваемый по компьютерной сети, структура которого определена протоколом IP.

6.**Что такое межсетевой экран?**

Верный ответ: Межсетевой экран — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу