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
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Капгер И.В. Идентификатор: R5d33df1e-KapgerIV-059b09ee	И.В. Капгер
(должность)	(подпись)	(расшифровка подписи)

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
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

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 способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности

2. ПК-1 способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты

3. ПК-3 способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов

4. ПК-4 способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности

5. ПК-7 способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента

6. ПК-8 способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

7. ПК-10 способностью проводить аттестацию объектов информатизации по требованиям безопасности информации

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					
Тема 1. Критерии оценки защищенных информационных систем		+			
Тема 2. Угрозы информационной безопасности		+			
Программно-аппаратные средства защищенных информационных систем					
Тема 3. Классификация программно-аппаратных средств защиты ИС.		+			
Тема 4. Принципы работы межсетевых экранов.			+		
Тема 5. Сканеры уязвимостей информационных систем.			+		
Тема 6. Системы защиты от утечек данных (DLP-системы).			+	+	
Тема 7. Вредоносные программы, их признаки и классификация.				+	
Инфраструктура открытых ключей в защищенных информационных системах					
Тема 8. Принципы аутентификации на основе модели «рукопожатия».					+
Тема 9. Использование асимметричной криптографии в системах аутентификации.					+
Тема 10. Отзыв сертификатов, его причины и стратегии					+
Тема 11. Способы хранения личных (закрытых) ключей.					+
	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
ОПК-1	ОПК-1(Компетенция)	Знать: формальные модели, лежащие в основе защищенных информационных систем	Защита практического задания №1 «Межсетевые экраны» (Отчет)
ПК-1	ПК-1(Компетенция)	Уметь: проводить анализ информационных систем с точки зрения обеспечения их защищенности	Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)
ПК-3	ПК-3(Компетенция)	Уметь: выбирать методы защиты информации при ее передаче по открытым компьютерным сетям	Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)
ПК-4	ПК-4(Компетенция)	Знать: каналы распространения вредоносных программ, способы предупреждения заражения вредоносными программами и методы их обнаружения	Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)
ПК-7	ПК-7(Компетенция)	Уметь: использовать формальные модели построения	Защита практического задания №1 «Межсетевые экраны» (Отчет)

		защищенных информационных систем	
ПК-8	ПК-8(Компетенция)	Уметь: применять методы и программно-аппаратные средства защиты информационных систем	Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет)
ПК-10	ПК-10(Компетенция)	Знать: угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети	Защита практического задания №1 «Межсетевые экраны» (Отчет)

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: 25
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:

Знать: формальные модели, лежащие в основе защищенных информационных систем	1.Какие требования предъявляются к межсетевым экранам?
Знать: угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети	1.Основные виды угроз информационной безопасности в информационных системах
Уметь: использовать формальные модели построения защищенных 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

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:

Уметь: применять методы и программно-аппаратные средства защиты информационных систем	1.Какие существуют угрозы информационной безопасности при компрометации информационных систем?

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

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: 25
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 называется процесс присвоение объектам и субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов?

Уметь: проводить анализ информационных систем с точки зрения обеспечения их защищенности	1.Для каких целей при администрировании, парольной системы, устанавливается ограничение числа попыток ввода пароля?

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

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: 25
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 открытым компьютерным сетям	1.Чем определяются правила доступа к ресурсам внутренней сети, при реализации политики межсетевого экранирования?

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

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: ОПК-1(Компетенция)

Вопросы, задания

1.Что сопровождает процесс внедрения систем контроля защищенности?

2.Методология анализа защищенности ИС.

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. Компетенция/Индикатор: ПК-1(Компетенция)

Вопросы, задания

1.Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС.

Материалы для проверки остаточных знаний

1.**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. Компетенция/Индикатор: ПК-3(Компетенция)

Вопросы, задания

1.Программно-аппаратные средства защищенных информационных систем. Классификация программно-аппаратных средств защиты ИС.

Материалы для проверки остаточных знаний

1.**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.

4. Компетенция/Индикатор: ПК-4(Компетенция)

Вопросы, задания

1.Каналы распространения и предупреждение заражения вредоносными программами.

Материалы для проверки остаточных знаний

1.**Что такое IP-пакет?**

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

5. Компетенция/Индикатор: ПК-7(Компетенция)

Вопросы, задания

1.Принцип работы и классификация межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сеансового и прикладного уровня. Настройка и использование межсетевых экранов.

Материалы для проверки остаточных знаний

1.Принцип работы и классификация межсетевых экранов

Верный ответ: Все экраны по способу их реализации можно разделить на несколько групп: аппаратные сетевые экраны, включающие в себя: предустановленные на специальные компьютеры; встроенные в маршрутизаторы; программные межсетевые экраны, которые устанавливаются поверх стандартных операционных систем. Аппаратные экраны более надежны, поставляются уже установленными и настроенными, но они более дорогие. Программные экраны дешевле, но представляют собой набор, который требует от администратора общих знаний об информационной безопасности. Межсетевой экран включает в себя фильтр пакетов. Эта служба может быть как встроенной в ядро операционной системы, на которой работает экран, так и устанавливаемой отдельно. Фильтр пакетов осуществляет работу с трафиком на низком уровне, определяя, пропустить или задержать пакет в зависимости от адреса его отправителя, получателя или TCP-службы. Это позволяет закрывать отдельные "подозрительные" адреса, с которых возможна атака, либо фильтровать обращения из внешней сети к конфиденциальным службам. Фильтр эффективен против простейших случаев атак и не может спасти от взлома, при котором проводится подмена IP-адреса. В этом случае производится маскировка атакующего под доверенный хост, - и фильтр пакетов доверчиво работает со взломщиком. Кроме того, фильтр прозрачен для различного рода некорректных пакетов, направляемых клиенту, поскольку не проверяет их содержимое. Для

организации виртуальных частных сетей в межсетевых экранах используются средства канального шифрования. Эта служба зашифровывает трафик при передаче через Интернет. На приемной стороне трафик расшифровывается и вводится в локальную сеть филиала предприятия. Люди, работающие в разных офисах, могут даже не замечать, что их компьютеры располагаются в сетях, удаленных друг от друга. Для сохранения конфиденциальности информации используются специальные шифры, которые не позволяют анализировать трафик, передаваемый по открытому сегменту виртуальной частной сети. Эта функция популярна среди компаний, имеющих сеть филиалов в разных городах. Межсетевые экраны могут опираться на один из двух взаимоисключающих принципов обработки поступающих пакетов данных.

6. Компетенция/Индикатор: ПК-8(Компетенция)

Вопросы, задания

1.Сканеры уязвимостей информационных систем. Системы обнаружения атак. Системы контроля содержимого.

Материалы для проверки остаточных знаний

1.**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

7. Компетенция/Индикатор: ПК-10(Компетенция)

Вопросы, задания

1.Основные угрозы информационной безопасности при подключении ИС к сети Интернет.

Материалы для проверки остаточных знаний

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

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

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

III. Правила выставления итоговой оценки по курсу