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 компьютерной безопасности

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. ПК-1 Оценивание уровня безопасности компьютерных систем и сетей
   ПК-1.3 Проводит анализ безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей» (Тестирование)
2. Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада (Тестирование)

Форма реализации: Устная форма

1. Контрольная работа: практическое задание №1 «Угрозы безопасности информации и каналы утечки информации» (Контрольная работа)
2. Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации» (Контрольная работа)

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
Угрозы и способы нарушения компьютерной безопасности					
Основные понятия курса		+			
Каналы утечки информации в компьютерных системах		+			
Теоретические основы построения систем аутентификации					
Типы базового секрета и атаки на системы парольной аутентификации			+	+	
Принципы биометрической аутентификации			+	+	
Классификация устройств аутентификации			+	+	
Стандарты оценки защищенности компьютерных систем и информационных технологий					

Основные определения и требования к защищенности компьютерных систем				+
Состав и общая характеристика руководящих документов ФСТЭК России по защите информации от несанкционированного доступа				+
Назначение и состав общих критериев оценки безопасности информационных технологий				+
Вес КМ:	20	20	20	40

$Общая часть/Для промежуточной аттестации$

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
ПК-1	ПК-1.З$_{ПК-1}$ Проводит анализ безопасности компьютерных систем	Знать: угрозы и методы нарушения безопасности компьютерных систем требования к защищенности автоматизированных систем и информационных технологий методологические основы обеспечения безопасности компьютерных систем Уметь: использовать критерии оценки защищенности автоматизированных систем и информационных технологий проводить анализ автоматизированных систем с точки зрения обеспечения компьютерной безопасности	Контрольная работа: практическое задание №1 «Угрозы безопасности информации и каналы утечки информации» (Контрольная работа) Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей» (Тестирование) Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации» (Контрольная работа) Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа: практическое задание №1 «Угрозы безопасности информации и каналы утечки информации»

Формы реализации: Устная форма
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выполнение практического задания

Краткое содержание задания:
Подготовить ответы на вопросы по теме: «Угрозы безопасности информации и каналы утечки информации». Каждый студент должен дать устный ответ на три индивидуальных вопроса.

Контрольные вопросы/задания:

Знать: методологические основы обеспечения безопасности компьютерных систем	1.Почему не применяется хеширование при хранении биометрических эталонов? 2.В чем особенность применение биометрия в задаче идентификации субъекта? 3.В чем особенность аутентификации по поведенческим биометрическим характеристикам?

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. Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей»

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 “Теоретические основы построения систем парольной и биометрической аутентификации пользователей”

Контрольные вопросы/задания:

Знать: угрозы и методы нарушения безопасности компьютерных систем	1.Что не относится к процессам защиты? а. Отказ б. Атака в. Защита г. Утрата 2.Какой термин определяется как «событие или действие, которое может вызвать изменение функционирования компьютерной системы»? а. Отказ б. Атака в. Защита г. Утрата 3.Какие каналы утечки информации не относятся к специальным? а. Вибрационный канал б. Оптический канал в. ПЭМИН г. Акустический канал
Уметь: использовать критерии оценки защищенности автоматизированных систем и информационных технологий	1.Что такое базовый секрет? а. Пароль б. Отпечаток в. Логин г. Идентификатор 2.Что относится к одноразовым паролям? а. Цифры б. Буквы в. Цифры и буквы г. Ничего из перечисленного

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. Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации»

Формы реализации: Устная форма
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Выполнение практического задания

Краткое содержание задания:

Подготовить ответы на вопросы по теме: «Принципы создания и использования устройств аутентификации». Каждый студент должен дать устный ответ на три индивидуальных вопроса.

Контрольные вопросы/задания:

Знать: угрозы и методы нарушения безопасности компьютерных систем	1.Что относится к верхнему и нижнему уровням представления требований безопасности в Общих критериях? 2.Что обозначают вторая и четвертая части в идентификаторе требования безопасности в Общих критериях? 3.Поясните смысл идентификатора требования безопасности FMT_MSA.1.1. К какой группе требований (функциональных или доверия) относится данное требование?
Уметь: использовать критерии оценки защищенности автоматизированных систем и информационных технологий	1.Какие уровни стойкости функций безопасности объекта оценки используются в Общих критериях? 2.В чем особенность классов требований доверия APE и ASE? 3.Какой максимальный оценочный уровень доверия может быть присвоен продукту информационных технологий, разработчик которого не желает раскрывать и формально описывать детали его проектирования и проверки?

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. Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада

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 “Требования к безопасности компьютерных систем и информационных технологий”

Контрольные вопросы/задания:

Знать: требования к защищенности автоматизированных систем и информационных технологий	1.Что понимается под качеством информации? а. Один из показателей качества информации б. Одно из свойств информации в. Один из грифов информации г. Один из элементов информации 2.Что не относится к способам нарушения защищенности информации? а. Нарушение передачи информации б. Нарушение сбора информации в. Нарушение хранения информации г. Нарушение защиты информации 3.Что не относится к биометрической аутентификации? а. Сравнение матриц б. Сравнения эталонов в. Сравнение хэшей г. Сравнение паролей
Уметь: проводить анализ автоматизированных систем с точки зрения обеспечения компьютерной безопасности	1.Что не относится к устройствам авторизации? а. СКУД б. Шлагбаум в. Механический дверной замок г. Электро-механический дверной замок 2.Что относится к системам строгой отчетности? а. База данных паролей б. База данных хэшей в. База данных пользователей

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: Зачет с оценкой

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: ПК-1.З$_{ПК-1}$ Проводит анализ безопасности компьютерных систем

Вопросы, задания

1.Какие создаются информационные угрозы для компании?
2.Перечислите основные информационные угрозы.
3.Что угрожает личности (физическому лицу)?
4.Назовите причины информационных угроз.
5.Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз информационной безопасности?
6.Какие действия и события нарушают информационную безопасность?
7.Какая характеристика, не зависящая от «порога совмещения» применяется для оценки качества системы биометрической аутентификации?
8.В чем недостатки и достоинства биометрической аутентификации?
9.Как с помощью криптографии обеспечивается подлинность считанных биометрических характеристик?
10.Как может быть обеспечена конфиденциальность биометрических персональных данных при их передаче по открытой сети?
11.Назовите структуры для объединения компонентов требований безопасности в Общих критериях.
12.Постарайтесь кратко сформулировать основное отличие оценки защищенности объекта в Общих критериях по сравнению с «Оранжевой книгой» и Руководящими документами ФСТЭК.
13.Приведите по два примера аутентификационных данных и секретов, используемых функциями безопасности объекта оценки.
14.К какой группе требований относится класс «Аудит безопасности»?

Материалы для проверки остаточных знаний

1.Что понимается под системой биометрической аутентификации?
Верный ответ: а. Сравнение матриц б. Сравнения эталонов в. Сравнение хэшей г. Сравнение паролей
2.Для чего может применяться асимметричная криптография?
Верный ответ: а. Шифрование больших файлов б. Шифрование небольших файлов в. Для всего перечисленного г. Ничего из перечисленного
3.Какой способ аутентификации пользователя является наиболее безопасным?
Верный ответ: а. С помощью логина б. С помощью пароля в. С помощью логина и пароля

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

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»