

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

Направление подготовки/специальность: 01.03.02 Прикладная математика и информатика

**Наименование образовательной программы: Математическое и программное обеспечение
вычислительных машин и компьютерных сетей**

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Защита данных**

**Москва
2023**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Хорев П.Б.
	Идентификатор	Rdf0a0f96-KhorevPB-ab4b01e2

П.Б. Хорев

СОГЛАСОВАНО:

Руководитель
образовательной
программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Ионова Т.В.
	Идентификатор	R5ac51726-IonovaTV-b9dd3591

Т.В. Ионова

Заведующий
выпускающей
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Варшавский П.Р.
	Идентификатор	R9a563c96-VarshavskyPR-efb4bbd

П.Р.
Варшавский

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-3 Способен выполнять анализ и работы по защите информации

ИД-1 Формирует методы защиты информации и умеет применять их на практике

ИД-2 Представляет результаты анализа состояния защиты данных и предлагает методы по ее улучшению

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Защита лабораторной работы 5; защита лабораторной работы 6 (Лабораторная работа)

2. Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2 (Лабораторная работа)

3. Защита лабораторной работы №2; защита лабораторной работы №3 (Лабораторная работа)

4. Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5 (Лабораторная работа)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
Комплексный подход к обеспечению информационной безопасности					
Комплексный подход к обеспечению информационной безопасности	+				
Защита от несанкционированного доступа к информации в компьютерных системах					
Защита от несанкционированного доступа к информации в компьютерных системах	+	+	+		
Криптографические методы и средства защиты информации					
Криптографические методы и средства защиты информации			+		
Защита от вредоносных программ и несанкционированного копирования информационных ресурсов					
Защита от вредоносных программ и несанкционированного копирования информационных ресурсов				+	

	Вес КМ:	25	25	25	25
--	---------	----	----	----	----

\$Общая часть/Для промежуточной аттестации\$

БРС курсовой работы/проекта

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	8	14	16
Проектирование интерфейса программной реализации		+		
Выполнение программной реализации			+	
Подготовка отчета о выполнении курсовой работы				+
	Вес КМ:	20	50	30

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-3	ИД-1 _{ПК-3} Формирует методы защиты информации и умеет применять их на практике	Знать: Модели и способы построения симметричных и асимметричных криптографических систем Методы разграничения полномочий пользователей и модели управления доступом к объектам компьютерных систем и сетей Способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем и сетей Общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию	Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2 (Лабораторная работа) Защита лабораторной работы №2; защита лабораторной работы №3 (Лабораторная работа) Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5 (Лабораторная работа)

		<p>методов ее решения</p> <p>Уметь:</p> <p>Использовать результаты анализа защищенности для устранения уязвимостей в подсистемах безопасности компьютерных систем и сетей</p> <p>Использовать средства анализа защищенности компьютерных систем и сетей</p> <p>Использовать методы и средства криптографической защиты информации</p> <p>Применять методы и программные средства защиты данных в компьютерных системах и сетях</p> <p>Определять цели и задачи разработки новых методов и программных средств защиты информации в компьютерных системах и сетях</p>	
ПК-3	ИД-2ПК-3 Представляет результаты анализа состояния защиты данных и предлагает методы по ее улучшению	<p>Знать:</p> <p>Достоинства и недостатки симметричных и асимметричных криптографических систем</p> <p>Достоинства и недостатки</p>	<p>Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2 (Лабораторная работа)</p> <p>Защита лабораторной работы №2; защита лабораторной работы №3 (Лабораторная работа)</p> <p>Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5 (Лабораторная работа)</p>

		<p>методов и программно-аппаратных средств защиты данных в компьютерных системах и сетях</p> <p>Стандарты оценки и методы анализа защищенности компьютерных систем и информационных технологий</p> <p>Тенденции развития методов защиты данных в компьютерных системах и сетях</p> <p>Тенденции развития средств защиты информации в операционных системах</p> <p>Уметь:</p> <p>Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации</p> <p>Разрабатывать новые программные средства защиты данных и безопасных информационных технологий</p>	<p>Защита лабораторной работы 5; защита лабораторной работы 6 (Лабораторная работа)</p>
--	--	--	---

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Защита лабораторной работы №1; подготовка отчета о выполнении лабораторной работы №2

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: 1. Выполнение и защита лабораторной работы 1. 2. Выполнение лабораторной работы 2.

Краткое содержание задания:

1. Разработка программы разграничения полномочий пользователей на основе паролей .
2. Изучение и освоение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.

Контрольные вопросы/задания:

Знать: Общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения	1.Что не относится к способам аутентификации пользователей, основанных на общем секрете? 2.Что такое авторизация субъектов компьютерной системы?
Знать: Тенденции развития методов защиты данных в компьютерных системах и сетях	1.В чем основной недостаток дискреционного управления доступом к объектам компьютерных систем? 2.Что означает термин "роль" в ролевом разграничении доступа?
Знать: Тенденции развития средств защиты информации в операционных системах	1.Зачем в учетной записи пользователя может храниться случайное значение?

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Лабораторная работа 1 выполнена в точном соответствии с заданием, лабораторная работа 2 выполнена полностью

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Лабораторная работа 1 выполнена в основном в соответствии с заданием, лабораторная работа 2 выполнена полностью

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Лабораторная работа 1 выполнена в основном в соответствии с заданием

Оценка: 2

Описание характеристики выполнения знания: Не выполнена ни одна из лабораторных работ 1-2

КМ-2. Защита лабораторной работы №2; защита лабораторной работы №3

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: 1. Защита лабораторной работы 2. 2. Выполнение и защита лабораторной работы 3.

Краткое содержание задания:

1. Изучение и освоение программных средств защиты от несанкционированного доступа и разграничения прав пользователей.
2. Разработка и программная реализация алгоритмов симметричной криптографии и криптографического хеширования.

Контрольные вопросы/задания:

Знать: Методы разграничения полномочий пользователей и модели управления доступом к объектам компьютерных систем и сетей	1.Что такое многофакторная аутентификация в компьютерных системах?
Знать: Модели и способы построения симметричных и асимметричных криптографических систем	1.В чем главный недостаток шифров простой замены?
Знать: Способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем и сетей	1.Где хранится информация об ограничениях на возможности работы локального пользователя операционной системы? 2.На каких способах шифрования основаны симметричные криптосистемы?
Знать: Достоинства и недостатки методов и программно-аппаратных средств защиты данных в компьютерных системах и сетях	1.В чем разница между шифрованием и криптографическим хешированием? 2.В чем достоинства и недостатки дискреционного разграничения доступа к объектам компьютерных систем?
Уметь: Использовать результаты анализа защищенности для устранения уязвимостей в подсистемах безопасности компьютерных систем и сетей	1.Как скрыть отображаемые на экране пароли из базы данных программного менеджера паролей, но при этом сохранить возможность их переноса в требуемую программу? 2.Как в операционной системе Windows включить требование к минимальной сложности паролей пользователей?
Уметь: Использовать средства анализа защищенности компьютерных систем и сетей	1.Как в программе реализовать выполнения арифметических операций с вычетами по модулю? 2.Как в операционной системе Windows ограничить права пользователей на выполнение определенных действий?
Уметь: Применять методы и	1.Как установить защиту от атак угадывания

программные средства защиты данных в компьютерных системах и сетях	(подбора) паролей? 2.Как в программе реализовать генерацию псевдослучайной последовательности при использовании шифрования гаммированием?
Уметь: Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации	1.Как создать новую базу данных паролей с помощью программного менеджера паролей и защитить ее от несанкционированного доступа?

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 90% контрольных вопросов при защите лабораторной работы 2, лабораторная работа 3 выполнена в точном соответствии с заданием

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 70% контрольных вопросов при защите лабораторной работы 2, лабораторная работа 3 выполнена в основном в соответствии с заданием

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 50% контрольных вопросов при защите лабораторной работы 2 или лабораторная работа 3 выполнена в основном в соответствии с заданием

Оценка: 2

Описание характеристики выполнения знания: Правильные ответы даны менее чем 50% контрольных вопросов при защите лабораторной работы 2, лабораторная работа 3 не выполнена

КМ-3. Защита лабораторной работы №4; подготовка отчета о выполнении лабораторной работы №5

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: 1. Выполнение и защита лабораторной работы 4. 2. Выполнение лабораторной работы 5.

Краткое содержание задания:

1. Использование криптографических средств операционных систем в прикладных программах.
2. Изучение и освоение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ.

Контрольные вопросы/задания:

Знать: Достоинства и недостатки симметричных и асимметричных криптографических систем	1.В чем заключается основная проблема при использовании симметричной криптографии? 2.Как вычисляется и проверяется электронная
---	---

	подпись?
Уметь: Использовать методы и средства криптографической защиты информации	1.Как в программе реализовать вывод сеансового ключа шифрования из введенной пользователем парольной фразы? 2.Как создать самоподписанный сертификат открытого ключа?
Уметь: Определять цели и задачи разработки новых методов и программных средств защиты информации в компьютерных системах и сетях	1.Как добавить электронную подпись к макросу в документе офисного приложения? 2.Как в операционной системе Windows включить шифрование папок и (или) файлов?
Уметь: Разрабатывать новые программные средства защиты данных и безопасных информационных технологий	1.Как в программе реализовать симметричное шифрование файлов по выбранному алгоритму? 2.Как в программе сгенерировать ключ шифрования (расшифрования) из введенной пользователем парольной фразы?

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Лабораторная работа 4 выполнена в точном соответствии с заданием, лабораторная работа 5 выполнена полностью

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Лабораторная работа 4 выполнена в основном в соответствии с заданием, лабораторная работа 5 выполнена полностью

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Лабораторная работа 4 выполнена в основном в соответствии с заданием

Оценка: 2

Описание характеристики выполнения знания: Не выполнена ни одна из лабораторных работ 4-5

КМ-4. Защита лабораторной работы 5; защита лабораторной работы 6

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: 1. Защита лабораторной работы 5. 2. Выполнение и защита лабораторной работы 6.

Краткое содержание задания:

1. Изучение и освоение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ.
2. Разработка средств защиты программного обеспечения от несанкционированного использования и копирования.

Контрольные вопросы/задания:

Знать: Стандарты оценки и методы анализа защищенности компьютерных систем и информационных технологий	<p>1.Что такое компьютерный вирус и какие существуют другие разновидности вредоносных программ?</p> <p>2.Что понимается под защитой объектов интеллектуальной собственности от несанкционированного копирования?</p>
---	--

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 90% контрольных вопросов при защите лабораторной работы 5, лабораторная работа 6 выполнена в точном соответствии с заданием

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 70% контрольных вопросов при защите лабораторной работы 5, лабораторная работа 6 выполнена в основном в соответствии с заданием

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Даны полные и точные ответы не менее чем на 50% контрольных вопросов при защите лабораторной работы 5 или лабораторная работа 6 выполнена в основном в соответствии с заданием

Оценка: 2

Описание характеристики выполнения знания: Правильные ответы даны менее чем 50% контрольных вопросов при защите лабораторной работы 6, лабораторная работа 3 не выполнена

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Проблема защиты информации и подходы к ее решению.
1. 2. Протокол Диффи-Хеллмана.
2. 3. Зашифровать перестановкой P =безопасность данных на ключе K =ФамилияИО (фамилия и инициалы студента, без пробелов).

Процедура проведения

1. При подготовке студенты письменно отвечают на вопросы экзаменационного билета. 2. Студенты устно отвечают на вопросы экзаменационного билета и дополнительные вопросы преподавателя.

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

1. Компетенция/Индикатор: ИД-1_{ПК-3} Формирует методы защиты информации и умеет применять их на практике

Вопросы, задания

1. Основные понятия защиты информации
2. Зашифровать и расшифровать $M=3$ по алгоритму RSA (выбор ключей начать с $p=3$, $q=11$)
3. Принципы построения и свойства асимметричных криптосистем
4. Дискреционное, мандатное и ролевое разграничение доступа к объектам
5. Протокол Kerberos
6. Зашифровать P =безопасность данных многоалфавитной подстановкой на ключе $K=d,d,m,m$ (день и месяц рождения студента, 4 цифры, первую цифру 0, если она есть в дате, заменить на 8, вторую цифру 0 – на 9)

Материалы для проверки остаточных знаний

1. В чем заключается проверка электронной подписи?

Ответы:

В сличении ее с эталонной В сличении ее с закрытым ключом автора документа В проверке совпадения расшифрованной на открытом ключе автора подписи и хеш-значения документа В проверке совпадения расшифрованной на закрытом ключе автора подписи и хеш-значения документа В проверке хеш-кода документа

Верный ответ: В проверке совпадения расшифрованной на открытом ключе автора подписи и хеш-значения документа

2. Какая из криптосистем не относится к асимметричным?

Ответы:

RSA AES ElGamal Эллиптических кривых

Верный ответ: AES

3. Чему равно $-7 \pmod{5}$?

Ответы:

7 -2 3 5

Верный ответ: 3

4. Что является основным критерием при выборе элемента аппаратного обеспечения для аутентификации пользователей?

Ответы:

Стоимость изготовления Сложность копирования Скорость считывания ключевой информации Объем памяти и наличие микропроцессора

Верный ответ: Сложность копирования

5. Какие методы и средства защиты информации являются обязательными в любой системе защиты?

Ответы:

Криптографические Программно-аппаратные Инженерно-технические Организационные

Верный ответ: Организационные

6. В чем разница между криптографией и стеганографией?

Ответы:

Это тождественные понятия Целью криптографии является скрытие конфиденциальной информации и самого ее наличия, а целью стеганографии - только скрытие информации Целью криптографии является скрытие содержания конфиденциальной информации, а целью стеганографии - скрытие факта ее наличия

Верный ответ: Целью криптографии является скрытие содержания конфиденциальной информации, а целью стеганографии - скрытие факта ее наличия

2. Компетенция/Индикатор: ИД-2ПК-3 Представляет результаты анализа состояния защиты данных и предлагает методы по ее улучшению

Вопросы, задания

1. Методы обнаружения и удаления вредоносных программ

2. Компьютерная стеганография и ее применение

3. Применение и обзор современных симметричных криптосистем

4. Аудит событий безопасности в ОС Windows и Unix

5. Способы аутентификации пользователей

6. Способы нарушения защищенности информации и защиты от него в компьютерных системах

Материалы для проверки остаточных знаний

1. Что такое удостоверяющий центр?

Ответы:

Орган, создающий секретные ключи пользователей Орган, осуществляющий резервное копирование криптографических ключей Орган, занимающийся проверкой электронной подписи под документами Орган, выдающий сертификаты открытых ключей пользователей

Верный ответ: Орган, выдающий сертификаты открытых ключей пользователей

2. Какое требование не применяется при построении идеального шифра (по К. Шеннону)?

Ответы:

Длина ключа \geq длины открытого текста Ключ выбирается совершенно случайно В ключе равномерно распределены нулевые и единичные биты Ключ не используется дважды

Верный ответ: В ключе равномерно распределены нулевые и единичные биты

3. В чем основной недостаток дискреционного управления доступом к объектам?

Ответы:

Снижение производительности системы Невозможность аудита попыток доступа Возможность утечки конфиденциальной информации при выполнении санкционированных действий Сложность администрирования

Верный ответ: Возможность утечки конфиденциальной информации при выполнении санкционированных действий

4. Что означает термин "аутентификация"?

Ответы:

Проверка регистрации в базе данных Подтверждение подлинности Ограничение прав
Учет и регистрация событий

Верный ответ: Подтверждение подлинности

5. Какие виды антивирусных программ принципиально могут обнаруживать только уже известные вредоносные программы?

Ответы:

Эвристические анализаторы Инспекторы (ревизоры) Сканеры Мониторы (сторожа)
Вакцины

Верный ответ: Сканеры

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Точные и в основном полные ответы на вопросы экзаменационного билета и дополнительные вопросы

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Точные и в основном полные ответы на вопросы экзаменационного билета и большинство дополнительных вопросов

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Точные и в основном полные ответы на большинство вопросов экзаменационного билета и дополнительных вопросов

Оценка: 2

Описание характеристики выполнения знания: Неточные ответы или отсутствие ответа на большинство вопросов экзаменационного билета и дополнительных вопросов

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 экзаменационной составляющих

Для курсового проекта/работы:

7 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

1. Демонстрация разработанной программы. 2. Представление отчета о выполнении курсовой работы. 3. Ответы на вопросы членов комиссии по приему курсовой работы.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Корректная работа представленной программы, точные и в основном полные ответы на вопросы членов комиссии

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Корректная работа представленной программы, точные и в основном полные ответы на большинство вопросов членов комиссии

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Корректная работа представленной программы для большинства обязательных для реализации функций, точные и в основном полные ответы на большинство вопросов членов комиссии

Оценка: 2

Описание характеристики выполнения знания: Некорректная работа программы или неправильные ответы (отсутствие ответа) на вопросы членов комиссии

III. Правила выставления итоговой оценки по курсу

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»