

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

Направление подготовки/специальность: 02.03.02 Фундаментальная информатика и информационные технологии

Наименование образовательной программы: Информационные технологии и системы искусственного интеллекта

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Криптографические методы защиты информации**

**Москва
2024**

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	Чернецов А.М.
	Идентификатор	Re594826f-ChernetsovAM-0080e09

А.М. Чернецов

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-1 Способен проектировать и реализовывать программное обеспечение, базы данных и выполнять работы по защите информации

ИД-1 Определяет необходимый уровень прав доступа к данным и выполняет работы по защите информации

ИД-5 Определяет методы тестирования и умеет проводить все виды контроля программ с применением интеллектуальных технологий

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Выполнение и защита лабораторной работы 1 (Лабораторная работа)

2. Выполнение и защита лабораторной работы 3; защита расчетного задания (Лабораторная работа)

Форма реализации: Письменная работа

1. Тест по разделу 1 (Тестирование)

Форма реализации: Смешанная форма

1. Выполнение и защита лабораторной работы 2; защита реферата (Лабораторная работа)

БРС дисциплины

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Тест по разделу 1 (Тестирование)

КМ-2 Выполнение и защита лабораторной работы 1 (Лабораторная работа)

КМ-3 Выполнение и защита лабораторной работы 2; защита реферата (Лабораторная работа)

КМ-4 Выполнение и защита лабораторной работы 3; защита расчетного задания (Лабораторная работа)

Вид промежуточной аттестации – Экзамен.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	7	11	14

Основные понятия и классификация криптографических протоколов				
Основные понятия и классификация криптографических протоколов	+			
Протоколы распределения ключей и аутентификации				
Протоколы распределения ключей и аутентификации		+		
Протоколы разделения секрета, предсказания и голосования				
Протоколы разделения секрета, предсказания и голосования			+	
Криптографические методы в инфраструктуре открытых ключей				
Криптографические методы в инфраструктуре открытых ключей				+
Вес КМ:	20	25	25	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-1	ИД-1 _{ПК-1} Определяет необходимый уровень прав доступа к данным и выполняет работы по защите информации	Знать: Способы управления криптографическими ключами и сертификатами открытых ключей; Российские и международные стандарты в области криптографических алгоритмов и протоколов Тенденции развития криптографических методов защиты информации Особенности использования криптографических методов защиты информации при решении различных прикладных задач Уметь: Использовать литературу и источники сети Интернет для получения	КМ-2 Выполнение и защита лабораторной работы 1 (Лабораторная работа) КМ-3 Выполнение и защита лабораторной работы 2; защита реферата (Лабораторная работа) КМ-4 Выполнение и защита лабораторной работы 3; защита расчетного задания (Лабораторная работа)

		информации о создании новых криптографических методов и средств защиты информации Использовать методы и средства криптографической защиты информации для создания защищенного электронного документооборота Определять цели и задачи разработки новых методов и программных средств криптографической защиты информации в компьютерных системах и сетях Использовать методы и средства криптографической защиты информации при обеспечении информационной безопасности компьютерных систем и сетей	
ПК-1	ИД-5ПК-1 Определяет методы тестирования и умеет проводить все виды контроля программ с применением интеллектуальных	Знать: Достоинства и недостатки современных криптографических систем Современные технологии создания программных	КМ-1 Тест по разделу 1 (Тестирование) КМ-2 Выполнение и защита лабораторной работы 1 (Лабораторная работа) КМ-3 Выполнение и защита лабораторной работы 2; защита реферата (Лабораторная работа) КМ-4 Выполнение и защита лабораторной работы 3; защита

	технологий	средств криптографической защиты информации Способы построения симметричных и асимметричных криптографических систем Уметь: Разрабатывать новые безопасные информационные технологии с использованием криптографических методов и средств Предлагать методы и средства повышения информационной безопасности компьютерных систем и сетей, основанные на криптографической защите информации Анализировать эффективность используемых криптографических методов и средств защиты информации	расчетного задания (Лабораторная работа)
--	------------	--	--

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест по разделу 1

Формы реализации: Письменная работа

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Проверка ответов на вопросы теста.

Краткое содержание задания:

Подготовка ответов на контрольные вопросы

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: Достоинства и недостатки современных криптографических систем	1.Какие возможны атаки на криптографические протоколы? 2.Какие атаки на криптографические протоколы наиболее опасны?
Знать: Способы построения симметричных и асимметричных криптографических систем	1.Что понимается под криптографическим протоколом? 2.Какие виды криптографических протоколов существуют?

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Даны правильные ответы не менее чем на 90% вопросов

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Даны правильные ответы не менее чем на 70% вопросов

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Даны правильные ответы не менее чем на 50% вопросов

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Даны правильные ответы менее чем на 50% вопросов

КМ-2. Выполнение и защита лабораторной работы 1

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Проверка правильности и самостоятельности выполнения лабораторной работы 1.

Краткое содержание задания:**Методы и средства аутентификации электронных документов****Контрольные вопросы/задания:**

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: Способы управления криптографическими ключами и сертификатами открытых ключей;	1.Как могут быть получены несколько подписей под одним электронным документом? 2.Что такое неоспоримая электронная подпись?
Уметь: Анализировать эффективность используемых криптографических методов и средств защиты информации	1.Как использовать классы асимметричных криптоалгоритмов DSA и RSA для вычисления и проверки электронной подписи? 2.Как использовать для вычисления и проверки электронной подписи классы криптографии на основе эллиптических кривых?

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Программа для лабораторной работы 1 работает корректно и полностью соответствует заданию.

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Программа для лабораторной работы 1 работает в основном корректно и полностью соответствует заданию.

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Программа для лабораторной работы 1 работает в основном корректно, но не полностью соответствует заданию.

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Программа для лабораторной работы 1 работает некорректно или не соответствует заданию.

КМ-3. Выполнение и защита лабораторной работы 2; защита реферата

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: 1. Представление отчета о выполнении лабораторной работы и ответами на контрольные вопросы. 2. Выступление с докладом и компьютерной презентацией, ответы на вопросы.

Краткое содержание задания:

Запрос и получение сертификатов открытых ключей

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: Особенности использования криптографических методов защиты информации при решении различных прикладных задач	1.Какие виды мошенничества при разделении секрета возможны и в чем может заключаться защита от них? 2.Как может быть организован подсознательный канал для передачи конфиденциальной информации?
Уметь: Использовать методы и средства криптографической защиты информации при обеспечении информационной безопасности компьютерных систем и сетей	1.Как создать самоподписанный сертификат? 2.Как при вызове программы makescert задаются имена субъекта и издателя получаемого сертификата?
Уметь: Разрабатывать новые безопасные информационные технологии с использованием криптографических методов и средств	1.Как просмотреть информацию, содержащуюся в сертификате? 2.Какие шаблоны сертификатов допустимы при подаче запроса сертификата в корпоративном удостоверяющем центре?

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Полные и точные ответы даны не менее чем на 90% контрольных вопросов; реферат и доклад полностью соответствуют выбранной теме

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Полные и точные ответы даны не менее чем на 70% контрольных вопросов; реферат и доклад соответствуют выбранной теме

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Полные и точные ответы даны не менее чем на 50% контрольных вопросов; реферат и доклад соответствуют выбранной теме

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Полные и точные ответы даны менее чем на 50% контрольных вопросов или реферат и доклад не соответствуют выбранной теме

КМ-4. Выполнение и защита лабораторной работы 3; защита расчетного задания

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 30

Процедура проведения контрольного мероприятия: 1. Проверка работоспособности, соответствия заданию и самостоятельности выполнения программы для лабораторной работы 3. 2. Проверка работоспособности, соответствия заданию и самостоятельности выполнения программы для расчетного задания.

Краткое содержание задания:

Методы и средства создания и использования защищенного электронного документооборота с использованием сертификатов открытых ключей

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: Российские и международные стандарты в области криптографических алгоритмов и протоколов	1.Какая информация содержится в сертификате открытого ключа в соответствии со стандартом X.509 ITU? 2.Что может быть причиной отзыва сертификатов до истечения срока их действия?
Знать: Тенденции развития криптографических методов защиты информации	1.Какие существуют варианты запроса сертификата в удостоверяющем центре?
Знать: Современные технологии создания программных средств криптографической защиты информации	1.В чем необходимость использования сертификатов открытых ключей и удостоверяющих центров? 2.Какие возможны способы организации архитектуры удостоверяющих центров в инфраструктуре открытых ключей?
Уметь: Использовать литературу и источники сети Интернет для получения информации о создании новых криптографических методов и средств защиты информации	1.Как использовать в программе классы для хранилища сертификатов открытых ключей?
Уметь: Использовать методы и средства криптографической защиты информации для создания защищенного электронного документооборота	1.Как в программе проверить действительность сертификата открытого ключа?
Уметь: Определять цели и задачи разработки новых методов и программных средств криптографической защиты информации в компьютерных системах и сетях	1.Как использовать в программе класс для сертификата открытого ключа?
Уметь: Предлагать методы и средства повышения информационной безопасности компьютерных систем и сетей, основанные на криптографической защите информации	1.Как использовать в программе класс для выполнения стандартного диалога выбора сертификата в операционной системе? 2.Как использовать в программе класс для построения цепочки сертификации?

Описание шкалы оценивания:*Оценка: 5 («отлично»)**Нижний порог выполнения задания в процентах: 90*

Описание характеристики выполнения знания: Программа для лабораторной работы 3 работает корректно и полностью соответствует заданию; программа для расчетного задания работает корректно и соответствует заданию

*Оценка: 4 («хорошо»)**Нижний порог выполнения задания в процентах: 70*

Описание характеристики выполнения знания: Программа для лабораторной работы 3 работает корректно и соответствует заданию; программа для расчетного задания работает корректно и в основном соответствует заданию

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Программа для лабораторной работы 3 работает в основном корректно и соответствует заданию; программа для расчетного задания работает в основном корректно и соответствует заданию

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Программы для лабораторной работы 3 и расчетного задания работают некорректно или не соответствуют заданию

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Понятие и классификация криптографических протоколов.
2. Одновременное подписание контракта.

Процедура проведения

1. Подготовка письменного ответа на вопросы экзаменационного билета.
2. Устный ответ на вопросы экзаменационного билета и дополнительные вопросы экзаменатора.

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

1. Компетенция/Индикатор: ИД-1_{ПК-1} Определяет необходимый уровень прав доступа к данным и выполняет работы по защите информации

Вопросы, задания

1. Требования к распределению ключей и способы его реализации
2. Управление доступом к устройству с личным (закрытым) ключом
3. Структура сертификата открытого ключа
4. Вычисления с секретными данными
5. Электронное бросание монеты
6. Электронная подпись вслепую
7. Протокол Фиата-Шамира

Материалы для проверки остаточных знаний

1. Какие требования не предъявляются к протоколу электронного бросания монеты?

Ответы:

Бросающий не может «бросить монету» прежде, чем угадывающий предскажет, какой «стороной» она упадет

Бросающему придется «бросить монету» прежде, чем угадывающий предскажет, какой «стороной» она упадет

Бросающий не сможет изменить результат «бросания» монеты после того, как услышит, на какую «сторону» монеты сделал свою ставку угадывающий

Угадывающий не узнает, что выпало – «орел» или «решка» до тех пор, пока не примет окончательное решение и не сообщит о нем бросающему

Верный ответ: Бросающий не может «бросить монету» прежде, чем угадывающий предскажет, какой «стороной» она упадет

2. Для чего используются протоколы с нулевой передачей знаний?

Ответы:

Для подтверждения подлинности открытого ключа пользователя

Для защиты закрытого ключа пользователя от перехвата при его передаче

Для доказательства обладания закрытым ключом без его передачи

Для усложнения получения закрытого ключа пользователя из его открытого ключа

Верный ответ: Для доказательства обладания закрытым ключом без его передачи

3.Какое требование не предъявляется к протоколу к распределению ключей?

Ответы:

Оперативность распределения

Точность распределения

Конфиденциальность распределяемых ключей

Анонимность распределяемых ключей

Верный ответ: Анонимность распределяемых ключей

4.В чем разница понятий алгоритма и протокола?

Ответы:

Алгоритм является конечной последовательностью действий, а протокол может выполняться бесконечно

Алгоритм состоит из однозначно определенных действий, а протокол может включать неоднозначные действия

Алгоритм выполняется одним исполнителем, а в выполнении протокола участвует более одной стороны

Это тождественные понятия

Верный ответ: Алгоритм выполняется одним исполнителем, а в выполнении протокола участвует более одной стороны

5.Что не относится к элементам инфраструктуры открытых ключей?

Ответы:

Список отозванных сертификатов

Удостоверяющий центр

Реестр (репозиторий) сертификатов

Архив сертификатов

Верный ответ: Список отозванных сертификатов

6.Что относится к преимуществам хранения закрытого ключа в файле?

Ответы:

Закрытый ключ не выходит за границы устройства, на котором хранится файл

Возможность прямого контроля пользователя за своим закрытым ключом

Возможность использования легко запоминаемого пароля для защиты закрытого ключа

Применение закрытого ключа для выполнения криптографических операций в оперативной памяти компьютера (мобильного устройства)

Верный ответ: Возможность прямого контроля пользователя за своим закрытым ключом

2. Компетенция/Индикатор: ИД-5ПК-1 Определяет методы тестирования и умеет проводить все виды контроля программ с применением интеллектуальных технологий

Вопросы, задания

1.Распространение сертификатов и списков отозванных сертификатов

2.Голосование с центральной избирательной комиссией

3.Электронные деньги с обнаружением мошенника

4.Обмен зашифрованными ключами. Депонирование ключей

5.Атака «человек посередине» и методы защиты от нее

Материалы для проверки остаточных знаний

1.Какая информация не содержится в сертификате открытого ключа?

Ответы:

Серийный № сертификата

Имя издателя сертификата

Начало и окончание периода действия сертификата

Электронная подпись владельца сертификата

Верный ответ: Электронная подпись владельца сертификата

2. Для чего в протоколе электронного голосования могут использоваться слепые электронные подписи?

Ответы:

Для того, чтобы каждый избиратель голосовал не более одного раза

Для невозможности изменения выбора избирателя после его голосования

Для сохранения тайны голосования конкретного лица и единственности его бюллетеня

Для того, чтобы голосовали только имеющие право голоса

Верный ответ: Для сохранения тайны голосования конкретного лица и единственности его бюллетеня

3. Для чего не может применяться электронная подпись “вслепую”?

Ответы:

Для создания и использования электронных наличных

Для заверения нотариусом закрытых завещаний

Для подписи документов без знания его полного содержания

Для подписи документов без знания закрытого ключа

Верный ответ: Для подписи документов без знания закрытого ключа

4. Что понимается под депонирование секретных ключей?

Ответы:

Создание их резервных копий

Разделение ключа на несколько частей, хранящихся у разных лиц

Передача ключей государственным органам

Дополнительная защита ключей

Верный ответ: Разделение ключа на несколько частей, хранящихся у разных лиц

5. Для чего применяются протоколы группы обмена зашифрованными ключами (Encrypted Key Exchange)?

Ответы:

Для усложнения задачи подбора пароля при перехвате зашифрованных сообщений

Для генерации пары асимметричных ключей из парольной фразы

Для защиты открытого ключа пользователя с помощью пароля

Для защиты закрытого ключа пользователя с помощью пароля

Верный ответ: Для усложнения задачи подбора пароля при перехвате зашифрованных сообщений

6. Для чего применяется открытый ключ в асимметричной криптографии?

Ответы:

Для шифрования данных и вычисления электронной подписи

Для шифрования данных и проверки электронной подписи

Для расшифрования данных и вычисления электронной подписи

Для расшифрования данных и проверки электронной подписи

Верный ответ: Для шифрования данных и проверки электронной подписи

II. Описание шкалы оценивания

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Правильные ответы даны не менее чем на 90% вопросов

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Правильные ответы даны не менее чем на 70% вопросов

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Правильные ответы даны не менее чем на 50% вопросов

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Правильные ответы даны менее чем на 50% 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.