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

Направление подготовки/специальность: 09.04.01 Информатика и вычислительная техника

Наименование образовательной программы: Информационные и вычислительные технологии

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Криптографические методы защиты информации

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Андреева И.Н. Идентификатор: Rb5322c60-AndreevaIN-0472a135	И.Н. Андреева
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Андреева И.Н. Идентификатор: Rb5322c60-AndreevaIN-0472a135	И.Н. Андреева
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Топорков В.В. Идентификатор: Rc76a6458-ToporkovVV-1f71a135	В.В. Топорков
(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-2 Способен применять методологии разработки программного обеспечения
   ИД-1 Использует методы управления информационными ресурсами и создания информационных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Алгоритмы симметричного шифрования (Контрольная работа)
2. Нормативные документы (Контрольная работа)
3. Хеширование и ЭЦП (Контрольная работа)

БРС дисциплины

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	4	8	15
Основные правовые нормы и классификация средств защиты информации и про-граммного обеспечения				
Основные правовые нормы и классификация средств защиты информации и программного обеспечения		+		
Криптографические методы защиты. Электронные цифровые подписи				
2.Криптографические методы защиты. Электронные цифровые подписи			+	+
Стеганографические методы защиты информации				
Стеганографические методы защиты информации			+	+
	Вес КМ:	20	40	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-2	ИД-1$_{ПК-2}$ Использует методы управления информационными ресурсами и создания информационных систем	Знать: методологию разработки системного и прикладного программного обеспечения для защиты данных Уметь: работать с информационными ресурсами и системами для решения задач обеспечения информационной безопасности	Нормативные документы (Контрольная работа) Алгоритмы симметричного шифрования (Контрольная работа) Хеширование и ЭЦП (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Нормативные документы

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Ответы на вопросы на КР

Краткое содержание задания:
Основные правовые нормы и базовые принципы организации систем защиты данных

Контрольные вопросы/задания:

Уметь: работать с информационными ресурсами и системами для решения задач обеспечения информационной безопасности	1.Назовите основные документы РФ по информационной безопасности 2.Назовите классификационные признаки трёх типов классов безопасности

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
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: 75
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: 60
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Алгоритмы симметричного шифрования

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 40
Процедура проведения контрольного мероприятия: Ответы на вопросы КР

Краткое содержание задания:
Использование симметричных алгоритмов шифрования

Контрольные вопросы/задания:

Знать: методологию разработки системного и прикладного программного обеспечения для защиты данных	1. использование криптопровайдеров 2. методики формирования ключей для алгоритмов шифрования

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
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: 75
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: 60
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Хеширование и ЭЦП

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 40
Процедура проведения контрольного мероприятия: Ответы на вопросы КР

Краткое содержание задания:
Изучение алгоритмов асимметричного шифрования и ЭЦП

Контрольные вопросы/задания:

Знать: методологию разработки системного и прикладного программного обеспечения для защиты данных	1. методика выбора алгоритма хеширования 2.Создание моделей электронной цифровой подписи

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
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: 75
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: 60
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3 семестр

Форма промежуточной аттестации: Зачет

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

1. Компетенция/Индикатор: ИД-1$_{ПК-2}$ Использует методы управления информационными ресурсами и создания информационных систем

Вопросы, задания

1.Понятие защиты информации. Какая система считается надёжной?
2.Отечественные и международные стандарты в области информационной безопасности
3.Основные критерии оценки надежности: политика безопасности и гарантированность
4.Криптографические методы защиты информации. Симметричные криптосистемы. Требования к криптографическим системам защиты информации.
5.Системы с открытым ключом. Электронная (цифровая) подпись. Алгоритмы формирования и верификации электронной цифровой подписи.

Материалы для проверки остаточных знаний

1.**Политика безопасности в системе (сети) – это комплекс:**

Ответы:

а) Руководств, требований обеспечения необходимого уровня безопасности б) Инструкций, алгоритмов поведения пользователя в сети в) Нормы информационного права, соблюдаемые в сети

Верный ответ: а) Руководств, требований обеспечения необходимого уровня безопасности

2.**Утечкой информации в системе называется ситуация, характеризуемая:**

Ответы:

а) Потерей данных в системе б) Изменением формы информации в) Изменением содержания информации

Верный ответ: а) Потерей данных в системе

3.**Наиболее распространены средства воздействия на сеть офиса:**

Ответы:

а) Слабый трафик, информационный обман, вирусы в интернет б) Вирусы в сети, логические мины (закладки), информационный перехват в) Компьютерные сбои, изменение администрирования, топологии

Верный ответ: в) Вирусы в сети, логические мины (закладки), информационный перехват

4.**Наиболее распространены угрозы информационной безопасности сети:**

Ответы:

а) Распределенный доступ клиент, отказ оборудования б) Моральный износ сети, инсайдерство в) Сбой (отказ) оборудования, нелегальное копирование данных

Верный ответ: в) Сбой (отказ) оборудования, нелегальное копирование данных

5.**ЭЦП – это:**

Ответы:

а) Электронно-цифровой преобразователь б) Электронно-цифровая подпись в) Электронно-цифровой процессор

Верный ответ: б) Электронно-цифровая подпись

6.**Когда получен спам по e-mail с приложенным файлом, следует:**

Ответы:

а) Прочитать приложение, если оно не содержит ничего ценного – удалить б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама в) Удалить письмо с приложением, не раскрывая (не читая) его

Верный ответ: в) Удалить письмо с приложением, не раскрывая (не читая) его

7.**Принципом политики информационной безопасности является принцип:**

Ответы:

а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы) б) Одноуровневой защиты сети, системы в) Совместимых, однотипных программно-технических средств сети, системы

Верный ответ: а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

8.**Принципом политики информационной безопасности является принцип:**

Ответы:

а) Усиления защищенности самого незащищенного звена сети (системы) б) Перехода в безопасное состояние работы сети, системы в) Полного доступа пользователей ко всем ресурсам сети, системы

Верный ответ: а) Усиления защищенности самого незащищенного звена сети (системы)

9.**Принципом политики информационной безопасности является принцип:**

Ответы:

а) Невозможности миновать защитные средства сети (системы) б) Усиления основного звена сети, системы в) Полного блокирования доступа при риск-ситуациях

Верный ответ: а) Невозможности миновать защитные средства сети (системы)

10.**Принципом информационной безопасности является принцип недопущения:**

Ответы:

а) Неоправданных ограничений при работе в сети (системе) б) Рисков безопасности сети, системы в) Презумпции секретности

Верный ответ: а) Неоправданных ограничений при работе в сети (системе)

11.**К основным функциям системы безопасности можно отнести все перечисленное:**

Ответы:

а) Установление регламента, аудит системы, выявление рисков б) Установка новых офисных приложений, смена хостинг-компании в) Внедрение аутентификации, проверки контактных данных пользователей

Верный ответ: а) Установление регламента, аудит системы, выявление рисков

12.**Основными источниками угроз информационной безопасности являются все указанное в списке**

Ответы:

а) Хищение жестких дисков, подключение к сети, инсайдерство б) Перехват данных, хищение данных, изменение архитектуры системы в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

Верный ответ: б) Перехват данных, хищение данных, изменение архитектуры системы

13.**Угроза информационной системе (компьютерной сети) – это:**

Ответы:

а) Вероятное событие б) Детерминированное (всегда определенное) событие в) Событие, происходящее периодически

Верный ответ: а) Вероятное событие

14. **Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

Ответы:

а) Владелец сети б) Администратор сети в) Пользователь сети

Верный ответ: а) Владелец сети

15.**Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:**

Ответы:

а) Программные, технические, организационные, технологические б) Серверные, клиентские, спутниковые, наземные в) Личные, корпоративные, социальные, национальные

Верный ответ: а) Программные, технические, организационные, технологические

16.**Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

Ответы:

а) Регламентированной б) Правовой в) Защищаемой

Верный ответ: в) Защищаемой

17.**Наиболее распространены угрозы информационной безопасности корпоративной системы:**

Ответы:

а) Покупка нелицензионного ПО б) Ошибки эксплуатации и неумышленного изменения режима работы системы в) Сознательного внедрения сетевых вирусов

Верный ответ: б) Ошибки эксплуатации и неумышленного изменения режима работы системы

18.**Основными субъектами информационной безопасности являются:**

Ответы:

а) руководители, менеджеры, администраторы компаний б) органы права, государства, бизнеса в) сетевые базы данных, фаерволлы

Верный ответ: б) органы права, государства, бизнеса

19.**К основным принципам обеспечения информационной безопасности относится:**

Ответы:

а) Экономической эффективности системы безопасности б) Многоплатформенной реализации системы в) Усиления защищенности всех звеньев системы

Верный ответ: а) Экономической эффективности системы безопасности

20.**Основными рисками информационной безопасности являются:**

Ответы:

а) Искажение, уменьшение объема, перекодировка информации б) Техническое вмешательство, выведение из строя оборудования сети в) Потеря, искажение, утечка информации

Верный ответ: в) Потеря, искажение, утечка информации

21.**Основные объекты информационной безопасности:**

Ответы:

а) Компьютерные сети, базы данных б) Информационные системы, психологическое состояние пользователей в) Бизнес-ориентированные, коммерческие системы

Верный ответ: а) Компьютерные сети, базы данных

22.**Виды информационной безопасности:**

Ответы:

а) Персональная, корпоративная, государственная б) Клиентская, серверная, сетевая в) Локальная, глобальная, смешанная

Верный ответ: а) Персональная, корпоративная, государственная

23.**Цели информационной безопасности – своевременное обнаружение, предупреждение:**

Ответы:

а) несанкционированного доступа, воздействия в сети б) инсайдерства в организации в) чрезвычайных ситуаций

Верный ответ: а) несанкционированного доступа, воздействия в сети

24.**К правовым методам, обеспечивающим информационную безопасность, относятся:**

Ответы:

а) Разработка аппаратных средств обеспечения правовых данных б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Верный ответ: в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

25.**Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

Ответы:

а) Целостность б) Доступность в) Актуальность

Верный ответ: а) Целостность

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

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: 75

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: 60

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