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

Направление подготовки/специальность: 27.04.04 Управление в технических системах

Наименование образовательной программы: Интеллектуальные технологии управления в технических системах, обработка и анализ данных

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Информационная безопасность в компьютерных системах

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Елисеев В.Л. Идентификатор: R37a37292-YeliseevVL-9b2e3978	В.Л. Елисеев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бобряков А.В. Идентификатор: R2c90f415-BobriakovAV-70dec1fa	А.В. Бобряков
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бобряков А.В. Идентификатор: R2c90f415-BobriakovAV-70dec1fa	А.В. Бобряков

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. РПК-2 Способен разрабатывать и применять информационные системы обработки и анализа данных для автоматизации процессов управления в сложных технических и организационно-технических системах

ИД-1 Демонстрирует умение организовывать экспериментальные исследования и сбор экспертной информации, проводить анализ и предварительную обработку данных с применением автоматизированных информационных систем, выбирать обоснованные способы обеспечения защиты данных

ИД-2 Может разрабатывать информационные и информационно-аналитические системы автоматизации процессов управления в сложных технических и организационно-технических системах

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Тест № 1 (Тестирование)
2. Тест № 2 (Тестирование)
3. Тест № 3 (Тестирование)
4. Тест № 4 (Тестирование)

Форма реализации: Компьютерное задание

1. Лабораторная работа № 1 (Лабораторная работа)
2. Лабораторная работа № 2 (Лабораторная работа)
3. Лабораторная работа № 3 (Лабораторная работа)
4. Лабораторная работа № 4 (Лабораторная работа)

БРС дисциплины

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Тест № 1 (Тестирование)
КМ-2 Лабораторная работа № 1 (Лабораторная работа)
КМ-3 Тест № 2 (Тестирование)
КМ-4 Лабораторная работа № 2 (Лабораторная работа)
КМ-5 Тест № 3 (Тестирование)
КМ-6 Лабораторная работа № 3 (Лабораторная работа)
КМ-7 Тест № 4 (Тестирование)
КМ-8 Лабораторная работа № 4 (Лабораторная работа)

Вид промежуточной аттестации – Экзамен.

Раздел дисциплины	Веса контрольных мероприятий, %								
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8
	Срок КМ:	3	4	7	8	11	12	14	15
Основы информационной безопасности									
Введение в информационную безопасность (ИБ).				+	+	+			+
Правовые аспекты и преступления в сфере ИБ.				+	+	+			+
Стандарты и рекомендации в сфере ИБ.	+			+	+	+			+
Управление доступом.	+	+		+	+	+	+	+	+
Основы криптографии и симметричные криптосистемы									
. Введение в криптографию.	+	+		+			+	+	
Блочные шифры и сеть Фейстеля.	+	+		+			+	+	
SP-сети.	+	+		+	+		+	+	
Односторонние функции.	+	+		+	+		+	+	
Асимметричные криптосистемы, электронная подпись и инфраструктура открытых ключей									
Свойства симметричной криптографии.	+	+		+	+		+	+	
Протокол распределения ключей Диффи-Хеллмана.	+			+		+			+
Инфраструктура открытых ключей (PKI).						+			+
Защита информации при сетевом взаимодействии									
Уровни защиты данных при их передаче по сети.		+			+	+	+	+	+
Протокол IPsec.	+	+				+	+	+	+
Средства защиты информационных и коммуникационных систем									
Объекты защиты информационных и коммуникационных систем.	+	+					+	+	
Технологии злоумышленников и уязвимости.		+			+		+	+	
Новые технологии информационной безопасности									
Облегченная криптография.	+			+					

Вес КМ:	10	15	15	15	10	10	15	10

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
РПК-2	ИД-1$_{РПК-2}$ Демонстрирует умение организовывать экспериментальные исследования и сбор экспертной информации, проводить анализ и предварительную обработку данных с применением автоматизированных информационных систем, выбирать обоснованные способы обеспечения защиты данных	Знать: основные подходы к решению задач информационной безопасности; назначение и общие принципы использования криптографических алгоритмов. Уметь: выбирать комплекс мер для защиты информации и информационных систем.	КМ-1 Тест № 1 (Тестирование) КМ-2 Лабораторная работа № 1 (Лабораторная работа) КМ-3 Тест № 2 (Тестирование) КМ-5 Тест № 3 (Тестирование) КМ-6 Лабораторная работа № 3 (Лабораторная работа) КМ-7 Тест № 4 (Тестирование) КМ-8 Лабораторная работа № 4 (Лабораторная работа)
РПК-2	ИД-2$_{РПК-2}$ Может разрабатывать информационные и информационно-аналитические системы автоматизации процессов управления в сложных технических и организационно-технических системах	Знать: возможности и ограничения средств защиты информации и информационных систем. Уметь: настраивать и использовать средства защиты информации и информационных систем.	КМ-2 Лабораторная работа № 1 (Лабораторная работа) КМ-3 Тест № 2 (Тестирование) КМ-4 Лабораторная работа № 2 (Лабораторная работа) КМ-5 Тест № 3 (Тестирование) КМ-6 Лабораторная работа № 3 (Лабораторная работа) КМ-7 Тест № 4 (Тестирование) КМ-8 Лабораторная работа № 4 (Лабораторная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест № 1

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: прохождение тестирования путем выдача студентам бланков с вопросами для тестирования, либо прохождение тестирования с помощью средств дистанционного обучения. Проверка результатов выполнения.

Краткое содержание задания:
тест включает 18 вопросов по теме «Основные понятия и положения информационной безопасности». Каждый вопрос требует выбора одного из правильных ответов, установления соответствия понятий, упорядочения последовательности действий или решения примера с вводом ответа. На ответы выделяется ограниченное время – 60 минут.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: назначение и общие принципы использования криптографических алгоритмов.	1.Установите соответствие между терминами информационной безопасности и их определениями. 2.Какие виды тайны законодательно определены в России?
Уметь: выбирать комплекс мер для защиты информации и информационных систем.	1.Как построить систему двухфакторной аутентификации? 2.Как организовать разделение доступа к файлам в операционной системе Linux?

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Лабораторная работа № 1

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: выдача студентам индивидуальных контрольных заданий. Консультации по содержанию задания. Выполнение заданий студентами. Проверка результатов выполнения.

Краткое содержание задания:
лабораторная работа по теме «Управление локальным и удаленным доступом». Цель – получить теоретические и практические навыки управления доступом в ОС Linux и ОС Windows. Теоретическая часть содержит определения основных терминов управления доступом, описание дискреционной и мандатной модели доступа. Практическая часть включает в себя пример установок доступа в ОС Linux и ОС Windows.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: возможности и ограничения средств защиты информации и информационных систем.	1.Чем различаются мандатная и ролевая модели доступа 2.Какие атрибуты управления доступом к файлу имеются в ОС Linux
Уметь: выбирать комплекс мер для защиты информации и информационных систем.	1.Установите атрибуты файла для записи и чтения владельцем и запрет любого доступа для всех остальных 2.Как узнать, имеет ли пользователь доступ к файлу, как член группы

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Тест № 2

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 15

Процедура проведения контрольного мероприятия: выдача студентам индивидуальных контрольных заданий. Консультации по содержанию задания. Выполнение заданий студентами. Проверка результатов выполнения.

Краткое содержание задания:

тест включает 24 вопроса по теме «Симметричные криптографические алгоритмы». Каждый вопрос требует выбора одного из правильных ответов, установления соответствия понятий, упорядочения последовательности действий или решения примера с вводом ответа. На ответы выделяется ограниченное время – 60 минут.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: назначение и общие принципы использования криптографических алгоритмов.	1.Укажите условия, при которых идеальный шифр Вернама (одноразовый блокнот) обладает абсолютной криптостойкостью. 2.Хэш-функцию с ключом можно использовать в качестве электронной подписи сообщения. Каким основным недостатком обладает такой способ?
Уметь: настраивать и использовать средства защиты информации и информационных систем.	1.Зашифруйте шифром Вернама указанный открытый текст приведенным ниже ключом. 2.Зашифруйте шифром перестановки указанный открытый текст приведенным ниже ключом.

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Лабораторная работа № 2

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: выдача студентам индивидуальных контрольных заданий. Консультации по содержанию задания. Выполнение заданий студентами. Проверка результатов выполнения.

Краткое содержание задания:

лабораторная работа по теме «Защита сетевого соединения». Цель - получить практические навыки настройки межсетевого экрана (фаервола), а также настройки переадресации сетевых соединений и трансляции адресов (NAT).

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: возможности и ограничения средств защиты информации и информационных систем.	1.Можно ли с помощью межсетевого экрана в Linux запретить работу с Яндекс.Диск, сохранив возможность работы с Яндекс.Почта 2.Для чего предназначен режим NAT
Уметь: настраивать и использовать средства защиты информации и информационных систем.	1.Как установить запрет на любый входящие сетевые соединения 2.Приведите пример правила, реализующего статическую трансляцию адреса и порта

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-5. Тест № 3

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: прохождение тестирования путем выдача студентам бланков с вопросами для тестирования, либо прохождение тестирования с помощью средств дистанционного обучения. Проверка результатов выполнения.

Краткое содержание задания:
тест включает 23 вопроса по теме «Асимметричные криптографические алгоритмы и PKI». Каждый вопрос требует выбора одного из правильных ответов, установления соответствия понятий, упорядочения последовательности действий или решения примера с вводом ответа. На ответы выделяется ограниченное время – 90 минут.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: основные подходы к решению задач информационной безопасности;	1.Даёт ли возможность публикации открытого ключа отправлять секретные сообщения владельцу соответствующего закрытого ключа? 2.Постройте в правильном порядке последовательность шагов при проверке электронной подписи с указанным сертификатом.
Уметь: настраивать и использовать средства защиты информации и информационных систем.	1.Вычислите общий секретный ключ по протоколу Диффи-Хелмана. 2.Зашифруйте сообщение шифром RSA указанным открытым ключом и проверьте корректность расшифровки приватным ключом.

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-6. Лабораторная работа № 3

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: выдача студентам индивидуальных контрольных заданий. Консультации по содержанию задания. Выполнение заданий студентами. Проверка результатов выполнения.

Краткое содержание задания:
лабораторная работа по теме «Анализ безопасности Web-приложений». Цель – получить практические навыки анализа Web-приложений на предмет наличия основных уязвимостей. Теоретическая часть содержит описание основных уязвимостей и атак на Web-приложения, таких как SQL injection, межсайтовый скриптинг (XSS), подбор паролей, обратный путь в директориях, прямой доступ к объектам, некорректная настройка механизмов безопасности и использование компонентов с известными уязвимостями. Практическая часть включает настройку программного инструмента тестирования Web-приложений Burp Suite и проведение с его помощью атак на специальные сайты, используемые для изучения ИБ.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: возможности и ограничения средств защиты информации и информационных систем.	1.Что такое атака SQL injection? 2.Опишите технологию атаки XSS.
Уметь: выбирать комплекс мер для защиты информации и информационных систем.	1.Проведите атаку подбора пароля. 2.Проведите атаку обратного пути в директорию.

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-7. Тест № 4

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: прохождение тестирования путем выдача студентам бланков с вопросами для тестирования, либо прохождение тестирования с помощью средств дистанционного обучения. Проверка результатов выполнения.

Краткое содержание задания:
тест включает 24 вопроса по теме «Технологии информационной безопасности». Каждый вопрос требует выбора одного из правильных ответов, установления соответствия понятий, упорядочения последовательности действий или решения примера с вводом ответа. На ответы выделяется ограниченное время – 120 минут.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: возможности и ограничения средств защиты информации и информационных систем.	1.Установите правильное соответствие прикладной задачи и используемого протокола. 2.Какие тенденции и технологии снижают эффективность периметрового подхода к защите корпоративных информационных систем?

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: выбирать комплекс мер для защиты информации и информационных систем.	1.Предложите комплекс защитных технологий на шлюзе индустриальной сети АСУТП. 2.Выберите подходящий криптографический протокол для описанной прикладной задачи.

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-8. Лабораторная работа № 4

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Лабораторная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: выдача студентам индивидуальных контрольных заданий. Консультации по содержанию задания. Выполнение заданий студентами. Проверка результатов выполнения.

Краткое содержание задания:
лабораторная работа по теме «Социальная инженерия». Цель – получить теоретические и практические навыки социальной инженерии и методов противодействия. Теоретическая часть содержит определения основных терминов социальной инженерии, перечень техник и мер противодействия. Практическая часть включает в себя пример использования техник социальной инженерии: поиска информации, подготовки и проведения атаки.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: основные подходы к решению задач информационной безопасности;	1.Что такое фишинг? 2.Опишите техники, используемые для внедрения программ в защищенный периметр.
Уметь: настраивать и использовать средства защиты информации и информационных систем.	1.Проведите поиск номеров кредитных карт на сайте. 2.Исследуйте локальную сеть на

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	наличие принтеров.

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1) Правовые основы защиты информации. Виды тайны и законодательные акты по её охране. Регуляторы информационной безопасности в России и их специализация.
2) Недостатки сети Фейстеля. Шифр типа SP-сеть.

Процедура проведения

Процедура проведения экзамена определяется текущим положением об экзаменах и зачетах НИУ «МЭИ». Студент получает билет с 2 вопросами по лекционному курсу. Время на подготовку ответа – 60 мин. Далее он отвечает на поставленные вопросы, а также на дополнительные вопросы преподавателя, принимающего зачет. По результатам ответов выставляется оценка за экзамен, которая сообщается студенту.

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

1. Компетенция/Индикатор: ИД-1$_{РПК-2}$ Демонстрирует умение организовывать экспериментальные исследования и сбор экспертной информации, проводить анализ и предварительную обработку данных с применением автоматизированных информационных систем, выбирать обоснованные способы обеспечения защиты данных

Вопросы, задания

1.Модульная арифметика. Группы вычетов. Функция Эйлера. Теорема Эйлера.
2.Практические аспекты RSA: назначение, вычислительная сложность, стойкость.
3.Структура сертификата X.509.

Материалы для проверки остаточных знаний

1.Что удостоверяет Удостоверяющий Центр PKI?
Ответы:
1. Корректность работы асимметричных криптографических алгоритмов пользователя
2. Наличие пары закрытого и открытого ключа у пользователя
3. Идентификацию пользователя, владеющего закрытым ключом
4. Разрешение совершать операции подписи в рамках данного домена доверия

Верный ответ: 3

2.Укажите, какие свойства отличают криптографическую хэш-функцию от обычной
Ответы:
1. Преобразует неограниченную последовательность байтов в значение в ограниченном диапазоне
2. Не позволяет восстановить входную последовательность по значению хэш-функции
3. Для последовательности байт должно быть вычислительно трудно подобрать другую последовательность, дающую то же значение хэш-функции
4. По значению хэш-функции должно быть вычислительно трудно восстановить возможные последовательности из которых она могла быть получена
5. Алгоритм вычисления должен быть стандартизован
6. Должно быть вычислительно трудно найти две последовательности, дающие одинаковый хэш

Верный ответ: 3,4,6

3.Укажите возможные варианты аутентификации при установлении TLS сессии

Ответы:

1. Без аутентификации
2. Парольная аутентификация
3. Аутентификация клиентом сервера по его сертификату
4. Аутентификация сервером клиента по его сертификату
5. Двухсторонняя аутентификация клиента и сервера по их сертификатам

Верный ответ: 3,5

4.Локальная сеть промышленного объекта состоит из управляющего компьютера SCADA системы и множества PLC, управляющих технологическими процессами. Эта сеть через шлюз подключена к Интернет, для того, чтобы можно было осуществлять мониторинг и управление из головного офиса предприятия. Какие защитные технологии целесообразно установить на шлюзе?

Ответы:

1. Межсетевой экран
2. Криптошлюз
3. Сетевой IDS
4. Сетевой IPS
5. NGFW
6. WAF
7. SOC
8. Антивирус

Верный ответ: 1,2,4

5.Частотный анализ позволяет дешифровать

Ответы:

1. шифр подстановки
2. шифр перестановки

Верный ответ: 1

6.Выберите варианты однофакторной аутентификации

Ответы:

1. электронный ключ для замка ("таблетка")
2. карта Тройка
3. банковская карта (при снятии денег в банкомате)
4. криптотокен для доступа на сайт Госуслуги
5. отпечаток пальца
6. имя пользователя и пароль
7. имя пользователя, пароль и код из SMS

Верный ответ: 1,2,5,6

7.По какой причине квантовое распределение ключей обеспечивает защиту от атак на криптографию с помощью квантового компьютера?

Ответы:

1. Квантовый компьютер не имеет преимуществ перед квантовыми протоколами, а только перед классическими
2. Частая смена ключей шифрования защищает от снижения стойкости классических симметричных шифров
3. Запрет клонирования квантовых частиц не позволяет скопировать секретный ключ, передаваемый по квантовому протоколу

Верный ответ: 2

2. Компетенция/Индикатор: ИД-2$_{РПК-2}$ Может разрабатывать информационные и информационно-аналитические системы автоматизации процессов управления в сложных технических и организационно-технических системах

Вопросы, задания

1.Шифр ГОСТ Р 34.12-2018 «Магма» и его параметры.

2.Структура пакетов AH и ESP. Туннельный и транспортный режимы.

Материалы для проверки остаточных знаний

1.В каком из полей сертификата находится информация о способе, как узнать, что этот сертификат не отозван?

Ответы:

1. Issuer
2. Valid from
3. AuthorityInfoAccess
4. CRLDistributionPoints
5. ExtendedKeyUsages
6. KeyUsage

Верный ответ: 4

2.Вычислите криптостойкость (число переборов) идеальной хэш-функции, дающей значение длиной 16 бит

Верный ответ: 256

3.На чем основан подход к легальной инспекции защищенного трафика - так называемый легальный Man-in-the-Middle?

Ответы:

1. На подборе криптографического ключа, используемого для шифрования
2. На знании паролей всех пользователей корпоративной сети
3. На установке в хранилища корневых сертификатов корпоративных компьютеров корневого сертификата корпоративного УЦ
4. На организации проксирования всего исходящего трафика корпоративной сети на шлюзе

Верный ответ: 3

4.Выберите правильное определение ключевого расписания

Ответы:

1. Время смены мастер-ключа с целью контроля нагрузки на ключ
2. Порядок смены вектора инициализации (IV) в процессе шифрования большого количества блоков
3. Порядок смены раундовых ключей в многораундовом блочном шифре

Верный ответ: 3

5.Подберите подходящие примеры понятию "уязвимость":

Ответы:

1. Низкая квалификация в информационной безопасности сотрудников, обслуживающих информационную систему предприятия
2. Наличие многочисленных хакерских инструментов для проникновения в информационные системы предприятий
3. Простой пароль администратора главного сервера предприятия
4. Бушующая в мире эпидемия вируса-шифровальщика WannaCry
5. Старая версия Windows, подверженная атаке Ping-of-the-Death, установленная на компьютере бухгалтера, не подключенном к локальной сети

Верный ответ: 1,3

6.Относится ли АСУ ТП кондитерской фабрики к объектам критической информационной инфраструктуры?

Ответы:

1. Да
2. Нет

Верный ответ: 2

7.Куда в обязательном порядке передается информация о компьютерных атаках на объекты критической информационной инфраструктуры в рамках системы ГосСОПКА?

Ответы:

1. Ситуационный центр Администрации Президента России
2. Национальный координационный центр по компьютерным инцидентам при ФСБ России
3. Центральный банк России
4. Ситуационный центр при ФСТЭК России

Верный ответ: 2

II. Описание шкалы оценивания

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка 5 «отлично» выставляется, если задание выполнено в полном объеме или имеет несущественные погрешности.

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 4 «хорошо» выставляется, если задание выполнено в полном объеме, но имеется не более 2 ошибок.

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Оценка 3 «удовлетворительно» выставляется, если задание выполнено не менее, чем на 60% или имеется не более 4 ошибок.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 «неудовлетворительно» выставляется, если задание выполнено менее, чем на 60%, имеется более 4 ошибок или полностью отсутствует ответ на один из 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.