МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

Естественнонаучный факультет

Кафедра «Информатика и информационные технологии»

«Утверждаю»
«28» августа2024 г.
Зав. кафедрой к.э.н., доцент

Лешукович А.И.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

Криптографические методы зашиты информации

Направление подготовки - 09.03.03 “Прикладная информатика”
Наименование профиля – Программная инженерия
Форма подготовки - очная
Уровень подготовки - бакалавриат

Душанбе - 2024

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Криптографические методы зашиты информации»

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**Знать:** принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.	устный опрос
		Уметь: принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.	устный опрос
		Владеет: навыками научного поиска и практической работы с информационными источниками; методами принятия решений	устный опрос

1) Общепрофессиональные компетенции выпускников и индикаторы их достижения

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	**Знать:** основы математики, физики, вычислительной техники и программирования.	устный опрос
		Умеет: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	Эссе
		Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности.	устный опрос
ОПК-6	Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования	**Знать:** - основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования.	устный опрос
		Умеет: - применять методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия	к/работа

		решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий.	
		Владеть: - навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий.	устный опрос

2) Профессиональные компетенции: проектная деятельность:

Код	**Формируемая компетенция**	**Содержание этапа формирования компетенции**	**Форма контроля**
ПК-5	Способность моделировать прикладные (бизнес) процессы и предметную область.	**Знать:** - способы организации розничной торговли в Интернет; модели организации закупок через Интернет; основные группы услуг, оказываемых через Интернет и особенности их оказания; способы оплаты товаров и услуг в электронной коммерции; методологические основы планирования бизнеса; основные методы и технологию бизнес-планирования; место и роль бизнес-плана при управлении компаниями; методические особенности составления различных типов бизнес-планов используемых при управлении бизнесом; основные классы систем электронной коммерции; способы организации розничной торговли в Интернет; основные методы стимулирования продаж в Интернет-магазине; модели организации закупок через Интернет; основные группы услуг, оказываемых через Интернет и особенности их оказания; способы оплаты товаров и услуг в электронной коммерции; Российское, таджикское и международное законодательство в области электронной коммерции.	эссе
		Уметь:- использовать навыки менеджера в процессе управления проектной группой с использованием ИКТ; использовать методы современного бизнес-планирования как базовой технологии управления бизнесом; составлять различные разделы бизнес-планов; проводить анализ деятельности предприятия и выявлять участки производства,	устный опрос

		нуждающиеся в реинжиниринге; осуществлять сбор и подготовку аналитических данных для оценки эффективности рекламы в Интернет; изучать и анализировать методы предоставления различных услуг в Интернет; создавать веб-страницы и сайты, в том числе с активным содержимым, создавать графический материал для наполнения страниц, готовить текстовый материал для размещения на странице, настраивать программное обеспечение веб-серверов.	
		Владеть: - методикой составления управленческого бизнес-плана; инструментами создания бизнес-моделей и моделирования новых бизнес-процессов; средствами для разработки веб-приложений	

Перечень оценочных средств

МОУ ВО РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Естественнонаучный факультет

Кафедра информатики и информационных технологий

по «Криптографические методы зашиты информации»

наименование дисциплины (модуля)

09.03.03

шифр/направление

«Прикладная информатика»

наименование профиля / специализации / программы

очная

форма обучения

Российско-Таджикский (Славянский) Университет
Кафедра «Информатики и информационных технологий »
Экзаменационный билет по дисциплине «Криптографические методы зашиты информации»

направление «Прикладная информатика»

№ 1

1. Основные понятия и определения, относящиеся к информационной безопасности.
2. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.
3. Задание

Утверждено на заседании кафедры, протокол №1 от 29 августа 2024 г.
Зав. кафедрой _____ /Лешукович А.И./

№ п/п	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1.	Работа в сети с информационными ресурсами	Средства контроля как устный опрос преподавателя с обучающимся на определенные темы, связанные с изучаемой дисциплиной. Задания к контрольным работам, текущие и рубежные тесты. Устный опрос. Контрольные работы, коммуникативные задачи для зачета	Вопросы по темам

2.	Беседа	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
3.	Решения задач	полный и корректный анализ условия поставленной задачи; - правильно и обоснованно определена структура алгоритма;	Проверка условия поставленной задачи
4.	Поиск информации в сети	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Задания к контрольным работам, текущие и рубежные тесты. Устный опрос. Контрольные работы, коммуникативные задачи для зачета	Фонд тестовых заданий
5.	Реферат	рассматриваемые понятия определяются четко и полно, приводятся соответствующие примеры, - используемые понятия строго соответствуют теме, - самостоятельность выполнения работы Анализ и оценка информации - грамотно применяется категория анализа, - умело используются приемы сравнения и обобщения для анализа взаимосвязи понятий и явлений, - изложение ясное и четкое, - приводимые доказательства	Вопрос по темам

		логичны -приводятся различные точки зрения и их личная оценка (при необходимости).	
6.	Решения индивидуальных вариантов задач	полный и корректный анализ условия поставленной задачи; - правильно и обоснованно определена структура алгоритма.	Проверка условия поставленной задачи
7.	Разработка программ	Средства проверки умений применять полученные знания для решения задач определенного типа по теме или разделу. Задания к контрольным работам, текущие и рубежные тесты. Устный опрос. Контрольные работы, коммуникативные задачи для зачета	Комплект контрольных
8.	Опрос	Продукт самостоятельной работы обучающихся с помощью программы Power Point, излагать определенные темы по дисциплине. Подготовка рефератов, КСР.	Темы презентации

МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»
направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки -бакалавриат
форма обучения - очная
Кафедра информатики и информационных технологий

УСТНЫЙ ОПРОС

по дисциплине «Криптографические методы зашиты информации»

1. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности.
2. Классификация атак; модели сетевой безопасности и безопасности информационной системы.
3. Шифры Цезаря.
4. Шифры Виженера.
5. Шифры Полибия.
6. Шифры Гронсфельда.
7. Шифры Плейфер.
8. Дисковые шифраторы.
9. Шифр Сцитало.
10. Шифр маршрутной перестановки.
11. Шифр вертикальной перестановки.
12. Шифр поворотная решётка (Кардано).
13. Шифр двойной перестановки.
14. Системы с открытым ключом.
15. Понятия однонаправленной функции и однонаправленной функции с лазейкой.
16. Функции дискретного логарифмирования и основанные на ней алгоритмы.
17. Схема Диффи-Хеллмана.
18. Шифр Шамира.
19. Схема Эль-Гамаля.
20. Схема RSA.
21. Арифметика остатков и теория сравнений.
22. Малая теорема Ферма.
23. Наибольший общий делитель.
24. Обобщенный алгоритм Евклида.
25. Инверсия по модулю m.
26. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext.
27. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования.
28. Сеть Фейштеля.

29. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ.
30. Схема шифрования алгоритма DES.
31. Режимы использования DES.
32. Криптостойкость алгоритма DES.
33. Увеличение криптостойкости DES.
34. Алгоритмы Rijndael и RC6.
35. Математические понятия, лежащие в основе алгоритма Rijndael.
36. Описание AES. Алгоритм обработки ключа. Варианты алгоритма.
37. Криптостойкость.
38. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой.
39. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых.
40. Алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

Критерии оценивания устного опроса:

Оценкой **отлично** оценивается ответ, который показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.

Оценкой **хорошо** оценивается ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

Оценкой **удовлетворительно** оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.

Оценкой **неудовлетворительно** оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»
направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки - бакалавриат
форма обучения - очная
Кафедра информатики и информационных технологий

Темы самостоятельных работ

1. Общие вопросы информационной безопасности. Основные понятия и определения, относящиеся к информационной безопасности.
2. Классификация несанкцированных атак.
3. Модели сетевой безопасности и безопасности информационной системы.
4. Шифры замены.Основные понятия и определения.
5. Исследования Шеннона в области криптографии.
6. Не раскрываемость шифра Вернама.
7. Шифры перестановки. Основные понятия и определения.
8. Шифр двойной перестановки. Асимметричные системы шифрования (системы с открытым ключом).
9. Понятия однонаправленной функции и однонаправленной функции с лазейкой.
10. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана.
11. Шифр Шамира. Схема Эль-Гамаля.
12. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.
13. Элементы теории чисел. Арифметика остатков и теория сравнений. Малая теорема Ферма.
14. Наибольший общий делитель. Обобщенный алгоритм Евклида.
15. Алгоритмы симметричного шифрования. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext.
16. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования.

17. Сеть Фейштеля.
18. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ.
19. Схема шифрования алгоритма DES.Режимы использования DES.
20. Криптостойкость алгоритма DES. Увеличение криптостойкости DES.
21. Стандарт криптографической защиты 21 века(AES).
22. Алгоритмы Rijndael и RC6.
23. Математические понятия, лежащие в основе алгоритма Rijndael.
24. Структура шифра. Описание AES.
25. Алгоритм обработки ключа. Варианты алгоритма. Криптостойкость.
26. Криптография с использованием эллиптических кривых.
27. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой.
28. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма шифрования с открытым ключом получателя на эллиптических кривых.
29. Безопасность современных сетевых технологий.
30. Способы несанкционированного доступа к информации в компьютерных сетях.
31. Классификация способов несанкционированного доступа и жизненный цикл атак.
32. Способы противодействия несанкционированному межсетевому доступу.

Критерии оценки выполнения самостоятельной работы.

В основу разработки балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Студентам выставляются следующие баллы за выполнение задания к ПК:

- оценка «отлично» (10 баллов): контрольные тесты, а также самостоятельно выполненные семестровые задания, выполненные полностью и сданные в срок в соответствии с предъявляемыми требованиями;

- оценка «хорошо» (8-9 баллов): задание выполнено и в целом отвечает предъявляемым требованиям, но имеются отдельные замечания в его оформлении или сроке сдачи;

- оценка «удовлетворительно» (6-7 баллов): задание выполнено не до конца, отсутствуют ответы на отдельные вопросы, имеются отклонения в объеме, содержании, сроке выполнения;

- оценка «неудовлетворительно» (5 и ниже): отсутствует решение

задачи, задание переписано (скачано) из других источников, не проявлена самостоятельность при его выполнении.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;
- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;
- выполнение контрольной работы и обсуждение результатов;
- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;

МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»

направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки - бакалавриат
форма обучения - очная
Кафедра информатики и информационных технологий

Темы рефератов и письменных работ (рефератов, письменных работ)

1. Криптография в Древнем мире.
2. Исторические методы стеганографии.
3. Криптография в Средние века и в Новое время.
4. Шифр Марии Стюарт, королевы Шотландии.
5. Дисковые шифраторы.
6. Криптография на рубеже 19-20 вв.
7. История российской криптографии.
8. Шифрование аналогового сигнала.
9. Взлом «Энигмы».
10. Клод Шеннон и его вклад в криптографию.
11. Алан Тьюринг и его вклад в криптографию.
12. Лауреаты премии Алана Тьюринга.
13. Первый блочный шифр – Lucifer.
14. Современная стеганография – математические методы.
15. Электронные водяные знаки.
16. Ади Шамир и его вклад в криптографию.
17. Шифрование и аутентификация в современных беспроводных сетях вязи.
18. Парольные схемы аутентификации.
19. Одноразовые пароли.
20. Протоколы с нулевым разглашением.

21. Информационные геополитические и экономические процессы современного общества.
22. Программно-аппаратные средства обеспечения ИБ функционирования организаций.
23. Международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации.
24. Организационные, физико-технические, информационные и программно-математические угрозы.
25. Классификация способов несанкционированного доступа и жизненный цикл атак.
26. Способы противодействия несанкционированному межсетевому доступу.

Критерии оценки реферата:

Оценка **«отлично»** выставляется за реферат, который носит исследовательский характер, содержит грамотно изложенный материал, с полностью раскрытой темой и соответствующими обоснованными выводами; оценка «хорошо» выставляется за грамотно выполненный во всех отношениях реферат при наличии небольших недочетов в его содержании или оформлении;

Оценка **«удовлетворительно»** выставляется за реферат, который удовлетворяет всем предъявляемым требованиям, но отличается поверхностностью, в нем просматривается непоследовательность, несвязанность и нелогичность изложения материала, представлены необоснованные выводы;

Оценка **«неудовлетворительно»** выставляется за реферат, который не соответствует принципу научности, не носит исследовательского характера, не содержит анализа источников и подходов по выбранной теме, выводы носят декларативный характер.

Студент, не представивший готовый реферат или представивший работу, которая была оценена на «неудовлетворительно», не допускается к сдаче зачета по дисциплине.

МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»

направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки - бакалавриат
форма обучения - очная
Кафедра информатики и информационных технологий

Основной курс

Тема 1. Виды криптографических преобразований информации. Основные понятия и определения криптографии. Принципы криптографической защиты информации. История развития криптографии. Шифрующие криптографические преобразования. Односторонние функции. Хэш - функции. Электронная цифровая подпись. Генераторы псевдослучайных последовательностей. Шифры перестановки. Шифры замены (подстановки). Шифры гаммирования. Композиционные блочные шифры и принципы их построения. Криптоанализ и виды криптоаналитических атак.

Тема 2. Алгоритмы симметричного шифрования. Основные понятия,

относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Схема шифрования алгоритма DES. Режимы использования DES. Криптостойкость алгоритма DES. Увеличение криптостойкости DES

Тема 3. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Описание AES. Алгоритм обработки ключа. Варианты алгоритма. Криптостойкость.

Тема 4.Хэш-функции и аутентификация сообщений. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

Тема 5. Цифровая подпись. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.

Тема 6. Криптография с использованием эллиптических кривых. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

Критерии оценки:

«Зачтено» выставляется, если студент:

1. знает фактический материал по дисциплине;
2. владеет понятиями системы знаний по дисциплине, умеет определять сущность понятий, выделять главное в учебном материале;
3. умеет самостоятельно находить эффективный способ решения поставленной задачи;
4. умеет использовать знания в стандартных и нестандартных ситуациях, логично и доказательно излагать учебный материал, владеет точной речью;
5. умеет аргументированно отвечать на вопросы, вступать в диалоговое общение.

«Не зачтено» выставляется, если студент:

1. не имеет знаний по дисциплине, представления по вопросу;
2. не понимает материал по дисциплине;
3. не умеет связать теорию и практику;
4. не умеет решать задачи;
5. не может сформулировать свою точку зрения, ввиду наличия коммуникативных «барьеров»

МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»

направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки - бакалавриат
форма обучения - очная
Кафедра информатики и информационных технологий

Структура и содержание практической части курса (16 часов)

1. Программная реализация шифра Цезаря. Одноалфавитная замена. Пропорциональные шифры (2 часа).
2. Методы перестановки. Понятие композиционного шифра. Программная реализация шифра Вижинера (2 часа).
3. Шифры многобуквенной замены на примере шифра Хилла (2 часа).
4. Обобщенный алгоритм Евклида. Инверсия по модулю m (2 часа)..
5. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана. Шифр Шамира. Схема Эль-Гамаля (2 часа)..
6. Сеть Фейстеля. DES-шифрование (2 часа).
7. Стандарт симметричного шифрования AES RIJNDAEL (2 часа).
8. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых (2 часа).

Критерии оценки практических работ

Оценку «зачтено» заслуживает обучающийся, обнаруживший всесторонние, систематические и глубокие знания по вопросам содержания практических заданий; показавший умение свободно логически анализировать литературу и нормативно-правовые документы, в процессе подготовки практических заданий (по необходимости), правильно оценивать и четко, сжато, ясно излагать свою точку зрения по проблемам, заявленным в практических заданиях; проявивший творческие способности в процессе изложения самостоятельно подготовленного материала; продемонстрировавший в процессе изложения заданного материала на аудиторных занятиях твердые навыки и умение приложить теоретические знания к практическому их применению в профессиональной деятельности.

Критерии оценки знаний при форме контроля «дифференцированный зачет», «экзамен»:

Оценка «5» («отлично») соответствует следующей качественной характеристике: изложено (письменно/устно) правильное понимание лабораторных и практических заданий, подробное описание предмета содержания, приведены и раскрыты в тезисной форме основные понятия, приведены результаты, относящиеся к результатам практического задания, представлен документ, содержание которого раскрыто полно, профессионально, грамотно.

Оценка «4» («хорошо») соответствует следующей качественной характеристике: изложено правильное понимание вопросов практического

задания, дано достаточно подробное описание предмета содержания, приведены и раскрыты в тезисной форме основные понятия, приведены результаты, относящиеся к результатам практического задания, ошибочных положений нет. Выставляется обучающемуся, обнаружившему полное знание материала, грамотно и, по существу, отвечающему на вопрос проверяющего и не допускающему при этом существенных неточностей.

Оценка «3» («удовлетворительно») выставляется обучающемуся: обнаружившему опыт проведения практических работ в объеме, необходимом для реализации рабочей учебной программы, но допустившему неточности в представлении результатов, оформлении при выполнении отчетов о лабораторных и практических заданий, но обладающими необходимыми знаниями для их устранения под руководством педагогического работника.

Оценка «2» («неудовлетворительно») выставляется обучающемуся, обнаружившему принципиальные ошибки в выполнении предусмотренных рабочей программой дисциплины в части выполнения практических работ.

МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»

направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки - бакалавр
форма обучения - очная
Кафедра информатики и информационных технологий

Структура и содержание КСР (8 часов).

1. Многоалфавитные подстановки, методы гаммирования (2 часа).
2. Поточные шифры (2 часа).
3. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости (2 часа).
4. Аутентификация документов на основе электронно-цифровой подписи (2 часа).

Оценки	Баллы	Критерии оценки качества результатов КСР студентов
Превосходно	10	-систематизированные, глубокие и полные знания (в т.ч. устные либо письменные ответы) по всем вопросам задания (в т.ч. темы, раздела), а также по основным вопросам, выходящим за ее пределы; – точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы; – безупречное владение инструментарием темы (раздела) (методами комплексного анализа, техникой информационных технологий), умение его эффективно использовать в постановке и решении научных и профессиональных задач; – выраженная способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; – полное и глубокое усвоение содержания основной и дополнительной литературы, рекомендованной преподавателем; – творческая самостоятельная работа при выполнении КСР; – высокий уровень культуры исполнения задания (оформление работы в соответствии с требованиями, соблюдение установленных сроков представления работы на проверку и т.п.).
Отлично	9	-систематизированные, глубокие и полные знания (в т.ч. устные либо письменные ответы) по всем вопросам задания (в т.ч. темы, раздела); – точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы; – владение инструментарием темы (раздела) (методами комплексного анализа, техникой информационных технологий), умение его эффективно использовать в постановке и решении научных и профессиональных задач; – способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках заданной темы (раздела); – полное и глубокое усвоение содержания основной и дополнительной литературы, рекомендованной преподавателем; – творческая самостоятельная работа при выполнении КСР; – высокий уровень культуры исполнения задания (оформление работы в соответствии с требованиями, соблюдение

		установленных сроков представления работы на проверку и т.п.).
Почти отлично	8	-систематизированные, глубокие и полные знания (в т.ч. устные либо письменные ответы) по всем вопросам задания (в т.ч. темы, раздела); – использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; –владение инструментарием темы (раздела) (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; – способность самостоятельно решать сложные проблемы в рамках заданной темы (раздела); – усвоение содержания основной и дополнительной литературы, рекомендованной преподавателем; – самостоятельная работа при выполнении КСР; – высокий уровень культуры исполнения задания (оформление работы в соответствии с требованиями, соблюдение установленных сроков представления работы на проверку и т.п.).
Очень хорошо	7	-систематизированные, глубокие и полные знания (в т.ч. устные либо письменные ответы) по всем вопросам задания (в т.ч. темы, раздела); – использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; –владение инструментарием темы (раздела), умение его использовать в постановке и решении научных и профессиональных задач; – способность самостоятельно решать сложные проблемы в рамках заданной темы (раздела); – усвоение содержания основной и дополнительной литературы, рекомендованной преподавателем; – самостоятельная работа при выполнении КСР; – высокий уровень культуры исполнения задания (оформление работы в соответствии с требованиями, соблюдение установленных сроков представления работы на проверку и т.п.).
Хорошо	6	- достаточно полные и систематизированные знания (в т.ч. устные либо письменные ответы) по всем

		вопросам задания (в т.ч. темы, раздела); – использование необходимой научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; – владение инструментарием темы (раздела), умение его использовать в постановке и решении научных и профессиональных задач; – способность самостоятельно применять типовые решения в рамках заданной темы (раздела); – усвоение содержания основной литературы, рекомендованной преподавателем; – самостоятельная работа при выполнении КСР; – хороший уровень культуры исполнения задания (несущественные замечания по оформлению работы, соблюдение установленных сроков представления работы на проверку и т.п.).
Почти хорошо	5	- достаточные знания (в т.ч. устные либо письменные ответы) в объеме задания (в т.ч. темы, раздела); – использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы; – владение инструментарием темы (раздела), умение его использовать в постановке и решении научных и профессиональных задач; – способность самостоятельно применять типовые решения в рамках заданной темы (раздела); – усвоение основной литературы, рекомендованной преподавателем; – самостоятельная работа при выполнении КСР; – средний уровень культуры исполнения задания (несущественные замечания по оформлению работы, несоблюдение установленных сроков представления работы на проверку и т.п.).
Удовлетвори-тельно (зачтено)	4	-достаточные знания (в т.ч. устные либо письменные ответы) в объеме задания (в т.ч. темы, раздела); – использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок; – владение инструментарием темы (раздела), умение его использовать в решении стандартных (типовых) задач; – умение под руководством преподавателя решать стандартные (типовые) задачи в рамках заданной темы (раздела); – знание содержания основной литературы, рекомендованной преподавателем;

		–самостоятельная работа при выполнении КСР; – допустимый уровень культуры исполнения задания (существенные замечания по оформлению работы, несоблюдение установленных сроков представления работы на проверку и т.п.).
Неудовлетво-рительно (незачтено)	3	- недостаточно полный объем знаний (в т.ч. устные либо письменные ответы) в объеме задания (в т.ч. темы, раздела); – знание содержания части основной литературы, рекомендованной преподавателем; – использование научной терминологии, изложение ответа на вопросы с существенными логическими ошибками; – слабое владение инструментарием темы (раздела); – некомпетентность в решении стандартных (типовых) задач; – низкий уровень культуры исполнения задания (оформление работы не в соответствии с требованиями, несоблюдение установленных сроков представления работы на проверку и т.п.).

Критерии оценки качества результатов КСР студентов
МОУ ВО «Российско-Таджикский (Славянский) университет»
по дисциплине «Криптографические методы зашиты информации»

направление подготовки- 09.03.03. «Прикладная информатика»
уровень подготовки - бакалавриат
форма обучения - очная
Кафедра Информатики и информационных технологий

Примерные тестовые задания (первые 10):

1. Что означает термин «многократное шифрование» применительно к блочным шифрам?

1) повторное применение алгоритма шифрования к зашифрованному тексту с теми же ключами;
2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
3) увеличение числа этапов шифрования открытого текста.

2.Гаммирование чаще всего осуществляется:(несколько верных ответов)

1) по модулю 2, если открытый текст представляется в виде бинарной последовательности;
2) по модулю 256, если открытый текст представляется в виде последовательности байтов;
3) по модулю 16, если открытый текст представлен в цифровом виде;

4) по модулю 10, если открытый текст представлен в виде последовательности цифр, что иногда делается в ручных системах шифрования.

3. Основой построения большинства поточных шифров являются:

1) генераторы псевдослучайных чисел, в частности, различные комбинации регистров сдвига;
2) схемы суммирования по mod 16;
3) таблицы подстановок.

4. Зашифрованный методом перестановки открытый текст: «Сертификаты ключей ЭЦП», при ключе длинной 7, и перестановке: {4132756}, имеет вид:

1) тСреиифыктал кйюечЦ Э П ;
2) юклчТи ЭСЦ еиртфаикт ы ;
3) чКилют рСекиафиЭтПы Ц .

5. Зашифровать слово «выборочность» методом перестановки с ключом {3142}:

1) бвоычрнотоьс ; 2) ыовбрчоонсьт ; 3) ывброончотсь .

6. Зашифровать открытый текст – «field» методом Виженера, ключ – «moon» (алфавит – латиница):

1) rwcup; 2) rwsyp;3) rvsyp

7. Частотный анализ может эффективно применяться для дешифрования шифров:

1) перестановки; 2) многоалфавитной замены;3) простой замены.

8. Какие меры практической стойкости шифра относительно метода криптоанализа вы можете выделить: (несколько верных ответов)

1) вероятность дешифрования за время, не превосходящее Т;
2) среднее время, необходимое для дешифрования шифра;
3) скорость дешифрования шифра.

9. Какие шифры можно называть имитостойкими?

1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

10. Какие шифры можно называть помехоустойчивыми?

1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

Итоговые оценки студентов

Буквенное обозначение итоговых оценок студентов и их цифровые эквиваленты:

Буквенная оценка	Цифра	Общий балл	Традиционная оценка
A	4	95≤A≤100	отлично
A-	3,67	90≤A-<95	

B+	3,33	85≤B+<90	хорошо
B	3	80≤B<85	
B-	2,67	75≤B-<80	
C+	2,33	70≤C+<75	удовлетворительно
C	2	65≤C<70	
C-	1,67	60≤C-<65	
D+	1,33	55≤D+<60	
D	1	50≤D<55	
Fx	0	45≤Fx<50	неудовлетворительно
F	0	0<F<45	

Критерии выведения итоговой оценки промежуточной аттестации:

«Отлично» - средняя оценка ≥ 3,67.

«Хорошо» - средняя оценка ≥ 2,67 и ≤ 3,33.

«Удовлетворительно» - средняя оценка ≥ 1,0 и ≤ 2,33.

«Неудовлетворительно» - средняя оценка 0<1,0.

Составитель: к.ф.-м.н., доцент Замонов М.З.