Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент
И.Л. Рева
“ ___ ” _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Образовательная программа: 10.04.01 Информационная безопасность, профиль: Методы и средства обеспечения технической защиты информации

Новосибирск - 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций проверяются при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме зачета, который направлен на оценку сформированности результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-1 и соотнесенных с ними индикаторов.

Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании критериев, приведенных в п. 2, осуществляется оценка уровней достигнутых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенции ОПК-1, закрепленных за дисциплиной.

2. Общая характеристика уровней результатов обучения, соотнесенных с индикаторами достижения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт зачета

по дисциплине «Криптографические методы защиты информации», 3 семестр

1. Методика оценки Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Тестовые задания охватывают все содержание дисциплины «Криптографические методы защиты информации».

Тест состоит из вопросов различного вида и позволяет проверить результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на 5/6 вопросов теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов и не допускает ошибок при решении задач. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 18 до 20 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления, не допускает существенных ошибок при решении задач. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 14 до 17 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от 1/2 до 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает непринципиальные ошибки, например, вычислительные. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 10 до 13 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее 10 баллов.*

3. Шкала оценки Зачет считается сданным, если сумма баллов по всем заданиям билета составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине зачетные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста[1]) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	1. знает требования по криптографической защите информационных систем

Вопросы теста для оценки сформированности компетенции ОПК-1

Вопрос 1. Размер блока шифра AES (бит)

- ☐ **128 ✓**
- ☐ 64
- ☐ 32

(один вариант)

Вопрос 2. Верно ли утверждение: хэш-функции классифицируют на ключевые и бесключевые? *Ответ:*

Решение: да

Вопрос 3. Дополните понятие шифры замены. Шифрами замены называются шифры, которые ___ ____ открытого текста символами того же или другого алфавита.

Ответ:

Решение:. Заменяют символы

Вопрос 4. Какие шифры называются полиалфавитными (многоалфавитными)

Ответ:

Решение: используют более одного алфавита.

Вопрос 5. Размер ключа шифра AES (бит)

- ☐ 128
- ☐ 192
- ☐ 256
- ☐ **Все варианты верны ✓**

(один вариант)

Вопрос 6. Дополните понятие алфавит. Алфавит А любого языка представляет собой множество упорядоченных кодов символов, обозначающих ___ этого языка

Ответ:

Решение: буквы

[1] Правильные ответы выделены галочкой

Вопрос 7. Дополните понятие коллизия. Коллизия - это ситуация, в которой для разных пар входных сообщений формируется ___ хэш- функция

Ответ:

Решение: одинаковая

Вопрос 8. Размер блока шифра ГОСТ 28147-89 (бит)

- ☐ 8
- ☐ **64 ✓**
- ☐ 2

(один вариант)

Вопрос 9. Современные системы шифрования можно разделить на два больших класса. Какие?

Ответ:

Решение: симметричные и ассиметричные.

Вопрос 10. Дополните определение жизненный цикл ключей. Жизненный цикл ключей - это последовательность стадий, которые проходят ключи от момента генерации __ _____ ____

Ответ:

Решение:. до момента уничтожения

Вопрос 11. Какие шифры называются одноалфавитными (моноалфавитными)?

Ответ:

Решение: используют один алфавит

Вопрос 12. Размер ключа шифра ГОСТ 28147-89 (бит)

- ☐ 16
- ☐ 64
- ☐ 32
- ☐ **256 ✓**

(один вариант)

Вопрос 13. Дополните понятие тайнопись. Тайнопись – ____ части или всей информации при использовании стандартного для неѐ способа отображения. По сути, это синоним слова «криптография».

Ответ:

Решение: невоспроизводимость

Вопрос 14. В чем состоит принцип стеганографии

Ответ:

Решение: в сокрытии факта существования секретной информации

Вопрос 15. Количество базовых циклов шифрования в шифре DES

- ☐ 3
- ☐ 4
- ☐ 9
- ☐ **16 ✓**

(один вариант)

Вопрос 16. Дополните понятие цикл или раунд в шифровании. Циклом или раундом в криптографии обычно называется ____ ____ многократного циклического шифрования

Ответ:

Решение: один шаг

Вопрос 17. Какими шифрами являются системы Цезаря, Полибия и простой замены

Ответ:

Решение: одноалфавитными

Вопрос 18. Количество базовых циклов шифрования в шифре ГОСТ 28147-89

- ☐ 2
- ☐ 4
- ☐ 6
- ☐ **32 ✓**

(один вариант)

Вопрос 19. Какие шифры называются симметричными

Ответ:

Решение: используют один ключ для шифрования и расшифрования

Вопрос 20. Какая функция отображает электронные сообщения произвольной длины в значения фиксированной длины?

Ответ:

Решение: Хэш-функция

Вопрос 21. Первым шифром, позволяющим организовать обмен секретными сообщениями по открытой линии связи для лиц, которые не имеют защищенных каналов и секретных ключей, в виде трехступенчатого протокола, является какой шифр?

Ответ:

Решение: шифр Шамира

Вопрос 22. Количество базовых циклов шифрования в шифре AES-128

- ☐ **10 ✓**
- ☐ 2
- ☐ 6
- ☐ 8

(один вариант)

Вопрос 23. Дополните определение шифров перестановки. Шифрами перестановки называют такие шифры, которые ___ ____ шифруемого текста в пределах блока текста фиксированного размера по одному ключу

Ответ:

Решение: переставляют символы

Вопрос 24. Дополните определение Аутентификация — это основа безопасности любой системы, которая заключается в проверке _____ ____ о пользователе сервером.

Ответ:

Решение: подлинности данных

Вопрос 25. Дополните определение кластеризация. Кластеризация - это ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается ____ шифротекст.

Ответ:

Решение: одинаковый

Вопрос 26. Приведите один из примеров идентификации.

Ответ:

Решение: логин, электронная почта, номер телефона

Вопрос 27. Дополните понятие имитовставка в шифре ГОСТ 28147-89. Имитовставка в ГОСТ 28147-89 – это хэш-функция, зависящая от ___ _____ и секретной ключевой информации

Ответ:

Решение: открытых данных

Вопрос 28. В каких единицах измеряется стойкость шифра по Шеннону

Ответ:

Решение: в битах

Вопрос 29. Дополните определение идентификации. Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его _____, однозначно определяющий этого субъекта в информационной системе.

Ответ:

Решение: идентификатор

Вопрос 30. Приведите один из примеров аутентификации.

Ответ:

Решение: пароль, пин-код, секретное слово